



Windows 用户指南

Amazon FSx for Windows File Server



Amazon FSx for Windows File Server: Windows 用户指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

什么是 FSx for Windows File Server ?	1
Amazon FSx 资源	1
访问文件共享	2
安全与数据保护	2
可用性与持久性	2
管理文件系统	3
灵活的价格与性能	3
Amazon FSx 的定价	3
假设	3
先决条件	4
Amazon FSx for Windows File Server 论坛	4
您是否是首次接触 Amazon FSx 的用户 ?	4
FSx for Windows 最佳实践	6
一般最佳实践	6
在转移到生产环境之前测试您的工作负载	6
创建监控计划	6
确保您的文件系统有足够的资源	6
定期备份文件系统	6
安全最佳实操	7
网络安全	7
Active Directory	7
配置文件系统并调整其大小	9
选择部署类型	9
选择存储类型	9
选择吞吐能力	9
增加存储容量和吞吐能力	9
在空闲期间修改吞吐能力	10
开始使用	11
设置你的 AWS 账户	11
.....	12
创建您的文件系统	13
将您的文件共享映射到运行 Windows 服务器的 EC2 实例	18
将数据写入您的文件共享	19
备份您的文件系统	19

清理资源	20
Amazon FSx 文件系统状态	21
支持的客户端、访问方法和环境	22
支持的客户端	22
支持的访问方法	23
使用文件系统的默认 DNS 名称访问文件系统	23
使用 DNS 别名访问文件系统	24
使用 FSx for Windows File Server 文件系统和 DFS 命名空间	24
支持的环境	25
从本地访问 FSx	26
从另一个 VPC、账户、或 AWS 区域 访问 FSx for Windows File Server 文件系统。	26
可用性与持久性	27
选择单可用区或多可用区文件系统部署	27
按部署类型划分的功能支持	27
FSx for Windows File Server 失效转移进程	28
Windows 客户端上的失效转移经验	29
Linux 客户端的失效转移经验	29
在文件系统上测试失效转移	29
使用单可用区和多可用区文件系统资源	29
子网	29
文件系统弹性网络接口	30
使用 Amazon FSx 优化成本	31
存储和吞吐量选择灵活且独立	31
优化存储成本	31
使用存储类型优化成本	31
使用重复数据删除优化存储成本	32
查看使用情况和账单	32
使用 Active Directory	33
使用 AWS Managed Microsoft AD	34
联网先决条件	35
使用资源林隔离模型	40
测试 Active Directory 配置	40
AWS Managed Microsoft AD 在不同的 VPC 或账户中使用	41
验证与 Active Directory 域控制器的连接	42
使用自行管理的 Active Directory	44
自行管理的 Active Directory 的先决条件	47

自行管理的 Active Directory 最佳实践	51
验证 Active Directory 配置	54
将 FSx 加入到自行管理的 Active Directory	58
获取用于 DNS 的正确的文件系统 IP 地址	68
更新自行管理的 Active Directory 配置	68
使用 Microsoft Windows 文件共享	73
访问文件共享	73
在 Amazon EC2 Windows 实例上映射文件共享	73
在 Amazon EC2 Mac 实例上挂载文件共享	75
在 Amazon EC2 Linux 实例上挂载文件共享	78
在未加入 Active Directory 的 Amazon Linux EC2 实例上自动挂载文件共享	83
迁移到 Amazon FSx	86
将文件存储迁移到 FSx for Windows File Server	86
迁移最佳实践	87
使用迁移文件 AWS DataSync	87
使用 Robocopy 迁移文件	89
迁移文件共享配置	93
迁移 DNS 配置以使用 Amazon FSx	94
割接到 Amazon FSx	97
准备割接到 Amazon FSx	98
为 Kerberos 身份验证配置 SPN	98
更新 Amazon FSx 文件系统的 DNS CNAME 记录	101
将 FSx for Windows File Server 与 Microsoft SQL Server 结合使用	103
使用 Amazon FSx 处理 SQL Server 活动数据文件	103
创建持续可用的共享	104
配置 SMB 超时设置	104
使用 Amazon FSx 作为 SMB 文件共享见证	104
将 FSx for Windows File Server 与 Amazon Kendra 结合使用	105
文件系统性能	105
保护您的数据	106
使用备份	106
使用每日自动备份	107
使用用户启动备份	107
AWS Backup 与 Amazon FSx 搭配使用	108
复制备份	109
还原备份	112

删除备份	113
备份大小	113
使用影子副本	114
最佳实践	115
设置卷影副本	115
将卷影副本配置为使用默认设置	117
还原单个文件和文件夹	119
设置卷影副本的最大存储量	121
查看影子副本存储空间	123
删除影子副本的存储空间、计划和所有影子副本	123
创建自定义影子副本计划	124
查看影子副本计划	126
删除影子副本计划	126
创建影子副本	126
查看现有影子副本	126
删除影子副本	127
计划复制	128
管理文件系统	129
使用亚马逊 FSx 定制版 PowerShell	129
启动 Amazon FSx 远程会话 PowerShell	131
DNS 别名	131
DNS 别名状态	133
在 Kerberos 中使用 DNS 别名	133
查看现有 DNS 别名	134
将 DNS 别名与文件系统关联	134
管理现有文件系统上的 DNS 别名	136
管理文件共享	139
管理文件共享 (GUI)	140
使用管理文件共享 PowerShell	141
文件访问审计	144
审核事件日志目标	145
迁移审核控制措施	146
查看事件日志	146
设置文件和文件夹审计控制	154
管理文件访问审计	155
用户会话和打开的文件	160

使用 GUI 管理用户和会话	160
PowerShell 用于管理用户会话和打开文件	163
重复数据删除	164
最佳实践	164
管理重复数据删除	165
启用重复数据删除	166
创建重复数据删除计划	166
修改重复数据删除计划	167
查看节省的空间量	167
重复数据删除问题排查	168
存储配额	170
管理用户存储配额	170
管理传输中加密	171
管理存储配置	172
管理存储容量	172
管理存储类型	185
管理 SSD IOPS	188
管理吞吐能力	192
何时修改吞吐能力	193
如何修改吞吐能力	193
监控吞吐能力更改	195
标记资源	197
有关标签的基本知识	197
标记您的资源	198
标签限制	198
权限和标签	199
维护时段	199
最佳实践	200
一次性管理设置任务	201
持续管理任务可监控您的文件系统	203
使用 DFS 命名空间为文件系统分组	204
设置 DFS 命名空间以为多个文件系统分组	204
监控 FSx for Windows	207
监控工具	207
自动化工具	207
手动监控工具	208

使用监控指标 CloudWatch	209
FSx 指标 CloudWatch	210
如何使用 FSx for Windows File Server 指标	215
性能警告和建议	218
访问 FSx for Windows File Server 指标	219
创建警报	222
CloudTrail 日志	224
CloudTrail 中的 Amazon FSx 信息	225
了解 Amazon FSx 日志文件条目	225
Performance	228
文件系统性能	228
其他性能注意事项	229
延迟	229
吞吐量和 IOPS	229
单客户端性能	229
突增性能	230
吞吐能力和性能	230
选择吞吐能力	232
存储配置和性能	233
HDD 突增性能	233
示例：存储容量和吞吐能力	234
使用 CloudWatch 指标衡量绩效	234
性能问题排查	234
演练	235
演练 1：入门先决条件	235
步骤 1：设置 Active Directory	235
步骤 2：在 Amazon EC2 控制台中启动 Windows 实例	236
步骤 3：连接到您的实例	238
步骤 4：将实例加入 AWS Directory Service 目录	239
演练 2：从备份创建文件系统	241
演练 3：更新现有文件系统	242
演练 4：将 Amazon FSx 与 Amazon AppStream 2.0 结合使用	243
为每位用户提供个人永久存储	243
提供用户间提供共享文件夹	245
演练 5：使用 DNS 别名访问文件系统	246
步骤 1：将 DNS 别名关联到 Amazon FSx 文件系统	247

步骤 2：为 Kerberos 配置服务主体名称 (SPN)	248
步骤 3：更新或创建文件系统的 DNS CNAME 记录	251
使用 GPO 强制执行 Kerberos 身份验证	253
演练 6：使用分片横向扩展性能	254
设置 DFS 命名空间以横向扩展性能	254
演练 7：将备份复制到另一个 AWS 区域	256
安全性	257
数据加密	257
何时使用加密	258
静态加密	258
传输中加密	260
Windows ACL	260
相关链接	261
使用 Amazon VPC 进行文件系统访问控制	261
Amazon VPC 安全组	262
Amazon VPC 网络 ACL	265
身份和访问管理	265
受众	266
使用身份进行身份验证	266
使用策略管理访问	269
如何结合使用 Amazon FSx for Windows File Server 和 IAM	271
基于身份的策略示例	277
AWS 托管策略	279
问题排查	289
在 Amazon FSx 上使用标签	291
使用服务相关角色	296
合规性验证	301
接口 VPC 端点	302
Amazon FSx 接口 VPC 端点注意事项	302
为 Amazon FSx API 创建接口 VPC 端点	303
为 Amazon FSx 创建 VPC 端点策略	303
限额	304
您可以增加的限额	304
每个文件系统的资源限额	305
其他注意事项	306
Microsoft Windows 的特有限额	306

问题排查	307
您无法访问您的文件系统	307
文件系统弹性网络接口已修改或删除	308
连接到文件系统弹性网络接口的弹性 IP 地址已删除	308
文件系统安全组缺少所需的进站或出站规则。	308
计算实例的安全组缺少所需的出站规则	308
计算实例未加入 Active Directory	308
文件共享不存在	308
Active Directory 用户缺少所需权限	309
移除了允许完全控制 NTFS ACL 权限	309
无法使用本地客户端访问文件系统	309
新文件系统未在 DNS 中注册	309
无法使用 DNS 别名访问文件系统	310
无法使用 IP 地址访问文件系统	311
创建文件系统失败	311
已加入 AWS 托管活动目录的文件系统	312
创建加入自我管理的 Active Directory 的文件系统失败	312
文件系统处于配置错误状态	319
文件系统配置错误：Amazon FSx 无法访问 DNS 服务器或域的域控制器。	320
文件系统配置错误：服务账户凭证无效	321
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	321
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	322
文件系统配置错误：服务账户无权访问 OU	322
在 FSx for Windows File Server 上使用远程 PowerShell 排查问题	323
New-F SxSmbShare 命令因单向信任而失败	323
您无法使用 Remote 访问您的文件系统 PowerShell	323
您无法在多可用区或单可用区 2 文件系统上配置 DFS-R	324
存储或吞吐能力更新失败	324
存储容量增加失败，因为 Amazon FSx 无法访问文件系统的 KMS 加密密钥	324
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	325
由于吞吐能力不足，存储容量增加失败	325
吞吐能力更新到 8 MB/s 失败	325
恢复备份时将存储类型切换到 HDD 失败	325
卷影副本问题排查	326
最早的卷影副本丢失	326
我所有的卷影副本都丢失了	327

无法在最近恢复或更新的文件系统上创建 Amazon FSx 备份或访问卷影副本	327
性能问题排查	327
确定文件系统吞吐量和 IOPS 限制	327
什么是网络 I/O，什么是磁盘 I/O？它们为什么不同？	328
为什么网络 I/O 很低时 CPU 或内存利用率仍然很高？	328
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？	328
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？	329
我的指标暂时丢失，我应该担心吗？	329
其他信息	330
设置自定义备份计划	330
架构概述	330
AWS CloudFormation 模板	331
自动部署	331
其他选项	333
使用 DFS 复制	334
设置 DFS 复制	335
为失效转移设置 DFS 命名空间	337
使用维护时段和 FSx 多可用区	340
文档历史记录	341
.....	cccl

什么是 FSx for Windows File Server ?

适用于 Windows File Server 的 Amazon FSx 提供完全托管式的 Microsoft Windows 文件服务器，由完全原生的 Windows 文件系统提供支持。FSx for Windows File Server 的功能、性能和兼容性可轻松实现将企业应用程序直接迁移至 AWS Cloud。

Amazon FSx 支持一系列广泛的企业 Windows 工作负载，并在 Microsoft Windows Server 上构建了完全托管的文件存储。Amazon FSx 本机支持 Windows 文件系统功能和业界标准的服务器消息块 (SMB) 协议，以便通过网络访问文件存储。Amazon FSx 针对中的企业应用程序进行了优化 AWS Cloud，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。

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

作为一项完全托管式服务，FSx for Windows File Server 消除了设置并预置文件服务器和存储卷的管理开销。此外，Amazon FSx 可使 Windows 软件保持最新，检测并排除硬件故障以及执行备份。它还提供了与其他 AWS 服务（如 [AWS IAM](#)、[AWS Directory Service for Microsoft Active Directory](#)、[Amazon WorkSpaces](#) 和）的丰富集成 [AWS CloudTrail](#)。 [AWS Key Management Service](#)

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

文件系统和备份是 Amazon FSx 中的主要资源。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 和吞吐能力（以 MB/s 为单位）。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](#)。

for Windows File Server 的 fsX 备份非常耐用，而且 file-system-consistent 是增量的。为确保文件系统一致性，Amazon FSx 使用 Microsoft Windows 中的卷影复制服务 (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](#)。

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 Microsoft Windows 文件共享](#)。

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

Amazon FSx 可以通过采用 SMB 协议 (支持 2.0 到 3.1.1 版本) 的计算实例进行访问。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 实例和虚拟机上的 VMware Cloud 上映射亚马逊 FSx 文件共享。WorkSpaces AWS

您可以使用 AWS Direct Connect 或 AWS VPN 从本地计算实例访问文件共享。除了访问与文件系统处于相同 VPC、AWS 账户和 AWS 区域的文件共享之外，您还可以访问位于不同 Amazon VPC、账户或区域中的计算实例上的共享。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 [支持的访问方法](#)。

安全与数据保护

Amazon FSx 提供多个级别的安全性和合规性，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 AWS Key Management Service (文件系统和备份 AWS 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。

Amazon FSx 通过 Windows 访问控制列表 (ACL) 提供文件和文件夹级别的访问控制。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 AWS 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 FSx 与集成 AWS CloudTrail 以监控和记录您的 API 调用，让您查看用户对您的 Amazon FSx 资源执行的操作。

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 FSx 中的安全性](#)。

可用性与持久性

FSx for Windows File Server 为文件系统提供两种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。AWS 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](#)。

管理文件系统

您可以使用自定义远程管理命令 PowerShell 管理适用于 Windows File Server 文件系统的 FSx，或者在某些情况下使用 Windows 原生 GUI。要了解有关管理 Amazon FSx 文件系统的更多信息，请参阅[管理文件系统](#)。

灵活的价格与性能

FSx for Windows File Server 提供固态硬盘 (SSD) 和硬盘驱动器 (HDD) 存储类型，为您打造灵活的价格与性能之选。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。

通过 FSx for Windows File Server，您可以单独进行文件系统存储、固态硬盘 IOPS 和吞吐量的预配置操作，获得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。有关更多信息，请参阅[使用 Amazon FSx 优化成本](#)。

Amazon FSx 的定价

使用 Amazon FSx，无需预付硬件或软件成本。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。有关与该服务相关的定价和费用的信息，请参阅[Amazon FSx for Windows File Server 定价](#)。

假设

要使用 Amazon FSx，您需要一个 AWS 账户，其中包含在支持类型的 AWS 环境中运行 VMware Cloud 的 Amazon EC2 实例、实例、AppStream 2.0 实例或虚拟机。WorkSpaces

在本指南中，我们做出了以下假设：

- 如果您使用的是 Amazon EC2，则假设您足够了解 Amazon EC2。有关如何使用 Amazon EC2 的更多信息，请参阅[Amazon Elastic Compute Cloud 文档](#)。
- 如果您正在使用 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](#)。
- 如果你在上面使用 VMware Cloud AWS，我们假设你已经熟悉了。有关更多信息，请参阅[VMware Cloud on AWS](#)。

- 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，您需要具备以下条件：

- 具有创建 Amazon FSx 文件和 Amazon EC2 实例所需权限的 AWS 账户。有关更多信息，请参阅 [设置你的 AWS 账户](#)。
- 一个 Amazon EC2 实例，该实例在虚拟私有云 (VPC) 中运行 Microsoft Windows Server，并且基于您希望与您的 Amazon FSx 文件系统关联的 Amazon VPC 服务。有关如何创建实例的信息，请参阅亚马逊 EC2 用户指南中的 [Amazon EC2 Windows 实例入门](#)。
- Amazon FSx 与 Microsoft Active Directory 共同执行用户身份验证和访问控制。在创建 Amazon FSx 文件系统时，您可以将其加入 Microsoft Active Directory。有关更多信息，请参阅 [在 FSx for Windows File Server 中使用 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。如果更改了，则您需要添加必要的规则，允许从 Amazon EC2 实例到 Amazon FSx 文件系统的网络流量。有关更多详细信息，请参阅 [Amazon FSx 中的安全性](#)。
- 安装并配置 AWS Command Line Interface (AWS CLI)。支持 1.9.12 和更高版本。有关更多信息，请参阅《AWS Command Line Interface 用户指南》中的 [安装、更新和卸载 AWS CLI](#)。

Note

你可以用 `aws --version` 命令检查 AWS CLI 你正在使用的版本。

Amazon FSx for Windows File Server 论坛

如果您在使用 Amazon FSx 时遇到问题，请使用 [论坛](#)。

您是否是首次接触 Amazon FSx 的用户？

如果您是 Amazon FSx 新用户，我们建议您按顺序阅读以下内容：

1. 如果您已准备好创建第一个 Amazon FSx 文件系统，请参阅 [开始使用适用于 Windows File Server 的亚马逊 FSx](#)。
2. 有关性能的信息，请参阅 [FSx for Windows File Server 性能](#)。

3. 有关 Amazon FSx 安全性详细信息，请参阅[Amazon FSx 中的安全性](#)。
4. 有关 Amazon FSx API 的更多信息，请参阅[Amazon FSx API 参考](#)。

FSx for Windows File Server 最佳实践

在使用 Amazon FSx for Windows File Server 时，我们建议您遵循以下最佳实践。单击以下链接，了解有关所讨论主题的更多信息。

主题

- [一般最佳实践](#)
- [安全最佳实操](#)
- [配置文件系统并调整其大小](#)

一般最佳实践

在转移到生产环境之前测试您的工作负载

我们建议使用与生产环境具有相同配置的暂存环境测试工作负载。例如，使用相同的 Active Directory (AD) 和网络配置、文件系统大小和配置以及 Windows 功能，例如重复数据删除和影子副本。在模拟所需生产流量的暂存环境中运行测试工作负载有助于确保进程顺利运行。

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文件系统的预期恢复行为。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](#)。

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。通过监控您的 Amazon FSx 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[监控 FSx for Windows File Server](#)。

定期备份文件系统

定期备份能让您满足数据留存、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 AWS Backup 集中备份解决方案 AWS 服务。AWS 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。

安全最佳实操

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 以实现您的安全性和合规性目标的更多详细信息，请参阅 [Amazon FSx 中的安全性](#)。

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 文件系统可通过虚拟私有云 (VPC) 中的弹性网络接口 (ENI) 访问，该接口与文件系统关联。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 ACL

您可以使用安全组和网络访问控制列表 (ACL) 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 ACL 允许端口流量。有关更多信息，请参阅 [Amazon VPC 安全组](#)。

Active Directory

创建 Amazon FSx 文件系统时，您可以将其加入您的 Microsoft AD 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 AD 账户连接到文件共享并访问其中的文件和文件夹。此外，您还可以将现有安全 ACL 配置迁移到 Amazon FSx，而无需进行任何修改。Amazon FSx 为 Active Directory 提供了两个选项：AWS 托管的 Microsoft AD 或自行管理的 Microsoft AD。

如果您使用的是 AWS 托管的 Microsoft AD，我们建议您保留 AD 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 AD，则还可以通过其他选项配置文件系统。在结合使用 Amazon FSx 与自行管理的 Microsoft AD 时，我们建议您遵循以下最佳实践：

- 将子网分配给单个 AD 站点：如果您的 AD 环境有大量域控制器，请使用 Active Directory 站点和服务将 Amazon 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 AD 站点。确保 VPC 安全组、VPC 网络 ACL、您的 DC 上的 Windows 防火墙规则以及您的 AD 基础设施中的任何其他网络路由控制允许 Amazon FSx 通过所需端口进行通信。这允许 Windows 在无法使用分配的 AD 站点时还原至其他 DC。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)：为您的 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 的先决条件](#) 和 [向 Amazon FSx 服务账户委派权限](#)。
- 持续验证您的 Amazon FSx 配置：创建 Amazon FSx 文件系统之前，针对您的 AD 配置运行 [Amazon FSx Active Directory 验证工具](#)，以验证您的配置是否适用于 Amazon FSx，并发现该工具可能暴露的任何警告和错误。

避免因 AD 配置错误而失去可用性

将 Amazon FSx 与自我托管式 Microsoft AD 配合使用时，拥有有效的 AD 配置对于创建文件系统，以及确保持续的操作和可用性都非常重要。在故障恢复事件、例行维护事件和吞吐能力更新操作期间，Amazon FSx 会将文件服务器资源重新加入您的 Active Directory。如果 AD 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 FSx 更新您的 AD 配置：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 AD 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 AD 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 和监控 Amazon FSx 文件系统的运行状况](#)。EventBridge AWS Lambda
- 定期验证您的 AD 配置：如果您想主动检测 AD 配置错误，我们建议您针对您的 AD 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 FSx 创建的计算机对象：Amazon FSx 使用您提供的服务账户和权限在您的 AD 中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。

Windows ACL

通过 Amazon FSx，您可以使用标准的 Windows 访问控制列表 (ACL) 进行精细的共享、文件和文件夹级别的访问控制。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 ACL。

- 请勿更改 SYSTEM 用户的 NTFS ACL 权限：Amazon FSx 要求 SYSTEM 用户拥有对文件系统内所有文件夹的完全控制 NTFS ACL 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。

如果您决定使用 HDD 存储，请测试您的文件系统以确保它能够满足您的性能要求。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](#)。

您可以随时使用 Amazon FSx 控制台或 Amazon FSx API 将存储类型从 HDD 升级到 SSD。有关更多信息，请参阅 [管理存储类型](#)。

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。我们建议在文件系统上始终保持至少 10% 的可用存储容量。我们还建议在扩展存储空间之前将存储容量至少增加 20%，因为在扩展过程中无法增加存储容量。您可以使用 FreeStorage 容量 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 workload 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 workload 需求何时接近或超过性能限制，从而确定文件系统对 workload 的配置是否不足。

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，大多数 workload 对性能的影响微乎其微，但是具有大型活动数据集的写入量大的应用程序的写入性能可能会暂时降低一半。

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 workload，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](#)。

开始使用适用于 Windows File Server 的亚马逊 FSx

接下来，你可以学习如何开始使用适用于 Windows File Server 的 FSx。此入门练习包括以下步骤。

1. 注册 AWS 账户 并在该帐户中创建管理员用户。
2. 使用创建 AWS 托管的 Microsoft AD 活动目录 AWS Directory Service。您将把您的文件系统和计算实例加入活动目录。
3. 创建运行微软 Windows Server 的亚马逊弹性计算云计算实例。您将使用此实例访问您的文件系统。
4. 使用亚马逊 FSx 控制台为 Windows 文件服务器创建亚马逊 FSx 文件系统。
5. 将您的文件系统映射到 EC2 实例
6. 将数据写入您的文件系统。
7. 备份您的文件系统。
8. 清理您创建的资源。

主题

- [设置你的 AWS 账户](#)
- [创建您的文件系统](#)
- [将您的文件共享映射到运行 Windows 服务器的 EC2 实例](#)
- [将数据写入您的文件共享](#)
- [备份您的文件系统](#)
- [清理资源](#)
- [Amazon FSx 文件系统状态](#)

设置你的 AWS 账户

首次使用 Amazon FSx 前，请完成以下任务：

1. [注册获取 AWS 账户](#)
2. [创建具有管理访问权限的用户](#)

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

报名参加 AWS 账户

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

在注册时，将接到一通电话，要求使用电话键盘输入一个验证码。

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

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

创建具有管理访问权限的用户

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

保护你的 AWS 账户根用户

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

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

2. 为您的根用户启用多重身份验证 (MFA)。

有关说明，请参阅 [IAM 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备 \(控制台\)](#)。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 [启用 AWS IAM Identity Center](#)。

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

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

以具有管理访问权限的用户身份登录

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

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

将访问权限分配给其他用户

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

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 [创建权限集](#)。

2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 [添加组](#)。

创建您的文件系统

要创建您的亚马逊 FSx 文件系统，您必须创建 Windows 亚马逊弹性计算云 (Amazon EC2) 实例和目录。AWS Directory Service 如果您尚未进行设置，请参阅 [演练 1：入门先决条件](#)。

创建您的文件系统（控制台）

1. 通过以下网址打开 Amazon FSx 控制台：<https://console.aws.amazon.com/fsx/>。
2. 在控制面板上，选择创建文件系统以启动文件系统创建向导。
3. 在选择文件系统类型页面上，选择 FSx for Windows File Server，然后选择下一步。显示创建文件系统页面。
4. 对于创建方法，选择标准创建。

文件系统详情

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。
 - 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 for Windows File Server 提供固态硬盘 (SSD) 和硬盘驱动器 (HDD) 存储类型。SSD 存储专为性能最高、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 [使用存储类型优化成本](#)。

4. 在预置的 SSD IOPS 中，您可以选择自动或用户预置模式。

若选择“自动”模式，FSx for Windows File Server 会自动扩展您的 SSD IOPS，使每 GiB 的存储容量保持为 3 SSD IOPS。如果您选择用户配置模式，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

若要启用文件访问审计，则必须选择 32 MB/s 或更大的吞吐能力。有关更多信息，请参阅 [文件访问审计](#)。

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 AWS Directory Service 目录和 Amazon 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 AWS 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。

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

添加与您要用于访问文件系统的客户端计算实例关联的 IP 地址或安全组 ID。

- b. 添加出站规则，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 AWS 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 AWS Managed Microsoft AD 安全组规则。如果是，请确保此安全组具有必需的允许您的 Amazon FSx 文件系统的流量入站规则。有关必需的入站规则的更多信息，请参阅《AWS Directory Service 管理指南》中的 [AWS 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. 多可用区文件系统有主文件服务器和备用文件服务器，每个服务器位于自己的可用区和子网中。如果您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。

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 AWS 由管理的 Microsoft Active Directory 域，请选择托管 Microsoft Active Directory AWS，然后从列表中选择您的 AWS Directory Service 目录。有关更多信息，请参阅 [在 FSx for Windows File Server 中使用 Microsoft Active Directory](#)。

如果你想将文件系统加入自我管理的 Microsoft Active Directory 域，请选择自我管理的 Microsoft Active Directory，然后为你的活动目录提供以下详细信息。有关更多信息，请参阅 [将 Amazon FSX 与自行管理的 Microsoft Active Directory 结合使用](#)。

- 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 AWS Directory Service 和自行管理的 Active Directory 域名。Amazon FSx 需要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 AWS Virtual Private Network VPC 对等 AWS Direct Connect 互连或 AWS Transit Gateway 关联。

- DNS 服务器 IP 地址 – 域的 DNS 服务器的 IPv4 地址

Note

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

- 服务账户用户名 – 现有 Active Directory 中服务账户的用户名。请勿包含域前缀或后缀。

- 服务账户密码 – 服务账户的密码。
- (可选) 组织单位 (OU) – 文件系统要加入的组织单位的可分辨路径名称。
- (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 [向 Amazon FSx 服务账户委派权限](#)。

加密、审计和访问 (DNS 别名)

1. 对于加密，选择用于 AWS 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) AWS KMS、现有密钥或客户托管的密钥。有关更多信息，请参阅 [静态加密](#)。
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[创建文件系统时启用文件访问审计 \(控制台 \)](#)。
3. 在访问 – 可选项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](#)。

Backup 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](#)。

1. 对于每日自动备份，默认情况下处于启用状态。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，则它们将在称为备份窗口的时间段内进行。您可以使用默认窗口，也可以选择自动备份窗口的开始时间。
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执行的备份 AWS Backup。
4. 对于标签 – 可选，您可以输入键和价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 [标记 Amazon FSx 资源](#)。

选择 下一步。

查看您的配置并创建

1. 检查创建文件系统页面上显示的文件系统配置。您可以查看创建文件系统后可以修改哪些文件系统设置和不能修改哪些文件系统设置，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。

将您的文件共享映射到运行 Windows 服务器的 EC2 实例

现在，您可以将亚马逊 FSX 文件系统挂载到已加入目录的基于微软 Windows 的 Amazon EC2 实例上。AWS Directory Service 文件共享的名称与文件系统的名称不同。

使用 GUI 将文件共享映射到 Amazon EC2 Windows 实例

1. 必须先启动 EC2 实例并将其加入一个 AWS Directory Service for Microsoft Active Directory 到，然后才能在 Windows 实例上挂载文件共享。要执行此操作，请选择《AWS Directory Service 管理指南》中以下过程之一：
 - [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 Amazon 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 名称或使用您选择的 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[演练 5：使用 DNS 别名访问文件系统](#)。

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`。您可以在 Amazon FSx 控制台 <https://console.aws.amazon.com/fsx/>、Windows 文件服务器 > 网络与安全部分或者在 API 命令的 `CreateFileSystem` 或 `DescribeFileSystems` 响应中找到 DNS 名称。

- 对于加入 AWS 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
```

- 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。

将数据写入您的文件共享

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。

备份您的文件系统

现在，您已可以开始使用您的 Amazon FSx 文件系统及其文件共享，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. 通过以下网址打开 Amazon FSx 控制台：<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。

清理资源

完成本练习后，您应按照以下步骤清理资源并保护您的 AWS 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. 通过以下网址打开 Amazon FSx 控制台：<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. 如果您在中为本练习创建了 AWS Directory Service 目录[演练 1：入门先决条件](#)，则可以立即将其删除。有关更多信息，请参阅《AWS Directory Service 管理指南》中的[删除目录](#)。

Amazon FSx 文件系统状态

您可以使用 [Amazon FSx 控制台](#)、[describe-file-systems AWS CLI 命令](#) 或 [API 操作系统](#) 来查看 Amazon FSx 文件系统的状态。[DescribeFile](#)

文件系统状态	描述
AVAILABLE	文件系统处于正常状态，可以访问并可供使用。
CREATING	Amazon FSx 正在创建新的文件系统。
DELETING	Amazon FSx 正在删除现有文件系统。
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	<ul style="list-style-type: none"> Amazon FSx 无法在创建一个新文件系统的同时再创建新的文件系统。 文件系统不可用。 文件系统故障，且 Amazon FSx 无法恢复。 Amazon FSx 无法创建备份。

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

无论是从 AWS，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](#)
- [支持的访问方法](#)
- [支持的环境](#)

支持的客户端

Amazon FSx 支持通过各种计算实例和操作系统连接您的文件系统。它通过支持使用服务器消息块 (SMB) 协议 (版本 2.0 到 3.1.1) 进行访问来实现这一点。

支持将以下 AWS 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[访问文件共享](#)。
- 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 AWS 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 AWS 博客文章 [Using Amazon FSx with Amazon AppStream 2.0](#)。
- AWS 环境下运行在 VMware Cloud 中的 VM – 要了解更多信息，请参阅 AWS 博客文章 [Storing and Sharing Files with FSx for Windows File Server in a VMware Cloud on AWS 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

支持的访问方法

您可以将以下访问方法与 Amazon FSx 结合使用。

使用文件系统的默认 DNS 名称访问文件系统

FSx for Windows File Server 为每个文件系统提供了一个域名系统 (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 Microsoft Windows 文件共享](#)。

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 DNS 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 AWS 托管的 Microsoft Active Directory 的所有单可用区文件系统的 DNS 名称如下所示：`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 名称如下所示：`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 AWS 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 \(KFSO\)](#)。

使用 DNS 别名访问文件系统

FSx for Windows File Server 为每个文件系统提供了一个 DNS 名称，可以用于访问文件共享。您还可以为 FSx for Windows File Server 文件系统注册别名来允许通过 DNS 名称，而非 Amazon FSx 创建的默认 DNS 名称访问 Amazon FSx。

使用 DNS 别名，您可以将 Windows 文件共享数据移至 Amazon FSx，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。有关更多信息，请参阅[管理 DNS 别名](#)。

Kerberos 身份验证使用 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)。

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。

有关更多信息，请参阅[演练 5：使用 DNS 别名访问文件系统](#)。

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

FSx for Windows File Server 支持使用 Microsoft 分布式文件系统 (DFS) 命名空间。您可以使用 DFS 命名空间将多个文件系统上的文件共享组织到一个用于访问整个文件数据集的公共文件夹结构 (命名空间)。您可以使用 DFS 命名空间中的名称来访问您的 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 命名空间为多个文件系统分组](#)。

支持的环境

您可以从与您的文件系统位于同一 VPC 中的资源访问您的文件系统。有关更多信息和详细说明，请参阅[演练 1：入门先决条件](#)。

您还可以通过本地资源以及其他 VPC、AWS 账户或 AWS 区域中的资源访问 2019 年 2 月 22 日之后创建的文件系统。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 块	✓	✓	✓
创建文件系统的 VPC 的辅助 CIDR		IP 地址在 RFC 1918 私有 IP 地址范围内的客户端：	IP 地址在以下 CIDR 块范围之外的客户端：
其他 CIDR 或对等网络		<ul style="list-style-type: none"> • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16 	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](#)。

下面，您可以看到有关如何从本地以及不同的 VPC、AWS 账户或 AWS 区域访问 FSx for Windows File Server 文件系统的信息。

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

FSx for Windows File Server 支持使用 AWS Direct Connect 或 AWS VPN 从本地计算实例访问您的文件系统。有了对 AWS 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 AWS 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 AWS Direct Connect 的更多信息，请参阅《[AWS Direct Connect 用户指南](#)》。有关设置 AWS VPN 连接的更多信息，请参阅《Amazon VPC 用户指南》中的 [VPN 连接](#)。

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](#)》。

从另一个 VPC、账户、或 AWS 区域访问 FSx for Windows File Server 文件系统。

您可以从不同于您的文件系统所关联的 VPC、AWS 账户或 AWS 区域中的计算实例访问 FSx for Windows File Server 文件系统。为此，您可以使用 VPC 对等连接或传输网关。使用 VPC 对等连接或中转网关连接 VPC 时，一个 VPC 中的计算实例可以访问另一个 VPC 中的 Amazon FSx 文件系统。即使 VPC 属于不同账户，或位于不同的 AWS 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 AWS 区域或两个 AWS 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。

可用性与持久性：单可用区和多可用区文件系统

Amazon FSx for Windows File Server 提供两种文件系统部署类型：单可用区和多可用区。以下各节提供的信息可帮助您为工作负载选择正确的部署类型。有关该服务的可用性 SLA（服务等级协议）的信息，请参阅 [Amazon FSx 服务等级协议](#)。

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。在这些故障恢复事件期间，以及在为文件系统配置的维护时段内进行计划的文件系统维护期间，单可用区文件系统处于离线状态，时间通常不到 20 分钟。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。这样您就可以继续访问数据，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

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。在计划内的文件系统维护或计划外服务中断的情况下，可用性需求宽松的工作负载可以承受长达 20 分钟的可用性暂时丧失，而 RPO 需求宽松的工作负载在极少数情况下可以容忍自最近一次备份以来的数据更新丢失。

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	✓		✓	✓	✓	

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 2	✓	✓	✓		✓	✓*
多可用区	✓	✓	✓		✓	✓*

Note

* 虽然您可以在单可用区 2 文件系统中创建持续可用的 (CA) 共享，但在 SQL Server HA 部署中，您应该在多可用区文件系统中使用 CA 共享。

FSx for Windows File Server 失效转移进程

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故障切换和回切的短时间内，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，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，此进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。

在文件系统中测试失效转移

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](#)。

使用单可用区和多可用区文件系统资源

子网

创建 VPC 时，其可跨越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。每个子网都必须完全位于一个可用区之内，不能跨越多个可用区。创建单可用区 Amazon FSx 文件系统时，您需要为该文件系统指定单个子网。您选择的子网将定义您创建的文件系统中的可用区。

创建多可用区文件系统时需要指定两个子网，分别用于首选文件服务器和备用文件服务器。您选择的两个子网必须位于同一 AWS 区域内的不同可用区中。

对于AWS 应用程序内，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，以最大限度地减少延迟。

文件系统弹性网络接口

当您创建 Amazon FSx 文件系统时，Amazon FSx 会在您与文件系统关联的 [Amazon Virtual Private Cloud \(VPC \)](#) 中预置一个或多个[弹性网络接口](#)。此类网络接口允许您的客户端与 FSx for Windows File Server 文件系统通信。该网络接口虽然是您账户 VPC 的一部分，但仍被视为在 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

您不得修改或删除与您的文件系统关联的弹性网络接口。修改或删除该网络接口可能会导致永久丢失您的 VPC 和文件系统之间的连接。

下表汇总了 FSx for Windows File Server 文件系统部署类型的子网、弹性网络接口和 IP 地址资源：

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

创建文件系统后，在删除文件系统之前，其 IP 地址不会更改。

Important

Amazon FSx 不支持从公共互联网访问文件系统，也不支持将文件系统向公共互联网公开。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 Amazon FSx 优化成本

FSx for Windows File Server 提供了多种功能，可帮助您根据应用程序需求优化总拥有成本（TCO）。您可以选择存储类型（HDD 或 SSD），以实现应用程序成本和性能需求的适当平衡。您可以灵活地将吞吐能力与存储容量分开选择，以优化成本。而且，您可以使用重复数据删除来消除文件系统上的冗余数据，从而优化存储成本。

主题

- [存储和吞吐量选择灵活且独立](#)
- [优化存储成本](#)
- [查看使用情况和账单](#)

存储和吞吐量选择灵活且独立

借助 FSx for Windows File Server，您可以独立配置文件系统的存储、SSD IOPS 和吞吐能力。这使您能够灵活实现成本和性能的适当组合。例如，您可以选择为冷（通常为非活动）工作负载提供吞吐能力相对较低的大量存储，以节省不必要的吞吐量成本。或者，再举一个例子，您可以选择在相对较小的存储容量中提供较大的吞吐能力。吞吐能力越高，用于文件服务器缓存的内存量也越大。您可以利用文件服务器上的快速缓存来优化主动访问数据的性能。有关更多信息，请参阅[FSx for Windows File Server 性能](#)。

创建文件系统后，您可以随时增加存储容量。有关更多信息，请参阅[管理存储容量](#)。创建文件系统后，您可以随时独立于存储容量扩展 SSD IOPS。有关更多信息，请参阅[管理 SSD IOPS](#)。您可以随时增加或减少吞吐能力，从而灵活地满足不断变化的性能需求。有关更多信息，请参阅[管理吞吐能力](#)。

优化存储成本

您可以通过多种方式借助 Amazon FSx 优化存储成本，如下所述。

使用存储类型优化成本

FSx for Windows File Server 提供两种类型的存储 – 硬盘驱动器（HDD）和固态硬盘（SSD），使您能够优化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。有关更多信息，请参阅[延迟](#)和[Amazon FSx for Windows File Server 定价](#)。

使用重复数据删除优化存储成本

大型数据集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 [重复数据删除](#)。

查看使用情况和账单

您可以通过 AWS Billing 控制面板或 AWS Cost Explorer 查看文件系统的使用情况，包括存储容量、吞吐能力、备份和数据传输。这些工具允许您查看资源的使用情况，并按使用类型、区域和其他相关标准进行筛选和分组。请注意，要查看单个文件系统或单个文件系统备份的使用情况，您需要启用该特定资源的标签并启用基于标签的账单报告。有关更多信息，请参阅《AWS Billing 用户指南》中的 [使用 AWS 成本分配标签](#)。

在 FSx for Windows File Server 中使用 Microsoft Active Directory

亚马逊 FSx 与微软 Active Directory 合作，与你现有的微软 Windows 环境集成。Active Directory 是 Microsoft 目录服务，用于存储有关网络上对象的信息，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。

创建 Amazon FSx 文件系统时，您可以将其加入您的 Microsoft AD 域，以提供用户身份验证以及文件和文件夹级别的访问控制。然后，您的用户可以使用其在 Active Directory 中的现有用户身份自行进行身份验证并访问 Amazon FSx 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以及这些项目的安全访问控制列表 (ACL) 配置迁移到 Amazon FSx，而无需进行任何修改。

Amazon FSx 为您提供了 [将 Amazon FSx 与 AWS Directory Service for Microsoft Active Directory](#) 和 [将 Amazon FSX 与自行管理的 Microsoft Active Directory 结合使用](#) 两个选项，使您可以通过 Active Directory 使用 FSx for Windows File Server 文件系统。

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

创建文件系统后，您无法更改已加入的 Microsoft AD 的以下属性：

- DomainName
- OrganizationalUnitDistinguishedName
- FileSystemAdministratorsGroup

但是，你可以通过备份创建新的文件系统，并在 Microsoft Active Directory 集成配置中为新文件系统更改这些属性。有关更多信息，请参阅 [演练 2：从备份创建文件系统](#)。

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 AWS Directory Service for Microsoft Active Directory](#)
- [将 Amazon FSX 与自行管理的 Microsoft Active Directory 结合使用](#)

将 Amazon FSx 与 AWS Directory Service for Microsoft Active Directory

AWS Directory Service for Microsoft Active Directory (AWS 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 AWS Managed Microsoft AD 管理身份和设备，我们建议您将您的 Amazon FSx 文件系统与集成。AWS Managed Microsoft AD 通过这样做，您将获得使用 Amazon FSx 的交钥匙解决方案。AWS Managed Microsoft AD AWS 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，使您能够专注于有效地操作自己的工作负载。

要在您的 AWS Managed Microsoft AD 设置中使用亚马逊 FSx，您可以使用亚马逊 FSx 控制台。在控制台中为 Windows File Server 文件系统创建新的 FSx 时，请在 Windows 身份验证部分下 AWS 选择托管 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[创建您的文件系统](#)。

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[将 Amazon FSX 与自行管理的 Microsoft Active Directory 结合使用](#)。

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，您可以将您的资源（包括您的 Amazon FSx 文件系统）隔离到与您的用户所在的单独的 Active Directory 林中。

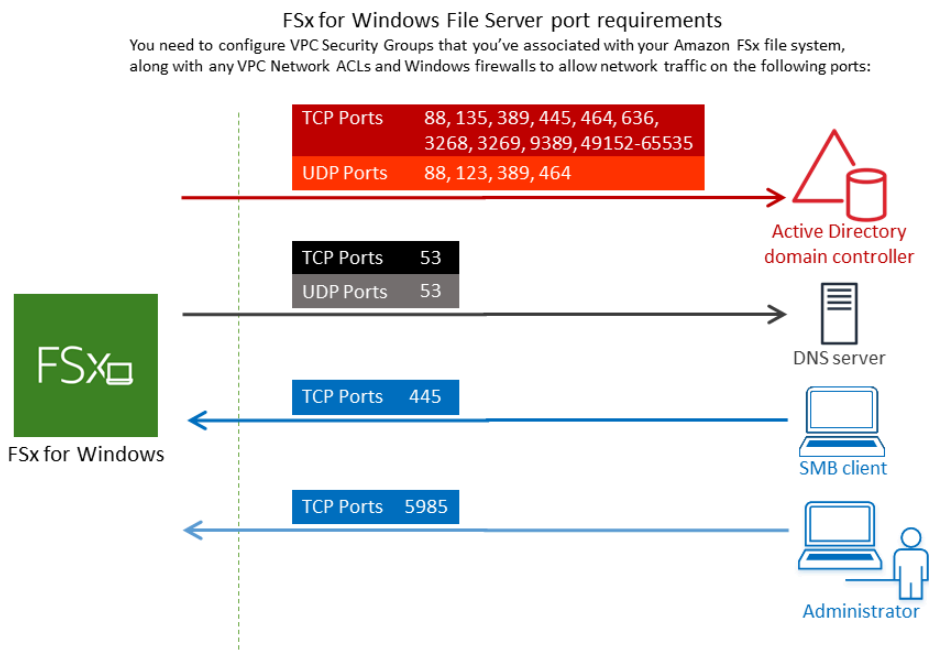
⚠ Important

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

联网先决条件

在创建加入 AWS 微软托管 Active Directory 域的 Windows File Server 文件系统的 FSx 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	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)

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 (DCERPM)
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 (LDAP)
TCP	3268	Microsoft 全局目录
TCP	3269	基于 SSL 的 Microsoft 全局目录

协议	端口	角色
TCP	5985	WinRM (PowerShell 远程管理)
TCP	9389	微软 AD DS Web 服务, PowerShell
TCP	49152 - 65535	RPC 的临时端口

 Important

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

Note

如果您使用的是 VPC 网络 ACL，则还必须允许动态端口（49152-65535）上的出站流量。

- 如果您要将您的 Amazon FSx 文件系统连接到其他 VPC 或账户中的托管 Microsoft Active Directory，请确保该 VPC 与您要在其中创建文件系统的亚马逊 VPC 之间的连接。有关更多信息，请参阅 [在不同的 VPC 或账户 AWS Managed Microsoft AD 中使用 Amazon FSx](#)。

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 AWS Managed Microsoft AD 设置。然后，您可以在您创建的 AWS 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 AWS 托管林信任公司域林。

您的公司域扮演可信域的角色，而 AWS 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 FSx 仅与托管的域进行交互。然后，托管的域会将身份验证请求传递到您的企业域。

测试 Active Directory 配置

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

当你使用适用于 Windows File Server 的 FSx 时 AWS Directory Service for Microsoft Active Directory，以下相关资源可以为你提供帮助：

- 《AWS Directory Service 管理指南》AWS [中的“Directory Service”是什么](#)
- 在《[AWS Directory Service 管理指南](#)》中创建您的托管活动目录

- 《AWS Directory Service 管理指南》中的[何时创建信任关系](#)。
- [演练 1：入门先决条件](#)

在不同的 VPC 或账户 AWS Managed Microsoft AD 中使用 Amazon FSx

您可以使用 VPC 对等连接将适用于 Windows File Server 文件系统的 FSx 加入到 AWS Managed Microsoft AD 同一账户内不同 VPC 中的目录。您还可以使用 AWS Managed Microsoft AD 目录共享将您的文件系统加入到不同 AWS 账户下的目录。

Note

您只能选择与 AWS Managed Microsoft AD 您的文件系统 AWS 区域 相同的。如果要使用跨区域 VPC 对等互连设置，则应使用自我管理的 Microsoft Active Directory。有关更多信息，请参阅 [将 Amazon FSX 与自行管理的 Microsoft Active Directory 结合使用](#)。

将您的文件系统加入其他 VPC 中的工作流程包括以下步骤：AWS Managed Microsoft AD

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《AWS Directory Service 管理指南》中的[共享目录](#)。

要设置您的网络环境，您可以使用 AWS Transit Gateway 或 Amazon VPC 并创建 VPC 对等连接。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。您可以使用 VPC 对等连接同一 AWS 区域内或区域之间 AWS 的 VPC。有关 VPC 对等的更多信息，请参阅《Amazon VPC 对等指南》中的[什么是 VPC 对等？](#)。

将文件系统加入到与文件系统账户不同的 AWS Managed Microsoft AD 目录时，还有另一个先决条件。你还需要与其他账户共享你的 Microsoft 活动目录。为此，您可以使用 AWS 托管 Microsoft Active

Directory 的目录共享功能。要了解更多信息，请参阅《AWS 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。无论你是在托管 Microsoft Active Directory 中使用适用于 Windows File Server AWS 的 FSx，还是使用自我管理的 Active Directory 配置，你都可以使用这个测试。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全套网络连接检查。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《AWS Directory Service 管理指南》中的[手动加入 Windows 实例](#)。
3. 连接到您的 EC2 实例。有关更多信息，请参阅 Amazon 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. 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}, @
Server                             10.0.75.243
UdpDetails                         {@{Port=88; Result=Timed Out; Description=Kerberos authentication}, @
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


```

## 将 Amazon FSX 与自行管理的 Microsoft Active Directory 结合使用

如果您的组织在本地或云端自行管理的 Active Directory 上管理身份和设备，则您可以将您的 Amazon FSx 文件系统直接加入现有的自我管理的 Active Directory 域。要将 Amazon FSx 与之搭配使用 AWS Managed Microsoft AD，您可以使用亚马逊 FSx 控制台。在控制台中创建新的 FSx for Windows File Server 文件系统时，请选择 Windows 身份验证下的自行管理的 Microsoft Active Directory。为自行管理的 Active Directory 提供以下详细信息：

- 自行管理的目录的完全限定域名

**Note**

域名不能采用单标签域 ( SLD ) 格式。Amazon FSx 目前不支持 SLD 域。

**Note**

对于单可用区 2 和多可用区文件系统，Active Directory 域名不得超过 47 个字符。

- 域的 DNS 服务器的 IP 地址

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

对于 2020 年 12 月 17 日之前创建的文件系统

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

对于 2020 年 12 月 17 日之后创建的文件系统

IP 地址可以位于任何范围内，但以下情况除外：

- 与 Amazon Web Services 在该 AWS 地区拥有的 IP 地址冲突的 IP 地址。有关按地区划分的 AWS 拥有的 IP 地址列表，请参阅 [AWS IP 地址范围](#)。
- 以下 CIDR 块范围内的 IP 地址：198.19.0.0/16

**Note**

您的 Active Directory 域控制器必须是可写的。

- Active Directory 域中服务账户的用户名和密码，供 Amazon FSx 用于将文件系统加入您的 Active Directory 域中
- ( 可选 ) 您希望将文件系统加入其中的域中的组织单位 ( 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 ( ACL )、获取文件和文件夹的所有权等。如果您未指定此组，Amazon FSx 会默认将此授权委派给 Active Directory 域中的域管理员组。



**Note**

您提供的域组名称在 Active Directory 中必须是唯一的。在以下情况下，适用于 Windows File Server 的 FSx 将不会创建域组：

- 如果已经存在一个名为你指定的群组
- 如果您未指定名称，并且您的 Active Directory 中已存在名为“域管理员”的群组。

有关更多信息，请参阅 [将 Amazon FSx 文件系统加入到自行管理的 Microsoft Active Directory 域](#)。

**Important**

只有当您使用 Microsoft DNS 作为默认 DNS 服务时，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，则需要在创建文件系统后手动设置 Amazon FSx 文件系统的 DNS 条目。

当您直接将文件系统加入自行管理的 Active Directory 时，您的 FSx for Windows File Server 与您的用户和现有资源（包括现有文件服务器）位于同一个 Active Directory 林（包含域、用户和计算机的 Active Directory 配置中的顶层逻辑容器）和同一个 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托管 Active Directory，并在您创建的 AWS 托管 Active Directory 和您现有的自行 AWS 管理的 Active Directory 之间建立单向林信任关系。

**主题**

- [使用自行管理的 Microsoft Active Directory 的先决条件](#)
- [将 FSx for Windows File Server 文件系统加入自行管理的 Microsoft Active Directory 域的最佳实践](#)
- [验证 Active Directory 配置](#)
- [将 Amazon FSx 文件系统加入到自行管理的 Microsoft Active Directory 域](#)
- [获取用于 DNS 的正确的文件系统 IP 地址](#)
- [更新自行管理的 Active Directory 配置](#)

## 使用自行管理的 Microsoft Active Directory 的先决条件

在创建加入自行管理的 Microsoft Active Directory 域的 Amazon FSx 文件系统之前，请查看以下先决条件。

### 主题

- [本地配置](#)
- [网络配置](#)
- [服务账户权限](#)

### 本地配置

确保您有一个本地或其他自行管理的 Microsoft Active Directory，您可以在其中加入 Amazon FSx 文件系统。您的本地 Active Directory 应具有以下配置：

- 您 Active Directory 域控制器的域功能级别为 Windows Server 2008 R2 或更高版本。
- DNS 服务器 IP 地址和 Active Directory 域控制器 IP 地址如下所示，具体取决于文件系统的创建时间：

#### 对于 2020 年 12 月 17 日之前创建的文件系统

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

#### 对于 2020 年 12 月 17 日之后创建的文件系统

IP 地址可以位于任何范围内，但以下情况除外：

- 与 Amazon Web Services 在该 AWS 地区拥有的 IP 地址冲突的 IP 地址。有关按地区划分的 AWS 拥有的 IP 地址列表，请参阅 [AWS IP 地址范围](#)。
- 以下 CIDR 块范围内的 IP 地址：198.19.0.0/16

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 FSx for 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。有关更多信息，请参阅 [使用备份](#)。

- 非单标签域 ( SLD ) 格式的域名。Amazon FSx 不支持 SLD 域。
- 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。

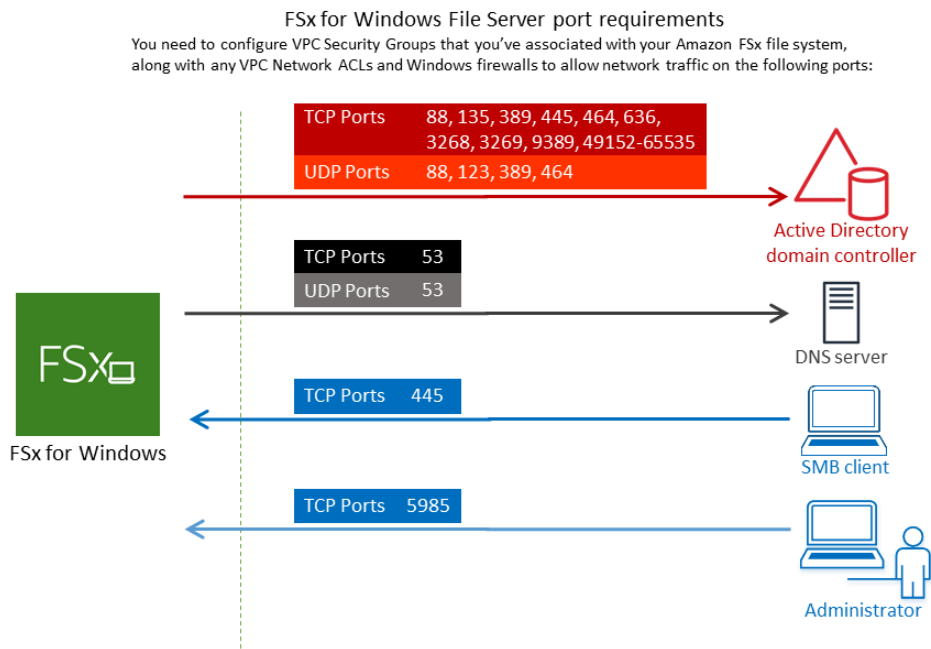
- 如果您已定义 Active Directory 站点，则必须在 Active Directory 站点中定义与 Amazon FSx 文件系统关联的 VPC 中的子网，且 VPC 中的子网与您其他站点中的子网之间不存在冲突。
- 您可能需要向防火墙添加规则，以允许 Active Directory 域控制器与 Amazon FSx 之间的 ICMP 流量。

## 网络配置

本节介绍将文件系统加入您自行管理的 Active Directory 所需的网络配置。

我们建议您先使用 [Amazon FSx Active Directory 验证工具](#) 测试您的网络设置，然后再尝试将文件系统加入自行管理的 Active Directory。

- 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 AWS Direct Connect、[AWS Virtual Private Network](#)、[VPC 对等互连](#) 或 [AWS Transit Gateway](#) 来设置此连接。
- 对于 VPC 安全组，用于您的默认 Amazon VPC 的默认安全组必须添加到控制台中的文件系统。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            | Kerberos 身份验证                        |
| TCP/UDP | 464           | 更改/设置密码                              |
| TCP/UDP | 389           | 轻型目录访问协议 ( LDAP )                    |
| UDP     | 123           | 网络时间协议 ( NTP )                       |
| TCP     | 135           | 分布式计算环境/端点映射器 ( DCE/EPMAP )          |
| TCP     | 445           | 目录服务 SMB 文件共享                        |
| TCP     | 636           | 基于 TLS/SSL 的轻型目录访问协议 ( LDAPS )       |
| TCP     | 3268          | Microsoft 全局目录                       |
| 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        |
| TCP     | 49152 - 65535 | RPC 的临时端口                            |

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 FSx 管理员的防火墙上。

#### 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。

**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。

**Important**

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

## 服务账户权限

确保您在自行管理的 Microsoft Active Directory 中有一个服务账户，该账户具有将计算机加入该域的委派权限。服务账户是自行管理的 Microsoft Active Directory 中的一个用户账户，该账户已被委派某些任务。

服务账户至少需要在您要加入文件系统的 OU 中获得以下权限：

- 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

这些权限代表将计算机对象加入到您的 Active Directory 至少需要具备的一组权限。有关更多信息，请参阅主题为 [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](#)。

有关如何创建具有正确权限的服务账户的更多信息，请参阅 [向 Amazon FSx 服务账户委派权限](#)。

Amazon FSx 在 Amazon FSx 文件系统的整个生命周期中都需要有一个有效的服务账户。Amazon FSx 必须能够使用服务账户全面管理文件系统并执行需要退出并重新加入您的 Active Directory 域的任务。这些任务包括更换出现故障的文件服务器或修补 Windows Server 软件。必须使用 Amazon FSx 更新您的活动目录配置，包括服务账户证书。有关更多信息，请参阅 [更新您的活动目录配置](#)。

Amazon FSx 需要连接到您的 Active Directory 环境中的所有域控制器。如果您有多个域控制器，请确保所有域控制器都满足上述要求，并确保对您的服务账户所做的任何更改都会传播到所有域控制器。

您可以使用 [Amazon FSx Active Directory 验证工具](#) 验证您的 Active 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 AWS 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

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

## 将 FSx for Windows File Server 文件系统加入自行管理的 Microsoft Active Directory 域的最佳实践

我们建议在将 Amazon FSx for Windows File Server 文件系统加入自行管理的 Microsoft Active Directory 时实施以下最佳实践。

### 向 Amazon FSx 服务账户委派权限

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

要将 Amazon FSx 文件系统加入您的域，请确保服务账户具有委派的权限。域管理员组的成员具有足够执行此任务的权限。但是，作为最佳实践，请使用仅具有此任务的最低执行权限的服务账户。以下过程演示如何仅将加入 Amazon FSx 文件系统所需的权限委派到您的域中。

您可以使用 Active Directory 用户和计算机 MMC 管理单元中的委托控制或高级功能来分配这些权限。

在已加入活动目录并安装了 Active Directory User and Computers MMC 管理单元的计算机上执行以下任一过程。

### 使用委派控制向服务帐号或群组分配权限

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，添加您的 Amazon FSx 服务账户或群组名称，然后选择下一步。
7. 在 Tasks to Delegate (要委派的任务) 页面上，选择 Create a custom task to delegate (创建要委派的自定义任务)，然后选择 Next (下一步)。
8. 选择仅文件夹中的以下对象，然后选择计算机对象。
9. 选择在此文件夹中创建选定对象和删除此文件夹中的选定对象。然后选择下一步。
10. 在权限中，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. 在权限条目页面上，选择选择主体，然后输入您的 Amazon FSx 服务账户或群组的名称。对于“应用于:”，选择“后代计算机对象”。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。

### Important

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

## 更新您的活动目录配置

为了帮助确保您的 Amazon FSx 文件系统持续、不间断地可用，您需要在更改自行管理的 Active Directory 设置时随时更新文件系统的活动目录配置。

例如，如果您的 Active Directory 使用基于时间的密码重置策略，则在密码重置后，请务必使用 Amazon FSx 更新服务账户密码。同样，如果您的 Active Directory 域的 DNS 服务器 IP 地址发生变化，请在更改发生后立即使用 Amazon FSx 更新 DNS 服务器 IP 地址。有关更多信息，请参阅 [更新自行管理的 Active Directory 配置](#)。

更新 Amazon FSx 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。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。

要了解有关排查可能存在的自行管理的 Active Directory 错误配置问题的更多信息，请参阅 [文件系统处于配置错误状态](#)。

## 使用安全组限制 VPC 内的流量

要限制虚拟私有云 (VPC) 内的网络流量，您可以在 VPC 中实施最低权限原则。换言之，您可以将权限限制为所需的最低权限。为此，请使用安全组规则。要了解更多信息，请参阅 [Amazon VPC 安全组](#)。

## 为文件系统的网络接口创建出站安全组规则

为提高安全性，请考虑使用出站流量规则来配置安全组。这些规则应仅允许出站流量流向自行管理的 Active Directory 域控制器或子网或安全组内部。将此安全组应用于与您的 Amazon FSx 文件系统的弹性网络接口关联的 VPC。要了解更多信息，请参阅 [使用 Amazon VPC 进行文件系统访问控制](#)。



## 验证 Active Directory 配置

在创建已加入 Active Directory 的 FSx for Windows File Server 文件系统之前，我们建议您使用 Amazon FSx Active Directory 验证工具来验证 Active Directory 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。确保您的 EC2 实例具有所需的 AmazonEC2ReadOnlyAccess IAM 权限。您可以使用 IAM policy simulator 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 policy simulator 测试 IAM policy](#)。
2. 将 EC2 Windows 实例加入 Active Directory 有关更多信息，请参阅《AWS Directory Service 管理指南》中的[手动加入 Windows 实例](#)。
3. 连接到您的 EC2 实例。有关更多信息，请参阅 Amazon 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：

- Active Directory 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 AWS 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 ( *SUBNET\_1*、*SUBNET\_2* ，例如 subnet-04431191671ac0d19 )。

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

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

 # Subnet IDs for Amazon FSx file server(s)
 SubnetIds = @('SUBNET_1', 'SUBNET_2')

 Credential = $Credential
}
```

9. ( 可选 ) 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 [Amazon FSx 问题排查](#) 中包含的《问题排查指南》。

## 将 Amazon FSx 文件系统加入到自行管理的 Microsoft Active Directory 域

当您创建新的 FSx for Windows File Server 文件系统时，您可以配置 Microsoft Active Directory 集成，使其加入您自行管理的 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。

### Note

Amazon FSx 目前不支持单标签域 ( SLD )。

- 域的 DNS 服务器的 IP 地址。
- 本地 Microsoft Active Directory 域中的服务账户凭证。Amazon FSx 使用这些凭证加入您自行管理的 Active Directory。

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 )。
- 为成员授予 Amazon FSx 文件系统管理权限的域组的名称。

### Note

您提供的域组名称在 Active Directory 中必须是唯一的。在以下情况下，适用于 Windows File Server 的 FSx 将不会创建域组：

- 如果已经存在一个名为您指定的群组
- 如果您未指定名称，并且您的 Active Directory 中已存在名为“域管理员”的群组。

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

### Important

只有当您加入的 Active Directory 域使用 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，则需要在创建文件系统后手动设

置 Amazon FSx 文件系统的 DNS 条目。有关为文件系统选择正确 IP 地址的更多信息，请参阅[获取用于 DNS 的正确的文件系统 IP 地址](#)。

## 开始前的准备工作

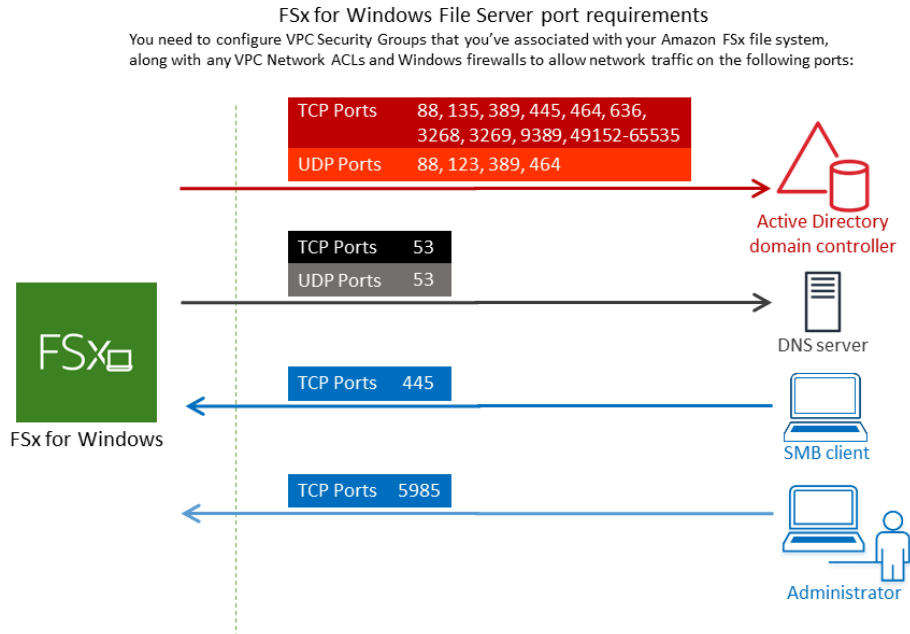
确保您已完成 [将 Amazon FSX 与自行管理的 Microsoft Active Directory 结合使用](#) 中详述的 [使用自行管理的 Microsoft Active Directory 的先决条件](#)。

创建一个连接自行管理的 Active Directory ( 控制台 ) 的 FSx for Windows File Server 文件系统

1. 通过以下网址打开 Amazon FSx 控制台：<https://console.aws.amazon.com/fsx/>。
2. 在控制面板上，选择创建文件系统以启动文件系统创建向导。
3. 选择 FSx for Windows File Server，然后选择下一步。显示创建文件系统页面。
4. 为您的文件提供名称。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 AWS 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 | Kerberos 身份验证 |


| 协议      | 端口  | 角色              |
|---------|-----|-----------------|
| 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)    |



| 协议  | 端口  | 角色                                 |
|-----|-----|------------------------------------|
| TCP | 135 | 分布式计算环境/<br>端点映射器<br>(DCI)<br>EPMA |
| TCP | 445 | 目录服务<br>SMB<br>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 (LDAP) |
| TCP | 3268 | Microsoft 全局目录              |
| TCP | 3269 | 基于 SSL 的 Microsoft 全局目录     |

| 协议  | 端口            | 角色                                   |
|-----|---------------|--------------------------------------|
| TCP | 5985          | WinRM 2.0 ( Microsoft Windows 远程管理 ) |
| TCP | 9389          | 微软活动目录 DS Web 服务, PowerI             |
| 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。

- 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 FSx 管理员的防火墙上。

**Note**

如果您已定义 Active Directory 站点，您必须确保在 Active Directory 站点中定义了与 Amazon FSx 文件系统关联的 VPC 中的子网，且 VPC 中的子网与您其他站点中的子网之间不存在冲突。您可以使用 Active Directory Sites and Services MMC 管理单元查看和更改这些设置。

**Important**

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

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。

**⚠ 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 目录的组织单位值。

**ℹ 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. 在自行管理的 Active Directory 域上的账户的服务账户用户名中输入一个字符串值，例如 ServiceAcct。Amazon FSx 使用此用户名加入您的 Microsoft Active Directory 域。

**⚠ 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. 在自行管理的 Active Directory 域上的账户的服务账户密码中输入一个值。Amazon FSx 使用此密码加入您的 Microsoft Active Directory 域。
16. 在确认密码中重新输入密码以进行确认。
17. 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 FSx 将使用内置 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**

如果您没有提供委派的文件系统管理员组，则默认情况下，Amazon FSx 会尝试在您的 Active Directory 域中使用内置 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**

在提供组名参数时，请勿包含域前缀 (corp.com\ FSxAdmins) 或域后缀 (F SxAdmins @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=F SxAdmins、ou=Example、dc=Corp、dc=com。

创建一个连接自行管理的 Active Directory ( AWS CLI ) 的 FSx for Windows File Server 文件系统

以下为在 us-east-2 可用区中创建带有 SelfManagedActiveDirectoryConfiguration 的 FSx for Windows File Server 文件系统的示例。

```
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**

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

## 获取用于 DNS 的正确的文件系统 IP 地址

只有当您使用 Microsoft DNS 作为默认 DNS 服务时，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，则需要手动设置 Amazon FSx 文件系统的 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 <https://console.aws.amazon.com/fsx/> 中，选择要获取 IP 地址的文件系统，以显示文件系统详细信息页面。
2. 在网络与安全选项卡中，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弹性网络接口，打开 Amazon EC2 控制台中的网络接口页面。
    - 要使用的单可用区 1 文件系统的 IP 地址显示在主要私有 IPv4 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弹性网络接口，打开 Amazon EC2 控制台中的网络接口页面。
    - 要使用的首选子网的 IP 地址显示在辅助私有 IPv4 IP 列中。
    - 在 Amazon FSx 的备用子网面板中，选择网络接口下显示的弹性网络接口，打开 Amazon EC2 控制台中的网络接口页面。
    - 要使用的备用子网的 IP 地址显示在辅助私有 IPv4 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 [使用 Amazon FSx CLI PowerShell](#)。

## 更新自行管理的 Active Directory 配置

您可以使用 Amazon FSx API 或 AWS CLI 更新文件系统自我管理的 Active Directory 配置的服务账户用户名和密码以及 DNS 服务器 IP 地址。AWS Management Console 您可以随时使用 AWS

Management Console、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. 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。
5. 选择更新以启动 Active Directory 配置更新。

您可以使用 AWS Management Console 或[监控更新进度](#) AWS CLI。

### 更新自行管理的 Active Directory 配置 (CLI)

- [要更新适用于 Windows File Server 文件系统的自行管理的 Active Directory 配置，请使用 update-file-system AWS CLI 命令。](#) 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。
  - `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 `AdministrativeActions` 对象描述了请求及其状态。



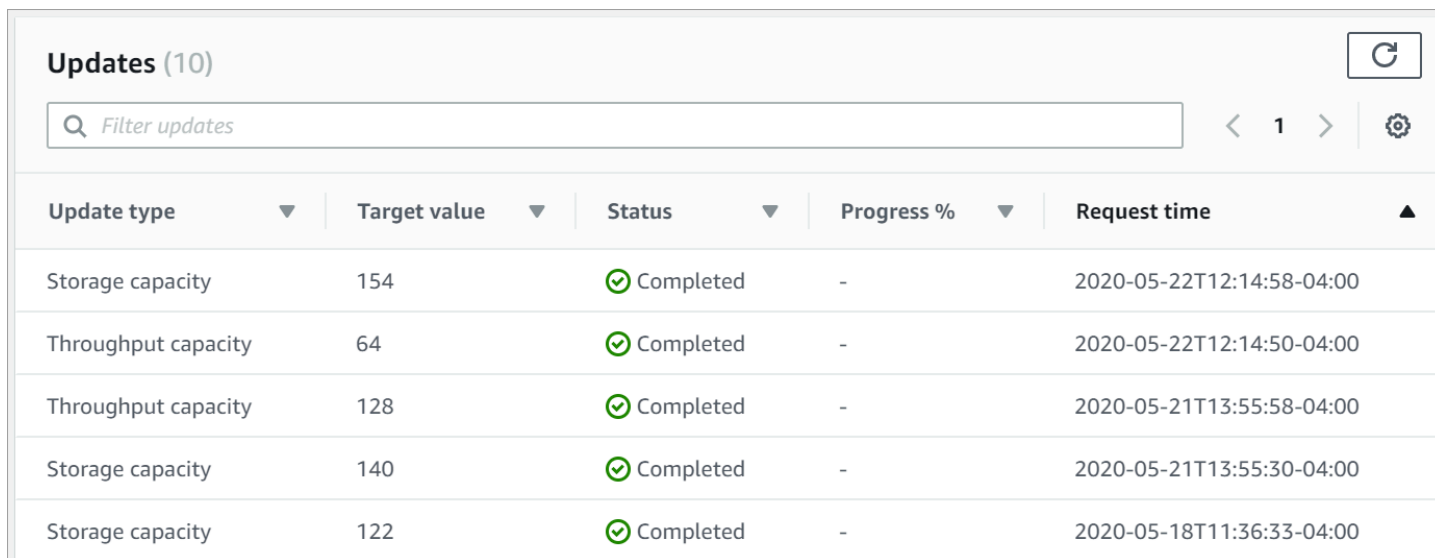
## 监控自行管理的 Active Directory 更新

更新文件系统的自我管理的 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” — 请注意，更新最多可能需要几分钟才能完成。

您可以使用以下各节所述的 AWS Management Console、API 或，监控自行管理的 Active Directory 配置更新的进度。AWS CLI

### 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。



The screenshot shows the 'Updates (10)' section in the AWS Management Console. It includes a search bar labeled 'Filter updates', a refresh button, and a table with the following columns: Update type, Target value, Status, Progress %, and Request time. The table lists five completed updates for 'Storage capacity' and 'Throughput capacity'.

| Update type         | Target value | Status    | Progress % | Request time              |
|---------------------|--------------|-----------|------------|---------------------------|
| Storage capacity    | 154          | Completed | -          | 2020-05-22T12:14:58-04:00 |
| Throughput capacity | 64           | Completed | -          | 2020-05-22T12:14:50-04:00 |
| Throughput capacity | 128          | Completed | -          | 2020-05-21T13:55:58-04:00 |
| Storage capacity    | 140          | Completed | -          | 2020-05-21T13:55:30-04:00 |
| Storage capacity    | 122          | Completed | -          | 2020-05-18T11:36:33-04:00 |

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。

- 正在进行中 – 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 AWS CLI 和 API 监控更新

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

以下示例摘录了 `describe-file-systems` CLI 命令响应，其中显示了两个自行管理的 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."
 }
 }
],
 .
 .
 .
```

# 使用 Microsoft Windows 文件共享

Microsoft Windows 文件共享是文件系统中的特定文件夹。它包括文件夹的子文件夹，您可以使用服务器消息块 (SMB) 协议让这些子文件夹可供计算实例访问。文件系统随附名为 share 的默认 Windows 文件共享。您可以使用名为 Shared Folders 的 Windows 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。

## 访问文件共享

要访问文件共享，您可以使用 Windows Map Network Drive 功能，将计算实例上的驱动器盘符映射到 Amazon FSx 文件共享。将文件共享映射到计算实例上的驱动器，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。

以下是在不同的支持计算实例上映射文件共享的过程。

### 主题

- [在 Amazon EC2 Windows 实例上映射文件共享](#)
- [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](#)
- [在未加入 Active Directory 的 Amazon Linux EC2 实例上自动挂载文件共享](#)

## 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。

在 Amazon EC2 Windows 实例上映射文件共享 (控制台)

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《AWS Directory Service 管理指南》中选择以下过程：
  - [无缝加入 Windows EC2 实例](#)
  - [手动加入 Windows 实例](#)
2. 连接到您的 EC2 Windows 实例。有关更多信息，请参阅 Amazon EC2 用户指南中的[连接到您的 Windows 实例](#)。
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，您可以在 [CreateFile 系统或 DescribeFile 系统](#) 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 AWS 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
```

- 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。

```
\\famznfsxaa11bb22.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《AWS Directory Service 管理指南》中选择以下过程：
  - [无缝加入 Windows EC2 实例](#)
  - [手动加入 Windows 实例](#)
2. 以 AWS Managed Microsoft AD 目录中的用户身份连接您的 EC2 Windows 实例。有关更多信息，请参阅 Amazon EC2 用户指南中的[连接到您的 Windows 实例](#)。
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 AWS 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
```

- 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: \\amznfsxaa11bb22.ad-domain.com\share /persistent:yes
```

除了 net use 命令之外，您还可以使用任何支持的 PowerShell 命令来装载文件共享。

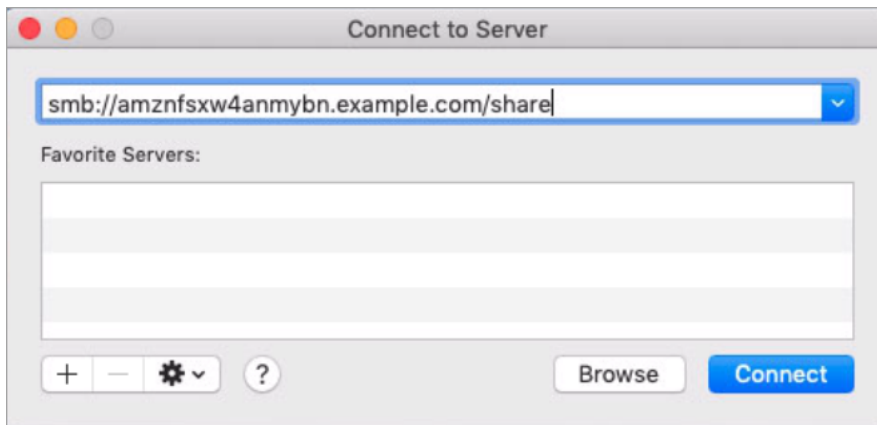
## 在 Amazon EC2 Mac 实例上挂载文件共享

不管 Amazon EC2 Mac 实例是否已加入您的 Active Directory，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。

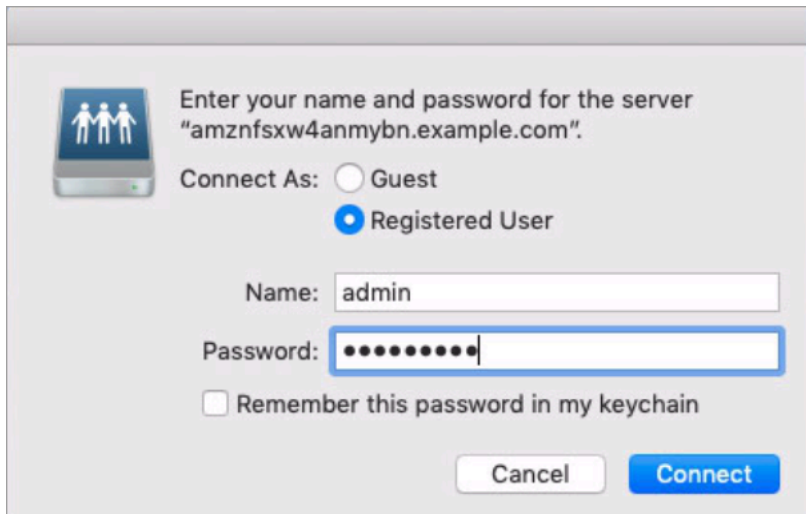
## 在 Amazon EC2 Mac 实例上挂载文件共享 ( GUI )

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](#)
  - [使用启动 Mac 实例 AWS CLI](#)
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 连接到您的实例](#)。
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，您可以在[CreateFile 系统或 DescribeFile 系统](#) 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](#)
  - [使用启动 Mac 实例 AWS CLI](#)
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 连接到您的实例](#)。
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 AWS 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
```

- 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 实例是否已加入您的 Active Directory，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 实例上安装文件共享

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《AWS 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[连接到您的 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,cuid=ad_user,rsiz=CIFSMaxBufSize,wsiz=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 AWS 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
```

- 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。Amazon FSx for Windows File Server 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 命令或等效的 [DescribeFile 系统](#) 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 [连接到您的 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=ntlmssp,cred=/home/ec2-user/
creds.txt,rsize=CIFSMaxBufSize,wsiz=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。Amazon FSx for Windows File Server 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)
```

## 在未加入 Active Directory 的 Amazon Linux EC2 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。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。文本文件 `creds.txt` 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
```

### 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 [连接到您的 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,wsiz=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. 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。Amazon FSx for Windows File Server 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。



# 将现有文件存储迁移到 Amazon FSx

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。迁移到 FSx for Windows File Server 的过程包括以下步骤：

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 [割接到 Amazon FSx](#)。

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](#)
- [将文件共享配置迁移到 Amazon FSx](#)
- [迁移 DNS 配置以使用 Amazon FSx](#)
- [割接到 Amazon FSx](#)

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

要将现有文件迁移到适用于 Windows File Server 文件系统的 FSx，我们建议 AWS DataSync 使用一种在线数据传输服务，该服务旨在简化、自动执行和加速向存储服务复制大量数据。AWS DataSync 通过互联网复制数据或 AWS Direct Connect。作为一项完全托管的服务，DataSync 无需修改应用程序、开发脚本或管理基础架构。有关更多信息，请参阅 [使用 AWS 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 [还原备份](#)。

## 使用 AWS DataSync 将现有文件迁移到 FSx for Windows File Server

我们建议使用 AWS DataSync 在 FSx for Windows File Server 文件系统之间传输数据。DataSync 是一项数据传输服务，可通过 Internet 或，简化、自动化和加速本地存储系统与其他 AWS 存储服务之间的数据移动和复制。AWS Direct Connect DataSync 可以传输您的文件系统数据和元数据，例如所有权、时间戳和访问权限。

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

您可以使用 DataSync 在两个 FSx for Windows File Server 文件系统之间传输文件，也可以使用 AWS 区域不同的 AWS 帐户将数据移动到文件系统。你可以将适用于 Windows DataSync s File Server 文件系统的 FSx 用于其他任务。例如，您可以执行一次性数据迁移、定期摄取分布式工作负载的数据以及按计划复制以实现数据保护与恢复。

在中 AWS DataSync，Windows File Server 的 fsX 的位置是适用于 Windows 文件服务器的 fsX 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《AWS DataSync 用户指南》中的 [使用位置](#)。

DataSync 使用服务器消息块 (SMB) 协议访问你的 FSx for Windows File Server。它使用您在 AWS DataSync 控制台或 AWS CLI 中配置的用户名和密码进行身份验证。

### 先决条件

要将数据迁移到你的 Amazon FSx for Windows File Server 设置中，你需要一台符合要求 DataSync 的服务器和网络。要了解更多信息，请参阅《AWS DataSync 用户指南》DataSync 中的 [要求](#)。

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 任务涉及文件元数据的扫描，这可能会耗尽 HDD 文件系统的磁盘 IOPS 限制，从而导致长时间迁移和文件系统性能影响。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超过单个 DataSync 任务消耗的带宽，则还可以使用横向扩展架构来加速数据传输。有关更多信息，请参阅：[如何使用横向 AWS DataSync 扩展架构加速数据传输](#)。

可以使用 [FSx 性能指标](#) 监控文件系统的磁盘 I/O 利用率。

## 使用迁移文件的基本步骤 DataSync

要使用将文件从源位置传输到目标位置 DataSync，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适用于 Windows File Server 的 FSx，请参阅《[用户指南](#)》中的[自管理存储 AWS 与之间的数据传输、为 SMB 创建位置和为 Windows 文件服务器的 Amazon FSx 创建位置](#)。AWS DataSync

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《[AWS 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

您可以使用 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。您还可以使用 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. 为源文件系统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. 创建并配置 DataSync 任务以将数据从源传输到目标。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。这使您能够估计数据传输过程需要多长时间，并提前对 DataSync 错误进行故障排除。

为了最大限度地缩短直接转换时间，您可以提前运行 DataSync 任务，将大部分数据从源文件系统移动到目标文件系统。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。

您可以将 DataSync 任务配置为仅在某些目录中运行，或者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中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：[演练 5：使用 DNS 别名访问文件系统](#)。

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 任务处理过程中，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 监控指标 CloudWatch](#)。
- 设置 [DataSync 监控](#) 以帮助了解正在进行的任务的进度。如果您遇到任何错误，也可以向 Amazon CloudWatch Logs 组发送 DataSync 日志，以帮助调试任务。

## 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。

## 先决条件

在开始之前，请确保完成了以下操作：

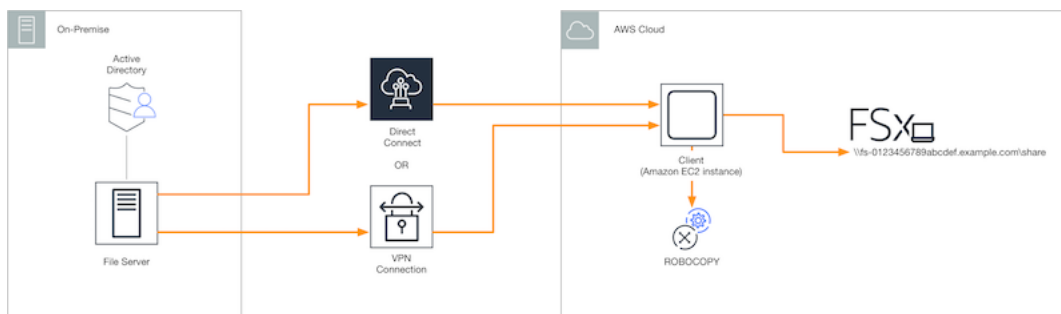
- 在您的本地 Active Directory 和要在其中创建 Amazon FSx 文件系统的 VPC 之间建立网络连接（使用 AWS Direct Connect 或 VPN）。
- 在 Active Directory 上创建具有将计算机加入域的委派权限的服务账户。有关更多信息，请参阅《AWS Directory Service 管理指南》中的[向您的服务账户委派权限](#)。
- 创建一个 Amazon FSx 文件系统，并将其加入了自行管理的（本地）Microsoft AD 目录。
- 记下包含要传输到 Amazon FSx 的现有文件的文件共享（本地或内部 AWS）的位置（例如）。\Source\Share
- 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 的 Backup Operators 组的成员，并使用 /b 标志。RoboCopy | 用户必须是 Amazon FSx 文件系统管理员组* 的成员，并使用 /b 标志。RoboCopy |
| 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。                                 | 用户必须是 Amazon FSx 文件系统管理员组的成员*，并使用 /b 标志 RoboCopy  |

**Note**

\* 对于加入 AWS 托管 Microsoft AD 的文件系统，Amazon FSx 文件系统管理员组是委托 AWS 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。



## 如何使用 Robocopy 将现有文件迁移到 Amazon FSx

可以使用以下过程，将现有文件迁移到 Amazon FSx。

将现有文件迁移到 Amazon FSx

1. 在 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 Command Prompt，将现有文件服务器（本地或内部 AWS）上的源文件共享映射到驱动器号（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 AWS 托管 Microsoft AD 的文件系

统，该组是**AWS 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 [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

- /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 PowerShell 身份打开 Windows。
2. SmbShares.xml 通过在中运行以下命令，将源文件服务器的文件共享导出到名为的文件中 PowerShell。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 AWS 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 }
}
```

## 迁移 DNS 配置以使用 Amazon FSx

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。

**Manage DNS aliases** [X]

Associate new DNS aliases

transactions.corp.example.com

Specify up to 50 aliases separated with commas, or put each on a new line.

**Associate**

**Current DNS aliases (1)** [Refresh] **Disassociate**

filesystem.domain.name.com < 1 > [Settings]

| <input type="checkbox"/> | DNS name                    | Status    |
|--------------------------|-----------------------------|-----------|
| <input type="checkbox"/> | financials.corp.example.com | Available |

If you associate or disassociate DNS aliases, your file system will experience a temporary loss of availability.

**Close**

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)

- 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
 }
]
}
```

要监控您关联的别名的状态，请使用 `CL describe-file-system-aliases l` 命令（等效 [DescribeFileSystemAliases](#) 的 API 操作）。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）。

## 割接到 Amazon FSx

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](#)
- [为 Kerberos 身份验证配置 SPN](#)
- [更新 Amazon FSx 文件系统的 DNS CNAME 记录](#)

## 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 AWS 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 活动目录模块

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. PowerShell 以管理员身份打开。
3. 使用以下命令安装 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 [迁移 DNS 配置以使用 Amazon FSx](#) 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 [迁移 DNS 配置以使用 Amazon FSx](#) 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 [迁移 DNS 配置以使用 Amazon FSx](#) 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。您还可以在[DescribeFile 系统](#) API 操作的响应中获取 DNS 名称。

- 将 *alias\_fqdn* 替换为在 [迁移 DNS 配置以使用 Amazon FSx](#) 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。

您还可以在[DescribeFile 系统](#) API 操作的响应中获取 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 [迁移 DNS 配置以使用 Amazon FSx](#) 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 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. 作为拥有 DNS 管理权限的群组 ( AWS 托管 AWS Microsoft 活动目录中的委托域名系统管理员，以及您自行管理的 Active Directory 中已向其委派 DNS 管理权限的域管理员或其他群组 ) 的用户登录加入您的 Amazon FSx 文件系统所加入的 Amazon FSx 文件系统的 Windows 实例

有关更多信息，请参阅 Amazon EC2 用户指南中的 [连接到您的 Windows 实例](#)。

2. PowerShell 以管理员身份打开。
3. 需要 PowerShell 使用 DNS 服务器模块来执行此过程中的指令。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 [迁移 DNS 配置以使用 Amazon FSx](#) 中与文件系统关联的每个 DNS 别名重复上述步骤。

# 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 AWS 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 AWS](#)
- [Simplify SQL Server Always On deployments with AWS 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`。要了解有关创建新 CA 共享的更多信息，请参阅[创建持续可用 \(CA\) 共享](#)。

## 配置 SMB 超时设置

如 [FSx for Windows File Server 失效转移进程](#) 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 服务器失效转移群集部署的 SMB 文件共享见证。

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

Amazon Kendra 是一项高度准确的智能搜索服务。FSx for Windows File Server 文件系统可以用作 Amazon Kendra 的数据来源，从而索引和智能搜索存储在文件系统的文档中包含的信息。

- 有关 Amazon Kendra 的更多信息，请参阅《Amazon Kendra 开发人员指南》<https://docs.aws.amazon.com/kendra/latest/dg/what-is-kendra.html>中的什么是 Amazon Kendra。
- 有关如何将文件系统添加为 Amazon Kendra 数据来源的更多信息，请参阅《Amazon Kendra 开发人员指南》中的 [Amazon FSx 数据源入门 \(控制台\)](#)。
- 关于 Amazon Kendra 的概述信息，请参阅 [Amazon Kendra 网站](#)。
- 有关如何使用 Amazon Kendra 搜索文件系统的过程，请参阅 AWS Machine Learning Blog 上的 [Securely search unstructured data on Windows file systems with the Amazon Kendra connector for Amazon FSx for Windows File Server](#)。

## 文件系统性能

当您将 FSx for Windows File Server 文件系统添加为数据来源时，Amazon Kendra 会按常规同步频率爬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 性能的更多信息，请参阅 [FSx for Windows File Server 性能](#)。

## 通过备份、影子副本和计划复制来保护您的数据

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

- 原生 Amazon FSx 备份能够满足您在 Amazon FSx 中的备份保留和合规需求。
- AWS Backup Amazon FSx 文件系统的备份是云端和本地 AWS 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。
- AWS DataSync 按计划将 Amazon FSx 文件系统复制到第二个文件系统可提供数据保护和恢复。

### 主题

- [使用备份](#)
- [使用卷影副本保护您的数据](#)
- [使用计划复制 AWS DataSync](#)

## 使用备份

使用 Amazon FSx，备份非常耐用 file-system-consistent，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。为确保文件系统一致性，Amazon FSx 使用 Microsoft Windows 中的卷影复制服务 (VSS)。为确保高持久性，Amazon FSx 在 Amazon Simple Storage Service (Amazon S3) 中存储备份。

无论是使用每日自动备份还是用户启动的备份功能生成，Amazon FSx 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点，存储 I/O 可能会短暂暂停，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会短暂体验这种 I/O 暂停。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。

定期为文件系统创建备份是一种最佳实践，可以补充 Amazon FSx for Windows File Server 对文件系统执行的复制。Amazon FSx 备份有助于满足您的备份保留和合规需求。使用 Amazon FSx 备份非常

简单，无论是创建备份、复制备份、从备份中还原文件系统还是删除备份。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](#)
- [使用用户启动备份](#)
- [AWS Backup 与 Amazon FSx 搭配使用](#)
- [复制备份](#)
- [还原备份](#)
- [删除备份](#)
- [备份大小](#)

## 使用每日自动备份

默认情况下，Amazon FSx 可以每天自动备份文件系统。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，我们建议您选择一天中比较方便的时间。理想情况下，这个时间是在使用文件系统的应用程序的正常运行时间之外。

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。Amazon 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 AWS CLI 或其中一个 AWS SDK 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 [演练 3：更新现有文件系统](#)。

## 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 AWS Command Line Interface (AWS CLI) 来执行此操作。Amazon FSx 文件系统的用户启动备份永不过期，

您可以将这些备份保留任意长的时间。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 Amazon FSx 控制台、API 或 CLI 删除用户启动备份。Amazon FSx 永远不会自动删除这些备份。有关更多信息，请参阅 [删除备份](#)。

如果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。

## 创建用户启动备份

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

### 创建用户启动文件系统备份

1. 通过以下网址打开 Amazon FSx 控制台：<https://console.aws.amazon.com/fsx/>。
2. 在控制台控制面板中，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。在左侧导航中选择备份，即可在 Amazon FSx 控制台中找到包含所有备份的表。您可以搜索您为备份提供的名称，通过表格筛选条件仅显示匹配的结果。

当您按照此过程所述创建用户启动备份时，它具有 USER\_INITIATED 类型，并且在完全可用之前显示为 CREATING 状态。

## AWS Backup 与 Amazon FSx 搭配使用

AWS 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。AWS 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。AWS Backup 可以更轻松地法律、监管和专业合规制定集中备份策略。AWS Backup 还提供了一个可以执行以下操作的中心位置，从而简化了对 AWS 存储卷、数据库和文件系统的保护：

- 配置和审核要备份的 AWS 资源。
- 计划自动备份。
- 设置保留策略。
- 跨 AWS 地区和跨 AWS 账户复制备份。

- 监控所有最近的备份、复制和还原活动。

AWS Backup 使用 Amazon FSx 的内置备份功能。从 AWS Backup 控制台获取的备份与通过 Amazon FSx 控制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。与您进行的任何其他 Amazon FSx 备份相比，从中获取的备份 AWS Backup 是增量的，无论是用户启动的还是自动的。

如果您使用 AWS 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 AWS Backup 保留不可变的备份。这样可以防止意外或恶意删除。

执行的备份被 AWS Backup 视为用户启动的备份，它们计入 Amazon FSx 用户启动的备份配额。您可以在 Amazon FSx 控制台、CLI 和 API AWS Backup 中查看和还原所做的备份。但是，您无法删除 AWS Backup 在 Amazon FSx 控制台、CLI 或 API 中拍摄的备份。有关如何使用 AWS Backup 备份您的 Amazon FSx 文件系统的更多信息，请参阅《开发人员指南》中的“[使用亚马逊 FSx 文件系统](#)”。AWS Backup

## 复制备份

您可以使用 Amazon FSx 将同一 AWS 账户内的备份手动复制到另一个 AWS 区域（跨区域副本）或同一区域内的备份（AWS 区域内副本）。您只能在同一个 AWS 分区内制作跨区域副本。您可以使用 Amazon FSx 控制台 AWS CLI 或 API 创建用户启动的备份副本。创建用户启动备份副本时，其类型为 USER\_INITIATED。

您还可以 AWS Backup 使用跨 AWS 区域和跨 AWS 账户复制备份。AWS 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 AWS 区域，这样在主 AWS 区域发生灾难时，您可以从备份中恢复并快速恢复另一个 AWS 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 AWS 区域或同一 AWS 区域内。您可以使用 Amazon FSx 控制台或 Amazon FSx API 在同一个 AWS 账户（跨区域或区域内）内制作备份副本。AWS CLI 您还可以使用 [AWS 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 AWS 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）。



您可以使用 `with su` AWS Organizations `pports` AWS Backup 来制作跨账户备份副本。跨账户副本的账户界限由 AWS Organizations 政策定义。有关使用 AWS Backup 制作跨账户备份副本的更多信息，请参阅 AWS Backup 开发者指南 AWS 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）AWS 区域之间，以及（美国东部）和 AWS GovCloud AWS 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 AWS 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 AWS 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 policy 声明来授予执行备份复制操作的权限。要与源 AWS 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 AWS 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。

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

有关 IAM policy 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 AWS 区域或目标 AWS 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 AWS 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 AWS 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。

使用控制台在同一账户（跨区域或区域内）内复制备份

1. 通过以下网址打开 Amazon FSx 控制台：<https://console.aws.amazon.com/fsx/>。
2. 在导航窗格中，选择备份。
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 AWS 区域。目的地可以位于其他 AWS 区域（跨区域副本）或同一 AWS 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 AWS 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 AWS 账户中复制到所选 AWS 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 [CopyBackup](#) API 操作在同一个 AWS 账户内复制备份，无论是在一个 AWS 区域还是在同一个 AWS 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 CLI 命令或 `AP describe-backups` 操作以编程方式查看备份。[DescribeBackups](#)

## 还原备份

您可以使用可用备份来创建新的文件系统，从而有效地恢复另一个文件系统的 point-in-time 快照。您可以使用控制台 AWS CLI、或其中一个 AWS SDK 恢复备份。将备份还原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。从备份中还原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 AD 域信任。有关 Active Directory 的更多信息，请参阅[在 FSx for Windows File Server 中使用 Microsoft Active Directory](#)。

以下过程将指导您如何使用控制台还原备份以创建新的文件系统。

### Note

您只能将备份还原到与原始部署类型和存储容量相同的文件系统。您可以在还原的文件系统的存储容量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](#)。

## 从备份还原文件系统

1. 通过以下网址打开 Amazon FSx 控制台：<https://console.aws.amazon.com/fsx/>。
2. 在控制台控制面板的左侧导航窗格中选择备份。
3. 选择备份表中您要还原的备份，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。

您已从备份中还原，并且正在创建新的文件系统。当其状态更改为 AVAILABLE 时，您可以照常使用文件系统。

## 删除备份

删除备份是一项永久性且不可恢复的操作。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。您无法在 Amazon FSx 控制台 AWS Backup、CLI 或 API 中删除由拍摄的、类型为 Backup 的 AWS 备份。

### 删除备份

1. 通过以下网址打开 Amazon FSx 控制台：<https://console.aws.amazon.com/fsx/>。
2. 在控制台控制面板的左侧导航窗格中选择备份。
3. 选择备份表中您要删除的备份，然后选择删除备份。
4. 在打开的删除备份对话框中，确认备份 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。借助 Amazon FSx，重复数据删除和压缩所节省的存储效率不仅适用于主 SSD/HDD 存储，还适用于备份。

为了提供 file-system-consistent 持久的增量备份，Amazon FSx 在块级别备份数据。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 AWS Billing 控制面板中找到，或者 AWS Cost Management Console。要计算单个文件系统备份的大小和成本，您可以标记单个备份并启用基于标签的账单报告。

## 使用卷影副本保护您的数据

Microsoft Windows 影子副本是 Windows 文件系统在某个时间点的快照。启用卷影副本后，用户可以快速恢复存储在网络上的已删除或更改的文件，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。

卷影副本与文件系统的数据库一起存储，并且仅消耗文件系统的存储容量用于文件中已更改的部分。文件系统中存储的所有卷影副本都包含在文件系统备份中。

### Note

默认情况下，FSx for Windows File Server 上未启用影子副本。要使用卷影副本保护文件系统上的数据，必须启用卷影副本，并在文件系统上设置卷影复制计划。有关更多信息，请参阅 [将卷影副本配置为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

- [使用卷影副本时的最佳做法](#)
- [设置卷影副本](#)
- [将卷影副本配置为使用默认存储和计划](#)
- [还原单个文件和文件夹](#)
- [设置卷影副本的最大存储量](#)
- [查看影子副本存储空间](#)
- [删除影子副本的存储空间、计划和所有影子副本](#)
- [创建自定义影子副本计划](#)
- [查看影子副本计划](#)
- [删除影子副本计划](#)
- [创建影子副本](#)
- [查看现有影子副本](#)

## • [删除影子副本](#)

### 使用卷影副本时的最佳做法

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。Amazon FSx 使用 Microsoft Windows Server 提供的影子副本功能。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：根据设计，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三次 I/O 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 FSx for Windows 需要对影子副本存储进行一致性检查。由于 Windows 版 FSx 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长的 I/O 操作延迟。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[失效转移事件](#)期间，FSx for Windows 会运行一致性检查，要求在新的活动文件服务器处于联机状态之前扫描文件系统上的影子副本存储。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影子副本。

### 设置卷影副本

您可以使用 Amazon FSx 定义的 Windows PowerShell 命令在文件系统上启用和安排定期卷影复制。以下是在您的 FSx for Windows File Server 文件系统上配置卷影副本时的三个主要设置：

- 设置卷影副本在文件系统上可以消耗的最大存储量

- ( 可选 ) 设置文件系统上可以存储的最大卷影副本数。默认值为 20。
- ( 可选 ) 设置一个时间表来定义制作卷影副本的时间和间隔，例如每天、每周和每月

在任何时间点，每个文件系统最多可以存储 500 个卷影副本；但是，为了确保可用性和性能，我们建议在任何时候保持少于 64 个卷影副本。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影子复制的信息，请参阅 [将卷影副本配置为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[设置卷影副本的最大存储量](#)。

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](#)。

## 设置卷影副本的最大数量时的注意事项

启用卷影副本时，可以指定存储在文件系统上的卷影副本的最大数量。默认限制为 20，为了最大限度地减少卷影副本对可用性和性能的影响，Microsoft 建议将卷影副本的最大数量配置为低于 64 个。由于 Windows 需要高水平的 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。

您可以将卷影副本的最大数量设置为 500。但是，如果您在单个文件系统上有大量卷影副本或卷影副本占用大量存储空间 ( TB 级 )，则故障切换和故障恢复等过程所花费的时间可能比预期的要长。这是

因为 Windows 需要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长的 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。Amazon FSx 提供由 Microsoft Windows Server 提供的影子副本功能。根据设计，Microsoft Windows 使用一种 copy-on-write 方法来记录自最近一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三次 I/O 操作。如果 Windows 无法跟上每秒 I/O 操作的传入速度，则可能导致删除所有卷影副本，因为它无法再通过维护卷影副本 copy-on-write。因此，必须为文件系统上的工作负载需求预置足够的 I/O 性能容量（决定文件服务器 I/O 性能的吞吐能力维度，以及决定存储 I/O 性能的存储类型和容量）。
- 我们通常建议您在启用影子副本时使用配置为 SSD 存储而非 HDD 存储的文件系统，因为 Windows 维护影子副本消耗的 I/O 性能更高，而且 HDD 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](#)。

## 将卷影副本配置为使用默认存储和计划

您可以使用默认的卷影副本存储设置和计划，在文件系统上快速设置卷影副本。默认的卷影副本存储设置允许卷影副本占用文件系统存储容量的 10%。如果增加文件系统的存储容量，则当前分配的卷影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 AWS Managed Microsoft AD，该组是AWS 授权的 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 Amazon 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 Amazon 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
```

### 设置默认卷影复制时间表

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 AWS Managed Microsoft AD，该组是AWS 授权的 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 Amazon 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卷影复制时间表。

```
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
```

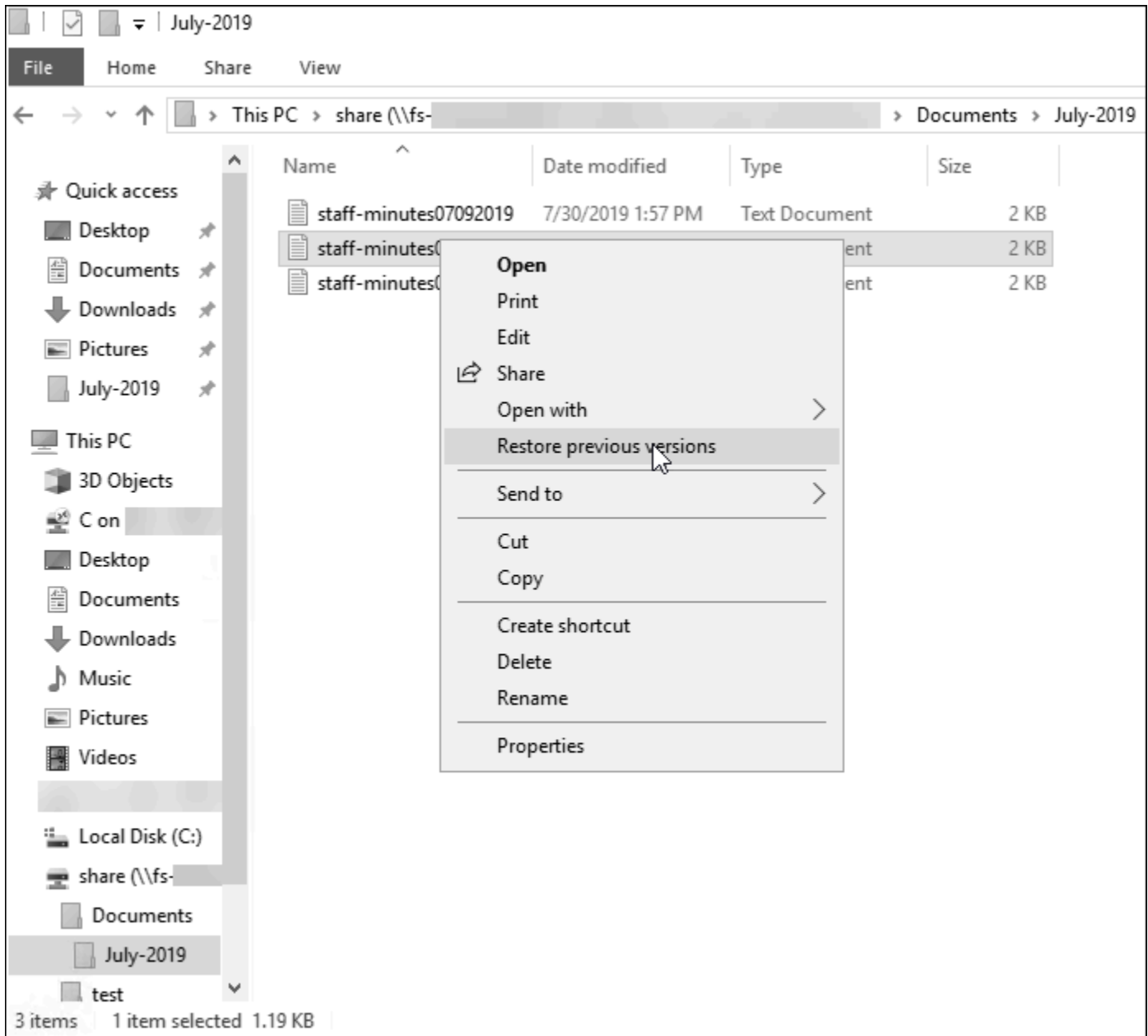
| Start Time                | Days of week                                 | WeeksInterval |
|---------------------------|----------------------------------------------|---------------|
| -----                     | -----                                        | -----         |
| 2019-07-16T07:00:00+00:00 | 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](#)。

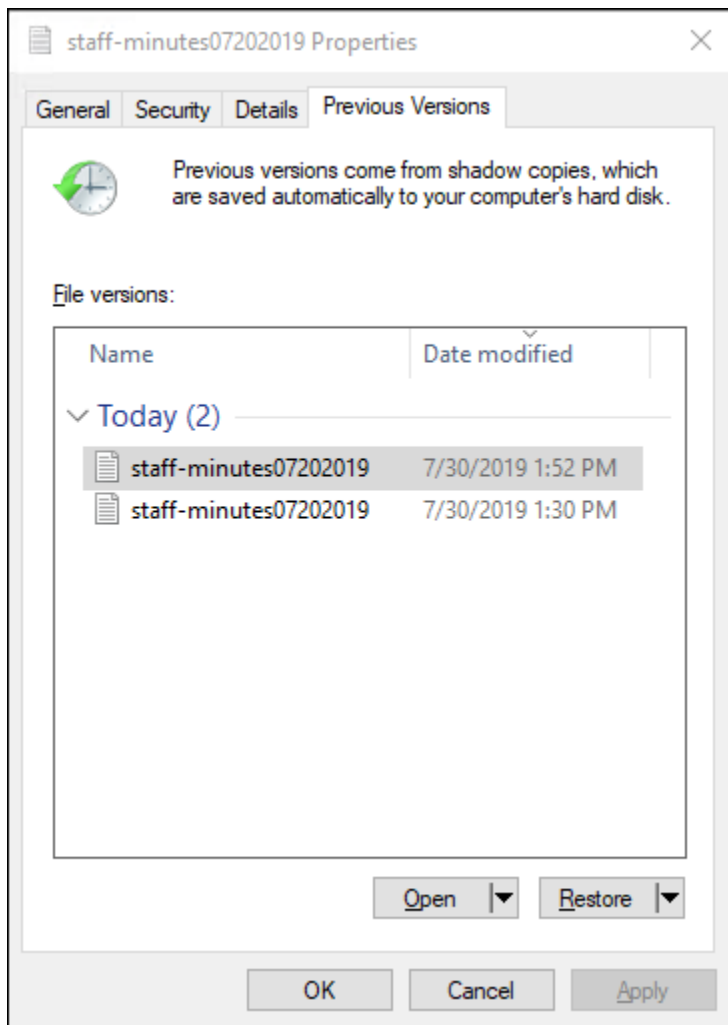
## 还原单个文件和文件夹

在 Amazon FSx 文件系统中配置卷影副本后，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。



## 设置卷影副本的最大存储量

您可以使用 `Set-FsxShadowStorage` 自定义 PowerShell 命令定义卷影副本在文件系统中可以消耗的最大存储量。您可以使用 `-Maxsize` 或 `-Default` 参数指定卷影副本可以增长到的最大大小。使用可将文件系统存储容量的最大值 `Default` 设置为 10%。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[将卷影副本配置为使用默认存储和计划](#)。

### 设置 FSx for Windows File Server 文件系统的影子副本存储量

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 AWS Managed Microsoft AD，该组是 AWS 授权的 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 Amazon 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 Amazon 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-psession -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` 选项将阴影存储量设置为卷的 10%，将影子应对的最大数量设置为 20。

```
[fs-1234567890abcef12]: PS>Set-FsxShadowStorage -Default
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace MaxSpace MaxShadowCopyNumber

0 0 32530536858 20
```

通过使用带 `-MaxShadowCopyNumber` 参数的 `Set-FsxShadowStorage` 命令并指定介于 1-500 之间的值，可以限制文件系统上允许的最大卷影副本数。默认情况下，卷影副本的最大数量设置为 20，这是 Microsoft 针对活跃工作负载所建议的。

## 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子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 [使用 Amazon FSx CLI 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卷影子副本的存储量（以字节为单位）。该值初始为 0。
- `UsedSpace`— 卷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`— 影子存储可以增长到的最大存储量，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卷影子副本数，介于 1-500 之间。

当卷影子副本 `UsedSpace` 数量达到配置的最大卷影子副本存储量 (`MaxSpace`) 或卷影子副本数量达到配置的最大卷影子副本数量 (`MaxShadowCopyNumber`) 时，您拍摄的下一个卷影子副本将替换最旧的卷影子副本。如果您不想丢掉最早影子副本，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

自动或手动创建卷影子副本时，卷影子副本使用您配置为存储限制的卷影子副本存储量。卷影子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子副本存储量 (`MaxSpace`)。

## 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话 PowerShell 中输入该 `Remove-FsxShadowStorage` 命令。有关在文件系统中启动远程 PowerShell 会话的说明，请参阅 [使用 Amazon FSx CLI 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.
```

## 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](#)。

在文件系统中运行 `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[将卷副本配置为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 Amazon 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

要查看文件系统中现有的卷影复制时间表，请在文件系统的远程会话 PowerShell 中输入以下命令。有关在文件系统中启动远程 PowerShell 会话的说明，请参阅[使用 Amazon FSx CLI 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
```

## 删除影子副本计划

要删除文件系统中现有的卷影复制计划，请在文件系统的远程会话 PowerShell 中输入以下命令。有关在文件系统中启动远程 PowerShell 会话的说明，请参阅[使用 Amazon FSx CLI 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>
```

## 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话 PowerShell 中输入以下命令。有关在文件系统中启动远程 PowerShell 会话的说明，请参阅[使用 Amazon FSx CLI PowerShell](#)。

```
[fs-0123456789abcdef1]PS> New-FsxShadowCopy

Shadow Copy {ABCDEF12-3456-7890-ABCD-EF1234567890} taken successfully
```

## 查看现有影子副本

要查看文件系统中的现有卷影副本集，请在文件系统的远程会话 PowerShell 中输入以下命令。有关在文件系统中启动远程 PowerShell 会话的说明，请参阅[使用 Amazon FSx CLI 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。有关在文件系统中启动远程 PowerShell 会话的说明，请参阅 [使用 Amazon FSx CLI 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影子副本、指定多个影子副本 ID 或指定的影子副本 ID 无效，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 PowerShell 会话中输入以下命令。

```
[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.
```

要删除文件系统中一定数量的最旧卷影副本，请将 `-MaxShadowCopyNumber` 参数更新为所需的剩余卷影副本数量。但是，此更改只有在拍摄下一个卷影副本快照后才会生效，届时系统将自动删除多余的卷影副本。在文件系统的远程会话 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
```

## 使用计划复制 AWS DataSync

您可以使用计划定期 AWS DataSync 将 FSx for Windows File Server 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 AWS DataSync 将现有文件迁移到 FSx for Windows File Server](#)本指南和 AWS DataSync 用户指南中的[AWS 存储服务之间的数据传输](#)。

# 管理文件系统

本章介绍如何访问 Amazon FSx CLI 进行远程管理 PowerShell，以及如何执行可用的文件系统管理任务。你也可以使用 Microsoft Windows 原生图形用户界面 (GUI) 来执行一些管理任务。

## 主题

- [使用 Amazon FSx CLI PowerShell](#)
- [启动 Amazon FSx 远程会话 PowerShell](#)
- [管理 DNS 别名](#)
- [在 FSx 上管理 Windows File Server 文件系统的文件共享](#)
- [文件访问审计](#)
- [用户会话和打开的文件](#)
- [重复数据删除](#)
- [存储配额](#)
- [管理传输中加密](#)
- [管理存储配置](#)
- [管理吞吐能力](#)
- [标记 Amazon FSx 资源](#)
- [使用 Amazon FSx 维护时段](#)
- [管理 Amazon FSx 文件系统的最佳实践](#)

## 使用 Amazon FSx CLI PowerShell

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 FSx for Windows File Server 文件系统中启动远程 PowerShell 会话，您首先需要满足以下先决条件：

- 能够连接到与 FSx for Windows File Server 文件系统具有网络连接的 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 AWS Managed Microsoft AD 的是 AWS 委派 FSx 管理员组。如果你使用的是自我管理的 Microsoft Active Directory，那就是你在创建文件系统时为管理指定的域管理员群组或自定义群组。有关更多信息，请参阅 [自行管理的 Active Directory 最佳实践](#)。

- 您的文件系统的 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 身份验证对用户凭据进行身份验证。
- 连接的客户端和文件系统之间的管理会话通信使用 Kerberos 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](#)。

使用遥控器时，您需要使用文件系统的 Windows 远程 PowerShell 端点 PowerShell。使用 AWS Management Console，您可以在文件系统详细信息页面的网络和安全选项卡中找到终端节点。使用 AWS CLI `describe-file-systems` 命令，将在响应中返回该 `RemoteAdministrationEndpoint` 属性。例如，远程管理端点使用格式 `amznfsxctlyaa1k.ActiveDirectory-DNS-nameamznfsxctlyaa1k.corp.example.com`。

您可以使用 `Get-Command cmdlet` 获取有关可用的 `cmdlet`、函数和别名的信息。PowerShell 有关更多信息，请参阅 Microsoft [Get-Command](#) 文档。

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

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

有关如何在 FSx for Windows File Server 文件系统中启动长期远程 PowerShell 会话的说明，请参阅 [启动 Amazon FSx 远程会话 PowerShell](#)

## 启动 Amazon FSx 远程会话 PowerShell

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

在您的文件系统中启动远程 PowerShell 会话

1. 作为您在创建文件系统时选择的委托 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 文件系统中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-psession -ComputerName Remote-PowerShell-Endpoint
-ConfigurationName FsxRemoteAdmin
[fs-0123456789abcdef0]: PS>
```

如果您的实例不是 Amazon FSx Active 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证。如果您的实例已加入域，则系统将不会要求您提供凭证。

## 管理 DNS 别名

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。您也可以使用自行选择的 DNS 别名访问您的文件系统。DNS 别名使您能够在将文件系统存储从本地迁移到 Amazon FSx 时，继续使用现有 DNS 名称访问存储在 Amazon FSx 上的数据。有关更多信息，请参阅 [将现有文件存储迁移到 Amazon FSx](#)。

### Note

美国东部时间 2020 年 11 月 9 日下午 12:00 之后创建的 FSx for Windows File Server 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 [还原备份](#)。

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。

只有当您加入的 AD 域使用 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，则需要在创建文件系统后手动设置 Amazon FSx 文件系统的 DNS 条目。有关为文件系统选择正确 IP 地址的更多信息，请参阅[获取用于 DNS 的正确文件系统 IP 地址](#)。

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。

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 ( SPN )。
- 为 DNS 别名配置一个新的 DNS CNAME 记录，将其解析为 Amazon FSx 文件系统的默认 DNS 名称。

有关更多信息，请参阅 [演练 5：使用 DNS 别名访问文件系统](#)。

适用于 Windows File Server 文件系统的 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 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。

若您尝试关联已与文件系统关联的别名，则操作无效。若您尝试取消关联未关联至此文件系统的文件系统别名，则 Amazon FSx 会响应请求错误。

### Note

当 Amazon FSx 在文件系统上添加或删除别名时，已连接的客户端会暂时断开并自动重新连接到该文件系统。由映射非持续可用（非 CA）共享的客户端在断开连接时打开的任何文件，都必须使用该客户端重新打开。

## 主题

- [DNS 别名状态](#)
- [Kerberos 身份验证使用 DNS 别名](#)
- [查看文件系统和备份的 DNS 别名](#)
- [将 DNS 别名与文件系统关联](#)
- [管理现有文件系统上的 DNS 别名](#)

## DNS 别名状态

DNS 别名可以具有以下状态值之一：

- 可用 – DNS 别名已与 Amazon FSx 文件系统相关联。
- 正在创建 – Amazon FSx 正在创建 DNS 别名并将其与文件系统关联。
- 正在删除 – Amazon FSx 正在取消 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 无法取消 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 (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。有关更多信息，请参阅 [演练 5：使用 DNS 别名访问文件系统](#)。

## 查看文件系统和备份的 DNS 别名

您可以使用 Amazon FSx 控制台、CLI 和 AP AWS I 查看当前与文件系统和备份关联的 DNS 别名。本主题提供有关如何查看文件系统和备份的 DNS 别名的说明。

### 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 [DescribeFileSystemAliases](#) API 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 [DescribeBackups](#) API 操作。

## 将 DNS 别名与文件系统关联

本主题介绍在从头开始为 Windows File Server 文件系统创建新 FSx 时，或者使用 AWS Management Console、和 API 从备份创建文件系统时，如何关联 DNS 别名。AWS CLI

### 在创建新文件系统时关联 DNS 别名（控制台）

1. 通过以下网址打开 Amazon FSx 控制台：<https://console.aws.amazon.com/fsx/>。
2. 按照“入门”部分的[创建您的文件系统](#)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。

### ▼ Access - optional

#### Aliases

List any custom DNS names that you want to associate with the file system

```
financials.corp.example.com
acctsrcv.corp.example.com
transactions.corp.example.com
```

Specify up to 50 aliases separated with commas, or put each on a new line.

4. 当文件系统为可用状态时，您可以使用 DNS 别名对其进行访问，方法是配置服务主体名称（SPN），并为该别名更新或创建 DNS CNAME 记录。有关更多信息，请参阅 [演练 5：使用 DNS 别名访问文件系统](#)。

在创建新的 Amazon FSx 文件系统时关联 DNS 别名 ( CLI )

1. 创建新文件系统时，使用 [CreateFileSystem](#) API 操作中的 `Aliases` 属性将 [DNS 别名](#) 与新文件系统关联。

```
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,acctsrcv.corp.example.com]
```

2. 当文件系统为可用状态时，您可以使用 DNS 别名对其进行访问，方法是配置服务主体名称（SPN），并为该别名更新或创建 DNS CNAME 记录。有关更多信息，请参阅 [演练 5：使用 DNS 别名访问文件系统](#)。

在恢复备份时添加或删除 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 [CreateFileSystemFromBackup](#) API 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 命令会将两个别名关联到使用备份创建的 Amazon FSx 文件系统。

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

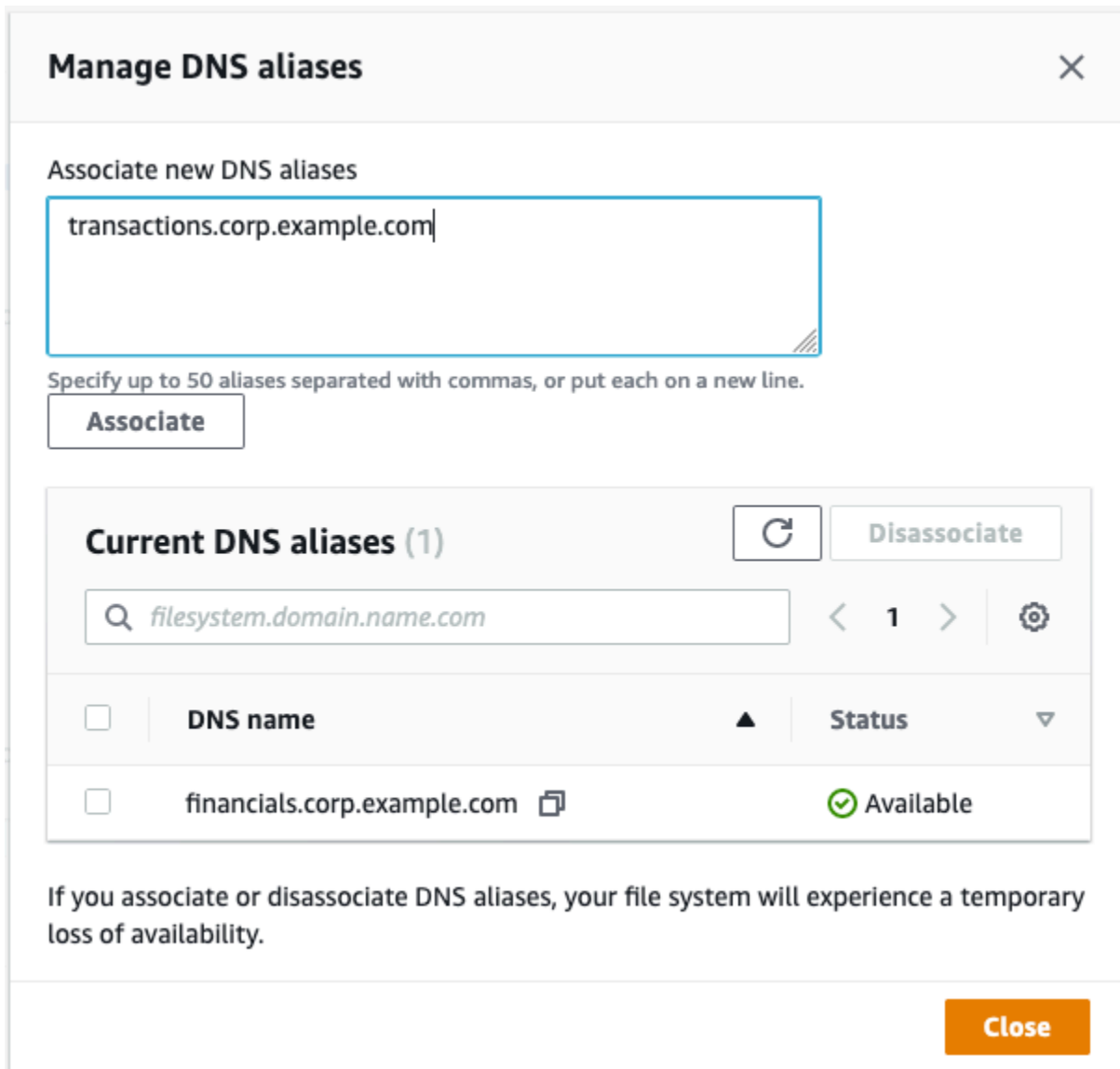
2. 当文件系统为可用状态时，您可以使用 DNS 别名对其进行访问，方法是配置服务主体名称 (SPN)，并为该别名更新或创建 DNS CNAME 记录。有关更多信息，请参阅 [演练 5：使用 DNS 别名访问文件系统](#)。

## 管理现有文件系统上的 DNS 别名

本主题介绍如何使用 AWS Management Console 和 AWS CLI 在现有文件系统上添加和删除别名。

### 管理文件系统 DNS 别名 (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 别名对话框。



- 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. 当别名为可用状态时，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（SPN），并为该别名更新或创建 DNS CNAME 记录。有关更多信息，请参阅 [演练 5：使用 DNS 别名访问文件系统](#)。

## 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 [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
 }
]
}
```

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 Lifecycle 值为“AVAILABLE”时 ( 过程最多需要 2.5 分钟 ) , 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 ( SPN ) , 并为该别名更新或创建 DNS CNAME 记录。有关更多信息, 请参阅 [演练 5 : 使用 DNS 别名访问文件系统](#)。

## 解除 DNS 别名与文件系统的关联 (CLI)

- 使用 `disassociate-file-system-aliases` CLI 命令或 [DisassociateFileSystemAliases](#) API 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
```

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

响应显示了 Amazon FSx 正在解除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。

## 在 FSx 上管理 Windows File Server 文件系统的文件共享

本主题介绍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
- 移除现有文件共享

你可以使用 Windows 原生共享文件夹 GUI 和用于远程管理的 Amazon FSx CLI 来管理 PowerShell 适用于 Windows File Server 文件系统的 FSx 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。为避免这些延迟，请使用 PowerShell 来管理位于多个文件系统上的文件共享。

请注意，对于 Windows 支持的所有文件系统，其文件和目录名称都必须遵循相应规则和限制。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《AWS Directory Service 管理指南》中选择以下过程：
  - [无缝加入 Windows EC2 实例](#)
  - [手动加入 Windows 实例](#)
2. 以文件系统管理员组成员的用户身份连接到实例。在 AWS 托管的 Microsoft Active Directory 中，该组被称为 AWS 委托 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。您还可以在[DescribeFilesystem](#) API 操作的响应中获取 DNS 名称。

6. 选择确定。随后，共享文件夹工具的列表中将显示 Amazon FSx 文件系统的条目。

现在，共享文件夹已连接到您的 Amazon FSx 文件系统，您可以管理文件系统上的 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 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。为避免这些延迟，您可以使用下述方法 PowerShell 管理文件共享。

## 使用管理文件共享 PowerShell

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

- 将现有文件服务器上的文件共享迁移到 Amazon FSx



- 跨 AWS 区域同步文件共享以进行灾难恢复
- 对持续工作流程的文件共享进行编程管理，如团队文件共享预置

要了解如何使用 Amazon FSx CLI 在上进行远程管理 PowerShell，请参阅。[使用 Amazon FSx CLI PowerShell](#)

下表列出了可用于管理适用于 Windows File Server 文件系统的 FSx 上文件共享的 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 )。 |
| 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 -?。

### 将凭据传递给 New-F 共享 SxSmb

您可以将凭据传递给 New-F，SxSmbShare 这样您就可以循环运行它来创建成百上千个共享，而不必每次都重新输入凭据。

使用以下方法之一，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 AWS 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) 共享

您可以在上使用用于远程管理的 Amazon FSx CLI 创建持续可用 (CA) 共享。PowerShell 在 FSx for Windows 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-fsxshare -name share_name }
```

如果启用 CA，则输出将包括以下行：

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

如果未启用 CA，则输出将包括以下行：

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

要在现有文件共享上启用“持续可用”，请使用以下命令：

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

## 文件访问审计

适用于 Windows File Server 的 Amazon FSx 支持审核最终用户对文件、文件夹和文件共享的访问权限。您可以选择将文件系统的审核事件日志发送到其他提供丰富功能的 AWS 服务。其中包括启用查询、处理、存储和存档日志、发布通知以及触发操作，以进一步推进您的安全与合规目标。

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](#)。

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。审核控制措施也称为 NTFS 系统访问控制列表 (SACL)。如果您已经对现有文件数据设置了审计控制措施，可以通过创建新的 Amazon FSx for Windows File Server 文件系统并迁移数据来使用文件访问审计。

Amazon FSx 支持以下针对文件、文件夹和文件共享访问的 Windows 审核事件：

- 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。

对于文件、文件夹和文件共享访问，Amazon FSx 支持记录成功的尝试（例如具有足够权限的用户成功访问文件或文件共享）、失败的尝试或同时记录两者。

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

- [审核事件日志目标](#)
- [迁移审核控制措施](#)
- [查看事件日志](#)
- [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 FSx 向其发送审核事件日志的 AWS 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 File Server 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。
- 如果您想将事件持续流式传输到亚马逊 S3 中的存储、亚马逊 Redshift 中的数据库、OpenSearch 亚马逊服务或合作伙伴解决方案（例如 Splunk 或 Datadog）AWS 进行进一步分析，请选择 Firehose。

默认情况下，Amazon FSx 将在您的账户中创建并使用默认 CloudWatch 日志组作为审核事件日志目标。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前 aws-fsx- 缀开头。如果您没有 Firehose 传送流，则可以在控制台创建或更新文件系统时创建一个 Firehose 传送流。
- 必须将 Firehose 传输流配置为 Direct PUT 用作其来源。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 Amazon FSx 文件系统位于同一个 AWS 分区中。AWS 区域 AWS 账户

您可以随时更改审核事件日志的目标（例如，从 Lo CloudWatch logs 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，审计事件日志记录会在几分钟内传送到目的地，但有时可能需要更长的时间。在极少数情况下，审核事件日志记录可能会有遗漏。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

如果您已对现有文件数据设置了审核控制措施（SACL），则可以创建 Amazon FSx 文件系统并将数据迁移到新的文件系统。我们建议使用 AWS DataSync 将数据和相关的 SACL 传输到您的 Amazon FSx 文件系统。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

Amazon FSx 开始发出审核事件日志之后，您便可以查看这些日志。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可以从中读取的目标。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 Data 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 指已访问的目标文件、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 是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 <YYYY-MM-DDThh:mm:ss.s> 以 Z 格式显示的时间。
- 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 |
| 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>
```

以下示例显示了从文件写入/追加数据，这些数据可以通过 AccessList %%4417 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='2021-06-03T19:12:16.813827100Z' />
<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;0ICI;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'>\\AMZNFSXCVDKLDZZ\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 logs 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

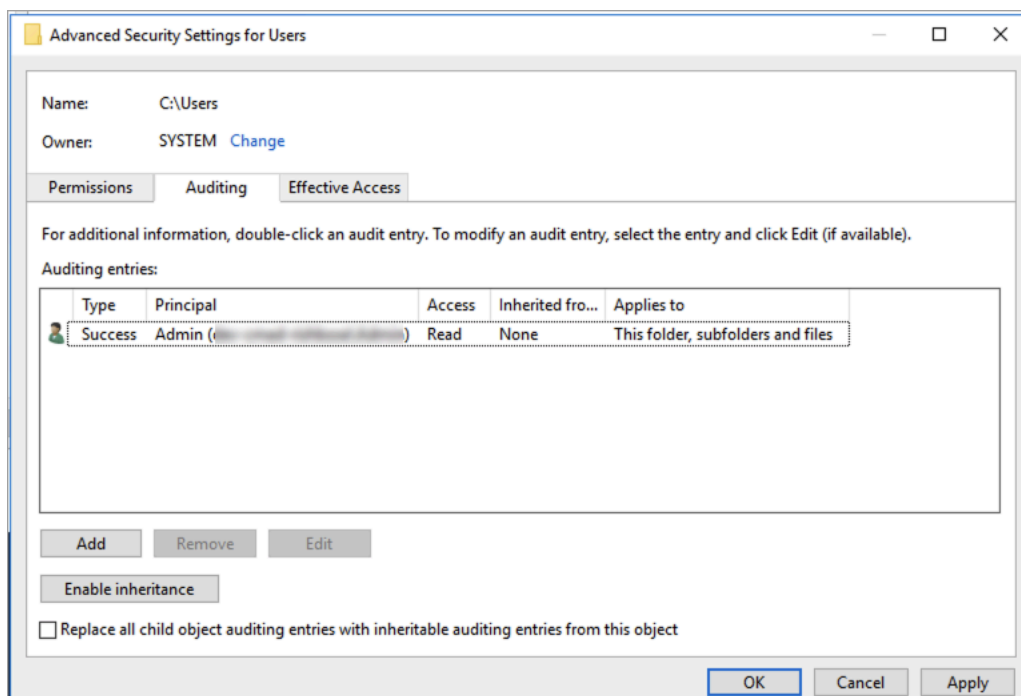
您需要为要审核用户访问尝试的文件和文件夹设置审核控制措施。审核控制措施也称为 NTFS 系统访问控制列表 (SACL)。

您可以使用 Windows 原生 GUI 界面或使用 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

您可以在创建新的 Amazon FSx for Windows File Server 文件系统时启用文件访问审计。当通过 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。

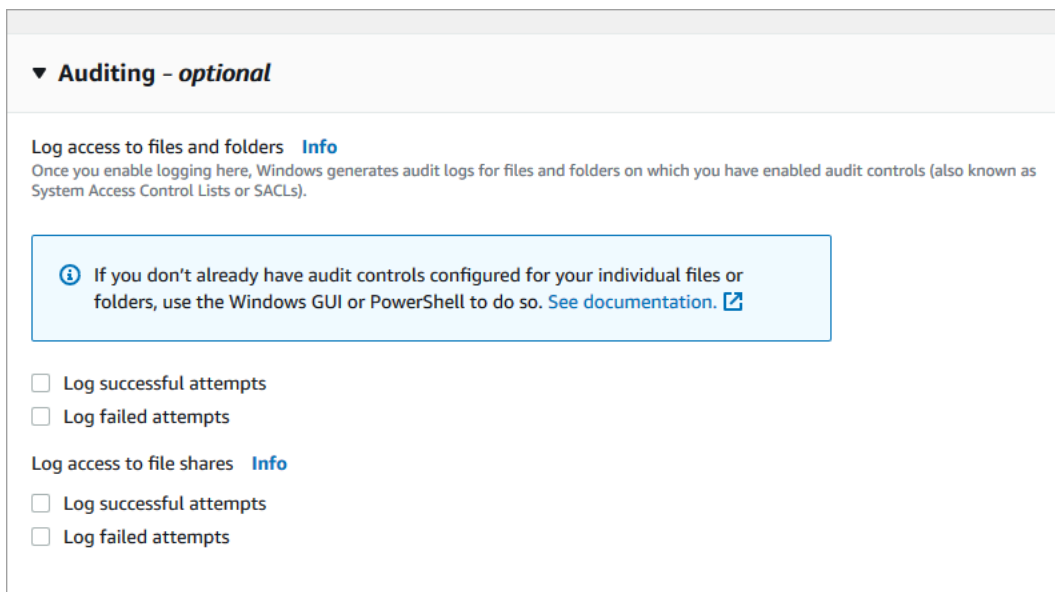
### AWS CLI

**Note**

只有吞吐能力为 32 Mb/s 或以上的 Amazon FSx for Windows File Server 文件系统支持文件访问审计。如果启用了文件访问审计，则无法创建或更新吞吐能力低于 32 MB/s 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. 通过以下网址打开 Amazon FSx 控制台：<https://console.aws.amazon.com/fsx/>。
2. 按照“入门”部分的[创建您的文件系统](#)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。



**▼ Auditing - optional**

**Log access to files and folders** [Info](#)  
Once you enable logging here, Windows generates audit logs for files and folders on which you have enabled audit controls (also known as System Access Control Lists or SACLs).

**Info** If you don't already have audit controls configured for your individual files or folders, use the Windows GUI or PowerShell to do so. [See documentation.](#)

Log successful attempts  
 Log failed attempts

**Log access to file shares** [Info](#)

Log successful attempts  
 Log failed attempts

4. 要启用和配置文件访问审计，请执行以下操作。
  - 对于文件和文件夹的日志访问权限，请选择成功和/或失败尝试日志记录。如果未做出选择，则会禁用文件和文件夹的日志记录。
  - 对于文件共享的日志访问权限，请选择成功和/或失败尝试日志记录。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。

▼ **Auditing - optional**

**Log access to files and folders** [Info](#)  
Once you enable logging here, Windows generates audit logs for files and folders on which you have enabled audit controls (also known as System Access Control Lists or SACLs).

**i** If you don't already have audit controls configured for your individual files or folders, use the Windows GUI or PowerShell to do so. [See documentation.](#)

Log successful attempts  
 Log failed attempts

**Log access to file shares** [Info](#)

Log successful attempts  
 Log failed attempts

Choose an audit event log destination

**CloudWatch Logs**  
View and search audit logs in the AWS management console and run queries on logs using CloudWatch Logs Insights

**Kinesis Data Firehose**  
Continuously stream audit events to S3, an Amazon Redshift database, Amazon ElasticSearch, or to partner solutions such as Splunk and Datadog for further analysis

Choose a CloudWatch Logs destination

/aws/fsx/windows ▼

[Create new](#)

**Pricing**  
Standard Amazon CloudWatch Logs pricing applies based on your usage. [Learn more](#)

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 [CreateFileSystem](#) API 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 \
 --audit-log-configuration {
 "LogAccessToFilesAndFolders": {
 "LogFailedAttempts": true,
 "LogSuccessfulAttempts": true,
 "Destination": "CloudWatchLogs",
 "DestinationName": "/aws/fsx/windows"
 },
 "LogAccessToFileShares": {
 "LogFailedAttempts": true,
 "LogSuccessfulAttempts": true,
 "Destination": "CloudWatchLogs",
 "DestinationName": "/aws/fsx/windows"
 }
 }
```

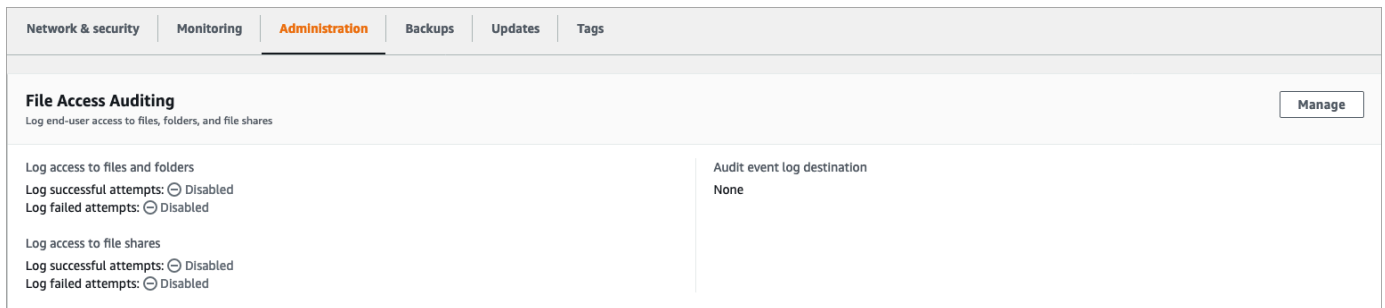


```
--windows-configuration
AuditLogConfiguration='{FileAccessAuditLogLevel="SUCCESS_AND_FAILURE", \
 FileShareAccessAuditLogLevel="SUCCESS_AND_FAILURE", \
 AuditLogDestination="arn:aws:logs:us-east-1:123456789012:log-group:/aws/fsx/my-
customer-log-group"}'
```

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. 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。

### Manage file access auditing settings ✕

**Log access to files and folders**  
Amazon FSx can log successful attempts to access files and folders, failed attempts to access files and folders, neither, or both. Once enabled here, audit logs are generated for files and folders on which audit controls (also known as System Access Control Lists or SACLs) have been configured.

Log successful attempts

Log failed attempts

**Log access to file shares**  
Amazon FSx can log successful attempts to access file shares, failed attempts to access file shares, neither, or both.

Log successful attempts

Log failed attempts

**Choose an audit event log destination**  
Amazon FSx supports access audit logging to one of the following audit destinations. If you change your audit destination, events will no longer be published to any previous audit destinations.

**CloudWatch Logs**  
View and search audit logs in the AWS management console and run queries on logs using CloudWatch Logs Insights

**Kinesis Data Firehose**  
Continuously stream audit events to S3, an Amazon Redshift database, Amazon Elasticsearch, or to partner solutions such as Splunk and DataDog for further analysis

**Choose a CloudWatch Logs destination**  
Use a default CloudWatch Logs log stream created by Amazon FSx, an existing log stream, or create a new log stream.

▼
[Create new](#)

**Pricing**  
Standard Amazon CloudWatch Logs pricing applies based on your usage. [Learn more](#)

Cancel Save

- 对于文件和文件夹的日志访问权限，请选择成功和/或失败尝试日志记录。如果未做出选择，则会禁用文件和文件夹的日志记录。
- 对于文件共享的日志访问权限，请选择成功和/或失败尝试日志记录。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"}'
```

## 用户会话和打开的文件

您可以使用“共享文件夹”工具，在 FSx for Windows File Server 文件系统中监视已连接的用户会话和打开的文件。共享文件夹工具提供了一个中心位置，用于监视谁连接到文件系统，以及打开了哪些文件以及由谁打开了哪些文件。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 来管理 PowerShell 用户会话，并在适用于 Windows 文件服务器的 FSx 文件系统中打开文件。

## 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 Amazon FSx 文件系统上的文件。

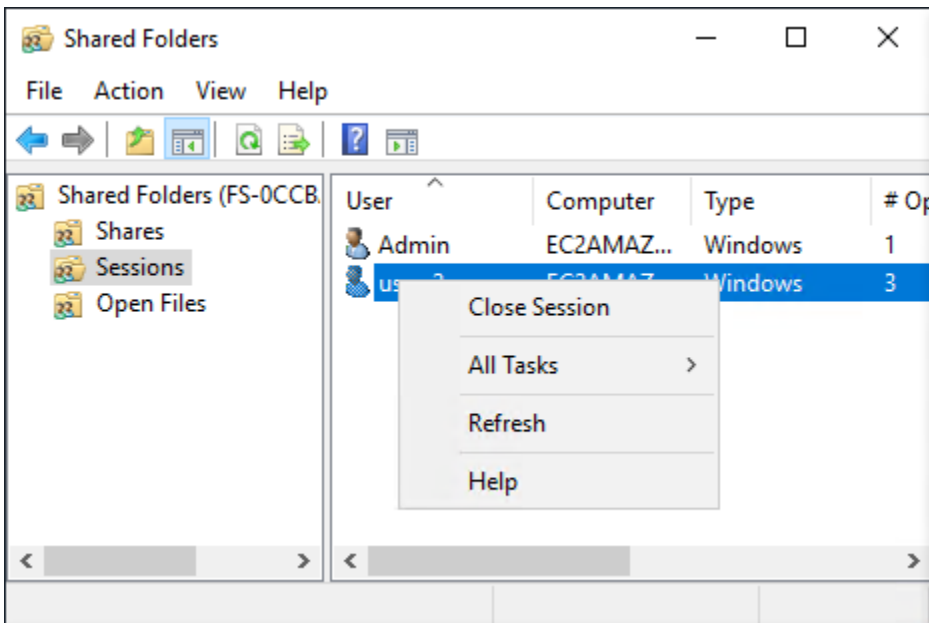
### 启动共享文件夹工具

1. 启动 Amazon EC2 实例，并将其连接到 Amazon FSx 文件系统加入的 Microsoft Active Directory。为此，请从《AWS Directory Service 管理指南》中选择以下过程：
  - [无缝加入 Windows EC2 实例](#)
  - [手动加入 Windows 实例](#)
2. 以文件系统管理员组成员的用户身份连接到实例。在 AWS 托管的 Microsoft Active Directory 中，该组被称为 AWS 委托 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 Amazon EC2 用户指南中的[连接到您的 Windows 实例](#)。
3. 打开开始菜单，然后使用 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。

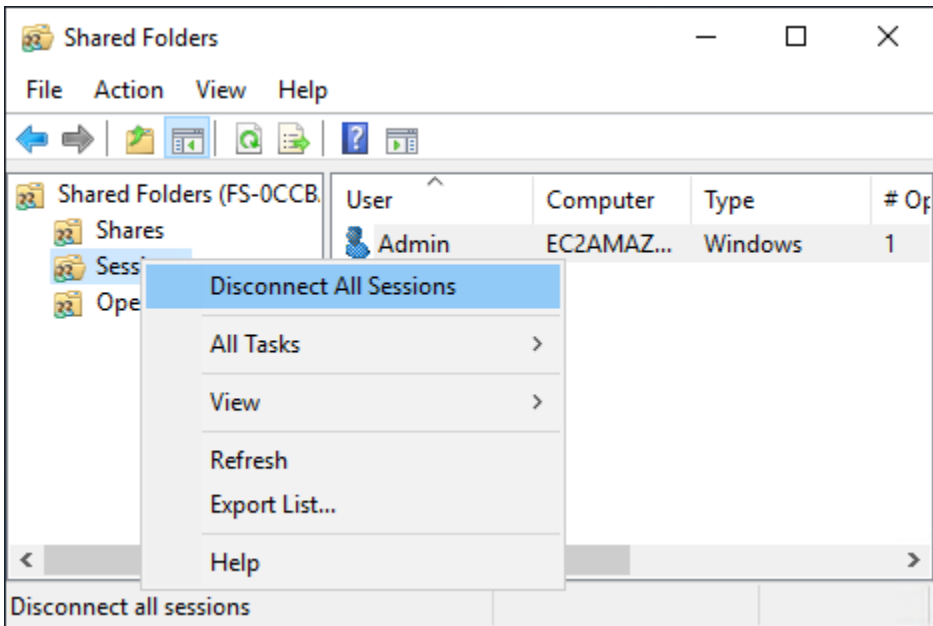
5. 在另一台计算机中，输入您的 Amazon FSx 文件系统的 DNS 名称，例如 `fs-012345678901234567.ad-domain.com`。
6. 选择确定。随后，共享文件夹工具的列表中将显示 Amazon FSx 文件系统的条目。

## 管理用户会话 (GUI)

在“共享文件夹”工具中，选择会话，查看连接到 FSx for Windows File Server 文件系统的所有用户会话。如果有用户或应用程序正在访问您的 Amazon FSx 文件系统上的文件共享，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。

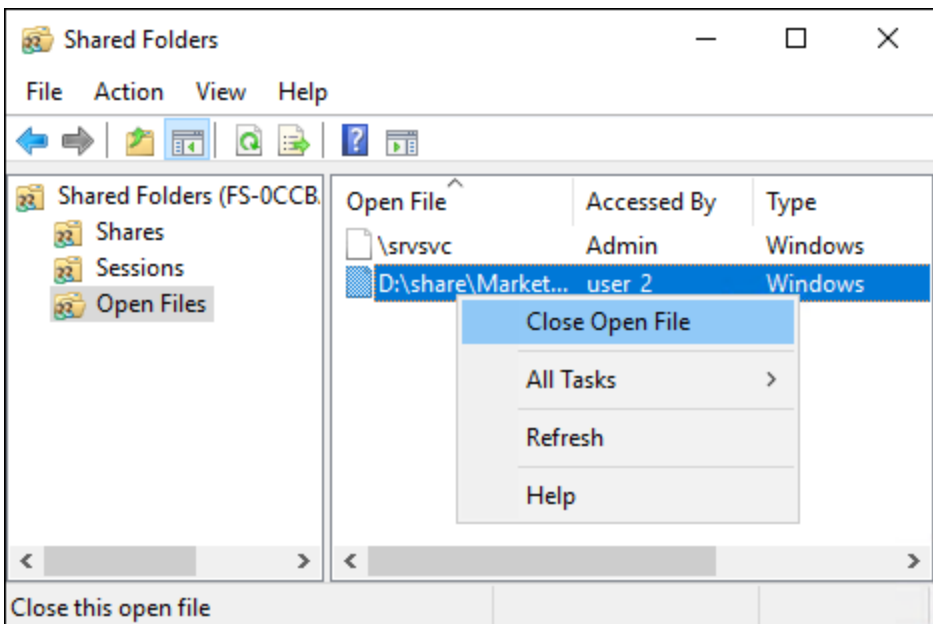


要断开所有打开的会话连接，请打开会话的上下文（右键单击）菜单，选择断开所有会话连接，然后确认操作。

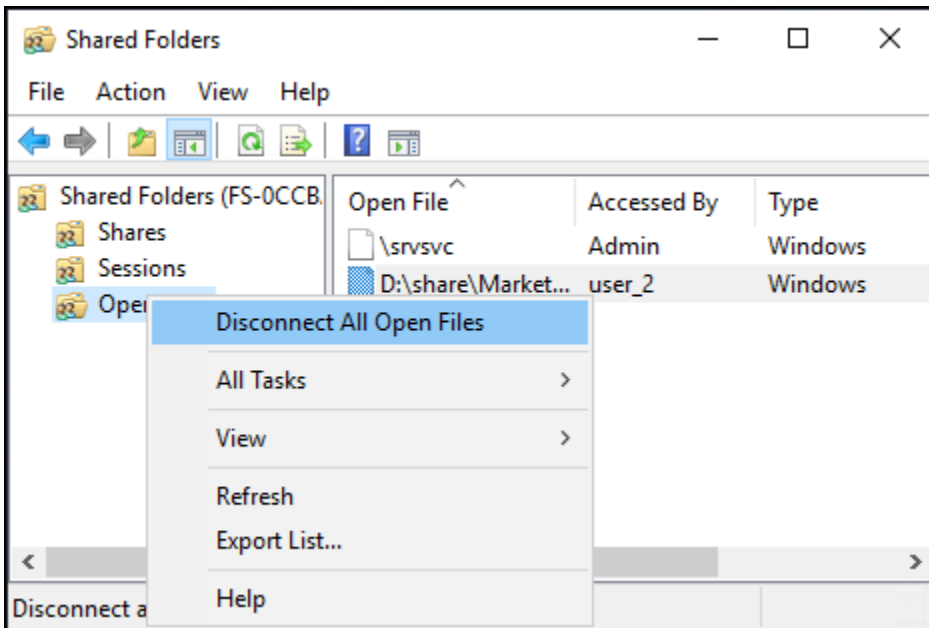


## 管理打开的文件 (GUI)

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 管理文件系统上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 [使用 Amazon FSx CLI PowerShell](#)。

下述为可用于管理用户会话和打开的文件的命令。

| 命令                   | 描述                                           |
|----------------------|----------------------------------------------|
| 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 -?`。

## 重复数据删除

FSx 支持使用 Microsoft 重复数据删除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，多个用户可以通过用户文件共享来存储同一文件的多个副本或版本。软件开发共享使得许多二进制文件在各个构建中都保持不变。

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。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。系统会在您使用重复数据删除功能时默认启用数据压缩，而在重复数据删除后进行压缩的操作会进一步减少数据存储量。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%。您可以使用下述命令 `Measure-FSxDedupFileMetadata` 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，因此我们建议使用下述命令 `Get-FSxDedupStatus` 来监控重复数据删除作业的状态。

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。

### Note

请参阅我们的最佳实践：[使用重复数据删除的最佳实践](#)。如果您在成功运行重复数据删除作业时遇到问题，请参阅[重复数据删除问题排查](#)。

### 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存在大量数据流失，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 [重复数据删除](#)。

## 管理重复数据删除

您可以使用 Amazon FSx CLI 来管理文件系统上的重复数据删除，以便在上进行远程 PowerShell 管理。要了解如何使用此 CLI，请参阅 [使用 Amazon FSx CLI 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                                                        |
|------------------------------------|-----------------------------------------------------------|
| <a href="#">Enable-FSxDedup</a>    | 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。        |
| <a href="#">Get-FSxDedupStatus</a> | 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。                                     |



| 重复数据删除命令                             | 描述                                                                             |
|--------------------------------------|--------------------------------------------------------------------------------|
| 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。                                                              |
| <a href="#">New-FSxDedupSchedule</a> | 创建和自定义重复数据删除计划。                                                                |
| <a href="#">Set-FSxDedupSchedule</a> | 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 Amazon FSx for Windows File Server 文件共享上启用重复数据删除，如下所示。

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxxxxx.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 amznfsxzzzzzzzzz.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 命令禁用默认的重叠数据删除计划，如下所示。

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzzz.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 amznfsxzzzzzzzzz.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 amznfsxxxxzzzzzzz.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不可靠，您不应使用这些值：容量 FreeSpace、UsedSpace UnoptimizedSize、和 SavingsRate。

## 重复数据删除问题排查

重复数据删除问题的潜在原因有很多，如下一部分所述。

### 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

按照我们的[重复数据删除文档](#)中的说明，运行 Get-FSxDedupStatus 命令以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 300 MB + 50 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。
- 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。内存分配是可以配置的（使用带参数 -Memory 的命令 Set-FSxDedupSchedule），但是消耗额外的内存可能会影响文件的性能。

- 您可以修改重复数据删除作业的配置，以进一步降低内存需求。例如，您可以将优化限制为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 的值意外设置为 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。

## 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。

## 管理用户存储配额

您可以使用 Amazon FSx CLI 来管理文件系统上的用户存储配额，以便在上进行远程管理。PowerShell 要了解如何使用此 CLI，请参阅 [使用 Amazon FSx CLI 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。 |
| Disable-FSxUserQuotas | 停止跟踪和强制执行用户存储配额。   |

| 用户存储配额命令                 | 描述                           |
|--------------------------|------------------------------|
| 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 -?`。

## 管理传输中加密

您可以使用一组自定义 PowerShell 命令来控制 FSx for Windows File Server 文件系统和客户端之间传输的数据的加密。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，`data-in-transit` 以便始终对文件系统进行加密。启用加密强制功能后 `data-in-transit`，从不支持 SMB 3.0 加密的客户端访问文件系统的用户将无法访问已启用加密功能的文件共享。

您还可以在文件共享级别而不是文件服务器级别控制加密。`data-in-transit` 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 在文件系统上管理用户传输中的加密，以便在上进行远程 PowerShell 管理。要了解如何使用此 CLI，请参阅 [使用 Amazon FSx CLI 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。                                                                                                                                                                        |
| Set-FSxSmbServerConfiguration | 此命令有两个用于配置传输中加密的选项： <ul style="list-style-type: none"> <li><code>-EncryptData \$True \$False</code> — 将此参数设置 <code>True</code> 为可开启传输中数据加密。将此参数设置 <code>False</code> 为可关闭传输中数据加密。</li> </ul> |

| 传输中加密命令 | 描述                                                                                                                                                                      |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | <ul style="list-style-type: none"><li>• <code>-RejectUnencryptedAccess \$True \$False</code> — 将此参数设置为，不允许不支持加密的客户机访问文件系统。True将此参数设置为，允许不支持加密的客户机访问文件系统。False</li></ul> |

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 -?`。

## 管理存储配置

文件系统的存储配置包括存储容量、存储类型和 SSD IOPS。可以在创建文件系统期间和之后，配置这些资源以及吞吐能力，以实现工作负载所需的性能级别。有关更多信息，请参阅以下主题。

主题

- [管理存储容量](#)
- [管理存储类型](#)
- [管理 SSD IOPS](#)

## 管理存储容量

您可以根据需要增加 FSx for Windows File Server 文件系统上配置的存储容量。您可以使用 Amazon FSx 控制台、Amazon RDS API 或 AWS Command Line Interface ( AWS CLI ) 来实现。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。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](#)。

主题



- [增加存储容量时需要了解的重要事项](#)
- [何时增加存储容量](#)
- [增加存储容量并提升文件系统性能](#)
- [如何增加存储容量](#)
- [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](#)

## 增加存储容量时需要了解的重要事项

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 65536 GiB。
- 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 16 MB/s。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](#)。

## 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 监控指标 CloudWatch](#)。

我们建议在文件系统上始终保持至少 10% 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 AWS 开发的自定义 AWS 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。具有大型活动数据集的写入密集型应用程序可能会暂时出现写入性能降低多达一半的情况。对于这些情况，您可以先增加文件系统的吞吐能力，然后再增加存储容量。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](#)。

## 如何增加存储容量

您可以使用 Amazon FSx 控制台、AWS CLI 或 Amazon FSx API 增加文件系统的存储容量。

### 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。

### Update storage capacity ×

File system ID  
fs-0257922e39ff24649


Current storage capacity  
100 GiB

Input type  
 Percentage  
 Absolute

Desired % increase  
 %  
Minimum 110 GiB (10% above current); Maximum 65536 GiB.  
New storage capacity: 110

Cancel Update

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 AWS 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 AWS 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

您可以使用 Amazon FSx 控制台、API 或 AWS CLI 监控存储容量的增加进度。

#### 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。

| Updates (10)                                                                                  |                |              |              |                           |
|-----------------------------------------------------------------------------------------------|----------------|--------------|--------------|---------------------------|
| <input type="text" value="Filter updates"/> <span style="float: right;">&lt; 1 &gt; ⚙️</span> |                |              |              |                           |
| Update type ▼                                                                                 | Target value ▼ | Status ▼     | Progress % ▼ | Request time ▲            |
| Storage capacity                                                                              | 154            | ✔️ Completed | -            | 2020-05-22T12:14:58-04:00 |
| Throughput capacity                                                                           | 64             | ✔️ Completed | -            | 2020-05-22T12:14:50-04:00 |
| Throughput capacity                                                                           | 128            | ✔️ Completed | -            | 2020-05-21T13:55:58-04:00 |
| Storage capacity                                                                              | 140            | ✔️ Completed | -            | 2020-05-21T13:55:30-04:00 |
| Storage capacity                                                                              | 122            | ✔️ Completed | -            | 2020-05-18T11:36:33-04:00 |

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。

### Target value (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 AWS CLI 和 API 监控增量

您可以使用 [describe-file-systems](#) AWS 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

当可用存储容量低于您指定的定义阈值时，您可以使用以下解决方案动态增加 FSx for Windows File Server 文件系统的存储容量。此 AWS 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 AWS Lambda 函数。

该解决方案会自动部署所需的所有组件，并采用以下参数：

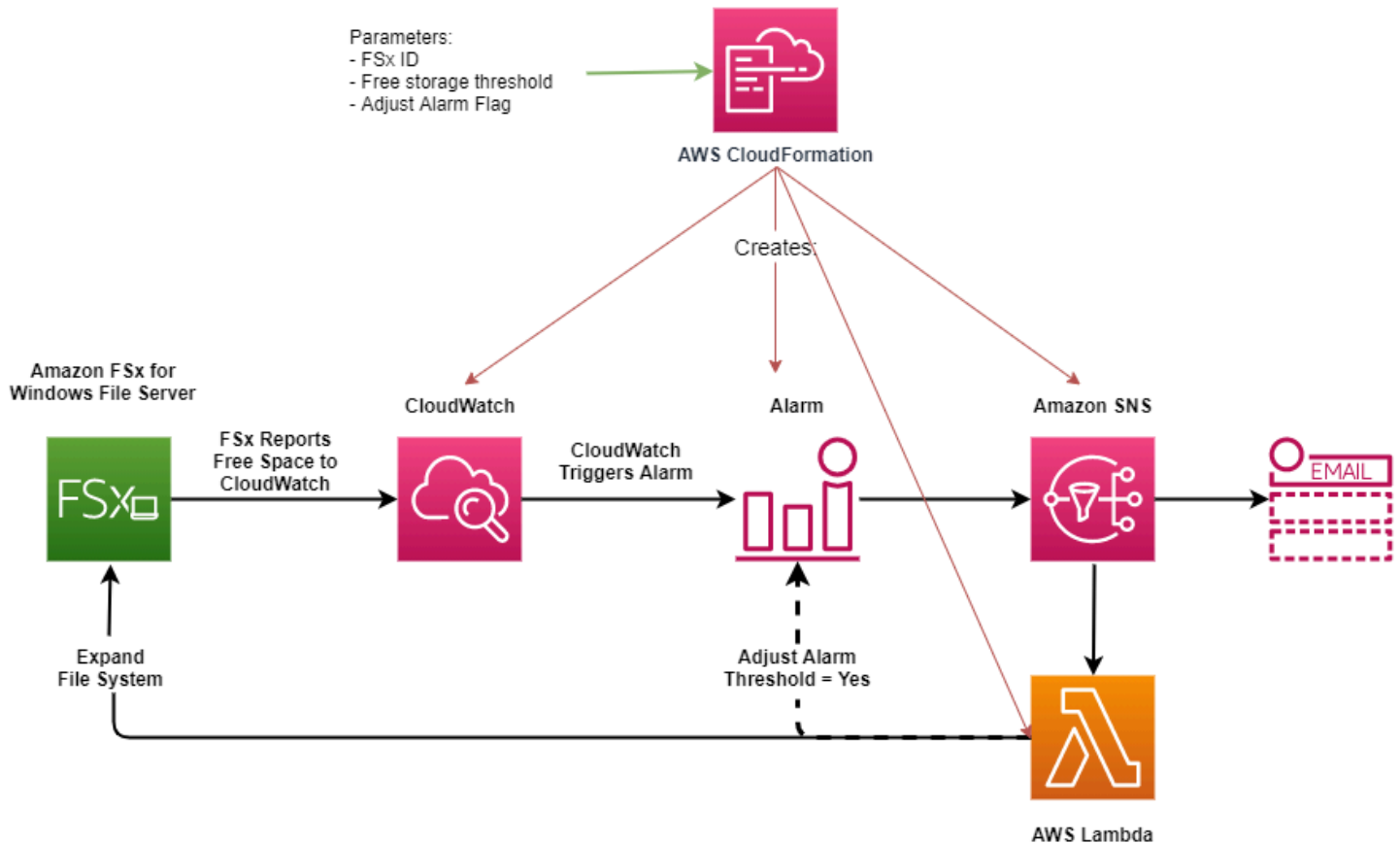
- 文件系统 ID
- 可用存储容量阈值（数值）
- 计量单位（百分比 [默认] 或 GiB）
- 增加存储容量的百分比（%）
- 订阅 SNS 的电子邮件地址
- 调整警报阈值（是/否）

### 主题

- [架构概述](#)
- [AWS CloudFormation 模板](#)
- [使用 AWS CloudFormation 自动部署](#)

### 架构概述

部署此解决方案将在 AWS 云中生成以下资源。



下图说明了以下步骤：

1. AWS CloudFormation 模板部署 CloudWatch 警报、AWS Lambda 函数、Amazon Simple Notification Service ( Amazon SNS ) 队列，以及所有必需的 AWS 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，您必须使订阅确认电子邮件中提供的链接来确认 Amazon SNS 主题订阅。



## AWS CloudFormation 模板

此解决方案使用 AWS 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](#) AWS CloudFormation 模板。

该模板使用如下所述的参数。查看模板参数及其默认值，并根据文件系统的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 AWS CloudFormation 自动部署

以下过程会配置和部署 AWS 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 AWS 服务的账单。有关更多信息，请参阅有关这些服务的定价详细信息页面。

在开始之前，您的 AWS 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[开始使用适用于 Windows File Server 的亚马逊 FSx](#)。

启动自动存储容量增加解决方案堆栈

1. 下载 [IncreaseFSxSize](#) AWS CloudFormation 模板。有关如何创建 CloudFormation 堆栈的更多信息，请参阅《AWS CloudFormation 用户指南》中的[在 AWS CloudFormation 控制台上创建堆栈](#)。

**Note**

Amazon FSx 目前仅在特定的 AWS 区域可用。您必须在可以使用 Amazon FSx 的 AWS 区域启动此解决方案。有关更多信息，请参阅《AWS 一般参考》中的[Amazon FSx 端点和配额](#)。

2. 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。

## Specify stack details

**Stack name**

Stack name

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

**Parameters**

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

**File System Parameters**

FileSystemId  
Amazon FSx file system ID

**Alarm Notification**

LowFreeDataStorageCapacityThreshold  
Low free data storage capacity threshold (GiB or %)

LowFreeDataStorageCapacityThresholdUnit  
Specify the Storage Capacity threshold Unit (GiB or %)

EmailAddress  
The email address for alarm notification.

**Other parameters**

AlarmModificationNotification  
Would you like to adjust the percent increase for the next FSx storage increase event proportionate to the requested increase?

PercentIncrease  
Provide the percent increase for File System Storage. This value should be between 10 and 100

Cancel Previous Next

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 Create (创建) 以部署堆栈。

您可以在 AWS CloudFormation 控制台的 Status (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《AWS CloudFormation 用户指南》中的[直接更新堆栈](#)。

## 管理存储类型

FSx for Windows File Server 提供固态硬盘 (SSD) 和磁性硬盘驱动器 (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。

您可以使用 Amazon FSx 控制台或 Amazon FSx API 将文件系统存储类型从 HDD 更改为 SSD。无法将文件系统存储类型从 SSD 更改为 HDD。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。

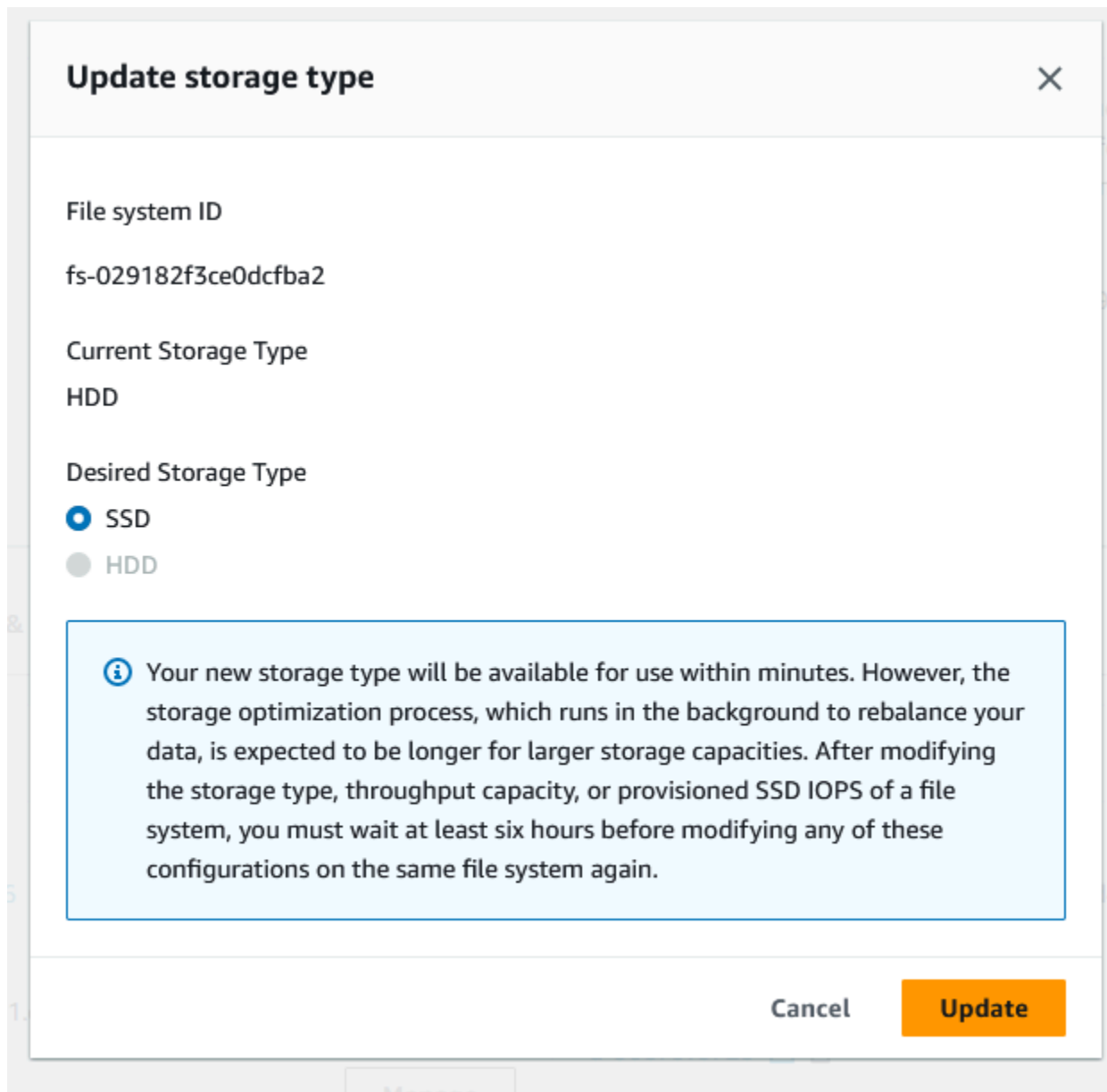
此外，还可以通过以下方法将文件系统存储类型从 HDD 更改为 SSD：还原可用备份以创建新的文件系统并选择新的存储类型。有关更多信息，请参阅[还原备份](#)。

## 如何更新存储类型

您可以使用 Amazon FSx 控制台、AWS CLI 或 Amazon FSx API 更新文件系统的存储类型。

### 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。
5. 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 AWS CLI 命令 [update-file-system](#)。设置以下参数：

- 将 `--file-system-id` 设置为要更新的文件系统的 ID。
- 将 `--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 AWS CLI 命令 [describe-file-systems](#) 来监控更新进度。在输出中，查找 `administrative-actions`。

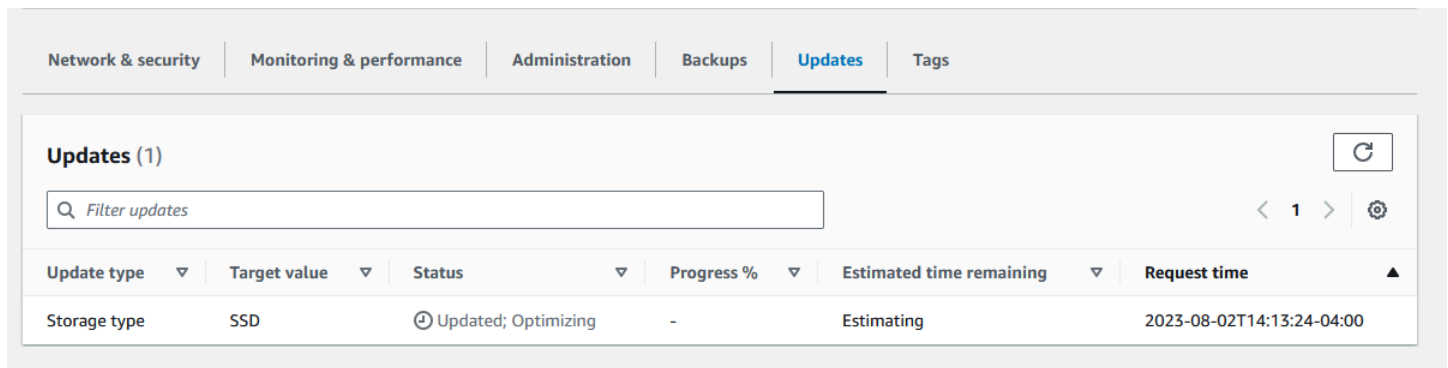
有关更多信息，请参阅 [AdministrativeAction](#)。

## 监控存储类型更新

您可以使用 Amazon FSx 控制台、API 或 AWS CLI 监控存储类型的更新进度。

### 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。



| Update type  | Target value | Status              | Progress % | Estimated time remaining | Request time              |
|--------------|--------------|---------------------|------------|--------------------------|---------------------------|
| Storage type | SSD          | Updated; Optimizing | -          | Estimating               | 2023-08-02T14:13:24-04:00 |

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。

### Target value (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 存储性能可用于工作负载的写入操作。您的更新将进入已更新；正在优化状态，该状态通常持续几个小时，在此期间，工作负载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 AWS CLI 和 API 监控更新

您可以使用 [describe-file-systems](#) AWS 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。

## 管理 SSD IOPS

对于 SSD 存储卷，您可以独立于存储容量选择和扩展 IOPS。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容量才能支持请求的 SSD IOPS 级别。有关更多信息，请参阅 [FSx for Windows File Server 性能](#) 和 [管理吞吐能力](#)。

## 主题

- [更新 SSD IOPS 时需要了解的重要事项](#)
- [如何更新 SSD IOPS](#)
- [监控预置的 SSD IOPS 更新](#)

## 更新 SSD IOPS 时需要了解的重要事项

更新 SSD IOPS 时，需要考虑以下几个重要事项：

- 要为文件系统指定预置 SSD IOPS 量，必须从以下两种 IOPS 模式中选择一种：
  - 自动 — Amazon FSx 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，每个文件系统最多保持 400,000 个固态硬盘 IOPS。
  - 用户配置 — 您可以将固态硬盘 IOPS 的数量指定在 96—400,000 范围内。为所有推出 Amazon FSx 的 AWS 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。如果 SSD IOPS 的数量不是每 GiB 至少 3 IOPS，则请求将失败。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 – 如果您增加了存储容量，且新容量所需的 SSD IOPS 级别高于用户预置的 SSD IOPS 级别，则 Amazon FSx 会自动将您的文件系统切换到自动模式。
- 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 AWS 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 )。

## 如何更新 SSD IOPS

您可以使用 Amazon FSx 控制台、AWS CLI 或 Amazon FSx API 更新文件系统的 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。



### Update IOPS Provisioning ✕

File system ID  
fs-0cfaa5ad762b33e6

Current file system configuration  
Storage capacity: 32 GiB  
Throughput capacity: 32 MB/s

Current Provisioned SSD IOPS  
Automatic

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

User-provisioned IOPS  
  
Minimum 96 IOPS; Maximum 350,000 IOPS

**i** After modifying the storage type, throughput capacity, or provisioned SSD IOPS of a file system, you must wait at least six hours before modifying any of these configurations on the same file system again.

Cancel Update

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。如果选择“用户配置”，请输入 96—400,000 范围内的任意整数。
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：

- 如果要指定固态硬盘 IOPS 的数量，请使用 `Iops=number_of_IOPS`，在支持的AWS区域和 `Mode=USER_PROVISIONED` 中最多为 400,000。
- 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维护每 GiB 存储容量 3 个 SSD IOPS，在支持的区域中最多可保持 400,000 个 IOPS。AWS

您可以使用AWS CLI命令监视更新进度[describe-file-systems](#)。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

您可以使用 Amazon FSx 控制台、API 或 AWS CLI，监控预置的 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。

| Update type | Target value     | Status  | Progress % | Estimated time remaining | Request time              |
|-------------|------------------|---------|------------|--------------------------|---------------------------|
| IOPS Mode   | USER_PROVISIONED | Pending | -          | -                        | 2023-07-31T17:08:45-04:00 |
| SSD IOPS    | 350              | Pending | -          | -                        | 2023-07-31T17:08:45-04:00 |

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 AWS CLI 和 API 监控更新

您可以使用 [describe-file-systems](#) AWS 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。

## 管理吞吐能力

对于每个 FSx for Windows File Server 文件系统，您都可以在创建文件系统时为其配置一个吞吐能力。您可以根据需要随时修改文件系统的吞吐能力。吞吐能力是决定托管文件系统的文件服务器处理文件数据的速度的一个因素。吞吐能力的级别越高，用于在文件服务器上缓存数据的每秒 I/O 操作次数 ( IOPS ) 和内存也就越高。有关更多信息，请参阅 [FSx for Windows File Server 性能](#)。

当您修改文件系统的吞吐能力时，Amazon FSx 会在后台关闭文件系统的文件服务器。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，会自动进行失效转移和失效自动恢复。对于单可用区系统，在吞吐能力扩展期间，您的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后，您需要为新的吞吐能力付费。

**Note**

在后端维护操作期间，系统修改（例如对吞吐能力的修改）可能会出现延迟。维护会导致这些更改排队等待处理。

**主题**

- [何时修改吞吐能力](#)
- [如何修改吞吐能力](#)
- [监控吞吐能力更改](#)

## 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 监控指标 CloudWatch](#)。

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。

## 如何修改吞吐能力

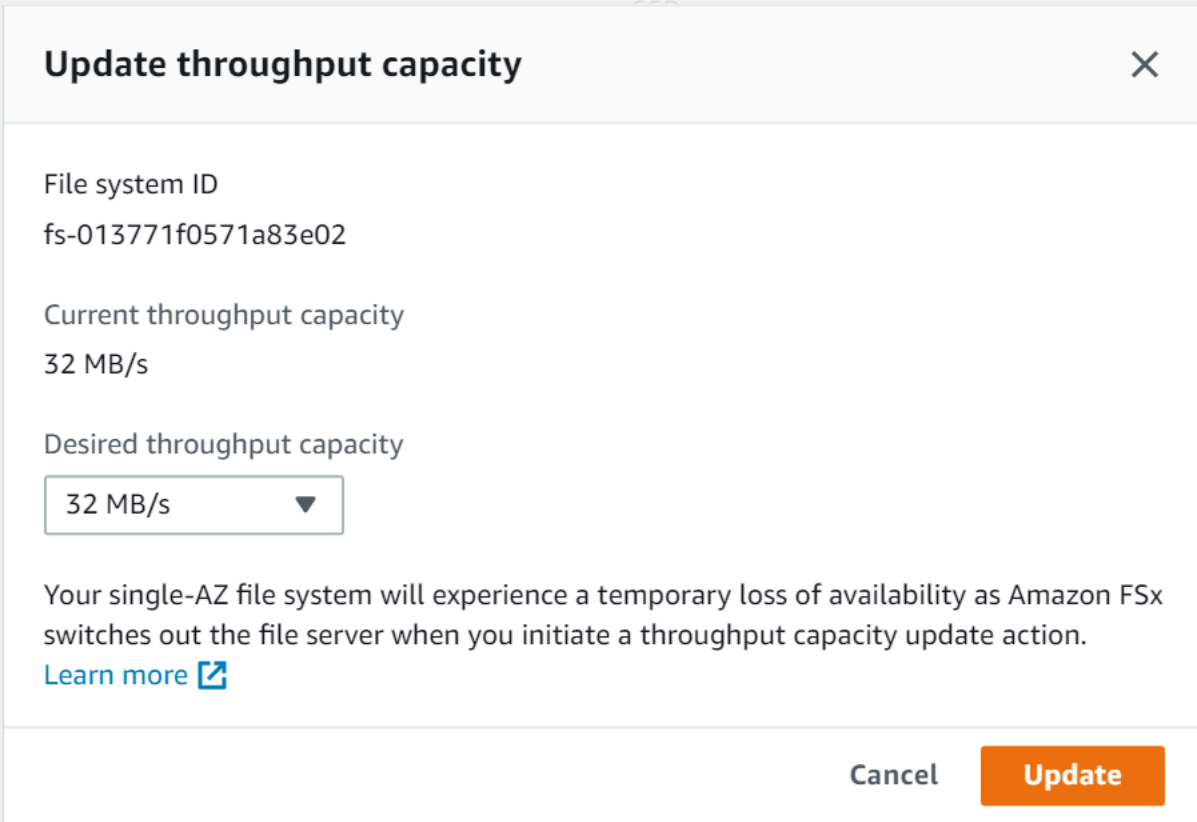
您可以使用 Amazon FSx 控制台、AWS Command Line Interface (AWS CLI) 或 Amazon FSx API 修改文件系统的吞吐能力。

## 修改文件系统的吞吐能力 (控制台)

1. 通过以下网址打开 Amazon FSx 控制台：<https://console.aws.amazon.com/fsx/>。
2. 导航到文件系统，然后选择要增加其吞吐能力的 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。




**Update throughput capacity** ✕

File system ID  
fs-013771f0571a83e02

Current throughput capacity  
32 MB/s

Desired throughput capacity  
32 MB/s ▼

Your single-AZ file system will experience a temporary loss of availability as Amazon FSx switches out the file server when you initiate a throughput capacity update action.  
[Learn more](#) 

Cancel **Update**

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、AWS CLI 和 API 来监控更新进度。有关更多信息，请参阅[监控吞吐能力更改](#)。

## 修改文件系统的吞吐能力 ( CLI )

要修改文件系统的吞吐能力，请使用 AWS CLI 命令 [update-file-system](#)。设置以下参数：

- 将 `--file-system-id` 设置为要更新的文件系统的 ID。
- 将 `ThroughputCapacity` 设置为要将文件系统更新到的所需值。

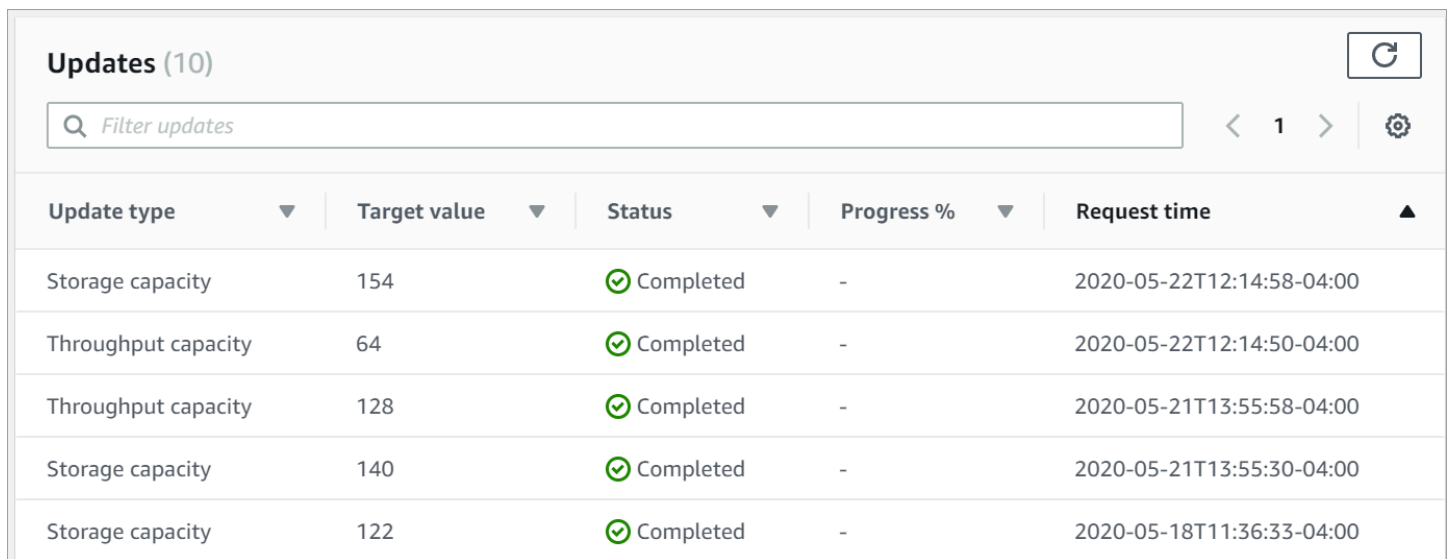
您可以使用 Amazon FSx 控制台、AWS CLI 和 API 来监控更新进度。有关更多信息，请参阅[监控吞吐能力更改](#)。

## 监控吞吐能力更改

您可以使用 Amazon FSx 控制台、API 和 AWS CLI 监控吞吐能力的修改进度。

### 在控制台中监控吞吐能力更改

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。



The screenshot shows the 'Updates (10)' section in the Amazon FSx console. It includes a search bar for filtering updates, a refresh button, and a table with columns for Update type, Target value, Status, Progress %, and Request time. The table lists five recent updates, all of which are 'Completed'.

| Update type         | Target value | Status    | Progress % | Request time              |
|---------------------|--------------|-----------|------------|---------------------------|
| Storage capacity    | 154          | Completed | -          | 2020-05-22T12:14:58-04:00 |
| Throughput capacity | 64           | Completed | -          | 2020-05-22T12:14:50-04:00 |
| Throughput capacity | 128          | Completed | -          | 2020-05-21T13:55:58-04:00 |
| Storage capacity    | 140          | Completed | -          | 2020-05-21T13:55:30-04:00 |
| Storage capacity    | 122          | Completed | -          | 2020-05-18T11:36:33-04:00 |

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。

### Target value (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 AWS 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 MB/s，目标吞吐能力为 256 MB/s。

```
.
. .
.
 "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](#)。

## 标记 Amazon FSx 资源

为帮助您管理文件系统和其他 Amazon FSx 资源，您可以通过标签的形式为每个资源分配您自己的元数据。标签可让您按各种标准（例如用途、所有者或环境）对 AWS 资源进行分类。这在您具有相同类型的很多资源时会很有用—您可以根据分配给特定资源的标签快速识别该资源。本主题介绍标签并说明如何创建标签。

### 主题

- [有关标签的基本知识](#)
- [标记您的资源](#)
- [标签限制](#)
- [权限和标签](#)

## 有关标签的基本知识

标签是为 AWS 资源分配的标记。每个标签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 AWS 资源进行分类。例如，您可以为账户中的 Amazon FSx 文件系统定义一组标签，以跟踪每个实例的所有者和堆栈级别。

我们建议您针对每类资源设计一组标签，以满足您的需要。使用一组连续的标签键，管理资源时会更加轻松。您可以根据添加的标签搜索和筛选资源。有关如何实施有效的资源标记策略的更多信息，请参阅 AWS 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 Amazon FSx API、AWS CLI 或 AWS SDK，则可以使用 TagResource API 操作向现有资源应用标签。此外，某些资源创建操作允许您在创建资源时为其指定标签。如果无法在资源创建期间应用标签，系统会回滚资源创建过程。这样可确保要么创建带有标签的资源，要么根本不创建资源，即任何时候都不会创建出未标记的资源。通过在创建时标记资源，您不需要在资源创建后运行自定义标记脚本。有关允许用户在创建时标记资源的更多信息，请参阅 [在创建过程中授予标记资源的权限](#)。

## 标记您的资源

您可以标记账户中已存在的 Amazon FSx 资源。如果您使用的是 Amazon FSx 控制台，您可以使用相关资源屏幕上的“标签”选项卡向资源应用标签。创建资源时，您可以应用带有值的“名称”键，也可以在创建新文件系统时应用您选择的标签。控制台可能根据“名称”标签对资源进行组织，但此标签对 Amazon FSx 服务没有任何语义意义。

对于支持在创建时进行标记的 Amazon FSx API 操作，您可以在 IAM policy 中应用基于标签的资源级权限，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 policy 中对 TagResource 和 UntagResource Amazon FSx 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《AWS 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 Amazon FSx 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 AWS 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 AWS 账户 可用；其他 AWS 账户 无权访问这些标签。为了对共享资源进行基于标签的访问控制，每个 AWS 账户 必须分配自己的一组标签来控制对资源的访问。

## 权限和标签

有关在创建时标记 Amazon FSx 资源所需权限的更多信息，请参阅[在创建过程中授予标记资源的权限](#)。有关如何在 IAM policy 中使用标签限制对 Amazon FSx 资源的访问权限的更多信息，请参阅[使用标签控制对 Amazon FSx 资源的访问权限](#)。

## 使用 Amazon FSx 维护时段

Amazon FSx for Windows File Server 会执行针对由其托管的 Microsoft Windows Server 软件的常规软件修补。您可以通过维护时段来控制该软件修补每周的周几和几点进行。您可以在创建文件系统期间选择维护时段。如果您没有时间偏好，则会为其分配一个 30 分钟的默认时段。

FSx for Windows File Server 允许您调整维护时段，适应您的工作负载和操作要求。您可以根据需要频繁更改维护时段，但至少每 14 天安排一次维护时段。如果已发布补丁但您未在 14 天内安排维护时段，FSx for Windows File Server 会执行文件系统维护，确保其安全性和可靠性。

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。您的多可用区文件系统会保持可用状态，并自动在首选文件服务器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[FSx for Windows File Server 失效转移进程](#)。由于多可用区文件系统的修补会引起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流向文件系统的所有流量。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 会在维护开始之前关闭所有机会性锁定，并完成对托管文件系统的底层存储卷的所有待处理写入操作。

您可以使用 Amazon FSx 管理控制台、AWS CLI、AWS API 或某个 AWS SDK 来更改文件系统的维护时段。

#### 更改每周维护时段 (控制台)

1. 通过以下网址打开 Amazon FSx 控制台：<https://console.aws.amazon.com/fsx/>。
2. 在左侧导航栏中选择文件系统。
3. 选择要更改每周维护时段的文件系统。随即显示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-system](#) CLI 命令更改每周维护时段，请参阅[演练 3：更新现有文件系统](#)。

## 管理 Amazon FSx 文件系统的最佳实践

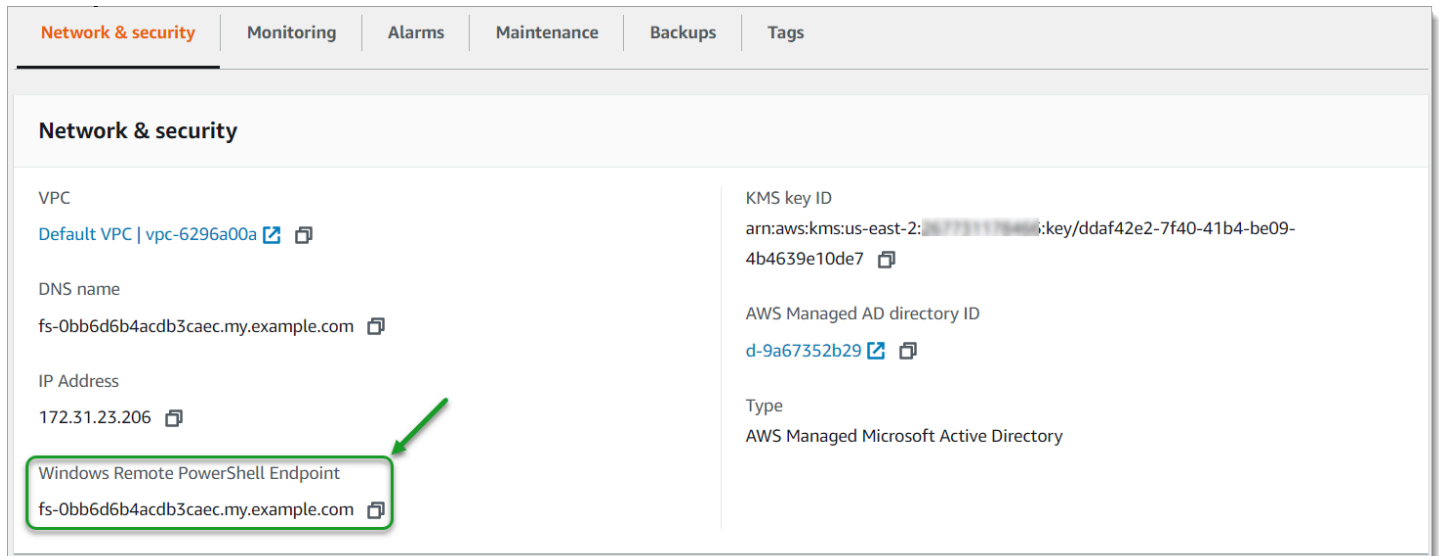
Amazon FSx 提供了多种功能，可帮助您实施管理文件系统的最佳实践，包括：

- 优化存储消耗量
- 使最终用户能够将文件和文件夹恢复到以前的版本
- 强制对所有连接的客户端加密

在 PowerShell 命令上使用以下 Amazon FSx CLI 进行远程管理，以便在您的文件系统上快速实施这些最佳实践。

要运行这些命令，你必须知道文件系统的 Windows 远程 PowerShell 端点。要找到此端点，请按照以下步骤操作：

1. 通过以下网址打开 Amazon FSx 控制台：<https://console.aws.amazon.com/fsx/>。
2. 选择文件系统。在“网络和安全”选项卡上，找到 Windows 远程 PowerShell 端点，如下所示。



有关更多信息，请参阅 [管理文件系统](#) 和 [使用 Amazon FSx CLI PowerShell](#)。

## 主题

- [一次性管理设置任务](#)
- [持续管理任务可监控您的文件系统](#)

## 一次性管理设置任务

以下是您可以为文件系统一次性快速设置的任务。

### 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 [重复数据删除](#)。

- 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 [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 [将卷影子副本配置为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](#)。

## 持续管理任务可监控您的文件系统

以下持续任务可帮助您监控文件系统的磁盘使用情况、用户限额和打开的文件。

### 监控重复数据删除状态

监控重复数据删除状态，包括在文件系统中实现的节省率，如下所示。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -
ConfigurationName FsxRemoteAdmin -ScriptBlock { Get-FSxDedupStatus } | select
OptimizedFilesCount,OptimizedFilesSize,SavedSpace,OptimizedFilesSavingsRate
```

### 监控用户级别的存储消耗量

获取有关当前用户存储限额条目的报告，包括他们消耗了多少空间，以及他们是否违反了限制和警告阈值。

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

### 监控和关闭打开的文件

通过查找已打开的文件并将其关闭来管理处于打开状态的文件。使用以下命令检查已打开的文件。

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

使用以下命令关闭已打开的文件。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock { Close-FSxSmbOpenFile -Confirm:$false}
```

## 使用 DFS 命名空间为多个文件系统分组

Amazon FSx for Windows File Server 支持使用 Microsoft 的分布式文件系统 (DFS)。您可以使用 DFS 命名空间将多个文件系统上的文件共享分组到一个用于访问整个文件数据集的公共文件夹结构 (命名空间)。DFS 命名空间可以帮助您整理和统一对跨多个文件系统的文件共享的访问。DFS 命名空间还可以帮助大型文件数据集扩展文件数据存储,使其超出每个文件系统所支持的容量 (64 TB),最高可达数百 PB。

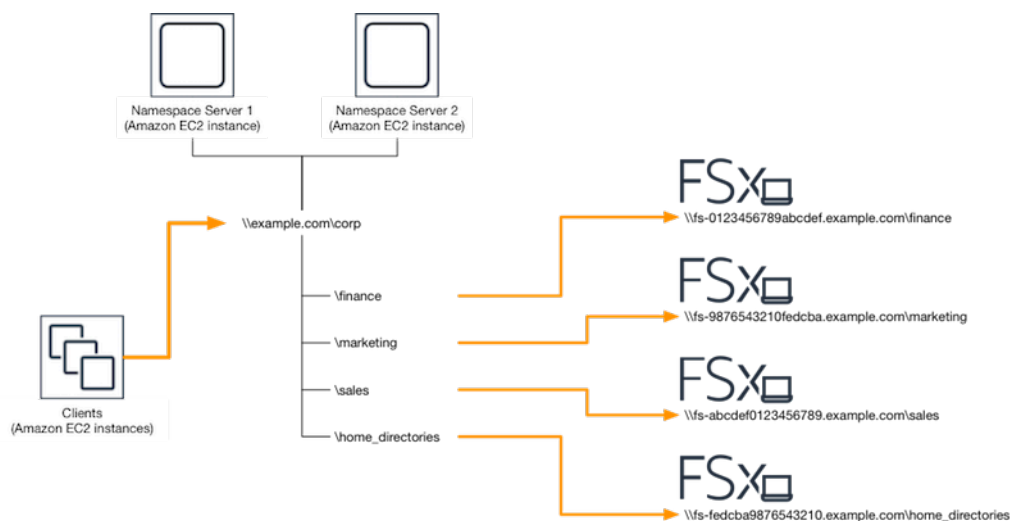
### 设置 DFS 命名空间以为多个文件系统分组

您可以使用 DFS 命名空间将多个文件系统分组到单个的命名空间。在以下示例中,基于域的命名空间 (example.com\corp) 创建在两个命名空间服务器上,合并了存储在多个 Amazon FSx 文件系统 (财务、营销、销售、home\_directories) 上的文件共享。这允许您的用户使用公共命名空间访问文件共享。因此他们无需为托管文件共享的每个文件系统指定文件系统 DNS 名称。

#### Note

无法将 Amazon FSx 添加到 DFS 共享路径的根目录。

这些步骤将指导您在两个命名空间服务器上创建单个命名空间 (example.com\corp)。您还可以在命名空间下设置四个文件共享,每个文件共享都会以透明方式将用户重定向到托管在单独的 Amazon FSx 文件系统上的共享。



## 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 [s etu](#) AWS CloudFormation p-dfsn-Servers.Template 模板启动一对高度可用的 DFS 命名空间服务器。有关创建 AWS CloudFormation 堆栈的更多信息，请参阅《AWS CloudFormation 用户指南》中的[在 AWS CloudFormation 控制台上创建堆栈](#)。
2. 以 AWS 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。有关更多信息，请参阅 Amazon EC2 用户指南中的[连接到您的 Windows 实例](#)。
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。

# 监控 FSx for Windows File Server

监控是维护 Amazon FSx 和您的 AWS 解决方案的可靠性、可用性和性能的重要组成部分。您应该从 AWS 解决方案的各个部分收集监控数据，以便在出现多点故障时可以更轻松地进行调试。不过，在开始监控 Amazon FSx 之前，您应制定一个监控计划并在计划中回答下列问题：

- 监控目的是什么？
- 您将监控哪些资源？
- 监控这些资源的频率如何？
- 您将使用哪些监控工具？
- 谁负责执行监控任务？
- 出现错误时应通知谁？

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

- [监控工具](#)
- [使用 Amazon 监控指标 CloudWatch](#)
- [使用 AWS CloudTrail 记录 Amazon FSx for Windows File Server 的 API 调用日志](#)

## 监控工具

AWS 提供了可用于监控 Amazon FSx 的各种工具。您可以配置其中的一些工具来为您执行监控任务，但有些工具需要手动干预。建议您尽可能实现监控任务自动化。

### 自动监控工具

您可以使用以下自动化监控工具来监控 Amazon FSx，并在出现错误时进行报告：

- A CloudWatch mazon Alarms — 在您指定的时间段内观察单个指标，并根据该指标在多个时间段内相对于给定阈值的值执行一项或多项操作。该操作是发送到亚马逊简单通知服务 (Amazon SNS) Simple Notification Scaling 主题或亚马逊 EC2 Auto Scaling 策略的通知。CloudWatch 警报不会仅仅因为它们处于特定状态就调用操作；该状态必须已更改并保持了指定的时间段。有关更多信息，请参阅 [使用 Amazon 监控指标 CloudWatch](#)。

- Amazon CloudWatch Logs — 监控、存储和访问来自 AWS CloudTrail 或其他来源的日志文件。有关更多信息，请参阅[什么是 Amazon CloudWatch 日志？](#) 在 Amazon CloudWatch 日志用户指南中。
- AWS CloudTrail 日志监控-在账户之间共享日志文件，通过将 CloudTrail 日志文件发送到“日志”来实时监控 CloudWatch 日志文件，用 Java 编写日志处理应用程序，并验证您的日志文件在传送后是否未更改 CloudTrail。有关更多信息，[请参阅AWS CloudTrail 用户指南中的使用 CloudTrail 日志文件。](#)

## 手动监控工具

监控 Amazon FSx 的另一个重要部分涉及手动监控亚马逊 CloudWatch 警报未涵盖的项目。Amazon FSx 和其他 AWS 控制台控制面板提供您的 AWS 环境状态 at-a-glance 视图。CloudWatch

Amazon FSx 控制台的监控和性能控制面板显示：

- 当前适用于 Windows File Server 的 FSx 警告 CloudWatch 和警报
- 显示文件系统活动摘要的图表
- 文件系统存储容量和利用率图表
- 文件服务器和存储卷性能图表
- CloudWatch 警报

CloudWatch 主页显示：

- 当前告警和状态
- 告警和资源图表
- 服务运行状况

此外，您还可以使用 CloudWatch 执行以下操作：

- 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。
- 搜索并浏览您的所有 AWS 资源指标。
- 创建和编辑告警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[如何使用 FSx for Windows File Server 指标](#)。

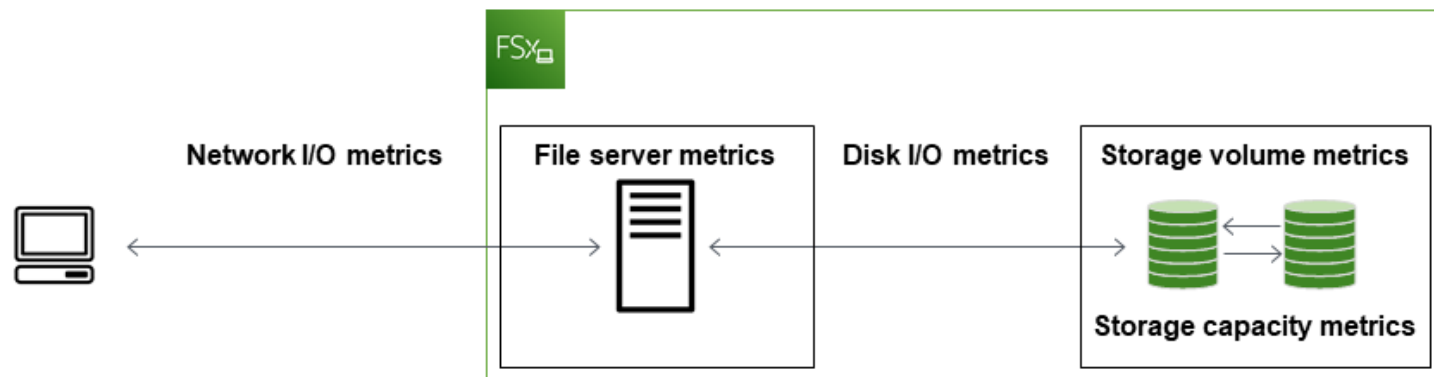
## 使用 Amazon 监控指标 CloudWatch

您可以使用亚马逊监控适用于 Windows File Server 文件系统的 FSx，CloudWatch 亚马逊收集来自适用于 Windows File Server 的 fsX 的原始数据，并将其处理为可读的、近乎实时的指标。这些统计数据会保存 15 个月，从而使您能够访问历史信息，并能够了解您的 Web 应用程序或文件系统的执行情况。

适用于 Windows File Server 的 FsX 在以下领域 CloudWatch 发布指标：

- 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 以 1 分钟为周期向发送指标数据 CloudWatch，但以下例外情况每隔 5 分钟发送一次：

- FileServerDiskThroughputBalance
- FileServerDiskIopsBalance

有关的更多信息 CloudWatch，请参阅 [Amazon 是什么 CloudWatch？](#) 在《亚马逊 CloudWatch 用户指南》中。

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。

有些 Amazon FSx CloudWatch 指标报告为原始字节。字节数不会舍入到十进制或二进制单位倍数。

## 主题

- [指标与维度](#)
- [如何使用 FSx for Windows File Server 指标](#)
- [性能警告和建议](#)
- [访问 FSx for Windows File Server 指标](#)
- [创建 CloudWatch 警报以监控 Amazon FSx](#)

## 指标与维度

FSx for Windows File Server 将以下指标发布到 CloudWatch 亚马逊AWS/FSx的命名空间中，适用于所有文件系统：

- DataReadBytes
- DataWriteBytes
- DataReadOperations
- DataWriteOperations
- MetadataOperations
- FreeStorageCapacity

FSx for Windows File Server 将以下所述的指标发布到AWS/FSx CloudWatch 亚马逊的命名空间中，适用于吞吐量至少为 32 Mbps 的文件系统。

## 主题

- [FSx for Windows 网络 I/O 指标](#)
- [FSx for Windows 文件服务器指标](#)

- [FSx for Windows 磁盘 I/O 指标](#)
- [FSx for Windows 存储卷指标](#)
- [FSx for Windows 存储容量指标](#)
- [FSx for Windows 维度](#)

## FSx for Windows 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。<br><br>单位：字节<br><br>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。<br><br>单位：字节<br><br>有效统计数据：Sum |
| DataReadOperations  | 访问文件系统的客户端的读取操作数。<br><br>单位：计数<br><br>有效统计数据：Sum   |
| DataWriteOperations | 访问文件系统的客户端的写入操作数。<br><br>单位：计数<br><br>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。<br><br>单位：计数<br><br>有效统计数据：Sum  |

| 指标                | 描述                          |
|-------------------|-----------------------------|
| ClientConnections | 客户端与文件服务器之间的活动连接数。<br>单位：计数 |

## FSx for Windows 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。<br>单位：百分比                            |
| CPUUtilization                      | 文件服务器 CPU 资源的利用率百分比。<br>单位：百分比                                      |
| MemoryUtilization                   | 文件服务器内存资源的利用率百分比。<br>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。<br>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。<br>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。<br>单位：百分比                 |

| 指标                        | 描述                                                                                |
|---------------------------|-----------------------------------------------------------------------------------|
| FileServerDiskIopsBalance | <p>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。</p> <p>单位：百分比</p> |

## FSx for Windows 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       | <p>访问存储卷的读取操作字节数。</p> <p>单位：字节</p> <p>有效统计数据：Sum</p>     |
| DiskWriteBytes      | <p>访问存储卷的写入操作字节数。</p> <p>单位：字节</p> <p>有效统计数据：Sum</p>     |
| DiskReadOperations  | <p>访问存储卷的文件服务器的读取操作数。</p> <p>单位：计数</p> <p>有效统计数据：Sum</p> |
| DiskWriteOperations | <p>访问存储卷的文件服务器的写入操作数。</p> <p>单位：计数</p> <p>有效统计数据：Sum</p> |



## 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。<br><br>单位：百分比      |
| DiskThroughputBalance     | (仅限 HDD) 存储卷磁盘吞吐量的可用突增点数百分比。<br><br>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。<br><br>单位：百分比 |

## FSx for Windows 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。<br><br>单位：字节<br><br>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。<br><br>单位：百分比                  |
| DeduplicationSavedStorage  | 启用了重复数据删除时节省的存储空间量。<br><br>单位：字节                      |

## FSx for Windows 维度

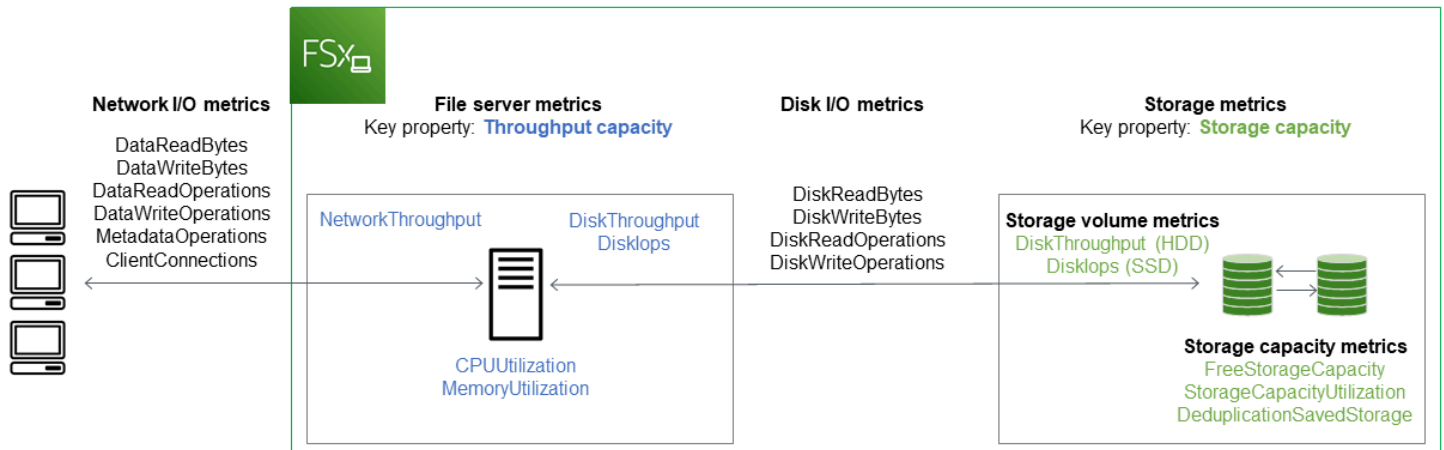
FSx for Windows File Server 指标使用 FSx 命名空间，并且为单个维度 FileSystemId 提供指标。您可以使用 [describe-file-systems](#) AWS CLI 命令或 [DescribeFileSystems](#) API 命令查找文件系统的 ID。文件系统 ID 采用 *fs-0123456789abcdef0* 形式。

## 如何使用 FSx for Windows File Server 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，用于托管文件系统的数据。

FSx for Windows File Server 报告 CloudWatch 中的指标，这些指标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供 CloudWatch 监控的性能和资源指标。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。



使用 Amazon FSx 控制台中的“监控和性能”面板查看下表中描述的 FSx for Windows File S CloudWatch erver 指标。

| “监控和性能”面板 | 如何...              | 图表     | 相关指标                       |
|-----------|--------------------|--------|----------------------------|
| Summary   | ...确定文件系统的总 IOPS ? | 总 IOPS | 总和 ( DataRead0 perations + |

| “监控和性能”面板  | 如何...                                              | 图表              | 相关指标                                                      |
|------------|----------------------------------------------------|-----------------|-----------------------------------------------------------|
|            |                                                    |                 | 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                                       |
|            | ...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                                |
| 存储         | ...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                                 |
|            | ...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                              |
| 性能 – 文件服务器 | ...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                       |
|            | ...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                           |

| “监控和性能”面板 | 如何...                                             | 图表                | 相关指标                           |
|-----------|---------------------------------------------------|-------------------|--------------------------------|
|           | ...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       | FileServerDiskIops Utilization |
|           | ...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      | FileServerDiskIops Balance     |
|           | ...确定文件服务器的 CPU 利用率百分比?                           | CPU 使用率           | CPUUtilization                 |
|           | ...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 存储卷的操作吞吐量的可用突增点数百分比?                  | 磁盘吞吐量突增平衡 (HDD)   | DiskThroughputBalance          |
|           | ...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**

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）。

## 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。每当其中一个 CloudWatch 指标接近或超过多个连续数据点的预定阈值时，Amazon FSx 就会显示针对一组指标的警告。这些警告会为您提供切实可行的建议，您可以使用这些建议来优化文件系统的性能。

可以在监控和性能控制面板的多个区域内访问警告。所有活动或最近的 Amazon FSx 性能警告以及为文件系统配置的处于 CloudWatch 警报状态的所有警报都将显示在“监控和性能”面板的“摘要”部分中。仪表板中显示指标图表的部分也会显示警告。

您可以为任何 Amazon FSx 指标创建 CloudWatch 警报。有关更多信息，请参阅 [创建 CloudWatch 警报以监控 Amazon FSx](#)。

### 使用性能警告提高文件系统的性能

Amazon FSx 会为您提供切实可行的建议，您可以使用这些建议来优化文件系统的性能。这些建议介绍了如何解决潜在的性能瓶颈。如果您希望继续进行活动，或者该活动对文件系统的性能造成了影响，您可以采取建议的操作。根据触发警告的指标，您可以通过增加文件系统的吞吐能力或存储容量来解决警告，如下表所述。

| 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            |                        |
| 文件服务器 > 磁盘 IOPS – 利用率  |                        |
| 文件服务器 > 磁盘吞吐量 – 利用率    | <a href="#">增加吞吐能力</a> |
| 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   |                        |

| 如果有针对此指标的警告                 | 请执行该操作                                                |
|-----------------------------|-------------------------------------------------------|
| 存储容量利用率                     | <a href="#">增加存储容量</a>                                |
| 存储卷 > 磁盘吞吐量 – 利用率 ( HDD )   | <a href="#">增加存储容量</a> 或 <a href="#">切换到 SDD 存储类型</a> |
| 存储卷 > 磁盘吞吐量 – 突增余额 ( HDD )  |                                                       |
| 存储卷 > 磁盘 IOPS – 利用率 ( SSD ) | <a href="#">提高 SSD IOPS</a>                           |

### 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 FSx for Windows File Server 指标

您可以通过以下方式查看 Amazon FSx CloudWatch 的指标。

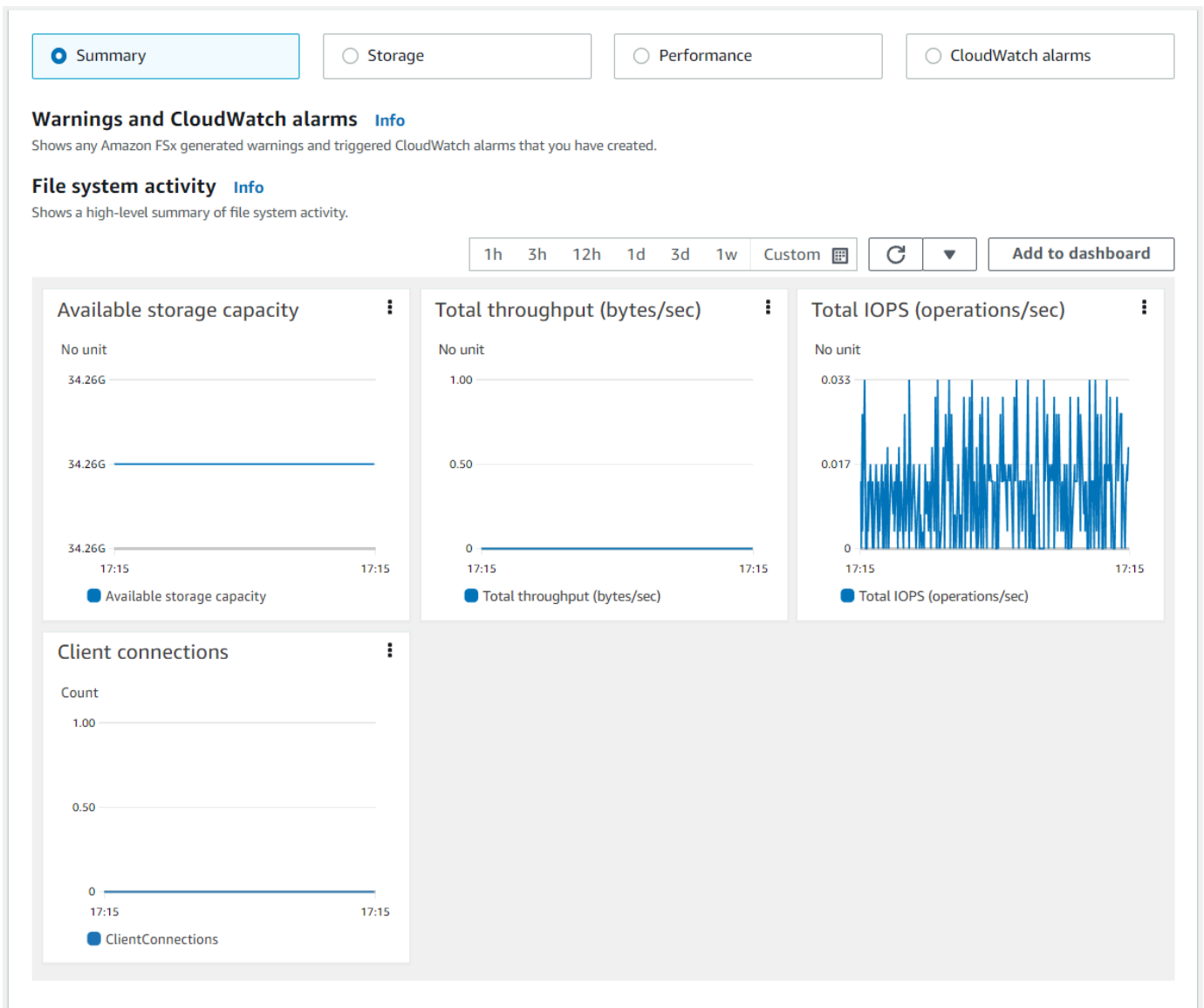
- Amazon FSx 控制台。
- 控制 CloudWatch 台。
- C CloudWatch LI ( 命令行界面 )。
- CloudWatch API。

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。

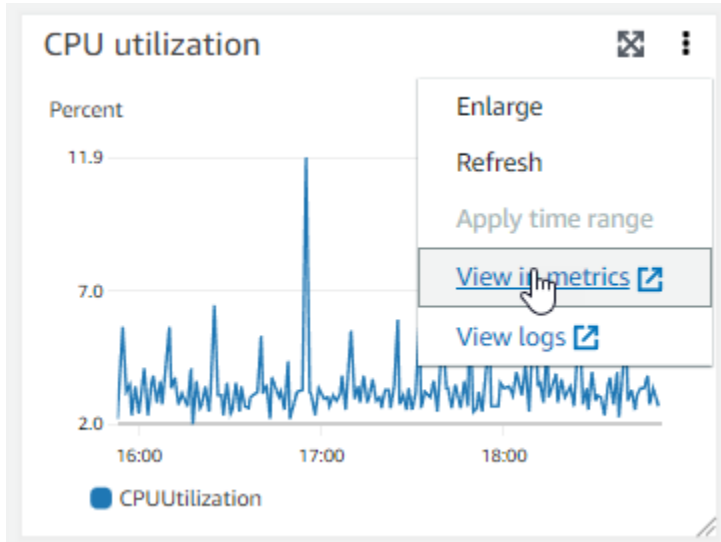


- 默认情况下会显示摘要指标，显示所有活动警告和 CloudWatch 警报以及文件系统活动指标。
- 选择存储可查看存储容量和利用率指标。
- 选择性能可查看文件服务器和存储性能指标。
- 选择 CloudWatch 警报以查看为文件系统配置的所有警报的图表。

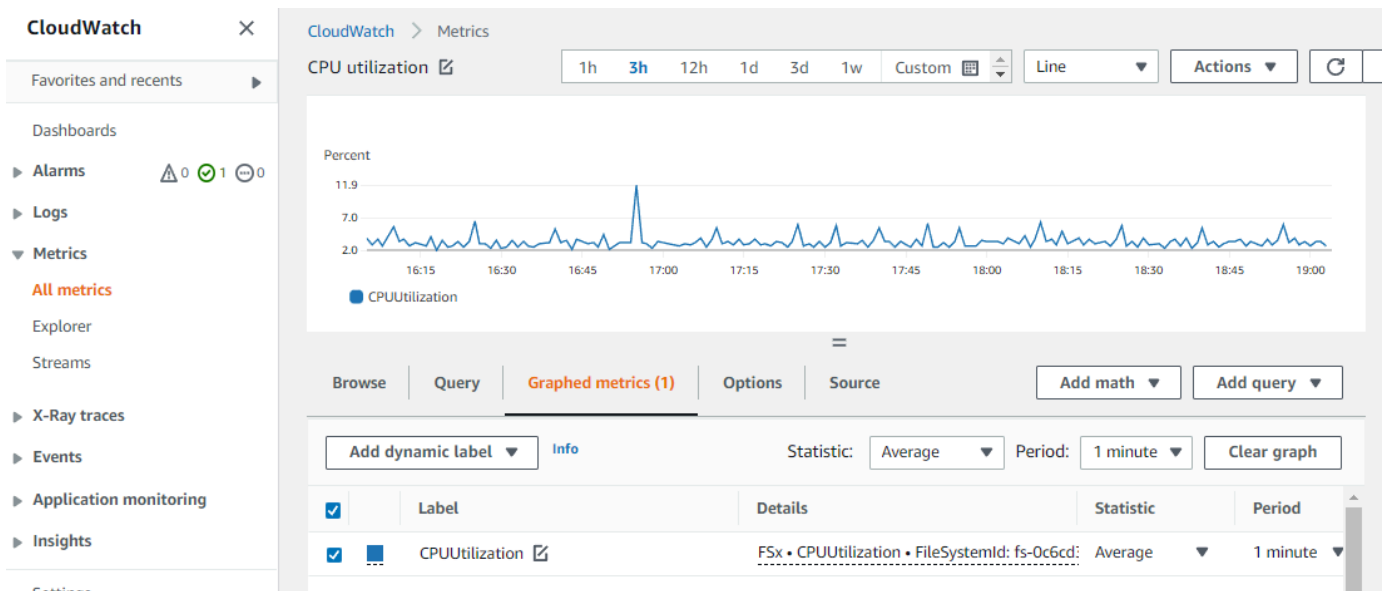
有关更多信息，请参阅 [如何使用 FSx for Windows File Server 指标](#)。

## 在 CloudWatch 控制台中查看指标

1. 要在亚马逊控制台的“指标”页面中查看文件系统指标，请在 Amazon FSx CloudWatch 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。



## 向 CloudWatch 控制面板添加指标

1. 要将一组 FSx for Windows 文件系统指标添加到 CloudWatch 控制台的控制面板，请在 Amazon FSx 控制台的“监控和性能”面板中选择一组指标（摘要、存储或性能）。



2. 选择面板右上角的“添加到仪表板”，即可打开 CloudWatch 控制台。
3. 从列表中选择现有 CloudWatch 仪表板，或创建新的仪表板。有关更多信息，请参阅[亚马逊 CloudWatch 用户指南中的使用亚马逊 CloudWatch 控制面板](#)。

### 要访问来自的指标 AWS CLI

- 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[AWS CLI 命令参考](#)。

### 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 警报以监控 Amazon FSx

您可以创建一个 CloudWatch 警报，在警报状态发生变化时发送 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。


警报仅针对持续的状态变化调用操作。CloudWatch 警报不会仅仅因为它们处于特定状态就调用操作；该状态必须已更改并保持了指定的时间段。您可以从 Amazon FSx 控制台或控制台创建警报。  
CloudWatch

以下过程介绍了如何使用控制台、AWS CLI和 API 为 Amazon FSx 创建警报。

### 使用 Amazon FSx 控制台设置警报

1. 通过以下网址打开 Amazon FSx 控制台：<https://console.aws.amazon.com/fsx/>。
2. 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。


- 在指标部分中，选择 FSx。
- 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。
- 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。为防止不必要和误导性的警报条件更改，并配置警报使其能够应对丢失的数据点，请参阅 Amazon CloudWatch 用户指南中的[配置 CloudWatch 警报如何处理丢失的数据](#)。

- 如果您 CloudWatch 想在警报状态触发操作时向您发送电子邮件或 SNS 通知，请在“每当此警报状态为”中选择警报状态。

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。

- 填写指标的名称、描述和每当值，然后选择下一步。
- 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

- 登录 AWS Management Console 并打开 CloudWatch 控制台，[网址为 https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/)。
- 选择创建警报以启动创建警报向导。
- 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。
- 填写指标的名称、描述和每当值。

5. 如果 CloudWatch 要在达到警报状态时向您发送电子邮件，请在“每当此警报”中选择“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 Create topic (创建主题) 创建一个新 Amazon SNS 主题，那么电子邮件地址在接收通知之前必须通过验证。当警报进入警报状态时，才会发送电子邮件。如果在验证电子邮件地址之前警报状态发生了变化，那么它们不会接收到通知。

6. 此时，可在警报预览区域预览即将创建的警报。选择创建警报。

#### 要使用设置警报 AWS CLI

- 调用 [put-metric-alarm](#)。有关更多信息，请参阅 [AWS CLI Command Reference](#)。

#### 使用 CloudWatch API 设置警报

- 调用 [PutMetricAlarm](#)。有关更多信息，请参阅 [Amazon CloudWatch API 参考](#)。

## 使用 AWS CloudTrail 记录 Amazon FSx for Windows File Server 的 API 调用日志

Amazon FSx for Windows File Server 与 AWS CloudTrail 集成，后者是在 Amazon FSx 中提供用户、角色或 AWS 服务所采取操作的记录的服务。CloudTrail 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 [《AWS CloudTrail 用户指南》](#)。

## CloudTrail 中的 Amazon FSx 信息

在您创建 AWS 账户时，将在该账户上启用 CloudTrail。当 Amazon FSx 中发生活动时，该活动将记录在 CloudTrail 事件中，并与其他 AWS 服务事件一同保存在事件历史记录中。您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅[使用 CloudTrail 事件历史记录查看事件](#)。

对于 AWS 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 可将日志文件传送到 Simple Storage Service（Amazon S3）存储桶。默认情况下，在使用控制台创建跟踪时，此跟踪应用于所有 AWS 区域。此跟踪在 AWS 分区中记录所有区域中的事件，并将日志文件传送到您指定的 Amazon S3 桶。此外，您可以配置其他 AWS 服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取行动。有关更多信息，请参阅下列内容：

- [创建跟踪概览](#)
- [CloudTrail 支持的服务和集成](#)
- [为 CloudTrail 配置 Amazon SNS 通知](#)
- [从多个区域接收 CloudTrail 日志文件](#)和[从多个账户接收 CloudTrail 日志文件](#)

所有 Amazon FSx 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 AWS Identity and Access Management（IAM）用户凭证发出的。
- 请求是使用角色还是联合身份用户的临时安全凭证发出的。
- 请求是否由其它 AWS 服务发出。

有关更多信息，请参阅 [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志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

以下示例显示了一个 CloudTrail 日志条目，该条目演示了从控制台为文件系统创建标签时的 TagResource 操作。

```
{
 "eventVersion": "1.05",
 "userIdentity": {
 "type": "Root",
 "principalId": "111122223333",
 "arn": "arn:aws:sts::111122223333:root",
 "accountId": "111122223333",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
 "attributes": {
 "mfaAuthenticated": "false",
 "creationDate": "2018-11-14T22:36:07Z"
 }
 }
 },
 "eventTime": "2018-11-14T22:36:07Z",
 "eventSource": "fsx.amazonaws.com",
 "eventName": "TagResource",
 "awsRegion": "us-east-1",
 "sourceIPAddress": "192.0.2.0",
 "userAgent": "console.amazonaws.com",
 "requestParameters": {
 "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-ab12cd34ef56gh789"
 },
 "responseElements": null,
 "requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
 "eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
 "eventType": "AwsApiCall",
 "apiVersion": "2018-03-01",
 "recipientAccountId": "111122223333"
}
```

以下示例显示了一个 CloudTrail 日志条目，该条目演示了从控制台删除文件系统标签时的 UntagResource 操作。

```
{
 "eventVersion": "1.05",
 "userIdentity": {
 "type": "Root",
 "principalId": "111122223333",
```

```
 "arn": "arn:aws:sts::111122223333:root",
 "accountId": "111122223333",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
 "attributes": {
 "mfaAuthenticated": "false",
 "creationDate": "2018-11-14T23:40:54Z"
 }
 }
 },
 "eventTime": "2018-11-14T23:40:54Z",
 "eventSource": "fsx.amazonaws.com",
 "eventName": "UntagResource",
 "awsRegion": "us-east-1",
 "sourceIPAddress": "192.0.2.0",
 "userAgent": "console.amazonaws.com",
 "requestParameters": {
 "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789"
 },
 "responseElements": null,
 "requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
 "eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
 "eventType": "AwsApiCall",
 "apiVersion": "2018-03-01",
 "recipientAccountId": "111122223333"
}
```

# 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。

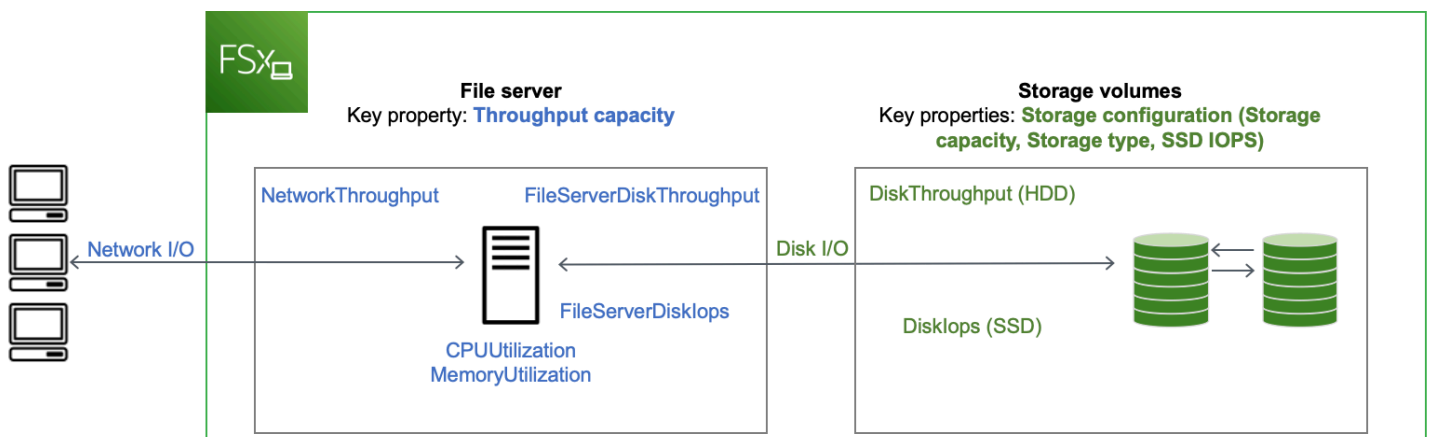
## 主题

- [文件系统性能](#)
- [其他性能注意事项](#)
- [吞吐能力对性能的影响](#)
- [选择正确的吞吐能力级别](#)
- [存储配置对性能的影响](#)
- [示例：存储容量和吞吐能力](#)
- [使用 CloudWatch 指标衡量绩效](#)
- [性能问题排查](#)

## 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 文件系统在所有可用 AWS 区域提供高达 2 Gb/s 和 80,000 IOPS，在美国东部（弗吉尼亚北部）、美国西部（俄勒冈）、美国东部（俄亥俄州）、欧洲（爱尔兰）、亚太地区（东京）和亚太地区（新加坡）提供 12 Gb/s 的吞吐量和 400,000 个 IOPS。您的工作负载可以在文件系统上驱动的具体吞吐量和 IOPS 数取决于文件系统的吞吐能力、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。此功能使它能够为访问您的文件系统的单个客户端提供多 GB/s 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 支持的中小型企业连接数量存在理论限制，但这个限制以百万为单位，而且实际上你可以拥有无限数量的 SMB 连接。



## 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 兆字节 (MBps) 的吞吐量级别，但请记住，这些级别适用于测试和开发工作负载，而不是生产工作负载。

### 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 吞吐容量<br>(兆字节每秒) | 网络吞吐量 (兆字节每秒) |            | 网络 IOPS | 内存 (GB) |
|---------------------|---------------|------------|---------|---------|
|                     | 基准            | 突增 (每天几分钟) |         |         |
| 32                  | 32            | 600        | 千       | 4       |

| FSx 吞吐容量<br>(兆字节每秒) | 网络吞吐量 (兆字节每秒) |               | 网络 IOPS | 内存 (GB) |
|---------------------|---------------|---------------|---------|---------|
|                     | 基准            | 突增 (每天 30 分钟) |         |         |
| 64                  | 64            | 600           | 数万      | 8       |
| 128                 | 150           | 1250          |         | 8       |
| 256                 | 300           | 1250          | 数十万     | 16      |
| 512                 | 600           | 1250          |         | 32      |
| 1024                | 1500          | –             |         | 72      |
| 2,048               | 3,125         | –             |         | 144     |
| 4,608               | 9,375         | –             | 数百万     | 192     |
| 6,144               | 12,500        | –             |         | 256     |
| 9,216               | 18,750        | –             |         | 384     |
| 12,288              | 21,250        | –             |         | 512     |

## 磁盘 I/O

| FSx 吞吐容量<br>(兆字节每秒) | 磁盘吞吐量 (兆字节每秒) |               | 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 吞吐容量<br>(兆字节每秒) | 磁盘吞吐量 (兆字节每秒)       |   | 磁盘 IOPS           |   |
|---------------------|---------------------|---|-------------------|---|
| 1024                | 1024                | – | 40K               | – |
| 2,048               | 2,048               | – | 80K               | – |
| 4,608               | 4,608               | – | 150K              | – |
| 6,144               | 6,144               | – | 200K              | – |
| 9,216               | 9,216 <sup>1</sup>  | – | 300K <sup>1</sup> | – |
| 12,288              | 12,288 <sup>1</sup> | – | 400K <sup>1</sup> | – |

### Note

<sup>1</sup> 如果您的多可用区文件系统的吞吐量为 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选择特定的吞吐能力来满足应用程序的需求。例如，如果您的工作负载需要将 1 GBps 的流量驱动至文件系统，则应选择至少 1,024 MBps 的吞吐能力。

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 FSx for Windows File Server 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 存储容量 MBps )       | 磁盘 IOPS ( 每 TiB 存储的 IOPS 数 ) |
|------|---------------------------------|------------------------------|
| SSD  | 750                             | 3,000*                       |
| HDD  | 基准 12；突增 80 ( 每个文件系统最多 1 GB/s ) | 基准 12；突增 80                  |

### Note

\*对于具有 SSD 存储类型的文件系统，您可以预置额外 IOPS，最大比率为每 GiB 存储 500 IOPS，每个文件系统 400,000 IOPS。

## 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，即卷累积吞吐量积分的速度。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：

$$(\text{Volume size}) \times (\text{Credit accumulation rate per TiB}) = \text{Throughput}$$

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

## 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 指标衡量绩效

您可以使用 Amazon CloudWatch 来衡量和监控文件系统的吞吐量和 IOPS。有关更多信息，请参阅 [使用 Amazon 监控指标 CloudWatch](#)。

## 性能问题排查

有关排查常见性能问题的帮助，请参阅[文件系统性能问题排查](#)。

# Amazon FSx 演练

在接下来的部分，您可以找到很多针对任务的演练，这些演练会指导您完成各种过程。

## 主题

- [演练 1：入门先决条件](#)
- [演练 2：从备份创建文件系统](#)
- [演练 3：更新现有文件系统](#)
- [演练 4：将 Amazon FSx 与 Amazon AppStream 2.0 结合使用](#)
- [演练 5：使用 DNS 别名访问文件系统](#)
- [演练 6：使用分片横向扩展性能](#)
- [演练 7：将备份复制到另一个 AWS 区域](#)

## 演练 1：入门先决条件

在完成入门练习之前，您必须已将基于 Microsoft Windows 的 Amazon EC2 实例加入您的 AWS Directory Service 目录。您还必须以目录管理员用户身份通过 Windows 远程桌面协议登录实例。以下演练演示如何执行这些必需的先决条件操作。

## 主题

- [步骤 1：设置 Active Directory](#)
- [步骤 2：在 Amazon EC2 控制台中启动 Windows 实例](#)
- [步骤 3：连接到您的实例](#)
- [步骤 4：将实例加入 AWS Directory Service 目录](#)

## 步骤 1：设置 Active Directory

借助 Amazon FSx，您可以为基于 Windows 的工作负载执行完全托管的文件存储。同样，AWS Directory Service 提供完全托管的目录，供您在工作负载部署中使用。如果有现有企业 AD 域在使用 EC2 实例的 AWS 虚拟私有云 (VPC) 中运行，您可以启用基于用户的身份验证和访问控制。为此，您可以在 AWS 托管的 Microsoft AD 与企业域之间建立信任关系。对于 Amazon FSx 中的 Windows 身份验证，您只需要单向林信任，即 AWS 托管的林信任企业域林。

您的企业域为受信任域，而 AWS 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 仅与托管的域进行交互。然后，托管的域会将身份验证请求传递到您的企业域。

#### Note

您还可以将外部信任类型与 Amazon FSx 一起用于可信域。

Active Directory 安全组必须允许从 Amazon FSx 文件系统的安全组进行入站访问。

为 Microsoft AD 创建 AWS 目录服务

- 如果还没有，请使用 AWS Directory Service 创建 AWS 托管的 Microsoft AD 目录。有关更多信息，请参阅《AWS Directory Service 管理指南》中的[创建 AWS 托管的 Microsoft AD 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，则需要使用新的 AWS Directory Service 目录和管理员用户身份重复本练习中的步骤。

- 如果您有现有 AD，请在 Microsoft AWS Managed Microsoft AD 与现有 AD 之间建立信任关系。有关更多信息，请参阅《AWS Directory Service 管理指南》中的[何时创建信任关系](#)。

## 步骤 2：在 Amazon EC2 控制台中启动 Windows 实例


您可以根据以下过程所述使用 AWS Management Console 启动 Windows 实例。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. 通过以下网址打开 Amazon EC2 控制台：<https://console.aws.amazon.com/ec2/>。
2. 从控制台控制面板中，选择启动实例。
3. Choose an Amazon Machine Image (AMI) 页面显示一组称为 Amazon Machine Image (AMI) 的基本配置，作为您的实例的模板。选择适用于 Windows Server 2016 Base 或 Windows Server 2012 R2 Base 的 AMI。请注意，这些 AMI 标记为“Free tier eligible”(符合条件的免费套餐)。

4. 在 Choose an Instance Type (选择实例类型) 页面上，您可以选择实例的硬件配置。选择 t2.micro 类型 (预设情况下的选择)。请注意，此实例类型适用免费套餐。
5. 选择 Review and Launch 让向导为您完成其它配置设置。
6. 在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，也可以选择您在设置时创建的安全组：
  - a. 选择 Edit security groups。
  - b. 在 Configure Security Group 页面上，确保 Select an existing security group 处于选中状态。
  - c. 从现有安全组列表中选择您的安全组，然后选择 Review and Launch。
7. 在 Review Instance Launch 页面上，选择 Launch。
8. 当系统提示提供密钥时，选择 Choose an existing key pair，然后选择您在进行设置时创建的密钥对。

另外，您也可以新建密钥对。选择 Create a new key pair，输入密钥对的名称，然后选择 Download Key Pair。这是您保存私有密钥文件的唯一机会，因此务必单击进行下载。将私有密钥文件保存在安全位置。当您启动实例时，您将需要提供密钥对的名称；当您每次连接到实例时，您将需要提供相应的私有密钥。

 Warning

请勿选择在没有密钥对的情况下继续选项。如果您启动的实例没有密钥对，就不能连接到该实例。

准备好后，选中确认复选框，然后选择 Launch Instances。

9. 确认页面会让您知道自己的实例已启动。选择 View Instances 以关闭确认页面并返回控制台。
10. 在实例屏幕上，您可以查看启动状态。启动实例只需很短的时间。启动实例时，其初始状态为 pending。实例启动后，其状态变为 running，并且会收到一个公有 DNS 名称。(如果 Public DNS (IPv4) 列已隐藏，请选择页面右上角的 Show/Hide Columns (齿轮状图标)，然后选择 Public DNS (IPv4)。)
11. 需要几分钟准备好实例，以便您能连接到实例。检查您的实例是否通过了状态检查；您可以在 Status Checks 列中查看此信息。



### Important

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，您将需要该 ID。

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 管理员账户的本地化名称](#)。

如果您已将实例加入到域，则可以使用您在 AWS 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。示例是 **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 Amazon EC2 控制台中，选择实例，然后选择 Connect (连接)。
2. 在连接到您的实例对话框中，选择获取密码 (密码在实例启动几分钟之后才可用)。
3. 选择 Browse 并导航至您启动实例时所创建的私有密钥文件。选择文件并选择 Open (打开)，以便将文件的全部内容复制到 Contents (内容) 字段。
4. 选择 Decrypt Password。控制台将在连接到您的实例对话框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 Details (详细信息) 选项卡，并向下滚动到 Thumbprint (指纹) 条目（在 Windows PC 上）或 SHA1 Fingerprints (SHA1 指纹) 条目（在 Mac 上）。这是远程计算机的安全证书的唯一标识符。
  - c. 在 Amazon EC2 控制台中，选择该实例，选择 Actions (操作)，然后选择 Get System Log (获取系统日志)。
  - d. 在系统日志输出中，查找标记为 RDPCERTIFICATE-THUMBPRINT 的条目。如果此值与证书的指纹匹配，则表示您已验证了远程计算机的标识。
  - e. 如果您正在从 Windows PC 使用 Remote Desktop Connection，请返回到 Certificate 对话框并选择 OK。如果您正在 Mac 上使用 Microsoft Remote Desktop，请返回到 Verify Certificate 并选择 Continue。
  - f. [Windows] 在 Remote Desktop Connection 窗口中选择 Yes 连接到您的实例。

现在，您已连接到实例，您可以将实例加入 AWS Directory Service 目录。

## 步骤 4：将实例加入 AWS Directory Service 目录

以下过程显示如何将现有 Amazon EC2 Windows 实例手动加入 AWS Directory Service 目录。

## 将 Windows 实例加入 AWS Directory Service 目录

1. 使用任何远程桌面协议客户端连接到实例。
2. 在实例上打开 TCP/IPv4 属性对话框。
  - a. 打开 Network Connections。

### Tip

您可以在实例上从命令提示符运行以下命令，直接打开 Network Connections。

```
%SystemRoot%\system32\control.exe ncpa.cpl
```

- b. 打开任何已启用网络连接的上下文（右键单击）菜单，然后选择属性。
  - c. 在连接属性对话框中，打开（双击）Internet Protocol Version 4。
3. （可选）选择使用以下 DNS 服务器地址，将首选 DNS 服务器和备用 DNS 服务器地址更改为 AWS Directory Service 提供的 DNS 服务器的 IP 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 AWS 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

可以输入完全限定的域名或 NetBios 名称，后跟反斜杠（\），然后是用户名（在此例中为 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 AWS 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，您可以创建您的 Amazon FSx 文件系统了。然后，您可以继续完成入门练习中的其他任务。有关更多信息，请参阅[开始使用适用于 Windows File Server 的亚马逊 FSx](#)。

## 演练 2：从备份创建文件系统

使用 Amazon FSx，您可以从备份创建文件系统。执行此操作时，您可以更改以下任何元素，以更好地适应新创建的文件系统的使用案例：

- 存储类型
- 吞吐能力
- VPC
- 可用区
- 子网
- VPC 安全组
- Active Directory 配置
- AWS KMS 加密密钥
- 每日自动备份开始时间
- 每周维护时段

以下过程将指导您从备份创建新文件系统。在创建此文件系统之前，您必须已有备份。有关更多信息，请参阅[使用备份](#)。

从现有备份创建文件系统

1. 通过以下网址打开 Amazon FSx 控制台：<https://console.aws.amazon.com/fsx/>。
2. 在右侧的导航列表中选择备份。
3. 从控制面板上的表中，选择用于创建新文件系统的备份。

### Note

您只能将备份还原到与原始存储容量相同的文件系统。您可以在还原的文件系统的存储容量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](#)。

4. 选择 Restore backup (还原备份)。这将启动创建文件系统向导。

5. 为这个新文件系统选择要更改的设置。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。
6. 选择审阅摘要，在创建文件系统之前查看您的设置。
7. 选择 Create file system。

现在，您已从现有备份成功创建新文件系统。

## 演练 3：更新现有文件系统

您可以使用本演练中的步骤更新三个元素。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 AWS CLI。有关更多信息，请参阅《AWS 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 AWS 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
```

## 演练 4：将 Amazon FSx 与 Amazon AppStream 2.0 结合使用

通过支持服务器消息块 (SMB) 协议，Amazon FSx for Windows File Server 支持通过 Amazon EC2、VMware Cloud on AWS、Amazon WorkSpaces 和 Amazon AppStream 2.0 实例访问您的文件系统。AppStream 2.0 是一项完全托管式应用程序流式服务。您可以在 AppStream 2.0 上集中管理您的桌面应用程序，并将它们安全地交付到任何计算机上的浏览器。有关 AppStream 2.0 的更多信息，请参阅 [《Amazon AppStream 2.0 管理指南》](#)。有关如何精简 Amazon AppStream 2.0 映像和实例集的管理的说明，请参阅 AWS 博客文章 [Automatically create customized AppStream 2.0 Windows images](#)。

本演练将指导您如何将 Amazon FSx 与 AppStream 2.0 结合用于两个用例：为每位用户提供个人永久存储，以及提供用户间共享文件夹以访问通用文件。

### 为每位用户提供个人永久存储

您可以使用 Amazon FSx 在 AppStream 2.0 流会话中为组织中的每位用户提供一个独有的存储驱动器。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 FSx 为域用户创建主文件夹

1. 创建一个 Amazon FSx 文件系统。有关更多信息，请参阅[开始使用适用于 Windows File Server 的亚马逊 FSx](#)。

2. 文件系统可用后，为 Amazon FSx 文件系统 中的每个域 AppStream 2.0 用户创建一个文件夹。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[在 FSx 上管理 Windows File Server 文件系统的文件共享](#)。

### 启动已加入域名的 AppStream 2.0 映像生成器

1. 登录 AppStream 2.0 控制台，网址为 <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《Amazon AppStream 2.0 管理指南》中的[将 Active Directory 与 AppStream 2.0 结合使用](#)。
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. 将在 Amazon FSx 文件系统所在的 VPC 中启动映像生成器。请确保将映像生成器关联到 Amazon FSx 文件系统已加入的同一 AWS Managed Microsoft AD 目录。与映像生成器关联的 VPC 安全组必须允许对您的 Amazon FSx 文件系统的访问权限。
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。

### 关联 Amazon FSx 文件共享与 AppStream 2.0

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:”作为驱动器盘符来映射 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（可以从 Amazon FSx 控制台的文件系统详细信息视图获取）。

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，然后运行 `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 AppStream 2.0 实例集。请确保也将 AppStream 2.0 实例集加入到用于映像生成器的 Active Directory 域中。将在 Amazon FSx 文件系统使用的 VPC 中启动该实例集。与实例集关联的 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《Amazon AppStream 2.0 管理指南》中的[使用 SAML 2.0 对 AppStream 2.0 进行单点登录访问](#)。
9. 在流会话中，您的 Amazon FSx 文件共享会被映射到“S:”驱动器盘符。

## 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 FSx 创建共享文件夹

1. 创建一个 Amazon FSx 文件系统。有关更多信息，请参阅[开始使用适用于 Windows File Server 的亚马逊 FSx](#)。
2. 默认情况下，每个 Amazon FSx 文件系统中都包含一个共享文件夹，您可以使用地址 `\\file-system-DNS-name\share` 或 `\\fqdn-DNS-alias\share`（使用 DNS 别名时）来访问该文件夹。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[在 FSx 上管理 Windows File Server 文件系统的文件共享](#)。



## 启动 AppStream 2.0 映像生成器

1. 通过 AppStream 2.0 控制台启动新的映像生成器或连接到现有的映像生成器。将在 Amazon FSx 文件系统使用的 VPC 中启动该映像生成器。与映像生成器关联的 VPC 安全组必须允许对您的 Amazon FSx 文件系统的访问权限。
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 AppStream 2.0 关联

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（可以从 Amazon FSx 控制台的文件系统详细信息视图中获取），以及用于访问共享文件夹的凭证。

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。

## 演练 5：使用 DNS 别名访问文件系统

FSx for Windows File Server 为每个文件系统提供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。您也可以使用自行选择的 DNS 别名访问您的文件系统。DNS 别名使您能够在将

文件系统存储从本地迁移到 Amazon FSx 时，继续使用现有 DNS 名称访问存储在 Amazon FSx 上的数据。每次最多可以将 50 个 DNS 别名与一个文件系统关联。

要使用 DNS 别名访问 Amazon FSx 文件系统，则必须执行以下三个步骤：

1. 将 DNS 别名关联到 Amazon FSx 文件系统。
2. 为文件系统的计算机对象配置服务主体名称 (SPN)。(这是在使用 DNS 别名访问文件系统时，获得 Kerberos 身份验证的必需条件。)
3. 更新或创建文件系统的 DNS CNAME 记录和 DNS 别名。

## 主题

- [步骤 1：将 DNS 别名关联到 Amazon FSx 文件系统](#)
- [步骤 2：为 Kerberos 配置服务主体名称 \(SPN\)](#)
- [步骤 3：更新或创建文件系统的 DNS CNAME 记录](#)
- [使用 GPO 强制执行 Kerberos 身份验证](#)

## 步骤 1：将 DNS 别名关联到 Amazon FSx 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](#)。

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 [创建您的文件系统](#) 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。

▼ **Access - optional**

Aliases  
List any custom DNS names that you want to associate with the file system

financials.corp.example.com  
acctsrcv.corp.example.com  
transactions.corp.example.com

Specify up to 50 aliases separated with commas, or put each on a new line.

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。

当您的新文件系统可用时，请继续按照步骤 2 操作。

## 步骤 2：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 活动目录模块

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. PowerShell 以管理员身份打开。
3. 使用以下命令安装 Act PowerShell ive 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[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。

您还可以在 [DescribeFile 系统](#) API 操作的响应中获取 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 one of the following commands, not both:
```

```
Set-AdComputer -Identity $FSxAdComputer -Add @{"msDS-
AdditionalDnsHostname"="$Alias"}
##Or
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。

您还可以在[DescribeFilesystem](#) API 操作的响应中获取 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。

有关如何强制客户端在连接到 Amazon FSx 文件系统时使用 Kerberos 身份验证和加密的信息，请参阅[使用 GPO 强制执行 Kerberos 身份验证](#)。

## 步骤 3：更新或创建文件系统的 DNS CNAME 记录

为文件系统正确配置 SPN 后，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 cmdlet

1. 以具有 DNS 管理权限的群组 ( AWSAWS 托管 Active Directory 中的委托域名系统管理员 , 以及您在自行管理的 Active Directory 中向其委派 DNS AWS 管理权限的域管理员或其他群组 ) 的用户身份登录加入您的 Amazon FS x 文件系统所加入的 Amazon FSx 文件系统的 Windows 实例。

有关更多信息 , 请参阅 Amazon EC2 用户指南中的[连接到您的 Windows 实例](#)。

2. PowerShell 以管理员身份打开。
3. 需要 PowerShell 使用 DNS 服务器模块才能执行此过程中的指令。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. 以拥有 DNS 管理权限的群组 ( AWS 托管 Active Directory 中的委托域名系统管理员 , 以及您在自行 AWS 管理的 Active Directory 中向其委派 DNS 管理权限的域管理员或其他群组 ) 的成员身份连接到您的 Amazon EC2 实例。

有关更多信息 , 请参阅 Amazon EC2 用户指南中的[连接到您的 Windows 实例](#)。

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 $ZoneName -Type NS | Where Type -eq 'A' |
 Select -ExpandProperty Name) | Select -First 1
foreach ($computer in $DnsServerComputerName)
{
 Add-DnsServerResourceRecordCName -Name $AliasHost -ComputerName $computer -
 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 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。

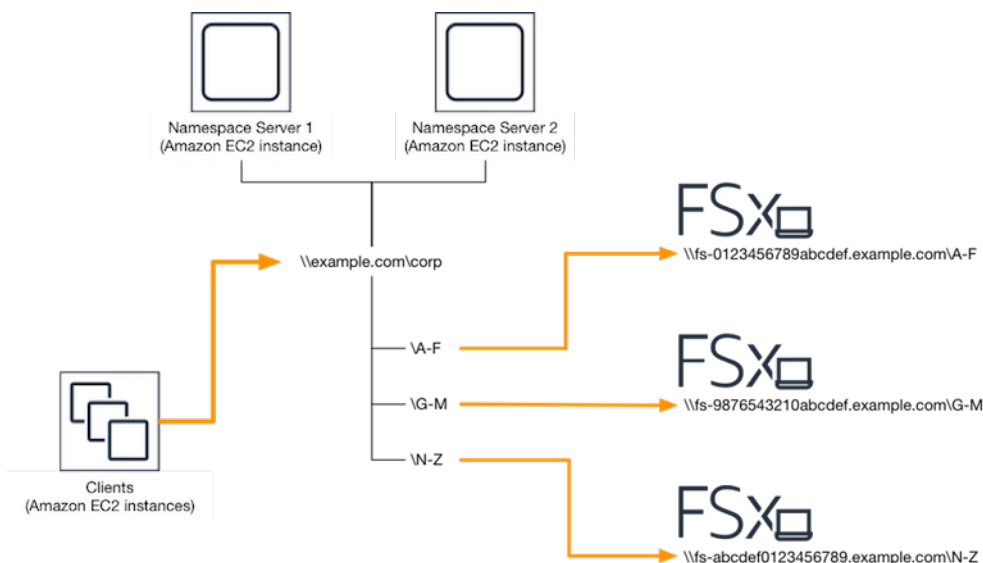
## 演练 6：使用分片横向扩展性能

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。

当您的工作负载需要对文件数据进行统一分布的读取/写入访问时（例如，如果计算实例的每个子集访问文件数据的不同部分），则可以使用此解决方案。

### 设置 DFS 命名空间以横向扩展性能

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 [setu](#) AWS CloudFormation p-dfsn-Servers.Template 模板启动一对高度可用的 DFS 命名空间服务器。有关创建 AWS CloudFormation 堆栈的更多信息，请参阅《AWS CloudFormation 用户指南》中的[在 AWS CloudFormation 控制台上创建堆栈](#)。
2. 以 AWS 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。有关更多信息，请参阅 Amazon EC2 用户指南中的[连接到您的 Windows 实例](#)。
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。

## 演练 7：将备份复制到另一个 AWS 区域

借助 Amazon FSx，您可以将同一 AWS 账户中的现有备份复制到另一个 AWS 区域（跨区域备份复制）或同一 AWS 区域（区域内备份复制）。

以下过程将指导您完成在同一 AWS 账户中创建备份副本。在创建此备份副本之前，必须已有备份。有关更多信息，请参阅[使用备份](#)。

复制同一 AWS 账户内的现有备份（跨区域或区域内）

1. 通过以下网址打开 Amazon FSx 控制台：<https://console.aws.amazon.com/fsx/>。
2. 在导航窗格中，选择备份。
3. 选择备份表中您要复制的备份。
4. 选择复制备份。这样做会打开复制备份向导。
5. 在目标区域列表中，选择要复制备份的目标 AWS 区域。目标可以位于另一个 AWS 区域，也可以在同一个 AWS 区域。
6. （可选）选择复制标签，将标签从源备份复制到目标备份。如果您在步骤 8 中选择复制标签并添加标签，则会合并所有标签。
7. 对于加密，选择 AWS KMS 加密密钥来加密复制的备份。
8. 对于标签 – 可选，输入键和值以将标签添加到您复制的备份。如果您在此步骤中添加标签，并在步骤 6 中选择复制标签，则会合并所有标签。
9. 选择复制备份。

现在，您已经成功地将同一 AWS 账户中的备份复制到另一个 AWS 区域或已在同一 AWS 区域中复制。

# Amazon FSx 中的安全性

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方 AWS 的共同责任。[责任共担模式](#)将其描述为云的安全性 和云中的安全性：

- 云安全 — AWS 负责保护在 Amazon Web Services 云中运行 AWS 服务的基础设施。AWS 还为您提供可以安全使用的服务。作为 [AWS 合规性计划](#) 的一部分，第三方审核人员将定期测试和验证安全性的有效性。要了解适用于 Amazon FSx for Windows File Server 的合规性计划，请参阅 [合规性计划范围内的 AWS 服务](#)。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您的公司的要求以及适用的法律法规。

该文档帮助您了解如何在使用 Amazon FSx for Windows File Server 时应用责任共担模式。以下主题说明如何配置 Amazon FSx 以实现您的安全性和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 Amazon FSx for Windows File Server 资源。

## 主题

- [Amazon FSx 中的数据加密](#)
- [使用 Windows ACL 进行文件和文件夹级别的访问控制](#)
- [使用 Amazon VPC 进行文件系统访问控制](#)
- [Amazon FSx for Windows File Server 的身份和访问管理](#)
- [Amazon FSx for Windows File Server 合规性验证](#)
- [Amazon FSx for Windows File Server 和接口 VPC 端点](#)

## Amazon FSx 中的数据加密

Amazon FSx for Windows File Server 支持两种形式的文件系统加密：传输中数据加密和静态加密。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。创建 Amazon FSx 文件系统时，系统会自动启用静态数据加密。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。

有关使用 Amazon FSx for Windows File Server 进行加密的更多信息，请参阅以下相关主题：

- [创建 Amazon FSx for Windows File Server 文件系统](#)
- 《IAM 用户指南》中的 [Amazon FSx 的操作、资源和条件键](#)

### 主题

- [静态加密](#)
- [传输中加密](#)

## 静态加密

所有 Amazon FSx 文件系统都使用 AWS Key Management Service ( AWS 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《AWS Key Management Service 开发人员指南》中的[加密基础知识](#)。

### Note

AWS 密钥管理基础设施使用经联邦信息处理标准 (FIPS) 140-2 批准的加密算法。该基础设施符合美国国家标准与技术研究院 ( NIST ) 800-57 建议。

## 亚马逊 FSx 是如何使用的 AWS KMS

Amazon FSx 与集成，AWS KMS 用于密钥管理。Amazon FSx 使用 AWS 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：

- AWS 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。有关创建客户托管密钥的更多信息，请参阅 AWS Key Management Service 开发人员指南中的[创建密钥](#)。

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，AWS 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《AWS Key Management Service 开发人员指南》AWS KMS keys 中的[轮换](#)。

文件系统静态加密和解密是透明处理的。但是，特定于 Amazon FSx 的 AWS 账户 ID 会出现在与 AWS CloudTrail 操作相关的 AWS KMS 日志中。

## Amazon FSx 的关键政策 AWS KMS

密钥政策是控制对 KMS 密钥访问的主要方法。有关密钥政策的更多信息，请参阅《AWS Key Management Service 开发人员指南》中的[使用 AWS KMS 中的密钥政策](#)。以下列表描述了 Amazon FSx 为静态加密文件系统支持的所有 AWS KMS 相关权限：

- kms:Encrypt – ( 可选 ) 将明文加密为加密文字。该权限包含在默认密钥策略中。
- kms:Decrypt – ( 必需 ) 解密密文。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，而不会在客户端暴露数据的明文。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 — ( 必填 ) 返回使用 KMS 密钥加密的数据加密密钥。此权限包含在 kms: K GenerateData ey\* 下的默认密钥策略中。
- km CreateGrant s: — ( 必填 ) 向密钥添加授权，以指定谁可以在什么条件下使用该密钥。授权是密钥政策的替代权限机制。有关授权的更多信息，请参阅《AWS Key Management Service 开发人员指南》中的[使用授权](#)。该权限包含在默认密钥策略中。
- kms: DescribeKey — ( 必填 ) 提供有关指定 KMS 密钥的详细信息。该权限包含在默认密钥策略中。
- km ListAliases s: — ( 可选 ) 列出账户中的所有密钥别名。在使用控制台创建加密的文件系统时，该权限将填充 KMS 密钥列表。我们建议您使用该权限以提供最佳的用户体验。该权限包含在默认密钥策略中。

## 传输中加密

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。Amazon FSx for Windows File Server 会在您访问文件系统时使用 SMB 加密自动加密传输中数据，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。

为了满足始终加密的合规性要求 data-in-transit，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。要了解有关在文件系统 encryption-in-transit 上进行管理的更多信息，请参阅[管理传输中加密](#)。

## 使用 Windows ACL 进行文件和文件夹级别的访问控制

Amazon FSx for Windows File Server 支持使用 Microsoft Active Directory 通过服务器消息块（SMB）协议进行基于身份的身份验证。Active Directory 是 Microsoft 目录服务，用于存储有关网络上对象的信息，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 FSx 中 Active Directory 支持的更多信息，请参阅[在 FSx for Windows File Server 中使用 Microsoft Active Directory](#)。

加入域的计算实例可以使用 Active Directory 凭证访问 Amazon FSx 文件共享。您可以使用标准的 Windows 访问控制列表（ACL）进行精细的文件和文件夹级别的访问控制。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 ACL。

每个 Amazon FSx 文件系统都附带一个名为 share 的默认 Windows 文件共享。此共享文件夹的 Windows ACL 已配置为允许域用户进行读取/写入访问。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 AWS 托管 Microsoft AD 集成，则该组是 AWS 委托 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 ACL，您可以将共享映射为担任委派的管理员组成员的用户。

**⚠ Warning**

Amazon FSx 要求 SYSTEM 用户拥有对文件系统内所有文件夹的完全控制 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 AWS Directory Service ?](#) 在《AWS Directory Service 管理指南》中。
- 在《[AWS Directory Service 管理指南](#)》中创建你的 [Microsoft AD 托管目录](#)。
- 《AWS Directory Service 管理指南》中的[何时创建信任关系](#)。
- [演练 1：入门先决条件](#)。

## 使用 Amazon VPC 进行文件系统访问控制

您可以通过弹性网络接口访问您的 Amazon 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 Amazon FSx 文件系统的域名服务 (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 AWS Direct Connect 或 VPN 与关联 VPC 连接的资源或对等 VPC 中的资源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 for Windows File Server 支持 VPC 共享，这使您可以查看、创建、修改和删除 AWS 另一个账户拥有的 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》中的[使用共享 VPC](#)。



## Amazon VPC 安全组

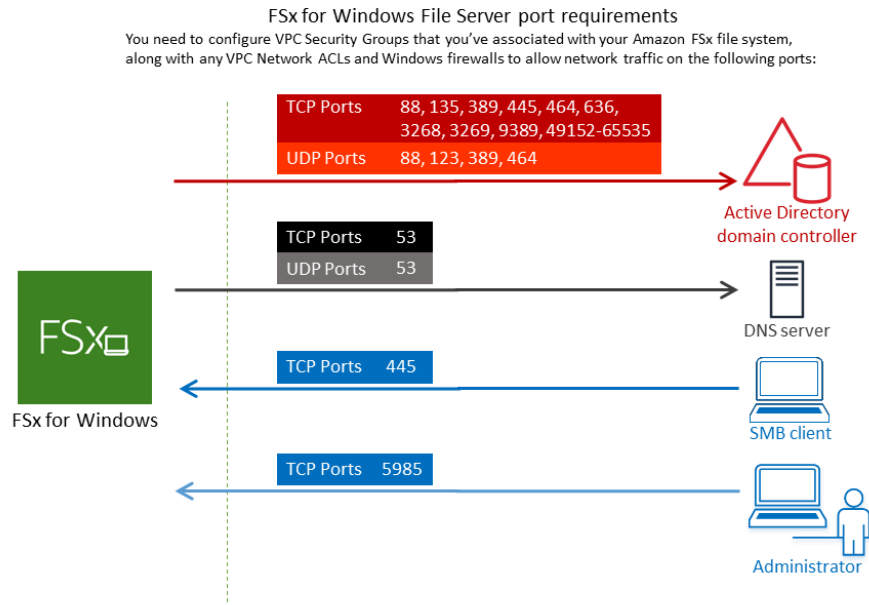
为了进一步控制通过 VPC 内文件系统弹性网络接口的网络流量，请使用安全组来限制对文件系统的访问。安全组是一种状态防火墙，用于控制进出其关联网络接口的流量。在这种情况下，关联的资源就是文件系统的网络接口。

要使用安全组控制对 Amazon FSx 文件系统的访问，请添加入站和出站规则。入站规则控制传入的流量，出站规则控制从文件系统传出的流量。确保您的安全组中有正确的网络流量规则，以便将 Amazon FSx 文件系统的文件共享映射到支持的计算实例上的文件夹。

有关安全组规则的更多信息，请参阅 Amazon EC2 用户指南中的[安全组规则](#)。

### 为 Amazon FSx 创建安全组


1. 打开 Amazon EC2 控制台，[网址为 https://console.aws.amazon.com/ec2](https://console.aws.amazon.com/ec2)。
2. 在导航窗格中，选择安全组。
3. 选择创建安全组。
4. 为安全组指定名称和描述。
5. 对于 VPC，请选择与您的文件系统关联的 Amazon VPC 以在该 VPC 中创建安全组。
6. 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   | Kerberos 身份验证                  |
| TCP/UDP | 464  | 更改/设置密码                        |
| TCP/UDP | 389  | 轻型目录访问协议 ( LDAP )              |
| UDP     | 123  | 网络时间协议 ( NTP )                 |
| TCP     | 135  | 分布式计算环境/端点映射器 ( DCE/EPMAP )    |
| TCP     | 445  | 目录服务 SMB 文件共享                  |
| TCP     | 636  | 基于 TLS/SSL 的轻型目录访问协议 ( 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 网络服务 , PowerShell           |
| TCP | 49152 - 65535 | RPC 的临时端口                            |


 Important

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


- 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 FSx 管理员的防火墙上。

 Important

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

 Note

如果您已定义 Active Directory 站点，您必须确保在 Active Directory 站点中定义了与 Amazon FSx 文件系统关联的 VPC 中的子网，且 VPC 中的子网与您其他站点中的子网之间不存在冲突。您可以使用 Active Directory 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 AWS 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必需的允许您的 Amazon FSx 文件系统的流量入站规则。

有关必需的入站规则的更多信息，请参阅《AWS Directory Service 管理指南》中的[AWS 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。

添加与您的 Amazon FSx 文件系统关联的安全组

1. 通过以下网址打开 Amazon FSx 控制台：<https://console.aws.amazon.com/fsx/>。
2. 在控制面板上，选择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，可以删除与文件系统的弹性网络接口关联的所有安全组，并将其替换为没有入站/出站规则的组。

## Amazon VPC 网络 ACL

另一种保护 VPC 内文件系统访问权限的方法是建立网络访问控制列表（网络 ACL）。网络 ACL 与安全组是分开的，但它们具有相似的功能，可以为 VPC 中的资源添加额外安全层。有关网络 ACL 的更多信息，请参阅《Amazon VPC 用户指南》中的[网络 ACL](#)。

## Amazon FSx for Windows File Server 的身份和访问管理

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以通过身份验证（登录）和获得授权（具有权限）来使用 Amazon FSx 资源。您可以使用 IAM AWS 服务，无需支付额外费用。

主题

- [受众](#)

- [使用身份进行身份验证](#)
- [使用策略管理访问](#)
- [如何结合使用 Amazon FSx for Windows File Server 和 IAM](#)
- [Amazon FSx for Windows File Server 基于身份的策略示例](#)
- [AWS 亚马逊 FSx 的托管策略](#)
- [Amazon FSx for Windows File Server 身份识别和访问问题排查](#)
- [在 Amazon FSx 上使用标签](#)
- [使用 Amazon FSx 的服务相关角色](#)

## 受众

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

**服务用户** – 如果您使用 Amazon FSx 服务来完成任务，则您的管理员会为您提供所需的凭证和权限。随着您使用更多 Amazon FSx 功能来完成工作，您可能需要额外权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 Amazon FSx 中的功能，请参阅[Amazon FSx for Windows File Server 身份识别和访问问题排查](#)。

**服务管理员** – 如果您在公司负责管理 Amazon FSx 资源，您可能对 Amazon FSx 具有完全访问权限。您有责任确定您的服务用户应访问哪些 Amazon FSx 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要了解有关您的公司如何将 IAM 与 Amazon FSx 搭配使用的更多信息，请参阅[如何结合使用 Amazon FSx for Windows File Server 和 IAM](#)。

**IAM 管理员** – 如果您是 IAM 管理员，您可能需要详细了解如何编写策略以管理对 Amazon FSx 的访问。要查看您可在 IAM 中使用的 Amazon FSx 基于身份的策略示例，请参阅[Amazon FSx for Windows File Server 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 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。AWS IAM Identity Center（IAM Identity Center）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。

当您以联合身份登录时，管理员以前使用 IAM 角色设置了身份联合验证。当您使用联合访问 AWS 时，您就是在间接扮演一个角色。

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

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

无论使用何种身份验证方法，您可能都需要提供其它安全信息。例如，AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center 用户指南》中的[多重身份验证](#)和《IAM 用户指南》中的[在 AWS 中使用多重身份验证 \(MFA\)](#)。

## AWS 账户 root 用户

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

## 联合身份

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

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

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

## IAM 用户和组

[IAM 用户](#)是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果有一些特定的使

用场景需要长期凭证以及 IAM 用户，我们建议轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的 [对于需要长期凭证的使用场景定期轮换访问密钥](#)。

[IAM 组](#)是一个用于指定一组 IAM 用户的身份。您不能使用组的身份登录。可以使用群组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，可能具有一个名为 IAMAdmins 的群组，并为该群组授予权限以管理 IAM 资源。

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

## IAM 角色

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

具有临时凭证的 IAM 角色在以下情况下很有用：

- Federated user access ( 联合用户访问 ) - 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的 [为第三方身份提供商创建角色](#)。如果使用 IAM Identity Center，则需要配置权限集。为控制身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的[权限集](#)。
- 临时 IAM 用户权限 – IAM 用户或角色可代入一个 IAM 角色，以暂时获得针对特定任务的不同权限。
- 跨账户访问 – 您可以使用 IAM 角色以允许不同账户中的某个人 ( 可信主体 ) 访问账户中的资源。角色是授予跨账户存取权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源 ( 而不是使用角色作为代理 )。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅 IAM 用户指南中的 [IAM 角色与基于资源的策略有何不同](#)。
- 跨服务访问 — 有些 AWS 服务使用其他 AWS 服务服务中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
- 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。AWS 服务只有当服务收到需要与其他

AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅[转发访问会话](#)。

- 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 [IAM 角色](#)。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的 [创建向 AWS 服务 委派权限的角色](#)。
- 服务相关角色-服务相关角色是一种链接到的服务角色。AWS 服务服务可以担任代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 Amazon EC2 上运行的应用程序 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这优先于在 EC2 实例中存储访问密钥。要向 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建附加到该实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的 [使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限](#)。

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

## 使用策略管理访问

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

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

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

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



## 基于身份的策略

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

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

## 基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 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。必须在基于资源的策略中 [指定主体](#)。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

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

## 访问控制列表 (ACL)

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

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

## 其他策略类型

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

- **权限边界** – 权限边界是一个高级功能，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 Principal 字段中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅《IAM 用户指南》中的 [IAM 实体的权限边界](#)。
- **服务控制策略 (SCP)**-SCP 是 JSON 策略，用于指定组织或组织单位 (OU) 的最大权限。AWS Organizations AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管

理的服务。如果在组织内启用了所有功能，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organizations 和 SCP 的更多信息，请参阅《AWS Organizations 用户指南》中的 [SCP 的工作原理](#)。

- 会话策略 – 会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅《IAM 用户指南》中的 [会话策略](#)。

## 多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的 [策略评估逻辑](#)。

## 如何结合使用 Amazon FSx for Windows File Server 和 IAM

在使用 IAM 管理对 Amazon FSx 的访问之前，了解哪些 IAM 功能可与 Amazon FSx 配合使用。

可以与 Amazon FSx for Windows File Server 结合使用的 IAM 功能

| IAM 特征                       | FSx 支持 |
|------------------------------|--------|
| <a href="#">基于身份的策略</a>      | 是      |
| <a href="#">基于资源的策略</a>      | 否      |
| <a href="#">策略操作</a>         | 是      |
| <a href="#">策略资源</a>         | 是      |
| <a href="#">策略条件键（特定于服务）</a> | 是      |
| <a href="#">ACL</a>          | 否      |
| <a href="#">ABAC（策略中的标签）</a> | 是      |
| <a href="#">临时凭证</a>         | 是      |
| <a href="#">转发访问会话</a>       | 是      |

| IAM 特征                 | FSx 支持 |
|------------------------|--------|
| <a href="#">服务角色</a>   | 否      |
| <a href="#">服务相关角色</a> | 是      |

要全面了解 FSx 和其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中[与 IAM 配合使用的AWS 服务](#)。

## FSx 的基于身份的策略

|           |   |
|-----------|---|
| 支持基于身份的策略 | 是 |
|-----------|---|

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

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

## FSx 的基于身份的策略示例

要查看 Amazon FSx 基于身份的策略示例，请参阅[Amazon FSx for Windows File Server 基于身份的策略示例](#)。

## FSx 内基于资源的策略

|           |   |
|-----------|---|
| 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。必须在基于资源的策略中[指定主体](#)。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户存取，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。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 AWS 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅 IAM 用户指南中的 [IAM 角色与基于资源的策略有何不同](#)。

## 适用于 FSx 的策略操作

支持策略操作

是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 Action 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看 FSx 操作列表，请参阅《服务授权参考》中的 [Amazon FSx for Windows File Server 定义的操作](#)。

FSx 中的策略操作在操作前使用以下前缀：

```
fsx
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
 "fsx:action1",
 "fsx:action2"
]
```

要查看 Amazon FSx 基于身份的策略示例，请参阅 [Amazon FSx for Windows File Server 基于身份的策略示例](#)。

## FSx 的策略资源

支持策略资源 是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

ResourceJSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 [Amazon 资源名称 \(ARN\)](#) 指定资源。对于支持特定资源类型（称为资源级权限）的操作，可以执行此操作。

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

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

要查看 FSx 资源类型及其 ARN 的列表，请参阅《服务授权参考》中的 [Amazon FSx for Windows File Server 定义的资源](#)。要了解您可以在哪些操作中指定每个资源的 ARN，请参阅 [Amazon FSx for Windows File Server 定义的操作](#)。

要查看 Amazon FSx 基于身份的策略示例，请参阅 [Amazon FSx for Windows File Server 基于身份的策略示例](#)。

## FSx 的策略条件键

支持特定于服务的策略条件键 是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

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

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

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

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的 [AWS 全局条件上下文密钥](#)。

要查看 Amazon FSx 条件键的列表，请参阅《服务授权参考》中的 [Amazon FSx for Windows File Server 的条件键](#)。要了解您可以对哪些操作和资源使用条件键，请参阅 [Amazon FSx for Windows File Server 定义的操作](#)。

要查看 Amazon FSx 基于身份的策略示例，请参阅 [Amazon FSx for Windows File Server 基于身份的策略示例](#)。

## FSx 中的 ACL

|        |   |
|--------|---|
| 支持 ACL | 否 |
|--------|---|

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

## ABAC 和 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，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以将标签附加到 IAM 实体（用户或角色）和许多 AWS 资源。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

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

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

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

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的[什么是 ABAC？](#) 要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的[使用基于属性的访问权限控制 \( ABAC \)](#)。

## 将临时凭证用于 FSx

支持临时凭证 是

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

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

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 [IAM 中的临时安全凭证](#)。

## FSx 的转发访问会话

支持转发访问会话 (FAS) 是

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

## FSx 的服务角色

支持服务角色 否

服务角色是由一项服务代入、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 AWS 服务 委派权限的角色](#)。

**⚠ Warning**

更改服务角色的权限可能会破坏 FSx 的功能。仅当 FSx 提供相关指导时才编辑服务角色。

## FSx 的服务相关角色

支持服务相关角色

是

服务相关角色是一种与服务相关联的 AWS 服务角色。服务可以担任代表您执行操作的角色。服务相关角色出现在您的 AWS 账户，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

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

## Amazon FSx for Windows File Server 基于身份的策略示例

默认情况下，用户和角色没有创建或修改 Amazon FSx 资源的权限。他们也无法使用 AWS Management Console、AWS Command Line Interface (AWS CLI) 或 AWS API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM policy。管理员随后可以向角色添加 IAM policy，然后用户就可以代入角色。

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

有关 FSx 定义的操作和资源类型的详细信息，包括每种资源类型的 ARN 格式，请参阅《服务授权参考》中的 [Amazon FSx for Windows File Server 的操作、资源和条件键](#)。

### 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

基于身份的策略确定某个人是否可以创建、访问或删除您账户中的 Amazon FSx 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：



- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的 AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 [AWS 托管策略](#) 或 [工作职能的 AWS 托管策略](#)。
- 应用最低权限 - 在使用 IAM policy 设置权限时，请仅授予执行任务所需的权限。为此，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，可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 AWS CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 [IAM JSON 策略元素：条件](#)。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言 (JSON) 和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 [IAM Access Analyzer 策略验证](#)。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到策略中。有关更多信息，请参阅《IAM 用户指南》中的 [配置受 MFA 保护的 API 访问](#)。

有关 IAM 中的最佳实践的更多信息，请参阅 IAM 用户指南中的 [IAM 中的安全最佳实践](#)。

## 使用 FSx 控制台

要访问 Amazon FSx for Windows File Server 控制台，您必须具有一组最低的权限。这些权限必须允许您列出和查看有关您的 Amazon FSx 资源的详细信息。AWS 账户如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色仍然可以使用 FSx 控制台，还要将 FSx AmazonFSxConsoleReadOnlyAccess AWS 托管策略附加到实体。有关更多信息，请参阅《IAM 用户指南》中的 [为用户添加权限](#)。

## 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策略和托管策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "ViewOwnUserInfo",
 "Effect": "Allow",
 "Action": [
 "iam:GetUserPolicy",
 "iam:ListGroupForUser",
 "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": "*"
 }
]
}
```

## AWS 亚马逊 FSx 的托管策略

AWS 托管策略是由创建和管理的独立策略 AWS。AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住，AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的[客户管理型策略](#)来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅 IAM 用户指南 中的 [AWS 托管策略](#)。

## AmazonF SxServiceRolePolicy

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

## AWS 托管策略：亚马逊 SxDeleteServiceLinkedRoleAccess

您不能将 AmazonFSxDeleteServiceLinkedRoleAccess 附加到自己的 IAM 实体。该策略关联到服务，仅用于该服务的服务相关角色。您不能附加、分离、修改或删除此策略。有关更多信息，请参阅 [使用 Amazon FSx 的服务相关角色](#)。

该策略授予管理权限，允许 Amazon FSx 删除用于访问 Amazon S3 的服务相关角色，仅供 Amazon FSx for Lustre 使用。

### 权限详细信息

此策略包括 iam 中的以下权限：允许 Amazon FSx 对用于访问 Amazon S3 的 FSx 服务相关角色进行查看、删除及查看其删除状态。

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

## AWS 托管策略：亚马逊 SxFullAccess

您可以将 AmazonF 附加 SxFullAccess 到您的 IAM 实体。Amazon FSx 还会将此策略附加到允许 Amazon FSx 代表您执行操作的服务角色。

提供对 Amazon FSx 的完全访问权限和对相关 AWS 服务的访问权限。

### 权限详细信息

该策略包含以下权限。

- fsx – 允许主体完全访问，可执行所有 Amazon FSx 操作，但 BypassSnaplockEnterpriseRetention 除外。

- ds— 允许委托人查看有关 AWS Directory Service 目录的信息。
- ec2
  - 允许委托人在指定条件下创建标签。
  - 为可用于 VPC 的所有安全组提供增强的安全组验证。
- iam – 允许主体代表用户创建 Amazon FSx 服务相关角色。这是必需的，这样 Amazon FSx 才能代表用户管理 AWS 资源。
- logs – 允许主体创建日志组、日志流并将事件写入日志流。这是必需的，这样用户才能通过向日志发送审核访问日志 CloudWatch 来监控 FSx 的 Windows File Server 文件系统访问权限。
- firehose— 允许委托人向 Amazon Data Firehose 写入记录。这是必需的，这样用户才能通过向 Firehose 发送审核访问日志来监控 FSx 的 Windows 文件服务器文件系统访问权限。

要查看此策略的权限，请参阅《AWS 托管策略参考指南》SxFullAccess 中的 [AmazonF](#)。

## AWS 托管策略：亚马逊 SxConsoleFullAccess

您可以将 AmazonFSxConsoleFullAccess 策略附加到 IAM 身份。

此策略授予管理权限，允许对 Amazon FSx 进行完全访问和通过访问相关 AWS 服务。AWS Management Console

### 权限详细信息

该策略包含以下权限。

- fsx – 允许主体在 Amazon FSx 管理控制台中执行所有操作，但 BypassSnaplockEnterpriseRetention 除外。
- cloudwatch— 允许委托人在 Amazon FSx 管理控制台中查看 CloudWatch 警报和指标。
- ds— 允许委托人列出有关 AWS Directory Service 目录的信息。
- ec2
  - 允许委托人在路由表上创建标签，列出网络接口、路由表、安全组、子网和与 Amazon FSx 文件系统关联的 VPC。
  - 为可用于 VPC 的所有安全组提供增强的安全组验证。
- kms— 允许委托人列出密钥的别名。AWS Key Management Service
- s3 – 允许主体列出 Amazon S3 桶中的部分或全部对象（最多 1000 个）。

- iam – 授予创建服务相关角色的权限，允许 Amazon FSx 代表用户执行操作。

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

## AWS 托管策略：亚马逊 SxConsoleReadOnlyAccess

您可以将 AmazonFSxConsoleReadOnlyAccess 策略附加到 IAM 身份。

此策略向 Amazon FSx 和相关 AWS 服务授予只读权限，以使用户可以在中查看有关这些服务的信息。AWS Management Console

### 权限详细信息

该策略包含以下权限。

- fsx – 允许主体在 Amazon FSx 管理控制台中查看有关 Amazon FSx 文件系统的信息，包括所有标签。
- cloudwatch— 允许委托人在 Amazon FSx 管理控制台中查看 CloudWatch 警报和指标。
- ds— 允许委托人在 Amazon FSx AWS Directory Service 管理控制台中查看有关目录的信息。
- ec2
  - 允许委托人在 Amazon FSx 管理控制台中查看网络接口、安全组、子网以及与 Amazon FSx 文件系统关联的 VPC。
  - 为可用于 VPC 的所有安全组提供增强的安全组验证。
- kms— 允许委托人在 Amazon FSx 管理控制 AWS Key Management Service 台中查看密钥的别名。
- log— 允许委托人描述与提出请求的账户关联的 Amazon Logs CloudWatch 日志组。必须具有此权限，主体才能查看 FSx for Windows File Server 文件系统的现有文件访问审计配置。
- firehose— 允许委托人描述与提出请求的账户关联的 Amazon Data Firehose 传输流。必须具有此权限，主体才能查看 FSx for Windows File Server 文件系统的现有文件访问审计配置。

要查看此策略的权限，请参阅《AWS 托管策略参考指南》SxConsoleReadOnlyAccess 中的 [AmazonF](#)。

## AWS 托管策略：亚马逊 SxReadOnlyAccess

您可以将 AmazonFSxReadOnlyAccess 策略附加到 IAM 身份。

此策略授予允许对 Amazon FSx 进行只读访问的管理权限。

- fsx – 允许主体在 Amazon FSx 管理控制台中查看有关 Amazon FSx 文件系统的信息，包括所有标签。
- ec2— 为可用于 VPC 的所有安全组提供增强的安全组验证。

要查看此策略的权限，请参阅《AWS 托管策略参考指南》SxReadOnlyAccess 中的 [AmazonF](#)。

## 亚马逊 FSx 更新了托管政策 AWS

查看自该服务开始跟踪这些更改以来对 Amazon FSx AWS 托管政策的更新的详细信息。要获得有关此页面更改的自动提示，请订阅 Amazon FSx [文档历史记录](#) 页面上的 RSS 源。

| 更改                                                    | 描述                                                                            | 日期             |
|-------------------------------------------------------|-------------------------------------------------------------------------------|----------------|
| <a href="#">亚马逊 SxServiceRolePolicy</a> -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 |
| <a href="#">亚马逊 SxReadOnlyAccess</a> -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 |
| <a href="#">亚马逊 SxConsoleReadOnlyAccess</a> -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 |
| <a href="#">亚马逊 SxFullAccess</a> -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               |
|------------------------------------------------------|---------------------------------------------------------------------------------------------|------------------|
| <a href="#">亚马逊 SxConsoleFullAccess-</a><br>对现有政策的更新 | Amazon FSx 增加了新权限 <code>ec2:GetSecurityGroupsForVpc</code> ，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   |
| <a href="#">亚马逊 SxFullAccess-</a> 对现有政策的更新           | Amazon FSX 增加了新的权限，使用户能够为 OpenZFS 文件系统的 FSX 执行跨区域和跨账户数据复制。                                  | 2023 年 12 月 20 日 |
| <a href="#">亚马逊 SxConsoleFullAccess-</a><br>对现有政策的更新 | Amazon FSX 增加了新的权限，使用户能够为 OpenZFS 文件系统的 FSX 执行跨区域和跨账户数据复制。                                  | 2023 年 12 月 20 日 |
| <a href="#">亚马逊 SxFullAccess-</a> 对现有政策的更新           | Amazon FSX 增加了新权限，允许用户按需复制 OpenZFS 文件系统的 FSX 卷。                                             | 2023 年 11 月 26 日 |
| <a href="#">亚马逊 SxConsoleFullAccess-</a><br>对现有政策的更新 | Amazon FSX 增加了新权限，允许用户按需复制 OpenZFS 文件系统的 FSX 卷。                                             | 2023 年 11 月 26 日 |
| <a href="#">亚马逊 SxFullAccess-</a> 对现有政策的更新           | Amazon FSx 添加了新的权限，使用户能够查看、启用和禁用对适用于 ONTAP 多可用区文件系统的 FSx 的共享 VPC 支持。                        | 2023 年 11 月 14 日 |
| <a href="#">亚马逊 SxConsoleFullAccess-</a><br>对现有政策的更新 | Amazon FSx 添加了新的权限，使用户能够查看、启用和禁用对适用于 ONTAP 多可用区文件系统的 FSx 的共享 VPC 支持。                        | 2023 年 11 月 14 日 |

| 更改                                                           | 描述                                                                                                 | 日期              |
|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------|-----------------|
| <a href="#">亚马逊 SxFullAccess</a> -对现有政策的更新                   | Amazon FSx 增加了新的权限，允许 Amazon FSx 管理 FSx for OpenZFS 多可用区文件系统的网络配置。                                 | 2023 年 8 月 9 日  |
| <a href="#">AWS 托管策略：AmazonFSxServiceRolePolicy</a> — 更新现有政策 | Amazon FSx 修改了现有 <code>cloudwatch:PutMetricData</code> 权限，以便亚马逊 FSx 将 CloudWatch 指标发布到命名空间。AWS/FSx | 2023 年 7 月 24 日 |
| <a href="#">亚马逊 SxFullAccess</a> -对现有政策的更新                   | Amazon FSx 更新了该策略，删除了 <code>fsx:*</code> 权限并添加了具体的 <code>fsx</code> 操作。                            | 2023 年 7 月 13 日 |
| <a href="#">亚马逊 SxConsoleFullAccess</a> -对现有政策的更新            | Amazon FSx 更新了该策略，删除了 <code>fsx:*</code> 权限并添加了具体的 <code>fsx</code> 操作。                            | 2023 年 7 月 13 日 |
| <a href="#">亚马逊 SxFullAccess</a> -对现有政策的更新                   | Amazon FSx 增加了新的权限，允许 Amazon FSx 管理 FSx for OpenZFS 多可用区文件系统的网络配置。                                 | 2023 年 5 月 31 日 |
| <a href="#">亚马逊 SxConsoleReadOnlyAccess</a> -对现有政策的更新        | Amazon FSx 增加了新的权限，用户能够在 Amazon FSx 控制台中查看 FSx for Windows File Server 文件系统的增强性能指标和建议的操作。          | 2022 年 9 月 21 日 |



| 更改                                                              | 描述                                                                                        | 日期              |
|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------|-----------------|
| <a href="#">亚马逊 SxConsoleFullAccess-</a><br>对现有政策的更新            | Amazon FSx 增加了新的权限，用户能够在 Amazon FSx 控制台中查看 FSx for Windows File Server 文件系统的增强性能指标和建议的操作。 | 2022 年 9 月 21 日 |
| <a href="#">亚马逊 SxReadOnlyAccess</a> —<br>已开始执行追踪政策             | 此策略授予对所有 Amazon FSx 资源及其相关标签的只读访问权限。                                                      | 2022 年 2 月 4 日  |
| <a href="#">亚马逊 SxDeleteServiceLinkedRoleAccess</a> — 已开始执行追踪政策 | 此策略授予管理权限，允许 Amazon FSx 删除用于访问 Amazon S3 的服务相关角色。                                         | 2022 年 1 月 7 日  |
| <a href="#">亚马逊 SxServiceRolePolicy-</a><br>对现有政策的更新            | 亚马逊 FSx 增加了新的权限，允许亚马逊 FSx 管理适用于 ONTAP 文件系统的亚马逊 FSx 的网络配置。NetApp                           | 2021 年 9 月 2 日  |
| <a href="#">亚马逊 SxFullAccess-</a> 对现有政策的更新                      | Amazon FSx 增加了新的权限，允许 Amazon FSx 在 EC2 路由表上创建标签，从而缩小了调用范围。                                | 2021 年 9 月 2 日  |
| <a href="#">亚马逊 SxConsoleFullAccess-</a><br>对现有政策的更新            | 亚马逊 FSx 增加了新的权限，允许亚马逊 FSx 为 ONTAP 多可用区文件系统创建亚马逊 FSX。NetApp                                | 2021 年 9 月 2 日  |
| <a href="#">亚马逊 SxConsoleFullAccess-</a><br>对现有政策的更新            | Amazon FSx 增加了新的权限，允许 Amazon FSx 在 EC2 路由表上创建标签，从而缩小了调用范围。                                | 2021 年 9 月 2 日  |

| 更改                                                | 描述                                                                                                                                                   | 日期             |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| <a href="#">亚马逊 SxServiceRolePolicy</a> -对现有政策的更新 | <p>Amazon FSx 添加了新的权限，允许 Amazon FSx 描述和写入日志流。 CloudWatch</p> <p>这是必需的，这样用户才能使用日志查看 FSx for Windows File Server 文件系统的 CloudWatch 文件访问审核日志。</p>        | 2021 年 6 月 8 日 |
| <a href="#">亚马逊 SxServiceRolePolicy</a> -对现有政策的更新 | <p>亚马逊 FSx 增加了新的权限，允许亚马逊 FSx 描述和写入亚马逊数据 Firehose 传输流。</p> <p>这是必需的，这样用户才能使用 Amazon Data Firehose 查看 FSx for Windows 文件服务器文件系统的文件访问审核日志。</p>          | 2021 年 6 月 8 日 |
| <a href="#">亚马逊 SxFullAccess</a> -对现有政策的更新        | <p>Amazon FSx 添加了新的权限，允许委托人描述和创建 CloudWatch 日志组、日志流以及将事件写入日志流。</p> <p>这是必需的，这样委托人才能使用日志查看 FSx for Windows File Server 文件系统的 CloudWatch 文件访问审核日志。</p> | 2021 年 6 月 8 日 |

| 更改                                                | 描述                                                                                                                                                               | 日期             |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| <a href="#">亚马逊 SxFullAccess</a> -对现有政策的更新        | <p>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。</p> <p>这是必需的，这样用户才能使用 Amazon Data Firehose 查看 FSx for Windows 文件服务器文件系统的文件访问审核日志。</p>                           | 2021 年 6 月 8 日 |
| <a href="#">亚马逊 SxConsoleFullAccess</a> -对现有政策的更新 | <p>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。</p> <p>这是必需的，这样委托人才能在为 FSx for Windows File Server 文件系统配置文件访问审计时选择现有的 CloudWatch 日志日志组。</p> | 2021 年 6 月 8 日 |
| <a href="#">亚马逊 SxConsoleFullAccess</a> -对现有政策的更新 | <p>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 传送流。</p> <p>这是必需的，这样委托人才能在为 FSx for Windows File Server 文件系统配置文件访问审计时选择现有的 Firehose 传送流。</p>          | 2021 年 6 月 8 日 |

| 更改                                                    | 描述                                                                                                                                   | 日期             |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|----------------|
| <a href="#">亚马逊 SxConsoleReadOnlyAccess</a> -对现有政策的更新 | Amazon FSx 添加了新的权限，允许委托人描述与提出请求的账户关联的 Amazon Logs CloudWatch 日志组。<br><br>必须具有此权限，主体才能查看 FSx for Windows File Server 文件系统的现有文件访问审计配置。 | 2021 年 6 月 8 日 |
| <a href="#">亚马逊 SxConsoleReadOnlyAccess</a> -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 传送流。<br><br>必须具有此权限，主体才能查看 FSx for Windows File Server 文件系统的现有文件访问审计配置。      | 2021 年 6 月 8 日 |
| Amazon FSx 开启了跟踪更改                                    | Amazon FSx 开始跟踪其 AWS 托管策略的变更。                                                                                                        | 2021 年 6 月 8 日 |

## Amazon FSx for Windows File Server 身份识别和访问问题排查

使用以下信息可帮助您诊断和修复在使用 Amazon FSx 和 IAM 时可能遇到的常见问题。

### 主题

- [我无权在 FSx 中执行操作](#)
- [我无权执行 iam : PassRole](#)
- [我想允许我以外的人 AWS 账户 访问我的 FSx 资源](#)

### 我无权在 FSx 中执行操作

如果您收到错误提示，表明您无权执行某个操作，则您必须更新策略以允许执行该操作。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 *my-example-widget* 资源的详细信息，但不拥有虚构 `fsx:GetWidget` 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
fsx:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 `fsx:GetWidget` 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

## 我无权执行 iam : PassRole

如果您收到一个错误，指明您无权执行 `iam:PassRole` 操作，则必须更新策略以允许您将角色传递给 Amazon FSx。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 marymajor 的 IAM 用户尝试使用控制台在 Amazon FSx 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

## 我想允许我以外的人 AWS 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。可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表 (ACL) 的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 Amazon FSx 是否支持这些功能，请参阅 [如何结合使用 Amazon FSx for Windows File Server 和 IAM](#)。

- 要了解如何提供对您拥有的资源的访问权限 AWS 账户，请参阅 [IAM 用户指南中的向您拥有 AWS 账户的另一个 IAM 用户提供访问权限](#)。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 [IAM 用户指南中的向第三方提供访问权限](#)。AWS 账户
- 要了解如何通过联合身份验证提供访问权限，请参阅《IAM 用户指南》中的 [为经过外部身份验证的用户 \(联合身份验证\) 提供访问权限](#)。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 [IAM 角色与基于资源的策略有何不同](#)。

## 在 Amazon FSx 上使用标签

您可以使用标签来控制对 Amazon FSx 资源的访问权限并实现基于属性的访问权限控制 (ABAC)。用户需要具有在创建期间对 Amazon FSx 资源应用标签的权限。

### 在创建过程中授予标记资源的权限

某些资源创建 Amazon FSx API 操作允许您在创建资源时指定标签。您可以使用资源标签来实现基于属性的访问控制 (ABAC)。有关更多信息，请参阅《IAM 用户指南》中的 [什么是适用于 AWS 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 AWS 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中创建备份，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。

有关标记 Amazon FSx 资源的更多信息，请参阅[标记 Amazon FSx 资源](#)。有关如何使用标签控制对 FSx 资源的访问权限的更多信息，请参阅[使用标签控制对 Amazon FSx 资源的访问权限](#)。

## 使用标签控制对 Amazon FSx 资源的访问权限

要控制对 Amazon FSx 资源和操作的访问权限，您可以使用基于标签的 AWS Identity and Access Management (IAM) 策略。您可以使用两种方法提供控制：

1. 根据这些资源上的标签控制对 Amazon FSx 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 AWS 资源访问的信息，请参阅 IAM 用户指南中的[使用标签控制访问权限](#)。有关在创建时标记 Amazon FSx 资源的更多信息，请参阅[在创建过程中授予标记资源的权限](#)。有关标记资源的更多信息，请参阅[标记 Amazon FSx 资源](#)。

根据资源上的标签控制访问权限

要控制用户或角色可以对 Amazon FSx 资源执行的操作，您可以使用资源上的标签。例如，您可能希望根据文件系统资源上的标签的键/值对允许或拒绝对该资源执行特定的 API 操作。

Example 策略 – 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 – 仅在带有特定标签的 Amazon FSx 文件系统上创建备份

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 Department=Finance 标签创建备份。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "fsx:CreateBackup"
],
 "Resource": "arn:aws:fsx:region:account-id:file-system/*",
 "Condition": {
```



```

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

```

### Example 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。

```

{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "fsx:CreateFileSystemFromBackup",
 "fsx:TagResource"
],
 "Resource": "arn:aws:fsx:region:account-id:backup/*",
 "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。

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

## 使用 Amazon FSx 的服务相关角色

适用于 Windows File Server 的 Amazon FSx AWS Identity and Access Management 使用 (IAM) [服务相关角色](#)。服务相关角色是一种独特类型的 IAM 角色，与 Amazon FSx 直接相关。服务相关角色由 Amazon FSx 预定义，包括该服务代表您调用 AWS 其他服务所需的所有权限。

服务相关角色可让您更轻松地设置 Amazon FSx，因为您不必手动添加必要的权限。Amazon FSx 定义其服务相关角色的权限，除非另外定义，否则只有 Amazon FSx 可以代入该角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其他 IAM 实体的权限策略。

只有在首先删除相关资源后，您才能删除服务相关角色。这将保护您的 Amazon FSx 资源，因为您不会无意中删除对资源的访问权限。

有关支持服务相关角色的其他服务的信息，请参阅[使用 IAM 的 AWS 服务](#)并查找服务相关角色列中显示为是的服务。选择是，可转到查看该服务的[服务相关角色文档](#)的链接。

### Amazon FSx 的服务相关角色权限

Amazon FSx 使用名为 `AWSServiceRoleForAmazonFSx` 的服务相关角色 – 在您的账户中执行某些操作，例如在 VPC 中为文件系统创建弹性网络接口。

角色权限策略允许 Amazon FSx 在所有适用 AWS 资源上完成以下操作：

您不能将 `AmazonFSxServiceRolePolicy` 附加到您的 IAM 实体。此策略附加到服务相关角色，允许 FSx 代表您 AWS 管理资源。有关更多信息，请参阅[使用 Amazon FSx 的服务相关角色](#)。

有关本政策的更新，请参阅 [AmazonFSxServiceRolePolicy](#)

此策略授予管理权限，允许 FSx 代表用户管理 AWS 资源。

权限详细信息

`AmazonFSxServiceRolePolicy` 角色权限由 `AmazonFSxServiceRolePolicy` AWS 托管策略定义。`AmazonFSxServiceRolePolicy` 拥有以下权限：

#### Note

所有亚马逊 F `SxServiceRolePolicy` Sx 文件系统类型都使用 AmazonF；列出的某些权限可能不适用于 Windows 版 FSx。

- `ds`— 允许 FSx 查看、授权和取消对您目录中的应用程序的授权。AWS Directory Service

- ec2 – 允许 FSx 执行以下操作：
  - 查看、创建与 Amazon FSx 文件系统关联的网络接口以及取消关联。
  - 查看一个或多个与 Amazon FSx 文件系统关联的弹性 IP 地址。
  - 查看与 Amazon FSx 文件系统关联的 Amazon VPC、安全组 and 子网。
  - 为可用于 VPC 的所有安全组提供增强的安全组验证。
  - 为获得 AWS 授权的用户创建在网络接口上执行某些操作的权限。
- cloudwatch— 允许 FSx 在 AWS /fsx 命名空间 CloudWatch 下发布指标数据点。
- route53 – 允许 FSx 将 Amazon VPC 与私有托管区关联。
- logs— 允许 FSx 描述和写入 CloudWatch 日志流。这样，用户就可以将 FSx for Windows File Server 文件系统的文件访问审核日志发送到日志 CloudWatch 流。
- firehose— 允许 FSx 描述和写入 Amazon Data Firehose 传送流。这样，用户就可以将 FSx for Windows File Server 文件系统的文件访问审核日志发布到亚马逊数据 Firehose 传输流。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "CreateFileSystem",
 "Effect": "Allow",
 "Action": [
 "ds:AuthorizeApplication",
 "ds:GetAuthorizedApplicationDetails",
 "ds:UnauthorizeApplication",
 "ec2:CreateNetworkInterface",
 "ec2:CreateNetworkInterfacePermission",
 "ec2>DeleteNetworkInterface",
 "ec2:DescribeAddresses",
 "ec2:DescribeDhcpOptions",
 "ec2:DescribeNetworkInterfaces",
 "ec2:DescribeRouteTables",
 "ec2:DescribeSecurityGroups",
 "ec2:DescribeSubnets",
 "ec2:DescribeVPCs",
 "ec2:DisassociateAddress",
 "ec2:GetSecurityGroupsForVpc",
 "route53:AssociateVPCWithHostedZone"
],
 "Resource": "*"
 }
]
}
```

```
 },
 {
 "Sid": "PutMetrics",
 "Effect": "Allow",
 "Action": [
 "cloudwatch:PutMetricData"
],
 "Resource": [
 "*"
],
 "Condition": {
 "StringEquals": {
 "cloudwatch:namespace": "AWS/FSx"
 }
 }
 },
 {
 "Sid": "TagResourceNetworkInterface",
 "Effect": "Allow",
 "Action": [
 "ec2:CreateTags"
],
 "Resource": [
 "arn:aws:ec2:*:*:network-interface/*"
],
 "Condition": {
 "StringEquals": {
 "ec2:CreateAction": "CreateNetworkInterface"
 },
 "ForAllValues:StringEquals": {
 "aws:TagKeys": "AmazonFSx.FileSystemId"
 }
 }
 },
 {
 "Sid": "ManageNetworkInterface",
 "Effect": "Allow",
 "Action": [
 "ec2:AssignPrivateIpAddresses",
 "ec2:ModifyNetworkInterfaceAttribute",
 "ec2:UnassignPrivateIpAddresses"
],
 "Resource": [
```

```

 "arn:aws:ec2:*:*:network-interface/*"
],
 "Condition": {
 "Null": {
 "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
 }
 }
},
{
 "Sid": "ManageRouteTable",
 "Effect": "Allow",
 "Action": [
 "ec2:CreateRoute",
 "ec2:ReplaceRoute",
 "ec2>DeleteRoute"
],
 "Resource": [
 "arn:aws:ec2:*:*:route-table/*"
],
 "Condition": {
 "StringEquals": {
 "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
 }
 }
},
{
 "Sid": "PutCloudWatchLogs",
 "Effect": "Allow",
 "Action": [
 "logs:DescribeLogGroups",
 "logs:DescribeLogStreams",
 "logs:PutLogEvents"
],
 "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
},
{
 "Sid": "ManageAuditLogs",
 "Effect": "Allow",
 "Action": [
 "firehose:DescribeDeliveryStream",
 "firehose:PutRecord",
 "firehose:PutRecordBatch"
],
 "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
}

```

```
 }
]
}
```

[亚马逊 FSx 更新了托管政策 AWS](#) 中介绍了本政策的所有更新。

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的[服务相关角色权限](#)。

## 为 Amazon FSx 创建服务相关角色

您无需手动创建服务相关角色。当您在 AWS Management Console、IAM CLI 或 IAM API 中创建文件系统时，Amazon FSx 会为您创建服务相关角色。

### Important

如果您在其他使用此角色支持的功能的服务中完成某个操作，此服务相关角色可以出现在您的账户中。要了解更多信息，请参阅[我的 IAM 账户中的新角色](#)。

如果您删除该服务相关角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。当您创建文件系统时，Amazon FSx 会再次为您创建服务相关角色。

## 为 Amazon FSx 编辑服务相关角色

Amazon FSx 不允许您编辑服务相关角色。创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色描述。有关更多信息，请参阅《IAM 用户指南》中的[编辑服务相关角色](#)。

## 删除 Amazon FSx 的服务相关角色

如果不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样就没有未被主动监控或维护的未使用实体。但是，您必须先删除所有文件系统和备份，然后才能手动删除服务相关角色。

### Note

如果当您试图删除资源时 Amazon FSx 服务正在使用该角色，则删除操作可能会失败。如果发生这种情况，请等待几分钟后重试。

## 使用 IAM 手动删除服务相关角色

使用 IAM 控制台、IAM CLI 或 IAM API 删除 服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的[删除服务相关角色](#)。

## Amazon FSx 服务相关角色支持的区域

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

## Amazon FSx for Windows File Server 合规性验证

要了解是否属于特定合规计划的范围，请参阅AWS 服务“[按合规计划划分的范围](#)”，然后选择您感兴趣的合规计划。AWS 服务 有关一般信息，请参阅[AWS 合规计划AWS](#)。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的“[下载报告](#)”中的“[AWS Artifact](#)”。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。AWS 提供了以下资源来帮助实现合规性：

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

### Note

并非所有 AWS 服务 人都符合 HIPAA 资格。有关更多信息，请参阅[符合 HIPAA 要求的服务参考](#)。

- [AWS 合规资源AWS](#) — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- [AWS 客户合规指南](#) — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践，AWS 服务 并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO) ) 的安全控制。
- [使用AWS Config 开发人员指南中的规则评估资源](#) — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。



- [AWS Security Hub](#)— 这 AWS 服务 提供了您内部安全状态的全面视图 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 [Security Hub 控件参考](#)。
- [Amazon GuardDuty](#) — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务检测您的工作负载、容器和数据面临的潜在威胁。GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- [AWS Audit Manager](#)— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

## Amazon FSx for Windows File Server 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 [AWS 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 AWS 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 AWS 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 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 AWS 账户中的 VPC 之间建立此连接。VPC 也可以位于两个不同的 AWS 区域中。

对等 VPC 之间的流量保留在 AWS 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 AWS Command Line Interface ( AWS 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 AWS 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 AWS 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）AWS 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 AWS 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](#)。

## 限额

接下来，您将了解使用 Amazon FSx for Windows File Server 时的限额。

### 主题

- [您可以增加的限额](#)
- [每个文件系统的资源限额](#)
- [其他注意事项](#)
- [Microsoft Windows 的特有限额](#)

## 您可以增加的限额

以下是您可以提高的每个 AWS 账户、每个 AWS 区域的 Amazon FSx for Windows File Server 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 Amazon FSx for Windows File Server 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 Amazon FSx for Windows File Server 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 Amazon FSx for Windows File Server 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 Amazon FSx for Windows File Server 文件系统的最大用户启动备份数量。 |

### 请求增加限额

1. 打开[服务限额控制台](#)。
2. 在导航窗格中，选择 AWS 服务。
3. 选择 Amazon FSx。
4. 选择一个限额。
5. 选择请求增加限额，然后按照说明请求增加限额。
6. 要查看限额申请的状态，请在控制台导航窗格中选择配额请求历史记录。

有关更多信息，请参阅《服务限额用户指南》中的[请求增加限额](#)。

## 每个文件系统的资源限额

以下是同一 AWS 区域中的 Amazon FSx for Windows File Server 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    |

| 资源                  | 每个文件系统的限额   |
|---------------------|-------------|
| 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 AWS Key Management Service ( AWS 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 AWS 区域 中位置的列表，请参阅《AWS 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。

# Amazon FSx 问题排查

参阅以下部分，帮助排查在使用 Amazon FSx 时遇到的问题。

如果您在使用 Amazon FSx 时遇到下文未列出的问题，请尝试在 [Amazon FSx 论坛](#) 中提问。

## 主题

- [您无法访问您的文件系统](#)
- [创建新的 Amazon FSx 文件系统失败](#)
- [文件系统处于配置错误状态](#)
- [在 FSx for Windows File Server 上使用远程 PowerShell 排查问题](#)
- [您无法在多可用区或单可用区 2 文件系统上配置 DFS-R](#)
- [存储或吞吐能力更新失败](#)
- [恢复备份时将存储类型切换到 HDD 失败](#)
- [卷影副本问题排查](#)
- [文件系统性能问题排查](#)

## 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](#)
- [连接到文件系统弹性网络接口的弹性 IP 地址已删除](#)
- [文件系统安全组缺少所需的入站或出站规则。](#)
- [计算实例的安全组缺少所需的出站规则](#)
- [计算实例未加入 Active Directory](#)
- [文件共享不存在](#)
- [Active Directory 用户缺少所需权限](#)
- [移除了允许完全控制 NTFS ACL 权限](#)
- [无法使用本地客户端访问文件系统](#)
- [新文件系统未在 DNS 中注册](#)
- [无法使用 DNS 别名访问文件系统](#)

- [无法使用 IP 地址访问文件系统](#)

## 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 FSx 弹性网络接口。有关更多信息，请参阅 [使用 Amazon VPC 进行文件系统访问控制](#)。

## 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 会自动分离任何连接到文件系统的弹性网络接口的弹性 IP 地址，该地址是可从互联网访问的公有 IP 地址。有关更多信息，请参阅 [Amazon FSx for Windows File Server 支持的客户端、访问方法和环境](#)。

## 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 AWS Managed Microsoft AD 目录。
- 与 AWS 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 AWS Managed Microsoft AD 目录。另一种类型是 Microsoft Active Directory 目录，该目录与该 AWS 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 AWS Directory Service for Microsoft Active Directory](#)。

## 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 [在 FSx 上管理 Windows File Server 文件系统的文件共享](#)。

## 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 (ACL) 允许需要访问的 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 [在 FSx 上管理 Windows File Server 文件系统的文件共享](#)。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 AWS 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 FSx for 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。有关更多信息，请参阅 [使用备份](#)。

## 新文件系统未在 DNS 中注册

对于加入自行管理的 Active Directory 的文件系统，Amazon FSx 在创建文件系统时并未注册文件系统 DNS，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 Amazon FSx 不会在 DNS 中注册文件系统。您必须为 Amazon FSx 文件系统手动设置 DNS A 条目。对于单可用区 1 文件系统，您需要添加一个 DNS A 条目；对于单可用区 2 和多可用区文件系统，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 <https://console.aws.amazon.com/fsx/> 中，选择要获取 IP 地址的文件系统，以显示文件系统详细信息页面。
2. 在网络与安全选项卡中，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弹性网络接口，打开 Amazon EC2 中的网络接口页面。
- 要使用的单可用区 1 文件系统的 IP 地址显示在主要私有 IPv4 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弹性网络接口，打开 Amazon EC2 中的网络接口页面。
  - 要使用的首选子网的 IP 地址显示在辅助私有 IPv4 IP 列中。
  - 在 Amazon FSx 的备用子网面板中，选择网络接口下显示的弹性网络接口，打开 Amazon EC2 控制台中的网络接口页面。
  - 要使用的备用子网的 IP 地址显示在辅助私有 IPv4 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 [DescribeFileSystemAliases](#) API 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 Amazon FSx 文件系统的 Active Directory 计算机对象上的 DNS 别名相对应的服务主体名称 ( SPN )。

有关更多信息，请参阅 [步骤 2：为 Kerberos 配置服务主体名称 \( SPN \)](#)。

  - 为 DNS 别名创建了 DNS CNAME 记录，将其解析为 Amazon FSx 文件系统的默认 DNS 名称。

有关更多信息，请参阅 [步骤 3：更新或创建文件系统的 DNS CNAME 记录](#)。
4. 如果您创建了有效的 SPN 和 DNS CNAME 记录，请验证客户端的 DNS 是否具有可解析为正确文件系统的 DNS CNAME 记录。

- 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该文件系统，请参阅[您无法访问您的文件系统](#)了解其他问题排查步骤。

## 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 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，你可以在 [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 AWS 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

- [对加入 AWS 托管的 Microsoft Active Directory 的文件系统进行问题排查](#)
- [创建加入自我管理的 Active Directory 的文件系统失败](#)

## 对加入 AWS 托管的 Microsoft Active Directory 的文件系统进行问题排查

阅读以下部分，帮助排查尝试创建加入自行管理的 Active Directory 的 FSx for Windows File Server 文件系统时遇到的问题。

### VPC 安全组和网络 ACL 配置不正确

确保 VPC 安全组和网络 ACL 配置为使用推荐的安全组配置。有关更多信息，请参阅[创建安全组](#)。

## 创建加入自我管理的 Active Directory 的文件系统失败

### 主题

- [文件系统管理员组名重复](#)
- [无法访问 DNS 服务器或域控制器](#)
- [服务账号凭证无效](#)
- [服务账号权限不足](#)
- [服务账户容量已超出](#)
- [Amazon FSx 无法访问组织单位 \(OU\)](#)
- [服务帐号无法访问管理员群组](#)
- [亚马逊 FSx 在域中断了连接](#)
- [服务帐号的权限不正确](#)
- [创建参数中使用的 Unicode 字符](#)

### 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 FSx 之所以没有创建文件系统，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”作为管理员组。如果有多个群组使用默认“域管理员”名称，则请求将失败。

使用以下步骤来解决问题。

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[活动目录的 FSx for Windows File Server 文件系统之前](#)，请使用 [Amazon FSx 活动目录验证工具](#) 验证您的自我管理的活动目录配置。
3. 使用 AWS Management Console 或创建新的文件系统 AWS CLI。有关更多信息，请参阅 [将 Amazon FSx 文件系统加入到自行管理的 Microsoft Active Directory 域](#)。
4. 为文件系统管理员组提供一个名称，该名称在您自行管理的 Active Directory 的域中是唯一的。

## 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. 确认您满足了在创建 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 [使用自行管理的 Microsoft Active Directory 的先决条件](#)。

使用 [Amazon FSx Active 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，则必须确保在 Active Directory 站点中定义了与 Amazon FSx 文件系统关联的 VPC 中的子网，且 VPC 中的子网与您其他站点中的子网之间不存在 IP 冲突。您可以使用 Active Directory Sites and Services MMC 管理单元查看和更改这些设置。

2. 确认您已将 Amazon FSx 文件系统关联的 VPC 安全组以及所有 VPC 网络 ACL 配置为允许所有端口上的出站网络流量。

 Note

如果要实施最低权限，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 Active Directory 域的域控制器上的防火墙规则允许来自 Amazon FSx 文件系统的流量。有关更多信息，请参阅 [Microsoft Active Directory 文档](#)。

## 服务账号凭证无效

创建加入自我管理的 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。

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 [向 Amazon FSx 服务账户委派权限](#)。

## 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 [向 Amazon FSx 服务账户委派权限](#)。

## 服务账户容量已超出

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 [向 Amazon FSx 服务账户委派权限](#)。

## Amazon 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 [向 Amazon FSx 服务账户委派权限](#)。

## 服务帐号无法访问管理员群组

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=FsxAdmins、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 FSx 会尝试使用 Active Directory 域中的 Built-in 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 FSx 在域中断了连接

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.

创建文件系统时，Amazon FSx 能够访问 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 域中。但是，在完成文件系统创建时，Amazon FSx 断开了与域的连接或失去了域成员资格。按照以下步骤排查并解决问题。

1. 确保您的 Amazon FSx 文件系统和 Active Directory 间的网络连接持续存在。同时，使用路由规则、VPC 安全组规则、VPC 网络 ACL 和域控制器防火墙规则，确保它们之间持续允许网络流量通过。
2. 确保 Amazon FSx 为 Active Directory 域中的文件系统创建的计算机对象仍处于活动状态，并且未被删除或以其他方式操纵。

## 服务帐号的权限不正确

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 [向 Amazon FSx 服务账户委派权限](#)。

## 创建参数中使用的 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.
```

Amazon 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。

如果您在使用 Amazon FSx 时遇到此处未列出的问题，请在 [Amazon FSx 论坛](#)上提问或联系 [Amazon Web Services 支持](#)。

## 文件系统处于配置错误状态

由于 Active Directory 环境发生了变化，FSx for Windows File Server 文件系统可能会进入配置错误状态。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。

配置错误状态包含一条错误消息和建议的纠正措施，您可以使用 Amazon FSx 控制台、API 或 AWS CLI 访问这些错误消息和建议的纠正措施。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。

( 有关 Active Directory 要求的完整列表，请参阅[使用自行管理的 Microsoft Active Directory 的先决条件](#)。您还可以使用 [Amazon FSx Active Directory 验证工具](#) 确认您的 Active Directory 环境是否已正确配置为满足这些要求。 )

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 Amazon FSx 控制台、API 或 AWS 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 Amazon 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 Amazon FSx 控制台、API 或 AWS CLI 中使用 StartMisconfiguredStateRecovery 命令。

## 主题

- [文件系统配置错误：Amazon FSx 无法访问 DNS 服务器或域的域控制器。](#)
- [文件系统配置错误：服务账户凭证无效](#)
- [文件系统配置错误：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 DNS 服务器或域的域控制器。

当 Amazon FSx 无法与 Microsoft Active Directory 域控制器或控制器通信时，文件系统将进入 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 FSx Active Directory 验证工具](#) 测试和验证自行管理的 Active Directory 的网络设置。有关更多信息，请参阅 [将 Amazon FSX 与自行管理的 Microsoft Active Directory 结合使用](#)。
3. 在 Amazon FSx 控制台中查看文件系统自行管理的 Active Directory 配置。
4. 要更新文件系统自行管理的 Active Directory 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 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

Amazon FSx 无法与您的 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 [将 Amazon FSX 与自行管理的 Microsoft Active Directory 结合使用](#)。

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. 然后通过 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。

您还可以使用 Amazon 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：提供的服务账户无权将文件系统加入域中

Amazon FSx 无法与您的 Microsoft 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，或者创建具有所需权限的新服务账户。有关此操作的更多信息，请参阅 [向 Amazon FSx 服务账户委派权限](#)。
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。您可以使用 Amazon FSx 控制台更新配置。
  - 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。

您还可以使用 Amazon 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

Amazon FSx 无法与您的 Microsoft 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. 然后通过 Amazon FSx 控制台，使用新的服务账户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。

您还可以使用 Amazon 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

Amazon FSx 无法与您的 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。

您还可以使用 Amazon 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。

## 在 FSx for Windows File Server 上使用远程 PowerShell 排查问题

您可以使用自定义 PowerShell 远程管理命令管理适用于 Windows File Server 文件系统的 FSx。

### 主题

- [New-F SxSmbShare 命令因单向信任而失败](#)
- [您无法使用 Remote 访问您的文件系统 PowerShell](#)

### New-F SxSmbShare 命令因单向信任而失败

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，Amazon FSx 不支持执行该 `New-F SxSmbShare` 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-F SxSmbShare` 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](#)。

### 您无法使用 Remote 访问您的文件系统 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 连接所需的进站规则

文件系统的安全组必须有允许端口 5985 上流量的进站规则，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 AWS 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")
```

## 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 KMS 加密密钥

存储容量增加请求失败，因为 Amazon FSx 无法访问文件系统的 AWS Key Management Service (AWS KMS) 加密密钥。

您需要确保 Amazon FSx 有权访问 AWS 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 密钥已删除，则必须使用新的 KMS 密钥从备份创建新文件系统。有关更多信息，请参阅 [演练 2：从备份创建文件系统](#)。新文件系统可用后，您可以重新尝试请求。
- 如果 KMS 密钥已禁用，请重新启用，然后重新尝试存储容量增加请求。有关更多信息，请参阅《AWS Key Management Service 开发人员指南》中的 [启用和禁用密钥](#)。
- 如果密钥因待删除无效，则必须使用新的 KMS 密钥从备份创建新文件系统。新文件系统可用后，您可以重新尝试请求。有关更多信息，请参阅 [演练 2：从备份创建文件系统](#)。
- 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《AWS 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能力设置为 8 MB/s。

请将文件系统的吞吐能力提高到至少 16 MB/s，然后重试请求。有关更多信息，请参阅 [管理吞吐能力](#)。

## 吞吐能力更新到 8 MB/s 失败

将文件系统的吞吐能力修改为 8 MB/s 的请求失败。

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 MB/s。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。

## 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中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 [还原备份](#)。

## 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](#)
- [我所有的卷影副本都丢失了](#)
- [无法在最近恢复或更新的文件系统上创建 Amazon FSx 备份或访问卷影副本](#)

## 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

文件系统上的 I/O 性能容量不足（例如，因为您使用的是 HDD 存储、HDD 存储容量暴增耗尽或吞吐能力不足）可能会导致 Windows Server 删除所有卷影副本，因为它无法使用可用的 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 Amazon FSx API 切换到使用固态硬盘存储。有关更多信息，请参阅 [管理存储类型](#)。
- 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](#)。

## 无法在最近恢复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 FSx 在最近恢复的文件系统上重建卷影副本状态，并且在重建卷影副本状态时不允许访问卷影副本和备份。

## 文件系统性能问题排查

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启用的任何功能，例如重复数据删除或卷影副本。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

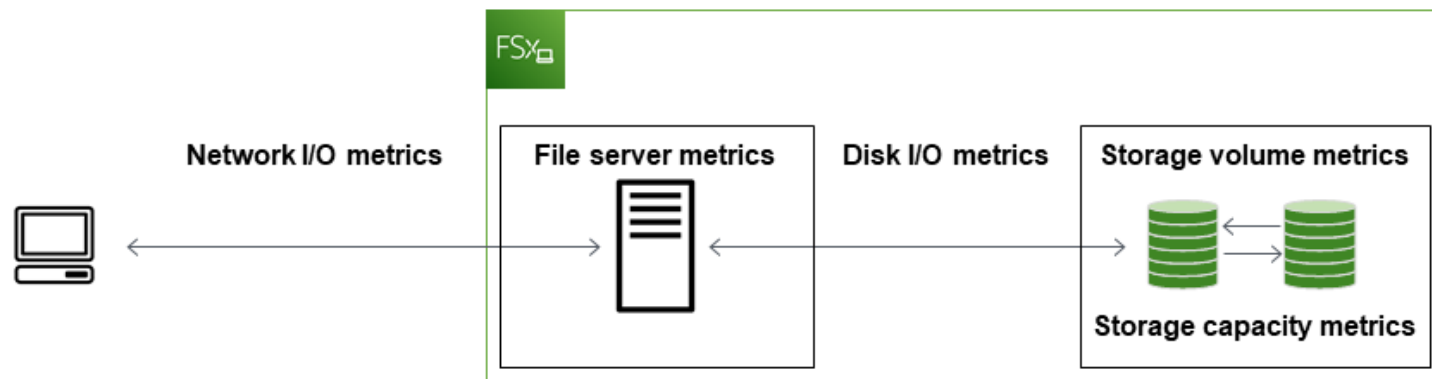
- [如何确定我的文件系统的吞吐量和 IOPS 限制？](#)
- [网络 I/O 和磁盘 I/O 有什么区别？为什么我的网络 I/O 与磁盘 I/O 不同？](#)
- [为什么即使我的网络 I/O 很低，CPU 或内存利用率仍然很高？](#)
- [什么是突增？我的文件系统使用了多少突增？突增点数用完时会发生什么？](#)
- [我在监控和性能页面上看到一条警告，我需要更改文件系统的配置吗？](#)
- [我的指标暂时丢失，我应该担心吗？](#)

## 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 监控指标 CloudWatch](#)。

## 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 [重复数据删除](#)。

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。

## 其他信息

本节提供了对受支持但已弃用的 Amazon FSx 功能的参考。

主题

- [设置自定义备份计划](#)
- [使用 Microsoft 分布式文件系统复制](#)

## 设置自定义备份计划

我们建议 AWS Backup 使用为您的文件系统设置自定义备份计划。如果您需要比使用时更频繁地安排备份，则此处提供的信息仅供参考 AWS Backup。

启用后，Amazon FSx for Windows File Server 将在每日备份时段内每天自动进行一次文件系统备份。Amazon FSx 会根据您为这些自动备份设定的保留期实施保留。它还支持用户启动备份，因此您可以随时进行备份。

接下来，您会发现部署自定义备份计划的资源和配置。自定义备份计划按照您定义的自定义计划在 Amazon FSx 文件系统中执行用户启动备份。例如，可能每六小时一次、每周一次，等等。该脚本还可配置删除超过指定保留期的备份。

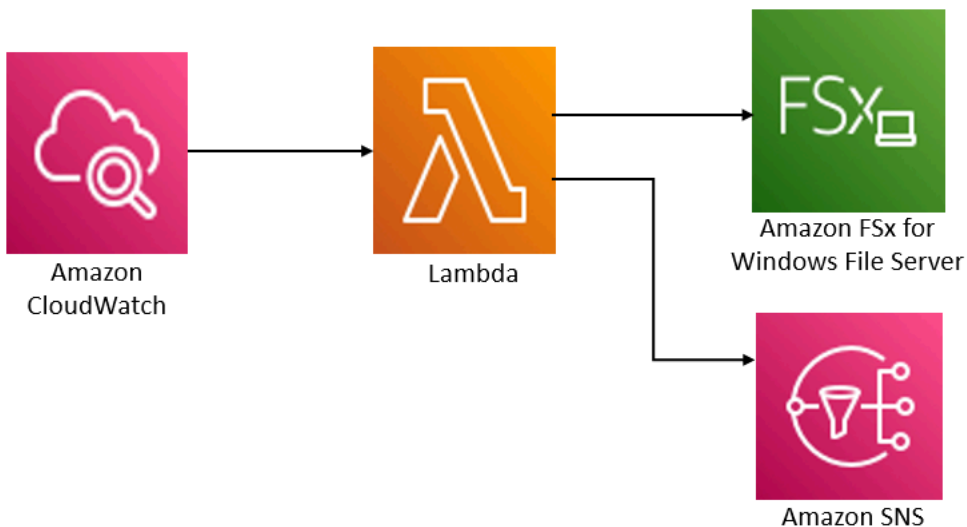
该解决方案会自动部署所需的所有组件，并接受以下参数：

- 文件系统
- 执行备份的 CRON 计划模式
- 备份保留期（以天为单位）
- 备份名称标签

有关 CRON 计划模式的更多信息，请参阅 Amazon CloudWatch 用户指南中的[规则计划表达式](#)。

## 架构概述

部署此解决方案将在 AWS Cloud 中生成以下资源。



该解决方案会执行以下操作：

1. 该 AWS CloudFormation 模板部署了一个 CloudWatch 事件、一个 Lambda 函数、一个 Amazon SNS 队列和一个 IAM 角色。IAM 角色授予 Lambda 函数调用 Amazon FSx API 操作的权限。
2. 在初始部署期间，该 CloudWatch 事件按您定义为 CRON 模式的时间表运行。此事件调用解决方案的备份管理器 Lambda 函数，该函数调用 Amazon FSx CreateBackup API 操作来启动备份。
3. 备份管理器使用 DescribeBackups 检索指定文件系统的现有用户启动备份列表。然后，它会删除超过保留期的备份，保留期是您于初始部署期间指定的。
4. 如果您选择在初始部署期间收到通知的选项，则备份管理器会在成功备份后向 Amazon SNS 队列发送一条通知消息。如果出现故障，系统会发送通知。

## AWS CloudFormation 模板

此解决方案 AWS CloudFormation 用于自动部署 Amazon FSx 自定义备份计划解决方案。要使用此解决方案，请下载 [fsx-schedu](#) AWS CloudFormation led-backup.template 模板。

## 自动部署

以下是配置和部署此自定义备份计划解决方案的过程步骤。部署大约需要五分钟。在开始之前，您的账户中必须有在亚马逊虚拟私有云（亚马逊 VPC）中运行的 Amazon FSx 文件系统的 AWS ID。有关创建这些资源的更多信息，请参阅[开始使用适用于 Windows File Server 的亚马逊 FSx](#)。

**Note**

实施此解决方案会产生相关 AWS 服务的账单。有关更多信息，请参阅有关这些服务的定价详细信息页面。

## 启动自定义备份解决方案堆栈

1. 下载 [fsx-schedu](#) AWS CloudFormation led-backup.template 模板。有关创建 AWS CloudFormation 堆栈的更多信息，请参阅《AWS CloudFormation 用户指南》中的 [在 AWS CloudFormation 控制台上创建堆栈](#)。

**Note**

默认情况下，此模板在美国东部（弗吉尼亚北部）AWS 区域启动。Amazon FSx 目前仅提供特定版本。AWS 区域您必须在可以使用 Amazon FSx 的 AWS 区域启动此解决方案。有关更多信息，请参阅《AWS 一般参考》中的 [AWS 区域和端点](#) 的 Amazon FSx 部分。

2. 对于参数，请查看模板的参数并根据文件系统的需求对其进行修改。该解决方案使用以下默认值。

| 参数                 | 默认值           | 描述                                       |
|--------------------|---------------|------------------------------------------|
| Amazon FSx 文件系统 ID | 无默认值          | 您想要备份的文件系统的文件系统 ID。                      |
| CRON 备份计划模式。       | 0 0/4 * * ? * | 运行 CloudWatch 事件的时间表，触发新的备份并删除保留期之外的旧备份。 |
| 备份保留期（天）           | 30            | 保留用户启动备份的天数。Lambda 函数会删除超过此天数的用户启动备份。    |
| 备份名称               | 用户计划备份        | 这些备份的名称显示在 Amazon FSx 管理控制台的备份名称栏中。      |

| 参数     | 默认值  | 描述                               |
|--------|------|----------------------------------|
| 备份通知   | 是    | 选择是否在成功启动备份时收到通知。如果出现错误，系统会发送通知。 |
| 电子邮件地址 | 无默认值 | 用于订阅 SNS 通知的电子邮件地址。              |

3. 选择下一步。
4. 在选项中，选择下一步。
5. 在审核中，审核并确认设置。必须选择复选框，以确认模板将创建 IAM 资源。
6. 选择创建以部署堆栈。

您可以在 AWS CloudFormation 控制台的“状态”列中查看堆栈的状态。您应该在大约五 ( 5 ) 分钟内看到 CREATE\_COMPLETE 状态。

## 其他选项

您可以使用此解决方案创建的 Lambda 函数对多个 Amazon FSx 文件系统执行自定义计划备份。文件系统 ID 将在事件的输入 JSON 中传递给 Amazon FSx 函数。CloudWatch 传递给 Lambda 函数的默认 JSON 如下所示，其中 FileSystemId 和 SuccessNotification 的值来自启动堆栈时指定的参数。AWS CloudFormation

```
{
 "start-backup": "true",
 "purge-backups": "true",
 "filesystem-id": "${FileSystemId}",
 "notify_on_success": "${SuccessNotification}"
}
```

要为其他 Amazon FSx 文件系统安排备份，请创建另一条 CloudWatch 事件规则。您可以使用 Schedule 事件源执行此操作，并将此解决方案创建的 Lambda 函数作为目标。在配置输入下，选择常量 ( JSON 文本 )。对于 JSON 输入，只需将要备份的 Amazon FSx 文件系统的文件系统 ID 替换为 \${FileSystemId}。另外，将上述 JSON 中的 \${SuccessNotification} 替换为 Yes 或 No。

您手动创建的任何其他 CloudWatch 事件规则都不是 Amazon FSx 自定义计划备份解决方案 AWS CloudFormation 堆栈的一部分。因此，如果您删除堆栈，将不会删除这些规则。



## 使用 Microsoft 分布式文件系统复制

### Note

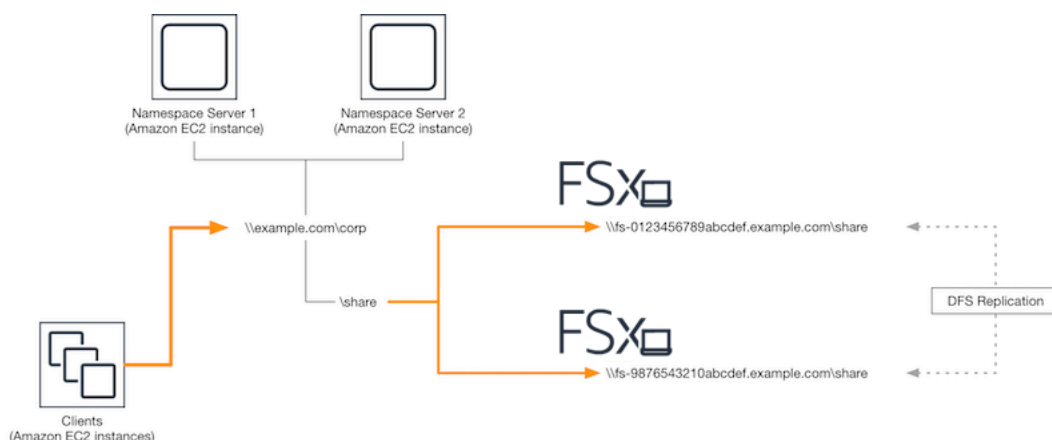
我们建议使用 Amazon FSx 多可用区来实现 FSx for Windows File Server 的高可用性。有关 Amazon FSx 多可用区的更多信息，请参阅[可用性与持久性：单可用区和多可用区文件系统](#)。

Amazon FSx 支持使用 Microsoft 分布式文件系统 (DFS) 进行跨多个可用区 (AZ) 的文件系统部署，以获得多可用区的可用性和持久性。使用 DFS 复制，可以在两个文件系统之间自动复制数据。使用 DFS 命名空间，您可以将一个文件系统配置为主文件系统，将另一个文件系统配置为备用文件系统，如果主文件系统无响应，则可以自动失效转移到备用文件系统。

在使用 DFS 复制之前，请执行以下步骤：

- 按照 Amazon FSx 入门的 [Step 8](#) 中所述设置安全组。
- 在一个区域内的不同可用区中创建两个 Amazon FSx 文件系统。AWS 有关创建文件系统的更多信息，请参阅[将数据写入您的文件共享](#)。
- 确保两个文件系统位于同一个 AWS Directory Service for Microsoft Active Directory 中。
- 创建文件系统后，请记下文件系统的 ID，以供日后使用。

在以下主题中，您将了解如何通过 Amazon FSx 来设置与使用跨可用区的 DFS 命名空间和 DFS 失效转移。



## 设置 DFS 复制

您可以使用 DFS 复制在两个 Amazon FSx 文件系统之间自动复制数据。这种复制是双向的，这意味着您可以写入任一文件系统，更改就会随即复制到另一个文件系统。

### Important

您无法使用 Microsoft Windows 管理工具 (dfsmgmt.msc) 中的 DFS 管理 UI 来配置 FSx for Windows File Server 文件系统上的 DFS 复制。

### 设置 DFS 复制 (脚本化)

1. 启动您的实例并将其连接到您加入 Amazon FSx 文件系统的 Microsoft Active Directory，开始 DFS 管理流程。为此，请从《AWS Directory Service 管理指南》中选择以下过程：
  - [无缝加入 Windows EC2 实例](#)
  - [手动加入 Windows 实例](#)
2. 以文件系统管理员组成员的 Active Directory 用户身份连接到实例。在 AWS 托管 AD 中，此组称为 AWS 委派 FSx 管理员。在您自行管理的 Microsoft AD 中，这个群组被称为“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。

此用户还必须是委派了 DFS 管理权限的组的成员。在 AWS 托管 AD 中，该组称为 AWS 委派分布式文件系统管理员。在您的自行管理的 AD 中，此用户必须是域管理员或您已向其委派 DFS 管理权限的其他组的成员。

有关更多信息，请参阅 Amazon EC2 用户指南中的[连接到您的 Windows 实例](#)。

3. 下载 [fsx-dfs-r-setu PowerShell](#) p.ps1 脚本。
4. 打开“开始”菜单并输入 PowerShell。从列表中选择 Windows PowerShell。
5. 使用以下指定参数运行 PowerShell 脚本，在两个文件系统之间建立 DFS 复制：
  - DFS 复制组和文件夹的名称
  - 您要在文件系统上复制的文件夹的本地路径 (例如 Amazon FSx 文件系统附带的默认共享的 D:\share)
  - 您在先决步骤中创建的主要和备用 Amazon FSx 文件系统的 DNS 名称

## Example

```
FSx-DFSr-Setup.ps1 -group Group -folder Folder -path ContentPath -
primary FSxFileSystem1-DNS-Name -standby FSxFileSystem2-DNS-Name
```

### 设置 DFS 复制 ( 分步教程 )

1. 启动您的实例并将其连接到您加入 Amazon FSx 文件系统的 Microsoft Active Directory，开始 DFS 管理流程。为此，请从《AWS Directory Service 管理指南》中选择以下过程：
  - [无缝加入 Windows EC2 实例](#)
  - [手动加入 Windows 实例](#)
2. 以文件系统管理员组成员的 Active Directory 用户身份连接到实例。在 AWS 托管 AD 中，此组称为 AWS 委派 FSx 管理员。在您自行管理的 Microsoft AD 中，这个群组被称为“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。

此用户还必须是委派了 DFS 管理权限的组的成员。在 AWS 托管 AD 中，该组称为 AWS 委派分布式文件系统管理员。在您的自行管理的 AD 中，此用户必须是域管理员或您已向其委派 DFS 管理权限的其他组的成员。

有关更多信息，请参阅 Amazon EC2 用户指南中的[连接到您的 Windows 实例](#)。

3. 打开“开始”菜单并输入 PowerShell。从列表中选择 Windows PowerShell。
4. 如果您的实例上尚未安装 DFS 管理工具，请使用以下命令进行安装。

```
Install-WindowsFeature RSAT-DFS-Mgmt-Con
```

5. 在 PowerShell 提示符下，使用以下命令创建 DFS 复制组和文件夹。

```
$Group = "Name of the DFS Replication group"
$Folder = "Name of the DFS Replication folder"

New-DfsReplicationGroup -GroupName $Group
New-DfsReplicatedFolder -GroupName $Group -FolderName $Folder
```

6. 使用以下命令确定与各个文件系统关联的 Active Directory 计算机名称。

```
$Primary = "DNS name of the primary FSx file system"
```

```
$Standby = "DNS name of the standby FSx file system"
```

```
$C1 = (Get-ADObject -Filter "objectClass -eq 'Computer' -and ServicePrincipalName -eq 'HOST/$Primary']").Name
```

```
$C2 = (Get-ADObject -Filter "objectClass -eq 'Computer' -and ServicePrincipalName -eq 'HOST/$Standby']").Name
```

7. 将您的文件系统添加为使用以下命令创建的 DFS 复制组的成员。

```
Add-DfsrMember -GroupName $Group -ComputerName $C1
```

```
Add-DfsrMember -GroupName $Group -ComputerName $C2
```

8. 使用以下命令将每个文件系统的本地路径 (例如 D:\share) 添加到 DFS 复制组。在此过程中, 由 *file system 1* 作为主要成员, 这意味着其内容会被最先同步到另一个文件系统。

```
$ContentPath1 = "Local path to the folder you want to replicate on file system 1"
```

```
$ContentPath2 = "Local path to the folder you want to replicate on file system 2"
```

```
Set-DfsrMembership -GroupName $Group -FolderName $Folder -ContentPath $ContentPath1
-ComputerName $C1 -PrimaryMember $True
```

```
Set-DfsrMembership -GroupName $Group -FolderName $Folder -ContentPath $ContentPath2
-ComputerName $C2 -PrimaryMember $False
```

9. 使用以下命令在文件系统之间添加连接。

```
Add-DfsrConnection -GroupName $Group -SourceComputerName $C1 -
DestinationComputerName $C2
```

几分钟之内, 两个文件系统都应开始同步之前 ContentPath 指定的内容。

## 为失效转移设置 DFS 命名空间

您可以使用 DFS 命名空间将一个文件系统设置为主文件系统, 将另一个文件系统设置为备用文件系统。由此, 您可以配置在主服务器无响应时自动失效转移到备用服务器。使用 DFS 命名空间, 您可以将不同服务器上的共享文件夹分组到一个命名空间, 此命名空间中的单个文件夹路径可以将文件存储在多个服务器上。DFS 命名空间由 DFS 命名空间服务器管理, 这些服务器会将映射 DFS 命名空间文件夹的计算实例定向到相应的文件服务器。

## 为失效转移设置 DFS 命名空间 ( UI )

1. 如果您尚未运行 DFS 命名空间服务器，请使用 [setu](#) AWS CloudFormation p-dfsn-Servers.Template 模板启动一对高度可用的 DFS 命名空间服务器。有关创建 AWS CloudFormation 堆栈的更多信息，请参阅《AWS CloudFormation 用户指南》中的 [在 AWS CloudFormation 控制台上创建堆栈](#)。
2. 以“AWS 委派管理员”组中的用户身份连接到在上一步中启动的 DFS 命名空间服务器之一。有关更多信息，请参阅 Amazon EC2 用户指南中的 [连接到您的 Windows 实例](#)。
3. 打开 DFS Management 控制台。打开开始菜单，运行 `dfsmanagement.msc`。此操作将打开 DFS Management GUI 工具。
4. 在操作中，选择新命名空间，然后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 Namespace server 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. 选择添加，在路径中输入主 Amazon FSx 文件系统上的文件共享的 UNC 名称（例如 `\fs-0123456789abcdef0.example.com\share`）作为文件夹目标，然后选择确定。
13. 选择添加，在路径中输入备用 Amazon FSx 文件系统上的文件共享的 UNC 名称（例如 `\fs-fedbca9876543210f.example.com\share`）作为文件夹目标，然后选择确定。
14. 在新文件夹窗口中，选择确定。新文件夹是使用命名空间的两个文件夹目标创建的。
15. 对要添加到命名空间中的每个文件共享重复操作最后三个步骤。

## 设置 DFS 命名空间以进行故障转移 () PowerShell

1. 如果您尚未运行 DFS 命名空间服务器，请使用 [setu](#) AWS CloudFormation p-dfsn-Servers.Template 模板启动一对高度可用的 DFS 命名空间服务器。有关创建 AWS CloudFormation 堆栈的更多信息，请参阅《AWS CloudFormation 用户指南》中的[在 AWS CloudFormation 控制台上创建堆栈](#)。
2. 以 AWS 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。有关更多信息，请参阅 Amazon EC2 用户指南中的[连接到您的 Windows 实例](#)。
3. 打开“开始”菜单并输入PowerShell。Windows PowerShell 出现在匹配项列表中。
4. 打开 Windows 的上下文 ( 右键单击 ) 菜单， PowerShell然后选择“以管理员身份运行”。
5. 如果您的实例上尚未安装 DFS 管理工具，请使用以下命令进行安装。

```
Install-WindowsFeature RSAT-DFS-Mgmt-Con
```

6. 如果您还没有现有 DFS 命名空间，则可以使用以下 PowerShell 命令创建一个命名空间。

```
$NSS1 = computer name of the 1st DFS Namespace server
$NSS2 = computer name of the 2nd DFS Namespace server

$DNSRoot = fully qualified Active Directory domain name (e.g. mydomain.com)
$Namespace = Namespace name you want to use
$Folder = Folder path you want to use within the Namespace
$FS1FolderTarget = Share path to Folder Target on File System 1
$FS2FolderTarget = Share path to Folder Target on File System 2

$NSS1,$NSS2 | ForEach-Object { Invoke-Command -ComputerName $_ -ScriptBlock { mkdir
 "C:\DFS\${using:Namespace}";
 New-SmbShare -Name ${using:Namespace} -Path "C:\DFS\${using:Namespace}" } }

New-DfsnRoot -Path "\\${DNSRoot}\${Namespace}" -TargetPath "\\${NSS1}.${DNSRoot}\
 ${Namespace}" -Type DomainV2
New-DfsnRootTarget -Path "\\${DNSRoot}\${Namespace}" -TargetPath "\\${NSS2}.
 ${DNSRoot}\${Namespace}"
```

7. 要在 DFS 命名空间中创建文件夹，可以使用以下 PowerShell命令。此操作将创建一个文件夹，该文件夹会默认将访问此文件夹的计算实例定向到您的主 Amazon FSx 文件系统。

```
$FS1 = DNS name of primary FSx file system
New-DfsnFolder -Path "\\${DNSRoot}\${Namespace}\${Folder}" -TargetPath "\\${FS1}\
 ${FS1FolderTarget}" -EnableTargetFailback $True -ReferralPriorityClass GlobalHigh
```

- 将您的备用 Amazon FSx 文件系统添加到同一 DFS 命名空间文件夹。如果访问该文件夹的计算实例无法连接到主 Amazon FSx 文件系统，则它们会回退到该文件系统。

```
$FS2 = DNS name of secondary FSx file system
New-DfsnFolderTarget -Path "\\${DNSRoot}\${Namespace}\${Folder}" -TargetPath "\\${FS2}\${FS2FolderTarget}"
```

现在，您可以使用先前指定的 DFS 命名空间文件夹的远程路径从计算实例访问数据。此操作会将计算实例定向到主 Amazon FSx 文件系统（如果主文件系统没有响应，则定向到备用文件系统）。

例如，打开开始菜单，输入 PowerShell。从列表中选择 Windows PowerShell 并运行以下命令。

```
net use Z: \\${DNSRoot}\${Namespace}\${Folder} /persistent:yes
```

## 使用维护时段和 FSx 多可用区

为了帮助确保多可用区文件系统部署的高可用性，我们建议多可用区部署中的两个 Amazon FSx 文件系统选择不重叠的维护时段。这样做有助于确保在系统维护时段内，应用程序和用户能够继续使用您的文件数据。

### Note

要允许进出文件系统的 DFS 复制流量，请确保如 [Amazon VPC 安全组](#) 中所述添加 VPC 安全组入站和出站规则。

## 文档历史记录

- API 版本 : 2018-03-01
- 最新文档更新 : 2024 年 1 月 17 日

下表介绍了《Amazon 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              |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <a href="#">在吞吐量为 4 Gb/s 及更高的文件系统上增加了对更高 IOPS 级别的支持</a>                                                                                                                   | for Windows File Server for File Server 将吞吐容量为 4 Gb/s 或更高的文件系统的最大 IOPS 从 130K 提高到 150K，吞吐容量为 6 Gb/s 或更高的文件系统从 17.5K 提高到 200 万，吞吐容量为 9 Gb/s 或更高的文件系统从 35 万提高到 400K，吞吐量为 12 Gb/s 的文件系统从 35 万提高到 400K 的吞吐容量或更高。有关更多信息，请参阅 <a href="#">FSx for Windows File Server 性能</a> 。 | 2024 年 1 月 17 日 |
| <a href="#">亚马逊 FSx 更新了 AmazonF、AmazonFSxFullAccess、AmazonFSxConsoleFullAccess、AmazonF 和 AmazonFSxReadOnlyAccess 托管策略 SxConsoleReadOnlyAccess SxServiceRolePolicy AWS</a> | 亚马逊 FSx 更新了 AmazonF、AmazonFSxFullAccess、AmazonFSxConsoleFullAccess、AmazonFSxReadOnlyAccess 和 AmazonFSxConsoleReadOnlyAccess 政策以添加权限 SxServiceRolePolicy。ec2:GetSecurityGroupsForVpc 有关更多信息，请参阅 <a href="#">Amazon</a>                                                   | 2024 年 1 月 9 日  |



|                                                                                  |                                                                                                                                                                                                  |                  |
|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| <a href="#">亚马逊 FSx 更新了 AmazonFSxFullAccess 和 AmazonFSxConsoleFullAccess AWS</a> | 亚马逊 FSx 更新了 AmazonFSxFullAccess 和 AmazonFSxConsoleFullAccess 政策以添加该操作。ManageCrossAccountDataReplication 有关更多信息，请参阅 <a href="#">Amazon FSx 对 AWS 托管策略的更新</a> 。                                    | 2023 年 12 月 20 日 |
| <a href="#">亚马逊 FSx 更新了 AmazonFSxFullAccess 和 AmazonFSxConsoleFullAccess AWS</a> | 亚马逊 FSx 更新了 AmazonFSxFullAccess 和 AmazonFSxConsoleFullAccess 政策以添加权限。fsx:CopySnapshotAndUpdateVolume 有关更多信息，请参阅 <a href="#">Amazon FSx 对 AWS 托管策略的更新</a> 。                                       | 2023 年 11 月 26 日 |
| <a href="#">亚马逊 FSx 更新了 AmazonFSxFullAccess 和 AmazonFSxConsoleFullAccess AWS</a> | 亚马逊 FSx 更新了 AmazonFSxFullAccess 和 AmazonFSxConsoleFullAccess 政策，添加了和权限。fsx:DescribeSharedVPCConfiguration fsx:UpdateSharedVPCConfiguration 有关更多信息，请参阅 <a href="#">Amazon FSx 对 AWS 托管策略的更新</a> 。 | 2023 年 11 月 14 日 |
| <a href="#">添加了对更新文件系统存储类型的支持</a>                                                | FSx for Windows File Server 文件系统现在支持从 HDD 存储类型更新到 SSD 存储类型。有关更多信息，请参阅 <a href="#">管理存储类型</a> 。                                                                                                   | 2023 年 8 月 9 日   |

|                                                                  |                                                                                                                                 |                 |
|------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <a href="#">添加了对提高最大吞吐能力的支持</a>                                  | FSx for Windows File Server 文件系统现在支持高达 12 GBps 的吞吐能力。有关更多信息，请参阅 <a href="#">FSx for Windows File Server 性能</a> 。                | 2023 年 8 月 9 日  |
| <a href="#">添加了对 SSD IOPS 预置的支持</a>                              | FSx for Windows File Server 文件系统现在支持独立于存储容量预置 SSD IOPS，最高可达 350,000 IOPS。有关更多信息，请参阅 <a href="#">管理 SSD IOPS</a> 。               | 2023 年 8 月 9 日  |
| <a href="#">亚马逊 FSx 更新了 AmazonF 托管策略 SxServiceRolePolicy AWS</a> | 亚马逊 FSx 更新了 Amazon cloudwatch:PutMetricData F 中的权限。SxServiceRolePolicy 有关更多信息，请参阅 <a href="#">AmazonF SxServiceRolePolicy</a> 。 | 2023 年 7 月 24 日 |
| <a href="#">亚马逊 FSx 更新了 AmazonF 托管策略 SxFullAccess AWS</a>        | 亚马逊 FSx 更新了 AmazonF SxFullAccess 政策，删除了 fsx:* 权限并添加了具体操作。fsx 有关更多信息，请参阅 <a href="#">AmazonF SxFullAccess</a> 政策。                | 2023 年 7 月 13 日 |
| <a href="#">亚马逊 FSx 更新了 AmazonF 托管策略 SxConsoleFullAccess AWS</a> | 亚马逊 FSx 更新了 AmazonF SxConsoleFullAccess 政策，删除了 fsx:* 权限并添加了具体操作。fsx 有关更多信息，请参阅 <a href="#">AmazonF SxConsole FullAccess</a> 政策。 | 2023 年 7 月 13 日 |

[增加了对适用于 Windows File Server 的亚马逊 FSx 新 CloudWatch 指标的支持](#)

FSx for Windows File Server 现在提供了 CloudWatch 其他指标，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](#)

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 FSx 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](#)

适用于 FSx for Windows File Server 文件系统的 Amazon 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 AWS PrivateLink 接口 VPC 终端节点添加了 Support。](#)

现在可以使用接口 VPC 端点从 VPC 访问 Amazon FSx API，而无需通过互联网发送流量。有关更多信息，请参阅[Amazon FSx 和接口 VPC 端点](#)。

2022 年 4 月 5 日

### [添加了对 Amazon Kendra 的支持](#)

现在，您可以将 FSx for Windows File Server 文件系统用作 Amazon Kendra 的数据源，从而索引和搜索存储在文件系统的文档中包含的信息。有关更多信息，请参阅 [FSx for Windows File Server 与 Amazon Kendra 结合使用](#)。

2022 年 3 月 26 日

### [添加了对文件访问审计的支持](#)

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 FSx 将同一 AWS 账户内的备份复制到另一个账户 AWS 区域（跨区域副本）或同一账户内的备份 AWS 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 AWS 开发的自定义 AWS 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 for Windows File Server 文件系统。有关更多信息，请参阅[支持的环境](#)。您可以将 FSx for Windows File Server 文件系统加入到带有使用非私有 IP 地址的 DNS 服务器和 AD 域控制器的自行管理的 Microsoft Active Directory 中。有关更多信息，请参阅[结合使用 Amazon FSx 与自行管理的 Microsoft Active Directory](#)。

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 FSx for Windows File Server 文件系统关联起来，以便使用这些别名访问文件系统上的数据。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](#)

您现在可以结合使用 FSx for Windows File Server 与 Amazon EC2。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 AWS Backup](#)

现在，除了使用原 AWS Backup 生 Amazon FSx 备份外，您还可以使用备份和恢复 FSx 文件系统。有关更多信息，请参阅[结合使用 AWS Backup 与 Amazon FSx](#)。

2020 年 11 月 9 日

|                                                                        |                                                                                                                                                     |                  |
|------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| <a href="#">添加了对吞吐能力扩展的支持</a>                                          | 现在，您可以随着吞吐量要求的变化修改现有 FSx for Windows File Server 文件系统的吞吐能力。有关更多信息，请参阅 <a href="#">管理吞吐能力</a> 。                                                      | 2020 年 6 月 1 日   |
| <a href="#">添加了对存储容量扩展的支持</a>                                          | 现在，您可以随着存储要求的变化增加现有 FSx for Windows File Server 文件系统的存储容量。有关更多信息，请参阅 <a href="#">管理存储容量</a> 。                                                       | 2020 年 6 月 1 日   |
| <a href="#">添加了对硬盘驱动器 (HDD) 存储的支持</a>                                  | 使用 FSx for Windows File Server 时，HDD 存储可灵活调整价格和性能。有关更多信息，请参阅 <a href="#">使用 Amazon FSx 优化成本</a> 。                                                   | 2020 年 3 月 26 日  |
| <a href="#">添加了对 Support 对使用文件传输的支持 AWS DataSync</a>                   | 现在，你可以使用 AWS DataSync 在 FSx for Windows File Server 之间来回传输文件。有关更多信息，请参阅 <a href="#">使用将文件迁移到适用于 Windows File Server AWS DataSync 的 Amazon FSx</a> 。 | 2020 年 2 月 4 日   |
| <a href="#">FSx for Windows File Server 发布了对其他 Windows 文件系统管理任务的支持</a> | 现在，您可以使用用于远程 PowerShell 管理的 Amazon FSx CLI 管理和文件共享、重复数据删除、存储配额和文件共享传输中的加密。有关更多信息，请参阅 <a href="#">管理文件系统</a> 。                                       | 2019 年 11 月 20 日 |

[FSx for Windows File Server 发布了对原生多可用区的支持](#)

您可以使用 FSx for Windows File Server 的多可用区部署，更轻松地创建跨多个可用区（AZ）的高可用性文件系统。有关更多信息，请参阅[可用性与持久性：单可用区和多可用区文件系统](#)。

2019 年 11 月 20 日

[FSx for Windows File Server 发布了对管理用户会话和打开的文件的支持](#)

现在，您可以使用 Microsoft Windows 的共享文件夹原生工具管理 FSx for Windows File Server 文件系统上的用户会话和打开的文件。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

[Amazon FSx 发布了对 Microsoft Windows 影子副本的支持](#)

现在，您可以在 FSx for Windows File Server 文件系统中配置 Windows 影子副本。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

[Amazon FSx 发布了对共享的 Microsoft Active Directory 的支持](#)

现在，您可以将 FSx for Windows File Server 文件系统加入 AWS Managed Microsoft AD 到位于不同 VPC 或与文件系统 AWS 账户不同的目录中。有关更多信息，请参阅[Active Directory 支持](#)。

2019 年 6 月 25 日

### [Amazon FSx 发布了对增强型 Microsoft Active Directory 的支持](#)

现在，您可以将 FSx for Windows File Server 文件系统加入您在本地或云端自行管理的 Microsoft Active Directory 域。有关更多信息，请参阅 [Active Directory 支持](#)。

2019 年 6 月 24 日

### [Amazon FSx 符合 SOC 认证](#)

Amazon FSx 已通过评估，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 AWS 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 Amazon FSx 文件系统可通过 VPN 和区域间 VPC 对等互连进行 AWS 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 AWS Direct Connect、VPN 和区域间 VPC 对等连接支持](#)

现在，您可以通过本地资源和其他 Amazon VPC 或 AWS 账户中的资源访问 Amazon FSx for Windows File Server 文件系统。有关更多信息，请参阅 [支持的访问方法](#)。

2019 年 2 月 22 日

### [Amazon FSx 现已正式发布](#)

Amazon FSx for Windows File Server 提供完全托管式的 Microsoft Windows 文件服务器，由完全原生的 Windows 文件系统提供支持。Amazon FSx for Windows File Server 的功能、性能和兼容性可轻松实现将企业应用程序直接迁移至 AWS。

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。