aws

Amazon FSx 文件网关用户指南

AWS Storage Gatewa

API 版本 2021-03-31

AWS Storage Gatewa: Amazon FSx 文件网关用户指南

Table of Contents

..... x
什么是 Amazon FSx 文件网关 1
FSx 文件网关的工作原理 1
入门 AWS Storage Gateway 3
注册 Amazon Web Services 3
创建具有管理员权限的 IAM 用户 4
正在访问 AWS Storage Gateway 5
AWS 区域 支持 Storage Gateway 5
文件网关设置要求 7
先决条件 7
硬件和存储要求 7
本地部署的硬件要求 VMs 8
对 Amazon EC2 实例类型的要求 8
存储需求 9
网络和防火墙要求 9
端口要求 10
硬件设备的网络和防火墙要求 19
允许通过防火墙和路由器进行网关访问 22
配置安全组 23
受支持的管理程序和主机要求 24
文件网关支持的 SMB 客户端 25
受支持的文件系统操作 25
管理本地磁盘 25
确定本地磁盘存储量 26
添加缓存存储 26
将临时存储与 EC2 网关结合使用 27
使用硬件设备 29
设置硬件设备 30
物理安装硬件设备 31
访问硬件设备控制台 33
配置硬件设备网络参数 34
激活硬件设备 35
在硬件设备上创建网关 36
在硬件设备上配置网关 IP 地址 37

从硬件设备中移除网关软件 39
删除硬件设备 40
创建网关 41
概述 - 网关激活 41
设置网关 41
连接到 AWS 41
检查并激活 42
概述 - 网关配置 42
概述 - 存储资源 42
创建 FSx 适用于 Windows 的 Amazon 文件服务器文件系统 42
创建并激活 Amazon FSx 文件网关 43
设置 Amazon FSx 文件网关 43
将您的 Amazon FSx 文件网关连接到 AWS 44
查看设置并激活您的 Amazon FSx 文件网关 45
配置您的 Amazon FSx 文件网关 46
在 VPC 中激活网关 48
为 Storage Gateway 创建 VPC 端点 49
配置 Microsoft Active Directory 域访问设置 51
附上 Amazon FSx 文件系统 53
挂载并使用您的 Amazon FSx 文件共享 56
在客户端上挂载您的 SMB 文件共享 56
测试您的 FSx 文件网关 57
管理您的 Amazon FSx 文件网关资源 59
网关状态 59
了解文件系统状态 60
编辑基本网关信息 60
设置网关安全级别 61
编辑 FSx 文件网关的活动目录设置 62
编辑 Amazon FSx 文件系统的设置 63
断开 Amazon FSx 文件系统 64
监控 Storage Gateway 66
了解 CloudWatch 警报 66
创建推荐的 CloudWatch 警报 68
创建自定义 CloudWatch警报 68
监控您的 文件网关 70
获取 文件网关运行状况日志 70

使用亚马逊 CloudWatch 指标 71
了解网关指标 72
了解文件系统指标 77
了解 关审核日志 79
维护网关 84
管理网关更新 84
更新频率和预期行为 85
开启或关闭维护更新 85
修改网关维护时段计划 86
手动应用更新 87
使用本地控制台执行维护任务 88
访问网关本地控制台 88
在虚拟机本地控制台上执行任务 91
在 EC2 本地控制台上执行任务 103
关闭网关虚拟机 109
用新实例替换现有文件网关 109
删除网关和移除资源 111
使用 Storage Gateway 控制台删除网关 111
性能和优化 113
的基本性能指南 113
FSx Windows 客户端上的文件网关性能 114
优化网关性能 114
在网关中添加资源 114
向应用程序环境添加资源 116
更大限度地提高 S3 文件网关吞吐量 116
将网关部署在与客户端相同的位置 117
减少磁盘速度慢引起的瓶颈 117
调整 CPU、RAM 和缓存磁盘的虚拟机资源分配 118
调整 SMB 安全级别 119
使用多个线程和客户端来并行执行写入操作 120
关闭自动缓存刷新 122
增加 Amazon S3 上传程序线程数 122
增大 SMB 超时设置 123
为兼容的应用程序开启操作锁定 123
根据工作文件集的大小调整网关容量 123
为更大的工作负载部署多个网关 124

为 SQL Server 数据库备份优化 S3 文件网关 124
将网关部署在与 SQL Server 相同的位置 125
减少磁盘速度慢引起的瓶颈 125
调整 S3 文件网关虚拟机的 CPU、RAM 和缓存磁盘资源分配 126
通过调整 S3 文件网关的安全级别来提高 SMB 客户端吞吐量 127
通过将 SQL 备份拆分为多个文件来提高 SMB 客户端吞吐量 128
通过增大 SMB 超时设置来防止大文件复制失败 129
增加 Amazon S3 上传程序线程数 129
关闭自动缓存刷新 129
部署多个网关以支持工作负载 130
用于数据库备份工作负载的其他资源 130
安全性 131
数据保护 131
数据加密 132
Identity and access management 133
受众 133
使用身份进行身份验证 133
使用策略管理访问 135
Stor AWS age Gateway 如何与 IAM 协作 136
基于身份的策略示例 140
问题排查 143
使用标签控制对 资源的访问 145
合规性验证 147
恢复能力 148
基础结构安全性 148
AWS 安全最佳实践 149
日志记录和监控 149
Storage Gateway 信息位于 CloudTrail 149
了解 Storage Gateway 日志文件条目 150
问题排查 153
故障排除：网关离线问题 153
检查关联的防火墙或代理 154
检查是否正在对网关的流量进行 SSL 检查或深度数据包检查 154
在重新启动或软件更新后检查 IOWait百分比指标 154
检查虚拟机监控程序主机上是否出现停电或硬件故障 154
检查关联的缓存磁盘是否有问题 154

故障排除：Active Directory 问题 155
通过运行 nping 测试来确认网关可以访问域控制器 155
检查 Amazon EC2 网关实例 VPC 的 DHCP 选项集 156
通过运行 dig 查询来确认网关可以解析域 156
检查域控制器设置和角色 157
检查网关是否已加入最近的域控制器 157
确认 Active Directory 在默认组织单元（OU）中创建了新的计算机对象 158
查看域控制器事件日志 158
故障排除：网关激活问题 158
解决使用公有端点激活网关时出现的错误 159
解决使用 Amazon VPC 端点激活网关时出现的错误 162
解决使用公有端点激活网关且同一 VPC 中有 Storage Gateway VPC 端点时出现的错误 165
故障排除：本地网关问题 166
开启 支持 访问权限以帮助排除网关故障 168
故障排除：Microsoft Hyper-V 设置问题 169
故障排除：Amazon EC2 网关问题 172
过了一会儿网关并未激活 172
在实例列表中找不到 EC2 网关实例 173
使用串行控制台连接到 Amazon EC2 网关 173
开启 支持 访问权限以帮助排除网关故障 173
故障排除：硬件设备问题 175
如何确定服务 IP 地址 175
如何执行出厂重置 175
如何执行远程重启 175
如何获得 Dell iDRAC 支持 176
如何找到硬件设备序列号 176
如何获得硬件设备支持 176
故障排除：文件网关问题 177
错误： FileMissing 177
错误： FsxFileSystemAuthenticationFailure 178
错误： FsxFileSystemConnectionFailure 178
错误： FsxFileSystemFull 178
错误： GatewayClockOutOfSync 178
错误： InvalidFileState 179
错误： ObjectMissing 179
错误： DroppedNotifications 180

通知： HardReboot 180
通知：重启 180
排查 Active Directory 域问题 181
使用 CloudWatch 指标进行故障排除 182
高可用性运行状况通知 184
故障排除：高可用性问题 184
运行状况通知 185
指标 186
最佳实践 187
恢复数据 187
从虚拟机意外关闭中恢复 187
从出现故障的缓存磁盘恢复数据 187
从不可访问的数据中心恢复数据 188
在 Amazon 上恢复数据 FSx 188
清理不必要的资源 189
其他资源 190
主机设置 190
为文件网关部署默认 Amazon EC2 主机 191
为文件网关部署自定义的 Amazon EC2 主机 193
修改 Amazon EC2 实例元数据选项 196
将 VM 时间与 Hyper-V 或 Linux KVM 主机时间同步 196
将 VM 时间与 VMware 主机时间同步 197
为网关配置网络适配器 198
使用 Storage Gateway 和 VMware HA 200
获取激活密钥 204
Linux (curl) 205
Linux (bash/zsh) 206
微软 Windows PowerShell 206
使用本地控制台 207
使用 Direct Connect 207
Active Directory 权限 208
获取网关 IP 地址 209
从 Amazon EC2 主机获取 IP 地址 209
了解资源和资源 IDs 210
使用资源 IDs 210
标记您的资源 211

使用标签 211
开源组件 213
Storage Gateway 的开源组件 213
Amazon FSx 文件网关的开源组件 213
配额 214
Amazon FSx 文件系统的配额 214
为网关建议的本地磁盘大小 214
API 参考 216
必需的请求标头 216
对请求进行签名 218
签名计算示例 219
错误响应 220
异常 221
操作错误代码 223
错误响应 242
操作 244
文档历史记录 245
早期更新 252

Amazon FSx 文件网关不再向新客户开放。 FSx File Gateway 的现有客户可以继续正常使用该服务。有关与 FSx 文件网关类似的功能，请访问此博客文章。

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。

什么是 Amazon FSx 文件网关

Amazon FSx 文件网关（FSx 文件网关）是一种新的文件网关类型，从本地设施提供云内适用于 Windows File Server 的 FSx 文件共享的低延迟和高效访问。如果由于延迟或带宽要求而保持本地部署文件存储，则可以改为使用 FSx 文件网关，以无缝访问由适用于 Windows File Server 的 FSx 在 AWS 云中提供的完全托管式、高度可靠且几乎不受限制的 Windows 文件共享。

使用 Amazon FSx 文件网关的好处

FSx 文件网关提供以下好处：

- 帮助消除本地文件服务器并将所有数据整合到 AWS 中，以利用云存储的规模和经济性。
- 提供可用于所有文件工作负载的选项，包括需要在本地访问云数据的工作负载。
- 需要驻留在本地的应用程序现在可以体验与其在 AWS 中相同的低延迟和高性能，而不会给您的网络带来负担，也不会影响要求最苛刻的应用程序所经历的延迟。

Amazon FSx 文件网关的工作原理

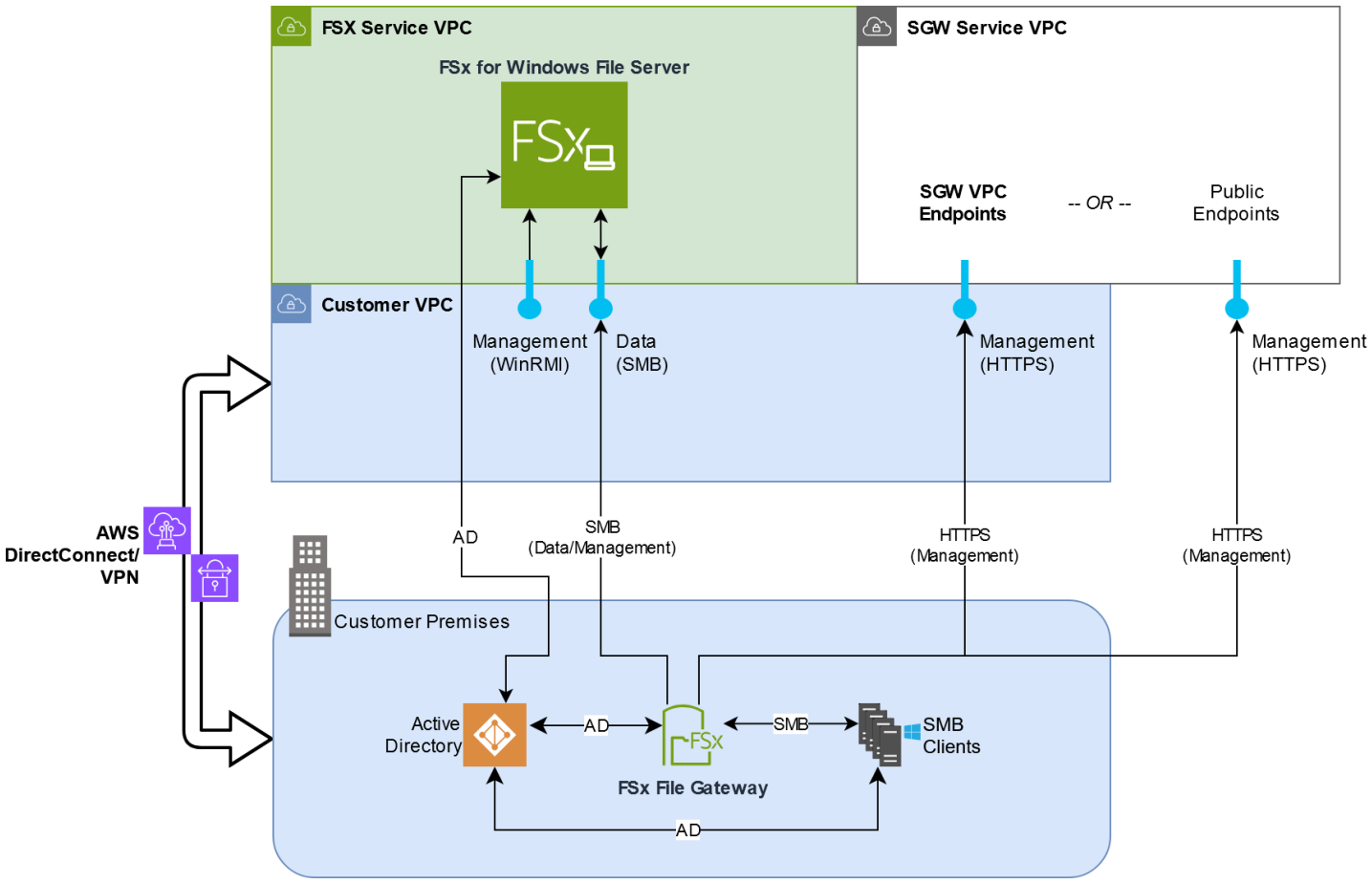
要使用 Amazon FSx 文件网关（FSx 文件网关），必须至少有一个适用于 Windows File Server 的 Amazon FSx 文件系统。您还必须通过 VPN 或通过 Direct Connect 连接在本地访问适用于 Windows File Server 的 FSx。有关使用 Amazon FSx 文件系统的更多信息，请参阅什么是适用于 Windows File Server 的 Amazon FSx？

您可以将网关作为在 VMware ESXi、Microsoft Hyper-V 或基于 Linux 内核的虚拟机（KVM）上运行的虚拟机（VM），或者作为从首选经销商处订购的硬件设备部署到本地环境中。您也可以在 VMware Cloud on AWS 中部署 Storage Gateway 虚拟机，或者在 Amazon EC2 中作为 AMI 部署。部署设备后，您可以从 Storage Gateway 控制台或通过 Storage Gateway API 激活 FSx 文件网关。

激活 Amazon FSx 文件网关并且可以访问适用于 Windows File Server 的 FSx 后，使用 Storage Gateway 控制台将其加入您的 Microsoft Active Directory 域。网关成功加入域后，您可以使用 Storage Gateway 控制台将网关连接到现有适用于 Windows File Server 的 FSx。适用于 Windows File Server 的 FSx 使服务器上的所有共享都作为共享在 Amazon FSx 文件网关上使用。然后，您可以使用客户端浏览并连接到 FSx 文件网关上与所选 FSx 文件网关相对应的文件共享。

连接文件共享后，您可以在本地读取和写入文件，同时利用适用于 Windows File Server 的 FSx 上提供的所有功能。FSx 文件网关将本地文件共享及其内容映射到远程存储在适用于 Windows File Server 的 FSx 中的文件共享。远程文件和本地可见文件与其共享文件之间存在 1:1 对应关系。

下图概述了 Storage Gateway 的文件存储部署。



注意图中的以下内容：

- 需要Direct Connect 或 VPN，才能允许 FSx 文件网关使用 SMB 访问 Amazon FSx 文件共享，以及允许适用于 Windows File Server 的 FSx 加入您的本地 Active Directory 域。
- 需要 Amazon Virtual Private Cloud（Amazon VPC）才能使用私有端点连接到适用于 Windows File Server 的 FSx 服务 VPC 和 Storage Gateway 服务 VPC。FSx 文件网关也可以连接到公共端点。

您可以在所有提供适用于 Windows File Server 的 FSx 的 AWS 区域使用 Amazon FSx 文件网关。

入门 AWS Storage Gateway

本节提供入门说明 AWS。您需要一个 AWS 账号才能开始使用 AWS Storage Gateway。可以使用现有 AWS 账户，也可以注册新账户。您的 AWS 账户中还需要一个属于群组的 IAM 用户，该用户具有执行 Storage Gateway 任务所需的管理权限。具有相应权限的用户可以访问 Storage Gateway 控制台和 Storage Gateway API，来执行网关部署、配置和维护任务。如果您是首次使用的用户，我们建议您在使用 Storage Gateway 之前查看支持的 AWS 区域和文件网关设置要求部分。

本节包含以下主题，这些主题提供有关开始使用 AWS Storage Gateway的更多信息：

主题

- 注册 Amazon Web Services-了解如何注册 AWS 和创建 AWS 帐户。
- 创建具有管理员权限的 IAM 用户：了解如何为您的 AWS 账户创建具有管理权限的 IAM 用户。
- 正在访问 AWS Storage Gateway-了解如何 AWS Storage Gateway 通过 Storage Gateway 控制台或使用以编程方式进行访问。 AWS SDKs
- AWS 区域 支持 Storage Gateway-了解在 Storage Gateway 中激活网关时可以使用哪些 AWS 区域来存储数据。

注册 Amazon Web Services

AWS 账户 是访问 AWS 服务的基本要求。您的 AWS 账户 是您作为 AWS 用户创建的所有 AWS 资源的基本容器。您的 AWS 账户 也是 AWS 资源的基本安全边界。您在账户中创建的任何资源均可供拥有该账户的凭证的用户使用。在开始使用之前 AWS Storage Gateway，您需要注册一个 AWS 账户.

如果您没有 AWS 账户，请完成以下步骤来创建一个。

要注册 AWS 账户

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

   在注册时，将接到电话或收到短信，要求使用电话键盘输入一个验证码。

   当您注册时 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。作为最佳安全实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

我们还建议您要求用户在访问 AWS时使用临时凭证。要提供临时证书，您可以使用联合身份验证和身份提供商，例如 AWS IAM Identity Center。如果您的公司已经在使用身份提供商，则可以将其与联合身份验证一起使用，以简化您提供对 AWS 账户中资源的访问权限的方式。

创建具有管理员权限的 IAM 用户

创建 AWS 账户后，使用以下步骤为自己创建 AWS Identity and Access Management (IAM) 用户，然后将该用户添加到具有管理权限的群组。有关使用该 AWS Identity and Access Management 服务控制 Storage Gateway 资源访问权限的更多信息，请参阅AWS Storage Gateway 的身份和访问管理。

要创建管理员用户，请选择以下选项之一。

选择一种方法来管理您的管理员	目标	方式	您也可以
在 IAM Identity Center 中（推荐）	使用短期凭证访问 AWS。 这符合安全最佳实操。有关最佳实践的信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。	有关说明，请参阅《AWS IAM Identity Center 用户指南》中的入门。	通过在《AWS Command Line Interface 用户指南》 AWS IAM Identity Center中配置 AWS CLI 要使用的来配置编程访问权限。
在 IAM 中（不推荐使用）	使用长期凭证访问 AWS。	按照《IAM 用户指南》中的创建用于紧急访问的 IAM 用户中的说明进行操作。	按照《IAM 用户指南》中的管理 IAM 用户的访问密钥，配置编程式访问。

> **Warning**
>
> IAM 用户具有长期凭证，这会带来安全风险。为帮助减轻这种风险，我们建议仅向这些用户提供执行任务所需的权限，并在不再需要这些用户时将其移除。

正在访问 AWS Storage Gateway

您可以使用 AWS Storage Gateway 控制台执行各种网关配置和维护任务，包括在部署中激活或移除 Storage Gateway 硬件设备、创建、管理和删除不同类型的网关、附加、管理和分离文件系统，以及监控 Storage Gateway 服务各组件的健康状况和运行状态。为了简单易用，本指南重点介绍使用 Storage Gateway 控制台 Web 界面来执行任务。可以通过 Web 浏览器访问 Storage Gateway 控制台，网址为：https://console.aws.amazon.com/storagegateway/home/。

如果您更喜欢编程方法，则可以使用 AWS Storage Gateway 应用程序编程接口 (API) 或命令行接口 (CLI) 来设置和管理 Storage Gateway 部署中的资源。有关 Storage Gateway API 的操作、数据类型和所需语法的更多信息，请参阅 Storage Gateway API Reference。有关 Storage Gateway CLI 的更多信息，请参阅 AWS CLI Command Reference。

您还可以使用开发与 Storage Gateway 交互的应用程序。 AWS SDKs AWS SDKs 适用于 Java、.NET 和 PHP 的封装了底层的 Storage Gateway API，以简化您的编程任务。有关下载 SDK 库的信息，请参阅 AWS 开发人员中心。

有关定价的信息，请参阅 AWS Storage Gateway 定价。

AWS 区域 支持 Storage Gateway

AWS 区域 是世界上 AWS 有多个可用区的物理位置。可用区由一个或多个独立 AWS 的数据中心组成，每个数据中心都具有冗余电源、网络和连接，位于不同的设施中。这意味着每个区域在物理上 AWS 区域 都是孤立的，并且独立于其他区域。区域提供容错能力、稳定性和弹性，还可以减少延迟。除非您明确使用 AWS 服务提供的复制功能，否则您在一个区域创建的资源不存在于任何其他区域。例如，Amazon S3 和 Amazon EC2 支持跨区域复制。某些服务（ AWS Identity and Access Management例如）没有区域资源。您可以在满足业务需求的地点启动 AWS 资源。例如，您可能需要启动 Amazon EC2 实例，以便 AWS 区域 在欧洲托管您的 AWS Storage Gateway 设备，以便更接近您的欧洲用户，或者满足法律要求。您可以 AWS 账户 决定特定服务支持的哪些区域可供您使用。

Amazon FSx File Gateway 将文件数据存储在您的亚马逊 FSx文件系统所在的 AWS 区域。在开始部署网关之前，请在 Storage Gateway 控制台右上角选择一个区域。

- Amazon FSx File Gateway — 有关支持的 AWS 区域以及您可以与 Amazon FSx 文件网关一起使用的 AWS 服务终端节点列表，请参阅中的亚马逊 FSx 文件网关终端节点和配额AWS 一般参考。
- Storage Gateway — 有关支持的 AWS 区域以及可以与 Storage Gateway 配合使用的 AWS 服务终端节点列表，请参阅中的AWS Storage Gateway 终端节点和配额AWS 一般参考。
- Storage Gateway 硬件设备 - 有关可与硬件设备一起使用的受支持区域，请参阅 AWS 一般参考 中的AWS Storage Gateway 硬件设备区域。

文件网关设置要求

除非另有说明，否则 AWS Storage Gateway中的所有文件网关类型都需要满足以下要求。您的设置必须满足本节中的要求。在部署网关之前，请查看适用于您的网关设置的要求。

主题

- 先决条件
- 硬件和存储要求
- 网络和防火墙要求
- 受支持的管理程序和主机要求
- 文件网关支持的 SMB 客户端
- 文件网关支持的文件系统操作
- 管理网关的本地磁盘

先决条件

在设置 Amazon FSx 文件网关（FSx 文件网关）之前，您必须满足以下先决条件：

- 创建并配置 FSx 适用于 Windows 的文件服务器文件系统。有关说明，请参阅《亚马逊 FSx Windows 文件服务器用户指南》中的 “步骤 1：创建您的文件系统”。
- 配置 Microsoft Active Directory（AD）并创建具有必要权限的 Active Directory 服务账户。有关更多信息，请参阅 Active Directory 服务账户权限要求。
- 确保网关和 AWS之间有足够的网络带宽。成功下载、激活和更新网关至少需要 100 Mbps。
- 配置要用于与部署网关的本地环境 AWS 之间的网络流量的连接。您可以使用公共互联网、私有网络、VPN 或 Direct Connect。如果您希望网关 AWS 通过私有连接与 Amazon Virtual Private Cloud 进行通信，请在设置网关之前设置亚马逊 VPC。
- 确保您的网关可以解析 Active Directory 域控制器的名称。您可以在 Active Directory 域中使用 DHCP 来处理解析，也可以从网关本地控制台的网络配置设置菜单中手动指定 DNS 服务器。

硬件和存储要求

以下各节提供了有关网关所需的最低硬件和存储配置的信息，以及为所需存储分配的最小磁盘空间量。

本地部署的硬件要求 VMs

在本地部署网关时，请确保部署网关虚拟机的基础硬件能够分配以下最低资源：

- 分配给 VM 的四个虚拟处理器
- 16 GiB 预留 RAM 用于文件网关
- 80 GiB 磁盘空间，用于安装 VM 映像和系统数据

对 Amazon EC2 实例类型的要求

在 Amazon Elastic Compute Cloud（Amazon EC2）上部署网关时，实例大小必须至少为 **`xlarge`**，网关才能正常工作。但是，对于计算优化型实例系列，大小必须至少为 **`2xlarge`**。

> **Note**
>
> Storage Gateway AMI 仅与使用 Intel 或 AMD 处理器的基于 x86 的实例兼容。不支持使用 Graviton 处理器的基于 ARM 的实例。

使用为您的网关类型推荐的以下实例类型之一。

建议用于文件网关类型

- 通用实例系列：m5、m6 或 m7 实例类型。选择 xlarge 或更高的实例大小，以满足 Storage Gateway 处理器和 RAM 要求。
- 计算优化型实例系列 - c5、c6 或 c7 实例类型。选择 2xlarge 或更高的实例大小，以满足 Storage Gateway 处理器和 RAM 要求。
- 内存优化型实例系列 - r5、r6 或 r7 实例类型。选择 xlarge 或更高的实例大小，以满足 Storage Gateway 处理器和 RAM 要求。
- 存储优化型实例系列 - i3 i4 或 i7 实例类型。选择 xlarge 或更高的实例大小，以满足 Storage Gateway 处理器和 RAM 要求。

> **Note**
>
> 当您在 Amazon EC2 中启动网关并且所选的实例类型支持短暂存储时，将自动列出磁盘。有关 Amazon EC2 实例存储的更多信息，请参阅《Amazon EC2 用户指南》中的实例存储。

存储需求

除了 80 GiB 的 VM 磁盘空间外，您的网关还需要额外的磁盘。

网关类型	缓存（最小值）	缓存（最大值）			
文件网关	150 GiB	64 TiB			

> **Note**
>
> 您可以为缓存配置一个或多个本地驱动器，其容量不超过最大容量。
> 向现有网关添加缓存时，务必在主机（虚拟机监控程序或 Amazon EC2 实例）中创建新磁盘。
> 如果先前已将现有磁盘分配为缓存，则不要更改这些磁盘的大小。

网络和防火墙要求

您的网关需要具有对 Internet、本地网络、域名服务 (DNS) 服务器、防火墙、路由器等的访问权。

网络带宽要求因网关上传和下载的数据量而异。成功下载、激活和更新网关至少需要 100Mbps。您的数据传输模式将决定支持您的工作负载所需的带宽。

在下文中，您可以找到有关所需端口的信息，并了解如何进行设置以允许通过防火墙和路由器进行访问。

> **Note**
>
> 在某些情况下，您可以在 Amazon EC2 上部署网关，或者使用其他类型的部署（包括本地部署），其网络安全策略会限制 AWS IP 地址范围。在这些情况下，当 AWS IP 范围值发生变化时，您的网关可能会遇到服务连接问题。您需要使用的 AWS IP 地址范围值位于您激活网关的 AWS 区域的 Amazon 服务子集中。有关当前 IP 范围值，请参阅《AWS 一般参考》中的 AWS IP 地址范围。

主题

- 端口要求

- Storage Gateway 硬件设备的网络和防火墙要求
- 允许通过防火墙和路由器进行 AWS Storage Gateway 访问
- 配置 Amazon EC2 网关实例的安全组

端口要求

FSx File Gateway 要求允许特定端口通过您的网络安全，才能成功部署和运行。有些端口是所有网关所必需的，而其他端口则仅用于特定配置，例如连接到 VPC 端点时。

对于 FSx File Gateway，必须使用 Microsoft Active Directory 来允许域用户访问服务器消息块 (SMB) 文件共享。您可以将您的文件网关加入到任何有效的 Microsoft Windows 域（可通过 DNS 解析）。

您也可以使用在 Directory Service 亚马逊 Web Ser AWS Managed Microsoft ADvices 云中创建。对于大多数 AWS Managed Microsoft AD 部署，您需要为您的 VPC 配置动态主机配置协议 (DHCP) 服务。有关创建 DHCP 选项集的信息，请参阅《AWS Directory Service 管理指南》中的创建 DHCP 选项集。

下表列出了必需的端口，并在注释列中描述了条件要求。

关的 FSx 端口要求

网络元素	来源	目标	协议	端口：	入站	出站	必需	注意
Web 浏览器	您的 Web 浏览器	Storage Gateway VM	TCP HTTP	80	✓	✓	✓	由本地系统用于获取 Storage Gateway 激活密钥。仅在激活 Storage Gateway 设备期间使用端口

网络元素	来源	目标	协议	端口：	入站	出站	必需	注意
								80。Storage Gateway VM 不要求可公开访问端口 80。端口 80 所需的访问级别取决于网络配置。如果您从 Storage Gateway 管理控制台激活了网关，则您连接到控制台所用的主机必须对网关端口 80 具有访问权限。

网络元素	来源	目标	协议	端口：	入站	出站	必需	注意
Web 浏览器	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓	AWS 管理控制台（所有其他操作）
DNS	Storage Gateway VM	域名服务 (DNS) 服务器	TCP 和 UDP DNS	53	✓	✓	✓	用于 Storage Gateway VM 和 DNS 服务器之间的通信，以解析 IP 名称。

网络元素	来源	目标	协议	端口：	入站	出站	必需	注意
NTP	Storage Gateway VM	网络时间协议 (NTP) 服务器	TCP 和 UDP NTP	123	✓	✓	✓	本地系统用于将 VM 时间与主机时间同步。Storage Gateway VM 配置为使用以下 NTP 服务器： • 0.amazon.pool.ntp.org • 1.amazon.pool.ntp.org • 2.amazon.pool.ntp.org • 3.amazon.pool.ntp.org Note 对于托管

网络元素	来源	目标	协议	端口：	入站	出站	必需	注意
								在 Amazon EC2 上的网关，则不是必需的。

网络元素	来源	目标	协议	端口：	入站	出站	必需	注意
Storage Gateway	Storage Gateway VM	支持 端点	TCP SSH	22	✓	✓	✓	支持 允许访问您的网关以帮助您解决网关问题。您无需打开此端口即可实现网关的正常操作，但在进行问题排查时需要如此。有关支持端点的列表，请参阅支持 端点。
Storage Gateway	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓	管理控制台
亚马逊 CloudFront	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓	用于激活

网络元素	来源	目标	协议	端口：	入站	出站	必需	注意
VPC	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓*	管理控制台 *仅在使用 VPC 端点时才需要
VPC	Storage Gateway VM	AWS	TCP HTTPS	1026		✓	✓*	控制面板端点 *仅在使用 VPC 端点时才需要
VPC	Storage Gateway VM	AWS	TCP HTTPS	1027		✓	✓*	Anon 控制面板（用于激活） *仅在使用 VPC 端点时才需要
VPC	Storage Gateway VM	AWS	TCP HTTPS	1028		✓	✓*	代理端点 *仅在使用 VPC 端点时才需要

网络元素	来源	目标	协议	端口：	入站	出站	必需	注意
VPC	Storage Gateway VM	AWS	TCP HTTPS	1031		✓	✓*	数据层面 *仅在使用 VPC 端点时才需要
VPC	Storage Gateway VM	AWS	TCP HTTPS	2222		✓	✓*	适用于 SSH Support 频道 VPCe *仅在使用 VPC 端点时才需要用于开启支持通道
VPC	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓*	管理控制台 *仅在使用 VPC 端点时才需要

网络元素	来源	目标	协议	端口：	入站	出站	必需	注意
文件共享客户端	SMB 客户端	Storage Gateway VM	TCP 或 UDP SMBv3	445	✓	✓	✓	文件共享数据传输会话服务。 取代 Microsoft Windows NT 及更高版本的端口 137-139。
Microsoft Active Directory	Storage Gateway VM	Active Directory 服务器	UDP NetBIOS	137	✓	✓	✓	名称服务
Microsoft Active Directory	Storage Gateway VM	Active Directory 服务器	UDP NetBIOS	138	✓	✓	✓	数据报服务
Microsoft Active Directory	Storage Gateway VM	Active Directory 服务器	TCP 和 UDP LDAP	389	✓	✓	✓	目录系统代理（DSA）客户端连接
Microsoft Active Directory	Storage Gateway VM	Active Directory 服务器	TCP 和 UDP Kerberos	88	✓	✓	✓	Kerberos

网络元素	来源	目标	协议	端口：	入站	出站	必需	注意
Microsoft Active Directory	Storage Gateway VM	Active Directory 服务器	TCP 分布式计算 Environment/End 点映射器 (DCE/EMAP)	135	✓	✓	✓	RPC
亚马逊 FSx 连接	Storage Gateway VM	FSx 适用于 Windows 文件服务器	TCP 或 UDP SMBv3	445	✓	✓	✓	文件共享数据传输会话服务

Storage Gateway 硬件设备的网络和防火墙要求

每个 Storage Gateway 硬件设备都需要以下网络服务：

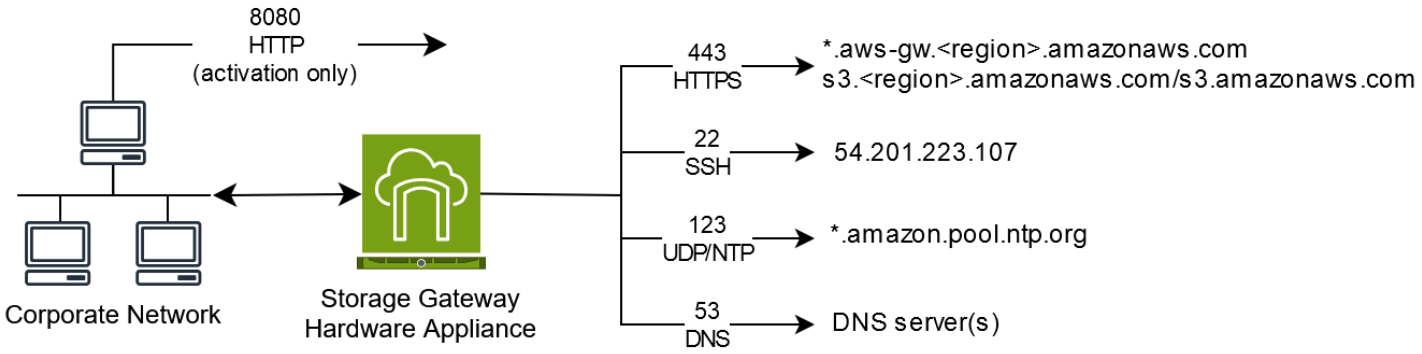
- Internet 访问 - 通过服务器上的任何网络接口实现与 Internet 的永久性网络连接。
- DNS 服务 - 用于硬件设备和 DNS 服务器之间的通信的 DNS 服务。
- 时间同步 - 必须可访问自动配置的 Amazon NTP 时间服务。
- IP 地址-分配的 DHCP IPv4 地址或静态地址。您不能分配 IPv6 地址。

Dell PowerEdge R640服务器的背面有五个物理网络端口。从左到右（面对服务器背面），这些端口如下所示：

1. iDRAC
2. em1
3. em2
4. em3

5. em4

您可以使用 iDRAC 端口进行远程服务器管理。



硬件设备需要以下端口才能运行。

协议	端口：	方向	来源	目标位置	用法
SSH	22	出站	硬件设备	54.201.223.107	支持渠道
DNS	53	出站	硬件设备	DNS 服务器	名称解析
UDP/NTP	123	出站	硬件设备	*.amazon.pool.ntp.org	时间同步
HTTPS	443	出站	硬件设备	*.amazonaws.com	数据传输
HTTP	8080	入站	AWS	硬件设备	激活（仅短时）

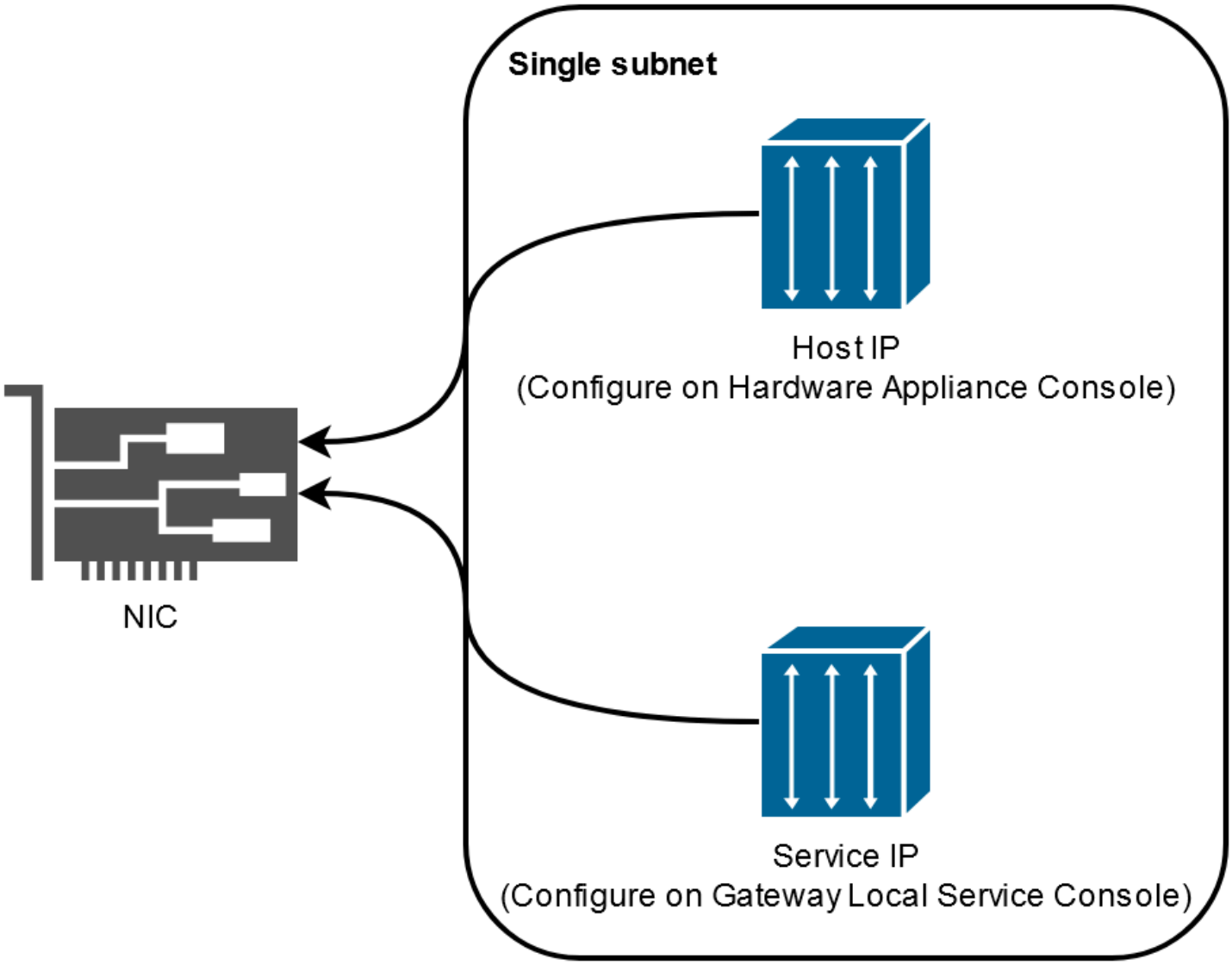
要按设计的方式运行，硬件设备需要下面所示的网络和防火墙设置：

- 在硬件控制台中配置所有连接的网络接口。
- 确保每个网络接口都位于唯一的子网中。
- 为所有连接的网络接口提供对上图中列出的端点的出站访问权限。

- 配置至少一个网络接口以支持硬件设备。有关更多信息，请参阅 配置硬件设备网络参数。

> **Note**
>
> 有关显示服务器背面及其端口的图示，请参阅物理安装硬件设备。

同一网络接口 (NIC) 上的所有 IP 地址（无论是用于网关还是主机）必须位于同一子网中。下图显示了寻址方案。



有关激活和配置硬件设备的更多信息，请参阅使用 AWS Storage Gateway 硬件设备。

允许通过防火墙和路由器进行 AWS Storage Gateway 访问

您的网关需要访问以下 Storage Gateway 服务端点才能与之通信 AWS。在网关设置过程中，根据您的网络环境选择网关的端点类型。如果使用防火墙或路由器来筛选或限制网络流量，则必须配置防火墙和路由器以允许这些服务端点与 AWS进行出站通信。

> **Note**
>
> 如果您为 Storage Gateway 配置私有 VPC 终端节点以用于连接和传出数据 AWS，则您的网关不需要访问公共互联网。有关更多信息，请参阅在 Virtual Private Cloud 中激活网关。

> **Important**
>
> *region*在以下终端节点示例中，将替换为适用于您的网关的正确 AWS 区域 字符串，例如us-west-2。
> *amzn-s3-demo-bucket*替换为您部署中的 Amazon S3 存储桶的实际名称。您也可以使用星号 (*) 代替在防火墙规则中创建通配符条目，这将允许列出所有存储桶名称的服务端点。*amzn-s3-demo-bucket*
> 如果您的网关部署 AWS 区域 在美国或加拿大，并且需要符合联邦信息处理标准 (FIPS) 的终端节点连接，请*s3*替s3-fips换为。

端点类型

标准端点

这些端点支持您的网关设备与之间的 IPv4 流量 AWS。

所有网关都需要以下服务端点才能执行 head-bucket 操作。

```
bucket-name.s3.region.amazonaws.com:443
```

所有网关的控制路径（anon-cp、client-cp、proxy-app）和数据路径（dp-1）操作均需要以下服务端点。

```
anon-cp.storagegateway.region.amazonaws.com:443
client-cp.storagegateway.region.amazonaws.com:443
```

```
proxy-app.storagegateway.region.amazonaws.com:443
dp-1.storagegateway.region.amazonaws.com:443
```

调用 API 需要使用以下网关服务端点。

```
storagegateway.region.amazonaws.com:443
```

以下示例是美国西部（俄勒冈州）区域 (us-west-2) 中的网关服务端点。

```
storagegateway.us-west-2.amazonaws.com:443
```

除了 Storage Gateway 和 Amazon S3 服务终端节点外，Storage Gateway VMs 还需要对以下 NTP 服务器进行网络访问：

```
time.aws.com
0.amazon.pool.ntp.org
1.amazon.pool.ntp.org
2.amazon.pool.ntp.org
3.amazon.pool.ntp.org
```

有关支持的终端节点 AWS 区域 和服务端点的更多信息，请参阅中的 Storage Gateway AWS 一般参考。

配置 Amazon EC2 网关实例的安全组

在中 AWS Storage Gateway，安全组控制您的 Amazon EC2 网关实例的流量。在配置安全组时，建议您执行以下操作：

- 安全组不应允许来自外部 Internet 的传入连接。它应仅允许网关安全组内的实例与网关进行通信。

  如果您需要允许实例从该安全组的外部连接到网关，建议您只允许端口 80（适用于激活）上的连接。
- 若要从网关的安全组外部的 Amazon EC2 主机激活您的网关，则需要允许从该主机的 IP 地址通过端口 80 进行传入连接。如果您不能确定激活主机的 IP 地址，则可以打开端口 80、激活网关，然后在完成激活后关闭端口 80 上的访问。
- 仅当使用端口 22 支持 进行故障排除时，才允许访问。有关更多信息，请参阅 你 支持 想帮忙排查你的 Amazon EC2 网关的问题。

受支持的管理程序和主机要求

您可以在本地将 Storage Gateway 作为虚拟机 (VM) 设备或物理硬件设备运行，也可以 AWS 作为 Amazon EC2 实例运行。

> **Note**
>
> 文件网关 2.x、Volume Gateway 3.x 和 Tape Gateway 3.x 需要禁用安全启动的 UEFI 启动模式（loader_secure=no）。每次下载 qcow 时都会提供一个 xml 文件作为快速设置配置。

Storage Gateway 支持以下管理程序版本和主机：

- VMware ESXi 虚拟机管理程序（版本 7.0 或 8.0）-对于此设置，还需要一个 VMware vSphere 客户端来连接到主机。
- Microsoft Hyper-V 虚拟机监控程序（2019、2022 或 2025）：对于此设置，您需要 Microsoft Windows 客户端计算机上的 Microsoft Hyper-V Manager 才能连接到主机。
- 基于 Linux 内核的虚拟机 (KVM) - 免费的开源虚拟化技术。Linux 2.6.20 及更高版本中都包括了 KVM。Storage Gateway 经过测试并支持 CentOS/RHEL 7.7、RHEL 8.6 Ubuntu 16.04 LTS 和 Ubuntu 18.04 LTS 发行版。任何其他现代 Linux 发行版可能有效，但不能保证功能或性能。如果您已经启动并运行了 KVM 环境并且您已经熟悉 KVM 的工作原理，我们建议使用此选项。有关建议的启动配置，请参阅提供的 aws-storage-gateway .xml 文件。文件网关 2.x、Volume Gateway 3.x 和 Tape Gateway 3.x 需要禁用安全启动的 UEFI 启动模式（loader_secure=no）。
- Nutanix AHV（雅典卫城虚拟机管理程序）从 10.0.1.1 版本开始，这是一个基于 KVM 的虚拟化平台，已集成到 Nutanix 超融合基础架构 (HCI) 解决方案中。
- Amazon EC2 实例 - Storage Gateway 提供了一个包含网关 VM 映像的 Amazon 系统映像 (AMI)。有关如何在 Amazon EC2 上部署网关的信息，请参阅为 FSx 文件网关部署默认 Amazon EC2 主机。
- Storage Gateway 硬件设备：对于虚拟机基础设施有限的位置，Storage Gateway 提供了物理硬件设备来作为本地部署选项。

> **Note**
>
> Storage Gateway 不支持从另一个网关虚拟机的快照或克隆创建的虚拟机或从 Amazon EC2 AMI 恢复网关。如果您的网关 VM 出现故障，请激活新网关并将您的数据恢复到该网关。有关更多信息，请参阅 从虚拟机意外关闭中恢复。

Storage Gateway 不支持动态内存和虚拟内存激增。

文件网关支持的 SMB 客户端

文件网关支持以下服务消息块（SMB）客户端：

- Microsoft Windows Server 2008 R2 及更高版本
- Windows 桌面版本：10、8 和 7。
- 在 Windows Server 2008 及更高版本上运行的 Windows 终端服务器

> **Note**
>
> 服务器消息块加密需要支持 SMB v3.x 方言的客户端。

文件网关支持的文件系统操作

您的 SMB 客户端可以写入、读取、删除和截断文件。当客户端向 Storage Gateway 发送写入内容时，它会同步写入本地缓存。然后，它通过优化的传输 FSx 异步写入 Amazon。首先通过本地缓存来提供读取内容。如果数据不可用，则会通过 Amazon FSx 作为读取缓存获取。

仅在通过网关传送的已更改或请求的部分中优化写入内容和读取内容。删除从 Amazon 移除的文件 FSx。

管理网关的本地磁盘

网关虚拟机（VM）使用您在本地分配的本地磁盘进行缓冲和存储。在 Amazon EC2 实例上创建的文件网关将使用 Amazon EBS 卷作为本地磁盘。要为网关分配的磁盘的数量和大小由您自己决定。网关使用您分配的缓存存储来提供对最近访问数据的低延迟访问。缓存存储空间充当待上传到 的数据的本地持久存储 FSx。文件网关至少需要一个 150 GiB 磁盘用作缓存。网关的初始配置和部署完成后，随着工作负载需求的增加，您可以添加更多磁盘作为缓存存储。本节包含以下主题，这些主题说明了与管理本地磁盘相关的概念和程序。

主题

- 确定本地磁盘存储量：了解如何确定要为文件网关分配的本地缓存磁盘的数量和大小。

- 配置额外的缓存存储：了解如何随着应用程序需求的变化增加文件网关的缓存存储容量。
- 将临时存储与 EC2 网关结合使用：了解在文件网关中使用临时磁盘存储时如何防止数据丢失。

确定本地磁盘存储量

部署 S 关时，请考虑要分配多少缓存磁盘。文件网关使用最近最少使用的算法自动从缓存中移出数据。S 上的缓存在该网关上的所有文件共享之间共享。如果您有多个活动共享，请务必注意，一个共享的利用率高会影响另一个共享可以获得的缓存资源量，从而可能影响性能。

在确定给定工作负载需要多少缓存磁盘时，请务必注意，您可以随时向网关添加缓存磁盘（不超过关的当前配额），但不能减少给定网关的缓存。您可以对数据集执行基本分析以确定合适的缓存磁盘容量，但是无法精确判断有多少数据是“热数据”（需要在本地存储），以及有多少数据是“冷数据”（可以分层到云端）。工作负载会随着时间的推移而变化，文件网关提供了与可消耗的资源量相关的灵活性和弹性。随时可以增加缓存量，因此可以从小规模起步，然后根据需要增加缓存量，这通常是最具成本效益的方法。

在网关设置期间，您可以使用 150 GiB 的初始近似值为缓存存储预置磁盘。然后，您可以使用 Amazon CloudWatch 运营指标监控缓存存储空间使用情况，并使用控制台根据需要配置更多存储空间。有关使用指标和设置警报的信息，请参阅 性能和优化。

> **Note**
>
> 底层物理存储资源在中表示为数据存储 VMware。部署网关 VM 时，您可选择用来存储 VM 文件的数据存储。预置本地磁盘（例如，用作缓存存储）时，您可以选择将虚拟磁盘存储在与 VM 相同的数据存储中，也可以选择将其存储在另一个数据存储中。
> 如果您有多个数据存储，强烈建议为缓存存储选择一个数据存储。如果将仅依托于一个底层物理磁盘的数据存储用于支持缓存存储，则可能会导致性能不佳。如果备份是性能较低的 RAID 配置（例如），也是如此。 RAID1

配置额外的缓存存储

随着应用程序需求的变化，您可以增加网关的缓存存储容量。您可以在不中断功能或导致停机的情况下为网关添加存储容量。添加更多存储时，在开启网关 VM 的情况下添加。

> **Important**
>
> 向现有网关添加缓存时，必须在网关主机虚拟机监控程序或 Amazon EC2 实例上创建新磁盘。请勿删除或更改已分配为缓存的现有磁盘的大小。

为网关配置额外的缓存存储

1. 在您的网关主机管理程序或 Amazon EC2 实例上预配置一个或多个新磁盘。有关如何在管理程序中预配置磁盘的信息，请参阅管理程序的文档。有关为 Amazon EC2 实例预配置 Amazon EBS 卷的信息，请参阅《适用于 Linux 实例的 Amazon Elastic Compute Cloud 用户指南》中的 Amazon EBS 卷。在以下步骤中，将此磁盘配置为缓存存储。
2. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
3. 在导航窗格中，选择网关。
4. 搜索您的网关并从列表中选择它。
5. 从操作菜单中选择配置缓存存储。
6. 在配置缓存存储部分，找到您预置的磁盘。如果您未看到您的磁盘，请选择刷新图标来刷新列表。对于每个磁盘，从已分配给下拉菜单中选择缓存。

   > **Note**
   >
   > 在文件网关上分配磁盘时，缓存是唯一可用的选项。

7. 选择保存更改来保存您的配置设置。

将临时存储与 EC2 网关结合使用

我们不建议在文件网关上 FSx 使用临时磁盘作为缓存存储。

临时磁盘为 Amazon EC2 实例提供临时块级存储。当您在 Amazon EC2 亚马逊机器映像中启动网关，并且所选的实例类型支持临时存储时，将自动列出临时磁盘。您可以选择其中一个磁盘来存储网关的缓存数据。有关更多信息，请参阅《Amazon EC2 用户指南》中的 Amazon EC2 实例存储。

应用程序写入网关的数据同步存储在临时磁盘的缓存中，然后异步上传到适用于 Windows 文件服务器的 A FSx zon S3 中的持久存储中。如果 Amazon EC2 实例在数据写入临时存储之后但在异步上传发生之前停止，则任何尚未上传到 S3 for Windows 文件服务器的数据都可能丢失。

Important

如果您停止并启动使用临时存储的 Amazon EC2 网关，则该网关将永久脱机。发生这种情况的原因是替换了物理存储磁盘。此问题没有解决方法。唯一的解决方案是删除该网关，然后在新的 EC2 实例上激活一个新网关。

使用 AWS Storage Gateway 硬件设备

> **Note**
>
> 终止上市通知：自 2025 年 5 月 12 日起，将不再提供 AWS Storage Gateway 硬件设备。使用 AWS Storage Gateway 硬件设备的现有客户可以继续使用并获得支持，直到 2028 年 5 月。作为替代方案，您可以使用该 AWS Storage Gateway 服务让您的本地和云端应用程序访问几乎无限的云存储。

AWS Storage Gateway 硬件设备是一种物理硬件设备，在经过验证的服务器配置中预装了 Storage Gateway 软件。您可以从 AWS Storage Gateway 控制台的硬件设备概述页面管理部署中的硬件设备。

硬件设备是一个高性能的 1U 服务器，您可以将其部署在您的数据中心或企业防火墙内的本地位置。在购买并激活硬件设备时，激活过程会将硬件设备与您的 AWS 账户关联。激活后，硬件设备会出现在控制台中的硬件设备概览页面上。您可以将硬件设备配置为 S3 文件网关、 FSx 文件网关、磁带网关或卷网关类型。用于在硬件设备上部署这些网关类型的过程与虚拟平台上的过程相同。

有关 AWS Storage Gateway 硬件设备可供激活和使用的支持 AWS 区域 区域列表，请参阅中的 AWS Storage Gateway 硬件设备区域AWS 一般参考。

在接下来的章节中，您可以找到有关如何设置、机架安装、通电、配置、激活、启动、使用和删除 AWS Storage Gateway 硬件设备的说明。

主题

- 设置 AWS Storage Gateway 硬件设备
- 物理安装硬件设备
- 访问硬件设备控制台
- 配置硬件设备网络参数
- 激活 AWS Storage Gateway 硬件设备
- 在硬件设备上创建网关
- 在硬件设备上配置网关 IP 地址
- 从硬件设备中移除网关软件
- 正在删除 AWS Storage Gateway 硬件设备

设置 AWS Storage Gateway 硬件设备

> **Note**
>
> 终止上市通知：自 2025 年 5 月 12 日起，将不再提供 AWS Storage Gateway 硬件设备。使用 AWS Storage Gateway 硬件设备的现有客户可以继续使用并获得支持，直到 2028 年 5 月。作为替代方案，您可以使用该 AWS Storage Gateway 服务让您的本地和云端应用程序访问几乎无限的云存储。

收到 Storage Gateway Hardware Appliance 后，您可以使用硬件设备本地控制台配置网络，以提供与设备的始终在线连接 AWS 并激活设备。激活会将您的设备与激活过程中使用的 AWS 帐户相关联。激活设备后，您可以从 Storage Gateway 控制台启动 S3 FSx 文件网关、文件网关、磁带网关或卷网关。

安装和配置硬件设备

1. 机架安装设备，然后通电并连接网络连接。有关更多信息，请参阅 物理安装硬件设备。
2. 为硬件设备（主机IPv4）设置互联网协议版本 4 () 地址。有关更多信息，请参阅 配置硬件设备网络参数。
3. 在您选择的 AWS 区域的主机硬件设备概述页面上激活硬件设备。有关更多信息，请参阅 激活 AWS Storage Gateway 硬件设备。
4. 在硬件设备上创建网关。有关更多信息，请参阅 创建网关。

   在硬件设备上设置网关的方式与在 VMware ESXi、Microsoft Hyper-V、基于 Linux 内核的虚拟机 (KVM) 或 Amazon EC2 上设置网关的方式相同。

增加可用缓存存储

您可以将硬件设备上的可用存储从 5 TB 增加到 12 TB。这样做可以为低延迟访问中的数据提供更大的缓存 AWS。如果您订购的是 5 TB 型号，则可以通过购买五个 1.92 TB SSDs（固态硬盘）将可用存储空间增加到 12 TB。

然后，您可以在激活硬件设备之前将 SSD 添加到硬件设备。如果您已激活硬件设备并希望将设备上的可用存储增加到 12 TB，请执行以下操作：

1. 将硬件设备重置为出厂设置。有关如何执行此操作的说明，请联系 AWS Support。
2. 向设备添加五个 1.92 TB SSDs 的容量。

网络接口卡选项

根据您订购的设备型号，它可能配有 10G-Base-T RJ45 铜缆或 10G DA/SFP+ 网卡。

- 10 G-Base-T 网卡配置：
  - 使用 10G 的 CAT6 电缆或 CAT5 (e) 用于 1G 的电缆
- 10G DA/SFP+ NIC 配置：
  - 使用最长 5 米的 Twinax 铜质直连线缆
  - 戴尔/英特尔兼容 SFP+ 光学模块（SR 或 LR）
  - 适用于 1 或 10G-Base-T 的 SFP/SFP+ 铜质收发器 G-Base-T

物理安装硬件设备

> **Note**
>
> 终止上市通知：自 2025 年 5 月 12 日起，将不再提供 AWS Storage Gateway 硬件设备。使用 AWS Storage Gateway 硬件设备的现有客户可以继续使用并获得支持，直到 2028 年 5 月。作为替代方案，您可以使用该 AWS Storage Gateway 服务让您的本地和云端应用程序访问几乎无限的云存储。

您的设备具有 1U 外形规格，可安装在符合国际电工委员会 (IEC) 标准的 19 英寸机架中。

先决条件

要安装您的硬件设备，需要以下组件：

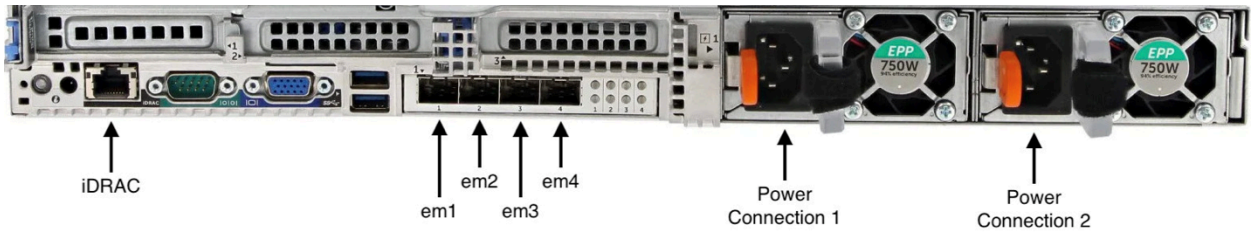
- 电源线：必需有一根，建议使用两根。
- 支持的网络布线（取决于硬件设备中包括的网络接口卡 (NIC)）。Twinax 铜质 DAC、SFP+ 光学模块（兼容英特尔）或 SFP 转 Base-T 铜质收发器。
- 键盘和显示器，或键盘、视频和鼠标 (KVM) 切换解决方案。

> **Note**
>
> 在执行以下程序之前，请确保您符合Storage Gateway 硬件设备的网络和防火墙要求中所述的 Storage Gateway 硬件设备的所有要求。

物理安装硬件设备

1. 拆开硬件设备包装，并按照箱内包含的说明操作，在机架上安装服务器。

   下图显示了硬件设备的背面，带有用于连接电源、以太网、显示器、USB 键盘和 iDRAC 的端口。
   带有网络和电源连接器标签的硬件设备一背面。



   带有网络和电源连接器标签的硬件设备一背面。

2. 插上到两个电源的电源连接。可以仅插上一个电源连接，但我们建议插上这两个电源连接来提供冗余。

3. 将以太网电缆插入 em1 端口以提供始终开启的 Internet 连接。em1 端口是后部的四个物理网络端口的第一个（从左至右）。

   > **Note**
   >
   > 硬件设备不支持 VLAN 中继。将用于连接硬件设备的交换机端口设置为非中继 VLAN 端口。

4. 将键盘和显示器插入电源。

5. 通过按前面板上的 Power (电源) 按钮来为服务器通电，如下图所示。
   带有电源按钮标签的硬件设备正面。

   带有电源按钮标签的硬件设备正面。

下一步

访问硬件设备控制台

访问硬件设备控制台

> **Note**
>
> 终止上市通知：自 2025 年 5 月 12 日起，将不再提供 AWS Storage Gateway 硬件设备。使用 AWS Storage Gateway 硬件设备的现有客户可以继续使用并获得支持，直到 2028 年 5 月。作为替代方案，您可以使用该 AWS Storage Gateway 服务让您的本地和云端应用程序访问几乎无限的云存储。

打开硬件设备的电源后，显示器上会显示硬件设备控制台。硬件设备控制台提供了一个专用于 AWS 设置管理员密码、配置初始网络参数和打开支持渠道的用户界面 AWS。

要使用硬件设备控制台，请通过键盘输入文本，然后使用 Up、Down、Right 和 Left Arrow 键按指示的方向在屏幕上移动。使用 Tab 键可在屏幕上按顺序向前移动项目。对于某些设置，您可以使用 Shift+Tab 按键按顺序向后移动。使用 Enter 键可保存选择，或者选择屏幕上的按钮。

首次出现硬件设备控制台时，将显示欢迎页面，系统会提示您为管理员用户账户设置密码，然后您才能访问控制台。

设置管理员密码

- 在请设置您的登录密码提示处，执行以下操作：

  a. 对于 Set Password (设置密码)，输入密码，然后按 Down arrow。
  b. 对于 Confirm (确认)，重新输入密码，然后选择 Save Password (保存密码)。

设置密码后，将显示硬件控制台主页。主页显示 em1、em2、em3 和 em4 网络接口的网络信息，并具有以下菜单选项：

- 配置网络
- 打开服务控制台
- 更改密码
- 注销
- 打开支持控制台

下一步

配置硬件设备网络参数

配置硬件设备网络参数

> **Note**
>
> 终止上市通知：自 2025 年 5 月 12 日起，将不再提供 AWS Storage Gateway 硬件设备。使用 AWS Storage Gateway 硬件设备的现有客户可以继续使用并获得支持，直到 2028 年 5 月。作为替代方案，您可以使用该 AWS Storage Gateway 服务让您的本地和云端应用程序访问几乎无限的云存储。

在硬件设备启动并且您在硬件控制台中设置了管理员用户密码（如访问硬件设备控制台中所述）后，使用以下过程来配置网络参数，以便硬件设备可以连接到 AWS。

设置网络地址

1. 在主页中，选择配置网络，然后按 Enter。将出现配置网络页面。配置网络页面显示硬件设备上 4 个网络接口中每个接口的 IP 和 DNS 信息，并包括用于为每个接口配置 DHCP 或静态地址的菜单选项。
2. 对于 em1 接口，执行以下操作之一：

   - 选择 DHCPEnter，然后按使用动态主机配置协议 (DHCP) 服务器分配给物理网络端口 IPv4 的地址。

     请记下此地址，以便稍后在激活步骤中使用。
   - 选择静态并按下Enter以配置静态 IPv4 地址。

     为 em1 网络接口输入有效的 IP 地址、子网掩码、网关和 DNS 服务器地址。

     完成后，选择保存，然后按 Enter 来保存配置。

   > **Note**
   >
   > 除了 em1 之外，还可以使用此过程配置其它网络接口。如果您配置其他接口，则它们必须为要求中列出的 AWS 端点提供相同的始终在线连接。
   > 硬件设备或 Storage Gateway 不支持网络绑定和链路聚合控制协议（LACP）。

建议不要在同一个子网上配置多个网络接口，因为这有时会导致路由问题。

从硬件控制台注销

1. 选择返回，然后按 Enter 来返回主页。
2. 选择注销，然后按 Enter 来返回欢迎页面。

下一步

激活 AWS Storage Gateway 硬件设备

激活 AWS Storage Gateway 硬件设备

Note

终止上市通知：自 2025 年 5 月 12 日起，将不再提供 AWS Storage Gateway 硬件设备。使用 AWS Storage Gateway 硬件设备的现有客户可以继续使用并获得支持，直到 2028 年 5 月。作为替代方案，您可以使用该 AWS Storage Gateway 服务让您的本地和云端应用程序访问几乎无限的云存储。

配置 IP 地址后，您可以在 AWS Storage Gateway 控制台的 “硬件” 页面上输入此 IP 地址以激活您的硬件设备。激活过程会将设备注册到您的 AWS 账户。

您可以选择在任何支持的设备中激活您的硬件设备 AWS 区域。有关支持的列表 AWS 区域，请参阅中的 Storage Gateway 硬件设备区域AWS 一般参考。

激活您的 AWS Storage Gateway 硬件设备

1. 打开 AWS Storage Gateway Management Console，使用您要用于激活硬件的账户凭证进行登录。

Note

如果只激活，必须满足以下条件：

- 您的浏览器必须与您的硬件设备位于同一网络上。

- 您的防火墙必须允许在 8080 端口上对设备的入站流量进行 HTTP 访问。

2. 从页面左侧的导航菜单中选择硬件。
3. 选择激活设备。
4. 在 IP 地址中，输入您为硬件设备配置的 IP 地址，然后选择连接。

   有关配置 IP 地址的更多信息，请参阅配置网络参数。
5. 在名称中，输入硬件设备的名称。名称长度最多为 255 个字符，并且不能包含斜杠字符。
6. 在硬件设备时区中，输入生成网关大部分工作负载的本地时区，然后选择下一步。

   时区控制硬件更新发生的时间，以凌晨 2 点作为执行更新的默认计划时间。理想情况下，如果时区设置正确，则默认情况下，更新将在本地工作日窗口之外进行。
7. 查看“硬件设备详细信息”部分的激活参数。您可以选择上一步返回并根据需要进行更改。否则，请选择激活以完成激活。

此时，硬件设备概览页面上会出现一个横幅，指示硬件设备已成功激活。

此时，该设备已与您的账户关联。下一步是在新设备上配置和启动 S3 文件网关、 FSx 文件网关、磁带网关或卷网关。

下一步

在硬件设备上创建网关

在硬件设备上创建网关

> **Note**
>
> 终止上市通知：自 2025 年 5 月 12 日起，将不再提供 AWS Storage Gateway 硬件设备。使用 AWS Storage Gateway 硬件设备的现有客户可以继续使用并获得支持，直到 2028 年 5 月。作为替代方案，您可以使用该 AWS Storage Gateway 服务让您的本地和云端应用程序访问几乎无限的云存储。

您可以在部署中的任何 AWS Storage Gateway 硬件设备上创建 S3 FSx 文件网关、文件网关、磁带网关或卷网关。

在硬件设备上创建网关

1. 登录 AWS 管理控制台 并在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 按照 Creating Your Gateway 中所述的过程，设置、连接和配置要部署的 Storage Gateway 类型。

在 Storage Gateway 控制台中完成网关创建后，Storage Gateway 软件会自动在硬件设备上开始安装。如果使用动态主机配置协议（DHCP），网关可能需要 5 到 10 分钟才能在控制台中显示为在线。要为已安装的网关分配静态 IP 地址，请参阅 Configuring an IP address for the gateway。

要向已安装的网关分配一个静态 IP 地址，接下来您要配置网关的网络接口，以便您的应用程序可以使用它。

下一步

在硬件设备上配置网关 IP 地址

在硬件设备上配置网关 IP 地址

> **Note**
>
> 终止上市通知：自 2025 年 5 月 12 日起，将不再提供 AWS Storage Gateway 硬件设备。使用 AWS Storage Gateway 硬件设备的现有客户可以继续使用并获得支持，直到 2028 年 5 月。作为替代方案，您可以使用该 AWS Storage Gateway 服务让您的本地和云端应用程序访问几乎无限的云存储。

在激活硬件设备之前，为其物理网络接口分配一个 IP 地址。您已激活设备并在设备上启动了 Storage Gateway，现在您需要为在硬件设备上运行的 Storage Gateway 虚拟机分配另一个 IP 地址。要向已安装在硬件设备上的网关分配静态 IP 地址，请从该网关的网关本地控制台配置 IP 地址。应用程序（如 NFS 或 SMB 客户端）会连接到此 IP 地址。可以从硬件设备控制台使用打开服务控制台选项来访问网关本地控制台。

在设备上配置 IP 地址以使用应用程序

1. 在硬件控制台上，选择打开服务控制台，然后按 `Enter` 来打开网关本地控制台的登录页面。
2. AWS Storage Gateway 本地控制台登录页面会提示您登录以更改网络配置和其他设置。

默认账户为 admin，默认密码为 password。

> **Note**
>
> 我们建议更改默认密码，方法是在 AWS 设备激活 - 配置主菜单中为网关控制台输入相应的数字，然后运行 passwd 命令。有关如何运行该命令的信息，请参阅在本地控制台上运行 Storage Gateway 命令。还可以从 Storage Gateway 控制台设置密码。有关更多信息，请参阅 从 Storage Gateway 控制台设置本地控制台密码。

3. AWS 设备激活 - 配置页面包括以下菜单选项：

   - HTTP/SOCKS 代理配置
   - 网络配置
   - 测试网关连接性
   - 查看系统资源检查
   - 系统时间管理
   - 许可证信息
   - 命令提示符

> **Note**
>
> 某些选项仅针对特定的网关类型或主机平台才显示。

输入相应的数字以导航到网络配置页面。

4. 执行以下操作之一来配置网关 IP 地址：

   - 要使用由动态主机配置协议（DHCP）服务器分配的 IP 地址，请为配置 DHCP 输入相应的数字，然后在下一页上输入有效的 DHCP 配置信息。
   - 要分配静态 IP 地址，请对于配置静态 IP 输入相应的数字，然后在下一页上输入有效的 IP 地址和 DNS 信息。

> **Note**
>
> 您在此处指定的 IP 地址必须与在硬件设备激活期间使用的 IP 地址位于相同的子网中。

退出网关本地控制台

- 按 Crtl+]（右方括号）按键。硬件控制台随即会出现。

> **Note**
>
> 这是在按按键之前退出网关本地控制台的唯一方式。

在已激活并配置您的硬件设备后，设备将显示在控制台中。现在，可以在 Storage Gateway 控制台中继续执行网关的设置和配置过程。有关说明，请参阅配置您的 Amazon FSx 文件网关。

从硬件设备中移除网关软件

> **Note**
>
> 终止上市通知：自 2025 年 5 月 12 日起，将不再提供 AWS Storage Gateway 硬件设备。使用 AWS Storage Gateway 硬件设备的现有客户可以继续使用并获得支持，直到 2028 年 5 月。作为替代方案，您可以使用该 AWS Storage Gateway 服务让您的本地和云端应用程序访问几乎无限的云存储。

如果您不再需要已部署在硬件设备上的特定 Storage Gateway，则可以从硬件设备中移除网关软件。移除网关软件后，可以选择在其位置部署新的网关，或者从 Storage Gateway 控制台中删除硬件设备本身。要从您的硬件设备中删除网关软件，请使用以下步骤。

从硬件设备中删除网关

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 从控制台页面左侧的导航窗格中选择硬件，然后对于要从中移除网关软件的设备选择硬件设备名称。
3. 从操作下拉菜单中，选择移除网关。

   此时会显示确认对话框。
4. 验证要从指定的硬件设备中移除网关软件，然后在确认框中键入单词 `remove`。
5. 选择移除来永久移除网关软件。

> **Note**
>
> 删除网关软件后，无法撤销该操作。对于某些网关类型，您可能在删除时丢失数据，特别是缓存数据。有关删除网关的更多信息，请参阅删除网关和移除关联的资源。

删除网关不会从控制台删除硬件设备。硬件设备将保留以供将来进行网关部署。

正在删除 AWS Storage Gateway 硬件设备

> **Note**
>
> 终止上市通知：自 2025 年 5 月 12 日起，将不再提供 AWS Storage Gateway 硬件设备。使用 AWS Storage Gateway 硬件设备的现有客户可以继续使用并获得支持，直到 2028 年 5 月。作为替代方案，您可以使用该 AWS Storage Gateway 服务让您的本地和云端应用程序访问几乎无限的云存储。

如果您不再需要已经激活的 AWS Storage Gateway 硬件设备，则可以将该设备从您的 AWS 帐户中完全删除。

> **Note**
>
> 要将设备移至其他 AWS 帐户或 AWS 区域，必须先使用以下步骤将其删除，然后打开网关的支持渠道并联系 支持 以执行软重置。有关更多信息，请参阅托管的网关进行故障排除。

删除硬件设备

1. 如果在硬件设备上安装了网关，则必须先删除网关，然后才能删除该设备。有关如何从硬件设备中删除网关的说明，请参阅从硬件设备中移除网关软件。
2. 在 Storage Gateway 控制台的硬件页面上，选择要删除的硬件设备。
3. 对于 Actions (操作)，选择 Delete Appliance (删除设备)。此时会显示确认对话框。
4. 确认要删除指定的硬件设备，然后在确认框中键入单词 delete 并选择删除。

   在删除硬件设备时，还会删除与设备上安装的网关关联的所有资源，但不会删除硬件设备上本身的数据。

创建网关

本页上的概述章节简要介绍了 Storage Gateway 创建过程的工作原理。有关使用 Storage Gateway 控制台创建特定类型网关的 step-by-step过程，请参阅以下主题：

- Create and activate an Amazon S3 File Gateway
- 创建并激活 Amazon FSx 文件网关
- Create and activate a Tape Gateway
- Create and activate a Volume Gateway

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

概述 - 网关激活

网关激活包括设置网关，将其连接到 AWS，然后查看您的设置并激活它。

设置网关

要设置 Storage Gateway，首先选择要创建的网关类型以及用于运行网关虚拟设备的主机平台。然后，您可以为所选平台下载网关虚拟设备模板，并将其部署到本地环境中。您还可以将 Storage Gateway 部署为从首选经销商处订购的物理硬件设备，或者将其部署为 AWS 云环境中的 Amazon EC2 实例。部署网关设备时，需要在虚拟化主机上分配本地物理磁盘空间。

连接到 AWS

下一步是将网关连接到 AWS。为此，您首先要选择要用于网关虚拟设备与云中 AWS 服务之间通信的服务端点类型。可以从公有互联网访问此端点，也可以限制为只能从 Amazon VPC 内访问，这样您就可以完全控制网络安全配置。然后，您可以指定网关的 IP 地址或其激活密钥，通过连接到网关设备上的本地控制台即可获得这些信息。

检查并激活

此时，您可以检查所选的网关和连接选项，如有需要，可进行更改。根据您的需要设置好一切之后，您可以激活网关。在开始使用已激活的网关之前，您需要配置一些额外设置并创建存储资源。

概述 - 网关配置

激活 Storage Gateway 后，您需要执行一些额外的配置。在此步骤中，分配您在网关主机平台上预配置的物理存储，将其用作高速缓存或网关设备的上传缓冲区。然后，您可以使用 Amazon CloudWatch 日志和 CloudWatch 警报配置设置以帮助监控网关的运行状况，并根据需要添加标签以帮助识别网关。在开始使用已激活和已配置的网关之前，您需要创建存储资源。

概述 - 存储资源

激活并配置 Storage Gateway 后，您需要创建云存储资源来供其使用。根据您创建的网关类型，您将使用 Storage Gateway 控制台创建卷、磁带或 Amazon S3 或 Amazon FSx 文件共享以与之关联。每种网关类型都使用其各自的资源来模拟相关类型的网络存储基础设施，并将您写入其中的数据传输到 AWS 云。

创建 FSx 适用于 Windows 的 Amazon 文件服务器文件系统

要在中创建亚马逊 FSx 文件网关 AWS Storage Gateway，第一步是创建 FSx 适用于 Windows 的亚马逊文件服务器文件系统。如果您已经创建了 Amazon FSx 文件系统，请转到下一步，创建并激活 Amazon FSx 文件网关。

> **Note**
>
> 从文件网关写入 Amazon FSx 文件系统时， FSx 存在以下限制：
>
> - 您的 Amazon FSx FSx 文件系统和文件网关必须归同一个 AWS 账户所有，并且位于同一 AWS 区域。
> - 每个网关可以支持五个附加的文件系统。连接文件系统时，Storage Gateway 控制台会通知您所选网关是否已达到容量。在这种情况下，必须先选择其他网关或分离文件系统，然后才能连接另一个网关。
> - FSx File Gateway 支持软存储配额（当用户超过其数据限制时发出警告），但不支持硬配额（通过拒绝写入访问来强制执行数据限制）。除 Amazon FSx 管理员用户外，所有用户均支持软配额。有关设置存储配额的更多信息，请参阅《Amazon FSx for Windows 文件服务器用户指南》中的存储配额。

- 我们不建议使用 Microsoft 分布式文件系统 (DFS) 通过文件网关将用户重定向到您的亚马逊 FSx FSx 文件系统。相反，请将 DFS 配置为直接重定向到亚马逊 FSx 文件系统， AWS 云如亚马逊版 Windows 文件服务器用户指南中使用 DFS 命名空间对多个文件系统 FSx 进行分组中所述。
- 文件网关上的某些 FSx 文件操作（例如顶级文件夹重命名或权限更改）可能会导致多个文件操作，从而导致您 FSx 的 Windows 文件服务器文件系统 I/O 负载过高。如果您的文件系统没有足够的性能资源来处理您的工作负载，则文件系统可能会删除卷影副本，因为它优先考虑持续的可用性 I/O 而不是历史卷影副本的保留。

  在 Amazon FSx 控制台中，查看监控和性能页面，查看您的文件系统是否配置不足。如果是，您可以切换到 SSD 存储、增加吞吐能力或增加 SSD IOPS 来处理您的工作负载。

创建 FSx 适用于 Windows 的文件服务器文件系统

1. 打开 AWS 管理控制台 at https://console.aws.amazon.com/fsx/home/，然后选择要在其中创建网关的区域。
2. 按照《亚马逊 Windows 文件服务器用户指南》 FSx中的 “亚马逊入门” 中的说明 FSx 进行操作。

创建并激活 Amazon FSx 文件网关

在此部分中，您可以找到有关如何在 AWS Storage Gateway中创建、部署和激活文件网关的说明。

主题

- 设置 Amazon FSx 文件网关
- 将您的 Amazon FSx 文件网关连接到 AWS
- 查看设置并激活您的 Amazon FSx 文件网关
- 配置您的 Amazon FSx 文件网关

设置 Amazon FSx 文件网关

设置新的 FSx 文件网关

1. 打开 AWS 管理控制台 at https://console.aws.amazon.com/storagegateway/home/，然后选择要创建网关 AWS 区域 的位置。
2. 选择创建网关来打开设置网关页面。

3. 在网关设置部分，执行以下操作：

   a. 对于 Gateway name (网关名称)，输入网关的名称。创建网关后，可以搜索此名称，以便在 AWS Storage Gateway 控制台中的列表页面上找到您的网关。

   b. 对于网关时区，选择要在其中部署网关的地区的本地时区。

4. 在网关选项部分，对于网关类型，选择 Amazon FSx 文件网关。

5. 在平台选项部分中，执行以下操作：

   a. 对于主机平台，选择要在其中部署网关的平台。然后按照 Storage Gateway 控制台页面上显示的平台特定说明来设置主机平台。可从以下选项中进行选择：

      - VMware ESXi— 使用下载、部署和配置网关虚拟机 VMware ESXi。
      - Microsoft Hyper-V - 使用 Microsoft Hyper-V 下载、部署和配置网关虚拟机。
      - Linux KVM - 使用 Linux 基于内核的虚拟机（KVM）下载、部署和配置网关虚拟机。有关建议的启动配置，请参阅提供的 aws-storage-gateway .xml 文件。文件网关 2.x、Volume Gateway 3.x 和 Tape Gateway 3.x 需要禁用安全启动的 UEFI 启动模式（loader_secure=no）。
      - Amazon EC2 - 配置并启动用于托管网关的 Amazon EC2 实例。
      - 硬件设备 — 订购专用的物理硬件设备 AWS 来托管您的网关。

   b. 对于确认设置网关，选中复选框来确认您已为所选的主机平台执行部署步骤。此步骤不适用于硬件设备主机平台。

6. 现在，您的网关已设置完毕，您必须选择您想要的网关连接和通信方式 AWS。选择下一步以继续。

将您的 Amazon FSx 文件网关连接到 AWS

将新的 FSx 文件网关连接到 AWS

1. 如果您尚未完成设置 Amazon 文件网关中所述的步骤，请完成设置 Amazon FSx 文件网关中所述的步骤。完成后，选择 “下一步”，在 AWS Storage Gateway 控制台中打开 “Connect t o AWS” 页面。

2. 在终端节点选项部分中，对于服务终端节点，选择网关将用于通信的终端节点的类型 AWS。可从以下选项中进行选择：

   - 可公开访问-您的网关通过公共 AWS 互联网与之通信。如果选择此选项，请使用已启用 FIPS 的端点复选框来指定连接是否必须符合联邦信息处理标准（FIPS）。

> **Note**
>
> 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-2 验证的加密模块，请使用符合 FIPS 标准的端点。有关更多信息，请参阅美国联邦信息处理标准 (FIPS) 140-2。
> FIPS 服务端点仅在某些 AWS 区域中可用。有关更多信息，请参阅 AWS 一般参考 中的 AWS Storage Gateway 端点和配额。

- VPC 托管 — 您的网关 AWS 通过与您的虚拟私有云 (VPC) 的私有连接进行通信，从而允许您控制自己的网络设置。如果您选择此选项，则必须指定现有 VPC 端点，方法是从下拉列表中选择其 VPC 端点 ID。您还可以提供其 VPC 端点域名系统（DNS）名称或 IP 地址。

3. 在网关连接选项部分的连接选项中，选择如何向 AWS标识您的网关。可从以下选项中进行选择：

   - IP 地址 - 在相应字段中提供网关的 IP 地址。此 IP 地址必须是公开的，或者可以从您当前的网络中访问，并且您必须能够通过 Web 浏览器连接到该地址。

     您可以通过从虚拟机管理程序客户端登录到网关的本地控制台来获取网关 IP 地址，或从 Amazon EC2 实例详情页面复制网关 IP 地址。
   - 激活密钥 - 在相应字段中提供网关的激活密钥。您可以使用网关的本地控制台来生成激活密钥。如果网关的 IP 地址不可用，请选择此选项。

4. 既然您已经选择了网关的连接方式 AWS，那么您必须激活网关。选择下一步以继续。

查看设置并激活您的 Amazon FSx 文件网关

激活新的 FSx 文件网关

1. 如果尚未完成以下主题中所述的程序，请先完成这些程序：

   - 设置 Amazon FSx 文件网关
   - 将您的 Amazon FSx 文件网关连接到 AWS

   完成后，选择下一步，在 AWS Storage Gateway 控制台中打开检查并激活页面。
2. 查看页面上每个部分的初始网关详细信息。
3. 如果某个部分包含错误，请选择编辑来返回到相应的设置页面并进行更改。

> **Important**
>
> 激活网关后，您无法修改网关选项或连接设置。

4. 您已经激活了网关，现在必须进行首次配置，以便分配本地存储磁盘和配置日志记录。选择下一步以继续。

配置您的 Amazon FSx 文件网关

在新 FSx 文件网关上执行首次配置

1. 如果尚未完成以下主题中所述的程序，请先完成这些程序：

   - 设置 Amazon FSx 文件网关
   - 将您的 Amazon FSx 文件网关连接到 AWS
   - 查看设置并激活您的 Amazon FSx 文件网关

   完成后，选择下一步，在 AWS Storage Gateway 控制台中打开配置网关页面。
2. 在配置存储部分，使用下拉列表为缓存分配至少一个容量至少为 150 千兆字节（GiB）的本地磁盘。本节中列出的本地磁盘对应于您在主机平台上预配置的物理存储。
3. 在CloudWatch 日志组部分，选择如何设置 Amazon CloudWatch Logs 以监控网关的运行状况。可从以下选项中进行选择：

   - 创建新日志组：设置新的日志组来监控您的网关。
   - 使用现有的日志组：从相应的下拉列表中选择现有日志组。
   - 停用日志记录-请勿使用 Amazon CloudWatch Logs 来监控您的网关。

> **Note**
>
> 要接收 Storage Gateway 运行状况日志，日志组资源策略中必须存在以下权限。将替换*highlighted section*为您部署的特定日志组 ResourceARN 信息。

```
"Sid": "AWSLogDeliveryWrite20150319",
      "Effect": "Allow",
      "Principal": {
```

```
        "Service": [
          "delivery.logs.amazonaws.com"
        ]
      },
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:eu-west-1:1234567890:log-group:/foo/bar:log-stream:*"
```

只有在您想要将权限显式应用于单个日志组时，才需要使用“Resource”元素。

4. 在CloudWatch 警报部分，选择如何设置 Amazon CloudWatch 警报，以便在网关的指标偏离定义的限制时通知您。可从以下选项中进行选择：

   - 创建 Storage Gateway 的推荐 CloudWatch 警报-创建网关时自动创建所有推荐的警报。有关推荐警报的更多信息，请参阅了解 CloudWatch 警报。

     > **Note**
     >
     > 此功能需要 CloudWatch 策略权限，而这些权限不会作为预配置的 Storage Gateway 完全访问策略的一部分自动授予。在尝试创建推荐 CloudWatch 警报之前，请确保您的安全策略授予以下权限：
     >
     > - `cloudwatch:PutMetricAlarm` - 创建警报
     > - `cloudwatch:DisableAlarmActions` - 关闭警报操作
     > - `cloudwatch:EnableAlarmActions` - 打开警报操作
     > - `cloudwatch:DeleteAlarms` - 删除警报

   - 创建自定义警报-配置新的 CloudWatch 警报，以接收有关网关指标的通知。选择 “创建警报”，在 Amazon CloudWatch 控制台中定义指标并指定警报操作。有关说明，请参阅亚马逊 CloudWatch 用户指南中的使用亚马逊 CloudWatch 警报。
   - 无警报-请勿使用 CloudWatch 警报来接收有关网关指标的通知。

5. （可选）在标签部分，选择添加新标签，然后输入区分大小写的键值对，协助您在 AWS Storage Gateway 控制台中搜索和筛选列表页面上的网关。重复此步骤，根据需要添加任意数量的标签。

6. （可选）在验证 VMware 高可用性配置部分中，如果您的网关部署在属于 VMware 高可用性 (HA) 集群 VMware 的主机上，请选择验证 VMware HA 以测试 HA 配置是否正常工作。

> **Note**
>
> 此部分仅适用于在 VMware主机平台上运行的网关。
> 完成网关配置过程不需要执行此步骤。您可以随时测试网关的 HA 配置。验证需要几分钟时间，然后重新启动 Storage Gateway 虚拟机。

7. 选择配置来完成网关的创建。

   要查看新网关的状态，请在 AWS Storage Gateway 控制台的网关概述页面上进行搜索。

您已经创建了网关，现在必须附加一个供网关使用的文件系统。有关说明，请参阅附加 Amazon f FSx or Windows 文件服务器文件系统。

如果您没有要附加的现有 Amazon FSx 文件系统，则必须创建一个。有关说明，请参阅 Amazon 入门 FSx。

在虚拟私有云中激活网关

您可以在本地网关设备和基于云的存储基础设施之间创建私有连接。您可以使用此连接激活网关，并将其配置为无需通过公共 Internet 进行通信即可将数据传输到 AWS 存储服务。使用 Amazon VPC 服务，您可以在自定义虚拟私有云 (VPC) 中启动 AWS 资源，包括私有网络接口终端节点。您可以使用 VPC 来控制网络设置，例如 IP 地址范围、子网、路由表和网络网关。有关更多信息 VPCs，请参阅什么是 Amazon VPC？ 在《亚马逊 VPC 用户指南》中。

要在 VPC 中激活您的网关，请使用 Amazon VPC 控制台为 Storage Gateway 创建 VPC 端点并获取 VPC 端点 ID，然后在创建并激活网关时指定此 VPC 端点 ID。有关更多信息，请参阅将您的亚马逊 FSx 文件网关连接到 AWS。

要将 FSx 文件网关配置为通过 VPC 传输数据，您必须在 Amazon FSx for Windows 文件服务器 VPC 和部署网关的网络之间建立 VPN 或 AWS DirectConnect 链接。

> **Note**
>
> 您必须在为 Storage Gateway 创建 VPC 端点时所在的同一个区域内激活网关。

为 Storage Gateway 创建 VPC 端点

按照这些说明创建 VPC 终端节点。如果您已经有用于 Storage Gateway 的 VPC 端点，则可以使用该端点。

为 Storage Gateway 创建 VPC 端点

1. 登录 AWS 管理控制台 并打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints (终端节点)，然后选择 Create Endpoint (创建终端节点)。
3. 在创建端点页面上，为服务类别选择 AWS 服务。
4. 对于服务名称，选择 `com.amazonaws.region.storagegateway`。例如 `com.amazonaws.us-east-2.storagegateway`。
5. 对于 VPC，选择您的 VPC 并记录其可用区和子网。
6. 确认未选中启用 DNS 名称。
7. 对于 Security group (安全组)，选择您要用于 VPC 的安全组。您可以接受默认安全组。验证在您的安全组中已经允许了以下所有的 TCP 端口：
   - TCP 443
   - TCP 1026
   - TCP 1027
   - TCP 1028
   - TCP 1031
   - TCP 2222
8. 选择创建端点。终端节点的初始状态为 pending (待处理)。创建终端节点时，记下您刚创建的 VPC 终端节点的 ID。
9. 在创建终端节点时，选择 Endpoints (终端节点)，然后选择新的 VPC 终端节点。
10. 在所选存储网关端点的详细信息选项卡中，在 DNS 名称下，使用第一个未指定可用区的 DNS 名称。您的 DNS 名称应类似于以下示例：`vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

现在，有了 VPC 端点，您可以创建并激活网关。有关更多信息，请参阅创建和激活 Amazon FSx 文件网关。

有关获取激活密钥的信息，请参阅获取网关的激活密钥。

配置 Microsoft Active Directory 域访问设置

在此步骤中，您将配置访问设置以将您的亚马逊 FSx 文件网关加入微软活动目录域。

要配置 Active Directory 设置，请执行以下操作：

1. 在 Storage Gateway 控制台中，从导航菜单中选择FSx 文件系统。
2. 选择 “附加 FSx 文件系统”。
3. 在确认网关页面上，从下拉菜单中选择要加入 Active Directory 域的网关。

   如果您没有网关，则必须创建一个。确保您的网关可以解析 Active Directory 域控制器的名称。有关信息，请参阅先决条件。
4. 输入 Active Directory 设置的值：

   > **Note**
   >
   > 如果您的网关已加入域，则无需再次加入。继续执行下一步。

   - 在域名中，输入您要使用的 Active Directory 的域名。
   - 在域用户中，输入您要用于将网关加入域的 Active Directory 用户名。此用户必须具有必要的权限。有关更多信息，请参阅 Active Directory 服务账户权限要求。
   - 在域密码中，输入该用户的密码。
   - 在组织单元（可选）中，您可以指定 Active Directory 所属的组织单元。

     > **Note**
     >
     > 如果将此字段留空，则加入域将在默认计算机容器（不是 OU）中创建一个 Active Directory 计算机账户，并使用网关的网关 ID 作为账户名（例如，SGW-1234ADE）。此账户的名称无法自定义。
     > 如果您的 Active Directory 环境要求您预先创建账户以简化加入域的流程，则需要提前创建此账户。
     > 如果您的 Active Directory 环境为新的计算机对象指定了 OU，则在加入域时必须指定该 OU。

   - 输入域控制器（可选）的值。

5. 选择 “下一步” 打开 “附加 FSx 文件系统” 页面。

下一步

附上 Amazon FSx for Windows 文件服务器文件系统

附上 Amazon FSx for Windows 文件服务器文件系统

必须先拥有 FSx 适用于 Windows 的文件服务器文件系统，然后才能将其连接到 FSx 文件网关。如果没有文件系统，则必须创建一个文件系统。有关说明，请参阅《亚马逊 FSx Windows 文件服务器用户指南》中的 “步骤 1：创建您的文件系统”。

下一步是将 Amazon FSx 文件系统连接到网关。当您连接 Amazon FSx 文件系统时，文件系统上的所有文件共享都可供亚马逊 FSx 文件网关（FSx 文件网关）供您装载。

> **Note**
>
> 从 Amazon File Gateway 写入亚马逊 FSx 文件系统时，存在以下限制： FSx
>
> - 您的 Amazon FSx 文件系统和 FSx 文件网关必须归他们所有， AWS 账户 并且位于同一个文件系统中 AWS 区域。
> - 每个网关最多可以支持五个附加的文件系统。连接文件系统时，如果所选网关已满，Storage Gateway 控制台会发出通知。在这种情况下，必须先选择其他网关或分离文件系统，然后才能连接另一个网关。
> - FSx File Gateway 支持软存储配额（当用户超过其数据限制时会向您发出警告），但不支持硬配额（通过拒绝写入访问来强制执行数据限制）。除 Amazon FSx 管理员用户外，所有用户均支持软配额。有关设置存储配额的更多信息，请参阅 Amazon FSx 用户指南中的存储配额。
> - 我们不建议使用 Microsoft 分布式文件系统 (DFS) 通过文件网关将用户重定向到您的亚马逊 FSx FSx 文件系统。相反，请将 DFS 配置为直接重定向到亚马逊 FSx 文件系统， AWS 云如亚马逊版 Windows 文件服务器用户指南中使用 DFS 命名空间对多个文件系统 FSx 进行分组中所述。

附加 Amazon FSx 文件系统

1. 在 Storage Gateway 控制台FSx 的文件系统 > 附加 FSx 文件系统页面上，填写FSx 文件系统设置部分中的以下字段：
   - 在FSx 文件系统名称中，从下拉列表中选择要附加的文件系统。
   - 对于本地端点 IP 地址，请输入客户端用于浏览文件系统上文件共享的 FSx 网关 IP 地址。

> **Note**
>
> - 必须为挂载到网关的每个文件系统指定 IP 地址。
> - 对于 Amazon EC2 网关，您可以指定 EC2 实例的私有 IP 地址，除非该地址已被其他文件系统使用，在这种情况下，您必须向网关添加新的私有地址，然后重启网关。有关更多信息，请参阅 Amazon EC2 用户指南中的多个 IP 地址。
> - 对于本地网关，您可以指定主网络接口（静态或 DHCP）的 IP 地址，除非该接口已被其他文件系统使用。如果已被其他文件系统使用，则必须提供与主接口位于同一子网中的另一个 IP 地址，该地址将作为虚拟 IP 地址提供。请勿使用分配给主接口以外任何网络接口的 IP 地址。

2. 在服务账户设置部分，提供与 Amazon FSx 文件系统关联的服务账户登录凭证。

> **Note**
>
> 此服务账户必须拥有与您的 Amazon FSx 文件系统关联的 Active Directory 服务的备份操作员权限或具有同等权限。

> **Important**
>
> 为了确保对文件、文件夹和文件元数据具有足够的权限，建议您将此服务账户设置为文件系统管理员组的成员。
> 如果你使用 AWS Directory Service 的是 Microsoft Active Directory 和 Amazon FSx for Windows 文件服务器，则服务账户必须是 AWS 授权 FSx 管理员组的成员。
> 如果您在 Amazon FSx for Windows 文件服务器上使用自行管理的 Active Directory，我们建议该服务账户成为您在创建亚马逊文件系统时为文件系统管理指定的自定义委托 FSx 文件系统管理员组的成员。
> 如果您在创建 Amazon 文件系统时选择不创建自定义委派 FSx 文件系统管理员组，则默认组为域管理员。虽然您可以将服务账户添加到此组，但这并非最佳实践，因此不建议这样做。
> 有关更多信息，请参阅《亚马逊版 Windows 文件服务器用户指南》中的 “向您的亚马逊 FSx FSx 服务账户委派权限”。

3. 在审核日志部分，选择现有日志组，然后选择要用于监控对您的 Amazon FSx 文件系统的访问的日志。您也可以创建新的日志组。如果您不想监控系统，请选择禁用日志记录。

4. 对于自动缓存刷新设置，如果您希望缓存自动刷新，请选择设置刷新间隔，并指定 5 分钟到 30 天之间的间隔。
5. （可选）在标签部分，选择添加新标签，可添加一个或多个密钥和值来标记您的设置。
6. 选择 Next（下一步），然后查看设置。您可以在每个部分中选择编辑来更改设置。
7. 完成后，选择 Finish。

下一步

挂载并使用您的 Amazon FSx 文件共享

挂载并使用您的 Amazon FSx 文件共享

在将文件共享挂载到客户端之前，请等待 Amazon FSx 文件系统的状态变为 “可用”。挂载文件共享后，您可以开始使用您的 Amazon FSx 文件网关（FSx 文件网关）。

主题

- 在客户端上挂载您的 SMB 文件共享
- 测试您的 FSx 文件网关

在客户端上挂载您的 SMB 文件共享

在该步骤中，您挂载 SMB 文件共享并将其映射到客户端可访问的驱动器。控制台的文件网关部分显示可用于 SMB 客户端的受支持挂载命令。接下来，您可以尝试一些其他选项。

您可以使用几种不同的方法来挂载 SMB 文件共享，包括：

- `net use` 命令：在系统重启之后不复存在，除非您使用 `/persistent:(yes:no)` 开关。
- `CmdKey` 命令行实用程序：创建到已挂载 SMB 文件共享（在重启后保留）的持久性连接。
- 在文件浏览器中映射的网络驱动器：将已挂载文件共享配置为在登录时重新连接并要求您输入网络凭证。
- PowerShell script-可以是永久性的，并且在装载时可以对操作系统可见或不可见。

> **Note**
>
> 如果您是 Microsoft Active Directory 用户，请咨询您的管理员以确保您在将 SMB 文件共享挂载到本地系统之前有权访问该文件共享。
> Amazon FSx File Gateway 不支持 SMB 锁定或 SMB 扩展属性。

使用 net use 命令为 Active Directory 用户挂载 SMB 文件共享

1. 在将 SMB 文件共享挂载到本地系统之前确保您有权访问该文件共享。
2. 对于 Microsoft Active Directory 客户端，请在命令提示符中输入以下命令：

```
net use [WindowsDriveLetter]: \\[Gateway IP Address]\[Name of the share on the FSx file system]
```

要在 Windows 上装载 SMB 文件共享，请使用以下命令 CmdKey

1. 按下 Windows 键并键入 **cmd** 以查看命令提示符菜单项。
2. 打开命令提示符的上下文（右键单击）菜单，然后选择以管理员身份运行。
3. 输入以下命令：

```
C:\>cmdkey /add:[Gateway VM IP address] /user:[DomainName]\[UserName] /
pass:[Password]
```

> **Note**
>
> 挂载文件共享时，您可能需要在客户端重启后重新挂载文件共享。

使用 Windows File Explorer 挂载 SMB 文件共享

1. 按下 Windows 键并在搜索 Windows 框中输入 **File Explorer**，或者按 **Win+E**。
2. 在导航窗格中选择这台电脑。然后，在计算机选项卡上，选择映射网络驱动器。
3. 在映射网络驱动器对话框中，为驱动器选择驱动器号。
4. 对于文件夹，输入 *****[File Gateway IP]****[SMB File Share Name]**，或者选择浏览以从对话框中行您的 SMB 文件共享。
5. （可选）如果您希望挂载点在重启后保留，请选择登录时重新连接。
6. （可选）如果您希望用户输入 Active Directory 登录或来宾账户用户密码，请选择使用其他凭证连接。
7. 选择完成以完成您的挂载点。

测试您的 FSx 文件网关

您可以将文件和目录复制到映射的驱动器。这些文件会自动上传到你 FSx 的 Windows 文件服务器文件系统。

将文件从 Windows 客户端上传到亚马逊 FSx

1. 在 Windows 客户端上，导航到您已挂载文件共享的驱动器。驱动器名称前面是您的文件系统名称。
2. 将文件或目录复制到驱动器。

> **Note**
>
> 文件网关不支持在文件共享上创建硬链接或符号链接。

管理您的 Amazon FSx 文件网关资源

以下各节提供有关如何管理您的亚马逊 FSx 文件网关（文件网关）资源的信息，包括连接和分离亚马逊FSx FSx 文件系统以及配置 Microsoft Active Directory 设置。

主题

- 了解网关状态
- 了解文件系统状态
- 编辑 FSx 文件网关的基本信息
- 设置网关的安全级别
- 编辑 FSx 文件网关的活动目录设置
- 编辑 Amazon FSx 文件系统的设置
- 断开 Amazon FSx 文件系统

了解网关状态

AWS Storage Gateway 部署中的每个网关都有一个关联状态，可以一目了然地告诉你网关的运行状况。大多数情况下，该状态表示网关运行正常，无需您采取任何措施。在某些情况下，状态指示有问题，可能需要您执行相关操作，也可能不需要。

您可以在 Storage Gateway 控制台的网关页面上查看部署中每个网关的状态。网关状态显示在网关名称旁边的状态栏中。运行正常的网关状态为 RUNNING。

下表列出了每个网关状态的说明，以及您是否应该根据该状态采取相应措施。网关在使用期间应始终或大部分时间保持 RUNNING 状态。

Status	含义
RUNNING	网关配置正确，可供使用。
OFFLINE	网关可能由于以下一个或多个原因处于 OFFLINE 状态： • 网关无法到达 Storage Gateway 服务端点。 • 网关意外关闭。 • 网关关联的缓存磁盘已断开连接、已被修改或发生故障。

了解文件系统状态

您可以通过查看文件系统的状态来快速了解其运行状况。如果状态显示文件系统运行正常，则无需您采取任何操作。如果状态显示存在问题，您可以进行调查以确定是否需要采取措施。

您可以在 Storage Gateway 控制台的状态栏中查看文件系统的状态。运行正常的文件系统状态显示为“可用”。大多数情况下，都应处于此状态。

下表列出了文件共享状态、其含义以及是否需要采取措施。

Status	含义
AVAILABLE	文件系统已正确配置，可供使用。这是文件系统正常运行的标准状态。
CREATING	文件系统尚未完全创建，尚不可用。CREATING (正在创建) 状态是过渡型状态。无需采取行动。如果文件系统停留在此状态，则可能是因为网关 VM 断开了与的连接 AWS。
UPDATING	文件系统配置正在更新。“正在更新”状态为过渡状态。无需采取行动。如果文件系统陷入这种状态，则可能是因为网关 VM 断开了与的连接 AWS。
DELETING	正在删除文件系统。只有将所有数据上传到，才会删除文件系统 AWS。DELETING 状态是过渡型状态，无需执行任何操作。
FORCE_DELETING	正在强制删除文件系统。文件系统会立即删除，数据不会上传到 AWS。FORCE_DELETING 状态是过渡性质的，无需执行任何操作。
ERROR	文件系统处于不佳状态。需要执行操作。可能的原因包括访问凭证或权限问题、连接问题或文件系统存储空间不足。在解决导致状态不佳的问题后，文件系统将恢复到 AVAILABLE 状态。

编辑 FSx 文件网关的基本信息

您可以使用 Storage Gateway 控制台编辑现有网关的基本信息，包括网关名称、时区和 CloudWatch 日志组。

编辑现有网关的基本信息

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 选择网关，然后选择要为其编辑基本信息的网关。
3. 从操作下拉菜单中，选择编辑网关信息。
4. 对于 Gateway name (网关名称)，输入网关的名称。可以搜索此名称，以便在 Storage Gateway 控制台中的列表页面上找到您的网关。

   > **Note**
   >
   > 网关名称必须介于 2 到 255 个字符之间，并且不能包含斜杠（\ 或 /）。
   > 更改网关名称将断开为监控网关而设置的所有 CloudWatch 警报。要重新连接警报，请在 CloudWatch控制台中GatewayName更新每个警报的。

5. 对于网关时区，选择要在其中部署网关的地区的本地时区。
6. 在选择如何设置日志组中，选择如何设置 Amazon L CloudWatch ogs 以监控网关的运行状况。可从以下选项中进行选择：
   - 创建新日志组：设置新的日志组来监控您的网关。
   - 使用现有的日志组：从相应的下拉列表中选择现有日志组。
   - 停用日志记录-请勿使用 Amazon CloudWatch Logs 来监控您的网关。
7. 完成修改要更改的设置时，选择保存更改。

设置网关的安全级别

您可以为 FSx 文件网关配置 SMB 安全级别，以指定网关是需要服务器消息块 (SMB) 签名还是 SMB 加密。

配置安全级别

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 选择网关，然后选择要编辑其 SMB 设置的网关。
3. 从操作下拉菜单中，选择编辑 SMB 设置，然后选择 SMB 安全设置。
4. 对于 Security level (安全级别)，请选择下列选项之一：

> **Note**
>
> 有关使用 API 配置此设置的信息，请参阅 AWS AP AWS Storage Gateway I 参考中的更新SMBSecurity策略。
> 较高的安全级别可能会影响性能。

- 强制加密-如果选择此选项，则 FSx 文件网关仅允许来自使用 256 位 AES 加密算法的 SMBv3 客户端的连接。不允许 128 位算法。对于处理敏感数据的环境，建议使用此选项。此选项适用于 Microsoft Windows 8、Windows Server 2012 或更高版本上的 SMB 客户端。
- 强制加密-如果选择此选项， FSx File Gateway 将仅允许来自已开启加密的 SMBv3 客户端进行连接。允许 256 位和 128 位算法。对于处理敏感数据的环境，建议使用此选项。此选项适用于 Microsoft Windows 8、Windows Server 2012 或更高版本上的 SMB 客户端。
- 强制签名-如果选择此选项， FSx File Gateway 仅允许来自 SMBv2 或已开启签名的 SMBv3 客户端的连接。此选项适用于 Microsoft Windows Vista、Windows Server 2008 或更高版本上的 SMB 客户端。

> **Note**
>
> FSx 文件网关的默认安全级别为强制加密。

5. 选择保存。

编辑 FSx 文件网关的活动目录设置

要使用您的公司 Microsoft Active Directory 或 AWS Managed Microsoft AD 通过用户身份验证访问您的亚马逊 FSx 文件系统，请编辑网关的 SMB 设置并提供您的 Active Directory 域凭证。这样做可以使网关加入 Active Directory 域并允许该域的成员访问文件系统。

> **Note**
>
> 使用 Directory Service，您可以在中创建托管的 Active Directory 域服务 AWS 云。
> 要 AWS Managed Microsoft AD 与 Amazon EC2 网关一起使用，您必须在与相同的 VPC 中创建 Amazon EC2 实例 AWS Managed Microsoft AD，将 _workspaceMembers 安全组添加到 Amazon EC2 实例，然后使用中的管理员证书加入 AD 域。 AWS Managed Microsoft AD

有关的更多信息 AWS Managed Microsoft AD，请参阅《AWS Directory Service 管理指南》。
有关 Amazon EC2 的更多信息，请参阅 Amazon Elastic Compute Cloud 文档。

开启 Active Directory 身份验证

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 选择网关，然后选择要编辑其 SMB 设置的网关。
3. 从操作下拉菜单中，选择编辑 SMB 设置，然后选择Active Directory 设置。
4. 在域名中，输入您希望网关加入的 Active Directory 域的名称。

   Note

   当网关从未加入域时，Active Directory status (Active Directory 状态) 显示 Detached (已分离)。
   您的 Active Directory 服务账户必须具有必要的权限。有关更多信息，请参阅 Active Directory 服务账户权限要求。
   加入域会在默认计算机容器（不是 OU）中创建一个 Active Directory 计算机账户，并使用网关的网关 ID 作为账户名（例如，SGW-1234ADE）。此账户的名称无法自定义。
   如果您的 Active Directory 环境要求您预先创建账户以简化加入域的流程，则需要提前创建此账户。
   如果您的 Active Directory 环境为新的计算机对象指定了 OU，则在加入域时必须指定该 OU。
   如果您的网关无法加入 Active Directory 目录，请尝试使用 JoinDomainAPI 操作使用该目录的 IP 地址加入。
5. 在域用户和域密码中，输入网关用于加入域的 Active Directory 服务账户的凭证。
6. （可选）对于组织单元（OU），输入您的 Active Directory 用于新计算机对象的指定 OU。
7. （可选）对于域控制器 (DC)，输入一个或多个 DCs 网关用于连接到 Active Directory 的名称。您可以输入多个 DCs 以逗号分隔的列表。您可以将此字段留空以允许 DNS 自动选择 DC。
8. 选择保存更改。

编辑 Amazon FSx 文件系统的设置

创建 Amazon FSx for Windows 文件服务器文件系统后，您可以编辑 CloudWatch 日志、自动缓存刷新和亚马逊 FSx 服务账户凭证的设置。

编辑 Amazon FSx 文件系统设置

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在导航窗格中，选择文件系统，然后选择要编辑其设置的文件系统。
3. 在操作中，选择编辑文件系统设置。
4. 在文件系统设置部分，验证网关、Amazon FSx 位置和 IP 地址信息。

   > **Note**
   >
   > 将文件系统的 IP 地址附加到网关后，您就无法对其进行编辑。要更改 IP 地址，必须断开并重新连接文件系统。

5. 在审核日志部分，选择一个选项以使用 CloudWatch日志组来监控对 Amazon FSx 文件系统的访问。您也可以使用现有日志组。
6. 对于自动缓存刷新设置，请选择一个选项。如果选择设置刷新间隔，您可以使用生存时间（TTL）设置刷新文件系统缓存的时间（以天、小时和分钟为单位）。

   TTL 指的是自上次刷新以来的时间长度。在该时间段之后访问该目录时，文件网关会从 Amazon FSx 文件系统刷新该目录的内容。

   > **Note**
   >
   > 有效的刷新间隔值介于 5 分钟到 30 天之间。

7. 在服务账户设置（可选）部分，输入用户名和密码。这些证书适用于具有与您的亚马逊 FSx 文件系统关联的 Active Directory 服务中的 Backup 管理员角色的用户。
8. 选择保存更改。

断开 Amazon FSx 文件系统

在 Windows 文件服务器中 FSx ，分离文件系统并不会删除您的数据。在分离文件系统之前写入这些文件系统的数据仍会上传到你的 Window FSx s 文件服务器。

断开 Amazon FSx 文件系统

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。

2. 选择FSx 文件系统，然后选择一个或多个要分离的文件系统。
3. 在操作中，选择分离文件系统。此时会显示确认对话框。
4. 确认要分离指定的文件系统，然后在确认框中键入分离，并选择分离。

监控 Storage Gateway

本节中的主题介绍如何使用 Amazon 监控网关 CloudWatch，包括监控缓存存储空间和其他与网关关联的资源。使用 Storage Gateway 控制台来查看网关的指标和警报。例如，您可以查看读取和写入操作中使用的字节数、读取和写入操作所花费的时间以及从 AWS 云端检索数据所花费的时间。借助指标，您可以跟踪网关的运行状况并设置警报，以便在一个或多个指标超出定义的阈值时通知您。

Storage Gateway 免费提供 CloudWatch 指标。记录为期两周的 Storage Gateway 指标。通过使用这些指标，您可以访问历史信息并更好地了解您的网关的表现。Storage Gateway 还提供 CloudWatch 警报，但高分辨率警报除外，无需额外付费。有关 CloudWatch 定价的更多信息，请参阅 Amazon CloudWatch 定价。有关的更多信息 CloudWatch，请参阅 Amazon CloudWatch 用户指南。

主题

- 了解 CloudWatch 警报-了解有关 CloudWatch 警报的基本信息，包括警报状态和推荐配置。
- 创建推荐的 CloudWatch 警报-了解如何在 File Gateway 初始设置过程中快速自动配置所有推荐的 CloudWatch 警报。
- 创建自定义 CloudWatch警报-了解如何创建自定义 CloudWatch 警报，使用特定的评估标准来监控特定指标，从而触发警报状态并发送通知。
- 监控您的 文件网关-了解如何查看 CloudWatch 日志和审核日志，并查找有关网关报告的特定网关和文件共享文件系统指标的信息。

了解 CloudWatch 警报

CloudWatch 警报根据指标和表达式监控有关您的网关的信息。您可以为网关添加 CloudWatch 警报并在 Storage Gateway 控制台中查看其状态。有关用于监控 的指标的更多信息，请参阅了解网关指标和了解文件系统指标。对于每个警报，您可以指定将激活其“警报”状态的条件。当处于“警报”状态时，Storage Gateway 控制台中的警报状态指示符会变成红色，便于您主动监控状态。您可以将警报配置为根据状态的持续变化自动调用操作。有关 CloudWatch 警报的更多信息，请参阅亚马逊 CloudWatch 用户指南中的使用亚马逊 CloudWatch警报。

> **Note**
>
> 如果您没有查看权限 CloudWatch，则无法查看警报。

对于每个激活的网关，我们建议您创建以下 CloudWatch 警报：

- 高 IO 等待：在 15 分钟内对于 3 个数据点，`IoWaitpercent` >= 20
- 缓存脏百分比：在 20 分钟内对于 4 个数据点，`CachePercentDirty` > 80
- 文件上传失败：在 5 分钟内对于 1 个数据点，`FilesFailingUpload` >= 1
- 文件系统错误：在 5 分钟内对于 1 个数据点，`FileSystem-ERROR` >= 1
- 运行状况通知：在 5 分钟内对于 1 个数据点，`HealthNotifications` >= 1。配置此警报时，请将缺少数据处理设置为 notBreaching。

> **Note**
>
> 仅当网关在 CloudWatch 中有先前的运行状况通知时，才能设置运行状况通知警报。

对于属于 VMware 高可用性集群 VMware 的主机平台上的网关，我们还建议使用此额外 CloudWatch 警报：

- 可用性通知：在 5 分钟内对于 1 个数据点，`AvailabilityNotifications` >= 1。配置此警报时，请将缺少数据处理设置为 notBreaching。

下表描述了 CloudWatch 警报状态。

州	说明
确定	指标或表达式在定义的阈值范围内。
警报	指标或表达式超出定义的阈值。
数据不足	警报刚启动，指标不可用，或指标数据不足以判断警报状态。
无	不会为网关创建警报。要创建新警报，请参阅为您的网关创建自定义 CloudWatch 警报。
Unavailable	警报状态是未知的。选择 Unavailable (不可用) 以查看 Monitoring (监控) 选项卡中的错误信息。

为您的网关创建推荐的 CloudWatch 警报

使用 Storage Gateway 控制台创建新网关时，可以选择在初始设置过程中自动创建所有推荐的 CloudWatch 警报。有关更多信息，请参阅配置您的亚马逊 FSx 文件网关。如果您想在首次完成设置后为现有网关添加或更新推荐的 CloudWatch 警报，请使用以下步骤。

为现有网关添加或更新推荐的 CloudWatch 警报

> **Note**
>
> 此功能需要 CloudWatch 策略权限，而这些权限不会作为预配置的 Storage Gateway 完全访问策略的一部分自动授予。在尝试创建推荐 CloudWatch 警报之前，请确保您的安全策略授予以下权限：
>
> - `cloudwatch:PutMetricAlarm` - 创建警报
> - `cloudwatch:DisableAlarmActions` - 关闭警报操作
> - `cloudwatch:EnableAlarmActions` - 打开警报操作
> - `cloudwatch:DeleteAlarms` - 删除警报

1. 在家中打开 Storage Gateway 控制台 https://console.aws.amazon.com/storagegateway//。
2. 在页面左侧的导航窗格中，选择 Gateways，然后选择要为其创建推荐 CloudWatch 警报的网关。
3. 在网关的详细信息页面上，选择监控选项卡。
4. 在警报下，选择创建推荐警报。自动创建推荐的警报。

   警报部分列出了特定网关的所有 CloudWatch 警报。在这里，您可以选择和删除一个或多个警报、打开或关闭警报操作以及创建新的警报。

为您的网关创建自定义 CloudWatch 警报

CloudWatch 使用亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 在警报状态发生变化时发送警报通知。警报会监控您指定的一段时间内的一个指标，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。操作是向 Amazon SNS 主题发送的通知。您可以在创建警报时创建 Amazon SNS 主题。 CloudWatch 有关 Amazon SNS 的更多信息，请参阅《Amazon Simple Notification Service 开发人员指南》中的什么是 Amazon SNS？

在 Storage Gateway 控制台中创建 CloudWatch 警报

1. 在家中打开 Storage Gateway 控制台 https://console.aws.amazon.com/storagegateway//。
2. 在导航窗格中，选择网关，然后选择要为其创建警报的网关。
3. 在网关详细信息页面上，选择监控选项卡。
4. 在 “警报” 下，选择 “创建警报” 以打开 CloudWatch 控制台。
5. 使用 CloudWatch 控制台创建所需的警报类型。您可以创建下列类型的警报：

   - 静态阈值警报：基于所选指标的设定阈值的警报。当指标在指定数量的评估周期内突破阈值时，警报将变为“警报”状态。

     要创建静态阈值警报，请参阅 Amazon CloudWatch 用户指南中的基于静态阈值创建 CloudWatch 警报。
   - 异常检测警报：异常检测挖掘过去的指标数据并创建预期值模型。您可以为异常检测阈值设置一个值，然后在模型中 CloudWatch 使用该阈值来确定该指标的 “正常” 值范围。阈值越高，所产生的“正常”值的范围越大。您可以选择仅当指标值高于预期值范围、低于预期值范围，或出现二者情况之一时激活警报。

     要创建异常检测警报，请参阅 A mazon CloudWatch 用户指南中的基于异常检测创建 CloudWatch 警报。
   - 指标数学表达式警报：基于数学表达式中使用的一个或多个指标的警报。您指定表达式、阈值和评估期。

     要创建指标数学表达式警报，请参阅 Amazon CloudWatch 用户指南中的基于指标数学表达式创建 CloudWatch 警报。
   - 复合警报：通过监控其他警报的警报状态来确定其警报状态的警报。复合警报可以帮助您降低警报噪音。

     要创建复合警报，请参阅 Amazon CloudWatch 用户指南中的创建复合警报。
6. 在 CloudWatch 控制台中创建警报后，返回到 Storage Gateway 控制台。您可以通过执行以下操作之一查看警报：

   - 在导航窗格中，选择网关，然后选择要查看其警报的网关。在详细信息选项卡的警报下，选择CloudWatch 警报。
   - 在导航窗格中，选择网关，选择要查看其警报的网关，然后选择监控选项卡。

警报部分列出了特定网关的所有 CloudWatch 警报。在这里，您可以选择和删除一个或多个警报、打开或关闭警报操作以及创建新的警报。

- 在导航窗格中，选择网关，然后选择要查看其警报的网关的警报状态。

有关如何编辑或删除警报的信息，请参阅编辑或删除 CloudWatch 警报。

> **Note**
>
> 当您使用 Storage Gateway 控制台删除网关时，与该网关关联的所有 CloudWatch 警报也会自动删除。

监控您的 文件网关

您可以使用 文件网关和中的相关资源。您还可以使用 “ CloudWatch 事件” 在文件操作完成后收到通知。

主题

- 使用日志组获取 文件网关运行状况日志 CloudWatch
- 使用亚马逊 CloudWatch 指标
- 了解网关指标
- 了解文件系统指标
- 了解 关审核日志

使用日志组获取 文件网关运行状况日志 CloudWatch

您可以使用 Amaz CloudWatch on Logs 来获取有关 和相关资源运行状况的信息。您可以使用日志来监控网关遇到的错误。此外，您还可以使用 Amazon CloudWatch 订阅筛选器实时自动处理日志信息。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的通过订阅实时处理日志数据。

例如，您可以配置一个 CloudWatch 日志组来监控您的网关，并在文件网关无法将 FSx 文件上传到 Amazon FSx 文件系统时收到通知。您可以在激活网关时或在激活网关并运行后配置组。有关如何在激活网关时配置 CloudWatch 日志组的信息，请参阅 配置您的 Amazon FSx 文件网关。有关 CloudWatch 日志组的一般信息，请参阅 Amazon CloudWatch 用户指南中的使用日志组和日志流。

有关如何对 可能报告的错误进行故障排除的信息，请参阅故障排除：文件网关问题。

在网关激活后配置 CloudWatch 日志组

以下过程说明如何在激活网关后配置 CloudWatch 日志组。

配置 CloudWatch 日志组以与您的 配合使用

1. 登录 AWS 管理控制台 并在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在导航窗格中，选择 Gateways，然后选择要为其配置 CloudWatch 日志组的网关。
3. 对于操作，选择编辑网关信息。
4. 对于选择如何设置日志组，选择以下选项之一：

   - 创建新的日志组以创建新的 CloudWatch日志组。
   - 使用现有日志组使用已存在的 CloudWatch 日志组。

     从现有日志组列表中选择一个日志组。
   - 如果您不想使用@@ 日志组监控网关，请停用 CloudWatch 日志记录。
5. 选择保存更改。
6. 要查看网关的运行状况日志，请执行以下操作：

   1. 在导航窗格中，选择 Gateways，然后选择您为其配置 CloudWatch 日志组的网关。
   2. 选择 “详细信息” 选项卡，然后在 “Healt h Logs” 下，选择 “CloudWatch日志”。日志组详细信息页面将在 CloudWatch 控制台中打开。

使用亚马逊 CloudWatch 指标

您可以使用 AWS 管理控制台 或 CloudWatch API 获取 文件网关的监控数据。控制台根据来自 CloudWatch API 的原始数据显示一系列图表。该 CloudWatch API 也可以通过其中一个AWS SDKs或 Amazon CloudWatch API 工具来使用。根据您的需求差异，您可能倾向于使用控制台中显示的图表，也可能倾向于检索自 API 的图表。

无论通过何种方法来使用指标，您都必须指定下列信息：

- 要使用的指标维度。维度 是帮助您对某指标进行唯一标识的名称/值对。Storage Gateway 的维度为 `GatewayId` 和 `GatewayName`。在 CloudWatch 控制台中，您可以使用`Gateway Metrics`视图来选择网关特定的维度。有关尺寸的更多信息，请参阅 Amazon CloudWatch 用户指南中的尺寸。
- 指标名称，如 `ReadBytes`。

下表总结了可供您使用的 Storage Gateway 指标数据的类型。

Amazon CloudWatch 命名空间	维度	说明
AWS/StorageGateway	GatewayId，GatewayName	这些维度筛选描述网关各个方面的指标数据。您可以通过指定和GatewayName 维度来识别要使用的 文件网关。GatewayId 网关的吞吐量和延迟数据基于网关中的所有文件共享。 数据在 5 分钟期间内自动可用，无需收费。

网关和文件指标的使用方式类似于其他服务指标。您可以在下面所列的 CloudWatch 文档中找到一个有关某些最常见的指标任务的讨论：

- 查看可用指标
- 获取指标的统计数据
- 创建 CloudWatch 警报

了解网关指标

下表描述了涵盖 FSx 文件网关的指标。每个网关均有与其关联的一组指标。某些特定于网关的指标与某些指标同名。 file-system-specific这些指标代表同类度量，但其范围限于网关，而不是用于文件系统。

在使用特定指标前，始终指定是要处理网关还是文件系统。具体而言，在使用网关指标时，必须为要查看其指标数据的网关指定 Gateway Name。有关更多信息，请参阅 使用亚马逊 CloudWatch 指标。

> **Note**
>
> 某些指标仅在最近的监控期内生成了新数据时才会返回数据点。

下表描述了可用于获取有关 的信息的指标。

指标	说明
AvailabilityNotifications	此指标报告了网关在报告期内生成的与可用性相关的运行状况通知的数量。 单位：计数
CacheDirectorySize	此指标用于跟踪网关缓存中文件夹的大小。文件夹大小根据其第一级中包含的文件和子文件夹的数量来确定，不会递归地统计子文件夹中的内容。 使用此指标和 Average 统计数据来衡量网关缓存中文件夹的平均大小。使用此指标和 Max 统计数据来衡量网关缓存中文件夹的最大大小。 单位：计数
CacheFileSize	此指标用于跟踪网关缓存中文件的大小。 使用此指标和 Average 统计数据来衡量网关缓存中文件的平均大小。使用此指标和 Max 统计数据来衡量网关缓存中文件的最大大小。 单位：字节
CacheFree	此指标报告网关缓存中的可用字节数。 单位：字节
CacheHitPercent	在来自网关的应用程序读取操作中，由缓存提供的操作所占百分比。样本在报告周期结束时采用。 当网关没有收到任何应用程序读取操作时，此指标会报告为 100%。 单位：百分比

指标	说明
CachePercentDirty	网关缓存中尚未持久化的总体百分比。 AWS样本在报告周期结束时采用。 单位：百分比
CachePercentUsed	使用的网关缓存存储的总体百分比。样本在报告周期结束时采用。 单位：百分比
CacheUsed	此指标报告网关缓存中的已用字节数。 单位：字节
CloudBytesDownloaded	在报告期内，网关从中 AWS 下载的总字节数。 将此指标与 Sum 统计数据结合使用可测量吞吐量，将其与 Samples 统计数据结合使用可测量 IOPS。 单位：字节
CloudBytesUploaded	网关在报告期内上传到的 AWS 总字节数。 将此指标与Sum统计数据结合使用以衡量吞吐量，将此指标与Samples统计数据结合使用以衡量每秒 input/output 操作数 (IOPS)。 单位：字节
FilesFailingUpload	此指标跟踪未能上传到 AWS的文件数。这些文件将生成运行状况通知，其中包含有关该问题的更多信息。 将此指标与 Sum 统计数据结合使用，可以显示当前无法上传到 AWS的文件数。 单位：计数

指标	说明
FileShares	此指标报告网关上的文件共享数量。 单位：计数
FileSystem-ERROR	此指标提供了此网关上处于“错误”状态的文件系统关联数量。 如果此指标报告任何文件系统关联处于“错误”状态，则网关很可能存在问题，这可能会导致工作流中断。建议在此指标报告非零值时创建警报。 单位：计数
HealthNotifications	此指标报告了此网关在报告期内生成的运行状况通知的数量。 单位：计数
IndexEvictions	此指标报告从文件元数据的缓存索引中移出其元数据以便为新条目腾出空间的文件数。网关维护此元数据索引，该索引是根据需要从 AWS 云端填充的。 单位：计数
IndexFetches	此指标报告已提取元数据的文件数。网关维护文件元数据的缓存索引，该索引是根据需要从 AWS 云端填充的。 单位：计数
IoWaitPercent	此指标报告 CPU 等待本地磁盘返回响应所花费的时间占总时间的百分比。 单位：百分比
MemTotalBytes	此指标报告网关上的总内存量。 单位：字节

指标	说明
MemUsedBytes	此指标报告网关上的已用内存量。 单位：字节
RootDiskFreeBytes	此指标报告网关的根磁盘上的可用字节数。 如果此指标报告的空闲空间少于 20 GB，则应增加根磁盘的大小。 要增加根磁盘的大小，可以增加 VM 上现有根磁盘的大小。当 VM 重新启动时，网关会识别根磁盘上增加的大小。 单位：字节
SmbV2Sessions	该指标报告网关上处于活动状态的 SMBv2 会话数。此指标会为与网关关联的每个文件系统分别发出一次。使用 SUM 统计数据计算所有文件系统的活动 SMBv2 会话总数。 单位：计数
SmbV3Sessions	该指标报告网关上处于活动状态的 SMBv3 会话数。此指标会为与网关关联的每个文件系统分别发出一次。使用 SUM 统计数据计算所有文件系统的活动 SMBv3 会话总数。 单位：计数
TotalCacheSize	此指标报告缓存的总大小。 单位：字节
UserCpuPercent	此指标报告网关处理所花费的时间百分比。 单位：百分比

了解文件系统指标

您可以在下面找到有关包含文件系统的 Storage Gateway 指标的信息。每个文件系统均有与其关联的一组指标。某些特定于文件系统的指标与某些特定于网关的指标同名。这些指标代表同类度量，但其范围限于文件系统。

始终在使用指标前指定要使用网关还是文件系统指标。尤其是使用文件系统指标时，您必须指定 `File system ID`，用于标识希望查看其指标的文件系统。有关更多信息，请参阅 使用亚马逊 CloudWatch 指标。

> **Note**
>
> 某些指标仅在最近的监控期内生成了新数据时才会返回数据点。

下表描述了可用来获取文件共享相关信息的 Storage Gateway 指标。

指标	说明
`CacheHitPercent`	在来自文件共享的应用程序读取操作中，由缓存提供的操作所占百分比。样本在报告周期结束时采用。 当文件共享没有收到任何应用程序读取操作时，此指标会报告为 100%。 单位：百分比
`CachePercentDirty`	在网关缓存中尚未持久化到 AWS的数据中，文件共享产生的部分所占比例。样本在报告周期结束时采用。 将此指标与 `Sum` 统计数据结合使用。 理想情况下，此指标应保持在较低水平。

指标	说明
	Note 使用网关的 CachePercentDirty 指标来查看尚未持久化到 AWS的网关缓存的总体比例。 单位：百分比
CachePercentUsed	整个网关使用的数据缓存的百分比。样本在报告周期结束时采用。这个文件共享特定指标报告的值与相应的网关特定指标报告的值相同。 单位：百分比
CloudBytesUploaded	网关在报告期内上传到的 AWS 总字节数。 将此指标与 Sum 统计数据结合使用可测量吞吐量，将其与 Samples 统计数据结合使用可测量 IOPS。 单位：字节
CloudBytesDownloaded	在报告期内，网关从中 AWS 下载的总字节数。 将此指标与Sum统计数据结合使用以衡量吞吐量，将此指标与Samples统计数据结合使用以衡量每秒 input/output 操作数 (IOPS)。 单位：字节

指标	说明
FilesFailingUpload	此指标跟踪未能上传到 AWS的文件数。这些文件将生成运行状况通知，其中包含有关该问题的更多信息。 将此指标与 Sum 统计数据结合使用，可以显示当前无法上传到 AWS的文件数。 单位：计数
ReadBytes	文件共享的报告周期内从本地应用程序读取的总字节数。 将此指标与 Sum 统计数据结合使用可测量吞吐量，将其与 Samples 统计数据结合使用可测量 IOPS。 单位：字节
WriteBytes	报告周期内写入到场内应用程序的总字节数。 将此指标与 Sum 统计数据结合使用可测量吞吐量，将其与 Samples 统计数据结合使用可测量 IOPS。 单位：字节

了解 关审核日志

Amazon FSx File Gateway（FSx 文件网关）审核日志为您提供有关用户访问文件系统关联中的文件和文件夹的详细信息。您可以使用审核日志来监控用户活动，并在发现异常活动模式时采取相应措施。这些日志的格式与 Windows Server 安全日志事件类似，从而可以与 Windows 安全事件的现有日志处理工具兼容。

操作

下表描述了 文件网关审核日志文件访问操作。

操作名称	定义
读取数据	读取文件的内容。
写入数据	更改文件的内容。
Create	创建新文件或文件夹。
重命名	重命名现有文件或文件夹。
删除	删除文件或文件夹。
写入属性	更新文件或文件夹的元数据（ACLs、所有者、群组、权限）。

属性

下表描述了 FSx File Gateway 审核日志文件访问属性。

属性	定义
`securityDescriptor`	显示在对象上设置的自由访问控制列表 (DACL)，使用 SDDL 格式。
`sourceAddress`	文件共享客户端计算机的 IP 地址。
`SubjectDomainName`	客户端账户所属的 Active Directory (AD) 域。
`SubjectUserName`	客户端的 Active Directory 用户名。
`source`	正在审核的 Storage Gateway `FileSystemAssociation` 的 ID。
`mtime`	在此时间修改对象的内容，由客户端设置。
`version`	审核日志格式的版本。
`ObjectType`	定义对象是文件还是文件夹。
`locationDnsName`	FSx 文件网关系统 DNS 名称。

属性	定义
objectName	对象的完整路径。
ctime	在此时间修改对象的内容或元数据，由客户端设置。
shareName	正在访问的共享的名称。
operation	对象访问操作的名称。
newObjectName	新对象重命名后的完整路径。
gateway	Storage Gateway ID。
status	操作的状态。仅记录成功（一般不记录失败，但会记录由于权限被拒绝而引发的失败）。
fileSizeInBytes	文件大小，以字节为单位，由客户端在文件创建时设置。

每个操作记录的属性

下表描述了每个 FSx 文件访问操作中记录的 File Gateway 审核日志属性。

	读取数据	写入数据	创建文件夹	创建文件	重命名文件/文件夹	删除文件/文件夹	写入属性（更改 ACL）	写入属性（chown）	写入属性（chmod）	写入属性（chgrp）
securiescrip							X			
sourceress	X	X	X	X	X	X	X	X	X	X

	读取数据	写入数据	创建文件夹	创建文件	重命名文件/文件夹	删除文件/文件夹	写入属性（更改 ACL）	写入属性（chown）	写入属性（chmod）	写入属性（chgrp）
Subjec mainNa	X	X	X	X	X	X	X	X	X	X
Subjec erName	X	X	X	X	X	X	X	X	X	X
source	X	X	X	X	X	X	X	X	X	X
mtime			X	X						
versic	X	X	X	X	X	X	X	X	X	X
object e	X	X	X	X	X	X	X	X	X	X
locati nsName	X	X	X	X	X	X	X	X	X	X
object e	X	X	X	X	X	X	X	X	X	X
ctime			X	X						
shareN	X	X	X	X	X	X	X	X	X	X
operat	X	X	X	X	X	X	X	X	X	X
newObj Name					X					
gatewa	X	X	X	X	X	X	X	X	X	X

	读取数据	写入数据	创建文件夹	创建文件	重命名文件/文件夹	删除文件/文件夹	写入属性（更改 ACL）	写入属性（chown）	写入属性（chmod）	写入属性（chgrp）
status	X	X	X	X	X	X	X	X	X	X
fileSizeInBytes				X						

维护网关

维护您的亚马逊 FSx 文件网关 需要进行一般维护以优化网关的性能。这些任务是所有网关类型的常见任务。

本节包含以下主题，这些主题描述了与维护您的亚马逊 FSx 文件网关 Amazon 3 文件网关相关的概念和程序：

主题

- 管理网关更新：了解如何开启或关闭维护更新，以及修改文件网关的维护时段计划。
- 使用本地控制台执行维护任务：了解如何使用网关本地控制台执行维护任务。
- 关闭网关虚拟机：了解在需要关闭或重启网关虚拟机来进行维护（例如为虚拟机监控程序应用补丁）时该怎么做。
- 用新实例替换现有文件网关— 了解当您想要提高性能或响应迁移网关的通知时，如何用新实例替换网关文件网关。
- 删除网关和移除关联的资源— 了解如何使用 AWS Storage Gateway 控制台删除网关并清理相关资源，以免因继续使用这些资源而被收费。

管理网关更新

Storage Gateway 由托管云服务组件和网关设备组件组成，您可以部署在本地或 AWS 云中的 Amazon EC2 实例上。这两个组件都会定期更新。本节中的主题描述了这些更新的节奏、如何应用它们以及如何在部署中的网关上配置与更新相关的设置。

> **Important**
>
> 应将 Storage Gateway 设备视为托管式虚拟机，并且不应尝试以任何方式访问或修改其安装或内容。尝试使用普通 AWS 网关更新机制以外的方法（例如 SSM 或虚拟机管理程序工具）安装或更新任何软件包可能会导致网关出现故障。
>
> Storage Gateway 会自动定期修补设备以维护安全性和稳定性。Storage Gateway 设备使用 Amazon Linux 作为其基础操作系统。您可以在 Amazon Linux 安全中心查看检测到的常见漏洞和风险（CVE）问题的状态。如 Amazon Linux 安全中心所示，CVE 补丁将在发布后 30 天内自动应用。在网关维护时间段内，只要您的网关处于联机状态，就会安装补丁。
>
> Storage Gateway 不支持使用 cloud-init 指令手动更新 Amazon EC2 网关。如果您使用此方法更新网关，则可能会遇到互操作性问题，使您无法激活或使用网关设备。

更新频率和预期行为

AWS 根据需要更新云服务组件，而不会对已部署的网关造成中断。已部署的网关设备会收到以下类型的更新：

- 维护：定期进行的更新，包括操作系统和软件升级、用于提升稳定性、性能和安全性的问题修复，以及对新功能的访问。
- 紧急：关键更新，包括会立即影响网关安全、性能或持久性的问题所需的修复。紧急更新可以在任何时候发布，不受每月例行维护和功能更新周期的限制。

所有更新均为累积更新，应用后会将网关升级到当前版本。有关每个更新中包含的具体更改的信息，请参阅。

所有网关设备更新都可能导致服务短暂中断。网关的 VM 主机在更新期间无需重启，但在网关设备更新和重新启动期间，网关将在短时间内不可用。

部署并激活网关后，将设置默认的维护时段计划。可以随时修改维护时段计划。也可以关闭维护更新，但建议将其保持为开启状态。

> **Note**
>
> 即使定期维护更新已关闭，也会根据维护时段计划应用紧急更新。

在将任何更新应用于您的网关之前， AWS 会在 Storage Gateway 控制台和您的 AWS Health Dashboard。有关更多信息，请参阅 AWS Health Dashboard。要修改发送软件更新通知的电子邮件地址，请参阅《账户管理参考指南》中的 “更新 AWS AWS 账户的备用联系人”。

在有更新可用时，网关详细信息选项卡会显示维护消息。可以在详细信息选项卡上查看应用上一次成功更新的日期和时间。

开启或关闭维护更新

开启维护更新后，网关会根据配置的维护时段计划自动应用这些更新。有关更多信息，请参阅 Modify the gateway maintenance window schedule。

如果关闭维护更新，网关将不会自动应用这些更新，但您可以随时使用 Storage Gateway 控制台、API 或 CLI 手动应用这些更新。无论此设置如何，都会有时在您配置的维护时段内应用紧急更新。

> **Note**
>
> 以下过程介绍如何使用 Storage Gateway 控制台开启或关闭网关更新。要使用 API 以编程方式更改此设置，请参阅 Storage Gateway API 参考UpdateMaintenanceStartTime中的。

要使用 Storage Gateway 控制台开启或关闭维护更新，请执行以下操作：

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在导航窗格中，选择网关，然后选择要为其配置维护更新的网关。
3. 选择操作，然后选择编辑维护设置。
4. 对于维护更新，请选择开启或关闭。
5. 完成后，选择保存更改。

可以在 Storage Gateway 控制台中所选网关的详细信息选项卡上验证已更新的设置。

修改网关维护时段计划

如果开启了维护更新，网关会根据维护时段计划自动应用这些更新。无论维护更新设置如何，都会有时在配置的维护时段内应用紧急更新。

> **Note**
>
> 以下过程介绍如何使用 Storage Gateway 控制台来修改维护时段计划。要使用 API 以编程方式更改此设置，请参阅 Storage Gateway API 参考UpdateMaintenanceStartTime中的。

要使用 Storage Gateway 控制台修改维护时段计划，请执行以下操作：

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在导航窗格中，选择网关，然后选择要为其配置维护更新的网关。
3. 选择操作，然后选择编辑维护设置。
4. 在维护时段开始时间下，执行以下操作：

    a. 对于计划，选择每周或每月以设置维护时段节奏。

    b. 如果选择每周，请修改星期和时间的值，以设置每周中维护时段将开始的具体时间点。

如果选择每月，请修改日期和时间的值，以设置每个月中维护时段将开始的具体时间点。

> **Note**
>
> 可以为月份中的某一天设置的最大值为 28。无法将维护计划设置为从日期 29 至日期 31 开始。
> 如果您在配置此设置时收到错误，则可能意味着网关软件已过期。考虑先手动更新网关，然后尝试再次配置维护时段计划。

5. 完成后，选择保存更改。

可以在 Storage Gateway 控制台中所选网关的详细信息选项卡上验证已更新的设置。

手动应用更新

如果网关有可用的软件更新，则可以按照以下过程手动应用该更新。此手动更新过程会忽略维护时段计划并立即应用更新，即使维护更新已关闭也是如此。

> **Note**
>
> 以下过程介绍了如何使用 Storage Gateway 控制台来手动应用更新。要使用 API 以编程方式执行此操作，请参阅 Storage Gateway API 参考UpdateGatewaySoftwareNow中的。

要使用 Storage Gateway 控制台手动应用网关软件更新，请执行以下操作：

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在导航窗格上，选择网关，然后选择要更新的网关。

   如果有可用更新，控制台将在网关详细信息选项卡上显示蓝色通知横幅，其中包括应用该更新的选项。
3. 选择立即应用更新以立即更新网关。

> **Note**
>
> 此操作会在安装更新时暂时中断网关功能。在此期间，Storage Gateway 控制台中的网关状态显示为离线。更新完成安装后，网关恢复正常运行，其状态更改为正在运行。

可以通过在 Storage Gateway 控制台中查看所选网关的详细信息选项卡，来验证网关软件已更新到最新版本。

使用本地控制台执行维护任务

本节包含以下主题，这些主题提供有关如何使用网关设备本地控制台来执行维护任务的信息。您可以通过本地虚拟机或托管网关设备的 Amazon EC2 实例访问本地控制台来执行这些任务。大多数任务对不同的主机平台来说具有共性，但也存在一些差异。

主题

- 访问网关本地控制台-了解如何登录托管在基于 Linux 内核的虚拟机 (KVM) VMware ESXi 或 Microsoft Hyper-V Manager 平台上的本地网关的本地控制台。
- 在虚拟机本地控制台上执行任务：了解如何使用本地控制台来为本地网关执行基本设置和高级配置任务，例如配置 HTTP 代理、查看系统资源状态或运行终端命令。
- 在 Amazon EC2 网关本地控制台上执行任务：了解如何登录到本地控制台来为 Amazon EC2 网关执行基本设置和高级配置任务，例如配置 HTTP 代理、查看系统资源状态或运行终端命令。

访问网关本地控制台

访问 VM 的本地控制台的方式取决于将网关 VM 部署到的管理程序的类型。在本节中，你可以找到有关如何使用基于 Linux 内核的虚拟机 (KVM) VMware ESXi 和 Microsoft Hyper-V Manager 访问虚拟机本地控制台的信息。

主题

- 使用 Linux KVM 访问网关本地控制台
- 使用访问网关本地控制台 VMware ESXi
- 使用 Microsoft Hyper-V 访问网关本地控制台

使用 Linux KVM 访问网关本地控制台

配置在 KVM 上运行的虚拟机的方法各有不同，具体取决于所使用的 Linux 发行版。有关从命令行访问 KVM 配置选项的说明如下所示。根据您的 KVM 实现，说明可能会有所不同。

使用 KVM 访问网关的本地控制台

1. 使用以下命令列出 KVM 中当前可用的内容。 VMs

```
# virsh list
```

该命令会返回一个列表，其中 VMs 包含每个列表的 ID、名称和状态信息。记下要为其启动网关本地控制台的 VM 的 Id。

2. 使用以下命令访问本地控制台。

```
# virsh console Id
```

*Id*替换为您在上一步中记下的虚拟机的 ID。

AWS 设备网关本地控制台会提示您登录以更改网络配置和其他设置。

3. 输入您的用户名和密码以登录网关本地控制台。有关更多信息，请参阅登录到文件网关本地控制台。

登录后，将出现 AWS 设备激活 - 配置菜单。可以从菜单选项中进行选择来执行网关配置任务。有关更多信息，请参阅 Performing tasks on the virtual machine local console。

使用访问网关本地控制台 VMware ESXi

要使用访问网关的本地控制台 VMware ESXi

1. 在 VMware vSphere 客户端中，选择您的网关虚拟机。
2. 确保网关 VM 已开启。

> **Note**
>
> 如果网关 VM 已开启，则应用程序窗口左侧的 VM 浏览器面板中会出现一个带有 VM 图标的绿色箭头图标。如果网关 VM 未开启，则可以通过选择位于应用程序窗口顶部的工具栏上的绿色开机图标将其开启。

3. 在应用程序窗口右侧的主信息面板中选择控制台选项卡。

片刻之后， AWS 设备网关本地控制台会提示您登录以更改网络配置和其他设置。

> **Note**
>
> 如需将光标从控制台窗口中释放出，请按 Ctrl+Alt。

4. 输入您的用户名和密码以登录网关本地控制台。有关更多信息，请参阅登录到文件网关本地控制台。

   登录后，将出现 AWS 设备激活 - 配置菜单。可以从菜单选项中进行选择来执行网关配置任务。有关更多信息，请参阅 Performing tasks on the virtual machine local console。

使用 Microsoft Hyper-V 访问网关本地控制台

访问网关的本地控制台 (Microsoft Hyper-V)

1. 从 Microsoft Hyper-V Manager 应用程序窗口左侧的虚拟机面板中选择网关设备 VM。
2. 确保网关已开启。

> **Note**
>
> 如果网关 VM 已开启，则在应用程序窗口左侧的虚拟机面板中，VM 的状态列中将显示 `Running`。如果网关 VM 未开启，则可以通过在应用程序窗口右侧的操作窗格中选择启动来将其开启。

3. 从操作面板中选择连接。

   这时，会显示 Virtual Machine Connection (虚拟机连接) 窗口。如果显示身份验证窗口，请键入管理程序管理员向您提供的登录凭证。

   片刻之后， AWS 设备网关本地控制台会提示您登录以更改网络配置和其他设置。

4. 输入您的用户名和密码以登录网关本地控制台。有关更多信息，请参阅登录到文件网关本地控制台。

   登录后，将出现 AWS 设备激活 - 配置菜单。可以从菜单选项中进行选择来执行网关配置任务。有关更多信息，请参阅 Performing tasks on the virtual machine local console。

在虚拟机本地控制台上执行任务

对于本地部署的文件网关，您可以使用 VM 主机的本地控制台执行以下维护任务。这些任务是微软 Hyper-V 和基于 Linux 内核的虚拟机 (KVM) 虚拟机管理程序的常见任务。 VMware

主题

- 登录到文件网关本地控制台：了解如何登录到本地控制台，您可以在控制台中配置网关网络设置和更改默认密码。
- 配置 HTTP 代理-了解如何将 Storage Gateway 配置为通过代理服务器路由所有 AWS 端点流量。
- 配置网关网络设置：了解如何将网关配置为使用 DHCP 或静态 IP 地址。
- 测试网关的网络连接：了解如何使用网关本地控制台来测试网络连接。
- 查看您的网关系统资源状态：了解如何检查网关的虚拟 CPU 内核、根卷大小和 RAM。
- 配置网关的网络时间协议（NTP）服务器：了解如何使用虚拟机监控程序主机查看和编辑网络时间协议（NTP）服务器配置并同步您网关上的时间。
- 在本地控制台上运行 Storage Gateway 命令-学习如何运行本地控制台命令来执行保存路由表、连接等任务。 支持

登录到文件网关本地控制台

在 VM 做好登录准备时，登录屏幕将显示。如果这是您首次登录虚拟机本地控制台，请使用临时登录凭证来登录。您可以使用这些临时凭证来访问本地控制台中的一些菜单，这些菜单可用来配置网关网络设置和更改密码。初始用户名为 `admin`，临时密码为 `password`。首次登录时必须更改密码。

更改临时密码

1. 在 AWS 设备激活 - 配置主菜单中，输入相应的数字来选择网关控制台。
2. 运行 `passwd` 命令。有关如何运行该命令的信息，请参阅在本地控制台上运行 Storage Gateway 命令。

从 Storage Gateway 控制台设置本地控制台密码

您也可以通过 Storage Gateway 基于 Web 的控制台来管理本地控制台的密码。使用基于 Web 的控制台成功更新的密码会覆盖网关虚拟机的本地控制台使用的密码，包括临时密码（如果您从未在本地登录）。如果当前无法通过网络访问网关，则密码更新过程会失败。

在 Storage Gateway 控制台上设置本地控制台密码

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在导航栏中，选择网关，然后选择要为其设置新密码的网关。
3. 对于 Actions (操作)，选择 Set Local Console Password (设置本地控制台密码)。
4. 在 Set Local Console Password (设置本地控制台密码) 对话框中，输入新密码，确认该密码，然后选择 Save (保存)。

   您的新密码会替换当前密码。Storage Gateway 服务不会保存、存储或记录密码，而是通过加密通道将其安全地传输到虚拟机，并在那里安全地存储密码。

   > **Note**
   >
   > 密码可以包含键盘上的任意字符，长度可以为 1 至 512 个字符。

配置 HTTP 代理

文件网关支持配置 HTTP 代理。

> **Note**
>
> 文件网关支持的唯一代理配置为 HTTP。

如果网关必须使用代理服务器与 Internet 通信，则需要为网关配置 HTTP 代理设置。为此，您可以为运行代理的主机指定 IP 地址和端口号。完成此操作后，Storage Gateway 会通过您的代理服务器路由所有 AWS 端点流量。即使使用 HTTP 代理，也会加密网关和端点之间的通信。有关网关的网络要求的信息，请参阅网络和防火墙要求。

为文件网关配置 HTTP 代理

1. 登录到网关的本地控制台：

   - 有关登录 VMware ESXi 本地控制台的更多信息，请参阅使用访问网关本地控制台 VMware ESXi。
   - 有关登录到 Microsoft Hyper-V 本地控制台的更多信息，请参阅使用 Microsoft Hyper-V 访问网关本地控制台。

- 有关登录到基于 Linux 内核的 Virtuam 计算机 (KVM) 的本地控制台的更多信息，请参阅使用 Linux KVM 访问网关本地控制台。

2. 在 AWS 设备激活 - 配置主菜单中，输入相应的数字来选择配置 HTTP 代理。
3. 在 AWS 设备激活 HTTP 代理配置菜单中，输入与要执行的任务对应的数字：

   - 配置 HTTP 代理 - 您需要提供主机名称和端口来完成配置。
   - 查看当前 HTTP 代理配置 - 如果未配置 HTTP 代理，则会显示消息 `HTTP Proxy not configured`。如果 HTTP 代理已配置，则会显示代理的主机名称和端口。
   - 移除 HTTP 代理配置 - 显示消息 `HTTP Proxy Configuration Removed`。
4. 重新启动 VM 以应用 HTTP 配置设置。

配置网关网络设置

网关的默认网络配置是动态主机配置协议 (DHCP)。使用 DHCP 时，系统会为您的网关自动分配 IP 地址。在某些情况下，您可能需要手动将网关的 IP 分配为静态 IP 地址，如下所述。

如需将您的网关配置为使用静态 IP 地址。

1. 登录到网关的本地控制台：

   - 有关登录 VMware ESXi 本地控制台的更多信息，请参阅使用访问网关本地控制台 VMware ESXi。
   - 有关登录到 Microsoft Hyper-V 本地控制台的更多信息，请参阅使用 Microsoft Hyper-V 访问网关本地控制台。
   - 有关登录到 KVM 本地控制台的更多信息，请参阅使用 Linux KVM 访问网关本地控制台。
2. 在 AWS 设备激活 - 配置主菜单中，输入相应的数字来选择网络配置。
3. 在网络配置菜单中，执行以下任务之一：

执行此任务	请执行此操作
获取有关网络适配器的信息	输入相应的数字来选择描述适配器。 将显示一个适配器名称列表，并且系统会提示您输入一个适配器名称例如 **`eth0`**。如果您指定的

执行此任务	请执行此操作
	适配器正在使用中，有关该适配器的下列信息就会显示： • 媒体访问控制 (MAC) 地址 • IP 地址 • 网络掩码 • 网关 IP 地址 • DHCP 启用状态 配置静态 IP 地址或设置网关的默认适配器时，使用此处列出的适配器名称。
配置 DHCP 路由	输入相应的数字来选择配置 DHCP。 系统将提示您将网络接口配置为使用 DHCP。

执行此任务	请执行此操作
为网关配置静态 IP 地址	输入相应的数字来选择配置静态 IP。 系统会提示您输入下列信息以配置静态 IP 地址： • 网络适配器名称 • IP 地址 • 网络掩码 • 默认网关地址 • 主要域名服务 (DNS) 地址 • 备用 DNS 地址 **Important** 如果网关已激活，则必须从 Storage Gateway 控制台关停并重启网关，这样设置才会生效。有关更多信息，请参阅关闭网关虚拟机。 如果网关使用多个网络接口，则必须将所有活跃的接口设置为使用 DHCP 或静态 IP 地址。 例如，假定您的网关 VM 使用两个配置为 DHCP 的接口。如果您稍后将一个接口设置为静态 IP，则会停用另一个接口。在这种情况下，要激活该接口，必须将其设置为静态 IP。

执行此任务	请执行此操作
	如果两个接口最初都设置为使用静态 IP 地址并且您之后将网关设置为使用 DHCP，那么两个接口都必须使用 DHCP。
为网关配置主机名	输入相应的数字来选择配置主机名。 系统会提示您选择网关是使用您指定的静态主机名，还是通过 DHCP 或 rDNS 自动获取主机名。 如果选择静态，则系统会提示您提供静态主机名，例如 `testgateway.example.com` 。输入 y 以应用配置。 **Note** 如果为网关配置静态主机名，请确保提供的主机名位于网关加入的域中。还必须在 DNS 系统中创建 A 记录，将网关的 IP 地址指向其静态主机名。
查看网关的主机名配置	输入相应的数字来选择查看主机名配置。 此时会显示网关的主机名、获取模式、域和 Active Directory 领域。

执行此任务	请执行此操作
将网关的所有网络配置重置为 DHCP	输入相应的数字来选择全部重置为 DHCP。 所有网络接口均设置为使用 DHCP。 **Important** 如果网关已激活，则必须从 Storage Gateway 控制台关停并重启网关，这样设置才会生效。有关更多信息，请参阅关闭网关虚拟机。
设置网关的默认路由适配器	输入相应的数字来选择设置默认适配器。 此时会显示可供网关使用的适配器，系统会提示您选择其中一个适配器，例如 **`eth0`**。
编辑网关的 DNS 配置	输入相应的数字来选择编辑 DNS 配置。 这将显示主 DNS 和备用 DNS 服务器的可用适配器。系统将提示您提供新的 IP 地址。

执行此任务	请执行此操作
查看网关的 DNS 配置	输入相应的数字来选择查看 DNS 配置。 这将显示主 DNS 和备用 DNS 服务器的可用适配器。 **Note** 对于某些版本的 VMware 虚拟机管理程序，您可以在此菜单中编辑适配器配置。
查看路由表	输入相应的数字来选择查看路由。 网关的默认路由将会显示。

测试网关的网络连接

您可以使用网关的本地控制台来测试网络连接。当排查网关的网络问题时，此测试可能会很有用。

测试网关的网络连接

1. 登录到网关的本地控制台：
   - 有关登录 VMware ESXi 本地控制台的更多信息，请参阅使用访问网关本地控制台 VMware ESXi。
   - 有关登录到 Microsoft Hyper-V 本地控制台的更多信息，请参阅使用 Microsoft Hyper-V 访问网关本地控制台。
   - 有关登录到 KVM 本地控制台的更多信息，请参阅使用 Linux KVM 访问网关本地控制台。
2. 在 AWS 设备激活 - 配置主菜单中，输入相应的数字来选择测试网络连接。

   如果您的网关已经激活，则连接测试会立即开始。对于尚未激活的网关，您必须指定终端节点类型， AWS 区域 如以下步骤所述。
3. 如果您的网关尚未激活，请输入相应的数字来选择网关的端点类型。

4. 如果您选择了公共终端节点类型，请输入相应的数字以选择 AWS 区域 要测试的。有关支持的 AWS 服务终端节点 AWS 区域 以及可以与 Storage Gateway 配合使用的服务终端节点列表，请参阅中的AWS Storage Gateway 终端节点和配额AWS 一般参考。

随着测试的进行，每个端点都会显示 [已通过] 或 [已失败]，按如下所示指示连接的状态：

Message	说明
[PASSED]	Storage Gateway 有网络连接。
[失败]	Storage Gateway 没有网络连接。

查看您的网关系统资源状态

当您的网关启动时，它会检查其虚拟 CPU 内核、根卷大小和 RAM。然后，它会确定这些系统资源是否足够让网关正常运行。您可以在网关的本地控制台上查看此检查的结果。

查看系统资源检查的状态

1. 登录到网关的本地控制台：
   - 有关登录 VMware ESXi 控制台的更多信息，请参阅使用访问网关本地控制台 VMware ESXi。
   - 有关登录到 Microsoft Hyper-V 本地控制台的更多信息，请参阅使用 Microsoft Hyper-V 访问网关本地控制台。
   - 有关登录到 KVM 本地控制台的更多信息，请参阅使用 Linux KVM 访问网关本地控制台。
2. 在 AWS 设备激活 - 配置主菜单中，输入相应的数字来选择查看系统资源检查。

   每个资源都显示 [正常]、[警告] 或 [失败]，按如下所示指示连接的状态：

Message	说明
[OK]	该资源通过了系统资源检查。
[警告]	资源不满足建议的要求，但网关可以继续正常工作。Storage Gateway 显示一条消息，描述资源检查的结果。

Message	说明
[FAIL]	资源不满足最低要求。您的网关可能无法正常工作。Storage Gateway 显示一条消息，描述资源检查的结果。

控制台还会在资源检查菜单选项旁边显示错误和警告的数量。

配置网关的网络时间协议（NTP）服务器

您可以使用管理程序主机查看和编辑网络时间协议 (NTP) 服务器配置并同步您网关上的 VM 时间。

管理系统时间

1. 登录到网关的本地控制台：
   - 有关登录 VMware ESXi 本地控制台的更多信息，请参阅使用访问网关本地控制台 VMware ESXi。
   - 有关登录到 Microsoft Hyper-V 本地控制台的更多信息，请参阅使用 Microsoft Hyper-V 访问网关本地控制台。
   - 有关登录到 KVM 本地控制台的更多信息，请参阅使用 Linux KVM 访问网关本地控制台。
2. 在 AWS 设备激活 - 配置主菜单中，输入相应的数字来选择系统时间管理。
3. 在系统时间管理菜单中，输入相应的数字来执行以下任务之一。

执行此任务	请执行此操作
查看 VM 时间并将其与 NTP 服务器时间同步。	输入相应的数字来选择查看和同步系统时间。 这将显示 VM 的当前时间。您的文件网关确定与网关 VM 的时差，NTP 服务器时间提示您将 VM 时间与 NTP 时间同步。 部署并运行网关后，在某些情况下，网关 VM 的时间可能出现偏差。例如，假定网络中断时间延长，并且您的管理程序主机和网关没有获取时间更新。在此情况下，网关 VM 的时间与实

执行此任务	请执行此操作
	际时间不同。当出现时间偏差时，操作 (如快照) 发生的预计时间和操作发生的实际时间之间会有差异。 对于部署在上的网关 VMware ESXi，设置虚拟机管理程序主机时间并将虚拟机时间同步到主机就足以避免时间偏差。有关更多信息，请参阅将 VM 时间与 VMware 主机时间同步。 对于在 Microsoft Hyper-V 上部署的网关，您应定期检查 VM 的时间。有关更多信息，请参阅将 VM 时间与 Hyper-V 或 Linux KVM 主机时间同步。 对于在 KVM 上部署的网关，您可以使用 KVM 的 `virsh` 命令行界面检查并同步 VM 时间。
编辑 NTP 服务器配置	输入相应的数字来选择编辑 NTP 配置。 系统将提示您提供首选和辅助 NTP 服务器。
查看 NTP 服务器配置	输入相应的数字来选择查看 NTP 配置。 这将显示您的 NTP 服务器配置。

在本地控制台上运行 Storage Gateway 命令

Storage Gateway 中的 VM 本地控制台有助于提供安全的环境来配置和诊断网关问题。使用本地控制台命令，您可以执行维护任务，例如保存路由表 支持、连接等。

运行配置或诊断命令

1. 登录到网关的本地控制台：

   - 有关登录 VMware ESXi 本地控制台的更多信息，请参阅使用访问网关本地控制台 VMware ESXi。

- 有关登录到 Microsoft Hyper-V 本地控制台的更多信息，请参阅使用 Microsoft Hyper-V 访问网关本地控制台。
- 有关登录到 KVM 本地控制台的更多信息，请参阅使用 Linux KVM 访问网关本地控制台。

2. 在 AWS 设备激活 - 配置主菜单中，输入相应的数字来选择网关控制台。
3. 在网关控制台命令提示符处输入 **h**。

   控制台会显示可用命令菜单，其中列出了可用的命令：

命令	函数
dig	从 dig 收集输出来进行 DNS 故障排除。
exit	返回到“配置”菜单。
h	显示可用的命令列表。
ifconfig	查看或配置网络接口。 **Note** 我们建议使用 Storage Gateway 控制台或专用的本地控制台菜单选项来配置网络或 IP 设置。有关说明，请参阅配置网关网络设置。
ip	显示/操作路由、设备和隧道。 **Note** 我们建议使用 Storage Gateway 控制台或专用的本地控制台菜单选项来配置网络或 IP 设置。有关说明，请参阅配置网关网络设置。
iptables	用于 IPv4 数据包过滤和 NAT 的管理工具。
ncport	测试与网络上特定 TCP 端口的连接。

命令	函数
nping	从 nping 收集输出来进行网络故障排除。
open-support-channel	Connect to S AWS upport。有关如何开启 AWS 支持访问权限的说明，请参阅希望 AWS 支持人员帮助您排除 EC2 网关故障。
passwd	更新身份验证令牌。
save-iptables	保留 IP 表。
save-routing-table	保存新添加的路由表条目。
tcptraceroute	收集有关流向目的地的 TCP 流量的 traceroute 输出。
sslcheck	返回证书颁发者的输出 **Note** Storage Gateway 使用证书颁发者验证，而不支持 ssl 检查。如果此命令返回 aws-appliance@amazon.com 以外的颁发者，则很可能是应用程序在执行 ssl 检查。在这种情况下，我们建议绕过 Storage Gateway 设备的 ssl 检查。

4. 在网关控制台命令提示符下，输入要使用的功能的相应命令，然后按照说明进行操作。

要了解命令，请在命令提示符*command name*下输入 **man +**。

在 Amazon EC2 网关本地控制台上执行任务

某些维护任务需要您在运行部署于 Amazon EC2 实例上的网关时登录到本地控制台。本节介绍如何登录到本地控制台并执行维护任务。

主题

- 登录到 Amazon EC2 网关本地控制台：了解如何使用 Secure Shell（SSH）客户端连接并登录到 Amazon EC2 实例的网关本地控制台。
- 通过 HTTP 代理路由在 Amazon EC2 上部署的网关-了解如何在部署在 Amazon EC2 实例上的网关之间 AWS 配置 Socket Secure 版本 5 (SOCKS5) 代理。
- 测试网关的网络连接：了解如何使用网关本地控制台来测试网关与各种网络资源之间的网络连接。
- 查看您的网关系统资源状态：了解如何使用网关本地控制台来检查网关的虚拟 CPU 内核、根卷大小和 RAM。
- 在 Amazon EC2 网关的本地控制台上运行 Storage Gateway 命令：了解如何运行本地控制台命令，以便执行其他任务，李丽茹保存路由表、连接到 支持等。
- 配置 Amazon EC2 网关网络设置：了解如何使用本地控制台来查看和配置 Amazon EC2 实例上网关的网络设置，例如 DNS 和主机名。

登录到 Amazon EC2 网关本地控制台

您可以使用 Secure Shell（SSH）客户端登录到 Amazon EC2 实例上的网关本地控制台。有关详细信息，请参阅《Amazon EC2 用户指南》中的连接到您的实例。要以这种方式连接，您需要在启动实例时指定的 SSH 密钥对。有关 Amazon EC2 密钥对的信息，请参阅《Amazon EC2 用户指南》中的 Amazon EC2 密钥对。

登录网关本地控制台

1. 使用 SSH 连接到 Amazon EC2 实例，并以管理员用户身份登录。
2. 登录后，您将看到 AWS 设备激活 - 配置主菜单，您可以通过这个菜单执行各种任务。

了解此任务	请参阅此主题
为网关配置 HTTP 代理	通过 HTTP 代理路由在 Amazon EC2 上部署的网关
为网关配置网络设置	配置 Amazon EC2 网关网络设置
测试网关连接性	测试网关的网络连接
查看系统资源检查	查看您的网关系统资源状态.
运行 Storage Gateway 控制台命令	在 Amazon EC2 网关的本地控制台上运行 Storage Gateway 命令

要关闭网关，请输入 **0**。

要退出配置会话，请输入 **X**。

通过 HTTP 代理路由在 Amazon EC2 上部署的网关

Storage Gateway 支持在 Amazon EC2 上部署的网关与 AWS之间配置 Socket Secure 版本 5 (SOCKS5) 代理。

如果网关必须使用代理服务器与 Internet 通信，则需要为网关配置 HTTP 代理设置。为此，您可以为运行代理的主机指定 IP 地址和端口号。完成此操作后，Storage Gateway 会通过您的代理服务器路由所有 AWS 端点流量。即使使用 HTTP 代理，也会加密网关和端点之间的通信。

通过本地代理服务器路由网关 Internet 流量

1. 登录到网关的本地控制台。有关说明，请参阅登录到 Amazon EC2 网关本地控制台。
2. 在 AWS 设备激活 - 配置主菜单中，输入相应的数字来选择配置 HTTP 代理。
3. 在 AWS 设备激活 HTTP 代理配置菜单中，输入与要执行的任务对应的数字：
   - 配置 HTTP 代理 - 您需要提供主机名称和端口来完成配置。
   - 查看当前 HTTP 代理配置 - 如果未配置 HTTP 代理，则会显示消息 `HTTP Proxy not configured`。如果 HTTP 代理已配置，则会显示代理的主机名称和端口。
   - 移除 HTTP 代理配置 - 显示消息 `HTTP Proxy Configuration Removed`。

测试网关的网络连接

您可以使用网关的本地控制台来测试网络连接。当排查网关的网络问题时，此测试可能会很有用。

测试网关的连接

1. 登录到网关的本地控制台。有关说明，请参阅登录到 Amazon EC2 网关本地控制台。
2. 在 AWS 设备激活 - 配置主菜单中，输入相应的数字来选择测试网络连接。

   如果您的网关已经激活，则连接测试会立即开始。对于尚未激活的网关，您必须指定终端节点类型， AWS 区域 如以下步骤所述。
3. 如果您的网关尚未激活，请输入相应的数字来选择网关的端点类型。
4. 如果您选择了公共终端节点类型，请输入相应的数字以选择 AWS 区域 要测试的。有关支持的 AWS 服务终端节点 AWS 区域 以及可以与 Storage Gateway 配合使用的服务终端节点列表，请参阅中的AWS Storage Gateway 终端节点和配额AWS 一般参考。

随着测试的进行，每个端点都会显示 [已通过] 或 [已失败]，按如下所示指示连接的状态：

Message	说明
[PASSED]	Storage Gateway 有网络连接。
[失败]	Storage Gateway 没有网络连接。

查看您的网关系统资源状态

当您的文件网关启动时，它会检查其虚拟 CPU 内核、根卷大小和 RAM。然后，它会确定可用系统资源是否足够让网关正常运行。您可以使用网关本地控制台来查看系统资源检查的结果。

查看系统资源检查的状态

1. 登录到 Amazon EC2 文件网关上的本地控制台。有关说明，请参阅登录到 Amazon EC2 网关本地控制台。
2. 在 AWS 设备激活 - 配置主菜单中，输入相应的数字来选择查看系统资源检查。

   网关本地控制台显示 [确定]、[警告] 或 [失败]，以指示资源的状态，如下所示：

Message	说明
[OK]	该资源通过了系统资源检查。
[警告]	资源不满足建议的要求，但网关可以继续正常工作。网关本地控制台会显示一条消息，描述资源检查的结果。
[FAIL]	资源不满足最低要求。您的网关可能无法正常工作。网关本地控制台会显示一条消息，描述资源检查的结果。

   本地控制台还会在资源检查菜单选项旁边显示错误和警告的数量。

在 Amazon EC2 网关的本地控制台上运行 Storage Gateway 命令

AWS Storage Gateway 控制台有助于为配置和诊断网关问题提供安全的环境。使用控制台命令，您可以执行维护任务，例如保存路由表或连接到 支持。

运行配置或诊断命令

1. 登录到网关的本地控制台。有关说明，请参阅登录到 Amazon EC2 网关本地控制台。
2. 在 AWS 设备激活 - 配置主菜单中，输入相应的数字来选择网关控制台。
3. 在网关控制台命令提示符处输入 **h**。

   控制台会显示可用命令菜单，其中列出了可用的命令：

命令	函数
dig	从 dig 收集输出来进行 DNS 故障排除。
exit	返回到“配置”菜单。
h	显示可用的命令列表。
ifconfig	查看或配置网络接口。 **Note** 我们建议使用 Storage Gateway 控制台或专用的本地控制台菜单选项来配置网络或 IP 设置。有关说明，请参阅配置网关网络设置。
ip	显示/操作路由、设备和隧道。 **Note** 我们建议使用 Storage Gateway 控制台或专用的本地控制台菜单选项来配置网

命令	函数
	络或 IP 设置。有关说明，请参阅配置网关网络设置。
iptables	用于 IPv4 数据包过滤和 NAT 的管理工具。
ncport	测试与网络上特定 TCP 端口的连接。
nping	从 nping 收集输出来进行网络故障排除。
open-support-channel	Connect to S AWS upport。
save-iptables	保留 IP 表。
save-routing-table	保存新添加的路由表条目。
tcptraceroute	收集有关流向目的地的 TCP 流量的 traceroute 输出。

4. 在网关控制台命令提示符下，输入要使用的功能的相应命令，然后按照说明进行操作。

要了解命令，请在命令提示符*command name*下输入 **man** +。

配置 Amazon EC2 网关网络设置

您可以使用网关本地控制台来查看和配置 Amazon EC2 文件网关的网络设置。

配置您的网络设置

1. 登录到 Amazon EC2 文件网关上的本地控制台。有关说明，请参阅登录到 Amazon EC2 网关本地控制台。
2. 在 AWS 设备激活 - 配置主菜单中，输入相应的数字来选择网络配置。
3. 在 AWS 设备激活 - 网络配置菜单中，输入与要执行的任务对应的数字：

   - 编辑 DNS 配置：网关本地控制台显示主 DNS 服务器和辅助 DNS 服务器的可用适配器。然后，控制台会提示您提供新的 IP 地址。
   - 查看 DNS 配置：网关本地控制台显示主 DNS 服务器和辅助 DNS 服务器的可用适配器。

- 配置主机名：网关本地控制台提示您选择网关是使用您指定的静态主机名，还是通过 DHCP 或 rDNS 自动获取主机名。

  > **Note**
  >
  > 如果您选择为网关配置静态主机名，则必须在 DNS 系统中创建 A 记录，将网关的 IP 地址指向其静态主机名。

- 查看主机名配置：网关本地控制台显示您的 Amazon EC2 文件网关的主机名、获取模式、域和 Active Directory 领域。

关闭网关虚拟机

您可能需要关闭或重新启动虚拟机进行维护，例如在向虚拟机管理程序应用补丁时。您可以使用虚拟机监控程序界面关闭本地网关虚拟机，使用 Amazon EC2 控制台关闭 Amazon EC2 实例。

> **Important**
>
> 如果您停止并启动使用临时存储的 Amazon EC2 网关，则该网关将永久脱机。发生这种情况的原因是替换了物理存储磁盘。此问题没有解决方法。唯一的解决方案是删除该网关，然后在新的 EC2 实例上激活一个新网关。

用新实例替换现有文件网关

随着数据和性能需求的增长，或者收到迁移网关的 AWS 通知，您可以将现有的 网关文件网关替换为新实例。如果您想将网关迁移到更好的主机平台或更新的 Amazon EC2 实例，或者要刷新底层服务器硬件，则可能需要这样做。

> **Important**
>
> 这些说明仅适用于迁移运行 1.x 版的网关设备。您不能使用它们来迁移运行较低版本的网关设备。

> **Note**
>
> 只能在相同类型的网关之间执行迁移。例如，您无法将设置或数据从 FSx 文件网关迁移到 S3 文件网关。

要将FSx 文件网关网关替换为带有空缓存磁盘和新网关 ID 的新实例，请执行以下操作：

1. 停止任何正在写入现有 的应用程序。在新网关上设置文件系统关联之前，请确认监控选项卡上的 `CachePercentDirty` 指标为 `0`。
2. 使用 AWS Command Line Interface (AWS CLI) 通过执行以下操作来收集和保存有关现有 关FSx 文件网关和关联文件系统的配置信息：

   a. 保存 S 配置信息。

   ```
   aws storagegateway describe-gateway-information --gateway-arn
    "arn:aws:storagegateway:us-east-2:123456789012:gateway/sgw-12A3456B"
   ```

   此命令将输出一个 JSON 数据块，其中包含有关网关的元数据，例如其名称、网络接口、已配置时区和状态（网关是否正在运行）。

   b. 保存 S MB) 设置。

   ```
   aws storagegateway describe-smb-settings --gateway-arn
    "arn:aws:storagegateway:us-east-2:123456789012:gateway/sgw-12A3456B"
   ```

   此命令会输出一个 JSON 数据块，其中包含已加入网关的 Microsoft Active Directory 的域名。

   c. 保存与 系统的FSx 文件共享信息：

   对每个关联的文件系统使用以下命令。

   ```
   aws storagegateway describe-file-system-associations --file-system-
   association-arn-list "arn:aws:storagegateway:us-east-2:123456789012:fs-
   association/fsa-987A654B"
   ```

   此命令会输出一个 JSON 数据块，其中包含有关文件系统的元数据，例如其位置 ARN、审核日志目标、缓存刷新属性、已配置 IP 地址和标签。

3. 使用与旧网关文件网关。如有必要，请参阅在步骤 2 中保存的信息。

4. 使用与旧网关上配置的文件系统相同的设置和配置，为新网关创建新的文件系统关联。如有必要，请参阅在步骤 2 中保存的信息。
5. 确认您的新网关正常运行，然后以适合您环境的方式将客户端从旧文件系统重新映射/割接到新的文件系统。
6. 确认您的新网关正常运行，然后从 Storage Gateway 控制台中删除旧网关。

> **Important**
>
> 在删除 S 文件网关之前，请确保当前没有应用程序写入该网关的缓存。如果您在网关使用期间删除网关，则会造成数据丢失。

> **Warning**
>
> 删除网关后便无法恢复。

7. 删除旧网关 VM 或 Amazon EC2 实例。

删除网关和移除关联的资源

如果您不打算继续使用您的网关，则可以考虑删除该网关及其相关资源。删除资源可避免您不打算继续使用的资源产生费用并帮助减少您的月度账单的费用。

删除网关后，该网关将不再出现在 AWS Storage Gateway 管理控制台上，其系统连接也将关闭。所有类型的网关的删除过程都相同；但是，根据您要删除的网关的类型以及该网关部署到的主机，您应按照特定说明移除相关资源。

您可使用 Storage Gateway 控制台或以编程方式删除网关。您可以在下面找到有关如何使用 Storage Gateway 控制台删除网关的信息。如果要以编程方式删除网关，请参阅 AWS Storage Gateway API 参考。

使用 Storage Gateway 控制台删除网关

所有类型的网关的删除过程都相同。但是，根据您要删除的网关的类型以及该网关部署到的主机，您可能必须执行额外的任务才能删除与网关相关的资源。删除这些资源可帮助您避免为不打算使用的资源付费。

> **Note**
>
> 对于部署在 Amazon EC2 实例上的网关，实例将继续存在，直到您删除它。
> 对于部署在虚拟机 (VM) 上的网关，在您删除网关后，网关 VM 仍将存在于您的虚拟化环境中。要移除虚拟机，请使用 VMware vSphere 客户端、Microsoft Hyper-V Manager 或基于 Linux 内核的虚拟机 (KVM) 客户端连接到主机并移除虚拟机。请注意，您无法重复使用已删除的网关的 VM 来激活新网关。

删除网关

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 选择网关，然后选择一个或多个要删除的网关。
3. 对于 Actions (操作)，请选择 Delete gateway (删除网关)。此时会显示确认对话框。

   > **Warning**
   >
   > 在执行此步骤之前，请确保当前没有应用程序正写入到网关的卷。如果您在网关使用期间删除网关，则可能造成数据丢失。网关删除后便无法恢复。

4. 确认要删除指定的网关，然后在确认框中键入单词 delete 并选择删除。
5. （可选）如果您想提供有关已删除网关的反馈，请完成反馈对话框，然后选择提交。否则，请选择跳过。

> **Important**
>
> 删除网关后，您就不用再为软件付费，但 Amazon S3 存储桶和 Amazon EC2 实例等资源仍然存在。移除文件网关后，您可以移除网关 Amazon EC2 实例。

性能和优化

本节介绍优化文件网关性能的指导和最佳实践。

主题

- 的基本性能指南
- 优化网关性能
- 更大限度地提高 S3 文件网关吞吐量
- 为 SQL Server 数据库备份优化 S3 文件网关

的基本性能指南

在本节中，您可以找到有关为 FSx 文件网关虚拟机配置硬件的指南。表中列出的实例配置是示例，仅供参考。

为获得最佳性能，必须将缓存磁盘大小调整为活动工作集的大小。使用多个本地磁盘进行缓存时，可以通过并行访问数据来提高写入性能，从而提高 IOPS。

> **Note**
>
> 我们建议您不要使用短暂存储。有关使用短暂存储的更多信息，请参阅将临时存储与 EC2 网关结合使用。
> 连接到文件网关的文件系统中各个目录的建议大小限制为每个目录 1 万个文件。您可以将文件网关用于包含超过 1 万个文件的目录，但性能可能会受到影响。

在下表中，缓存命中读取操作从缓存提供的文件数据中读取。缓存未读操作是从 Amazon for Windows 文件服务器提供的文件数据中读 FSx 取的。

下表显示了 FSx 文件网关配置示例。

FSx Windows 客户端上的文件网关性能

示例配置	协议	写入吞吐量（文件大小 1 GB）	缓存命中读取吞吐量	缓存未命中读取吞吐量
根磁盘：80 GB，io1 SSD，4000 IOPS 缓存磁盘：2 x 2 TiB NVME 最低网络性能：10 Gbps CPU：32 vCPU | 内存：244 GB	SMBv3 -1 个话题	162 MiB/sec (1.4 Gbps)	403 MiB/sec (3.4 Gbps)	288 MiB/sec (2.4 Gbps)
	SMBv3 -8 个话题	511 MiB/sec (4.3 Gbps)	571 MiB/sec (4.8 Gbps)	567 MiB/sec (4.8 Gbps)

> **Note**
>
> 您的性能可能因主机平台配置和网络带宽而异。写入吞吐量性能会随着文件大小增大而降低，小文件（小于 32MiB）可实现的最高吞吐量为每秒 16 个文件。

优化网关性能

您可以在下面找到有关如何优化网关性能的信息。向网关添加资源以及向应用程序服务器添加资源是这些指导的基础。

在网关中添加资源

您可以使用以下一种或多种方法在网关中添加资源以优化网关性能。

使用更高性能的磁盘

要优化网关性能，您可以添加高性能磁盘，例如固态硬盘 (SSDs) 和控制器。 NVMe 您还可以直接从存储区域网络 (SAN) 而不是 Microsoft Hyper-V NTFS 将虚拟磁盘连接到 VM。磁盘性能的提高

通常会带来更好的吞吐量和更多的每秒 input/output 操作次数 (IOPS)。有关添加磁盘的信息，请参阅配置额外的缓存存储。

要测量吞吐量，请将 `ReadBytes` 和 `WriteBytes` 指标与 `Samples` Amazon CloudWatch 统计数据结合使用。例如，5 分钟的采样周期内的 `Samples` 指标的 `ReadBytes` 统计数据除以 300 秒可以得出 IOPS。一般来说，查看网关的这些指标时，应注意低吞吐量和低 IOPS 趋势，以便显示与磁盘相关的瓶颈。

> **Note**
>
> CloudWatch 并非所有网关都提供指标。有关网关指标的信息，请参阅监控您的 文件网关。

添加 CPU 资源到您的网关主机

网关主机服务器的最低要求是四个虚拟服务器。要优化网关性能，请确认分配给网关 VM 的四个虚拟处理器由四个内核提供支持。此外，请确认您没有超额订阅主机 CPUs 服务器的。

CPUs 向网关主机服务器添加其他内容时，可以提高网关的处理能力。这样一来，您的网关就可以并行处理将应用程序中的数据存储到本地存储以及将这些数据上传到适用FSx 于 Windows 文件服务器的 文件服务器。其他 CPUs 功能还有助于确保您的网关在与其他主机共享主机时获得足够的 CPU 资源 VMs。提供足够的 CPU 资源通常能取得增加吞吐量的效果。

Storage Gateway 支持 CPUs 在网关主机服务器中使用 24。您可以使用 24 CPUs 来显著提高网关的性能。我们建议您对网关主机服务器使用以下网关配置：

- 24 CPUs。
- 16 GiB 预留 RAM 用于文件网关
  - 对于缓存大小不超过 16 TiB 的网关，预留 16 GiB 的 RAM
  - 对于缓存大小为 16 TiB 至 32 TiB 的网关，预留 32 GiB 的 RAM
  - 对于缓存大小为 32 TiB 至 64 TiB 的网关，预留 48 GiB 的 RAM
- 磁盘 1 附加到半虚拟化控制器 1，将按如下方式用作网关缓存：
  - 使用 NVMe 控制器的固态硬盘。
- 在虚拟机网络 1 上配置网络适配器 1：
  - 使用虚拟机网络 1 并添加 VMXnet3 (10 Gbps) 以用于摄取。
- 在虚拟机网络 2 上配置网络适配器 2：
  - 使用虚拟机网络 2 并添加 VMXnet3 (10 Gbps) 以用于连接。 AWS

使用独立物理磁盘支持网关虚拟磁盘

在预置网关磁盘时，我们强烈建议您不要为使用相同底层物理存储磁盘的本地存储预置本地磁盘。例如，对于 VMware ESXi，底层物理存储资源表示为数据存储。部署网关 VM 时，您可选择用来存储 VM 文件的数据存储。在预置虚拟磁盘时（例如，作为上传缓冲区），您可以将虚拟磁盘存储在与 VM 相同的数据存储中，也可以将其存储在不同的数据存储中。

如果您有多个数据存储，则强烈建议为要创建的每个类型的本地存储选择一个数据存储。仅由一个底层物理磁盘支持的数据存储可能会导致性能下降。例如，在使用此类磁盘同时支持网关设置中的缓存存储和上传缓冲区时。同样，由性能不太高的 RAID 配置（如 RAID 1）支持的数据存储可能会导致性能下降。

向应用程序环境添加资源

提高应用程序服务器和网关之间的带宽

要优化网关性能，请确保应用程序和网关之间的网络带宽可满足您的应用程序需求。您可以使用网关的 `ReadBytes` 和 `WriteBytes` 指标来测量总数据吞吐量。

对于您的应用程序，请将测得的吞吐量与所需的吞吐量进行比较。如果测得吞吐量小于预期吞吐量，那么如果网络是瓶颈，提高应用程序和网关间的带宽可改善性能。同样地，您可以增加 VM 和本地磁盘之间的带宽 (如果它们不是直接连接的)。

向应用程序环境添加 CPU 资源

如果您的应用程序可以使用额外的 CPU 资源，那么添加更多 CPU 资源 CPUs 可以帮助您的应用程序扩展其 I/O 负载。

文件网关上的某些 FSx 文件操作（例如顶级文件夹重命名或权限更改）可能会导致多个文件操作，从而导致您 FSx 的 Windows 文件服务器文件系统 I/O 负载过高。如果您的文件系统没有足够的性能资源来处理您的工作负载，则文件系统可能会删除卷影副本，因为它优先考虑持续的可用性 I/O 而不是历史卷影副本的保留。

在 Amazon FSx 控制台中，查看监控和性能页面，查看您的文件系统是否配置不足。如果是，您可以切换到 SSD 存储、增加吞吐能力或增加 SSD IOPS 来处理您的工作负载。

更大限度地提高 S3 文件网关吞吐量

以下各节说明了更大限度地提高 NFS 和 SMB 客户端、S3 文件网关和 Amazon S3 之间吞吐量的最佳实践。各节中提供的指导有助于逐步提高总体吞吐量。虽然这些建议都不是必需的，也不是相互依赖

的，但它们是按照逻辑方式选择和排序的， 支持 用于测试和调整 S3 File Gateway 的实现。在实施和测试这些建议时，请记住，每个 S3 文件网关部署都是独特的，因此您的结果可能会有所不同。

S3 文件网关提供了一个文件接口，用于使用行业标准 NFS 或 SMB 文件协议存储和检索 Amazon S3 对象，文件和对象之间具有原生 1:1 映射。您可以将 S3 文件网关作为虚拟机部署在您 VMware的 Microsoft Hyper-V 或 Linux KVM 环境中，或者作为亚马逊 EC2 实例部署在 AWS 云中。S3 文件网关并不是设计用来完全替代企业级 NAS。S3 文件网关模拟文件系统，但它不是文件系统。使用 Amazon S3 作为持久后端存储会给每项 I/O 操作带来额外的开销，因此，与现有 NAS 或文件服务器相比，评估 S3 文件网关性能并不是等同的比较。

将网关部署在与客户端相同的位置

建议将 S3 文件网关虚拟设备部署在尽可能靠近 NFS 或 SMB 客户端的物理位置，从而尽可能缩短两者之间的网络延迟。在为网关选择位置时，请考虑以下事项：

- 降低网关的网络延迟有助于提高 NFS 或 SMB 客户端的性能。
- S3 文件网关设计为能够容忍网关与 Amazon S3 之间较高的网络延迟，但无法容忍网关与客户端之间的高延迟。
- 对于部署在 Amazon EC2 中的 S3 文件网关实例，建议将网关和 NFS 或 SMB 客户端放在同一个置放群组中。有关更多信息，请参阅《Amazon Elastic Compute Cloud 用户指南》中的 Amazon EC2 实例的置放群组。

减少磁盘速度慢引起的瓶颈

我们建议您监控该`IoWaitPercent` CloudWatch 指标，以确定可能由于 S3 文件网关上存储磁盘缓慢而导致的性能瓶颈。尝试优化与磁盘相关的性能问题时，请考虑以下几点：

- `IoWaitPercent` 报告 CPU 等待根磁盘或缓存磁盘返回响应所花费的时间占总时间的百分比。
- 当 `IoWaitPercent` 大于 5-10% 时，这通常表示由于磁盘性能不佳而引起网关性能瓶颈。该指标应尽可能接近 0%（这意味着网关几乎从不需要等待磁盘响应），从而有助于优化 CPU 资源的使用。
- 您可以`IoWaitPercent`在 Storage Gateway 控制台的 “监控” 选项卡上进行查看，或者将推荐的 CloudWatch 警报配置为在指标峰值超过特定阈值时自动通知您。有关更多信息，请参阅为您的网关创建推荐的 CloudWatch 警报。
- 我们建议使用 NVMe 或 SSD 作为网关的根磁盘和缓存磁盘，以最大限度地减少网关的根磁盘和缓存磁盘`IoWaitPercent`。

调整 CPU、RAM 和缓存磁盘的虚拟机资源分配

尝试优化 S3 文件网关的吞吐量时，重要的是为网关 VM 分配足够的资源，包括 CPU、RAM 和缓存磁盘。4 CPUs、16GB RAM 和 150GB 缓存存储空间的最低虚拟资源要求通常仅适用于较小的工作负载。在为较大的工作负载分配虚拟资源时，建议执行以下操作：

- 根据您的 S3 文件网关生成的典型 CPU 使用率，将分配的数量增加到 16 到 48 之间。 CPUs 您可以使用 `UserCpuPercent` 指标监控 CPU 使用率。有关更多信息，请参阅了解网关指标。
- 将分配的 RAM 增加到 32 GB 至 64 GB。

  > **Note**
  >
  > S3 文件网关使用的 RAM 不能超过 64 GB。

- 使用 NVMe 或 SSD 作为根磁盘和缓存磁盘，并调整缓存磁盘的大小，使其与计划写入网关的峰值工作数据集保持一致。有关更多信息，请参阅 Amazon Web Services 官方 YouTube 频道上的 S3 文件网关缓存大小调整最佳实践。
- 向网关添加至少 4 个虚拟缓存磁盘，而不是使用单个大磁盘。即使多个虚拟磁盘共享同一个底层物理磁盘，也可以提高性能，但是当虚拟磁盘位于不同的底层物理磁盘上时，性能提高通常会更大。

  例如，如果要部署 12TB 的缓存，则可以使用以下配置之一：

  - 4 x 3 TB 缓存磁盘
  - 8 x 1.5 TB 缓存磁盘
  - 12 x 1 TB 缓存磁盘

  通过这种方式，除了提高性能外，还可以随着时间的推移更有效地管理虚拟机。随着工作负载的变化，您可以逐步增加缓存磁盘的数量和总体缓存容量，同时让每个虚拟磁盘保持原始大小以确保网关的完整性。

  有关更多信息，请参阅确定本地磁盘存储量。

将 S3 文件网关部署为 Amazon EC2 实例时，请考虑以下事项：

- 您选择的实例类型会显著影响网关性能。Amazon EC2 为调整 S3 文件网关实例的资源分配提供了广泛的灵活性。
- 有关为 S3 文件网关推荐的 Amazon EC2 实例类型，请参阅对 Amazon EC2 实例类型的要求。

- 您可以更改托管活动 S3 文件网关的 Amazon EC2 实例类型。这使您可以轻松调整 Amazon EC2 硬件生成和资源分配，以找到理想的 price-to-performance比率。要更改实例类型，请在 Amazon EC2 中执行以下步骤：

  1. 停止 Amazon EC2 实例。
  2. 更改 Amazon EC2 实例类型。
  3. 启动 Amazon EC2 实例。

  > **Note**
  >
  > 停止托管 S3 文件网关的实例会暂时中断文件共享访问。如有必要，请务必提前安排维护时段。

- Amazon EC2 实例的 price-to-performance比率是指以您支付的价格获得的计算能力。通常，新一代的 Amazon EC2 实例提供的 price-to-performance比率最高，与老一代实例相比，硬件更新，性能更高，成本相对较低。实例类型、区域和使用模式等因素也会影响该比率，因此，为特定工作负载选择合适的实例，对于实现成本效益的最优化非常重要。

调整 SMB 安全级别

该 SMBv3 协议允许 SMB 签名和 SMB 加密，这在性能和安全性方面有一些权衡。要优化吞吐量，您可以调整网关的 SMB 安全级别，指定在客户端连接时实施了哪些安全功能。有关更多信息，请参阅为网关设置安全级别。

调整 SMB 安全级别时，需考虑以下事项：

- S3 文件网关的默认安全级别为强制加密。此设置对与网关文件共享的 SMB 客户端连接强制执行加密和签名，这意味着从客户端到网关的所有流量都经过加密。此设置不影响从网关到的流量 AWS，该流量始终处于加密状态。

  网关将每个加密的客户端连接限制为一个 vCPU。例如，如果您只有 1 个加密客户端，则即使为网关分配了 4 个或更多 v，该客户端CPUs 也只能使用 1 个 vCPU。因此，从单个客户端到 S3 文件网关的加密连接的吞吐量通常在 40-60 MB/s 之间会出现瓶颈。

- 如果您的安全要求允许更宽松的情形，则可以将安全级别更改为客户端协商，这样会禁用 SMB 加密且仅实施 SMB 签名。使用此设置，客户端与网关的连接可以利用多个 vCPUs，这通常会提高吞吐量性能。

> **Note**
>
> 更改 S3 文件网关的 SMB 安全级别后，必须在 Storage Gateway 控制台中等待文件共享状态从正在更新更改为可用，然后断开并重新连接 SMB 客户端，新设置才能生效。

使用多个线程和客户端来并行执行写入操作

通过一次仅使用一个 NFS 或 SMB 客户端来写入一个文件的 S3 文件网关很难实现最大吞吐量性能，因为从单个客户端按顺序写入是单线程操作。相反，建议从每个 NFS 或 SMB 客户端使用多个线程来并行写入多个文件，并同时使用多个 NFS 或 SMB 客户端写入到 S3 文件网关，从而更大限度地提高网关吞吐量。

使用多个线程可以显著提高性能。但是，使用更多线程需要更多系统资源，如果网关的大小不能满足增加的负载，这可能会对性能产生负面影响。在典型的部署中，随着添加更多线程和客户端，预期可以获得更好的吞吐量性能，直到达到网关的最大硬件和带宽限制。建议试用不同的线程数，以便针对您的特定硬件和网络配置，在速度和系统资源使用之间找到最佳平衡。

请参考以下关于常用工具的信息，这些工具可以帮助您测试线程和客户端配置：

- 您可以使用诸如 robocopy 之类的工具将一组文件复制到网关上的文件共享，从而测试多线程写入性能。默认情况下，robocopy 在复制文件时使用 8 个线程，但您最多可以指定 128 个线程。

  要在 robocopy 中使用多个线程，请在命令中添加 `/MT:n` 开关，其中 n 是要使用的线程数。例如：

  ```
  robocopy C:\source D:\destination /MT:64
  ```

  此命令将使用 64 个线程进行复制操作。

  > **Note**
  >
  > 在测试最大吞吐量时，我们不建议使用 Windows 资源管理器来拖放文件，因为此方法仅限于单个线程并会按顺序复制文件。

  有关更多信息，请参阅 Microsoft Learn 网站上的 robocopy。
- 您也可以使用常见的存储基准测试工具（例如 DISKSPD 或 FIO）进行测试。这些工具提供了调整线程数、I/O 深度和其他参数的选项，可以满足您的特定工作负载要求。

DiskSpd 允许您使用-t参数控制线程数。例如：

```
diskspd -c10G -d300 -r -w50 -t64 -o32 -b1M -h -L C:\testfile.dat
```

此示例命令执行以下操作：

- 创建一个 10 GB 的测试文件（ -c1G ）
- 运行 300 秒（ -d300 ）
- 执行随机 I/O 测试，50% 读取 50% 写入 (-r -w50)
- 使用 64 个线程（ -t64 ）
- 将每个线程的队列深度设置为 32（ -o32 ）
- 使用 1MB 的区块大小（ -b1M ）
- 禁用硬件和软件缓存（ -h -L ）

有关更多信息，请参阅 Microsoft Learn 网站上的 Use DISKSPD to test workload storage performance。

- FIO 使用 numjobs 参数来控制并行线程的数量。例如：

```
fio --name=mixed_test --rw=randrw --rwmixread=70 --bs=1M -- iodepth=64
--size=10G --runtime=300 --numjobs=64 --ioengine=libaio --direct=1 --
group_reporting
```

此示例命令执行以下操作：

- 执行随机 I/O 测试 (--rw=randrw)
- 执行 70% 读取和 30% 写入（ --rwmixread=70 ）
- 使用 1MB 的区块大小（ --bs=1M ）
- 将 I/O 深度设置为 64 (--iodepth=64)
- 在 10 GB 文件上进行测试（ --size=10G ）
- 运行 5 分钟（ --runtime=300 ）
- 创建 64 个并行作业（线程）（ --numjobs=64 ）
- 使用异步 I/O 引擎 (--ioengine=libaio)
- 对结果进行分组以便于分析（ --group_reporting ）

有关更多信息，请参阅 fio Linux man 页面。

关闭自动缓存刷新

借助自动缓存刷新功能，您的 S3 文件网关可以自动刷新其元数据，从而有助于捕获用户或应用程序通过直接写入 Amazon S3 存储桶（而不是通过网关）对您的文件集所作的任何更改。有关更多信息，请参阅刷新 Amazon S3 存储桶对象缓存。

为了优化网关吞吐量，建议在对 Amazon S3 存储桶的所有读取和写入都通过 S3 文件网关来执行的部署中关闭此功能。

在配置自动缓存刷新时，请考虑以下事项：

- 如果您因为部署中的用户或应用程序偶尔会直接写入 Amazon S3 而需要使用自动缓存刷新，那么建议在满足业务需求的前提下配置尽可能长的刷新时间间隔。较长的缓存刷新间隔有助于减少在浏览目录或修改文件时网关需要执行的元数据操作的数量。

  例如：如果您的工作负载可以接受，将自动缓存刷新设置为 24 小时而不是 5 分钟。
- 最短时间间隔为 5 分钟。最大间隔为 30 天。
- 如果您选择设置非常短的缓存刷新间隔，建议您测试 NFS 和 SMB 客户端的目录浏览体验。刷新网关缓存所需的时间会大幅增加，具体取决于您的 Amazon S3 存储桶中文件和子目录的数量。

增加 Amazon S3 上传程序线程数

默认情况下，S3 文件网关为 Amazon S3 数据上传打开 8 个线程，这对大多数典型部署来说已经提供了足够的上传能力。但是，网关接收 NFS 和 SMB 客户端数据的速率可能高于以标准 8 线程能力上传到 Amazon S3 的速率，从而导致本地缓存达到其存储限制。

在特定情况下， 支持 可以将网关的 Amazon S3 上传线程池数量从 8 增加到 40，从而允许并行上传更多数据。根据您的部署特定的带宽和其他因素，这可以显著提高上传性能，并有助于减少支持您的工作负载所需的缓存存储。

我们建议使用该`CachePercentDirty` CloudWatch 指标来监控存储在本地网关缓存磁盘上但尚未上传到 Amazon S3 的数据量，并联系 支持 以帮助确定增加上传线程池数量是否会提高 S3 文件网关的吞吐量。有关更多信息，请参阅了解网关指标。

> **Note**
>
> 此设置会消耗额外的网关 CPU 资源。建议监控网关 CPU 使用率，并在必要时增加分配的 CPU 资源。

增大 SMB 超时设置

当 S3 文件网关将大文件复制到 SMB 文件共享时，SMB 客户端连接在长时间操作后可能会超时。

建议将 SMB 客户端的 SMB 会话超时设置延长到 20 分钟或更长时间，具体取决于文件大小和网关的写入速度。默认值为 300 秒，即 5 分钟。有关更多信息，请参阅[您的网关备份作业失败，或在对网关进行写入时出现错误]。

为兼容的应用程序开启操作锁定

默认情况下，每个新的 S3 文件网关都会启用操作锁定（oplock）。在兼容的应用程序中使用操作锁定时，客户端会将多个较小的操作合并成更大的操作，这对客户端、网关和网络来说效率更高。如果您使用的是利用客户端本地缓存的应用程序（例如 Microsoft Office、Adobe Suite 等），建议开启操作锁定，这样可以显著提高性能。

如果您关闭操作锁定，则支持操作锁定的应用程序打开大文件（50 MB 或更大）的速度通常会慢得多。之所以出现这种延迟，是因为网关以 4 KB 的部分发送数据，这会导致吞吐量高 I/O 而低。

根据工作文件集的大小调整网关容量

网关容量参数指定网关在其本地缓存中可存储元数据的最大文件数量。默认情况下，网关容量设置为小，这意味着网关最多可存储 500 万个文件的元数据。因为在典型部署中，在任意时刻用户或应用通常只会访问一小部分文件，所以即使 Amazon S3 中有数亿甚至数十亿个对象，默认设置对大多数工作负载都能很好地运行。这组文件称为“工作集”。

如果您的工作负载经常访问大于 500 万个文件的工作集，则您的网关将需要频繁执行缓存移出操作，这些移出是存储在 RAM 中并保留在根磁盘上的小 I/O 操作。因为网关会从 Amazon S3 获取新数据，所以这样做会对网关性能产生负面影响。

您可以监控 `IndexEvictions` 指标以确定其元数据已从缓存中移出的文件数量，从而为新条目腾出空间。有关更多信息，请参阅[了解网关指标]。

建议使用 `UpdateGatewayInformation` API 操作来增加网关容量，使其与典型工作集中的文件数量相对应。有关更多信息，请参阅 [UpdateGatewayInformation]。

> **Note**
>
> 增加网关容量需要额外的 RAM 和根磁盘容量。
>
> - 小（500 万个文件）容量至少需要 16 GB 的 RAM 和 80 GB 的根磁盘。

- 中（1000 万个文件）容量至少需要 32 GB 的 RAM 和 160 GB 的根磁盘。
- 大（2000 万个文件）容量需要 64 GB 的 RAM 和 240 GB 的根磁盘。

Important

网关容量无法减少。

为更大的工作负载部署多个网关

建议尽可能将工作负载分散到多个网关，而不是在单个大型网关上整合许多个文件共享。例如，您可以将一个使用非常频繁的文件共享单独部署在一个网关上，而将多个使用频率较低的文件共享集中部署在另一个网关上。

在规划具有多个网关和文件共享的部署时，请考虑以下几点：

- 单个网关上文件共享的最大数量为 50，但是网关管理的文件共享数量会影响网关的性能。有关更多信息，请参阅具有多个文件共享的网关的性能指导。
- 每个 S3 文件网关上的资源由所有文件共享共同使用，不会进行划分。
- 使用量大的单个文件共享会影响网关上其他文件共享的性能。

Note

我们不建议从多个网关创建映射到同一个 Amazon S3 位置的多个文件共享，除非其中至少有一个文件共享是只读的。
从多个网关同时向同一个文件执行写入操作属于多写入器场景，这可能会导致数据完整性问题。

为 SQL Server 数据库备份优化 S3 文件网关

数据库备份是 S3 文件网关的常见和推荐使用案例，该功能将数据库备份存储在 Amazon S3 中，从而提供经济实惠的短期和长期保留，并支持根据需要将备份自动转移到成本更低的存储层级。借助此解决方案，您可以使用 SQL Server Management Studio 和 Oracle RMAN 等内置工具减少对企业备份应用程序的需求。

以下各节介绍调优 S3 文件网关部署的最佳实践，以实现高性能，并经济高效地支持数百 TB 的 SQL 数据库备份。各节中提供的指导有助于逐步提高总体吞吐量。虽然这些建议都不是必需的，也不是相互依赖的，但它们是按照逻辑方式选择和排序的， 支持 用于测试和调整 S3 File Gateway 的实现。在实施和测试这些建议时，请记住，每个 S3 文件网关部署都是独特的，因此您的结果可能会有所不同。

S3 文件网关提供了一个文件接口，用于使用行业标准 NFS 或 SMB 文件协议存储和检索 Amazon S3 对象，文件和对象之间具有原生 1:1 映射。您可以将 S3 文件网关作为虚拟机部署在您 VMware的 Microsoft Hyper-V 或 Linux KVM 环境中，或者作为亚马逊 EC2 实例部署在 AWS 云中。S3 文件网关并不是设计用来完全替代企业级 NAS。S3 文件网关模拟文件系统，但它不是文件系统。使用 Amazon S3 作为持久后端存储会给每项 I/O 操作带来额外的开销，因此，与现有 NAS 或文件服务器相比，评估 S3 文件网关性能并不是等同的比较。

将网关部署在与 SQL Server 相同的位置

建议将 S3 文件网关虚拟设备部署在尽可能靠近 SQL Server 的物理位置，从而尽可能缩短两者之间的网络延迟。在为网关选择位置时，请考虑以下事项：

- 降低网关的网络延迟有助于提高 SMB 客户端（例如，SQL Server）的性能。
- S3 文件网关设计为能够容忍网关与 Amazon S3 之间较高的网络延迟，但无法容忍网关与客户端之间的高延迟。
- 对于部署在 Amazon EC2 中的 S3 文件网关实例，建议将网关和 SQL Server 放在同一个置放群组中。有关更多信息，请参阅《Amazon Elastic Compute Cloud 用户指南》中的 Amazon EC2 实例的置放群组。

减少磁盘速度慢引起的瓶颈

我们建议您监控该`IoWaitPercent` CloudWatch 指标，以确定可能由于 S3 文件网关上存储磁盘缓慢而导致的性能瓶颈。尝试优化与磁盘相关的性能问题时，请考虑以下几点：

- `IoWaitPercent` 报告 CPU 等待根磁盘或缓存磁盘返回响应所花费的时间占总时间的百分比。
- 当 `IoWaitPercent` 大于 5-10% 时，这通常表示由于磁盘性能不佳而引起网关性能瓶颈。该指标应尽可能接近 0%（这意味着网关几乎从不需要等待磁盘响应），从而有助于优化 CPU 资源的使用。
- 您可以`IoWaitPercent`在 Storage Gateway 控制台的 “监控” 选项卡上进行查看，或者将推荐的 CloudWatch 警报配置为在指标峰值超过特定阈值时自动通知您。有关更多信息，请参阅为您的网关创建推荐的 CloudWatch 警报。
- 我们建议使用 NVMe 或 SSD 作为网关的根磁盘和缓存磁盘，以最大限度地减少网关的根磁盘和缓存磁盘`IoWaitPercent`。

调整 S3 文件网关虚拟机的 CPU、RAM 和缓存磁盘资源分配

尝试优化 S3 文件网关的吞吐量时，重要的是为网关 VM 分配足够的资源，包括 CPU、RAM 和缓存磁盘。4 CPUs、16GB RAM 和 150GB 缓存存储空间的最低虚拟资源要求通常仅适用于较小的工作负载。在为较大的工作负载分配虚拟资源时，建议执行以下操作：

- 根据您的 S3 文件网关生成的典型 CPU 使用率，将分配的数量增加到 16 到 48 之间。 CPUs 您可以使用 `UserCpuPercent` 指标监控 CPU 使用率。有关更多信息，请参阅了解网关指标。
- 将分配的 RAM 增加到 32 GB 至 64 GB。

> **Note**
>
> S3 文件网关使用的 RAM 不能超过 64 GB。

- 使用 NVMe 或 SSD 作为根磁盘和缓存磁盘，并调整缓存磁盘的大小，使其与计划写入网关的峰值工作数据集保持一致。有关更多信息，请参阅 Amazon Web Services 官方 YouTube 频道上的 S3 文件网关缓存大小调整最佳实践。
- 向网关添加至少 4 个虚拟缓存磁盘，而不是使用单个大磁盘。即使多个虚拟磁盘共享同一个底层物理磁盘，也可以提高性能，但是当虚拟磁盘位于不同的底层物理磁盘上时，性能提高通常会更大。

  例如，如果要部署 12TB 的缓存，则可以使用以下配置之一：

  - 4 x 3 TB 缓存磁盘
  - 8 x 1.5 TB 缓存磁盘
  - 12 x 1 TB 缓存磁盘

  通过这种方式，除了提高性能外，还可以随着时间的推移更有效地管理虚拟机。随着工作负载的变化，您可以逐步增加缓存磁盘的数量和总体缓存容量，同时让每个虚拟磁盘保持原始大小以确保网关的完整性。

  有关更多信息，请参阅确定本地磁盘存储量。

将 S3 文件网关部署为 Amazon EC2 实例时，请考虑以下事项：

- 您选择的实例类型会显著影响网关性能。Amazon EC2 为调整 S3 文件网关实例的资源分配提供了广泛的灵活性。
- 有关为 S3 文件网关推荐的 Amazon EC2 实例类型，请参阅对 Amazon EC2 实例类型的要求。

- 您可以更改托管活动 S3 文件网关的 Amazon EC2 实例类型。这使您可以轻松调整 Amazon EC2 硬件生成和资源分配，以找到理想的 price-to-performance比率。要更改实例类型，请在 Amazon EC2 中执行以下步骤：

  1. 停止 Amazon EC2 实例。
  2. 更改 Amazon EC2 实例类型。
  3. 启动 Amazon EC2 实例。

  > **Note**
  >
  > 停止托管 S3 文件网关的实例会暂时中断文件共享访问。如有必要，请务必提前安排维护时段。

- Amazon EC2 实例的 price-to-performance比率是指以您支付的价格获得的计算能力。通常，新一代的 Amazon EC2 实例提供的 price-to-performance比率最高，与老一代实例相比，硬件更新，性能更高，成本相对较低。实例类型、区域和使用模式等因素也会影响该比率，因此，为特定工作负载选择合适的实例，对于实现成本效益的最优化非常重要。

通过调整 S3 文件网关的安全级别来提高 SMB 客户端吞吐量

该 SMBv3 协议允许 SMB 签名和 SMB 加密，这在性能和安全性方面有一些权衡。要优化吞吐量，您可以调整网关的 SMB 安全级别，指定在客户端连接时实施了哪些安全功能。有关更多信息，请参阅为网关设置安全级别。

调整 SMB 安全级别时，需考虑以下事项：

- S3 文件网关的默认安全级别为强制加密。此设置对与网关文件共享的 SMB 客户端连接强制执行加密和签名，这意味着从客户端到网关的所有流量都经过加密。此设置不影响从网关到的流量 AWS，该流量始终处于加密状态。

  网关将每个加密的客户端连接限制为一个 vCPU。例如，如果您只有 1 个加密客户端，则即使为网关分配了 4 个或更多 v，该客户端CPUs 也只能使用 1 个 vCPU。因此，从单个客户端到 S3 文件网关的加密连接的吞吐量通常在 40-60 MB/s 之间会出现瓶颈。

- 如果您的安全要求允许更宽松的情形，则可以将安全级别更改为客户端协商，这样会禁用 SMB 加密且仅实施 SMB 签名。使用此设置，客户端与网关的连接可以利用多个 vCPUs，这通常会提高吞吐量性能。

> **Note**
>
> 更改 S3 文件网关的 SMB 安全级别后，必须在 Storage Gateway 控制台中等待文件共享状态从正在更新更改为可用，然后断开并重新连接 SMB 客户端，新设置才能生效。

通过将 SQL 备份拆分为多个文件来提高 SMB 客户端吞吐量

- 通过一次仅使用一个 SQL Server 来写入一个文件的 S3 文件网关很难实现最大吞吐量性能，因为从单个 SQL Server 按顺序写入是单线程操作。相反，建议从每个 SQL Server 使用多个线程来并行写入多个文件，并同时使用多个 SQL Server 写入到 S3 文件网关，从而更大限度地提高网关吞吐量。对于 SQL 备份，将备份拆分为多个文件，让每个文件可以使用单独的线程，每个单独的线程可将多个文件同时写入 S3 文件网关文件共享。您拥有的线程越多，所能达到的吞吐量就越高，直到达到网关本身的性能上限。
- SQL Server 支持在一次备份操作中同时写入多个文件。例如，您可以使用 T-SQL 命令或 SQL Server Management Studio（SSMS）指定多个文件目标。每个文件使用单独的线程将数据从 SQL Server 发送到网关文件共享。这种方法可以提高 I/O 吞吐量，从而显著提高备份速度和效率。

配置 SQL Server 备份时，需注意以下事项：

- 通过将备份拆分为多个文件，SQL Server 管理员可以优化备份时间并更有效地管理大型数据库备份。
- 使用的文件数量取决于服务器的存储配置和性能要求。对于大型数据库，建议将备份分成几个更小的文件，每个文件大小在 10 GB 到 20 GB 之间。
- SQL Server 在执行备份时，对可以写入的文件数量没有硬性限制，但实际决策应基于存储架构和网络带宽等现实因素来考量。

有关更多信息，请参阅:

- 通过写入多个文件，将 SQL Server 的备份速度提高了 43-67%
- 使用文件网关轻松将 SQL Server 备份存储在 Amazon S3 中

通过增大 SMB 超时设置来防止大文件复制失败

当 S3 文件网关将大型 SQL 备份文件复制到 SMB 文件共享时，SMB 客户端连接在长时间操作后可能会超时。建议将 SQL Server SMB 客户端的 SMB 会话超时设置延长到 20 分钟或更长时间，具体取决于文件大小和网关的写入速度。默认值为 300 秒，即 5 分钟。有关更多信息，请参阅[您的网关备份作业失败，或在对网关进行写入时出现错误]。

增加 Amazon S3 上传程序线程数

默认情况下，S3 文件网关为 Amazon S3 数据上传打开 8 个线程，这对大多数典型部署来说已经提供了足够的上传能力。但是，网关接收 SQL Server 数据的速率可能高于以标准 8 线程能力上传到 Amazon S3 的速率，从而导致本地缓存达到其存储限制。

在特定情况下， 支持 可以将网关的 Amazon S3 上传线程池数量从 8 增加到 40，从而允许并行上传更多数据。根据您的部署特定的带宽和其他因素，这可以显著提高上传性能，并有助于减少支持您的工作负载所需的缓存存储。

我们建议使用该`CachePercentDirty` CloudWatch 指标来监控存储在本地网关缓存磁盘上但尚未上传到 Amazon S3 的数据量，并联系 支持 以帮助确定增加上传线程池数量是否会提高 S3 文件网关的吞吐量。有关更多信息，请参阅[了解网关指标]。

> **Note**
>
> 此设置会消耗额外的网关 CPU 资源。建议监控网关 CPU 使用率，并在必要时增加分配的 CPU 资源。

关闭自动缓存刷新

借助自动缓存刷新功能，您的 S3 文件网关可以自动刷新其元数据，从而有助于捕获用户或应用程序通过直接写入 Amazon S3 存储桶（而不是通过网关）对您的文件集所作的任何更改。有关更多信息，请参阅[刷新 Amazon S3 存储桶对象缓存]。

为了优化网关吞吐量，建议在对 Amazon S3 存储桶的所有读取和写入都通过 S3 文件网关来执行的部署中关闭此功能。

在配置自动缓存刷新时，请考虑以下事项：

- 如果您因为部署中的用户或应用程序偶尔会直接写入 Amazon S3 而需要使用自动缓存刷新，那么建议在满足业务需求的前提下配置尽可能长的刷新时间间隔。较长的缓存刷新间隔有助于减少在浏览目录或修改文件时网关需要执行的元数据操作的数量。

  例如：如果您的工作负载可以接受，将自动缓存刷新设置为 24 小时而不是 5 分钟。
- 最短时间间隔为 5 分钟。最大间隔为 30 天。
- 如果您选择设置非常短的缓存刷新间隔，建议您测试 SQL Server 的目录浏览体验。刷新网关缓存所需的时间会大幅增加，具体取决于您的 Amazon S3 存储桶中文件和子目录的数量。

部署多个网关以支持工作负载

通过将工作负载分配到多个网关，Storage Gateway 可以支持具有数百个 SQL 数据库、多个 SQL Server 和数百 TB 备份数据的大型环境的 SQL 备份。

在规划具有多个网关和 SQL Server 的部署时，请考虑以下几点：

- 在有足够的硬件资源和带宽的情况下，单个网关通常每天最多可以上传 20 TB。您可以通过增加 Amazon S3 上传程序线程数，将此限制提高到每天 40 TB。
- 我们建议进行 proof-of-concept测试以衡量性能并考虑部署中的所有变量。确定 SQL 备份工作负载的峰值吞吐量后，您可以扩展网关数量以满足您的需求。
- 因为数据库的数量和数据库的大小可能会随着时间的推移而增加，建议您在设计解决方案时考虑到增长。要继续扩展和支持不断增加的工作负载，您可以根据需要部署额外网关。

用于数据库备份工作负载的其他资源

- 使用将 SQL Server 备份存储在 Amazon S3 中 AWS Storage Gateway
- 使用文件网关轻松将 SQL Server 备份存储在 Amazon S3 中
- AWS Storage Gateway 用于在 Amazon S3 中存储 Oracle 数据库备份
- Backing up Oracle databases to Amazon S3 at scale
- 使用将 SAP ASE 数据库集成到 Amazon S3 AWS Storage Gateway
- 一个 AWS 英雄如何使用云端 AWS Storage Gateway 备份
- S3 File Gateway cache sizing best practices

AWS Storage Gateway 中的安全

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

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云安全 — AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。 AWS 还为您提供可以安全使用的服务。作为AWS 合规计划合规计划合规计划合的一部分，第三方审计师定期测试和验证我们安全的有效性。要了解适用于 AWS Storage Gateway 的合规计划，请参阅按合规计划提供的范围内的 AWSAWS 服务按合规计划服务。
- 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、您公司的要求以及适用的法律法规。

此文档有助于您了解如何在使用 Storage Gateway 时应用责任共担模式。以下主题说明如何配置 Storage Gateway 来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 Storage Gateway 资源。

AWS Storage Gateway 中的数据保护

AWS 分担责任模型分担责任模型适用于 AWS Storage Gateway 中的数据保护。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS 云。您负责维护对托管在此基础结构上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS Security Blog 上的 AWS Shared Responsibility Model and GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 用于 SSL/TLS 与 AWS 资源通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。有关使用 CloudTrail 跟踪捕获 AWS 活动的信息，请参阅《AWS CloudTrail 用户指南》中的使用跟 CloudTrail 踪。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。

- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-3 版》https://aws.amazon.com/compliance/fips/。

强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您使用控制台、API 或 AWS 服务 使用 Storage Gateway 或其他 AWS CLI网站时 AWS SDKs。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供 URL，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

使用数据加密 AWS KMS

Amazon FSx File Gateway 支持最新 SMB v3.1.1 规格以下的 SMB 加密，包括 AES 128 CCM 和 AES 128 GCM。兼容的客户端将自动使用加密进行连接。此外， FSx 文件网关在与 FSx Windows 文件服务器通信时使用 SMB 加密。 AWS您必须配置指向的 Direct Connect 链接 AWS，并设置相应的策略以允许 SMB 流量和管理流量通过。 AWS

加密文件系统

有关信息，请参阅《亚马逊 Windows 文件服务器用户指南》 FSx中的 “亚马逊 FSx 数据加密”。

使用 AWS KMS 加密数据时，请记住以下几点：

- 您的数据在云中进行静态加密。也就是说，数据在 中经过加密 FSx。
- IAM 用户必须具有调用 AWS KMS API 操作所需的权限。有关更多信息，请参阅《AWS Key Management Service 开发人员指南》中的将 IAM 策略与 AWS KMS结合使用。

> **Important**
>
> 使用 AWS KMS 密钥进行服务器端加密时，必须选择对称密钥。Storage Gateway 不支持非对称密钥。有关更多信息，请参阅 AWS Key Management Service 开发人员指南中的使用对称和非对称密钥。

有关的更多信息 AWS KMS，请参阅什么是 AWS Key Management Service？

AWS Storage Gateway 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 管理员控制谁可以进行身份验证（登录）和授权（有权限）使用 AWS SGW 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
- Stor AWS age Gateway 如何与 IAM 协作
- Storage Gateway 的基于身份的 AWS 策略示例
- AWS Storage Gateway 身份和访问疑难解答
- 使用标签控制对网关和资源的访问

受众

您的使用方式 AWS Identity and Access Management (IAM) 因您的角色而异：

- 服务用户：如果您无法访问功能，请从管理员处请求权限（请参阅AWS Storage Gateway 身份和访问疑难解答）
- 服务管理员：确定用户访问权限并提交权限请求（请参阅Stor AWS age Gateway 如何与 IAM 协作）
- IAM 管理员：编写用于管理访问权限的策略（请参阅Storage Gateway 的基于身份的 AWS 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 用户身份进行身份验证 AWS 账户根用户，或者通过担任 IAM 角色进行身份验证。

您可以使用来自身份源的证书 AWS IAM Identity Center （例如（IAM Identity Center）、单点登录身份验证或 Google/Facebook 证书，以联合身份登录。有关登录的更多信息，请参阅《AWS 登录 用户指南》中的如何登录您的 AWS 账户。

对于编程访问， AWS 提供 SDK 和 CLI 来对请求进行加密签名。有关更多信息，请参阅《IAM 用户指南》中的适用于 API 请求的AWS 签名版本 4。

AWS 账户 root 用户

创建时 AWS 账户，首先会有一个名为 AWS 账户 root 用户的登录身份，该身份可以完全访问所有资源 AWS 服务 和资源。我们强烈建议不要使用根用户进行日常任务。有关需要根用户凭证的任务，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户使用与身份提供商的联合身份验证才能 AWS 服务 使用临时证书进行访问。

联合身份是指来自您的企业目录、Web 身份提供商的用户 Directory Service ，或者 AWS 服务 使用来自身份源的凭据进行访问的用户。联合身份代入可提供临时凭证的角色。

要集中管理访问权限，建议使用。 AWS IAM Identity Center有关更多信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？。

IAM 用户和群组

IAM 用户是对某个人员或应用程序具有特定权限的一个身份。建议使用临时凭证，而非具有长期凭证的 IAM 用户。有关更多信息，请参阅 IAM 用户指南中的要求人类用户使用身份提供商的联合身份验证才能 AWS 使用临时证书进行访问。

IAM 组指定一组 IAM 用户，便于更轻松地对大量用户进行权限管理。有关更多信息，请参阅《IAM 用户指南》中的 IAM 用户使用案例。

IAM 角色

IAM 角色是具有特定权限的身份，可提供临时凭证。您可以通过从用户切换到 IAM 角色（控制台）或调用 AWS CLI 或 AWS API 操作来代入角色。有关更多信息，请参阅《IAM 用户指南》中的担任角色的方法。

IAM 角色对于联合用户访问、临时 IAM 用户权限、跨账户访问、跨服务访问以及在 Amazon EC2 上运行的应用程序非常有用。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略定义了与身份或资源关联时的权限。 AWS 在委托人提出请求时评估这些政策。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概述。

管理员使用策略，通过定义哪个主体可以在什么条件下对哪些资源执行哪些操作来指定谁有权访问什么。

默认情况下，用户和角色没有权限。IAM 管理员创建 IAM 策略并将其添加到角色中，然后用户可以担任这些角色。IAM 策略定义权限，与执行操作所用的方法无关。

基于身份的策略

基于身份的策略是您附加到身份（用户、组或角色）的 JSON 权限策略文档。这些策略控制身份可以执行什么操作、对哪些资源执行以及在什么条件下执行。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

基于身份的策略可以是内联策略（直接嵌入到单个身份中）或托管策略（附加到多个身份的独立策略）。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。您必须在基于资源的策略中指定主体。

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

其他策略类型

AWS 支持其他策略类型，这些策略类型可以设置更常见的策略类型授予的最大权限：

- 权限边界 – 设置基于身份的策略可以授予 IAM 实体的最大权限。有关更多信息，请参阅《 IAM 用户指南》中的 IAM 实体的权限边界。
- 服务控制策略 (SCPs)-在中指定组织或组织单位的最大权限 AWS Organizations。有关更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略。

- 资源控制策略 (RCPs)-设置账户中资源的最大可用权限。有关更多信息，请参阅《AWS Organizations 用户指南》中的资源控制策略 (RCPs)。
- 会话策略 – 在为角色或联合用户创建临时会话时，作为参数传递的高级策略。有关更多信息，请参阅《IAM 用户指南》中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 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。

Stor AWS age Gateway 如何与 IAM 协作

在使用 IAM 管理对 AWS SGW 的访问权限之前，请先了解有哪些 IAM 功能可用于 S AWS GW。

你可以在 AWS Storage Gateway 中使用的 IAM 功能

IAM 功能	AWS SGW 支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	是
策略条件键（特定于服务）	是
ACLs	否
ABAC（策略中的标签）	部分
临时凭证	是
转发访问会话（FAS）	是
服务角色	是
服务关联角色	是

要全面了解 AWS SGW 和其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的AWS 服务。

SGW 基于身份的策略 AWS

支持基于身份的策略：是

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

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

SGW 基于身份的策略示例 AWS

要查看 AWS SGW 基于身份的策略的示例，请参阅。Storage Gateway 的基于身份的 AWS 策略示例

SGW 内部 AWS 基于资源的政策

支持基于资源的策略：否

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

要启用跨账户访问，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

AWS SGW 的政策行动

支持策略操作：是

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

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。在策略中包含操作以授予执行关联操作的权限。

要查看 AWS SGW 操作列表，请参阅《服务授权参考》中的 AWS Storage Gateway 定义的操作。

AWS SGW 中的策略操作在操作前使用以下前缀：

```
sgw
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
      "sgw:action1",
      "sgw:action2"
         ]
```

要查看 AWS SGW 基于身份的策略的示例，请参阅。Storage Gateway 的基于身份的 AWS 策略示例

AWS SGW 的政策资源

支持策略资源：是

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

`Resource` JSON 策略元素指定要向其应用操作的一个或多个对象。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于不支持资源级权限的操作，请使用通配符 (*) 指示语句应用于所有资源。

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

要查看 AWS SGW 资源类型及其列表 ARNs，请参阅《服务授权参考》中的 AWS Storage Gateway 定义的资源。要了解您可以使用哪些操作来指定每种资源的 ARN，请参阅 AWS Storage Gateway 定义的操作。

要查看 AWS SGW 基于身份的策略的示例，请参阅。Storage Gateway 的基于身份的 AWS 策略示例

AWS SGW 的策略条件密钥

支持特定于服务的策略条件键：是

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

Condition 元素根据定义的条件指定语句何时执行。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

要查看 AWS SGW 条件密钥列表，请参阅《服务授权参考》中的 AWS Storage Gateway 条件密钥。要了解可以使用条件键的操作和资源，请参阅 AWS Storage Gateway 定义的操作。

要查看 AWS SGW 基于身份的策略的示例，请参阅。Storage Gateway 的基于身份的 AWS 策略示例

ACLs 在 AWS SGW

支持 ACLs：否

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

带有 SGW 的 ABA AWS C

支持 ABAC（策略中的标签）：部分支持

基于属性的访问权限控制（ABAC）是一种授权策略，该策略基于称为标签的属性来定义权限。您可以将标签附加到 IAM 实体和 AWS 资源，然后设计 ABAC 策略以允许在委托人的标签与资源上的标签匹配时进行操作。

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

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

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权定义权限。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

在 AWS SGW 中使用临时证书

支持临时凭证：是

临时证书提供对 AWS 资源的短期访问权限，并且是在您使用联合身份或切换角色时自动创建的。AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的临时安全凭证和使用 IAM 的。AWS 服务

转发 AWS SGW 的访问会话

支持转发访问会话（FAS）：是

转发访问会话 (FAS) 使用调用主体的权限 AWS 服务，再加上 AWS 服务 向下游服务发出请求的请求。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

AWS SGW 的服务角色

支持服务角色：是

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。

> **Warning**
>
> 更改服务角色的权限可能会中断 AWS SGW 的功能。仅当 AWS SGW 提供相关指导时才编辑服务角色。

SGW 的 AWS 服务相关角色

支持服务关联角色：是

服务相关角色是一种与服务相关联的 AWS 服务服务角色。服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务关联角色的权限。

有关创建或管理服务相关角色的详细信息，请参阅能够与 IAM 搭配使用的AWS 服务。在表中查找服务相关角色列中包含 Yes 的表。选择是链接以查看该服务的服务相关角色文档。

Storage Gateway 的基于身份的 AWS 策略示例

默认情况下，用户和角色无权创建或修改 AWS SGW 资源。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。

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

有关 AWS SGW 定义的操作和资源类型（包括每种资源类型的格式）的详细信息，请参阅《服务授权参考》中的 AWS Storage Gateway 的操作、资源和条件密钥。 ARNs

主题

- 策略最佳实践
- 使用 AWS SGW 控制台
- 允许用户查看他们自己的权限

策略最佳实践

基于身份的策略决定了某人是否可以在您的账户中创建、访问或删除 AWS SGW 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的AWS 托管策略或工作职能的AWS 托管策略。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性：IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM Access Analyzer 验证策略。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 API 访问。

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

使用 AWS SGW 控制台

要访问 AWS Storage Gateway 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您 AWS 账户的 AWS SGW 资源的详细信息。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 AWS SGW 控制台，还要将 AWS SGW *ConsoleAccess* 或*ReadOnly* 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和托管式策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

AWS Storage Gateway 身份和访问疑难解答

使用以下信息来帮助您诊断和修复在使用 AWS SGW 和 IAM 时可能遇到的常见问题。

主题

- 我无权在 AWS SGW 中执行任何操作
- 我无权执行 iam：PassRole
- 我想允许我以外的人 AWS 账户 访问我的 AWS SGW 资源

我无权在 AWS SGW 中执行任何操作

如果您收到错误提示，指明您无权执行某个操作，则必须更新策略以允许执行该操作。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 *my-example-widget* 资源的详细信息，但不拥有虚构 sgw:*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:
 sgw: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 sgw:*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

如果您收到错误消息，提示您无权执行iam:PassRole操作，则必须更新您的策略以允许您将角色传递给 AWS SGW。

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 AWS SGW 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。

> **Important**
>
> Storage Gateway 可以代入使用 `iam:PassRole` 策略操作传递的现有服务角色，但不支持使用 `iam:PassedToService` 上下文密钥将操作限制到特定服务的 IAM 策略。
> 有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的以下主题：
>
> - IAM：将 IAM 角色传递给特定 AWS 服务
> - 向用户授予将角色传递给 AWS 服务的权限
> - IAM 的可用密钥

我想允许我以外的人 AWS 账户 访问我的 AWS SGW 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解 AWS SGW 是否支持这些功能，请参阅Stor AWS age Gateway 如何与 IAM 协作。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

使用标签控制对网关和资源的访问

要控制对网关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. 根据网关资源上的标签控制对这些资源的访问。
2. 控制可以在 IAM 请求条件中传递的标签。

有关如何使用标签控制访问的信息，请参阅使用标签控制访问。

根据资源上的的标签控制访问

要控制用户或角色可以对网关资源执行的操作，您可以使用网关资源上的标签。例如，您可能希望根据文件网关资源上的标签的键/值对允许或拒绝对该资源执行特定的 API 操作。

以下示例允许用户或角色对所有资源执行 `ListTagsForResource`、`ListFileShares` 和 `DescribeNFSFileShares` 操作。仅当资源上的标签将其键设置为 `allowListAndDescribe` 并将值设置为 `yes` 时，该策略才适用。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:ListTagsForResource",
                "storagegateway:ListFileShares",
                "storagegateway:DescribeNFSFileShares"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/allowListAndDescribe": "yes"
                }
            }
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "storagegateway:*"
            ],
            "Resource": "arn:aws:storagegateway:us-east-1:111122223333:*/*"
        }
    ]
}
```

根据 IAM 请求中的标签控制访问

要控制用户可以对网关资源执行的操作，您可以根据标签在 IAM 策略中使用条件。例如，您可以编写一个策略，以根据用户在创建资源时提供的标签允许或拒绝执行特定的 API 操作。

在以下示例中，只有在用户在创建网关时提供的标签的键值对为 **Department** 和 **Finance** 时，第一条语句才允许用户创建网关。在使用该 API 操作时，您可以将该标签添加到激活请求中。

只有在网关上的标签的键值对与 **Department** 和 **Finance** 匹配时，第二条语句才允许用户在网关上创建网络文件系统 (NFS) 或服务器消息块 (SMB) 文件共享。此外，用户还必须将标签添加到文件共享中，并且标签的键/值对必须为 **Department** 和 **Finance**。在创建文件共享时，您可以将标签添加到文件共享中。没有权限执行 AddTagsToResource 或 RemoveTagsFromResource 操作，因此，用户无法对网关或文件共享执行这些操作。

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "storagegateway:ActivateGateway"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/Department":"Finance"
            }
         }
      },
      {
         "Effect":"Allow",
```

```
            "Action":[
               "storagegateway:CreateNFSFileShare",
               "storagegateway:CreateSMBFileShare"
            ],
            "Resource":"*",
            "Condition":{
               "StringEquals":{
                  "aws:ResourceTag/Department":"Finance",
                  "aws:RequestTag/Department":"Finance"
               }
            }
         }
      ]
}
```

AWS Storage Gateway 的合规性验证

作为多项合规计划的一部分，第三方审计机构评估 AWS Storage Gateway 的安全 AWS 性和合规性。其中包括 SOC、PCI、ISO、FedRAMP、HIPAA、MTCS、C5、K-ISMS、ENS High、OSPAR 和 HITRUST CSF。

有关特定合规计划范围内的 AWS 服务列表，请参阅合规计划范围内的AWS 服务按合规计划。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 Storage Gateway 时的合规性责任由您的数据的敏感性、您公司的合规性目标以及适用的法律法规决定。 AWS 提供以下资源来帮助满足合规性要求：

- 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，并提供了在上部署以安全性和合规性为重点的基准环境的步骤。 AWS
- HIPAA 安全与合规架构白皮书 — 本白皮书描述了公司如何使用来 AWS 创建符合 HIPAA 标准的应用程序。
- 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。
- 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 CSPM— 此 AWS 服务可全面了解您的安全状态 AWS ，帮助您检查是否符合安全行业标准和最佳实践。

AWS Storage Gateway 中的弹性

AWS 全球基础设施是围绕 AWS 区域 可用区构建的。

AWS 区域 是指数据中心聚集在世界各地的物理位置。每组逻辑数据中心称为一个可用区（AZ）。每个区域都至少 AWS 区域 由三个在地理区域 AZs 内隔离且物理上独立的人员组成。与其他云提供商不同，他们通常将一个区域定义为单个数据中心，而每个 AWS 区域 提供商的多可用区设计都具有明显的优势。每个可用区都有独立的电源、冷却和物理安全，并通过冗余 ultra-low-latency网络进行连接。如果您的部署需要将重点放在高可用性上，则可以将服务和资源配置为多个， AZs 以实现更高的容错能力。

AWS 区域 满足最高级别的基础架构安全性、合规性和数据保护。之间的所有流量 AZs 都经过加密。网络性能足以实现两者之间的同步复制 AZs。 AZs 简化分区服务和资源以实现高可用性。如果您的部署是分区的 AZs，则可以更好地隔离和保护您的资源免受停电、雷击、龙卷风、地震等问题的影响。AZs 在物理上与任何其他亚利桑那州相隔一定距离，尽管所有亚利桑那州彼此相距不到 100 千米（60 英里）。

有关 AWS 区域 和可用区的更多信息，请参阅AWS 全球基础设施。

除了 AWS 全球基础架构外，Storage Gateway 还支持 VMware vSphere 高可用性 (VMware HA)，以帮助保护存储工作负载免受硬件、虚拟机管理程序或网络故障的影响。有关更多信息，请参阅将 v VMware Sphere 高可用性与存储网关一起使用 vSphere 高可用性与 Storag way 配合使用。

AWS Storage Gateway 中的基础设施安全

作为一项托管服务， AWS Storage Gateway受安全支柱——Well-Architected Framework中描述的 AWS 全球网络安全程序 AWS 的保护。

您可以使用 AWS 已发布的 API 调用通过网络访问 Storage Gateway。客户端必须支持传输层安全性（TLS）1.2。客户端还必须支持具有完全向前保密（PFS）的密码套件，例如 Ephemeral Diffie-Hellman（DHE）或 Elliptic Curve Ephemeral Diffie-Hellman（ECDHE）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

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

> **Note**
>
> 您应将 AWS Storage Gateway 设备视为托管虚拟机，并且不应尝试以任何方式访问或修改其安装。尝试使用除正常网关更新机制以外的方法安装扫描软件或更新任何软件包，可能会导致网关出现故障，并可能影响我们支持或修复网关的能力。
> AWS 定期审查、分析和补救 CVEs 。作为正常软件发布周期的一部分，我们将这些问题的修复程序纳入 Storage Gateway 中。这些修复程序通常在计划的维护时段内作为正常网关更新过程的一部分应用。有关网关更新的更多信息，请参阅使用控制台管理网关更新。 AWS Storage Gateway

AWS 安全最佳实践

AWS 提供了许多安全功能，供您在制定和实施自己的安全策略时考虑。这些最佳实践是一般准则，并不代表完整的安全解决方案。这些实践可能不适合您的环境或不满足您的环境要求，请将其视为有用的考虑因素而不是惯例。有关更多信息，请参阅 AWS 安全最佳实践。

登录和监控 AWS Storage Gateway

Storage Gateway 与 AWS CloudTrail一项服务集成，该服务提供用户、角色或 AWS 服务在 Storage Gateway 中采取的操作的记录。 CloudTrail 将 Storage Gateway 的所有 API 调用捕获为事件。捕获的调用包含来自 Storage Gateway 控制台的调用和对 Storage Gateway API 操作的代码调用。如果您创建了跟踪，则可以启用向 Amazon S3 存储桶持续传输 CloudTrail 事件，包括 Storage Gateway 的事件。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的 “事件历史记录” 中查看最新的事件。使用收集的信息 CloudTrail，您可以确定向 Storage Gateway 发出的请求、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

要了解更多信息 CloudTrail，请参阅《AWS CloudTrail 用户指南》。

Storage Gateway 信息位于 CloudTrail

CloudTrail 在您创建 AWS 账户时已在您的账户上激活。当 Storage Gateway 中发生活动时，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在自己的 AWS 账户中查看、搜索和下载最近发生的事件。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录 AWS 账户中的事件，包括 Storage Gateway 的事件，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。默认情况下，当您在控制台中创建跟踪时，该跟踪将应用于所有 AWS 区域。此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送至您指定的

Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

- 创建跟踪概述
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个区域的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail 日志文件

所有 Storage Gateway 操作都会记录下来，并记录在操作主题中。例如，对`ActivateGateway`、`ListGateways`和`ShutdownGateway`操作的调用会在 CloudTrail 日志文件中生成条目。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根证书还是 AWS Identity and Access Management (IAM) 用户凭证发出。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

了解 Storage Gateway 日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

以下示例显示了演示该操作的 CloudTrail 日志条目。

```
{ "Records": [{
                "eventVersion": "1.02",
                "userIdentity": {
                "type": "IAMUser",
                "principalId": "AIDAII5AUEPBH2M7JTNVC",
                "arn": "arn:aws:iam::111122223333:user/StorageGateway-team/JohnDoe",
                "accountId": "111122223333",
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                 "userName": "JohnDoe"
```

```
                },
                   "eventTime": "2014-12-04T16:19:00Z",
                   "eventSource": "storagegateway.amazonaws.com",
                   "eventName": "ActivateGateway",
                   "awsRegion": "us-east-2",
                   "sourceIPAddress": "192.0.2.0",
                   "userAgent": "aws-cli/1.6.2 Python/2.7.6 Linux/2.6.18-164.el5",
                    "requestParameters": {
                                          "gatewayTimezone": "GMT-5:00",
                                          "gatewayName": "cloudtrailgatewayvtl",
                                          "gatewayRegion": "us-east-2",
                                          "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
                                          "gatewayType": "VTL"
                                               },
                                               "responseElements": {
                                                                     "gatewayARN":
 "arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayvtl"
                                          },
                                          "requestID":
 "54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
                                          "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
                                          "eventType": "AwsApiCall",
                                          "apiVersion": "20130630",
                                          "recipientAccountId": "444455556666"
             }]
}
```

以下示例显示了演示该 ListGateways操作的 CloudTrail 日志条目。

```
{
 "Records": [{
                "eventVersion": "1.02",
                "userIdentity": {
                                  "type": "IAMUser",
                                  "principalId": "AIDAII5AUEPBH2M7JTNVC",
                                  "arn": "arn:aws:iam::111122223333:user/StorageGateway-
team/JohnDoe",
                                  "accountId:" 111122223333", " accessKeyId ":"
 AKIAIOSFODNN7EXAMPLE",
                                  " userName ":" JohnDoe "
                                  },
```

```
                                " eventTime ":" 2014 - 12 - 03T19: 41: 53Z ",
                                " eventSource ":" storagegateway.amazonaws.com ",
                                " eventName ":" ListGateways ",
                                " awsRegion ":" us-east-2 ",
                                " sourceIPAddress ":" 192.0.2.0 ",
                                " userAgent ":" aws - cli / 1.6.2 Python / 2.7.6
 Linux / 2.6.18 - 164.el5 ",
                                " requestParameters ":null,
                                " responseElements ":null,
                                "requestID ":"
 6U2N42CU37KAO8BG6V1I23FRSJ1Q8GLLE1QEU3KPGG6F0KSTAUU0 ",
                                " eventID ":" f76e5919 - 9362 - 48ff - a7c4 -
 d203a189ec8d ",
                                " eventType ":" AwsApiCall ",
                                " apiVersion ":" 20130630 ",
                                " recipientAccountId ":" 444455556666"
             }]
}
```

排查 Storage Gateway 部署问题

接下来，您可以找到与网关、主机平台、文件系统、高可用性、数据恢复和快照相关的最佳实践以及问题故障排除的信息。本地网关故障排除信息涵盖部署在支持的虚拟化平台上的网关。高可用性问题的故障排除信息涵盖在 VMware vSphere 高可用性 (HA) 平台上运行的网关。

主题

- 故障排除：网关离线问题：了解如何诊断可能导致网关在 Storage Gateway 控制台中显示为离线的问题。
- 故障排除：Active Directory 问题：了解在尝试将文件网关加入到 Microsoft Active Directory 域时，如果收到错误消息（例如 NETWORK_ERROR、TIMEOUT 或 ACCESS_DENIED）该怎么做。
- 故障排除：网关激活问题：了解在尝试激活 Storage Gateway 时收到内部错误消息的情况下该怎么做。
- 故障排除：本地网关问题-了解在使用本地网关时可能遇到的典型问题，以及如何允许 支持 连接到网关以帮助进行故障排除。
- 故障排除：Microsoft Hyper-V 设置问题：了解您在 Microsoft Hyper-V 平台上部署 Storage Gateway 时可能遇到的典型问题。
- 故障排除：Amazon EC2 网关问题：查找有关在使用部署到 Amazon EC2 上的网关时可能遇到的典型问题的信息。
- 故障排除：硬件设备问题-了解如何解决在使用 AWS Storage Gateway 硬件设备时可能遇到的问题。
- 故障排除：文件网关问题-查找可帮助您了解 File Gateway CloudWatch 日志中出现的错误和运行状况通知的原因的信息。
- 故障排除：高可用性问题-了解在 VMware HA 环境中部署的网关遇到问题时该怎么做。

故障排除：Storage Gateway 控制台中网关离线

使用以下故障排除信息，来确定当 AWS Storage Gateway 控制台显示网关处于离线状态时该怎么做。

网关可能由于以下一个或多个原因而显示为离线：

- 网关无法到达 Storage Gateway 服务端点。
- 网关意外关闭。

- 与网关关联的缓存磁盘已断开连接或经过修改，或者出现故障。

要使网关恢复在线，请确定并解决导致网关离线的问题。

检查关联的防火墙或代理

如果您将网关配置为使用代理，或者将网关置于防火墙后面，请查看代理或防火墙的访问规则。代理或防火墙必须可让流量进出 Storage Gateway 所需的网络端口和服务端点。有关更多信息，请参阅 Network and firewall requirements。

检查是否正在对网关的流量进行 SSL 检查或深度数据包检查

如果当前正在对网关与之间的网络流量执行 SSL 或深度数据包检查 AWS，则您的网关可能无法与所需的服务端点通信。要使网关恢复在线，必须禁用检查。

在重新启动或软件更新后检查 IOWait百分比指标

在重启或软件更新后，检查以了解文件网关的 `IOWaitPercent` 指标是否为 10 或更高。这可能会导致网关在将索引缓存重建到 RAM 时响应缓慢。有关更多信息，请参阅疑难解答：使用 CloudWatch 指标。

检查虚拟机监控程序主机上是否出现停电或硬件故障

网关的虚拟机监控程序主机出现停电或硬件故障，可能会导致网关意外关闭且无法访问。在恢复电源和网络连接后，网关将再次变为可访问。

网关恢复在线后，请务必采取措施来恢复数据。有关更多信息，请参阅 Best practices: recovering your data。

检查关联的缓存磁盘是否有问题

如果与网关关联的缓存磁盘中至少有一个被移除、更改或调整大小，或者它已损坏，则网关可能会进入离线状态。

如果从虚拟机监控程序主机上移除了正常工作的缓存磁盘：

1. 关闭网关。
2. 重新添加该磁盘。

> **Note**
>
> 确保将磁盘添加到同一个磁盘节点。

3. 重新启动网关。

如果缓存磁盘损坏、被更换或调整大小：

- 按照使用新实例替换现有 S3 文件网关中描述的方法 2 步骤来设置新网关并从 AWS 云重新下载缓存磁盘信息。

故障排除：将网关加入 Active Directory 时出现的问题

使用以下故障排除信息，确定在尝试将文件网关加入 Microsoft Active Directory 域时如果收到错误消息（例如 NETWORK_ERROR、TIMEOUT 或 ACCESS_DENIED）该怎么做。

要解决这些错误，请执行以下检查和配置。

通过运行 nping 测试来确认网关可以访问域控制器

要运行 nping 测试，请执行以下操作：

1. 使用虚拟机监控程序管理软件（VMware、Hyper-V 或 KVM）（用于本地网关）或使用 ssh（用于 Amazon EC2 网关），连接到网关本地控制台。
2. 输入相应的数字来选择网关控制台，然后输入 h 以列出所有可用命令。要测试 Storage Gateway 虚拟机与域之间的连接，请运行以下命令：

```
nping -d corp.domain.com -p 389 -c 1 -t tcp
```

> **Note**
>
> 将 corp.domain.com 替换为 Active Directory 域 DNS 名称，并将 389 替换为您的环境的 LDAP 端口。
> 确认已在防火墙内打开所需的端口。

以下示例说明 nping 测试成功，网关能够访问域控制器：

```
nping -d corp.domain.com -p 389 -c 1 -t tcp

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2022-06-30 16:24 UTC
SENT (0.0553s) TCP 10.10.10.21:9783 > 10.10.10.10:389 S ttl=64 id=730 iplen=40
 seq=2597195024 win=1480
RCVD (0.0556s) TCP 10.10.10.10:389 > 10.10.10.21:9783 SA ttl=128 id=22332 iplen=44
 seq=4170716243 win=8192 <mss 8961>

Max rtt: 0.310ms | Min rtt: 0.310ms | Avg rtt: 0.310ms
Raw packets sent: 1 (40B) | Rcvd: 1 (44B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 1.09 seconds<br>
```

以下 nping 测试示例表明没有与 corp.domain.com 目标建立连接，或者目标没有响应：

```
nping -d corp.domain.com -p 389 -c 1 -t tcp

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2022-06-30 16:26 UTC
SENT (0.0421s) TCP 10.10.10.21:47196 > 10.10.10.10:389  S ttl=64 id=30318 iplen=40
 seq=1762671338 win=1480

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 1 (40B) | Rcvd: 0 (0B) | Lost: 1 (100.00%)
Nping done: 1 IP address pinged in 1.07 seconds
```

检查 Amazon EC2 网关实例 VPC 的 DHCP 选项集

如果文件网关在 Amazon EC2 实例上运行，则必须确保已正确配置 DHCP 选项集，并连接到包含此网关实例的 Amazon Virtual Private Cloud（VPC）。有关更多信息，请参阅 Amazon VPC 中的 DHCP 选项集。

通过运行 dig 查询来确认网关可以解析域

如果网关无法解析域，则网关无法加入域。

要运行 dig 查询，请执行以下操作：

1. 使用虚拟机监控程序管理软件（VMware、Hyper-V 或 KVM）（用于本地网关）或使用 ssh（用于 Amazon EC2 网关），连接到网关本地控制台。
2. 输入相应的数字来选择网关控制台，然后输入 h 以列出所有可用命令。要测试网关能否解析域，请运行以下命令：

```
dig -d corp.domain.com
```

> **Note**
>
> 将 corp.domain.com 替换为您的 Active Directory 域 DNS 名称。

以下是成功响应的示例：

```
; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.amzn2.5.2 <<>> corp.domain.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24817
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;corp.domain.com.        IN    A

;; ANSWER SECTION:
corp.domain.com.    600    IN    A    10.10.10.10
corp.domain.com.    600    IN    A    10.10.20.10

;; Query time: 0 msec
;; SERVER: 10.10.20.228#53(10.10.20.228)
;; WHEN: Thu Jun 30 16:36:32 UTC 2022
;; MSG SIZE  rcvd: 78
```

检查域控制器设置和角色

确认域控制器未设置为只读，并且域控制器的角色具有必要的权限，可让计算机加入域。要对此进行测试，请尝试将网关 VM 所在的 VPC 子网中的其他服务器加入域。

检查网关是否已加入最近的域控制器

作为最佳实践，建议将网关加入在地理位置上靠近网关设备的域控制器。如果由于存在网络延迟，网关设备无法在 20 秒内与域控制器通信，则域加入过程会超时。例如，如果网关设备位于美国东部（弗吉尼亚北部），AWS 区域 而域控制器位于亚太地区（新加坡），则该过程可能会超时 AWS 区域。

> **Note**
>
> 要增加 20 秒的默认超时值，您可以在 AWS Command Line Interface (AWS CLI) 中运行 join-domain 命令并添加延长时间的`--timeout-in-seconds`选项。您也可以使用 JoinDomain API 调用并添加`TimeoutInSeconds`参数来延长时间。最大超时值为 3600 秒。
> 如果您在运行 AWS CLI 命令时收到错误，请确保您使用的是最新 AWS CLI 版本。

确认 Active Directory 在默认组织单元（OU）中创建了新的计算机对象

确保 Microsoft Active Directory 没有任何组策略对象会在默认 OU 以外的任何位置创建新的计算机对象。将网关加入 Active Directory 域之前，默认 OU 中必须有新的计算机对象。某些 Active Directory 环境经过自定义 OUs，新创建的对象会有所不同。为确保默认 OU 中有网关 VM 的新计算机对象，请在将网关加入域之前，尝试在域控制器上手动创建计算机对象。您也可以使用 AWS CLI运行 join-domain 命令。然后，指定 `--organizational-unit` 选项。

> **Note**
>
> 创建计算机对象的过程称为预配置。

查看域控制器事件日志

如果在尝试了前几节中描述的所有其他检查和配置后仍无法将网关加入域，建议检查域控制器事件日志。在域控制器的事件查看器中检查是否有任何错误。确认网关查询已到达域控制器。

故障排除：网关激活期间的内部错误

Storage Gateway 激活请求会经过两条网络路径。客户端发送的传入激活请求通过端口 80 连接到网关的虚拟机（VM）或 Amazon Elastic Compute Cloud（Amazon EC2）实例。如果网关成功收到激活请求，则网关将与 Storage Gateway 端点通信来接收激活密钥。如果网关无法到达 Storage Gateway 端点，则网关会以一则内部错误消息响应客户端。

使用以下故障排除信息，来确定在尝试激活 AWS Storage Gateway的过程中收到内部错误消息时该怎么做。

> **Note**
>
> - 确保使用最新的虚拟机映像文件或亚马逊机器映像（AMI）版本部署新的网关。如果您尝试激活使用过时 AMI 的网关，则会收到内部错误消息。
> - 在下载 AMI 之前，请务必选择要部署的正确网关类型。每种网关类型的.ova 文件都不同，并且不可互换。 AMIs

解决使用公有端点激活网关时出现的错误

要解决使用公有端点激活网关时的激活错误，请执行以下检查和配置。

检查所需的端口

对于本地部署的网关，请检查本地防火墙上的端口是否为打开状态。对于部署在 Amazon EC2 实例上的网关，请检查实例安全组上的端口是否为打开状态。要确认端口为打开状态，请从服务器上对公有端点运行 telnet 命令。此服务器必须与网关位于同一子网中。例如，以下 telnet 命令测试与端口 443 的连接：

```
telnet d4kdq0yaxexbo.cloudfront.net 443
telnet storagegateway.region.amazonaws.com 443
telnet dp-1.storagegateway.region.amazonaws.com 443
telnet proxy-app.storagegateway.region.amazonaws.com 443
telnet client-cp.storagegateway.region.amazonaws.com 443
telnet anon-cp.storagegateway.region.amazonaws.com 443
```

要确认网关本身是否可以到达端点，请访问网关的本地 VM 控制台（适用于本地部署的网关）。或者，可以通过 SSH 连接到网关的实例（适用于部署在 Amazon EC2 上的网关）。然后，运行网络连接测试。确认测试返回 [PASSED]。有关更多信息，请参阅 Testing your gateway's network connectivity。

> **Note**
>
> 网关控制台的默认登录用户名为 admin，默认密码为 password。

确保防火墙安全性不会修改从网关发送到公有端点的数据包

SSL 检查、深度数据包检查或其它形式的防火墙安全性可能会干扰从网关发送的数据包。如果 SSL 证书的修改结果与激活端点所预期的情况不同，则 SSL 握手失败。要确认没有正在进行的 SSL 检查，请在端口 443 上的主激活端点 (anon-cp.storagegateway.region.amazonaws.com) 上运行 OpenSSL 命令。必须从与网关位于同一子网中的计算机上运行此命令：

```
$ openssl s_client -connect  anon-cp.storagegateway.region.amazonaws.com:443 -
servername anon-cp.storagegateway.region.amazonaws.com
```

> **Note**
>
> *region*用你的 AWS 区域.

如果没有正在进行的 SSL 检查，则该命令将返回类似于以下内容的响应：

```
$ openssl s_client -connect anon-cp.storagegateway.us-east-2.amazonaws.com:443 -
servername anon-cp.storagegateway.us-east-2.amazonaws.com
CONNECTED(00000003)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-2.amazonaws.com
verify return:1
---
Certificate chain
 0 s:/CN=anon-cp.storagegateway.us-east-2.amazonaws.com
   i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
 1 s:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
   i:/C=US/O=Amazon/CN=Amazon Root CA 1
 2 s:/C=US/O=Amazon/CN=Amazon Root CA 1
   i:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
 3 s:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
   i:/C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority
---
```

如果正在进行 SSL 检查，则响应将显示更改的证书链，类似于以下内容：

```
$ openssl s_client -connect  anon-cp.storagegateway.ap-southeast-1.amazonaws.com:443 -
servername anon-cp.storagegateway.ap-southeast-1.amazonaws.com
CONNECTED(00000003)
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.ap-southeast-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

激活端点仅在识别 SSL 证书时才接受 SSL 握手。这意味着，网关到端点的出站流量必须免受网络中防火墙执行的检查。这些检查可能是 SSL 检查或深度数据包检查。

检查网关时间同步

时间偏差过大可能会导致 SSL 握手错误。对于本地网关，可以使用网关的本地 VM 控制台来检查网关的时间同步。时间偏差应不大于 60 秒。有关更多信息，请参阅 Synchronizing Your Gateway VM Time。

系统时间管理选项在托管于 Amazon EC2 实例上的网关中不可用。为确保 Amazon EC2 网关能够正确地同步时间，请确认 Amazon EC2 实例可以通过端口 UDP 和 TCP 123 连接到以下 NTP 服务器池列表：

- time.aws.com
- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org
- 2.amazon.pool.ntp.org
- 3.amazon.pool.ntp.org

解决使用 Amazon VPC 端点激活网关时出现的错误

要解决使用 Amazon Virtual Private Cloud（Amazon VPC）端点激活网关时出现的激活错误，请执行以下检查和配置。

检查所需的端口

确保本地防火墙（对于本地部署的网关）或安全组（对于部署在 Amazon EC2 中的网关）中的所需端口处于打开状态。将网关连接到 Storage Gateway VPC 端点所需的端口与将网关连接到公有端点时所需的端口不同。连接到 Storage Gateway VPC 端点需要以下端口：

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

有关更多信息，请参阅 Creating a VPC endpoint for Storage Gateway。

此外，请检查连接到 Storage Gateway VPC 端点的安全组。连接到端点的默认安全组可能不支持所需的端口。创建一个新的安全组，让来自网关 IP 地址范围的流量通过所需端口。然后，将该安全组连接到 VPC 端点。

> **Note**
>
> 使用 Amazon VPC 控制台来验证连接到 VPC 端点的安全组。从控制台查看 Storage Gateway VPC 端点，然后选择安全组选项卡。

要确认所需端口处于打开状态，可以在 Storage Gateway VPC 端点上运行 telnet 命令。必须从与网关位于同一子网中的服务器上运行这些命令。可以对第一个未指定可用区的 DNS 名称运行测试。例如，以下 telnet 命令使用 DNS 名称 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 测试所需的端口连接：

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 443
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1026
```

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1027
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1028
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1031
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 2222
```

确保防火墙安全性不会修改从网关发送到 Storage Gateway Amazon VPC 端点的数据包

SSL 检查、深度数据包检查或其它形式的防火墙安全性可能会干扰从网关发送的数据包。如果 SSL 证书的修改结果与激活端点所预期的情况不同，则 SSL 握手失败。要确认没有正在进行的 SSL 检查，请在 Storage Gateway VPC 端点上运行 OpenSSL 命令。必须从与网关位于同一子网中的计算机上运行此命令。针对每个必需的端口运行命令：

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:443 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1026 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1028 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1031 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:2222 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

如果没有正在进行的 SSL 检查，则该命令将返回类似于以下内容的响应：

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
```

```
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-1.amazonaws.com
verify return:1
---
Certificate chain
 0 s:CN = anon-cp.storagegateway.us-east-1.amazonaws.com
   i:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
 1 s:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
   i:C = US, O = Amazon, CN = Amazon Root CA 1
 2 s:C = US, O = Amazon, CN = Amazon Root CA 1
   i:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
 3 s:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
   i:C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification
 Authority
---
```

如果正在进行 SSL 检查，则响应将显示更改的证书链，类似于以下内容：

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.us-
east-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.us-east-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

激活端点仅在识别 SSL 证书时才接受 SSL 握手。这意味着，网关通过所需端口到 VPC 端点的出站流量免受由网络防火墙执行的检查。这些检查可能是 SSL 检查或深度数据包检查。

检查网关时间同步

时间偏差过大可能会导致 SSL 握手错误。对于本地网关，可以使用网关的本地 VM 控制台来检查网关的时间同步。时间偏差应不大于 60 秒。有关更多信息，请参阅 Synchronizing Your Gateway VM Time。

系统时间管理选项在托管于 Amazon EC2 实例上的网关中不可用。为确保 Amazon EC2 网关能够正确地同步时间，请确认 Amazon EC2 实例可以通过端口 UDP 和 TCP 123 连接到以下 NTP 服务器池列表：

- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org
- 2.amazon.pool.ntp.org
- 3.amazon.pool.ntp.org

检查 HTTP 代理并确认关联的安全组设置

在激活之前，请检查您是否在本地网关 VM 上将 Amazon EC2 上的 HTTP 代理配置为端口 3128 上的 Squid 代理。在此情况下，确认以下事项：

- 连接到 Amazon EC2 上 HTTP 代理的安全组必须具有入站规则。此入站规则必须在端口 3128 上支持来自网关 VM 的 IP 地址的 Squid 代理流量。
- 连接到 Amazon EC2 VPC 端点的安全组必须具有入站规则。这些入站规则必须在端口 1026-1028、1031、2222 和 443 上支持来自 Amazon EC2 上 HTTP 代理的 IP 地址的流量。

解决使用公有端点激活网关且同一 VPC 中有 Storage Gateway VPC 端点时出现的错误

要解决在同一 VPC 中有 Amazon Virtual Private Cloud（Amazon VPC）端点的情况下使用公有端点激活网关时出现的错误，请执行以下检查和配置。

确认 Storage Gateway VPC 端点上启用私有 DNS 名称设置未处于启用状态

如果启用私有 DNS 名称处于启用状态，则无法激活从该 VPC 到公有端点的任何网关。

要禁用 DNS 名称选项，请执行以下操作：

1. 打开 Amazon VPC 控制台。

2. 在导航窗格中，选择端点。
3. 选择 Storage Gateway VPC 端点。
4. 选择操作。
5. 选择管理私有 DNS 名称。
6. 对于启用私有 DNS 名称，清除为此端点启用。
7. 选择修改私有 DNS 名称来保存设置。

故障排除：本地网关问题

您可以在下面找到有关在使用本地网关时可能遇到的典型问题以及如何允许 支持 连接到网关以帮助进行故障排除的信息。

下表列出了您在使用场内网关时可能遇到的典型问题。

问题	要采取的操作
您找不到网关的 IP 地址。	请使用管理程序客户端连接主机，以便查找网关 IP 地址。 • 对于 VMware ESXi，虚拟机的 IP 地址可以在 vSphere 客户端的“摘要”选项卡上找到。 • 对于 Microsoft Hyper-V，可登录本地控制台查找 VM 的 IP 地址。 如果您仍然难以找到网关 IP 地址： • 检查 VM 是否已开启。仅在 VM 已开启的情况下，IP 地址才会分配给您的网关。 • 等待 VM 完成启动。如果您刚刚打开 VM，那么网关可能需要一些时间才能完成启动序列。
您遇到了网络或防火墙问题。	• 允许适用于网关的端口。 • 如果使用防火墙或路由器来筛选或限制网络流量，则必须配置防火墙和路由器以允许这些服务端点与 AWS进行出站通信。有关网络和防火墙要求的更多信息，请参阅网络和防火墙要求。
当您单击 Storage Gateway 管理控制台中的继续激活按	• 检查网关 VM 是否可通过从客户端 ping 通。

问题	要采取的操作
钮时，网关的激活过程会失败。	• 检查您的 VM 是否已与 Internet 建立网络连接。否则，您需要配置 SOCKS 代理。有关执行此操作的更多信息，请参阅 测试网关的网络连接。 • 检查主机的时间是否准确，主机是否已配置为与网络时间协议 (NTP) 服务器自动同步，以及网关 VM 的时间是否准确。有关同步虚拟机管理程序主机的时间和 VMs的信息，请参见。配置网关的网络时间协议（NTP）服务器 • 执行这些步骤后，您可以使用 Storage Gateway 控制台和设置并激活网关向导重新尝试网关部署。 • 检查您的虚拟机是否至少有 16 GB 的内存。如果内存少于 16 GB，则网关分配失败。有关更多信息，请参阅 文件网关设置要求。
您需要提高网关和 AWS之间的带宽。	您可以将互联网连接设置为 AWS 与连接应用程序和网关 VM 的网卡 (NIC) 分开的网络适配器 (NIC)，从而 AWS 改善从网关到的带宽。如果您有高带宽连接， AWS 并且想要避免带宽争用，尤其是在快照还原期间，则采用这种方法很有用。对于高吞吐量工作负载需求，您可以使用 Direct Connect 在本地网关和 AWS间建立专用网络连接。要测量从您的网关到的连接带宽 AWS，请使用网关的`CloudBytesDownloaded` 和`CloudBytesUploaded` 指标。有关本主题的更多信息，请参阅 性能和优化。提高 Internet 连接性能有助于确保您的上传缓冲区不被填满。

问题	要采取的操作

往返您网关的吞吐量将为零。	• 在 Storage Gateway 控制台的网关选项卡上，验证网关虚拟机的 IP 地址是否与使用虚拟机管理程序客户端软件（即 VMware vSphere 客户端或 Microsoft Hyper-V Manager）看到的 IP 地址相同。如果发现 IP 地址不一致，请从 Storage Gateway 控制台重启网关，如关闭网关虚拟机中所述。重启后，Storage Gateway 控制台的网关选项卡中 IP 地址列表中的地址应与您从管理程序客户端确定的网关 IP 地址相匹配。
	  • 对于 VMware ESXi，虚拟机的 IP 地址可以在 vSphere 客户端的 “摘要” 选项卡上找到。
	  • 对于 Microsoft Hyper-V，可登录本地控制台查找 VM 的 IP 地址。
	• 检查您的网关与的连接， AWS 如中所述测试网关的网络连接。
	• 在虚拟机监控程序管理客户端中检查网关的网络适配器配置，并确保要使用的所有网关接口均已激活。
	• 在网关本地控制台中检查网关的网络适配器配置。有关说明，请参阅配置网关网络设置。
	
	您可以从 Amazon CloudWatch 控制台查看进出网关的吞吐量。有关测量进出网关的吞吐量的更多信息 AWS，请参阅性能和优化。

在 Microsoft Hyper-V 中导入（部署）Storage Gateway 时遇到问题。	请参阅 故障排除：Microsoft Hyper-V 设置，其中对您在 Microsoft Hyper-V 上部署网关时遇到的部分常见问题进行了说明。
您收到一条消息，指出“已写入网关卷中的数据未安全存储在 AWS中”。	如果您的网关虚拟机是从另一个网关虚拟机的克隆或快照创建的，则您会收到此消息。如果不是这种情况，请联系 支持。

开启 支持 访问权限以帮助对本地托管的网关进行故障排除

Storage Gateway 提供了一个本地控制台，您可以使用它 支持 来执行多项维护任务，包括允许访问网关以帮助您解决网关问题。默认情况下，对您的网关的 支持 访问处于关闭状态。您可通过主机的

本地控制台启用此访问权限。要 支持 访问您的网关，请先登录主机的本地控制台，导航到 Storage Gateway 的控制台，然后连接到支持服务器。

开启对网关的 支持 访问权限

1. 登录到主机的本地控制台。

   - VMware ESXi — 有关更多信息，请参阅使用访问网关本地控制台 VMware ESXi。
   - Microsoft Hyper-V - 有关更多信息，请参阅使用 Microsoft Hyper-V 访问网关本地控制台。

2. 在提示符处输入相应的数字来选择网关控制台。
3. 输入 **h** 打开可用命令的列表。
4. 请执行以下操作之一：

   - 如果网关使用的是公有端点，请在可用命令窗口中，输入 **`open-support-channel`** 来连接到 Storage Gateway 的客户支持。允许 TCP 端口 22，以便您可以打开 AWS的支持通道。在连接到客户支持时，Storage Gateway 将为您分配支持编号。请记下您的支持编号。
   - 如果网关使用的是 VPC 端点，请在 AVAILABLE COMMANDS 窗口中，输入 **`open-support-channel`**。如果未激活网关，请提供要连接到 Storage Gateway 客户支持的 VPC 端点或 IP 地址。允许 TCP 端口 22，以便您可以打开 AWS的支持通道。在连接到客户支持时，Storage Gateway 将为您分配支持编号。请记下您的支持编号。

   > **Note**
   >
   > 信道号不是（传输控制Protocol/User Datagram Protocol (TCP/UDP）端口号。相反，网关会与 Storage Gateway 服务器建立 Secure Shell (SSH) (TCP 22) 连接，并提供用于连接的支持通道。

5. 建立支持渠道后，请向提供您的支持服务号码， 支持 支持 以便提供故障排除帮助。
6. 在支持会话完成后，输入 **q** 以将其结束。在 Amazon Web Services Support 通知您支持会话完成之前，请勿关闭该会话。
7. 输入 **`exit`** 来注销 Storage Gateway 控制台。
8. 按照提示操作退出本地控制台。

故障排除：Microsoft Hyper-V 设置

下表列出了您在 Microsoft Hyper-V 平台上部署 Storage Gateway 时可能遇到的典型问题。

问题	要采取的操作
您尝试导入网关并收到以下错误消息： “尝试导入虚拟机时发生服务器错误。导入失败。在位置 [...] 下找不到虚拟机导入文件。仅当使用 Hyper-V 创建和导出虚拟机时，才能导入虚拟机。”	出现此错误的原因如下： • 如果您没有指向解压缩网关源文件的根目录。您在导入虚拟机对话框中所指定位置的最后一部分应该是 AWS-Storage-Gateway 。例如： `C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\` . • 如果您已经部署了网关，但没有在导入虚拟机对话框中选择复制虚拟机选项和复制所有文件选项，则在解压缩的网关文件所在位置创建 VM，并且您无法再从这个位置导入。为了修复此问题，请获取最新的解压缩网关源文件副本，并将其复制到新的位置。将新的位置用作导入源目录。 如果您计划从一个已解压缩的源文件位置创建多个网关，则必须选择复制虚拟机，然后在导入虚拟机对话框中选中复制所有文件框。
您尝试导入网关并收到以下错误消息： “尝试导入虚拟机时发生服务器错误。导入失败。导入任务无法从 [...] 复制文件：文件存在。（0x80070050）”	如果您已经部署网关且试图重新使用存储了虚拟硬盘文件和虚拟机配置文件的默认文件夹，那么会出现此错误。要修复此问题，请在 Hyper-V 设置对话框左侧面板的服务器下方指定新位置。
您尝试导入网关并收到以下错误消息： “尝试导入虚拟机时发生服务器错误。导入失败。Import failed because the virtual machine must have a new identifier。Select a new identifier and try the import again.”	导入网关时，请确保在导入虚拟机对话框中选择复制虚拟机选项并选中复制所有文件框，来为 VM 创建新的唯一 ID。

问题	要采取的操作
您尝试启动网关 VM 并收到以下错误消息： “尝试启动选定的虚拟机时出错。子分区处理器设置与父分区不兼容。‘AWS-Storage-Gateway’无法初始化。（虚拟机 ID [...]）”	此错误可能是由于网关所需的 CPU 与主机 CPUs 上可用 CPUs 的 CPU 差异造成的。确保 VM 的 CPU 个数获得了底层管理程序的支持。 有关 Storage Gateway 要求的更多信息，请参阅文件网关设置要求。
您尝试启动网关 VM 并收到以下错误消息： “尝试启动选定的虚拟机时出错。‘AWS-Storage-Gateway’无法初始化。（虚拟机 ID [...]）无法创建分区：系统资源不足，无法完成所请求的服务。（0x800705AA）”	此错误很可能是该网关所需的 RAM 和主机上可用的 RAM 之间的差异导致的。 有关 Storage Gateway 要求的更多信息，请参阅文件网关设置要求。
您的快照和网关软件更新的出现时间会与预计的稍有不同。	网关 VM 的时钟可能会偏离实际的时间，这称为时钟漂移。使用本地网关控制台的时间同步选项，校验和纠正 VM 的时间。有关更多信息，请参阅 配置网关的网络时间协议（NTP）服务器。
您需要将解压缩的 Microsoft Hyper-V Storage Gateway 文件放入主机文件系统中。	按照访问典型 Microsoft Windows 服务器的方式访问主机。例如，如果虚拟机监控程序主机名为 `hyperv-server`，则可使用以下 UNC 路径 `\\hyperv-server\c$`，其中假定可解析名称 `hyperv-server`，或在本地 hosts 文件中定义了该名称。
在连接管理程序时，系统会提示您输入证书。	以本地管理员的身份使用 Sconfig.cmd 工具给管理程序主机添加用户证书。

问题	要采取的操作
如果对使用 Broadcom 网络适配器的 Hyper-V 主机开启虚拟机队列（VMQ），则可能会注意到网络性能不佳。	有关解决方法的信息，请参阅 Microsoft 文档：Poor network performance on virtual machines on a Windows Server 2012 Hyper-V host if VMQ is turned on。

故障排除：Amazon EC2 网关问题

在以下部分中，您可以找到在使用部署到 Amazon EC2 的网关时可能遇到的典型问题。若要详细了解本地网关和 Amazon EC2 中部署的网关之间的区别，请参阅 为 FSx 文件网关部署默认 Amazon EC2 主机。

主题

- 过了一会儿您的网关并未激活
- 您在实例列表中找不到 EC2 网关实例
- 您需要使用 Amazon EC2 Serial Console 连接到您的网关实例
- 你 支持 想帮忙排查你的 Amazon EC2 网关的问题

过了一会儿您的网关并未激活

在 Amazon EC2 控制台中检查以下项：

- 已在与实例关联的安全组中启用端口 80。有关添加安全组规则的更多信息，请参阅《Amazon EC2 用户指南》中的添加安全组规则。
- 网关实例会标记为“running”。在 Amazon EC2 控制台中，实例的状态应该是“正在运行”。
- 确保您的 Amazon EC2 实例类型满足最低要求，如存储需求中所述。

纠正该问题后，请尝试重新激活网关。为此，请打开 Storage Gateway 控制台，选择在 Amazon EC2 上部署新网关，然后重新输入实例的 IP 地址。

您在实例列表中找不到 EC2 网关实例

如果您没有为您的实例赋予资源标签，并且有很多实例在运行，则很难分辨哪个实例是您启动的。在这种情况下，可执行以下操作来查找网关实例：

- 检查实例说明选项卡上的 Amazon 系统映像 (AMI) 名称。基于 Storage Gateway AMI 的实例应以 **`aws-storage-gateway-ami`** 文本开头。
- 如果您有几个实例基于 Storage Gateway AMI，请查看实例启动时间来找到正确的实例。

您需要使用 Amazon EC2 Serial Console 连接到您的网关实例

您可以使用 Amazon EC2 Serial Console 来排查引导、网络配置和其他问题。有关说明和故障排除提示，请参阅《Amazon Elastic Compute Cloud 用户指南》中的 Amazon EC2 Serial Console。

你 支持 想帮忙排查你的 Amazon EC2 网关的问题

Storage Gateway 提供了一个本地控制台，您可以使用它 支持 来执行多项维护任务，包括允许访问网关以帮助您解决网关问题。默认情况下，对您的网关的 支持 访问处于关闭状态。通过 Amazon EC2 本地控制台启用此访问。通过 Secure Shell (SSH) 登录到 Amazon EC2 本地控制台。要通过 SSH 成功登录，您的实例的安全组必须具有开放 TCP 端口 22 的规则。

> **Note**
>
> 如果将新规则添加到现有安全组，则新规则适用于使用该安全组的所有实例。有关安全组以及如何添加安全组规则的更多信息，请参阅《Amazon EC2 用户指南》中的 Amazon EC2 安全组。

要 支持 连接您的网关，您需要先登录 Amazon EC2 实例的本地控制台，导航到存储网关的控制台，然后提供访问权限。

为部署在 Amazon EC2 实例上的网关开启 支持 访问权限

1. 登录到 Amazon EC2 实例的本地控制台。有关说明，请转到《Amazon EC2 用户指南》中的连接到您的实例。

   您可使用以下命令登录到 EC2 实例的本地控制台。

```
ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
```

> **Note**
>
> *PRIVATE-KEY*是包含您用于启动 Amazon EC2 实例的 EC2 密钥对的私有证书的.pem文件。有关更多信息，请参阅《Amazon EC2 用户指南》中的检索密钥对的公有密钥。*INSTANCE-PUBLIC-DNS-NAME*是运行网关的 Amazon EC2 实例的公有域名系统 (DNS) 名称。可通过在 EC2 控制台中选择 Amazon EC2 实例并单击说明选项卡来获取此公有 DNS 名称。

2. 在提示符处，输入 **6 - Command Prompt** 来打开 支持 通道控制台。
3. 输入 **h** 以打开 AVAILABLE COMMANDS 窗口。
4. 请执行以下操作之一：

   - 如果网关使用的是公有端点，请在可用命令窗口中，输入 **open-support-channel** 来连接到 Storage Gateway 的客户支持。允许 TCP 端口 22，以便您可以打开 AWS的支持通道。在连接到客户支持时，Storage Gateway 将为您分配支持编号。请记下您的支持编号。
   - 如果网关使用的是 VPC 端点，请在 AVAILABLE COMMANDS 窗口中，输入 **open-support-channel**。如果未激活网关，请提供要连接到 Storage Gateway 客户支持的 VPC 端点或 IP 地址。允许 TCP 端口 22，以便您可以打开 AWS的支持通道。在连接到客户支持时，Storage Gateway 将为您分配支持编号。请记下您的支持编号。

   > **Note**
   >
   > 信道号不是（传输控制Protocol/User Datagram Protocol (TCP/UDP）端口号。相反，网关会与 Storage Gateway 服务器建立 Secure Shell (SSH) (TCP 22) 连接，并提供用于连接的支持通道。

5. 建立支持渠道后，请向提供您的支持服务号码， 支持 支持 以便提供故障排除帮助。
6. 在支持会话完成后，输入 **q** 以将其结束。在 Amazon Web Services Support 通知您支持会话完成之前，请勿关闭该会话。
7. 输入 **exit** 来退出 Storage Gateway 控制台。
8. 通过控制台菜单操作来注销 Storage Gateway 实例。

故障排除：硬件设备问题

> **Note**
>
> 终止上市通知：自 2025 年 5 月 12 日起，将不再提供 AWS Storage Gateway 硬件设备。使用 AWS Storage Gateway 硬件设备的现有客户可以继续使用并获得支持，直到 2028 年 5 月。作为替代方案，您可以使用该 AWS Storage Gateway 服务为本地和云端应用程序提供对几乎无限的云存储的访问权限。

以下主题讨论了您在使用 AWS Storage Gateway 硬件设备时可能遇到的问题，以及解决这些问题的建议。

主题

- 您无法确定服务 IP 地址
- 如何执行出厂重置？
- 如何执行远程重启？
- 您在何处获得 Dell iDRAC 支持？
- 您找不到硬件设备序列号
- 在何处获得硬件设备支持

您无法确定服务 IP 地址

当尝试连接到您的服务时，请确保您使用的是该服务的 IP 地址，而不是主机的 IP 地址。在服务控制台中配置服务 IP 地址，并在硬件控制台中配置主机 IP 地址。您将在启动硬件设备时看到硬件控制台。要从硬件控制台转到服务控制台，请选择 Open Service Console (打开服务控制台)。

如何执行出厂重置？

如果您需要对设备执行出厂重置，请按以下支持部分所述联系 AWS Storage Gateway硬件设备团队寻求支持。

如何执行远程重启？

如果您需要远程重启设备，可以使用 Dell iDRAC 管理界面执行此操作。有关更多信息，请参阅 Dell Technologies InfoHub 网站上的 i DRAC9 虚拟电源循环：远程重启 Dell EMC PowerEdge 服务器。

您在何处获得 Dell iDRAC 支持？

戴尔 PowerEdge 服务器配有戴尔iDRAC管理接口。我们建议执行下列操作：

- 如果您使用 iDRAC 管理界面，则应更改默认密码。有关iDRAC凭证的更多信息，请参阅 PowerEdge 戴尔——iDRAC的默认登录凭据是什么？ 。
- 确保固件是 up-to-date为了防止安全漏洞。
- 将 iDRAC 网络接口移动到正常的 (em) 端口可能会导致性能问题或阻止设备正常运行。

您找不到硬件设备序列号

你可以使用 Storage Gateway 控制台找到 AWS Storage Gateway 硬件设备的序列号。

查找硬件设备序列号：

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 从页面左侧的导航菜单中选择硬件。
3. 从列表中选择硬件设备。
4. 在设备的详细信息选项卡上找到序列号字段。

在何处获得硬件设备支持

AWS 要联系您的硬件设备的技术支持，请参阅支持。

该 支持 团队可能会要求您激活支持渠道，以远程解决您的网关问题。您无需打开此端口即可实现网关的正常操作，但在进行问题排查时需要打开。您可以从硬件控制台激活支持通道，如下面的过程所示。

要打开支持频道 AWS

1. 打开硬件控制台。
2. 选择硬件控制台主页底部的打开支持渠道，然后按 `Enter`。

   如果没有网络连接或防火墙问题，分配的端口号应该在 30 秒内出现。例如：

   状态：在端口 19599 上打开
3. 记下端口号并将其提供给 支持。

故障排除：文件网关问题

您可以将文件网关配置为将日志条目写入 Amazon CloudWatch 日志组。配置好之后，您会收到有关网关的运行状况以及有关网关遇到的任何错误的通知。您可以在 CloudWatch 日志中找到有关这些错误和运行状况通知的信息。

在以下部分中，您可以找到相关信息来帮助您理解每个错误的原因、运行状况通知以及如何解决问题。

主题

- 错误： FileMissing
- 错误： FsxFileSystemAuthenticationFailure
- 错误： FsxFileSystemConnectionFailure
- 错误： FsxFileSystemFull
- 错误： GatewayClockOutOfSync
- 错误： InvalidFileState
- 错误： ObjectMissing
- 错误： DroppedNotifications
- 通知： HardReboot
- 通知：重启
- 故障排除：Active Directory 域问题
- 疑难解答：使用 CloudWatch 指标

错误： FileMissing

`FileMissing` 错误与 `ObjectMissing` 错误类似，解决错误的步骤也相同。当指定文件网关以外的写入器从 Amazon 中删除指定文件时，可能会`FileMissing`出现错误 FSx。任何后续上传到亚马逊 FSx 或从亚马逊检索该对象都将失 FSx 败。

要解决 FileMissing 错误

1. 将文件的最新副本保存到 SMB 客户端的本地文件系统中（需要在步骤 3 中复制此文件）。
2. 使用 SMB 客户端从文件网关删除文件。
3. FSx 使用您的 SMB 客户端复制您在步骤 1 Amazon 中保存的文件的最新版本。通过文件网关执行此操作。

错误： FsxFileSystemAuthenticationFailure

当挂载文件系统时提供的凭证过期或其权限已撤销时，会出现 `FsxFileSystemAuthenticationFailure` 错误。

要解决 FsxFileSystemAuthenticationFailure 错误

1. 确保在连接 Amazon FSx 文件系统时提供的凭证仍然有效。
2. 确保用户拥有附加 Amazon FSx for Windows 文件服务器文件系统中所述的所有必要权限。

错误： FsxFileSystemConnectionFailure

当无法从网关计算机访问 Amazon FSx 服务器时，您可能会`FsxFileSystemConnectionFailure`遇到错误。

要解决 FsxFileSystemConnectionFailure 错误

1. 确保所有防火墙和 VPC 规则都允许在网关计算机和 Amazon FSx 服务器之间建立连接。
2. 确保 Amazon FSx 服务器正在运行。

错误： FsxFileSystemFull

当 Amazon FSx 文件系统中没有足够的可用磁盘空间时，可能会`FsxFileSystemFull`出现错误。

要解决 FsxFileSystemFull 错误

- 增加 Amazon FSx 文件系统的存储空间。

错误： GatewayClockOutOfSync

当网关检测到本地系统时间与 AWS Storage Gateway 服务器报告的时间之间有 5 分钟或更长时间的差异时，您可能会收到`GatewayClockOutOfSync`错误消息。时钟同步问题可能会对网关和之间的连接产生负面影响 AWS。如果网关时钟不同步，NFS 和 SMB 连接可能会出现 I/O 错误，并且 SMB 用户可能会遇到身份验证错误。

要解决 GatewayClockOutOfSync 错误

- 检查网关和 NTP 服务器之间的网络配置。有关同步网关 VM 时间和更新 NTP 服务器配置的更多信息，请参阅为网关配置网络时间协议（NTP）服务器。

错误： InvalidFileState

当指定网关以外的写入器修改指定的文件共享中的指定文件时，会出现 `InvalidFileState` 错误。因此，网关上文件的状态与其在 Amazon 中的状态不匹配 FSx。随后从 Ama FSx zon 上传或检索文件都可能失败。

要解决 InvalidFileState 错误

1. 将文件的最新副本保存到 SMB 客户端的本地文件系统中（需要在步骤 4 中复制此文件）。如果 Amazon 中的文件版本 FSx 是最新版本，请下载该版本。为此，您可以使用任何 SMB 客户端直接访问 Amazon FSx 共享。
2. FSx 直接在 Amazon 中删除该文件。
3. 使用 SMB 客户端从网关删除文件。
4. 使用您的 SMB 客户端，通过文件网关将您在步骤 1 中保存的文件的最新版本复制到 Amazon FSx。

错误： ObjectMissing

当指定文件网关以外的写入器从 Amazon 中删除指定文件时，可能会`ObjectMissing`出现错误 FSx。任何后续上传到亚马逊 FSx或从亚马逊检索该对象都将失 FSx 败。

要解决 ObjectMissing 错误

1. 将文件的最新副本保存到 SMB 客户端的本地文件系统中（需要在步骤 3 中复制此文件）。
2. 使用 SMB 客户端从文件网关删除文件。
3. FSx 使用您的 SMB 客户端复制您在步骤 1 Amazon 中保存的文件的最新版本。通过文件网关执行此操作。

错误： DroppedNotifications

如果网关根磁盘上的可用存储空间小于 1 GB，或者在 1 分钟间隔内生成的运行状况通知超过 100 个，则可能会看到`DroppedNotifications`错误而不是其他预期类型的 CloudWatch 日志条目。在这种情况下，作为预防措施，网关会停止生成详细的 CloudWatch 日志通知。

要解决 DroppedNotifications 错误

1. 在 Storage Gateway 控制台的监控选项卡上查看您的网关的 `Root Disk Usage` 指标，以便确定可用的根磁盘空间是否不足。
2. 如果可用空间小于 1 GB，请增加网关根存储磁盘的大小。有关说明，请参阅您的虚拟机监控程序的文档。

   要增加 Amazon EC2 网关的根磁盘大小，请参阅《Amazon Elastic Compute Cloud 用户指南》中的请求对您的 EBS 卷进行修改。

   > **Note**
   >
   > 无法增加 AWS Storage Gateway 硬件设备的根磁盘大小。

3. 重新启动您的网关。

通知： HardReboot

当网关 VM 意外重启时，您会收到 `HardReboot` 通知。此类重启可能是因断电、硬件故障或其他事件导致的。对于 VMware 网关，vSphere 高可用性应用程序监控的重置可能会导致此事件。

当您的网关在这样的环境中运行时，请检查`HealthCheckFailure`通知是否存在，并查阅虚拟机 VMware 的事件日志。

通知：重启

在重新启动网关 VM 时，您会收到重启通知。您可以使用 VM 管理程序管理控制台或 Storage Gateway 控制台重新启动网关 VM。您也可以在网关维护周期内使用网关软件来重新启动。

如果重启时间在网关的已配置维护开始时间的 10 分钟内，则此重启可能是正常的，并不指示任何问题。如果重启发生在维护时段之外，请检查是否已手动重新启动网关。

故障排除：Active Directory 域问题

FSx 文件网关不会为 Active Directory 域问题生成特定的日志消息。如果在将网关加入 Active Directory 域时遇到问题，请执行以下操作：

- 确认网关没有尝试使用只读域控制器（RODC）来加入域。
- 确认网关配置为使用正确的 DNS 服务器。

  例如，如果您正在尝试将 Amazon EC2 网关实例加入 AWS托管的 Active Directory，请验证为您的 EC2 VPC 设置的 DHCP 选项是否指定了 AWS托管的 Active Directory DNS 服务器。

  您通过 VPC DHCP 选项集配置的 DNS 服务器将提供给 VPC 中的所有 EC2 实例。如果要为单个网关指定 DNS 服务器，则可以使用该网关的 EC2 本地控制台来指定。

  对于本地网关，使用虚拟机本地控制台来指定 DNS 服务器。
- 通过在网关本地控制台的命令提示符下运行以下命令来验证网关网络连接。将突出显示的变量替换为您的部署中的实际域名和 IP 地址。

```
dig -d ExampleDomainName
ncport -d ExampleDomainControllerIPAddress -p 445
ncport -d ExampleDomainControllerIPAddress -p 389
```

- 确认您的 Active Directory 服务账户具有必要的权限。有关更多信息，请参阅 Active Directory 服务账户权限要求。
- 确认网关加入了正确的组织单元（OU）。

  加入域会在默认计算机容器（不是 OU）中创建一个 Active Directory 计算机账户，并使用网关的网关 ID 作为账户名（例如，SGW-1234ADE）。此账户的名称无法自定义。

  如果您的 Active Directory 环境为新的计算机对象指定了 OU，则在加入域时必须指定该 OU。

  如果您在尝试加入指定的 OU 时遇到访问被拒绝错误，请咨询您的 Active Directory 域管理员。管理员可能需要预先设置网关的计算机账户，然后才能加入域。有关更多信息，请参阅如何排查将 Storage Gateway 文件网关加入到用于 Microsoft Active Directory 身份验证的域时遇到的问题？。
- 从网关本地控制台的命令提示符下运行以下命令，确认可以在 DNS 中解析网关的主机名。将突出显示的变量替换为您的网关的实际主机名。

```
dig -d ExampleHostName -r A
```

如果您为网关配置了自定义主机名，则必须手动添加指向其 IP 地址的 DNS A 记录。

- 确认网关和域控制器之间的网络延迟处于合理较低的水平。如果网关在 20 秒内没有收到来自域控制器的响应，则加入域的查询会超时。

  如果您使用 JoinDomainCLI 命令将网关加入域，则可以添加该`--timeout-in-seconds`标志将超时时间延长到最长 3,600 秒。

- 确认您用于将网关加入域的 Active Directory 用户具有加入域所需的权限。

疑难解答：使用 CloudWatch 指标

您可以在下面找到有关使用亚马逊 CloudWatch指标和 Storage Gateway 来解决问题的操作的信息。

主题

- 浏览目录时，您的网关反应缓慢
- 您的网关未响应
- 您在 Amazon 文件系统中看不到 FSx 文件
- 您在 Amazon FSx 文件系统中看不到较旧的快照
- 您的网关向 Amazon 传输数据速度很慢 FSx
- 您的网关备份作业失败，或在对网关进行写入时出现错误

浏览目录时，您的网关反应缓慢

如果您的 File Gateway 在运行ls命令或浏览目录时反应缓慢，请检查`IndexFetch`和`IndexEviction` CloudWatch 指标：

- 如果您在运行`ls`命令或浏览目录时该`IndexFetch`指标大于 0，则您的文件网关启动时没有有关受影响目录内容的信息，因此必须访问FSx 适用于 Windows 文件服务器的 。后续列出该目录内容的工作应更快地进行。
- 如果 `IndexEviction` 指标大于 0，则表示文件网关已达到当时可在其缓存中管理的内容的最大值。在此情况下，文件网关必须从最近访问最少的目录中释放一些存储空间以便列出新目录。如果这种情况经常发生并且会影响性能，请与联系 支持。

  与相 支持 关 Amazon FSx 文件系统的内容进行讨论，并根据您的用例提出提高性能的建议。

您的网关未响应

如果您的文件网关未响应，请执行以下操作：

- 如果存在最近重启或软件更新，请检查 IOWaitPercent 指标。此指标显示磁盘 I/O 请求未完成时 CPU 处于空闲状态的时间百分比。在某些情况下，此值可能会很高（10 或更高），并且可能会在服务器重启或更新后增大。在这些情况下，文件网关在将索引缓存重新构建到 RAM 时，可能会因根磁盘速度过慢而出现性能瓶颈。您可以通过为根磁盘使用更快的物理磁盘来解决此问题。
- 如果 MemUsedBytes 指标与 MemTotalBytes 指标相同或几乎相同，则文件网关将耗尽可用 RAM。确保您的文件网关至少具有所需的最小 RAM。如果您的文件网关已达到此要求，则可考虑根据工作负载和使用案例向网关添加更多 RAM。

  如果文件共享是 SMB，则问题可能也是因连接到文件共享的 SMB 客户端的数量导致的。要查看在任何给定时间连接的客户端数量，请检查 SMBV(1/2/3)Sessions 指标。如果连接了多个客户端，您可能需要向文件网关添加更多 RAM。

您在 Amazon 文件系统中看不到 FSx 文件

如果您发现网关上的文件未反映在 Amazon FSx 文件系统中，请检查该FilesFailingUpload指标。如果该指标报告某些文件上传失败，请查看运行状况通知。文件上传失败时，网关会生成运行状况通知，其中包含有关该问题的更多详细信息。

您在 Amazon FSx 文件系统中看不到较旧的快照

文件网关上的某些 FSx 文件操作（例如顶级文件夹重命名或权限更改）可能会导致多个文件操作，从而导致您 FSx 的 Windows 文件服务器文件系统 I/O 负载过高。如果您的文件系统没有足够的性能资源来处理您的工作负载，则文件系统可能会删除卷影副本，因为它优先考虑持续的可用性 I/O 而不是历史卷影副本的保留。

在 Amazon FSx 控制台中，查看监控和性能页面，查看您的文件系统是否配置不足。如果是，您可以切换到 SSD 存储、增加吞吐能力或增加 SSD IOPS 来处理您的工作负载。

您的网关向 Amazon 传输数据速度很慢 FSx

如果您的文件网关向 Amazon FSx for Windows 文件服务器传输数据速度很慢，请执行以下操作：

- 如果CachePercentDirty指标等于 80 或更高，则您的文件网关向磁盘写入数据的速度快于将数据上传到 Amazon for Windows 文件服务器 FSx 的速度。可以考虑增加从文件网关上传的带宽、添

加一个或多个缓存磁盘、减慢客户端写入速度，或者增加关联的 Amazon for Windows 文件服务器 FSx 的吞吐容量。

- 如果 CachePercentDirty 指标较低，请检查 IoWaitPercent 指标。如果 IoWaitPercent 大于 10，您的文件网关可能会受到本地缓存磁盘速度的限制。我们建议使用本地固态硬盘 (SSD) 磁盘作为缓存，最好是 NVM Express (NVMe)。如果此类磁盘不可用，请尝试使用来自单独物理磁盘的多个缓存磁盘来提高性能。

您的网关备份作业失败，或在对网关进行写入时出现错误

如果文件网关备份作业失败，或在对文件网关进行写入时出现错误，请执行以下操作：

- 如果 CachePercentDirty 指标为 90% 或更高，则因为缓存磁盘上的可用空间不足，文件网关无法接受对磁盘的新写入操作。要查看您的文件网关上传到 for Windows 文件服务器FSx 的速度有多快，请查看该CloudBytesUploaded指标。将该指标与 WriteBytes 指标进行比较，这将显示客户端将文件写入文件网关的速度。如果 SMB 客户端写入您的文件网关的速度超过了上传 FSx for Windows 文件服务器的速度，请添加更多的缓存磁盘以至少满足备份任务的大小。或者，增加上传带宽。
- 如果大文件复制（例如，备份作业）失败，但 CachePercentDirty 指标低于 80%，则您的文件网关可能会达到客户端会话超时。对于 SMB，您可以使用 PowerShell 命令Set-SmbClientConfiguration -SessionTimeout 300延长此超时时间。运行此命令会将超时设置为 300 秒。

高可用性运行状况通知

在 VMware vSphere 高可用性 (HA) 平台上运行网关时，您可能会收到运行状况通知。有关运行状况通知的更多信息，请参阅故障排除：高可用性问题。

故障排除：高可用性问题

如果您遇到可用性问题，则可在下面查找有关要采取的操作的信息。

主题

- 运行状况通知
- 指标

运行状况通知

当您在 VMware vSphere HA 上运行网关时，所有网关都会向您配置的 Amazon CloudWatch 日志组生成以下运行状况通知。这些通知将转至名为 `AvailabilityMonitor` 的日志流中。

主题

- 通知：重启
- 通知： HardReboot
- 通知： HealthCheckFailure
- 通知： AvailabilityMonitorTest

通知：重启

在重新启动网关 VM 时，您会收到重启通知。您可以使用 VM 管理程序管理控制台或 Storage Gateway 控制台重新启动网关 VM。您也可以在网关维护周期内使用网关软件来重新启动。

措施

如果重启时间在网关的已配置维护开始时间的 10 分钟内，则此情况可能是正常的，并不指示任何问题。如果重启发生在维护时段之外，请检查是否已手动重新启动网关。

通知： HardReboot

当网关 VM 意外重启时，您会收到 `HardReboot` 通知。此类重启可能是因断电、硬件故障或其他事件导致的。对于 VMware 网关，vSphere 高可用性应用程序监控的重置可能会导致此事件。

措施

当您的网关在这样的环境中运行时，请检查`HealthCheckFailure`通知是否存在，并查阅虚拟机 VMware 的事件日志。

通知： HealthCheckFailure

对于 VMware vSphere HA 上的网关，当运行状况检查失败并请求重启虚拟机时，您可以收到`HealthCheckFailure`通知。此事件也会在测试期间发生来监控可用性（由 `AvailabilityMonitorTest` 通知指示）。在此情况下，应会有 `HealthCheckFailure` 通知。

> **Note**
>
> 此通知仅适用于 VMware 网关。

措施

如果此事件重复发生，但没有 `AvailabilityMonitorTest` 通知，请检查您的 VM 基础设施是否存在问题（存储、内存等）。如果您需要其他帮助，请联系 支持。

通知： AvailabilityMonitorTest

对于 VMware vSphere HA 上的网关，当您在中运行可用性和应用程序监控系统测试时，您会`AvailabilityMonitorTest`收到通知。 VMware

指标

`AvailabilityNotifications` 指标适用于所有网关。此指标是网关生成的与可用性相关的运行状况通知数。使用 `Sum` 统计数据可观察网关是否遇到了任何与可用性相关的事件。有关事件的详细信息，请咨询您配置的 CloudWatch 日志组。

文件网关的最佳实践

本节包含以下主题，这些主题提供有关使用网关、文件共享、存储桶和数据的最佳实践的信息。我们建议您自行熟悉本节中概述的信息，并尝试遵循这些指南，以避免 AWS Storage Gateway出现问题。有关诊断和解决您在部署中可能遇到的常见问题的更多指导，请参阅排查 Storage Gateway 部署问题。

主题

- 最佳实践：恢复数据
- 直接在 Amazon 上从备份或快照中恢复 FSx
- 清理不必要的资源

最佳实践：恢复数据

虽然很少发生，但您的网关仍可能会遇到不可恢复的故障。这种故障可能在您的虚拟机 (VM)、网关本身、本地存储或其他位置发生。如果出现故障，我们建议您按照以下相应部分中的说明恢复您的数据。

> **Important**
>
> Storage Gateway 不支持从虚拟机管理程序创建的快照或从 Amazon EC2 Amazon 系统映像 (AMI) 恢复网关 VM。如果您的网关 VM 出现故障，则激活新网关，然后根据以下说明将您的数据恢复到该网关。

从虚拟机意外关闭中恢复

如果您的 VM 意外关闭，例如在停电期间，您的网关会变得不可访问。当电力和网络连接恢复后，您的网关会变得能够访问并开始正常运行。下面是此时您能够采取的有助于恢复数据的一些步骤：

- 如果断电导致网络连接问题，您可以进行对此问题进行排查。有关如何测试网络连接的信息，请参阅测试网关的网络连接。

从出现故障的缓存磁盘恢复您的数据

如果缓存磁盘出现故障，我们建议您根据具体情况采用以下步骤恢复数据：

- 如果故障是因将缓存磁盘从您的主机中移除导致的，则关闭网关，重新添加该磁盘，然后重新启动网关。

从不可访问的数据中心恢复您的数据

如果您的网关或数据中心出于某种原因变得无法访问，您可将数据恢复到位于不同数据中心的另一个网关或在 Amazon EC2 实例上托管的网关。如果您无权访问另一个数据中心，则建议在 Amazon EC2 实例上创建网关。您要执行的步骤取决于您要从中恢复数据的网关类型。

从无法访问的数据中心内的文件网关恢复数据

对于 File Gateway，您可以将新的文件系统映射到包含要恢复的数据的 Windows 文件服务器的 FSx 。

1. 在 Amazon EC2 主机上创建并激活新的文件网关。有关更多信息，请参阅 为 FSx 文件网关部署默认 Amazon EC2 主机。
2. 在创建的 EC2 网关上创建一个新的文件系统。有关更多信息，请参阅创建 FSx 适用于 Windows 文件服务器的文件系统。
3. 在客户端上安装您的文件系统，并将其映射到包含要恢复的数据的 Windows 文件服务器的 FSx 。有关更多信息，请参阅挂载并使用文件共享。

直接在 Amazon 上从备份或快照中恢复 FSx

在某些情况下，您可能需要使用较早时间点的备份或快照直接恢复 Amazon FSx 文件系统上的数据。在这些情况下，可能会在备份应用程序和 File Gateway 之间创建双写入器场景，这可能会导致 FSx 文件卡住或不匹配。为避免从备份或快照恢复 Amazon FSx 文件系统时出现问题，请使用以下步骤。

> **Note**
>
> 使用此过程从备份或快照中恢复 Amazon FSx 文件系统后，当前存储在 FSx 文件网关上的任何缓存数据都将失效。

为了避免在从备份或快照恢复 Amazon FSx 文件系统时出现问题

1. 使用 Storage Gateway 控制台将 Amazon FSx FSx 文件系统与文件网关分离。
2. 直接在您的 Amazon FSx 文件系统上恢复备份或快照。

3. 使用 Storage Gateway 控制台将 Amazon FSx FSx 文件系统重新连接到文件网关。

清理不必要的资源

作为最佳实践，建议清理 Storage Gateway 资源，以避免产生意外或不必要的费用。例如，如果您创建网关是为了演示练习或测试，请考虑将其及其虚拟设备从部署中删除。请执行以下步骤来清理资源。

清除不需要的资源

1. 如果您不再打算继续使用网关，请将其删除。有关更多信息，请参阅 删除网关和移除关联的资源。
2. 从本地主机中删除 Storage Gateway VM。如果您在 Amazon EC2 实例上创建了网关，请终止该实例。

其他 Storage Gateway 资源

本节包含以下主题，这些主题提供与设置和使用 AWS Storage Gateway相关的额外信息和资源：

主题

- 主机设置：了解如何为网关部署和配置虚拟机主机。
- 使用 Storage Gateway 和 VMware HA-了解如何设置 Storage Gateway 以使用 VMware vSphere 高可用性功能。
- 获取激活密钥：了解部署新网关时可以在哪里找到您需要提供的激活密钥。
- 使用 Direct Connect：了解如何在本地网关与 AWS 云之间创建专用网络连接。
- Active Directory 权限：了解您的服务账户必须具备哪些权限才能让您的网关加入 Active Directory 域。
- 获取网关设备的 IP 地址：了解在哪里可以找到网关的虚拟机主机 IP 地址，部署新网关时需要提供该地址。
- 了解资源和资源 IDs-了解如何 AWS 识别 Storage Gateway 创建的资源和子资源。
- 标记您的资源：了解如何使用元数据标签来对资源进行分类并使其更易于管理。
- 开源组件：了解用于提供 Storage Gateway 功能的第三方工具和许可证。
- 配额：了解文件网关的限制和配额，包括文件共享和本地缓存磁盘的最小和最大限制。

部署和配置网关 VM 主机

以下主题介绍为网关设置虚拟机主机平台。

主题

- 为 FSx 文件网关部署默认 Amazon EC2 主机
- 为 FSx 文件网关部署自定义的 Amazon EC2 主机
- 修改 Amazon EC2 实例元数据选项
- 将 VM 时间与 Hyper-V 或 Linux KVM 主机时间同步
- 将 VM 时间与 VMware 主机时间同步
- 为网关配置网络适配器
- 将 VMware vSphere 高可用性与 Storage Gateway 配合使用

为 FSx 文件网关部署默认 Amazon EC2 主机

本主题列出了使用默认规格部署 Amazon EC2 主机的步骤。

您可以在亚马逊弹性计算云 (A EC2) 实例上部署和激活 Amazon S3 FSx 文件网关亚马逊文件网关。AWS Storage Gateway Amazon 系统映像 (AMI) 以社区 AMI 形式提供。

> **Note**
>
> Storage Gateway 社区 AMIs 由发布并完全支持 AWS。你可以看到发布者是一个 AWS经过验证的提供商。

1. 要设置 Amazon EC2 实例，请在工作流的平台选项部分的主机平台下面选择 Amazon EC2。有关配置 Amazon EC2 实例的说明，请参阅部署亚马逊 EC2 实例来托管您的亚马逊 FSx 文件网关。
2. 选择启动实例，在 Amazon EC2 控制台中打开 AWS Storage Gateway AMI 模板并自定义其他设置，例如实例类型、网络设置和配置存储。
3. 或者，您可以在 Storage Gateway 控制台中选择使用默认设置，使用默认配置来部署 Amazon EC2 实例。

   使用默认设置创建的 Amazon EC2 实例具有以下默认规格：

   - 实例类型 - m5.xlarge
   - 网络设置
     - 对于 VPC，选择要在其中运行 EC2 实例的 VPC。
     - 对于子网，指定要在其中启动 EC2 实例的子网。

       > **Note**
       >
       > 只有在 VPC 管理控制台中为 VPC 子网激活了自动分配公有 IP 地址设置后，VPC 子网才会出现在下拉列表中。

     - 自动分配公有 IP – 已激活
     - 已创建 EC2 安全组并与 EC2 实例关联。安全组具有以下入站端口规则：

> **Note**
>
> 在网关激活期间，您需要打开端口 80。在激活后立即关闭该端口。此后，只能通过选定 VPC 中的其他端口来访问您的 EC2 实例。
> 只能通过与网关位于同一 VPC 中的主机来访问网关上的文件共享。如果需要从 VPC 之外的主机访问文件共享，则应更新相应的安全组规则。
> 您可以随时编辑安全组，方法是导航到 Amazon EC2 实例详细信息页面，选择安全，导航到安全组详细信息并选择安全组 ID。

端口：	协议	文件系统协议
80	TCP	用于激活的 HTTP 访问权限
137	UDP	NetBIOS
138	UDP	NetBIOS
139	TCP、UDP	SMB
389	TCP	LDAP
445	TCP	SMB

- 配置存储

默认设置	AMI 根卷	卷 2 缓存
设备名称		'/dev/sdb'
Size	80 GiB	165 GiB
卷类型	gp3	gp3
IOPS	3000	3000

默认设置	AMI 根卷	卷 2 缓存				
终止时删除	支持	是				
已加密	否	否				
吞吐量	125	125				

为 FSx 文件网关部署自定义的 Amazon EC2 主机

您可以在亚马逊弹性计算云 (A EC2) 实例上部署和激活 Amazon S3 FSx 文件网关亚马逊文件网关。AWS Storage Gateway Amazon 系统映像 (AMI) 以社区 AMI 形式提供。

> **Note**
>
> Storage Gateway 社区 AMIs 由发布并完全支持 AWS。你可以看到发布者是一个 AWS经过验证的提供商。
> 文件网关 AMIs 使用以下命名约定。AMI 名称中附加的版本号会随着每个版本的发布而变化。
> `aws-storage-gateway-FILE_FSX_SMB-2.2.3`

部署 Amazon EC2 实例来托管您的亚马逊 FSx 文件网关

1. 开始使用 Storage Gateway 控制台来设置新的网关。有关说明，请参阅设置亚马逊 FSx 文件网关。当您进入平台选项部分时，在主机平台中选择 Amazon EC2，然后按照以下步骤启动将托管您的文件网关的 Amazon EC2 实例。
2. 选择 “启动实例”，在 Amazon EC2 控制台中打开 AWS Storage Gateway AMI 模板，您可以在其中配置其他设置。

   使用 Quicklaunch 来启动具有默认设置的 Amazon EC2 实例。有关 Amazon EC2 Quicklaunch 默认规范的更多信息，请参阅 Amazon EC2 的 Quicklaunch 配置规范。
3. 在名称中，为 Amazon EC2 实例输入一个名称。实例部署完成后，您可以搜索此名称，在 Amazon EC2 控制台的列表页面上找到您的实例。
4. 在实例类型部分的实例类型列表中，为您的实例选择硬件配置。硬件配置必须满足某些最低要求才能支持您的网关。我们建议您首先使用 m5.xlarge 实例类型，它满足网关正常运行所需的最低硬件要求。有关更多信息，请参阅 对 Amazon EC2 实例类型的要求。

如果需要，您可以在启动后调整实例的大小。有关更多信息，请参阅《Amazon EC2 用户指南》中的调整实例大小。

> **Note**
>
> 某些实例类型，特别是 i3 EC2，使用 NVMe SSD 磁盘。这可能会在您启动或停止文件网关时导致出现问题；例如，您可能会丢失缓存中的数据。监控 `CachePercentDirty` Amazon CloudWatch 指标，只有在该参数为时才启动或停止系统`0`。要了解有关网关监控指标的更多信息，请参阅 CloudWatch 文档中的 Storage Gateway 指标和维度。

5. 在密钥对(登录) 部分的密钥对名称 -必需中，选择要用于安全连接到实例的密钥对。如有必要，您可以创建新的密钥对。有关更多信息，请参阅《适用于 Linux 实例的 Amazon Elastic Compute Cloud 用户指南》中的创建密钥对。
6. 在网络设置部分，检查预配置的设置并选择编辑来更改以下字段：
   a. 对于 VPC - 必需，请选择要在其中启动 Amazon EC2 实例的 VPC。有关 Amazon VPC 的更多信息，请参阅《Amazon Virtual Private Cloud 用户指南》中的 Amazon VPC 的工作原理。
   b. （可选）对于子网，请选择要在其中启动 Amazon EC2 实例的子网。
   c. 对于自动分配公有 IP，选择启用。
7. 在防火墙（安全组）子部分中，查看预配置的设置。如果您愿意，可以更改要为您的 Amazon EC2 实例创建的新安全组的默认名称和描述，也可以选择应用现有安全组中的防火墙规则。
8. 在入站安全组规则子部分中，添加防火墙规则来打开客户端用于连接实例的端口。有关 Amazon S3 文件网关 所需端口的更多信息，请参阅端口要求。 FSx 有关添加防火墙规则的更多信息，请参阅《适用于 Linux 实例的 Amazon Elastic Compute Cloud 用户指南》中的安全组规则。

> **Note**
>
> Amazon FSx File Gateway 要求在网关激活期间为入站流量开放 TCP 端口 80 和一次性 HTTP 访问。激活后，您可以关闭此端口。
> 此外，必须打开 TCP 端口 445 才能访问 SMB，打开 UDP 端口 137 才能访问 NetBIOS，打开 UDP 端口 138 才能访问 NetBIOS，打开 TCP 端口 389 才能访问 LDAP。

9. 在高级网络配置子部分中，检查预配置的设置，必要时进行更改。
10. 在配置存储部分，选择添加新卷，将存储添加到网关实例。

> **Important**
>
> 除了预配置的根卷外，您还必须至少添加一个容量至少为 150 GiB 的 Amazon EBS 卷作为缓存存储。为了提高性能，我们建议分配多个 EBS 卷作为缓存存储，每个卷至少为 150 GiB。

11. 在高级详细信息部分，检查预配置的设置，必要时进行更改。
12. 选择启动实例，使用已配置的设置启动您的新 Amazon EC2 网关实例。
13. 要确认您的新实例可成功启动，请导航至 Amazon EC2 控制台中的实例页面，然后按名称搜索您的新实例。确保实例状态显示为正在运行且带有绿色复选标记，并确保状态检查已完成且显示绿色复选标记。
14. 从详细信息页面中选择您的实例。从 “实例摘要” 部分复制公有 IP 地址，然后返回 Storage Gateway 控制台中的设置网关页面，继续设置 亚马逊 FSx 文件网关。

您可以使用 Storage Gateway 控制台或查询 AWS Systems Manager 参数存储来确定用于启动文件网关的 AMI ID。

要确定 AMI ID，请执行以下任一操作：

- 开始使用 Storage Gateway 控制台来设置新的网关。有关说明，请参阅设置亚马逊 FSx 文件网关。当您进入平台选项部分时，选择 Amazon EC2 作为主机平台，然后选择启动实例以在 Amazon EC2 控制台中打开 AWS Storage Gateway AMI 模板。

  您将被重定向到 EC2 社区 AMI 页面，在该页面中，您可以在 URL 中看到您 AWS 所在地区的 AMI ID。

- 查询 Systems Manager 参数存储。你可以使用 AWS CLI 或 Storage Gateway API 查询命名空间下的 Systems Manager 公共参数`/aws/service/storagegateway/ami/FILE_FSX_SMB/latest`。例如，使用以下 CLI 命令返回 AWS 区域 您指定的当前 AMI 的 ID。

  ```
  aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/
  FILE_FSX_SMB/latest
  ```

  该 CLI 命令会返回类似以下内容的输出：

  ```
  {
      "Parameter": {
  ```

```
        "Type": "String",
        "LastModifiedDate": 1561054105.083,
        "Version": 18,
         "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/
FILE_FSX_SMB/latest",
         "Name": "/aws/service/storagegateway/ami/FILE_FSX_SMB/latest",,
        "Value": "ami-033d1edba5606cffb"
    }
}
```

修改 Amazon EC2 实例元数据选项

实例元数据服务（IMDS）是实例上的组件，可提供对 Amazon EC2 实例元数据的安全访问。可以将实例配置为接受使用 IMDS 版本 1 (IMDSv1) 或要求所有元数据请求都使用 IMDS 版本 2 (IMDSv2) 的传入元数据请求。 IMDSv2 使用面向会话的请求并缓解了几种可用于尝试访问 IMDS 的漏洞。有关信息 IMDSv2，请参阅 Amazon Elastic Compute Cloud 用户指南中的实例元数据服务版本 2 的工作原理。

我们建议托管 Storage Gateway 的所有亚马逊 EC2 实例都需要 imdsv2。 IMDSv2 默认情况下，所有新启动的网关实例都是必需的。如果您的现有实例仍配置为接受 IMDSv1 元数据请求，请参阅 Amazon Elastic Compute Cloud 用户指南 IMDSv2中的要求使用，了解如何修改您的实例元数据选项以要求使用 IMDSv2。应用此更改不需要重启实例。

将 VM 时间与 Hyper-V 或 Linux KVM 主机时间同步

对于部署在上的网关 VMware ESXi，设置虚拟机管理程序主机时间并将虚拟机时间同步到主机就足以避免时间偏差。有关更多信息，请参阅 将 VM 时间与 VMware 主机时间同步。对于在 Microsoft Hyper-V 或 Linux KVM 上部署的网关，我们建议您使用下面介绍的过程来定期检查虚拟机时间。

查看虚拟机监控程序网关虚拟机的时间并将其同步到网络时间协议（NTP）服务器

1. 登录到网关的本地控制台：
   - 有关登录到 Microsoft Hyper-V 本地控制台的更多信息，请参阅使用 Microsoft Hyper-V 访问网关本地控制台。
   - 有关登录到基于 Linux 内核的虚拟机（KVM）的本地控制台的更多信息，请参阅使用 Linux KVM 访问网关本地控制台。
2. 在 Storage Gateway 配置主菜单屏幕上，输入相应的数字以选择系统时间管理。
3. 在系统时间管理菜单屏幕上，输入相应的数字以选择查看和同步系统时间。

网关本地控制台显示当前系统时间，并将其与 NTP 服务器报告的时间进行比较，然后以秒为单位报告两个时间之间的确切差异。

4. 如果时间差异大于 60 秒，请输入 **y** 来将系统时间与 NTP 时间同步。否则，请输入 **n**。

   时间同步可能需要一些时间。

将 VM 时间与 VMware 主机时间同步

若要成功激活网关，您必须确保 VM 时间与主机时间同步，并且主机时间设置正确。在本节中，您首先要将 VM 时间与主机时间同步。然后，您将检查主机时间，如果需要，您应设置主机时间并将主机配置为自动与网络时间协议 (NTP) 服务器同步。

> **Important**
>
> 要成功激活网关，就需要同步 VM 时间和主机时间。

如需将 VM 时间与主机时间同步

1. 配置您的 VM 时间。

   a. 在 vSphere 客户端中，在应用程序窗口左侧的面板中，右键单击网关 VM 的名称以打开虚拟机的快捷菜单，然后选择编辑设置。

      “Virtual Machine Properties”对话框打开。

   b. 选择 “选项” 选项卡，然后从选项列表中选择 “VMware 工具”。

   c. 选中虚拟机属性对话框右侧高级部分中的与主机同步访客时间选项，然后选择确定。

      VM 时间与主机进行同步。

2. 配置主机时间。

   请注意，确保您设置了正确的主机时间。如果您尚未配置主机时间，请执行下列步骤进行设置并将其与 NTP 服务器同步。

   a. 在 VMware vSphere 客户端中，在左侧面板中选择 vSphere 主机节点，然后选择配置选项卡。

   b. 在软件面板中选择时间配置，然后选择属性链接。

“Time Configuration”对话框显示。

c. 在日期和时间下，设置 vSphere 主机的日期和时间。

d. 将主机配置为自动将其时间与 NTP 服务器同步。

i. 在时间配置对话框中，选择选项，然后在 NTP 进程守护程序（ntpd）选项对话框中，选择左侧面板中的 NTP 设置。

ii. 选择 Add 以添加新 NTP 服务器。

iii. 在 Add NTP Server 对话框中，键入 NTP 服务器的 IP 地址或完全限定域名，然后选择 OK。

可以将 `pool.ntp.org` 用作域名。

iv. 在 NTP 进程守护程序（ntpd）选项对话框中，选择左侧面板中的常规。

v. 在服务命令下，选择启动来启动服务。

请注意，如果您稍后更改此 NTP 服务器参考或添加另一 NTP 服务器参考，则需要重启服务才能使用新服务器。

e. 选择 OK 以关闭 NTP Daemon (ntpd) Options 对话框。

f. 选择 OK 以关闭 Time Configuration 对话框。

为网关配置网络适配器

Storage Gateway 默认使用单个 VMXNET3 (10 GbE) 网络适配器，但您可以将网关配置为使用多个网络适配器，以便多个 IP 地址可以访问它。您可能希望在以下情况下执行此操作：

- 更大程度地增加吞吐量：当网络适配器成为瓶颈时，您可能希望更大程度地增加网关的吞吐量。
- 应用程序区分 - 您可能需要区分应用程序写入到网关的卷的方式。例如，您可以选择让关键存储应用程序独占使用为网关定义的一个特定适配器。
- 网络限制：您的应用程序环境可能要求您将文件共享及连接到这些共享的启动程序保留在一个独立网络中。该网络与网关用来与 AWS通信的网络不同。

在典型的多适配器用例中，将一个适配器配置为网关与之通信的路由 AWS （即默认网关）。除了这个适配器之外，启动程序必须与包含所连接文件共享的适配器位于同一个子网中。否则，可能无法与预定目标通信。如果目标配置在用于与之通信的同一适配器上 AWS，则该目标的文件共享流量和 AWS 流量将流经同一个适配器。

在某些情况下，您可以将一个适配器配置为连接到 Storage Gateway 控制台，然后添加另一个适配器。在此类情况下，Storage Gateway 会自动将路由表配置为使用第二个适配器作为首选路由。有关如何配置多个适配器的说明，请参阅以下主题：

主题

- 为 VMware ESXi 主机 NICs 上的多个网关配置网关
- 在 Microsoft Hyper-V NICs 主机中为多个网关配置网关

为 VMware ESXi 主机 NICs 上的多个网关配置网关

以下过程假设您的网关 VM 已经定义了一个网络适配器，并描述了如何在上面添加适配器 VMware ESXi。

将网关配置为使用 VMware ESXi 主机中的其他网络适配器

1. 关闭网关。
2. 在 VMware vSphere 客户端中，选择您的网关虚拟机。

   VM 在此过程中可能保持开启状态。
3. 在客户端中，打开网关 VM 的上下文（右键单击）菜单，然后选择 Edit Settings (编辑设置)。
4. 在虚拟机属性对话框的硬件选项卡上，选择添加来添加设备。
5. 按 Add Hardware (添加硬件) 向导添加网络适配器。

   a. 在 Device Type (设备类型) 窗格中，选择 Ethernet Adapter (以太网适配器) 以添加适配器，然后选择 Next (下一步)。

   b. 在网络类型窗格中，确保为类型选择开机时连接，然后选择下一步。

      我们建议您将 VMXNET3 网络适配器与 Storage Gateway 配合使用。有关适配器列表中可能出现的适配器类型的更多信息，请参阅ESXi 和 vCenter Server 文档中的网络适配器类型。

   c. 在 Ready to Complete (已准备好完成) 窗格中，查看信息，然后选择 Finish (完成)。
6. 选择 VM 的摘要选项卡，然后选择 IP 地址 框旁边的查看全部。虚拟机 IP 地址窗口显示您可以用来访问网关的全部 IP 地址。确认第二个 IP 地址已针对该网关列出。

> **Note**
>
> 适配器更改生效和 VM 摘要信息刷新可能需要少许时间。

7. 在 Storage Gateway 控制台中，打开网关。
8. 在 Storage Gateway 控制台的导航窗格中，选择网关，然后选择要在其中添加适配器的网关。确认 Details (详细信息) 选项卡中列出了第二个 IP 地址。

有关 Hyper-V 和 KVM 主机常见的本地控制台任务的信息，请参阅 VMware 在虚拟机本地控制台上执行任务

在 Microsoft Hyper-V NICs 主机中为多个网关配置网关

下列步骤假定您的网关 VM 已定义了一个网络适配器，并且您将添加第二个适配器。此过程演示如何为 Microsoft Hyper-V 主机添加适配器。

将网关配置为使用 Microsoft Hyper-V 主机中的另一个网络适配器

1. 在 Storage Gateway 控制台中，关闭网关。
2. 在 Microsoft Hyper-V Manager 中，从虚拟机面板中选择网关 VM。
3. 如果网关 VM 尚未关闭，请右键单击 VM 名称以打开上下文菜单，然后选择关闭。
4. 右键单击网关 VM 名称以打开上下文菜单，然后选择设置。
5. 在设置对话框中的硬件下，选择添加硬件。
6. 在设置对话框右侧的添加硬件面板中，选择网络适配器，然后选择添加来添加设备。
7. 配置网络适配器，然后选择 Apply (应用) 以应用设置。
8. 在设置对话框的硬件下，确认新的网络适配器已添加到硬件列表中，然后选择确定。
9. 使用 Storage Gateway 控制台开启网关。
10. 在 Storage Gateway 控制台的导航面板中，选择网关，然后选择向其中添加了适配器的网关。确认详细信息选项卡中列出了第二个 IP 地址。

有关 Hyper-V 和 KVM 主机常见的本地控制台任务的信息，请参阅 VMware 在虚拟机本地控制台上执行任务

将 VMware vSphere 高可用性与 Storage Gateway 配合使用

Storage Gateway VMware 通过一组与 VMware vSphere 高可用性 (HA) 集成的应用程序级运行状况检查提供高可用性。VMware 此方法有助于保护存储工作负载免受硬件、管理程序或网络故障的影响。它还有助于防止软件错误，例如连接超时和文件共享或卷不可用。

通过这种集成，部署在本地 VMware 环境或 VMware 云端环境中的网关可以 AWS 自动从大多数服务中断中恢复。此操作通常在 60 秒内完成，并且不会丢失数据。

> **Note**
>
> 如果您在 VMware HA 集群中部署 Storage Gateway，我们建议您执行以下操作：
>
> - 仅在 VMware 集群中的一台主机上部署包含 Storage Gateway 虚拟机的 ESX .ova 可下载软件包。
> - 在部署 .ova 程序包时，选择一个不在主机本地的数据存储。而是使用一个可供群集的所有主机访问的数据存储。如果您选择的是主机本地数据存储，而主机发生了故障，则群集中的其他主机可能无法访问该数据源，并且可能无法成功地故障转移到另一台主机。
> - 使用集群部署时，如果您将 .ova 程序包部署到集群，请在系统提示您这样做时选择一台主机。或者您也可以直接部署到群集中的主机里。

以下主题介绍如何在 VMware HA 集群中部署 Storage Gateway：

主题

- 配置您的 vSphere VMware 高可用集群
- 设置您的网关类型
- 部署网关
- （可选）为集群 VMs 上的其他人添加覆盖选项
- 激活网关
- 测试您的 VMware 高可用性配置

配置您的 vSphere VMware 高可用集群

首先，如果您尚未创建 VMware 集群，请创建一个集群。有关如何创建 VMware 集群的信息，请参阅文档中的创建 vSphere HA 集群。 VMware

接下来，将您的 VMware 集群配置为使用 Storage Gateway。

配置您的 VMware 集群

1. 在 VMware vSphere 的 “编辑集群设置” 页面上，确保为虚拟机和应用程序监控配置了虚拟机监控。为此，请为每个选项设置以下值：

- 主机故障响应：重新启动 VMs
- 主机隔离的响应：关闭并重启 VMs
- Datastore with PDL (具有 PDL 的数据存储)：Disabled (已禁用)
- Datastore with APD (具有 APD 的数据存储)：Disabled (已禁用)
- VM Monitoring (VM 监控)：VM and Application Monitoring (VM 和应用程序监控)

2. 通过调整以下值来微调集群的敏感度：

   - 故障间隔 - 在此间隔之后，如果未收到 VM 检测信号，则将重新启动 VM。
   - 最短正常运行时间 - 在 VM 开始监控 VM 工具的检测信号之后，集群等待的时间。
   - 每个 VM 的最大重置次数 - 集群在最大重置时段内重启 VM 的最大次数。
   - 最大重置次数的时段 - 计算每个 VM 的最大重置次数的时段。

   如果您不确定要设置的值，请使用以下示例设置：

   - Failure interval (故障间隔)：**30** 秒
   - Minimum uptime (最短正常运行时间)：**120** 秒
   - Maximum per-VM resets (每个 VM 的最大重置次数)：**3**
   - Maximum resets time window (最长重置时段)：**1** 小时

如果您在集群上 VMs 运行其他值，则可能需要专门为虚拟机设置这些值。在从 .ova 部署 VM 之前，无法执行此操作。有关设置这些值的更多信息，请参阅 （可选）为集群 VMs 上的其他人添加覆盖选项。

设置您的网关类型

按照以下程序来设置网关

下载适用于您的网关类型的 .ova 映像

- 从下列选项之一下载网关类型的 .ova 映像：
  - 文件网关：创建并激活 Amazon FSx 文件网关

部署网关

在已配置的集群中，将 .ova 映像部署到集群的主机之一。有关说明，请参阅 v VMware Sphere 在线文档中的部署 OVF 或 OVA 模板。

部署网关 .ova 映像

1. 将 .ova 映像部署到集群中的主机之一。
2. 确保为根磁盘和缓存选择的数据存储对集群中的所有主机可用。

（可选）为集群 VMs 上的其他人添加覆盖选项

如果您的集群上 VMs 正在运行其他虚拟机，则可能需要专门为每个 VM 设置集群值。有关说明，请参阅 VMware vSphere 在线文档中的自定义单个虚拟机。

为集群 VMs 上的其他人添加覆盖选项

1. 在 VMware vSphere 的 “摘要” 页面上，选择您的集群以打开集群页面，然后选择配置。
2. 选择 Configuration (配置) 选项卡，然后选择 VM Overrides (VM 覆盖)。
3. 添加新的 VM 覆盖选项来更改每个值。

   为 vSphere HA - VM 监控下的每个选项设置以下值：

   - VM 监控：已启用覆盖 - VM 和应用程序监控
   - VM 监控灵敏度：已启用覆盖 - VM 和应用程序监控
   - VM 监控：自定义
   - 故障间隔：**30** 秒
   - 最短正常运行时间：**120** 秒
   - Maximum per-VM resets (每个 VM 的最大重置次数)：**5**
   - 最大重置时段：**1** 小时内

激活网关

在您的 VMware 环境中部署.ova 后，使用 Storage Gateway 控制台激活您的网关。有关说明，请参阅查看设置以及激活您的亚马逊 FSx 文件网关。

测试您的 VMware 高可用性配置

激活网关后，请测试您的配置。

测试您的 VMware HA 配置

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在导航窗格上，选择 Gateways，然后选择要测试 VMware HA 的网关。
3. 对于操作，请选择验证 VMware HA。
4. 在出现的 “验证 VMware 高可用性配置” 框中，选择 “确定”。

   > **Note**
   >
   > 测试 VMware HA 配置会重新启动网关 VM 并中断与网关的连接。该测试可能需要几分钟才能完成。

   如果测试成功，则控制台中网关的详细信息选项卡中将显示 Verified (已验证) 状态。
5. 请选择 Exit（退出）。

您可以在 Amazon CloudWatch 日志组中找到有关 VMware HA 事件的信息。有关更多信息，请参阅使用日志组获取 文件网关运行状况日志 CloudWatch。

获取网关的激活密钥

要接收网关的激活密钥，请向网关虚拟机 (VM) 发出 Web 请求。VM 返回包含激活密钥的重定向，激活密钥作为 `ActivateGateway` API 操作的参数之一传递，用于指定网关的配置。有关更多信息，请参阅 Storage Gateway API 参考ActivateGateway中的。

> **Note**
>
> 如果未使用，网关激活密钥将在 30 分钟后过期。

您向网关 VM 发出的请求包括激活发生的 AWS 区域。响应中重定向返回的 URL 包含称为 `activationkey` 的查询字符串参数。此查询字符串参数是您的激活密钥。此查询字符串的格式如下

所示：`http://gateway_ip_address/?activationRegion=activation_region`。此查询的输出会返回激活区域和密钥。

URL 还包括 `vpcEndpoint`，即使用 VPC 端点类型连接的网关的 VPC 端点 ID。

> **Note**
>
> AWS Storage Gateway 硬件设备、虚拟机映像模板和 Amazon EC2 亚马逊系统映像 (AMI) 已预先配置了接收和响应本页所述网络请求所需的 HTTP 服务。不要求也不建议在网关上安装任何其他服务。

主题

- Linux (curl)
- Linux (bash/zsh)
- 微软 Windows PowerShell
- 使用本地控制台

Linux (curl)

以下示例向您显示如何使用 Linux (curl) 获取激活密钥。

> **Note**
>
> 将突出显示的变量替换为您的网关的实际值。可接受的值如下所示：
>
> - *gateway_ip_address*-您的网关 IPv4 地址，例如 `172.31.29.201`
> - *gateway_type*-您要激活的网关类型，例如`STOREDCACHED`、`VTL`、`FILE_S3`、或`FILE_FSX_SMB`。
> - *region_code*-您要激活网关的区域。请参阅《AWS 一般参考指南》中的区域端点。如果未指定此参数，或者提供的值拼写错误或与有效区域不匹配，则该命令将默认为 `us-east-1` 区域。
> - *vpc_endpoint*-例如，网关的 VPC 终端节点名称`vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com`。

要获取公有端点的激活密钥，请执行以下操作：

```
curl "http://gateway_ip_address/?activationRegion=region_code&no_redirect"
```

要获取 VPC 端点的激活密钥，请执行以下操作：

```
curl "http://gateway_ip_address/?
activationRegion=region_code&vpcEndpoint=vpc_endpoint&no_redirect"
```

Linux (bash/zsh)

以下示例显示如何使用 Linux (bash/zsh) 获取 HTTP 响应、分析 HTTP 标头以及获取激活密钥。

```
function get-activation-key() {
  local ip_address=$1
  local activation_region=$2
  if [[ -z "$ip_address" || -z "$activation_region" || -z "$gateway_type" ]]; then
    echo "Usage: get-activation-key ip_address activation_region gateway_type"
    return 1
  fi

  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region&gatewayType=$gateway_type"); then
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
    echo "$activation_key_param" | cut -f2 -d=
  else
    return 1
  fi
}
```

微软 Windows PowerShell

以下示例向您展示了如何使用 Microsoft Windows PowerShell 获取 HTTP 响应、解析 HTTP 标头和获取激活密钥。

```
function Get-ActivationKey {
  [CmdletBinding()]
  Param(
    [parameter(Mandatory=$true)][string]$IpAddress,
    [parameter(Mandatory=$true)][string]$ActivationRegion,
```

```
    [parameter(Mandatory=$true)][string]$GatewayType
  )
  PROCESS {
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion&gatewayType=$GatewayType" -MaximumRedirection 0 -
ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

使用本地控制台

以下示例显示了如何使用本地控制台来生成和显示激活密钥。

从本地控制台获取网关的激活密钥

1. 以管理员身份登录到本地控制台。
2. 登录并查看 AWS 设备激活 - 配置主菜单后，选择 0 来选择获取激活密钥。
3. 选择 Storage Gateway 作为网关系列选项。
4. 出现提示时，输入您要激活网关 AWS 区域 的位置。
5. 对于公有端点，输入 1，或对于 VPC 端点，输入 2 作为网络类型。
6. 对于标准端点，输入 1，或对于美国联邦信息处理标准 (FIPS) 端点，输入 2 作为端点类型。

Direct Connect 与 Storage Gateway 一起使用

Direct Connect 将您的内部网络链接到亚马逊 Web Services 云。通过 Direct Connect 与 Storage Gateway 配合使用，您可以创建满足高吞吐量工作负载需求的连接，从而在本地网关和 AWS之间提供专用的网络连接。

Storage Gateway 使用公有端点。 Direct Connect 建立连接后，您可以创建一个公共虚拟接口，以允许将流量路由到 Storage Gateway 端点。该公共虚拟接口将绕过您的网络路径中的 Internet 服务提供商。Storage Gateway 服务的公共终端节点可以与该 Direct Connect 位置位于同一个 AWS 区域，也可以位于不同的 AWS 区域。

下图显示了如何 Direct Connect 使用 Storage Gateway 的示例。

网络架构显示 Storage Gateway 使用 AWS 直接连接连接到云端。

以下过程假定您已创建正常运行的网关。

Direct Connect 与 Storage Gateway 配合使用

1. 在您的本地数据中心和 Storage Gateway 终端节点之间创建并建立 AWS Direct Connect 连接。有关如何创建连接的更多信息，请参阅《Direct Connect 用户指南》中的 Direct Connect入门。
2. 将您的本地 Storage Gateway 设备连接到 Direct Connect 路由器。
3. 创建一个公共虚拟接口，然后相应地配置您的本地路由器。有关更多信息，请参阅《Direct Connect 用户指南》中的创建虚拟接口。

有关的详细信息 Direct Connect，请参阅什么是 Direct Connect？ 在《Direct Connect 用户指南》中。

Active Directory 服务账户权限要求

如果您计划使用 Microsoft Active Directory 为用户提供对您的文件系统的经过身份验证的访问权限 AWS Storage Gateway，则需要确保您拥有 Active Directory 服务帐户，并且该服务帐户具有将计算机加入您的域的委派权限。服务账户是已委派权限来执行某些任务的 Active Directory 用户账户。当您将 Storage Gateway 加入您的 Active Directory 域时，您需要提供此账户的用户名和密码凭证。

在要将网关加入的 OU 中，必须为 Active Directory 服务账户委派以下权限：

- 能够创建和删除计算机对象
- 能够重置密码
- 能够修改权限
- 能够限制账户读取和写入数据
- 验证读取和写入账户限制的能力
- 验证写入服务主体名称的能力
- 验证写入 DNS 主机名的能力

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

获取网关设备的 IP 地址

在选择主机并部署网关 VM 后，您可以连接并激活网关。为此，需要使用网关 VM 的 IP 地址。您可以从网关的本地控制台获取 IP 地址。您可以登录到本地控制台并从控制台页面顶部获取 IP 地址。

对于本地部署的网关，您也可以从管理程序获取 IP 地址。对于 Amazon EC2 网关，您也可以从 Amazon EC2 管理控制台获取 Amazon EC2 实例的 IP 地址。要了解如何获取网关的 IP 地址，请参阅以下内容之一：

- VMware 主持人：使用访问网关本地控制台 VMware ESXi
- HyperV 主机：使用 Microsoft Hyper-V 访问网关本地控制台
- 基于 Linux 内核的虚拟机 (KVM) 主机：使用 Linux KVM 访问网关本地控制台
- EC2 主机：从 Amazon EC2 主机获取 IP 地址

找到 IP 地址之后，请记下它。然后返回到 Storage Gateway 控制台并在控制台中键入该 IP 地址。

从 Amazon EC2 主机获取 IP 地址

要获取用于部署网关的 Amazon EC2 实例的 IP 地址，请登录到 EC2 实例的本地控制台。然后从控制台页面顶部获取 IP 地址。有关说明，请参阅。

您也可以从 Amazon EC2 管理控制台获取 IP 地址。我们建议使用公有 IP 地址进行激活。要获取公有 IP 地址，请使用程序 1。如果您选择使用弹性 IP 地址，请参阅程序 2。

程序 1：使用公有 IP 地址连接到网关

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 在导航窗格中，选择 Instances (实例)，然后选择用于部署网关的 EC2 实例。
3. 选择底部的 Description (描述) 选项卡，然后记下公有 IP 地址。您可以使用此 IP 地址连接到网关。返回到 Storage Gateway 控制台并键入该 IP 地址。

如果您想使用弹性 IP 地址进行激活，可使用以下程序。

程序 2：使用弹性 IP 地址连接到网关

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 在导航窗格中，选择 Instances (实例)，然后选择用于部署网关的 EC2 实例。

3. 选择底部的 Description (描述) 选项卡，然后记下 Elastic IP (弹性 IP) 值。您可以使用此弹性 IP 地址连接到网关。返回到 Storage Gateway 控制台并键入弹性 IP 地址。

了解 Storage Gateway 资源和资源 IDs

在 Storage Gateway 中，主要资源是网关，其他资源类型是文件共享。文件共享称为子资源，除非这些资源与网关关联，否则视为不存在。

这些资源和子资源具有与之关联的唯一 Amazon 资源名称 (ARNs)，如下表所示。

资源类型	ARN 格式
网关 ARN	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`*
文件共享 ARN	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:share/`*`share-id`*

使用资源 IDs

在您创建某个资源时，Storage Gateway 会为该资源分配一个唯一资源 ID。此资源 ID 是资源 ARN 的一部分。资源 ID 采用以下格式：资源标识符后跟连字符，然后是 8 个字母与数字的唯一组合。例如，网关 ID 的格式为 `sgw-12A3456B`，其中 `sgw` 是网关的资源标识符。

Storage Gateway 资源 ID 使用大写字母。不过，当您将这些资源 ID 与 Amazon EC2 API 结合使用时，Amazon EC2 需要采用小写形式的资源 ID。您必须将资源 ID 更改为小写才能将其与 EC2 API 结合使用。例如，在 Storage Gateway 中，卷的 ID 可能为 `vol-1122AABB`。当您将此 ID 与 EC2 API 结合使用时，您必须将其更改为 `vol-1122aabb`。否则，EC2 API 的行为方式可能不符合预期。

> **Important**
>
> IDs 对于 Storage Gateway 卷和从网关卷创建的 Amazon EBS 快照正在更改为更长的格式。自 2016 年 12 月起，将使用包含 17 个字符的字符串创建所有新的卷和快照。从 2016 年 4 月开始，您将能够使用更长的时间， IDs 这样您就可以用新格式测试您的系统。有关更多信息，请参阅更长的 EC2 和 EBS 资源 IDs。
> 例如，具有加长卷 ID 格式的卷 ARN 如下所示：

arn:aws:storagegateway:us-west-2:111122223333:gateway/sgw-12A3456B/volume/vol-1122AABBCCDDEEFFG.
具有加长 ID 格式的快照 ID 如下所示：snap-78e226633445566ee。
欲了解更多信息，请参阅 2016 年发布的公告：Heads-up — Storage Gateway 卷更长，快照 IDs 将于 2016 年推出。

标记 Storage Gateway 资源

在 Storage Gateway 中，您可以使用标签来管理资源。利用标签，您可以向资源添加元数据和对资源分类，以便更轻松地管理它们。每个标签都包含您定义的一个键-值对。您可以向网关、卷和虚拟磁带添加标签。您可以根据添加的标签搜索和筛选这些资源。

例如，您可以使用这些标签标识组织中的每个部门使用的 Storage Gateway 资源。您可能为会计部使用的网关和卷添加类似于下面的标签：(key=department 和 value=accounting)。然后，您可以使用此标签进行筛选，以便标识会计部使用的所有网关和卷并使用此信息确定成本。有关更多信息，请参阅使用成本分配标签和使用标签编辑器。

如果您存档了一个已标记的虚拟磁带，则该磁带将在存档中保留其标签。同样，如果您将磁带从存档取回到另一网关，则该标记将保留在新网关中。

对于文件网关，您可以使用标签控制对资源的访问。有关如何执行此操作的信息，请参阅 使用标签控制对网关和资源的访问。

标签没有任何语义意义，应作为字符串进行解析。

以下限制适用于标签：

- 标签键和值区分大小写。
- 每个资源的最大标签数是 50。
- 标签键不能以 aws: 开头。此前缀是专为 AWS 使用而预留。
- 键属性的有效字符包括 UTF-8 字母和数字、空格以及特殊字符 +、-、=、.、_、:、/ 和 @。

使用标签

您可以使用 Storage Gateway 控制台、Storage Gateway API 或 Storage Gateway 命令行界面 (CLI) 处理标签。下面的过程介绍如何在控制台上添加、编辑和删除标签。

添加标签

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在导航窗格中，选择要标记的资源。

   例如，要标记网关，请选择 Gateways，然后从网关列表中选择要标记的网关。
3. 选择 Tags，然后选择 Add/edit tags。
4. 在 Add/edit tags 对话框中，选择 Create tag。
5. 为 Key 键入密钥，为 Value 键入值。例如，您可以键入 **`Department`** 作为密钥，并键入 **`Accounting`** 作为值。

   > **Note**
   >
   > 您可以将 Value 框留空。
6. 选择 Create Tag 以添加更多标签。您可以向资源添加多个标签。
7. 添加完标签后，选择 Save。

编辑标签

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 选择要编辑其标签的资源。
3. 选择 Tags 以打开 Add/edit tags 对话框。
4. 选择要编辑的标签旁的铅笔图标，然后编辑该标签。
5. 编辑完标签后，选择 Save。

删除标签

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 选择要删除其标签的资源。
3. 选择 Tags，然后选择 Add/edit tags 以打开 Add/edit tags 对话框。
4. 选择要删除的标签旁边的 X 图标，然后选择 Save。

使用开源组件 AWS Storage Gateway

本节介绍我们在提供 AWS Storage Gateway 功能时所依赖的第三方工具和许可证。

主题

- Storage Gateway 的开源组件
- Amazon FSx 文件网关的开源组件

Storage Gateway 的开源组件

一些第三方工具和许可证用于为卷网关、磁带网关和 Amazon S3 文件网关提供功能。

使用以下链接下载软件附带 AWS Storage Gateway 的某些开源软件组件的源代码：

- 对于部署在 VMware ESXi：sources.tar 上的 Storage Gateway 设备
- 对于在 Microsoft Hyper-V 上部署的 Storage Gateway 设备：sources_hyperv.tar
- 对于在 Linux 基于内核的虚拟机（KVM）上部署的 Storage Gateway 设备：sources_KVM.tar

该产品包括 OpenSSL Project 为在 OpenSSL Toolkit (http://www.openssl.org/) 中使用而开发的软件。有关所有依赖的第三方工具的相关许可证，请参阅第三方许可证。

Amazon FSx 文件网关的开源组件

一些第三方工具和许可证用于提供 Amazon FSx 文件网关（FSx 文件网关）功能。

使用以下链接下载 FSx File Gateway 软件中包含的某些开源软件组件的源代码：

- 适用于亚马逊 FSx 文件网关 2021-07-07 版本：-opensource.tgz sgw-file-fsx-smb
- 适用于亚马逊 FSx File Gateway 2021-04-06 版本：-20210406-opensource.tgz sgw-file-fsx-smb

该产品包括 OpenSSL Project 为在 OpenSSL Toolkit (http://www.openssl.org/) 中使用而开发的软件。对于所有相关第三方工具所涉及的许可证，请参阅以下链接：

- 适用于亚马逊 FSx File Gateway 2021-07-07 版本：第三方许可。
- 适用于 Amazon FSx File Gateway 2021-04-06 版本：第三方许可。

关的限制和配额 Amazon FSx 文件网关

Amazon FSx 文件系统的配额

下表列出了 Amazon FSx 文件系统的最低和最大限制和配额。

资源	每个 Amazon FSx 文件系统的限制
最大标签数	50 个标签
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 个请求
SSD 文件系统的最小存储容量	32 GiB
HDD 文件系统的最小存储容量	2,000 GiB
SSD 和 HDD 文件系统的最大存储容量	64 TiB
最低吞吐能力	8 MBps
最大吞吐能力	2,048 MBps
Amazon FSx 文件共享的最大数量	100000

为网关建议的本地磁盘大小

下表推荐了部署 AWS Storage Gateway 中每个本地磁盘存储的大小。

网关类型	缓存（最小值）	缓存（最大值）	
FSx 文件网关	150 GiB	64 TiB	

> **Note**
>
> 您可以为缓存配置一个或多个本地驱动器，其容量不超过最大容量。

向现有 FSx 文件网关添加缓存时，务必在虚拟主机（虚拟机监控程序或 Amazon EC2 实例）中创建新磁盘。如果先前已将现有磁盘分配为缓存，则不要更改这些磁盘的大小。

Storage Gateway 的 API 参考

除了使用控制台外，您还可以使用 AWS Storage Gateway API 以编程方式配置和管理您的网关。本节介绍 AWS Storage Gateway 操作、身份验证请求签名和错误处理。有关 Storage Gateway 可用的区域和端点的信息，请参阅《AWS 一般参考》中的 AWS Storage Gateway 端点和配额。

> **Note**
>
> 在使用 Storage Gateway 开发应用程序 AWS SDKs 时，也可以使用。 AWS SDKs 适用于 Java、.NET 和 PHP 的封装了底层的 Storage Gateway API，简化了你的编程任务。有关下载开发工具包库的信息，请参阅示例代码库。

主题

- AWS Storage Gateway 必填请求标头
- 对请求进行签名
- 错误响应
- Storage Gateway API 操作

AWS Storage Gateway 必填请求标头

本部分描述您每次向 AWS Storage Gateway发送 POST 请求时必须使用的标头。您将 HTTP 标头包含在内以识别有关请求的密钥信息，包括您希望调用的操作、请求的日期以及表示您拥有请求发送者授权的信息。标头区分大小写，其次序不重要。

以下示例显示了ActivateGateway操作中使用的标头。

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120425/us-east-2/
storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target,
 Signature=9cd5a3584d1d67d57e61f120f35102d6b3649066abdd4bf4bbcf05bd9f2f8fe2
x-amz-date: 20120912T120000Z
x-amz-target: StorageGateway_20120630.ActivateGateway
```

以下是您的 POST 请求中必须包含的标题 AWS Storage Gateway。下面显示的以 “x-amz” 开头的标题是 AWS特定标题。列出的其他所有标头均为 HTTP 事务中使用的普通标头。

标题	说明
`Authorization`	授权标头包含有关请求的几条信息，这些信息 AWS Storage Gateway 允许确定请求是否为请求者的有效操作。该标头的格式如下所示 (为便于阅读，添加了换行符)： `Authorization: AWS4-HMAC_SHA456 Credentials= YourAccessKey /yyymmdd/region/storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature= CalculatedSignature` 在前面的语法中，您可以指定YourAccessKey年、月和日 (yyyymmdd)、区域和。CalculatedSignature授权标头的格式由 AWS V4 签名过程的要求决定。签名的详细信息在主题 对请求进行签名 中进行讨论。
`Content-Type`	`application/x-amz-json-1.1` 用作所有请求的内容类型 AWS Storage Gateway。 `Content-Type: application/x-amz-json-1.1`
`Host`	使用 host 标头指定将请求发送到的 AWS Storage Gateway 终端节点。例如，`storagegateway.us-east-2.amazonaws.com` 是美国东部（俄亥俄州）区域的端点。有关可用终端节点的更多信息 AWS Storage Gateway，请参阅中的AWS Storage Gateway 终端节点和配额AWS 一般参考。 `Host: storagegateway. region.amazonaws.com`
`x-amz-date`	您必须在 HTTP `Date` 标头或 AWS `x-amz-date` 标头中提供时间戳。(部分 HTTP 客户端库文件不允许您设置`Date`标头。) 如果存在`x-amz-date` 标头，则会在请求身份验证期间 AWS Storage Gateway 忽略任

标题	说明
	何Date标头。该x-amz-date 格式必须是 YYYYMMDD'T'HHMMSS'Z' 格式 ISO8601 的基本格式。如果同时使用Date和x-amz-date 标题，则日期标题的格式不必是 ISO8601。 `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
x-amz-target	该标头指定 API 的版本以及您要请求的操作。目标标头值通过结合 API 版本和 API 名称而形成，其格式如下。 `x-amz-target: StorageGateway_ APIversion .operationName` 操作名称值（例如 ActivateGateway “”）可以从 API 列表中找到。Storage Gateway 的 API 参考

对请求进行签名

Storage Gateway 要求通过对请求进行签名，验证所发送的每个请求的身份。您使用加密哈希函数计算数字签名，从而对请求签名。加密哈希是根据输入内容返回唯一哈希值的函数。对哈希函数的输入内容包括您的请求文本和秘密访问密钥。哈希函数返回哈希值，您将该值包含在请求中，作为签名。该签名是您的请求的 Authorization 标头的一部分。

在收到您的请求后，Storage Gateway 将使用您用于对该请求进行签名的同一哈希函数和输入重新计算签名。如果所得签名与该请求中的签名相匹配，则 Storage Gateway 处理该请求。否则，请求将被拒绝。

Storage Gateway 支持使用 AWS 签名版本 4 进行身份验证。计算签名的过程可分为三个任务：

- 任务 1：创建规范请求

  将您的 HTTP 请求重新排列为规范格式。必须使用规范格式，因为 Storage Gateway 在重新计算签名以与您发送的签名进行比较时使用同一规范格式。
- 任务 2：创建待签字符串

创建一个字符串，将该字符串用作您的加密哈希函数输入值中的一项。该字符串称为待签字符串，是哈希算法名称、请求日期、凭证范围字符串以及来自上一任务的规范化请求的结合。凭证范围字符串本身是日期、区域和服务信息的结合。

- 任务 3：创建签名

  使用加密哈希函数为您的请求创建签名，该函数接受两种输入字符串：待签字符串和派生密钥。派生密钥的计算方法是从您的私有访问密钥开始，然后使用凭证范围字符串创建一系列基于哈希的消息身份验证码 () HMACs。

签名计算示例

以下示例引导您了解为ListGateways创建签名的详细信息。该示例可用作核查您的签名计算方法的参考。

示例假定以下各项：

- 请求的时间戳为“Mon, 10 Sep 2012 00:00:00”GMT。
- 端点是美国东部（俄亥俄州）区域。

通用请求语法（包括 JSON 正文）为：

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
x-amz-Date: 20120910T000000Z
Authorization: SignatureToBeCalculated
Content-type: application/x-amz-json-1.1
x-amz-target: StorageGateway_20120630.ListGateways
{}
```

为任务 1：创建规范请求计算的请求规范格式为：

```
POST
/

content-type:application/x-amz-json-1.1
host:storagegateway.us-east-2.amazonaws.com
x-amz-date:20120910T000000Z
x-amz-target:StorageGateway_20120630.ListGateways
```

```
content-type;host;x-amz-date;x-amz-target
44136fa355b3678a1146ad16f7e8649e94fb4fc21fe77e8310c060f61caaff8a
```

规范请求的最后一行是请求正文的哈希值。另外，请注意规范请求的第三行是空的。这是因为此 API（或任何 Storage Gateway APIs）没有查询参数。

任务 2：创建待签字符串 的待签字符串是：

```
AWS4-HMAC-SHA256
20120910T000000Z
20120910/us-east-2/storagegateway/aws4_request
92c0effa6f9224ac752ca179a04cecbede3038b0959666a8160ab452c9e51b3e
```

用来签名的请求的第一行是算法，第二行是时间戳，第三行是证书范围，最后一行是任务 1 中规范请求的哈希值。

对于 任务 3：创建签名，派生密钥可表示为：

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey,"20120910"),"us-
east-2"),"storagegateway"),"aws4_request")
```

如果使用秘密访问密钥 wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY，则计算出的签名为：

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

最终步骤是构造 Authorization 标头。对于示例访问密钥 AKIAIOSFODNN7EXAMPLE，标头（为了便于阅读，添加了换行符）为：

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120910/us-east-2/
storagegateway/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

错误响应

主题

- 异常
- 操作错误代码
- 错误响应

本节提供有关 AWS Storage Gateway 错误的参考信息。这些错误以错误例外和操作错误代码表示。例如，如果请求签名存在问题，那么会由任何 API 响应返回错误例外 `InvalidSignatureException`。但是，`ActivationKeyInvalid`仅返回 ActivateGatewayAPI 的操作错误代码。

根据错误类型的情况，Storage Gateway 可能只返回例外，或者可能同时返回例外和操作错误代码。错误响应 中显示了误差响应示例。

异常

下表列出了 AWS Storage Gateway API 异常。当 AWS Storage Gateway 操作返回错误响应时，响应正文包含其中一个异常。`InternalServerError` 和 `InvalidGatewayRequestException` 返回操作错误代码 (提供特定的操作错误代码的 操作错误代码 消息代码) 之一。

例外	Message	HTTP 状态代码
`IncompleteSignatureException`	指定的签名不完全。	400 错误请求
`InternalFailure`	由于某些未知错误、异常或故障导致请求处理失败。	500 内部服务器错误
`InternalServerError`	一个操作错误代码消息操作错误代码。	500 内部服务器错误
`InvalidAction`	所请求的操作或操作无效。	400 错误请求
`InvalidClientTokenId`	我们的记录中不存在提供的 X.509 证书或 AWS 访问密钥 ID。	403 禁止访问
`InvalidGatewayRequestException`	操作错误代码 中的操作错误代码消息之一。	400 错误请求

例外	Message	HTTP 状态代码
InvalidSignatureException	我们计算出的请求签名与您提供的签名不匹配。检查您的 AWS 访问密钥和签名方法。	400 错误请求
MissingAction	请求中遗漏了一个操作或运行参数。	400 错误请求
MissingAuthenticationToken	请求必须包含有效（已注册的）AWS 访问密钥 ID 或 X.509 证书。	403 禁止访问
RequestExpired	请求超过有效期或请求时间 (或用 15 分钟填补)，或将来发送请求的时间超过 15 分钟。	400 错误请求
SerializationException	序列化期间出现错误。查看您的 JSON 负载结构是否良好。	400 错误请求
ServiceUnavailable	由于服务器发生临时故障而导致请求失败。	503 服务不可用
SubscriptionRequiredException	AWS 访问密钥 ID 需要订阅该服务。	400 错误请求
ThrottlingException	费率已超。	400 错误请求
TooManyRequests	请求过多。	429 请求过多
UnknownOperationException	指定了未知操作。Storage Gateway API 操作 中列出了有效操作。	400 错误请求
UnrecognizedClientException	请求中包含的安全令牌无效。	400 错误请求
ValidationException	输入参数的值不正确或者超出范围。	400 错误请求

操作错误代码

下表显示了 AWS Storage Gateway 操作错误代码和可以返回代码 APIs 的错误代码之间的映射。返回所有操作错误代码，包含异常中所述的两个一般异常（`InternalServerError` 和 `InvalidGatewayRequestException`）之一。

操作错误代码	Message	返回此错误代码的操作
`ActivationKeyExpired`	指定的激活密钥已过期。	ActivateGateway
`ActivationKeyInvalid`	指定的激活密钥无效。	ActivateGateway
`ActivationKeyNotFound`	找不到指定的激活密钥。	ActivateGateway
`BandwidthThrottleScheduleNotFound`	找不到指定的带宽限制。	DeleteBandwidthRateLimit
`CannotExportSnapshot`	无法导出指定的快照。	CreateCachediSCSIVolume CreateStorediSCSIVolume
`InitiatorNotFound`	找不到指定的启动程序。	DeleteChapCredentials
`DiskAlreadyAllocated`	指定的磁盘已分配。	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
`DiskDoesNotExist`	指定的磁盘不存在。	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume

操作错误代码	Message	返回此错误代码的操作
DiskSizeNotGigAligned	指定的磁盘没有以 GB 为整单位。	CreateStorediSCSIVolume
DiskSizeGreaterThanVolumeMaxSize	指定的磁盘大小超过最高卷大小。	CreateStorediSCSIVolume
DiskSizeLessThanVolumeSize	指定的磁盘大小低于最高卷大小。	CreateStorediSCSIVolume
DuplicateCertificateInfo	指定的证书信息是副本。	ActivateGateway
FileSystemAssociationEndpointConfigurationConflict	现有文件系统关联端点配置与指定配置冲突。	AssociateFileSystem
FileSystemAssociationEndpointIpAddressAlreadyInUse	指定的端点 IP 地址已在使用中。	AssociateFileSystem
FileSystemAssociationEndpointIpAddressMissing	文件系统关联端点 IP 地址丢失。	AssociateFileSystem
FileSystemAssociationNotFound	找不到指定的文件系统关联。	UpdateFileSystemAssociation DisassociateFileSystem DescribeFileSystemAssociations
FileSystemNotFound	找不到指定的文件系统。	AssociateFileSystem

操作错误代码	Message	返回此错误代码的操作
GatewayInternalError	出现网关内部错误。	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

操作错误代码	Message	返回此错误代码的操作
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

操作错误代码	Message	返回此错误代码的操作
GatewayNotConnected	没有连接指定的网关。	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

操作错误代码	Message	返回此错误代码的操作
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

操作错误代码	Message	返回此错误代码的操作
GatewayNotFound	找不到指定的网关。	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage

操作错误代码	Message	返回此错误代码的操作
		ListLocalDisks ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

操作错误代码	Message	返回此错误代码的操作
GatewayProxyNetworkConnectionBusy	指定的网关代理网络连接忙。	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

操作错误代码	Message	返回此错误代码的操作
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

操作错误代码	Message	返回此错误代码的操作
InternalError	出现内部错误。	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

操作错误代码	Message	返回此错误代码的操作
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule

操作错误代码	Message	返回此错误代码的操作
InvalidParameters	指定的请求中包含无效参数。	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

操作错误代码	Message	返回此错误代码的操作
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
LocalStorageLimitExceeded	已超过本地存储限制。	AddCache AddUploadBuffer AddWorkingStorage
LunInvalid	指定的 LUN 无效。	CreateStorediSCSIVolume
MaximumVolumeCountExceeded	已超过最大卷计数。	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes

操作错误代码	Message	返回此错误代码的操作
NetworkConfigurationChanged	已更改网关网络配置。	CreateCachediSCSIVolume CreateStorediSCSIVolume

操作错误代码	Message	返回此错误代码的操作
NotSupported	不支持指定的操作。	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

操作错误代码	Message	返回此错误代码的操作
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
OutdatedGateway	指定的网关已过时。	ActivateGateway
SnapshotInProgress Exception	指定的快照在进行中。	DeleteVolume
SnapshotIdInvalid	指定的快照无效。	CreateCachediSCSIVolume CreateStorediSCSIVolume
StagingAreaFull	暂存区域已满。	CreateCachediSCSIVolume CreateStorediSCSIVolume

操作错误代码	Message	返回此错误代码的操作
TargetAlreadyExists	已存在指定的目标。	CreateCachediSCSIVolume CreateStorediSCSIVolume
TargetInvalid	指定的目标无效。	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials UpdateChapCredentials
TargetNotFound	找不到指定的目标。	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials DeleteVolume UpdateChapCredentials

操作错误代码	Message	返回此错误代码的操作
UnsupportedOperationForGatewayType	对于这类网关，指定的操作无效。	AddCache AddWorkingStorage CreateCachediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteSnapshotSchedule DescribeCache DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
VolumeAlreadyExists	已存在指定的卷。	CreateCachediSCSIVolume CreateStorediSCSIVolume
VolumeIdInvalid	指定的卷无效。	DeleteVolume
VolumeInUse	指定的卷已在使用中。	DeleteVolume

操作错误代码	Message	返回此错误代码的操作
VolumeNotFound	找不到指定的卷。	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint DeleteVolume DescribeCachediSCSIVolumes DescribeSnapshotSchedule DescribeStorediSCSIVolumes UpdateSnapshotSchedule
VolumeNotReady	指定的卷没有准备好。	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

错误响应

当存在错误时，响应头信息会包含：

- 内容类型：应用程序/ -1.1 x-amz-json
- 适当的 4xx 或 5xx HTTP 状态码

错误响应的正文会包含有关错误出现的信息。下列错误响应示例显示的是所有错误响应中常见的响应元素的输出语法。

```
{
    "__type": "String",
    "message": "String",
    "error":
        { "errorCode": "String",
          "errorDetails": "String"
        }
```

```
}
```

下表介绍了前一语法中显示的 JSON 错误响应字段。

__type

异常 中的例外之一。

类型：字符串

error

包含特定于 API 的错误详细信息。在常规的 (即不特定于任何 API 的) 错误中，不显示这个误差信息。

类型：集合

errorCode

其中一个操作错误代码。

类型：字符串

errorDetails

此字段不在 API 的当前版本中使用。

类型：字符串

message

一个操作错误代码消息。

类型：字符串

错误响应示例

如果您使用 DescribeStoredi SCSIVolumes API 并指定了不存在的网关 ARN 请求输入，则会返回以下 JSON 正文。

```
{
  "__type": "InvalidGatewayRequestException",
  "message": "The specified volume was not found.",
  "error": {
```

```
    "errorCode": "VolumeNotFound"
  }
}
```

如果 Storage Gateway 计算的签名不符合通过请求发送的签名，那么会返回如下 JSON 正文。

```
{
  "__type": "InvalidSignatureException",
  "message": "The request signature we calculated does not match the signature you
 provided."
}
```

Storage Gateway API 操作

有关 Storage Gateway 操作的列表，请参阅《AWS Storage Gateway API 参考》中的操作。

Amazon FSx 文件网关用户指南的文档历史记录

下表说明了在 2018 年 4 月后每次发布本用户指南时进行的重要更改。要获得本文档的更新通知，您可以订阅 RSS 源。

变更	说明	日期
FSx 文件网关可用性变更通知	Amazon FSx 文件网关不再向新客户开放。FSx File Gateway 的现有客户可以继续正常使用该服务。有关与FSx 文件网关类似的功能，请访问此博客文章。	2024 年 10 月 28 日
FSx 文件网关可用性变更通知	AWS Storage Gateway从 24 年 10 月 28 日起，新客户将不再使用的 FSx File Gateway。要使用该服务，必须在该日期之前注册。 FSx File Gateway 的现有客户可以继续正常使用该服务。有关与 FSx 文件网关类似的功能，请访问此博客文章。	2024 年 9 月 26 日
添加了开启或关闭维护更新的选项	Storage Gateway 会定期收到维护更新，其中可能包括操作系统和软件升级、用于解决稳定性、性能和安全性的修复程序以及对新功能的访问。现在，可以配置一项设置，来为部署中的每个单独网关开启或关闭这些更新。有关更多信息，请参阅使用控制台管理网关更新。 AWS Storage Gateway	2024 年 6 月 6 日

更新了推荐的 CloudWatch 警报	该 CloudWatch `HealthNotifications` 警报现在适用于所有网关类型和主机平台，并建议该警报适用于所有网关类型和主机平台。`HealthNotifications` 和 `AvailabilityNotifications` 的建议配置设置也已更新。有关更多信息，请参阅了解 CloudWatch警报。	2023 年 10 月 2 日
添加了 GatewayClockOutOfSync 疑难解答提示	“疑难解答：文件网关问题” 部分现在包含疑难解答指南，可帮助诊断网关系统时钟与 AWS Storage Gateway 服务器时间不同步时可能遇到的问题。有关更多信息，请参阅错误：GatewayClockOutOfSync。	2022 年 10 月 19 日
新增了 Active Directory 加入域故障排除提示	故障排除：文件网关问题部分现在包含故障排除指南，以帮助诊断您在尝试将网关加入到 Active Directory 域时可能遇到的问题。有关更多信息，请参阅故障排除：Active Directory 域问题。	2022 年 10 月 19 日
更新了网关创建程序	创建新网关的程序已更新，以反映 Storage Gateway 控制台中的更改。有关更多信息，请参阅创建并激活 Amazon S3 文件网关。	2021 年 10 月 12 日

多文件系统支持	Amazon FSx File Gateway 现在最多支持五个连接 FSx 的 Amazon 文件系统。有关更多信息，请参阅附加 Amazon f FSx or Windows 文件服务器文件系统。	2021 年 7 月 7 日
亚马逊 FSx 软存储配额支持	Amazon FSx File Gateway 现在支持在向配置了存储配额的连接的 Amazon FSx 文件系统写入数据时软存储配额（当用户超过其数据限制时会向您发出警告）。不支持硬配额（通过拒绝写入权限来强制执行数据限制）。软配额适用于除亚马逊 FSx管理员用户之外的所有用户。有关设置存储配额的更多信息，请参阅《Amazon FSx for Windows 文件服务器用户指南》中的存储配额。	2021 年 7 月 7 日
新指南	除了最初的文件网关（现在称为 Amazon S3 文件网关）之外，Storage Gateway 还提供亚马逊 FSx 文件网关（FSx 文件网关）。 FSx File Gateway 提供低延迟和从本地设施高效访问云端 FSx 的 Windows 文件服务器文件共享。有关更多信息，请参阅什么是 Amazon FSx 文件网关？	2021 年 4 月 27 日
FedRAMP 合规性	Storage Gateway 现已符合 FedRAMP 标准。有关更多信息，请参阅 Storage Gateway 的合规性验证。	2020 年 11 月 24 日

文件网关迁移	文件网关现在为使用新文件网关替换现有文件网关提供了一个记录在案的流程。有关更多信息，请参阅使用新文件网关替换文件网关。	2020 年 10 月 30 日
文件网关冷缓存读取性能提高 4 倍	Storage Gateway 将冷缓存读取性能提高 4 倍。有关更多信息，请参阅文件网关的性能指导。	2020 年 8 月 31 日
通过控制台订购硬件设备	现在，您可以通过 AWS Storage Gateway 控制台订购硬件设备。有关更多信息，请参阅使用 AWS Storage Gateway 硬件设备。	2020 年 8 月 12 日
支持新 AWS 区域的联邦信息处理标准 (FIPS) 终端节点	现在您可以在美国东部（俄亥俄州）、美国东部（弗吉尼亚州北部）、美国西部（北加利福尼亚）、美国西部（俄勒冈州）和加拿大（中部）区域通过 FIPS 端点激活网关。有关更多信息，请参阅《AWS 一般参考》中的 AWS Storage Gateway 端点和配额。	2020 年 7 月 31 日
文件网关本地缓存存储增加 4 倍	Storage Gateway 现在为文件网关支持高达 64 TB 的本地缓存，通过提供对更大工作数据集的低延迟访问来提高本地应用程序的性能。有关更多信息，请参阅《Storage Gateway 用户指南》中的为网关推荐的本地磁盘大小。	2020 年 7 月 7 日

在 Storage Gateway 控制台中查看亚马逊 CloudWatch 警报	现在，您可以在 Storage Gateway 控制台中查看 CloudWatch 警报。有关更多信息，请参阅了解 CloudWatch 警报。	2020 年 5 月 29 日
支持美国联邦信息处理标准 (FIPS) 端点	现在，您可以在 AWS GovCloud (US) 区域中通过 FIPS 终端节点激活网关。要为文件网关选择 FIPS 端点，请参阅选择服务端点。	2020 年 5 月 22 日
新 AWS 区域	Storage Gateway 现已在非洲（开普敦）和欧洲（米兰）区域推出。有关更多信息，请参阅《AWS 一般参考》中的 AWS Storage Gateway 端点和配额。	2020 年 5 月 7 日
支持 S3 Intelligent-Tiering 存储类	Storage Gateway 现在支持 S3 Intelligent-Tiering 存储类。S3 智能分层存储类可以通过自动将数据移至最具成本效益的存储访问层来优化存储成本，而不会影响性能或产生运营开销。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的可自动优化经常访问和不常访问对象的存储类。	2020 年 4 月 30 日
新 AWS 区域	Storage Gateway 现已在 AWS GovCloud（美国东部）地区推出。有关更多信息，请参阅《AWS 一般参考》中的 AWS Storage Gateway 端点和配额。	2020 年 3 月 12 日

支持基于 Linux 内核的虚拟机 (KVM) 管理程序	Storage Gateway 现在可将本地网关部署在 KVM 虚拟化平台上。KVM 上部署的网关与现有本地网关具有相同的功能和功能。有关更多信息，请参阅《Storage Gateway 用户指南》中的支持的虚拟机管理程序和主机要求。	2020 年 2 月 4 日
支持 VMware vSphere 高可用性	Storage Gateway 现在支持高可用性 VMware ，以帮助保护存储工作负载免受硬件、虚拟机管理程序或网络故障的影响。有关更多信息，请参阅《Storage G ateway 用户指南》中的 “将 VMware vSphere 高可用性与存储网关配合使用”。此版本还包含性能改进。有关更多信息，请参阅《Storage Gateway 用户指南》中的性能。	2019 年 11 月 20 日
支持 Amazon CloudWatch 日志	现在，您可以使用 Amazon CloudWatch 日志组配置文件网关，以获得有关错误以及网关及其资源的运行状况的通知。有关更多信息，请参阅 Storage Gateway 用户指南中的获取有关网关运行状况和亚马逊 CloudWatch 日志组错误的通知。	2019 年 9 月 4 日
New AWS 区域	Storage Gateway 现已在亚太地区（香港）区域推出。有关更多信息，请参阅《AWS 一般参考》中的 AWS Storage Gateway 端点和配额。	2019 年 8 月 14 日

New AWS 区域	Storage Gateway 现已在中东（巴林）区域推出。有关更多信息，请参阅《AWS 一般参考》中的 AWS Storage Gateway 端点和配额。	2019 年 7 月 29 日
支持在 Virtual Private Cloud (VPC) 中激活网关	现在，您可以在 VPC 中激活网关。您可以在本地软件设备和基于云的存储基础设施之间创建私有连接。有关更多信息，请参阅在 Virtual Private Cloud 中激活网关。	2019 年 6 月 20 日
文件网关支持基于标签的授权	文件网关现在支持基于标签的授权。您可以根据文件网关资源上的标签控制对这些资源的访问。您还可以根据可在 IAM 请求条件中传递的标签控制访问。有关更多信息，请参阅控制对文件网关资源的访问。	2019 年 3 月 4 日
AWS Storage Gateway 硬件设备在欧洲上市	AWS Storage Gateway 硬件设备现已在欧洲上市。有关更多信息，请参阅《AWS 一般参考》中的 AWS Storage Gateway 硬件设备区域。此外，您现在可以将 Storage Gateway Hardware Appliance 上的可用 AWS 存储空间从 5 TB 增加到 12 TB，并用 10 千兆位光纤网卡替换已安装的铜质网卡。有关更多信息，请参阅设置您的硬件设备。	2019 年 2 月 25 日

支持 AWS Storage Gateway 硬件设备	AWS Storage Gateway 硬件设备包括预安装在第三方服务器上的存储网关软件。您可以从 AWS 管理控制台管理设备。该设备可以承载文件、磁带和卷网关。有关更多信息，请参阅使用 Storage Gateway 硬件设备。	2018 年 9 月 18 日

早期更新

下表描述了 2018 年 5 月之前的每个 AWS Storage Gateway 用户指南发行版中的重要更改。

更改	描述	更改日期
全新 AWS 区域	磁带网关现已在亚太地区（新加坡）区域推出。有关详细信息，请参阅 AWS 区域 支持 Storage Gateway。	2018 年 4 月 3 日
全新 AWS 区域	Storage Gateway 现已在欧洲（巴黎）区域推出。有关详细信息，请参阅 AWS 区域 支持 Storage Gateway。	2017 年 12 月 18 日
支持 VMware ESXi Hypervisor 版本 6.5	AWS Storage Gateway 现在支持 VMware ESXi 虚拟机管理程序版本 6.5。这是对版本 4.1、5.0、5.1、5.5 和 6.0 支持提供的补充。有关更多信息，请参阅 受支持的管理程序和主机要求。	2017 年 9 月 13 日
文件网关支持 Microsoft Hyper-V 管理程序	现在您可以在 Microsoft Hyper-V 管理程序上部署文件网关。有关信息，请参阅受支持的管理程序和主机要求。	2017 年 6 月 22 日
全新 AWS 区域	Storage Gateway 现已在亚太地区（孟买）区域推出。有关详细信息，请参阅 AWS 区域 支持 Storage Gateway。	2017 年 5 月 02 日
支持 Amazon EC2 上的文件网关	AWS Storage Gateway 现在提供了在 Amazon EC2 中部署文件网关的功能。您可以使用现在以社区 AMI 形式存在的 Storage Gateway Amazon 系统映像 (AMI) 在	2017 年 2 月 8 日

更改	描述	更改日期
	Amazon EC2 中启动文件网关。有关如何创建文件网关并将其部署到 EC2 实例的信息，请参阅创建并激活 Amazon FSx 文件网关。有关如何启动文件网关 AMI 的信息，请参阅 为 FSx 文件网关部署默认 Amazon EC2 主机。 此外，文件网关现在支持 HTTP 代理配置。有关更多信息，请参阅 通过 HTTP 代理路由在 Amazon EC2 上部署的网关。	
全新 AWS 区域	Storage Gateway 现已在欧洲地区（伦敦）区域推出。有关详细信息，请参阅 AWS 区域 支持 Storage Gateway。	2016 年 12 月 13 日
全新 AWS 区域	Storage Gateway 现已在加拿大（中部）区域推出。有关详细信息，请参阅 AWS 区域 支持 Storage Gateway。	2016 年 12 月 8 日
支持文件网关	除了卷网关和磁带网关外，Storage Gateway 现在还提供文件网关。文件网关将服务和虚拟软件设备组合在一起，使您能够使用行业标准文件协议（例如，网络文件系统 (NFS)）在 Amazon S3 中存储和检索对象。利用网关，可以将 Amazon S3 中的对象作为 NFS 装载点上的文件进行访问。	2016 年 11 月 29 日