aws

用户指南

AWSStorage Gateway

API 版本 2013-06-30

AWSStorage Gateway: 用户指南

Table of Contents

什么是 Amazon S3 文件网关

AWSStorage Gateway 将本地软件设备与基于云的存储相连接，从而在本地 IT 环境与AWS存储基础设施。您可以使用该服务将数据存储在AWS云提供可扩展且经济高效的存储来帮助保持数据安全性AWS Storage Gateway 提供了基于文件、基于卷和基于磁带的存储解决方案

主题

Amazon S3 文件网关

Amazon S3 文件网关— Amazon S3 文件网关支持文件接口Amazon Simple Storage Service (Amazon S3)并将服务和虚拟软件设备组合在一起。通过使用此组合，可以使用行业标准文件协议（如网络文件系统 (NFS)）和服务器消息块 (SMB) 在 Amazon S3 中存储和检索对象。软件设备（或网关）作为在 VMware ESXi 或 Microsoft Hyper-V 或基于 Linux 内核的虚拟机 (KVM) 管理程序上运行的虚拟机 (VM) 部署到您的本地环境中。利用网关，可以将 S3 中的对象作为文件或文件共享挂载点进行访问。利用 S3 文件网关，可以执行以下操作：

- 您可以直接使用 NFS 版本 3 或 4.1 协议存储和检索文件。
- 您可以直接使用 SMB 文件系统版本 2 和 3 协议存储和检索文件。
- 您可以从任意直接访问 Amazon S3 中的数据。AWS云应用程序或服务。
- 您可以使用生命周期策略、跨区域复制和版本控制管理 S3 数据。您可以将 S3 文件网关视为 Amazon S3 上的文件系统挂载。

S3 文件网关简化了 Amazon S3 的文件存储，通过行业标准文件系统协议集成到现有应用程序中，并提供了对本地存储的经济高效的替代方法。它还通过透明本地缓存提供对数据的低延迟访问。S3 文件网关管理往返的数据传输AWS、缓冲应用程序避免网络拥堵，并行优化和流式处理数据，以及管理带宽消耗。S3 文件网关与AWS服务，例如以下服务：

- 使用 AWS Identity and Access Management (IAM) 的常见访问管理
- 使用 AWS Key Management Service (AWS KMS) 的加密
- 使用 Amazon CloudWatch (CloudWatch) 进行监控
- 使用审核AWS CloudTrail(CloudTrail)
- 使用 AWS Management Console和 AWS Command Line Interface (AWS CLI) 的操作

- 账单和成本管理

在以下文档中，您可以找到包含对所有网关通用的设置信息的“入门”部分，还可以找到一些特定于网关的设置部分。“入门”部分介绍了如何为网关部署、激活和配置存储。“管理”部分介绍了您可以如何管理网关和资源：

- 提供有关如何创建和使用 S3 文件网关的说明。其中演示了如何创建文件共享、将驱动器映射到 Amazon S3 存储桶以及将文件和文件夹上传到 Amazon S3。

- 介绍如何为所有网关类型和资源执行管理任务。

在本指南中，您主要可以找到如何使用 AWS Management Console执行网关操作。如果要以编程方式执行这些操作，请参阅AWSStorage Gateway API 参考.

Storage Gateway 的工作原理（架构）

在下面，您可以找到可用的 Storage Gateway 解决方案的架构概述。

主题

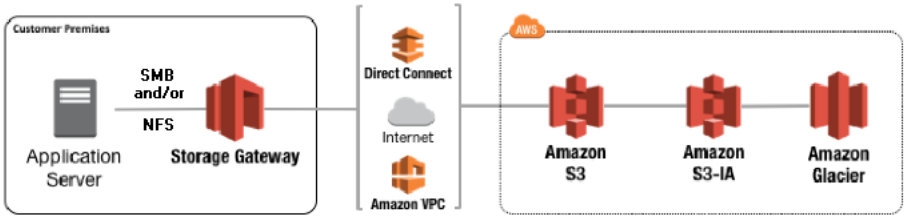
Amazon S3 文件网关

要使用 S3 文件网关，请首先下载网关的 VM 映像。然后，您可以从AWS Management Console或者通过 Storage Gateway API。您还可以使用 Amazon EC2 映像创建 S3 文件网关。

激活 S3 文件网关后，您可创建和配置文件共享并将该共享与 Amazon Simple Storage Service (Amazon S3) 存储桶关联。这样，客户端可使用网络文件系统 (NFS) 或服务器消息块 (SMB) 协议访问共享。写入到文件共享的文件将成为 Amazon S3 中的对象，使用路径作为密钥。文件与对象之间存在一对一的映射，在您更改文件时，网关会异步更新 Amazon S3 中的对象。Amazon S3 存储桶中的现有对象显示为文件系统中的文件，而键成为路径。使用 Amazon S3 服务器端加密密钥 (SSE-S3) 对象进行了加密。所有数据传输都是通过 HTTPS 完成的。

该服务优化了网关之间的数据传输AWS使用分段并行上传或字节范围下载，以更好地使用可用带宽。系统维护本地缓存以提供对最近访问数据的低延迟访问，并减少数据传出成本。CloudWatch 指标提供对 VM 上资源使用情况以及与之间的数据传输的深入见解。AWS. CloudTrail 跟踪所有 API 调用。

利用 S3 File Gateway 存储，您可以执行多个任务，例如将云工作负载注入 Amazon S3、执行备份和存档以及将存储数据迁移到AWS。下图概述了 Storage Gateway 的文件存储部署。



在将文件上传到 Amazon S3 时，S3 文件网关将文件转换为 S3 对象。对 S3 File Gateway 上的文件共享执行的文件操作与 S3 对象之间的交互需要在文件和对象之间进行转换时仔细考虑某些操作。

常见文件操作会更改文件元数据，从而导致删除当前 S3 对象并创建一个新的 S3 对象。下表显示了示例文件操作以及对 S3 对象的影响。

文件操作	S3 对象影响	存储类的含义
重命名文件	替换现有 S3 对象并为每个文件创建一个新的 S3 对象	可能会收取提前删除费和检索费
重命名文件	替换所有现有 S3 对象，并为文件夹结构中的每个文件夹和文件创建新的 S3 对象	可能会收取提前删除费和检索费
更改文件/文件夹权限	替换现有 S3 对象并为每个文件或文件夹创建一个新的 S3 对象	可能会收取提前删除费和检索费
更改文件/文件夹所有权	替换现有 S3 对象并为每个文件或文件夹创建一个新的 S3 对象	可能会收取提前删除费和检索费
追加到文件	替换现有 S3 对象并为每个文件创建一个新的 S3 对象	可能会收取提前删除费和检索费

当 NFS 或 SMB 客户端将文件写入 S3 文件网关时，文件网关会将文件的数据上传到 Amazon S3，然后是其元数据（所有权、时间戳等）。上传文件数据将创建 S3 对象，而上传文件的元数据将更新 S3 对象的元数据。此过程将创建对象的另一个版本，从而生成对象的两个版本。如果启用 S3 版本控制，将存储两个版本。

如果文件上传到 Amazon S3 后，NFS 或 SMB 客户端在 S3 文件网关中进行修改时，S3 文件网关会上传新的或修改的数据，而不是上传整个文件。修改文件会导致创建 S3 对象的新版本。

S3 文件网关上传较大的文件时，可能需要在客户端完成写入 S3 文件网关之前上传较小的文件块。造成这种情况的一些原因包括释放缓存空间或高写入文件共享的速率。这可能会导致 S3 存储桶中的对象的多个版本。

在设置生命周期策略将对象移动到不同的存储类之前，您应监控 S3 存储桶以确定存在多少版本的对象。您应该为之前的版本配置生命周期过期，以尽量减少 S3 存储桶中对象的版本数。在 S3 存储桶之间使用同区复制 (SRR) 或跨区域复制 (CRR) 将增加使用的存储空间。

为 Amazon S3 文件网关设置

本节提供有关 Amazon S3 文件网关入门的说明。要开始使用，请首先注册AWS. 如果您是新用户，我们建议您阅读区域和要求部分。

主题

注册 Amazon Web Services

如果您还没有 AWS 账户，请完成以下步骤创建一个。

注册 AWS 账户

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

   在注册时，您将接到一通电话，要求您使用电话键盘输入一个验证码。

创建 IAM 用户

在创建您的AWS请按照以下步骤创建AWS Identity and Access Management(IAM) 用户自己。然后，您将该用户添加到具有管理权限的组中。

自行创建管理员用户并将该用户添加到管理员组 (控制台)

1. 选择根用户并输入您的 AWS 账户 电子邮件地址，以账户拥有者身份登录 IAM 控制台。在下一页上，输入您的密码。

> **Note**
>
> 强烈建议您遵守以下使用 **Administrator** IAM 用户的最佳实践，妥善保存根用户凭证。只在执行少数账户和服务管理任务时才作为根用户登录。

2. 在导航窗格中，选择用户，然后选择添加用户。
3. 对于用户名，输入 **Administrator**。
4. 选中 AWS Management Console 访问旁边的复选框。然后选择自定义密码，并在文本框中输入新密码。
5. （可选）默认情况下，AWS要求新用户在首次登录时创建新密码。您可以清除用户必须在下次登录时创建新密码旁边的复选框以允许新用户在登录后重置其密码。
6. 选择 Next:。Permissions (下一步：权限)。
7. 在设置权限下，选择将用户添加到组。
8. 选择创建组。
9. 在创建组对话框中，对于组名称，输入 **Administrators**。
10. 选择筛选策略，然后选择 AWS 托管的工作职能以筛选表内容。
11. 在策略列表中，选中 AdministratorAccess 的复选框。然后选择创建组。

> **Note**
>
> 您必须先激活 IAM 用户和角色对账单的访问权限，然后才能使用 AdministratorAccess 权限访问 AWS Billing and Cost Management 控制台。为此，请按照“向账单控制台委派访问权限”教程第 1 步中的说明进行操作。

12. 返回到组列表中，选中您的新组所对应的复选框。如有必要，选择刷新以在列表中查看该组。
13. 选择 Next:。标签。
14. (可选) 通过以键值对的形式附加标签来向用户添加元数据。有关在 IAM 中使用标签的更多信息，请参阅 IAM 用户指南中的标记 IAM 实体。
15. 选择 Next:。审核以查看要添加到新用户的组成员资格的列表。如果您已准备好继续，请选择创建用户。

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

文件网关设置要求

除非另有说明，否则以下要求对于中的所有文件网关类型都需要：AWS Storage Gateway. 您的设置必须符合本节中的要求。在部署网关之前，请查看适用于网关设置的要求。

主题

必备条件

在使用 Amazon FSx 文件网关（FSx 文件网关）之前，您必须满足以下要求：

- 创建和配置 FSx for Windows File Server 文件系统。有关说明，请参阅第 1 步：创建您的文件系统中的Windows File Server 版 Amazon FSx for Windows File Server 用户指南.
- 配置 Microsoft Active Directory (AD)。
- 确保网关和之间有足够的网络带宽AWS. 成功下载、激活和更新网关至少需要 100 Mbps。
- 配置私人网络、VPN 或AWS Direct Connect在您的 Amazon 虚拟私有云 (Amazon VPC) 和您部署 FSx 文件网关的本地环境之间。
- 确保网关可以解析 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，或者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

以下部分提供有关网关所需的最小硬件和设置以及为所需存储分配的最小磁盘空间量的信息。

有关文件网关性能的最佳实践的信息，请参阅文件网关的性能指南。

本地 VM 的硬件要求

在本地部署网关时，请确保部署网关虚拟机 (VM) 的基础硬件可以专门使用以下最少资源：

- 为虚拟机分配四个虚拟处理器
- 用于文件网关的 16 GiB 预留 RAM
- 80GiB 磁盘空间，适用于安装虚拟机映像和系统数据

有关更多信息，请参阅优化网关性能。有关硬件如何影响网关 VM 的性能的信息，请参阅 文件共享的配额。

Amazon EC2 实例类型要求

在 Amazon Elastic Compute Cloud (Amazon EC2) 上部署网关时，实例大小必须至少为**xlarge**让你的网关正常运行。但是，对于计算优化型实例系列，大小必须至少为**2xlarge**. 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

- 通用型实例系列-m4 或 m5 实例类型。
- 计算优化型实例系列-c4 或 c5 实例类型。选择 2xlarge 实例大小或更大的大小，以满足所需的 RAM 要求。
- 内存优化型实例系列-r3 实例类型。
- 存储优化型实例系列-i3 实例类型。

> **Note**
>
> 在您在 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，请参阅实例存储中的Amazon EC2 用户指南。
> 应用程序写入会同步存储在缓存中，然后以异步方式上传到 Amazon S3 中的持久性存储中。如果由于在上传完成之前实例停止而导致短暂存储丢失，则数据仍位于缓存中并且尚未写入可能会丢失的 Amazon S3 (Amazon S3) 中。在停止托管网关的实例之前，请确保`CachePercentDirty`CloudWatch 指标为`0`. 有关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。有关监控存储网关的指标的信息，请参阅监控文件网关.
> 如果您的 S3 存储桶中有超过 500 万个对象，并且您使用的是通用型固态硬盘卷，则在启动期间，您的网关必须具有 350 GiB 的最小根 EBS 卷，才能实现可接受的性能。有关如何增加卷大小的信息，请参阅使用弹性卷修改 EBS 卷（控制台）.

存储需求

除了 VM 的 80 GiB 磁盘空间外，您还需要为网关提供其他磁盘。

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，最大容量不超过最大容量。
> 在向现有网关添加缓存时，在主机 (管理程序或 Amazon EC2 实例) 中创建新磁盘至关重要。
> 如果之前已将磁盘分配为缓存，请勿更改现有磁盘的大小。

有关网关配额的信息，请参阅文件共享的配额。

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。数据传输模式将决定支持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 FSx File Gateway 或者将其他类型的部署（包括本地部署）与限制的网络安全策略结合使用。AWSIP 地址范围。在这些情况下，您的网关时可能在AWSIP 范围值发生变化。这些区域有：AWS您需要使用的 IP 地址范围值位于 Amazon 服务子集中，适用于AWS您在其中激活网关的地区。有关当前 IP 范围值，请参阅AWSIP 地址范围中的AWS一般参考.

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

Storage Gateway 要求允许特定端口来执行其操作。下图显示了您必须允许每种类型的网关使用的必需端口。一些端口是所有网关类型必需的，另一些端口是特定网关类型必需的。有关端口要求的更多信息，请参阅端口要求。

所有网关类型的通用端口

下列端口是所有网关类型的通用端口，是所有网关类型所需要的。

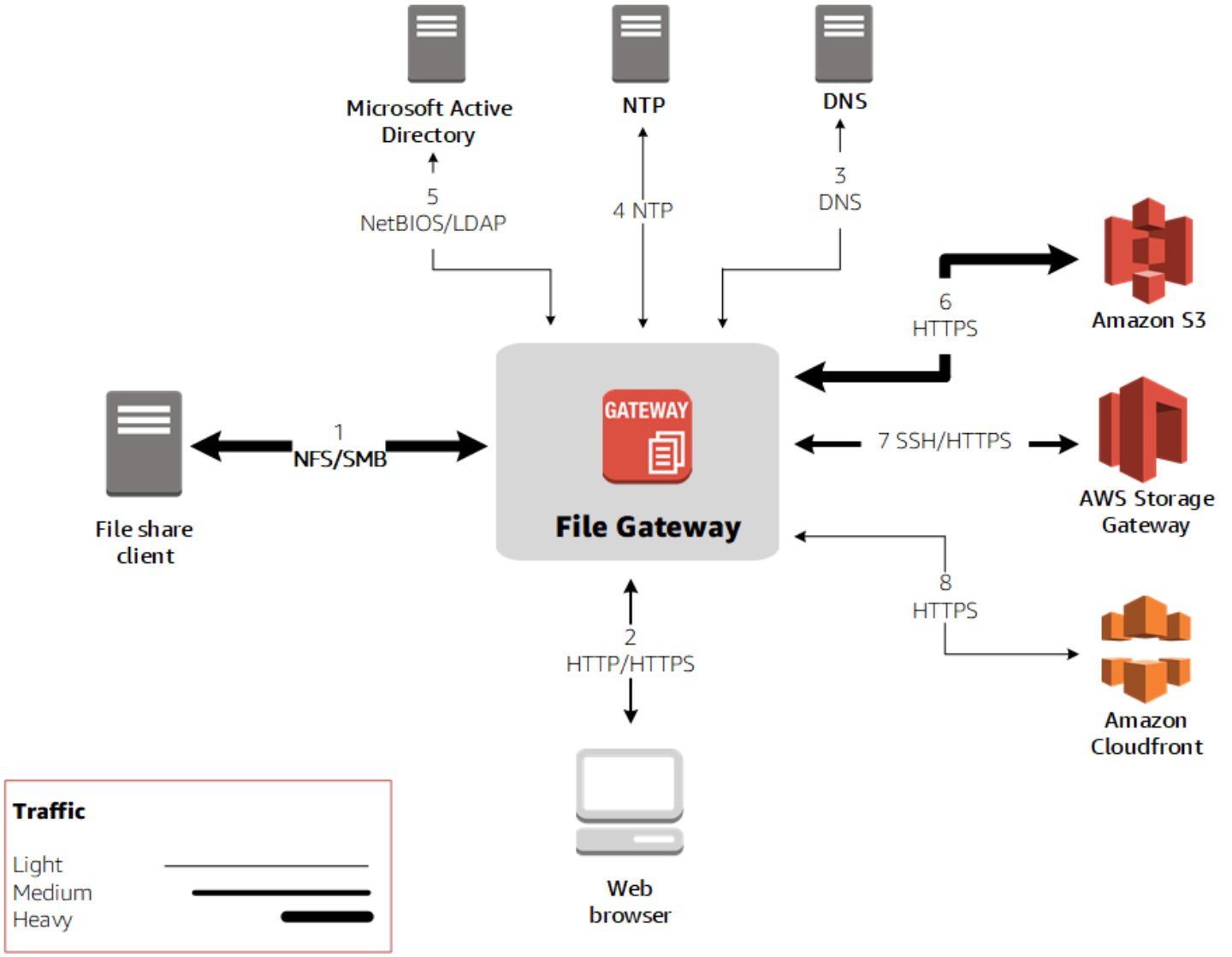
协议	端口	Direction	源	目标	如何使用
TCP	443 (HTTPS)	出站	Storage Gateway	AWS	用于从 Storage Gateway 到AWS服务终端节点。有关服务终端节点的信息，请参阅允许通过防火墙和路由器进行 AWS Storage Gateway 访问。
TCP	80 (HTTP)	入站	您从中连接到的主机AWS Management Console.	Storage Gateway	由本地系统用于获取 Storage Gateway 激活密钥。仅在

协议	端口	Direction	源	目标	如何使用
					激活 Storage Gateway 设备期间使用端口 80。 Storage Gateway 不要求可公开访问端口 80。所需的端口 80 访问级别取决于网络配置。如果从 Storage Gateway 控制台激活网关，则从中连接到控制台的主机必须有权访问网关的端口 80。
UDP/UDP	53 (DNS)	出站	Storage Gateway	DNS 服务器	适用于 Storage Gateway 和 DNS 服务器之间的通信。

协议	端口	Direction	源	目标	如何使用
TCP	22 (支持渠道)	出站	Storage Gateway	AWS Support	允许AWS Support访问网关以帮助您排查网关问题。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。
UDP	123 (NTP)	出站	NTP 客户端	NTP 服务器	由本地系统使用以将 VM 时间同步到主机时间。

文件网关的端口

下图显示了要为 S3 File Gateway 开放的端口。



> **Note**
>
> 有关特定端口要求，请参阅端口要求.

对于 S3 文件网关，您只需在希望允许域用户访问服务器消息块 (SMB) 文件共享时使用 Microsoft Active Directory。您可以将文件网关加入到任何有效的 Microsoft Windows 域（可由 DNS 解析）。

您也可以使用AWS Directory Service创建AWS Managed Microsoft AD在 Amazon Web Services 云中。对于大多数AWS Managed Microsoft AD部署时，您需要为 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，请参阅创建 DHCP 选项集中的AWS Directory Service管理指南.

Amazon S3 文件网关除了通用端口外，还需要以下端口。

协议	端口	Direction	源	目标	如何使用
TCP/UDP	2049 (NFS)	入站	NFS 客户端	Storage Gateway	您的网关会面向连接到 NFS 共享的本地系统公布。
TCP/UDP	111 (NFSv3)	入站	NFSv3 客户端	Storage Gateway	您的网关会面向连接到端口映射器的本地系统公布。 **Note** 此端口仅适用于 NFSv3。
TCP/UDP	20048 (NFSv3)	入站	NFSv3 客户端	Storage Gateway	您的网关会面向连接到您的网关公布的挂载的本地系统公布。 **Note** 此端口仅适用于 NFSv3。

Storage Gateway 硬件设备的网络和防火墙要求

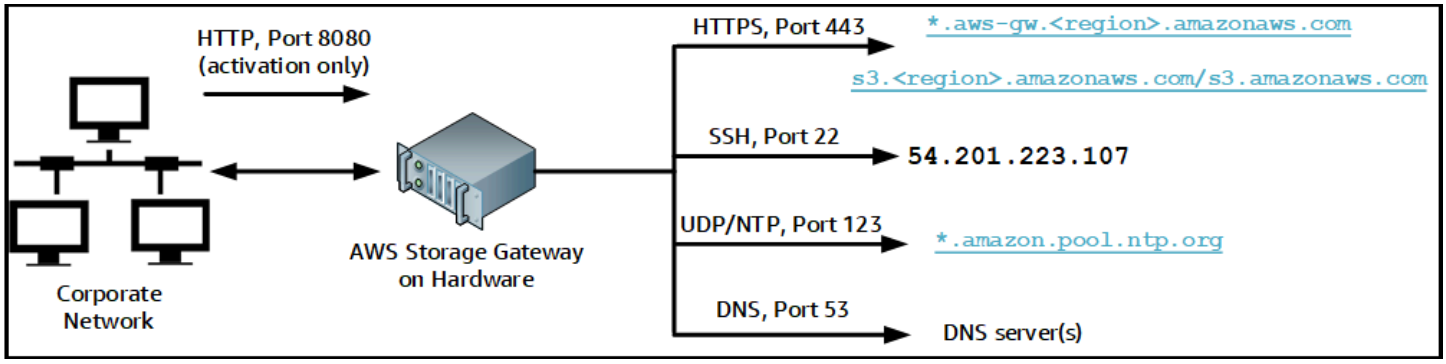
每个 Storage Gateway 硬件设备都需要以下网络服务：

- Internet 访问— 通过服务器上的任何网络接口与 Internet 的永久性网络连接。
- DNS 服务— DNS 服务，适用于硬件设备和 DNS 服务器之间的通信。
- 时间同步— 必须可访问自动配置的 Amazon NTP 时间服务。
- IP 地址— 已分配的 DHCP 或静态 IPv4 地址。您无法分配 IPv6 地址。

Dell PowerEdge R640 服务器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	Direction	源	目标	如何使用
SSH	22	出站	硬件设备	54.201.223.107	支持渠道

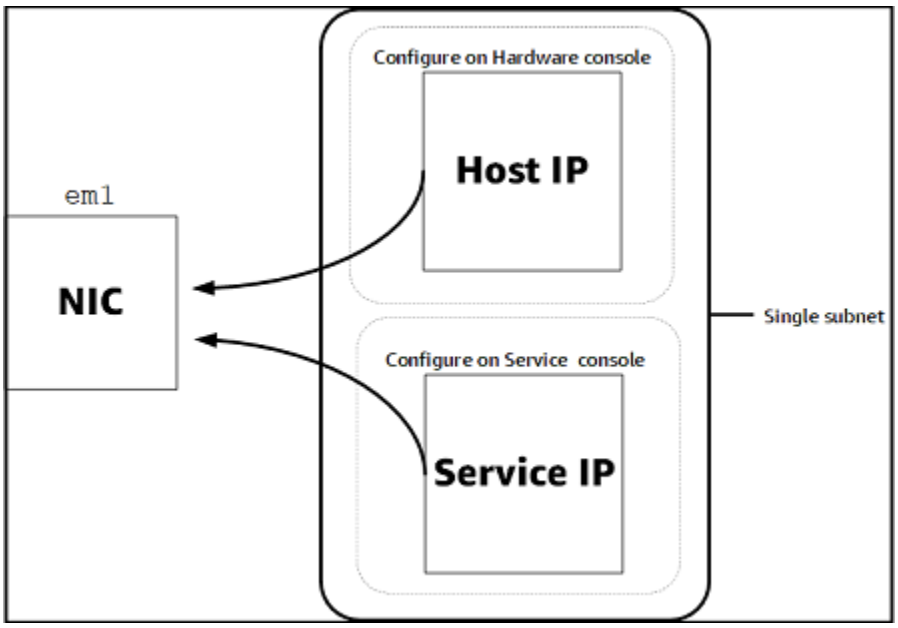
协议	端口	Direction	源	目标	如何使用
DNS	53	出站	硬件设备	DNS 服务器	名称解析
UDP/NTP	123	出站	硬件设备	`*.amazon.pool.ntp.org`	时间同步
HTTPS	443	出站	硬件设备	`*.amazonaws.com`	数据传输
HTTP	8080	入站	AWS	硬件设备	激活（仅短时）

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终端节点的出站访问权限。
- 配置至少一个网络接口以支持硬件设备。有关更多信息，请参阅配置网络参数。

> **Note**
>
> 有关显示服务器背面及其端口的图示，请参阅机架安装硬件设备并将其连接到电源.

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 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服务终端节点，以便与之通信：AWS. 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终端节点进行出站通信AWS.

> **Important**
>
> 取决于你的网关AWS地区，替换*##*在服务终端节点中使用正确的区域字符串。

所有网关都需要使用以下服务终端节点，才能实现头存储桶操作。

```
s3.amazonaws.com:443
```

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

```
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终端节点。

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

以下示例是美国西部（俄勒冈）区域 (us-west-2)。

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

下面显示的 Amazon S3 服务终端节点仅适用于文件网关。文件网关需要此终端节点才能访问文件共享映射到的 Amazon S3 存储桶。

```
s3.region.amazonaws.com
```

以下示例是美国东部（俄亥俄）区域的 Amazon S3 服务终端节点（us-east-2)。

```
s3.us-east-2.amazonaws.com
```

> **Note**
>
> 如果你的网关无法确定AWS您的 S3 存储桶所在的区域，此服务终端节点将默认为s3.us-east-1.amazonaws.com. 我们建议您允许访问美国东部（弗吉尼亚北部）区域 (us-east-1) 以及在其中激活网关的区域和 S3 存储桶所在的区域。

以下是适用于的 Amazon S3 服务终端节点AWS GovCloud (US)地区。

```
s3-fips-us-gov-west-1.amazonaws.com (AWS GovCloud (US-West) Region (FIPS))
s3-fips.us-gov-east-1.amazonaws.com (AWS GovCloud (US-East) Region (FIPS))
s3.us-gov-west-1.amazonaws.com (AWS GovCloud (US-West) Region (Standard))
s3.us-gov-east-1.amazonaws.com (AWS GovCloud (US-East) Region (Standard))
```

以下示例是中 S3 存储桶的 FIPS 服务终端节点。AWSGovCloud（美国西部）地区。

```
bucket-name.s3-fips-us-gov-west-1.amazonaws.com
```

Storage Gateway 获取可用列表时需要使用以下 Amazon CloudFront 终端节点。AWS地区。

```
https://d4kdq0yaxexbo.cloudfront.net/
```

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
```

- 存储网关 — 对于支持AWS地区和列表AWS可以与 Storage Gateway 一起使用的服务终端节点，请参阅AWS Storage Gateway终端节点和配额中的AWS一般参考.
- Storage Gateway 硬件设备-适用于受支持AWS可以用于硬件设备的区域，请参阅Storage Gateway 硬件设备区域中的AWS一般参考.

配置 Amazon EC2 网关实例的安全组

InAWS Storage Gateway，安全组会控制 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，我们建议您只允许端口 3260 (适用于 iSCSI 连接) 和端口 80 (适用于激活) 上的连接。
- 如果您想从网关安全组外部的 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。
- 仅在使用 AWS Support 进行故障诊断用途时，允许端口 22 上的访问。有关更多信息，请参阅你想AWS Support帮助对 EC2 网关进行故障排除。

在某些情况下，您可以使用 Amazon EC2 实例作为启动程序 (即，连接到您部署在 Amazon EC2 上的网关上的 iSCSI 目标)。在这种情况下，我们将为您推荐一种包含两个步骤的方法：

1. 您应在与网关相同的安全组中启动启动程序实例。
2. 您应配置访问权限，以便启动程序可与网关进行通信。

有关要为您的网关开放的端口的信息，请参阅端口要求。

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，或者在AWS作为 Amazon EC2 实例。

Storage Gateway 支持以下管理程序版本和主机：

- VMware ESXi 管理程序（版本 6.0、6.5 或 6.7）— VMware 的免费版本可从VMware 网站. 对于此设置，您还需要 VMware vSphere 客户端才能连接到主机。
- Microsoft Hyper-V 管理程序（版本 2012 R2 或 2016）-Hyper-V 的免费独立版本，可从Microsoft 下载中心. 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) — 一种免费的开源虚拟化技术。KVM 包含在所有版本的 Linux 2.6.20 及更新版本中。Storage Gateway 已针对 CentOS/RHEL 7.7、Ubuntu 16.04 LTS 和 Ubuntu 18.04 LTS 发行版进行了测试并得到它们的支持。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。
- 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，请参阅在 Amazon EC2 主机上部署文件网关.
- Storage Gateway 硬件设备 — Storage Gateway 为虚拟机基础架构有限的位置提供了物理硬件设备以作为本地部署选项

> **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，请参阅从意外的虚拟机关闭中恢复。
> Storage Gateway 不支持动态内存和虚拟内存激增。

文件网关支持的 NFS 客户端

文件网关支持以下网络文件系统 (NFS) 客户端：

- Amazon Linux
- Mac OS X

> **Note**
>
> 我们建议设置`rsize`和`wsize`将选项挂载到 64KB 以提高在 Mac OS X 上装载 NFS 文件共享时的性能

- RHEL 7
- SUSE Linux Enterprise Server 11 和 SUSE Linux Enterprise Server 12
- Ubuntu 14.04
- Microsoft Windows 10 企业版、Windows Server 2012 和 Windows Server 2016。本机客户端仅支持 NFS 版本 3。
- Windows 7 企业版和 Windows Server 2008。

  本机客户端仅支持 NFS 版本 3。支持的最大 NFS I/O 大小为 32 KB，因此，您可能会在这些版本的 Windows 上遇到性能下降的情况。

> **Note**
>
> 现在，您可以在需要通过 Windows (SMB) 客户端（而不是 Windows NFS 客户端）进行访问时使用 SMB 文件共享。

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 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 Server

> **Note**
>
> 服务器消息块加密需要支持 SMB v2.1 的客户端。

文件网关支持的文件系统操作

您的 NFS 或 SMB 客户端可以写入、读取、删除和截断文件。当客户端向AWS Storage Gateway它会同步写入本地缓存。然后，通过经优化的传输异步写入 Amazon S3。首先通过本地缓存来提供读取内容。如果数据不可用，则通过 S3 将数据作为缓存的读取内容捕获。

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。从 Amazon S3 中删除对象。使用与 Amazon S3 控制台中相同的语法，将目录作为 S3 中的文件夹对象进行管理。

HTTP 操作（如 GET、PUT、UPDATE 和 DELETE）可以修改文件共享中的文件。这些操作与原子创建、读取、更新和删除 (CRUD) 功能一致。

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管理任务。本指南的“入门”章节和其他章节使用此控制台来阐释网关功能。

此外，您还可以使用 AWS Storage Gateway API 以编程方式配置并管理网关。有关该 API 的更多信息，请参阅Storage Gateway 的 API 参考。

您也可以使用AWS开发工具包，以开发与 Storage Gateway 交互的应用程序。这些区域有：AWS适用于 Java、.NET 和 PHP 的 SDK 包含底层 Storage Gateway API 以简化您的编程任务。有关下载开发工具包库的信息，请参阅AWS开发者中心.

有关定价的信息，请参阅 AWS Storage Gateway 定价。

支持的 AWS 区域

- Storage Gateway — 对于支持AWS地区和列表AWS可以与 Storage Gateway 一起使用的服务终端节点，请参阅AWS Storage Gateway终端节点和配额中的AWS一般参考.
- Storage Gateway 硬件设备 — 有关可与硬件设备配合使用的受支持的区域，请参阅AWS Storage Gateway硬件设备地区中的AWS一般参考.

使用 Storage Gateway 硬件设备

Storage Gateway 硬件设备是在验证的服务器配置上预装了 Storage Gateway 软件的物理硬件设备。您可以从管理硬件设备Hardware (硬件)上的页面AWS Storage Gateway控制台。

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中。在购买并激活您的硬件设备时，激活过程会将硬件设备与您的AWSaccount. 在激活后，您的硬件设备会以控制台的网关形式显示在控制台中Hardware (硬件)页. 您可以将硬件设备配置为文件网关、磁带网关或卷网关类型。用于在硬件设备上部署和激活这些网关类型的过程与虚拟平台上的过程相同。

Storage Gateway 硬件设备可以直接从AWS Storage Gateway控制台。

订购硬件设备

1. 在处打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home然后选择AWS您希望设备在其中。
2. 选择Hardware (硬件)从导航窗格中。
3. 选择订购设备，然后选择继续. 系统会将您重定向到AWS元素设备和软件管理控制台以请求销售报价。
4. 填写必要的信息然后选择提交.

审核信息后，将生成销售报价，您可以继续订购流程并提交采购订单，或安排预付款。

查看硬件设备的销售报价或订单历史记录

1. 在处打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
2. 选择Hardware (硬件)从导航窗格中。
3. 选择报价和订单，然后选择继续. 系统会将您重定向到AWS元素设备和软件管理控制台可查看销售报价和订单历史记录。

在以下各部分中，您可以了解有关如何设置、配置、激活、启动和使用 Storage Gateway 硬件设备的说明。

主题

- 机架安装硬件设备并将其连接到电源
- 配置网络参数
- 激活硬件设备
- 启动网关
- 为网关配置 IP 地址
- 配置网关
- 从硬件设备中删除网关
- 删除硬件设备

支持的 AWS 区域

Storage Gateway 硬件设备可在全球范围内运输，美国政府在法律允许和允许出口的情况下。有关受支持的信息AWS地区，请参阅Storage Gateway 硬件设备区域中的AWS一般参考.

设置硬件设备

在收到 Storage Gateway 硬件设备后，您可以使用硬件设备控制台配置网络以提供始终开启的连接AWS然后激活你的设备。激活将您的设备与AWS激活过程中使用的帐户。在激活设备后，您可以从 Storage Gateway 控制台启动文件、卷或磁带网关。

要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，请参阅机架安装硬件设备并将其连接到电源。
2. 同时为硬件设备（主机）和 Storage Gateway（服务）设置 Internet 协议版本 4 (IPv4) 地址。有关更多信息，请参阅配置网络参数。
3. 在控制台上激活硬件设备Hardware (硬件)中的页面AWS您选择的区域。有关更多信息，请参阅激活硬件设备。
4. 在硬件设备上安装 Storage Gateway。有关更多信息，请参阅配置网关。

   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。这样做会提供更大的缓存，从而在中进行低延迟的数据访问AWS. 如果您订购了 5 TB 机型，您可以通过购买五个 1.92 TB SSD（固态硬盘）来将可用存储增加到 12 TB（控制台上提供）。Hardware (硬件)页. 您可以按照与订购硬件设备和从 Storage Gateway 控制台请求销售报价相同的订购流程订购额外的 SSD。

然后，您可以在激活硬件设备之前将它们添加到硬件设备。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。联系人AWS有关如何执行该操作的说明的 Support。
2. 将五个 1.92 TB SSD 添加到设备中。

选择网络接口卡

根据您订购的设备型号，它可能附带 10G-Base-T 铜质网卡或 10G DA/SFP+ 网卡。

- 10G-Base-T 网卡配置：
  - 使用 CAT6 电缆进行 10G 或 CAT5 (e) 对于 1G
- 10G DA/SFP+ 网卡配置：
  - 使用 Twinax 铜质直接连接电缆长达 5 米
  - 戴尔/英特尔兼容 SFP+ 光模块（SR 或 LR）
  - SFP/SFP+ 铜质收发器，适用于 1G-Base-T 或 10G-Base-T

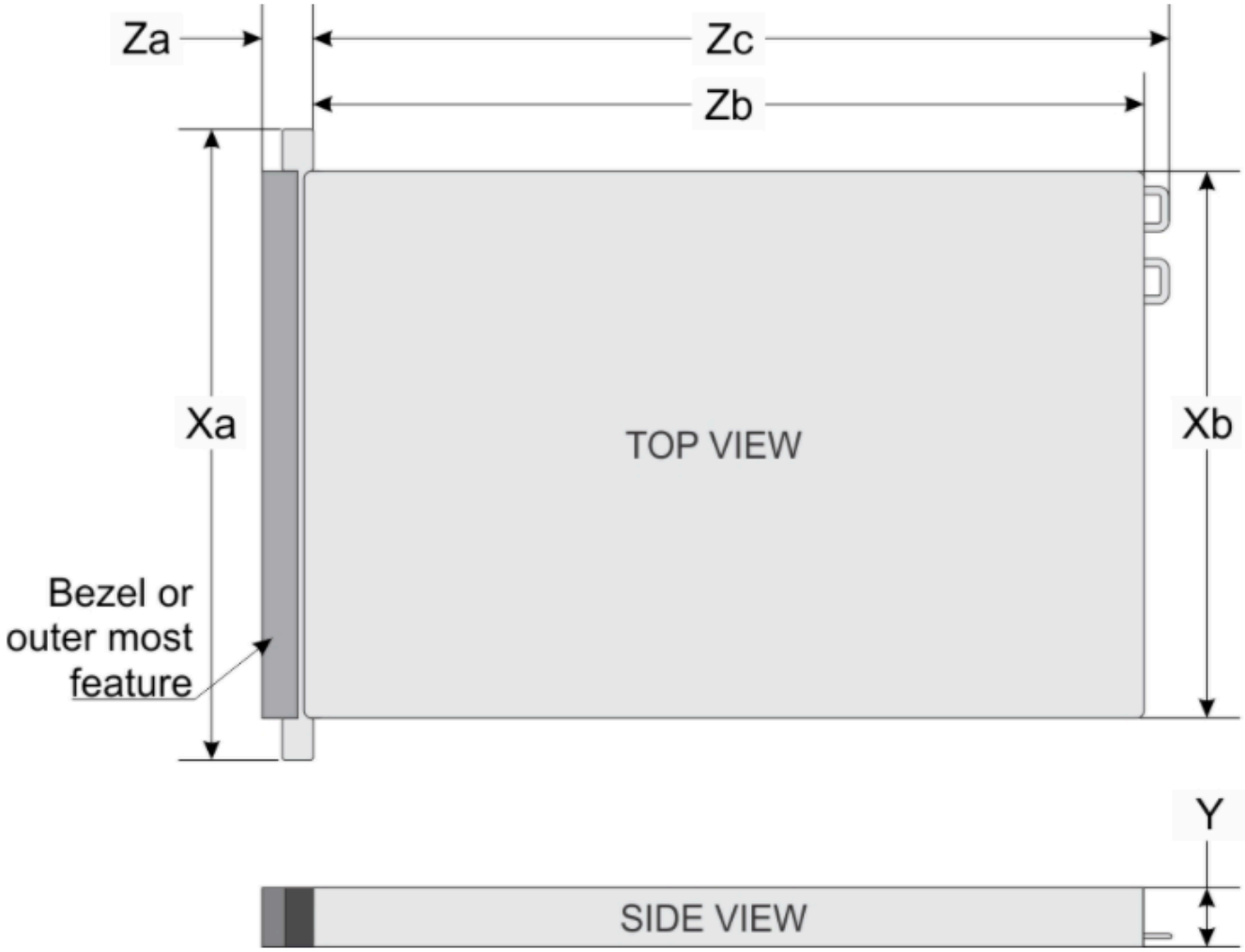
机架安装硬件设备并将其连接到电源

在拆开您的 Storage Gateway 硬件设备后，请按照箱内包含的说明操作，机架安装该服务器。您的设备有一个 1U 外形规格并适合安装在符合国际电工委员会 (IEC) 标准的 19 英寸机架中。

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含的网络接口卡 (NIC)）。Twinax Copor DAC、SFP + 光模块（英特尔兼容）或 SFP 转 Base-T 铜缆收发器。
- 键盘和显示器，或键盘、视频和鼠标 (KVM) 切换解决方案。

硬件设备尺寸



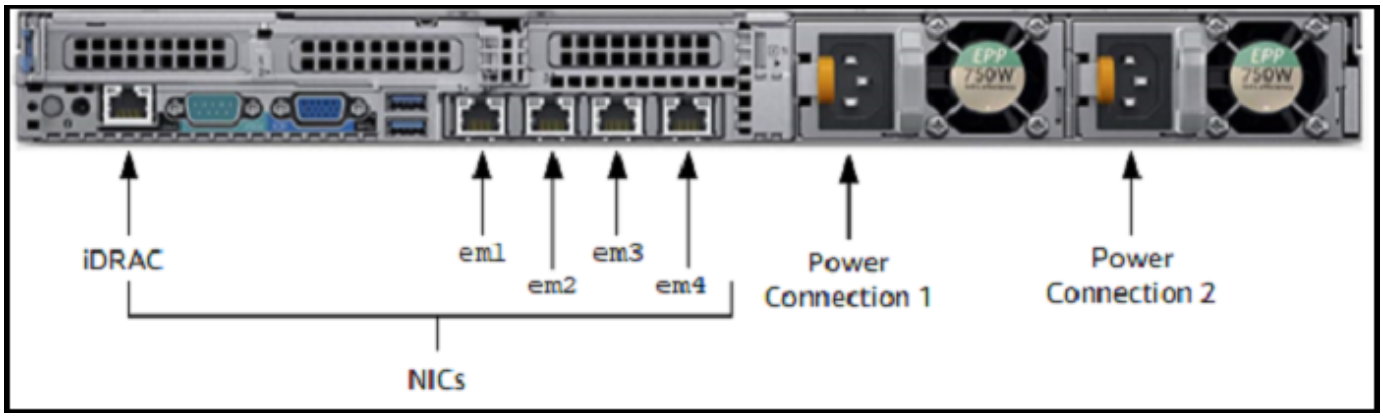
System	Xa	Xb	Y	Za (with bezel)	Za (without bezel)	Zb*	Zc
10 x 2.5-inches	482.0 mm (18.97-inches)	434.0 mm (17.08-inches)	42.8 mm (1.68-inches)	35.84 mm (1.41-inches)	22.0 mm (0.87-inches)	733.82 mm (29.61-inches)	772.67 mm (30.42-inches)

将硬件设备连接至电源

> **Note**
>
> 在执行以下过程之前，请确保您符合 Storage Gateway 硬件设备的所有要求，如中所述。Storage Gateway 硬件设备的网络和防火墙要求.

1. 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。

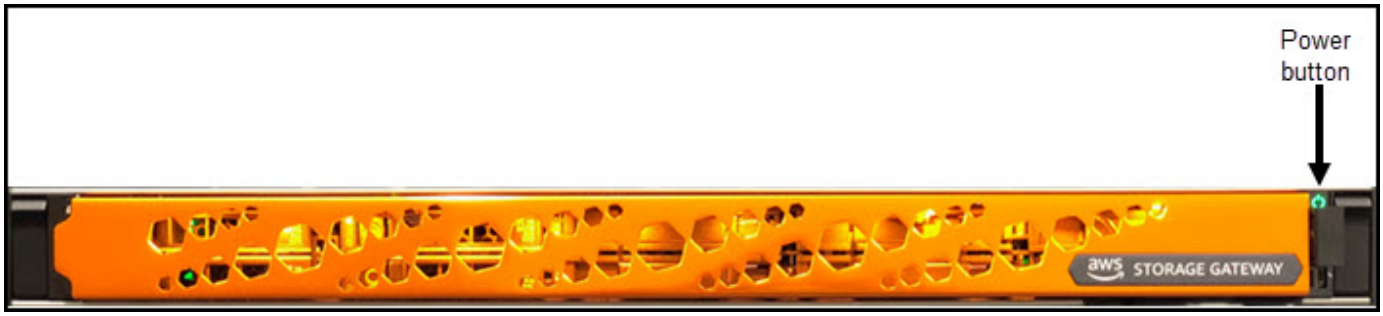
   在下图中，您可以看到具有不同连接的硬件设备。



2. 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。将连接硬件设备的交换机端口设置为非中继 VLAN 端口。

3. 将键盘和显示器插入电源。
4. 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。

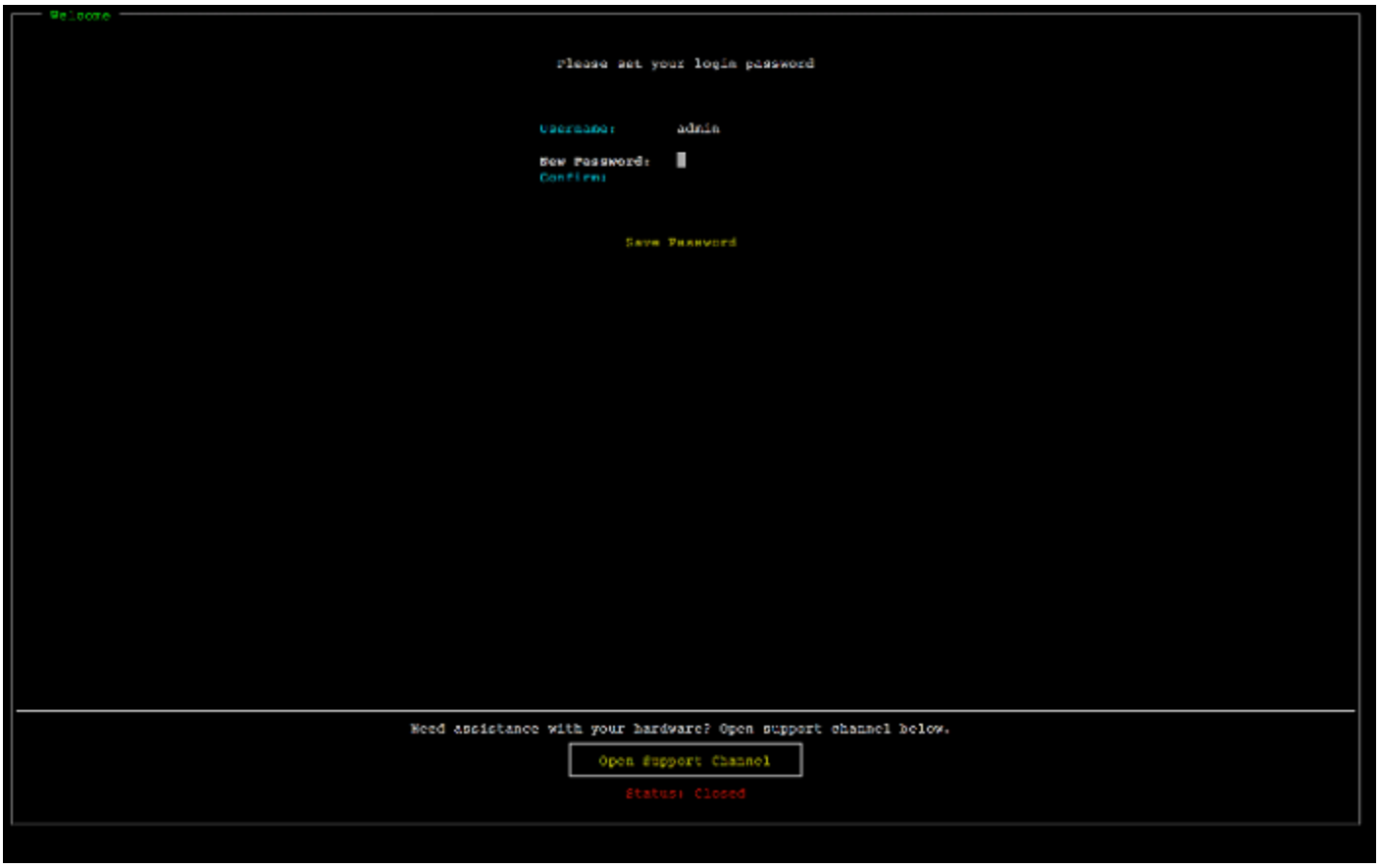


在服务器启动后，硬件控制台会显示在显示器上。硬件控制台提供了一个特定于的用户界面AWS可用于配置初始网络参数。您可以将这些参数配置为将设备连接到AWS通过以下方式开放故障排除支持通道。AWSSupport。

要使用硬件控制台，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。

首次设置密码

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



此时您位于硬件控制台中，如下所示。

下一步

[配置网络参数]

配置网络参数

在服务器启动后，您可以在硬件控制台中输入您的第一个密码，如[机架安装硬件设备并将其连接到电源]中所述。

接下来，在硬件控制台中，执行以下步骤来配置网络参数以便您的硬件设备可以连接到：AWS.

设置网络地址

1. 选择 Configure Network (配置网络)，然后按 `Enter` 键。此时会显示以下 Configure Network (配置网络) 屏幕。

2. 对于 IP Address (IP 地址)，输入来自以下源之一的有效的 IPv4 地址：

   - 使用由您的动态主机配置协议 (DHCP) 服务器分配到您的物理网络端口的 IPv4 地址。

     如果这样做，请记下此 IPv4 地址以便在稍后激活步骤中使用。
   - 分配一个静态 IPv4 地址。为此，请选择静态中的em1按部分，然后按Enter以查看如下所示的配置静态 IP 屏幕。

     em1 部分位于端口设置组中的左上部分。

   在输入有效的 IPv4 地址后，按 Down arrow 或 Tab。

   > **Note**
   >
   > 如果配置任何其他接口，则它必须提供相同的始终开启的连接AWS要求中列出的终端节点。

3. 对于 Subnet (子网)，输入有效的子网掩码，然后按 Down arrow。
4. 对于 Gateway (网关)，输入您的网关的 IPv4 地址，然后按 Down arrow。
5. 对于 DNS1，输入域名服务 (DNS) 服务器的 IPv4 地址，然后按 Down arrow。
6. （可选）对于 DNS2，输入另一个 IPv4 地址，然后按 Down arrow。如果第一个 DNS 服务器变得不可用，另一个 DNS 服务器分配将提供额外冗余。
7. 选择 Save (保存)，然后按 Enter 以保存设备的静态 IPv4 地址设置。

从硬件控制台注销

1. 选择 Back (返回) 以返回到主屏幕。
2. 选择 Logout (注销) 以返回到登录屏幕。

下一步

激活硬件设备

激活硬件设备

在配置您的 IP 地址后，请在控制台的 Hardware (硬件) 页面上输入该 IP 地址，如下所述。激活过程验证您的硬件设备具有适当的安全凭证并将设备注册到您的AWSaccount.

您可以选择在任何支持的中激活您的硬件设备。AWS地区。有关受支持的列表AWS地区，请参阅Storage Gateway 硬件设备区域中的AWS一般参考.

要首次激活您的设备或AWS没有部署网关的区域

1. 登录到AWS Management Console然后打开 Storage Gateway 控制台AWS Storage Gateway管理控制台使用用于激活硬件的帐户凭据。

   如果这是你的第一个网关AWS区域，您会看到启动屏幕。在此中创建网关后AWS地区，屏幕不再显示。

   > **Note**
   >
   > 对于仅激活，必须满足以下条件：
   >
   > - 您的浏览器必须位于与您的硬件设备相同的网络上。
   > - 您的防火墙必须允许在端口 8080 上的 HTTP 访问设备的入站流量。

2. 选择试用以查看创建网关向导，然后选择硬件设备在选择主机平台页面，如下所示。
3. 选择 Next (下一步) 以查看如下所示的 Connect to hardware (连接到硬件) 屏幕。
4. 适用于IP 地址中的Connect 到硬件设备部分中，输入设备的 IPv4 地址，然后选择Connect (连接)以转至如下所示的激活硬件屏幕。
5. 对于 Hardware name (硬件名称)，输入设备的名称。名称长度最多为 255 个字符，并且不能包含斜杠字符。
6. 适用于硬件时区中，输入您的本地设置。

   时区控制硬件更新发生的时间，其中以本地时间凌晨 2 点作为更新时间。

   > **Note**
   >
   > 我们建议设置设备的时区，因为这将确定超出常规工作日范围的标准更新时间。

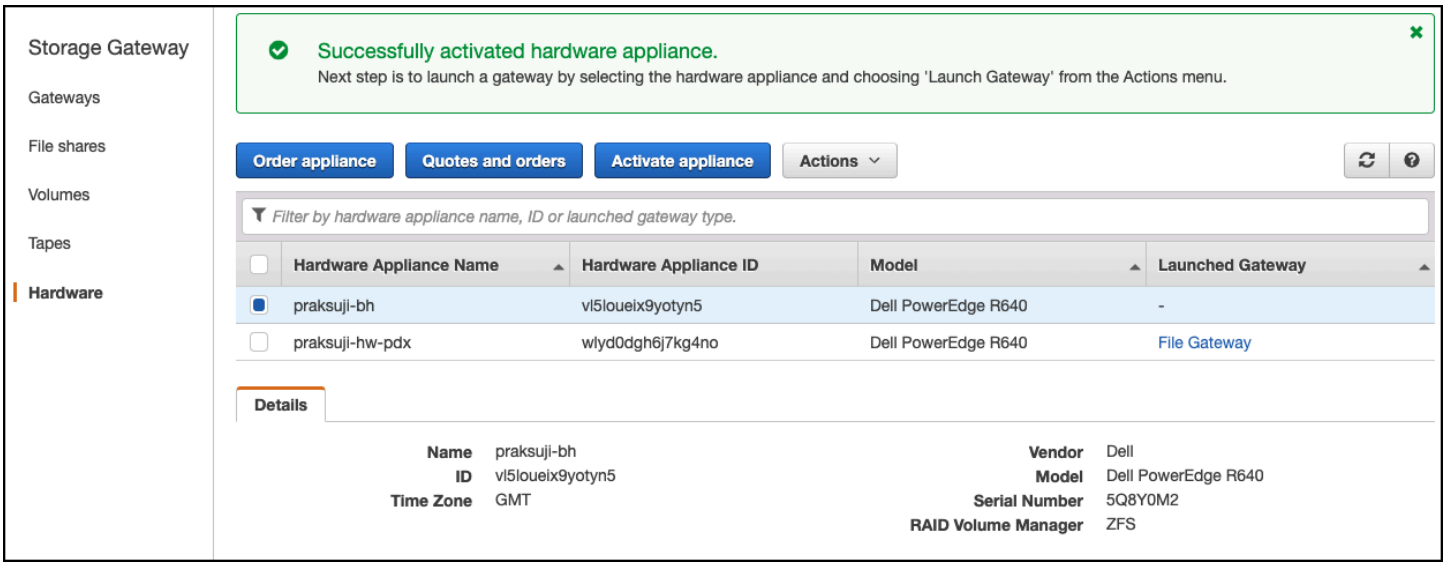
7. （可选）将 RAID Volume Manager (RAID 卷管理器) 设置为 ZFS。

ZFS 用作硬件设备上的 RAID 卷管理器，以提供更好的性能和数据保护。ZFS 是一个基于软件的开源文件系统和逻辑卷管理器。该硬件设备专门针对 ZFS RAID 而优化。有关 ZFS RAID 的更多信息，请参阅 ZFS Wikipedia 页面。

8. 选择 Next (下一步) 以完成激活。

将在 Hardware (硬件) 页面上显示控制台横幅以指示硬件设备已成功激活，如下所示。

此时，该设备已与您的账户关联。下一步是在您的设备上启动文件、磁带或缓存卷网关。



下一步

启动网关

启动网关

您可以在设备上启动三种存储网关中的任一一种文件网关、卷网关（缓存）或磁带网关。

在硬件设备上启动网关

1. 登录到AWS Management Console然后打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
2. 选择 Hardware (硬件)。
3. 对于 Actions (操作)，选择 Launch Gateway (启动网关)。
4. 对于 Gateway Type (网关类型)，选择 File Gateway (文件网关)、Tape Gateway (磁带网关) 或 Volume Gateway (Cached) (卷网关（缓存）)。

5. 对于 Gateway name (网关名称)，输入网关的名称。名称长度可以为 255 个字符，并且不能包含斜杠字符。
6. 选择 Launch gateway (启动网关)。

将适用于您所选网关类型的 Storage Gateway 软件安装在设备上。要将网关显示为可能需要长达 5-10 分钟时间。线上在控制台中。

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

[为网关配置 IP 地址]

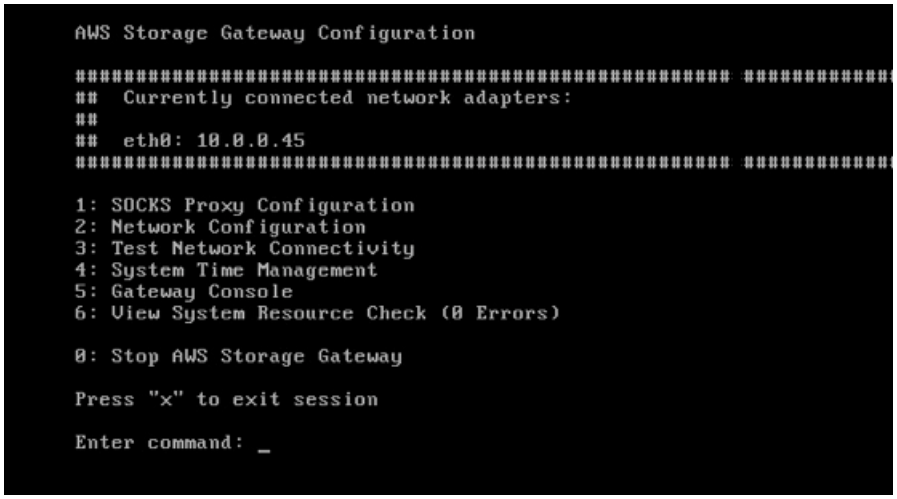
为网关配置 IP 地址

在激活硬件设备之前，您为其物理网络接口分配了 IP 地址。既然您已激活设备并在其上启动了 Storage Gateway，您需要为硬件设备上运行的 Storage Gateway 虚拟机分配另一个 IP 地址。要为硬件设备上安装的网关分配静态 IP 地址，请从本地控制台中为该网关配置 IP 地址。您的应用程序（如您的 NFS 或 SMB 客户端、iSCSI 启动程序等）会连接到此 IP 地址。您可以从硬件设备控制台访问该网关本地控制台。

在设备上配置 IP 地址以使用应用程序

1. 在硬件控制台中，选择 Open Service Console (打开服务控制台) 以打开网关本地控制台的登录屏幕。
2. 输入 localhost login (登录) 密码，然后按 `Enter`。

   默认账户为 `admin`，默认密码为 `password`。
3. 更改默认密码。依次选择 Actions (操作) 和 Set Local Password (设置本地密码)，然后在 Set Local Password (设置本地密码) 对话框中输入新的凭证。
4. （可选）配置代理设置。有关说明，请参阅[机架安装硬件设备并将其连接到电源]。
5. 导航到网关本地控制台的网络设置页面，如下所示。



6. 键入 2 以转到如下所示的 Network Configuration (网络配置) 页面。

7. 在您的硬件设备上为网络端口配置静态 IP 地址或 DHCP IP 地址，以为应用程序显示文件、卷和磁带网关。此 IP 地址必须位于与硬件设备激活期间使用的 IP 地址相同的子网中。

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。

下一步

[配置网关]

配置网关

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，您可以创建您希望使用的网关的类型。为网关类型继续进行安装。有关说明，请参阅 配置您的 Amazon S3 文件网关。

从硬件设备中删除网关

要从您的硬件设备中删除网关软件，请使用以下步骤。完成此操作后，网关软件将从您的硬件设备中卸载。

从硬件设备中删除网关

1. 选择网关对应的复选框。
2. 对于 Actions (操作)，选择 Remove Gateway (删除网关)。
3. 在 Remove gateway from hardware appliance (从硬件设备中删除网关) 对话框中，选择 Confirm (确认)。

> **Note**
>
> 在删除网关后，您将无法撤消此操作。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，请参阅使用 AWS Storage Gateway 控制台删除网关并清除相关资源。

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。

删除硬件设备

在中激活硬件设备之后AWS账户时，您可能需要移动该帐户并在不同的中进行激活。AWSaccount. 在这种情况下，请先从AWS账户然后在另一个账户中激活AWSaccount. 您可能还需要从您的中完全删除设备。AWS帐户是因为您不再需要它。请按照以下说明删除您的硬件设备。

删除硬件设备

1. 如果在硬件设备上安装了网关，您必须先删除网关，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。从硬件设备中删除网关.
2. 在 Hardware (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)。
4. 在 Confirm deletion of resource(s) (确认删除资源) 对话框中，选中确认复选框，然后选择 Delete (删除)。将显示一条消息以指示删除成功。

   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本身上的数据。

开始使用 AWS Storage Gateway

在此部分中，您可以找到有关如何创建和激活文件网关的说明。AWS Storage Gateway. 开始之前，请确保您的设置符合所需的前提条件和其他要求。为 Amazon S3 文件网关设置.

主题

- 创建并激活 Amazon S3 文件网关

创建并激活 Amazon S3 文件网关

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

主题

- 设置 Amazon S3 文件网关
- 将您的 Amazon S3 文件网关 Connect 到AWS
- 查看设置并激活 Amazon S3 文件网关
- 配置您的 Amazon S3 文件网关

设置 Amazon S3 文件网关

如需设置新的 S3 文件网关

1. 打开AWS Management Console在https://console.aws.amazon.com/storagegateway/home/，然后选择AWS 区域您要在其中创建网关的位置。
2. 选择创建网关以打开设置网关页.
3. 在网关设置部分中，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，您可以搜索此名称以在AWS Storage Gateway控制台。
   b. 适用于网关时区中，为您想要部署网关的世界地区选择当地时区。
4. 在网关选项部分，网关类型，选择Amazon S3 文件网关.
5. 在平台选项部分中，执行以下操作：
   a. 适用于主机平台中，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特定于平台的说明来设置主机平台。可从以下选项中进行选择：

- VMware ESXi— 使用 VMware ESXi 下载、部署和配置网关虚拟机。
- Microsoft Hyper-V— 使用 Microsoft Hyper-V 下载、部署和配置网关虚拟机。
- Linux KVM— 使用基于 Linux 内核的虚拟机 (KVM) 下载、部署和配置网关虚拟机。
- Amazon EC2— 配置和启动 Amazon EC2 实例，以托管您的网关。
- 硬件设备— 从下单订购专用物理硬件设备AWS托管网关。

b. 适用于确认设置网关中，选中复选框以确认您已为选择的主机平台执行了部署步骤。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之前，您必须选择希望如何连接和通信。AWS. 选择下一步以继续。

将您的 Amazon S3 文件网关 Connect 到AWS

将新的 S3 文件网关连接到AWS

1. 如果您尚未这样做，请完成中所述的过程。设置 Amazon S3 文件网关. 完成后，选择下一步以打开连接到AWS中的 “中” 页面AWS Storage Gateway控制台。
2. 在端点选项部分，服务终端节点中，选择网关将用于与之通信的终端节点类型AWS. 可从以下选项中进行选择：

   - 公开访问— 你的网关与AWS在公共 Internet 上。如果选择此选项，则使用启用 FIPS 的终端节点复选框以指定连接是否必须符合联邦信息处理标准 (FIPS)。

     > **Note**
     >
     > 如果在访问时需要经过 FIPS 140-2 验证的加密模块AWS通过命令行界面或 API，使用 FIPS 兼容的终端节点。有关更多信息，请参阅美国联邦信息处理标准 (FIPS) 140-2。FIPS 服务终端节点仅在部分中可用AWS地区。有关更多信息，请参阅 。AWS Storage Gateway终端节点和配额中的AWS一般参考.

   - VPC 托管— 你的网关与AWS通过与 Virtual Private Cloud (VPC) 的私有连接，您可以控制您的网络设置。如果选择此选项，则必须通过从下拉列表中选择 VPC 终端节点 ID 来指定现有 VPC 终端节点 ID。您还可以提供其 VPC 终端节点域名系统 (DNS) 名称或 IP 地址。
3. 在网关连接选项部分，连接选项，选择如何识别您的网关AWS. 可从以下选项中进行选择：

   - IP 地址— 在相应的字段中提供网关的 IP 地址。此 IP 地址必须是公共或可从当前网络中访问的，并且您必须能够从 Web 浏览器连接到该 IP 地址。

您可以通过从虚拟机管理程序客户端登录网关的本地控制台或从 Amazon EC2 实例详细信息页面复制该网关 IP 地址来获取网关 IP 地址。

- 激活密钥— 在相应的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生成激活密钥。如果网关的 IP 地址不可用，请选择此选项。

4. 现在你已经选择了你希望网关连接到的方式AWS，你必须激活网关。选择下一步以继续。

查看设置并激活 Amazon S3 文件网关

激活新的 S3 文件网关

1. 如果您尚未这样做，请完成以下主题中所述的过程：

   - 设置 Amazon S3 文件网关
   - 将您的 Amazon S3 文件网关 Connect 到AWS

   完成后，选择下一步以打开查看并激活中的 “中” 页面AWS Storage Gateway控制台。

2. 查看页面上每个部分的初始网关详细信息。
3. 如果部分包含错误，请选择编辑返回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. 现在您已激活网关，必须执行首次配置才能分配本地存储磁盘并配置日志记录。选择下一步以继续。

配置您的 Amazon S3 文件网关

在新的 S3 文件网关上执行首次配置

1. 如果您尚未完成，请完成以下主题中描述的过程：

   - 设置 Amazon S3 文件网关
   - 将您的 Amazon S3 文件网关 Connect 到AWS
   - 查看设置并激活 Amazon S3 文件网关

完成后，选择下一步以打开配置网关中的 “中” 页面AWS Storage Gateway控制台。

2. 在配置缓存存储部分中，使用下拉列表至少分配一个至少有 150 GB (GiB) 容量的本地磁盘缓存. 本节中列出的本地磁盘与您在主机平台上配置的物理存储空间相对应。
3. 在CloudWatch 日志组部分中，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：

   - 创建新的日志组— 设置新的日志组以监控网关。
   - 使用现有日志组— 从相应的下拉列表中选择现有的日志组。
   - 停用日志记录— 不要使用 Amazon CloudWatch Logs 来监控您的网关。
4. 在CloudWatch 警报部分中，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：

   - 取消激活警报— 不要使用 CloudWatch 警报接收有关网关指标的通知。
   - 创建自定义 CloudWatch 警报— 配置新的 CloudWatch 警报以接收有关网关指标的通知。选择创建警报以在 Amazon CloudWatch 控制台中定义指标和指定警报操作。有关说明，请参阅使用 Amazon CloudWatch 警报中的Amazon CloudWatch 用户指南.
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/值对以帮助您在AWS Storage Gateway控制台。重复此步骤以添加所需数量的标签。
6. （可选）在验证 VMware High Availability 配置部分中，如果将您的网关作为已启用 VMware 高可用性 (HA) 的集群的一部分部署到 VMware 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 (VM)。
7. 选择配置完成网关的创建。

   要检查您的新网关的状态，请在网关的页面AWS Storage Gateway控制台。

现在，您已经创建网关，您必须创建文件共享才能使用。有关说明，请参阅创建文件共享.

创建文件共享

在此部分中，您可以找到有关如何创建文件共享的说明。您可以创建可使用网络文件系统 (NFS) 或服务器消息块 (SMB) 协议访问的文件共享。

> **Note**
>
> 当 NFS 或 SMB 客户端将文件写入文件网关时，文件网关会将文件的数据上传到 Amazon S3，然后是其元数据（所有权、时间戳等）。上传文件数据将创建 S3 对象，上传文件的元数据将更新 S3 对象的元数据。此过程将创建对象的另一个版本，从而生成对象的两个版本。如果启用 S3 版本控制，将存储两个版本。
>
> 如果您更改文件网关中存储的文件的元数据，则会创建一个新的 S3 对象并替换现有 S3 对象。这种行为与编辑文件系统中的文件不同，在文件系统中编辑文件不会导致创建新文件。测试您计划与之配合使用的所有文件操作AWSStorage Gateway，以便您了解每个文件操作如何与 Amazon S3 存储交互。
>
> 当您从文件网关上传数据时，请仔细考虑在 Amazon S3 中使用 S3 版本控制和跨区域复制 (CRR)。启用 S3 版本控制后，将文件从文件网关上传到 Amazon S3 会导致至少两个版本的 S3 对象。
>
> 某些涉及大型文件和文件写入模式的工作流程（例如，分几个步骤执行的文件上传）可能会增加存储的 S3 对象版本的数量。如果文件网关缓存由于高文件写入率而需要释放空间，则可能会创建多个 S3 对象版本。如果启用 S3 版本控制，这些方案会增加 S3 存储空间，并增加与 CRR 相关的传输成本。测试您计划与 Storage Gateway 一起使用的所有文件操作，以便了解每个文件操作如何与 Amazon S3 存储交互。
>
> 将 Rsync 实用程序与文件网关结合使用会导致在缓存中创建临时文件并在 Amazon S3 中创建临时 S3 对象。S3 标准-不常访问 (S3 标准 — IA) 和 S3 智能分层存储类中产生提前删除费用。

默认情况下，当您创建 NFS 共享时，有权访问 NFS 服务器的任何人都能访问 NFS 文件共享。您可以通过 IP 地址限制对客户端的访问。

对于 SMB，您可以拥有三种不同的身份验证模式之一：

- 具有 Microsoft Active Directory (AD) 访问权限的文件共享。任何经过身份验证的 Microsoft AD 用户都将获得对此文件共享类型的访问权限。
- 具有有限访问权限的 SMB 文件共享。只有您指定的特定域用户和组被允许访问（通过允许列表）。用户和组也可以被拒绝访问（通过拒绝列表）。

- 具有来宾访问权限的 SMB 文件共享。可以提供来宾密码的任何用户都将获得对此文件共享的访问权限。

> **Note**
>
> 通过 NFS 文件共享网关导出的文件共享支持 POSIX 权限。对于 SMB 文件共享，您可以使用访问控制列表 (ACL) 来管理文件共享中的文件和文件夹的权限。有关更多信息，请参阅使用 Microsoft Windows ACL 控制对 SMB 文件共享的访问。

文件网关可以托管一个或多个不同类型的文件共享。您可以在一个文件网关上有多个 NFS 和 SMB 文件共享。

> **Important**
>
> 要创建文件共享，文件网关要求您激活 AWS Security Token Service (AWS STS)。确保AWS STS已在AWS 区域您正在创建文件网关。如果AWS STS在那里没有激活AWS 区域，激活它。有关如何激活的信息AWS STS请参阅,激活和停用AWS STS在AWS 区域中的AWS Identity and Access Management用户指南.

> **Note**
>
> 您可以使用AWS Key Management Service(AWS KMS) 加密文件网关在 Amazon S3 中存储的对象。若要使用 Storage Gateway 控制台执行此操作，请参阅创建 NFS 文件共享要么创建 SMB 文件共享. 您也可以通过使用 Storage Gateway API 来执行此操作。有关说明，请参阅CreateNFSFileShare要么CreateSMBFileShare中的AWSStorage Gateway API 参考.
> 默认情况下，文件网关在将数据写入 S3 存储桶时使用 Amazon S3 (SSE-S3) 托管的服务器端加密。如果您使用 SSE-KMS (服务器端加密)AWS KMS— 托管密钥) 您的 S3 存储桶的默认加密，文件网关存储在该处的对象将使用 SSE-KMS 进行加密。
> 要结合使用 SSE-KMS 与您自己的 AWS KMS 密钥进行加密，您必须启用 SSE-KMS 加密。当您执行此操作时，需要在创建文件共享时提供 KMS 密钥的 Amazon 资源名称 (ARN)。您也可以通过使用 UpdateNFSFileShare 或 UpdateSMBFileShare API 操作来更新文件共享的 KMS 设置。更新后，此更新应用于存储在 Amazon S3 存储桶中的对象。
> 如果将文件网关配置为使用 SSE-KMS 进行加密，则必须手动添加`kms:Encrypt`、`kms:Decrypt`、`kms:ReEncrypt`、`kms:GenerateDataKey`,

和kms:DescribeKey对与文件共享关联的 IAM 角色的权限。有关更多信息，请参阅 。为 Storage Gateway 使用基于身份的策略 (IAM 策略).

主题

- 创建 NFS 文件共享
- 创建 SMB 文件共享

创建 NFS 文件共享

要创建网络文件系统 (NFS) 文件共享，请按照以下过程操作。

Note

当 NFS 客户端将文件写入文件网关时，文件网关会将文件的数据上传到 Amazon S3，然后是其元数据（所有权、时间戳等）。上传文件数据将创建 S3 对象，上传文件的元数据将更新 S3 对象的元数据。此过程将创建对象的另一个版本，从而生成对象的两个版本。如果启用 S3 版本控制，将存储两个版本。

如果您更改文件网关中存储的文件的元数据，则会创建一个新的 S3 对象并替换现有 S3 对象。这种行为与编辑文件系统中的文件不同，在文件系统中编辑文件不会导致创建新文件。测试您计划与之配合使用的所有文件操作AWSStorage Gateway，以便您了解每个文件操作如何与 Amazon S3 存储交互。

当您从文件网关上传数据时，请仔细考虑在 Amazon S3 中使用 S3 版本控制和跨区域复制 (CRR)。启用 S3 版本控制后，将文件从文件网关上传到 Amazon S3 会导致至少两个版本的 S3 对象。

某些涉及大型文件和文件写入模式的工作流程（例如，分几个步骤执行的文件上传）可能会增加存储的 S3 对象版本的数量。如果文件网关缓存由于高文件写入率而需要释放空间，则可能会创建多个 S3 对象版本。如果启用了 S3 版本控制，这些方案会增加 S3 存储空间，并增加与 CRR 相关的传输成本。测试您计划与 Storage Gateway 一起使用的所有文件操作，以便了解每个文件操作如何与 Amazon S3 存储交互。

将 Rsync 实用程序与文件网关结合使用会导致在缓存中创建临时文件并在 Amazon S3 中创建临时 S3 对象。S3 标准-不常访问 (S3 标准 — IA) 和 S3 智能分层存储类中产生提前删除费用。

创建 NFS 文件共享

1. 打开AWS在 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home/.
2. 选择创建文件共享以打开文件共享设置页.
3. 适用于网关，请从列表中选择您的 Amazon S3 文件网关。
4. 适用于Amazon S3 位置，请执行以下操作之一：

   - 若要将文件共享直接连接到 S3 存储桶，请选择S3 存储桶名称，然后输入 S3 存储桶名称以及文件共享创建的对象的前缀名称（可选）。您的网关使用此存储桶来存储和检索文件。有关创建新存储桶的信息，请参阅如何创建 S3 存储桶？中的Amazon S3 用户指南中).
   - 要通过访问点将文件共享连接到 S3 存储桶，请选择S3 接入点，然后输入 S3 接入点名称以及文件共享创建的对象的前缀名称（可选）。您的存储桶策略必须配置为将访问控制委派给接入点。有关访问点的信息，请参阅使用 Amazon S3 访问点管理数据访问和将访问控制委派到访问点中的Amazon S3 用户指南中).
   - 要通过接入点别名将文件共享连接到 S3 存储桶，请选择S3 接入点别名，然后输入 S3 接入点别名，也可以选择输入由文件共享创建的对象的前缀名称。如果选择此选项，则文件网关无法创建新的AWS Identity and Access Management(IAM) 角色和访问策略代表您。您必须选择现有的 IAM 角色并在访问您的 S3 存储桶的访问接下来的部分。有关访问点别名的更多信息，请参阅为您的接入点使用存储桶式别名中的Amazon S3 用户指南中).

   > **Note**
   >
   > - 如果输入前缀名称，或者选择通过接入点或接入点别名进行连接，则必须输入文件共享名称。
   > - 前缀名称必须以正斜杠结尾 (/)。
   > - 文件共享创建后，前缀名称无法修改或删除。
   > - 有关使用前缀名称的信息，请参阅使用前缀组织对象中的Amazon S3 用户指南中).

5. 适用于AWS 区域，选择AWS 区域S3 存储桶。
6. 适用于文件共享名称中，输入文件共享的名称。默认名称是 S3 存储桶名称或访问点名称。

   > **Note**
   >
   > - 如果输入了前缀名称，或者选择通过接入点或接入点别名进行连接，则必须输入文件共享名称。

- 创建文件共享后，无法删除文件共享名称。

7. （可选）对于AWS PrivateLink对于 S3中，执行以下操作：

   1. 要配置文件共享以通过支持的虚拟私有云 (VPC) 中的接口终端节点连接到 S3，请执行以下操作：AWS PrivateLink，选择使用 VPC 终端节点.
   2. 要确定您希望文件共享连接的 VPC 接口终端节点，请选择任一VPC 终端节点 ID要么VPC 终端节点 DNS 名称，然后在相应的字段中提供所需的信息。

   > **Note**
   >
   > - 如果文件共享通过 VPC 接入点或通过与 VPC 访问点关联的别名连接到 S3，则需要执行此步骤。
   > - 使用文件共享连接AWS PrivateLinkFIPS 网关不支持。
   > - 有关的信息AWS PrivateLink请参阅,AWS PrivateLink适用于 Amazon S3中的Amazon S3 用户指南中).

8. 对于 Access objects using (使用以下工具访问对象)，请选择 Network File System (NFS) (网络文件系统 (NFS))。
9. 对于 Audit logs (审核日志)，请选择以下选项之一：

   - 要禁用日志记录，选择Disable logging (禁用日志记录).
   - 要创建新的审核日志，请选择创建新的日志组.
   - 要使用现有审计日志，请选择使用现有日志组，然后从列表中选择审核日志。

   有关审核日志的更多信息，请参阅了解文件网关审核日志。

10. 适用于从 S3 自动刷新缓存，选择设置刷新间隔，并设置使用生存时间 (TTL) 刷新文件共享缓存的时间（以天、小时和分钟为单位）。TTL 是自上次刷新以来的时间长度。TTL 时间间隔过后，访问该目录会导致文件网关首先从 Amazon S3 存储桶刷新该目录的内容。
11. 适用于文件上传通知，选择结算时间（秒）以便在文件网关完全上传到 S3 时收到通知。设置沉淀时间以秒为单位来控制客户端在生成文件之前写入文件的最后一个时间点之后等待的秒数`ObjectUploaded`通知功能. 由于客户端可以对文件进行许多小写入，因此最好尽可能长时间设置此参数，以避免在较短的时间段内为同一文件生成多个通知。有关更多信息，请参阅获取文件上传通知。

> **Note**
>
> 此设置不影响对象上传到 S3 的时间，仅影响通知的时间。

12. （可选）在 Add tags (添加标签) 部分中，输入键和值以将标签添加到您的文件共享。标签是帮助您管理、筛选和搜索文件共享的区分大小写的键/值对。
13. 选择下一步。这些区域有：配置文件在 Amazon S3 中的存储方式此时将显示页。
14. 适用于新对象的存储类，选择要用于在 Amazon S3 存储桶中创建的新对象的存储类：

    - 要将您经常访问的对象数据冗余存储在地理上分开的多个可用区中，选择S3 标准. 有关 S3 标准存储类的更多信息，请参阅经常访问对象的存储类中的Amazon Simple Storage Service 用户指南.
    - 要通过自动将数据移动到经济高效的存储访问层来优化存储成本，请选择S3 智能分层. 有关 S3 智能分层存储类的更多信息，请参阅。可自动优化经常访问和不经常访问的对象的存储类中的Amazon Simple Storage Service 用户指南.
    - 要将您不常访问的对象数据冗余存储在地理上分开的多个可用区中，选择S3 标准 – IA. 有关 S3 标准 — IA 存储类的更多信息，请参阅不经常访问对象的存储类中的Amazon Simple Storage Service 用户指南.
    - 要将您不常访问的对象数据存储在单个可用区中，选择S3 单区-IA. 有关 S3 单区 — IA 存储类的更多信息，请参阅不经常访问对象的存储类中的Amazon Simple Storage Service 用户指南.

    为了帮助监控 S3 账单，请使用AWS Trusted Advisor. 有关更多信息，请参阅 。监控工具中的Amazon Simple Storage Service 用户指南.
15. 对于对象元数据，选择要使用的元数据：

    - 要根据文件扩展名猜测已上传对象的 MIME 类型，请选择猜 MIME 类型.
    - 要向映射到 NFS 文件共享的 S3 存储桶的所有者授予完全控制权限，请选择让存储桶拥有者完全控制. 有关使用文件共享来访问其他账户拥有的存储桶中的对象的更多信息，请参阅使用文件共享进行跨账户访问.
    - 如果您在要求请求者或读取者（而不是存储桶拥有者）支付访问费用的存储桶上使用此文件共享，请选择启用申请者付款. 有关更多信息，请参阅申请方付款存储桶。
16. 适用于访问您的 S3 存储桶的访问，选择AWS Identity and Access Management(IAM) 角色，您希望文件网关用来访问您的 Amazon S3 存储桶：

- 要使文件网关能够代表您创建新的 IAM 角色和访问策略，请选择创建新的 IAM 角色. 如果文件共享使用接入点别名连接到 Amazon S3，则此选项不可用。
- 要选择现有的 IAM 角色并手动设置访问策略，请选择使用现有的 IAM 角色. 如果您的文件共享使用接入点别名连接到 Amazon S3，则必须使用此选项。在IAM 角色框中，输入用于访问您的存储桶的角色的 Amazon 资源名称 (ARN)。有关 IAM 角色的信息，请参阅。IAM 角色中的AWS Identity and Access Management用户指南.

有关 S3 存储桶访问权限的更多信息，请参阅授予对 Amazon S3 存储桶的访问权限。

17. 适用于加密选择要用于加密文件网关在 Amazon S3 中存储的对象的加密密钥类型：

    - 若要使用由 Amazon S3 托管的服务器端加密 (SSE-S3)，请选择S3 托管密钥 (SSE-S3).
    - 若要使用托管的服务器端加密AWS Key Management Service（SSE-KMS），选择KMS 托管的密钥 (SSE-KMS). 在主键对话框中，选择现有AWS KMS key或者选择创建新的 KMS 密钥在中创建新的 KMS 密钥AWS Key Management Service(AWS KMS) 控制台。有关 的更多信息AWS KMS请参阅,是什么AWS Key Management Service?中的AWS Key Management Service开发人员指南.

    > **Note**
    >
    > 要指定AWS KMS带有未列出别名的 key 或使用AWS KMS来自不同的钥匙AWS 账户，您必须使用AWS Command Line Interface(AWS CLI)。有关更多信息，请参阅 。CreateNFSFileShare中的AWSStorage Gateway API 参考.
    > 不支持非对称 KMS 密钥。

18. 选择下一步以配置文件访问设置。

配置文件访问设置

1. 适用于允许的客户端，指定是允许还是限制每个客户端对文件共享的访问。为您要允许的客户端提供 IP 地址或 CIDR 表示法。有关受支持的 NFS 客户端的信息，请参阅 文件网关支持的 NFS 客户端。
2. 适用于挂载选项中，指定您所需的选项壁球等级和导出为.

   对于 Squash level (Squash 级别)，请选择下列选项之一：

   - 所有壁球：所有用户访问权限将映射到用户 ID (UID) (65534) 和组 ID (GID) (65534)。

- 没有根壁球：远程超级用户（root 用户）以根用户身份接收访问权限。
- 根壁球（默认）：对于远程超级用户（root 用户）的访问权限将映射到 UID (65534) 和 GID (65534)。

对于 Export as (导出为)，选择以下选项之一：

- Read-write (读/写)
- Read-only

> **Note**
>
> 对于装载在 Microsoft Windows 客户端上的文件共享，如果你选择Read-only，您可能会看到有关某个错误阻止您创建文件夹的消息。您可以忽略此消息。

3. 对于 File metadata defaults (文件元数据默认值)，您可以编辑 Directory permissions (目录权限)、File permissions (文件权限)、User ID (用户 ID) 和 Group ID (组 ID)。有关更多信息，请参阅编辑 NFS 文件共享的元数据默认值。
4. 选择下一步。
5. 检查文件共享配置设置，然后选择Finish.

   在创建 NFS 文件共享之后，您可以在文件共享的详细信息选项卡中查看文件共享设置。

下一步

在客户端上装载 NFS 文件共享

创建 SMB 文件共享

在创建服务器消息块 (SMB) 文件共享之前，请确保为文件网关配置 SMB 安全设置。您还必须配置 Microsoft Active Directory (AD) 或来宾访问以进行身份验证。一个文件共享仅提供一种类型的 SMB 访问。有关说明，请参阅编辑网关的 SMB 设置.

> **Note**
>
> 除非在安全组中打开必需的端口，否则 SMB 文件共享无法正常运行。有关更多信息，请参阅端口要求。

> **Note**
>
> 当中小型企业客户端将文件写入文件网关时，文件网关会将文件的数据上传到 Amazon S3，然后是其元数据（所有权、时间戳等）。上传文件数据将创建 S3 对象，上传文件的元数据将更新 S3 对象的元数据。此过程将创建对象的另一个版本，从而生成对象的两个版本。如果启用 S3 版本控制，将存储两个版本。
>
> 如果您更改文件网关中存储的文件的元数据，则会创建一个新的 S3 对象并替换现有 S3 对象。这种行为与编辑文件系统中的文件不同，在文件系统中编辑文件不会导致创建新文件。测试您计划与之配合使用的所有文件操作AWSStorage Gateway，以便您了解每个文件操作如何与 Amazon S3 存储交互。
>
> 当您从文件网关上传数据时，请仔细考虑在 Amazon S3 中使用 S3 版本控制和跨区域复制 (CRR)。启用 S3 版本控制后，将文件从文件网关上传到 Amazon S3 会导致至少两个版本的 S3 对象。
>
> 某些涉及大型文件和文件写入模式的工作流程（例如，分几个步骤执行的文件上传）可能会增加存储的 S3 对象版本的数量。如果文件网关缓存由于高文件写入率而需要释放空间，则可能会创建多个 S3 对象版本。如果启用 S3 版本控制，这些方案会增加 S3 存储空间，并增加与 CRR 相关的传输成本。测试您计划与 Storage Gateway 一起使用的所有文件操作，以便了解每个文件操作如何与 Amazon S3 存储交互。
>
> 将 Rsync 实用程序与文件网关结合使用会导致在缓存中创建临时文件并在 Amazon S3 中创建临时 S3 对象。S3 标准-不常访问 (S3 标准 — IA) 和 S3 智能分层存储类中产生提前删除费用。

创建 SMB 文件共享

创建 SMB 文件共享

1. 打开AWS在 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home/.
2. 选择创建文件共享以打开文件共享设置页.
3. 适用于网关，请从列表中选择您的 Amazon S3 文件网关。

4. 适用于Amazon S3 位置，请执行以下操作之一：

   - 若要将文件共享直接连接到 S3 存储桶，请选择S3 存储桶名称，然后输入存储桶名称以及文件共享创建的对象的前缀名称（可选）。您的网关使用此存储桶来存储和检索文件。有关创建新存储桶的信息，请参阅如何创建 S3 存储桶？中的Amazon S3 用户指南中).
   - 要通过访问点将文件共享连接到 S3 存储桶，请选择S3 接入点，然后输入 S3 接入点名称以及文件共享创建的对象的前缀名称（可选）。您的存储桶策略必须配置为将访问控制委派给接入点。有关访问点的信息，请参阅使用 Amazon S3 访问点管理数据访问和将访问控制委派到访问点中的Amazon S3 用户指南中).
   - 要通过接入点别名将文件共享连接到 S3 存储桶，请选择S3 接入点别名，然后输入 S3 接入点别名，也可以选择输入由文件共享创建的对象的前缀名称。如果选择此选项，则文件网关无法创建新的AWS Identity and Access Management(IAM) 角色和访问策略代表您。您必须选择现有的 IAM 角色并在访问您的 S3 存储桶的访问接下来的部分。有关访问点别名的更多信息，请参阅为您的接入点使用存储桶式别名中的Amazon S3 用户指南中).

   > **Note**
   >
   > - 如果输入前缀名称，或者选择通过接入点或接入点别名进行连接，则必须输入文件共享名称。
   > - 前缀名称必须以正斜杠结尾 (/)。
   > - 文件共享创建后，前缀名称无法修改或删除。
   > - 有关使用前缀名称的信息，请参阅使用前缀组织对象中的Amazon S3 用户指南中).

5. 适用于AWS 区域，选择AWS 区域S3 存储桶。
6. 适用于文件共享名称中，输入文件共享的名称。默认名称是 S3 存储桶名称或访问点名称。

   > **Note**
   >
   > - 如果输入了前缀名称，或者选择通过接入点或接入点别名进行连接，则必须输入文件共享名称。
   > - 创建文件共享后，无法删除文件共享名称。

7. （可选）对于AWS PrivateLink对于 S3中，执行以下操作：

1. 要配置文件共享以通过支持的虚拟私有云 (VPC) 中的接口终端节点连接到 S3，请执行以下操作：AWS PrivateLink，选择使用 VPC 终端节点.
2. 要确定您希望文件共享连接的 VPC 接口终端节点，请选择任一VPC 终端节点 ID要么VPC 终端节点 DNS 名称，然后在相应的字段中提供所需的信息。

> **Note**
>
> - 如果文件共享通过 VPC 接入点或通过与 VPC 访问点关联的别名连接到 S3，则需要执行此步骤。
> - 使用文件共享连接AWS PrivateLinkFIPS 网关不支持。
> - 有关的信息AWS PrivateLink请参阅,AWS PrivateLink适用于 Amazon S3中的Amazon Simple Storage Service 用户指南.

8. 对于使用以下工具访问对象，选择服务器消息块 (SMB).
9. 对于 Audit logs (审核日志)，请选择以下选项之一：

   - 要禁用日志记录，选择Disable logging (禁用日志记录).
   - 要创建新的审核日志，请选择创建新的日志组.
   - 要使用现有日志组，请选择使用现有日志组，然后从列表中选择审核日志。

   有关审核日志的更多信息，请参阅了解文件网关审核日志。
10. 适用于从 S3 自动刷新缓存，选择设置刷新间隔，然后使用生存时间 (TTL) 设置以天、小时和分钟为单位的时间，以刷新文件共享的缓存。TTL 是自上次刷新以来的时间长度。TTL 时间间隔过后，访问该目录会导致文件网关首先从 Amazon S3 存储桶刷新该目录的内容。
11. 适用于文件上传通知，选择结算时间（秒）以便在文件网关完全上传到 S3 时收到通知。设置沉淀时间以秒为单位来控制客户端在生成文件之前写入文件的最后一个时间点之后等待的秒数`ObjectUploaded`通知功能. 由于客户端可以对文件进行许多小写入，因此最好尽可能长时间设置此参数，以避免在较短的时间段内为同一文件生成多个通知。有关更多信息，请参阅获取文件上传通知。

> **Note**
>
> 此设置不影响对象上传到 S3 的时间，仅影响通知的时间。

12. （可选）在标签部分，选择添加新标签，然后输入键和值以将标签添加到文件共享。标签是帮助您管理、筛选和搜索文件共享的区分大小写的键/值对。
13. 选择下一步。这些区域有：Amazon S3 存储设置此时将显示页。
14. 适用于新对象的存储类，选择要用于在 Amazon S3 存储桶中创建的新对象的存储类：

    - 要将您经常访问的对象数据冗余存储在地理上分开的多个可用区中，选择S3 标准. 有关 S3 标准存储类的更多信息，请参阅经常访问对象的存储类中的Amazon Simple Storage Service 用户指南.
    - 要通过自动将数据移动到经济高效的存储访问层来优化存储成本，请选择S3 智能分层. 有关 S3 智能分层存储类的更多信息，请参阅。可自动优化经常访问和不经常访问的对象的存储类中的Amazon Simple Storage Service 用户指南.
    - 要将您不常访问的对象数据冗余存储在地理上分开的多个可用区中，选择S3 标准 – IA. 有关 S3 标准 — IA 存储类的更多信息，请参阅不经常访问对象的存储类中的Amazon Simple Storage Service 用户指南.
    - 要将您不常访问的对象数据存储在单个可用区中，选择S3 单区-IA. 有关 S3 单区 — IA 存储类的更多信息，请参阅不经常访问对象的存储类中的Amazon Simple Storage Service 用户指南.

    为了帮助监控 S3 账单，请使用AWS Trusted Advisor. 有关更多信息，请参阅 。监控工具中的Amazon Simple Storage Service 用户指南.
15. 对于对象元数据，选择要使用的元数据：

    - 要根据文件扩展名猜测已上传对象的 MIME 类型，请选择猜 MIME 类型.
    - 要向映射到 SMB 文件共享的 S3 存储桶的所有者授予完全控制权限，请选择让存储桶拥有者完全控制. 有关使用文件共享来访问其他账户拥有的存储桶中的对象的更多信息，请参阅使用文件共享进行跨账户访问.
    - 要向映射到 SMB 文件共享的 S3 存储桶的所有者授予完全控制权限，请选择启用申请者付款. 有关更多信息，请参阅申请方付款存储桶。
16. 适用于访问您的 S3 存储桶的访问，选择AWS Identity and Access Management(IAM) 角色，您希望文件网关用来访问您的 Amazon S3 存储桶：

    - 要使文件网关能够代表您创建新的 IAM 角色和访问策略，请选择创建新的 IAM 角色. 如果文件共享使用接入点别名连接到 Amazon S3，则此选项不可用。
    - 要选择现有的 IAM 角色并手动设置访问策略，请选择使用现有的 IAM 角色. 如果您的文件共享使用接入点别名连接到 Amazon S3，则必须使用此选项。在IAM 角色框中，输入用于访问您的

存储桶的角色的 Amazon 资源名称 (ARN)。有关 IAM 角色的信息，请参阅。IAM 角色中的AWS Identity and Access Management用户指南.

有关 S3 存储桶访问权限的更多信息，请参阅授予对 Amazon S3 存储桶的访问权限。

17. 适用于加密选择要用于加密文件网关在 Amazon S3 中存储的对象的加密密钥类型：

    - 若要使用由 Amazon S3 托管的服务器端加密 (SSE-S3)，请选择S3 托管密钥 (SSE-S3).
    - 若要使用托管的服务器端加密AWS Key Management Service（SSE-KMS），选择KMS 托管的密钥 (SSE-KMS). 在主键对话框中，选择现有AWS KMS key或者选择创建新的 KMS 密钥在中创建新的 KMS 密钥AWS Key Management Service(AWS KMS) 控制台。有关 的更多信息AWS KMS请参阅,是什么AWS Key Management Service?中的AWS Key Management Service开发人员指南.

    > **Note**
    >
    > 要指定AWS KMS带有未列出别名的 key 或使用AWS KMS来自不同的钥匙AWS 账户，您必须使用AWS Command Line Interface(AWS CLI)。有关更多信息，请参阅 。CreateNFSFileShare中的AWSStorage Gateway API 参考.
    > 不支持非对称 KMS 密钥。

18. 选择下一步。这些区域有：文件访问设置此时将显示页。
19. 适用于验证方法中，选择要使用的身份验证方法。

    - 要使用企业 Microsoft AD 对 SMB 文件共享进行经过身份验证的访问，请选择Active Directory. 您的文件网关必须加入域。
    - 要仅提供访客访问权限，请选择访客访问. 如果您选择此身份验证方法，您的文件网关不必是 Microsoft AD 域的一部分。您还可以使用作为 AD 域成员的文件网关来创建具有来宾访问权限的文件共享。您必须在相应的字段中为 SMB 服务器设置来宾密码。

    > **Note**
    >
    > 这两种访问类型同时可用。

20. 在SMB 共享设置部分中，选择您的设置。

    对于 Export as (导出为)，选择以下选项之一：

- Read-write (读写) (默认值)
- Read-only

> **Note**
>
> 对于装载在 Microsoft Windows 客户端上的文件共享，如果你选择Read-only，您可能会看到有关某个错误阻止您创建文件夹的消息。您可以忽略此消息。

对于 File/directory access controlled by (文件/目录访问控制方式)，选择下列选项之一：

- 要为 SMB 文件共享中的文件和文件夹设置精细控制权限，请选择Windows 访问控制列表. 有关更多信息，请参阅使用 Microsoft Windows ACL 控制对 SMB 文件共享的访问。
- 要使用 POSIX 权限控制对通过 NFS 或 SMB 文件共享存储的文件和目录的访问，请选择POSIX 权限.

如果你的身份验证方法是Active Directory，对于管理员用户/组中，输入 AD 用户和组的逗号分隔列表。如果您希望管理员用户有权更新文件共享中所有文件和文件夹的访问控制列表 (ACL)，请执行此操作。之后，这些用户和组将具有文件共享的管理员权限。组的前缀必须为@例如，角色，`@group1`.

适用于区分大小写中，选择以下选项之一：

- 要允许网关控制区分大小写，请选择客户端指定.
- 要允许客户控制区分大小写，请选择强制区分大小写.

> **Note**
>
> - 如果选中此选项，此设置将立即应用于新的 SMB 客户端连接。现有的 SMB 客户端连接必须断开与文件共享的连接，然后重新连接才能使设置生效。

适用于基于访问的枚举中，选择以下选项之一：

- 要使共享中的文件和文件夹仅对具有读取权限的用户可见，请选择对文件和目录禁用.

- 要在目录枚举期间使共享上的文件和文件夹对所有用户都可见，请选择为文件和目录启用.

> **Note**
>
> 基于访问的枚举是一种系统，它根据共享的访问控制列表 (ACL) 筛选 SMB 文件共享上的文件和文件夹枚举。

适用于机会主义锁（oplock）中，选择以下选项之一：

- 要允许文件共享使用机会锁定来优化文件缓冲策略，请选择Enabled (已启用). 在大多数情况下，启用机会锁定可以提高性能，特别是在 Windows 上下文菜单方面。
- 要防止使用机会锁定，请选择Disabled. 如果环境中的多个 Windows 客户端频繁同时编辑相同的文件，那么禁用机会锁定有时可以提高性能。

> **Note**
>
> 对于涉及在不同情况下访问同名文件的工作负载，建议不要对区分大小写的共享启用机会锁定。

21. （可选）在用户和组文件共享访问部分中，选择您的设置。

    适用于允许的用户和组，选择添加允许用户要么添加允许组输入要允许文件共享访问的 AD 用户或组。重复此过程可根据需要允许尽可能多的用户和组。

    适用于被拒绝的用户和组，选择添加拒绝用户要么添加拒绝组输入要拒绝文件共享访问的 AD 用户或组。重复此过程可根据需要拒绝尽可能多的用户和组。

    > **Note**
    >
    > 这些区域有：用户和组文件共享访问仅在以下情况下才会Active Directory已选择。
    > 仅输入 AD 用户或组名称。域名由网关加入的特定 AD 中的网关成员资格表示。
    > 如果您未指定任何允许或拒绝的用户或组，任何经过身份验证的 AD 用户都可以导出文件共享。

22. 选择下一步。
23. 检查文件共享配置设置，然后选择Finish.

在创建 SMB 文件共享之后，您可以在文件共享的 Details (详细信息) 选项卡中查看文件共享设置。

下一步

在客户端上装载您的 SMB 文件共享

装载并使用您的文件共享

在下文中，您可以找到有关如何在客户端上装载您的文件共享，测试文件网关以及根据需要清理资源的说明。有关支持的网络文件系统 (NFS) 客户端的更多信息，请参阅文件网关支持的 NFS 客户端。有关支持的服务消息块 (SMB) 客户端的更多信息，请参阅文件网关支持的 SMB 客户端。

您可以在 AWS Management Console中找到挂载您的文件共享的示例命令。在以下部分中，您可以找到有关如何在客户端上挂载文件共享，使用共享，测试文件网关以及根据需要清理资源的详细信息。

主题

在客户端上装载 NFS 文件共享

现在，您在客户端驱动器上挂载了 NFS 文件共享并将其映射到您的 Amazon S3 存储桶。

装载文件共享并将其映射到 Amazon S3 存储桶

1. 如果您使用 Microsoft Windows 客户端，建议您创建 SMB 文件共享并使用已在 Windows 客户端上安装的 SMB 客户端访问它。如果使用 NFS，请在 Windows 中开启 NFS 的服务。
2. 挂载 NFS 文件共享：

   - 对于 Linux 客户端，请在命令提示符下键入以下命令：

     ```
     sudo mount -t nfs -o nolock,hard [Your gateway VM IP address]:/[S3 bucket name] [mount path on your client]
     ```

   - 对于 MacOS 客户端，请在命令提示符下键入以下命令：

     ```
     sudo mount_nfs -o vers=3,nolock,rwsize=65536,hard -v [Your gateway VM IP address]:/[S3 bucket name] [mount path on your client]
     ```

   - 对于 Windows 客户端，请在命令提示符下键入以下命令：

```
mount -o nolock -o mtype=hard [Your gateway VM IP address]:/[S3 bucket name] [Drive letter on your windows client]
```

例如，假设在 Windows 客户端上，您的 VM 的 IP 地址是 123.123.1.2，Amazon S3 存储桶名称是`test-bucket`. 还假设要映射到驱动器 T。在这种情况下，您的命令应如下所示。

```
mount -o nolock -o mtype=hard 123.123.1.2:/test-bucket T:
```

> **Note**
>
> 在装载文件共享时，请注意事项：
>
> - 您可能会遇到 Amazon S3 存储桶中存在文件夹和对象并且名称相同的情况。在这种情况下，如果对象名称不包含尾部斜杠，则只有文件夹在文件网关中可见。例如，如果存储桶包含名为的对象`test`要么`test/`以及名为的文件夹`test/test1`，仅限`test/`和`test/test1`在文件网关中可见。
> - 在重新启动客户端之后，您可能需要重新装载文件共享。
> - 默认情况下，Windows 使用软装载来装载您的 NFS 共享。当存在连接问题时，软装载更容易超时。我们建议使用硬装载，因为硬装载更安全，并可以更好地保存您的数据。软装载命令会省略 **`-o mtype=hard`** 开关。Windows 硬装载命令使用 `-o mtype=hard` 开关。
> - 如果您使用的是 Windows 客户端，请在通过不含选项的 `mount` 命令进行装载后检查您的 `mount` 选项。该响应应确认使用提供的最新选项装载文件共享。它还应在确认您未在使用缓存的旧条目，这需要至少 60 秒才能清除。

下一步

测试 S3 文件网关

在客户端上装载您的 SMB 文件共享

现在，您挂载了 SMB 文件共享并将其映射到可供客户端访问的驱动器。控制台的文件网关部分显示了可用于 SMB 客户端的受支持挂载命令。接下来，您可以找到一些其他选项进行尝试。

您可以使用几种不同的方法来挂载 SMB 文件共享，包括：

- 命令提示符 (cmdkey和net use) — 使用命令提示符挂载您的文件共享。使用存储您的凭据cmdkey，然后用安装驱动器net use并包括/persistent:yes和/savecred如果您希望连接在系统重新之后保持不变，请参阅。您使用的具体命令将会有所不同，具体取决于您是否要装载驱动器以便 Microsoft Active Directory (AD) 访问或来宾用户访问。示例如下。
- 文件资源管理器（映射网络驱动器）— 使用 Windows 文件资源管理器挂载文件共享。配置设置以指定是否希望连接在系统重新启动过程中保留并提示输入网络凭据。
- PowerShell 脚本 — 创建自定义 PowerShell 脚本以挂载文件共享。根据您在脚本中指定的参数，连接可以在系统重新之后保持不变，并且在装载后可以对操作系统可见或不可见。

> **Note**
>
> 如果您是 Microsoft AD 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。
> 如果您是来宾用户，请在尝试挂载文件共享之前确保您拥有来宾用户账户密码。

使用命令提示符为授权 Microsoft AD 用户挂载您的 SMB 文件共享，请执行以下操作：

1. 在将 SMB 文件共享挂载到该用户的系统之前，请确保 Microsoft AD 用户对 SMB 文件共享有必要的权限。
2. 在命令提示符处，输入以下命令以装载文件共享：

```
net use WindowsDriveLetter: \\GatewayIPAddress\FileShareName /
persistent:yes
```

使用命令提示符使用特定的用户名和密码组合挂载 SMB 文件共享：

1. 在将 SMB 文件共享挂载到系统之前确保该用户帐户有权访问该文件共享。
2. 在命令提示符处，输入以下命令以在 Windows 凭据管理器中保存用户凭据：

```
cmdkey /add:GatewayIPAddress /user:DomainName\UserName /pass:Password
```

3. 在命令提示符处，输入以下命令以装载文件共享：

```
net use WindowsDriveLetter: \\GatewayIPAddress\FileShareName /
persistent:yes /savecred
```

使用命令提示符为来宾用户挂载您的 SMB 文件共享：

1. 在挂载文件共享之前确保您拥有来宾用户账户密码。
2. 在命令提示符处，键入以下命令以在 Windows 凭据管理器中保存来宾凭据：

   ```
   cmdkey /add:GatewayIPAddress /user:DomainName\smbguest /pass:Password
   ```

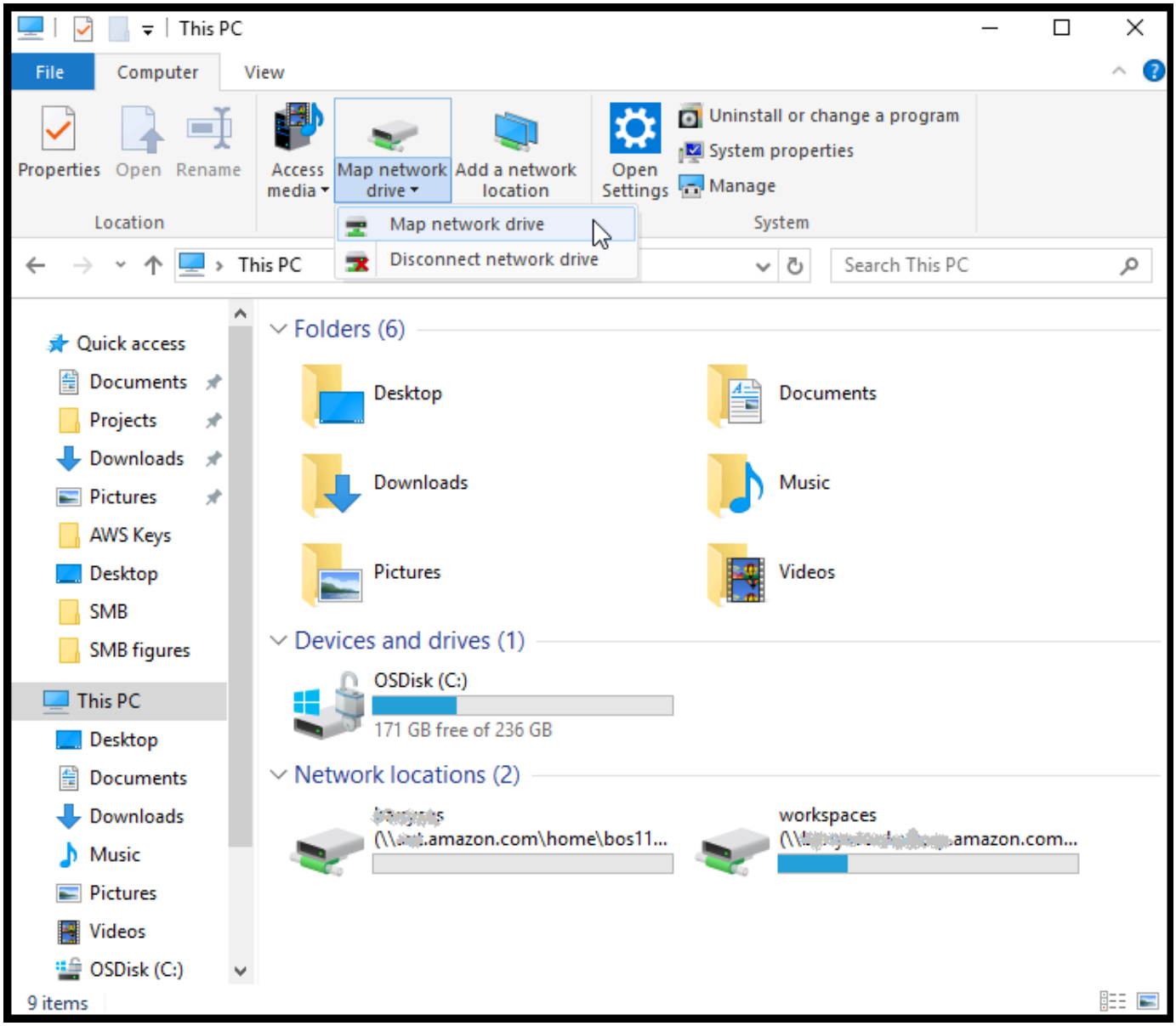
3. 在命令提示符处，键入以下命令。

   ```
   net use WindowsDriveLetter: \\$GatewayIPAddress\$Path /user:$GatewayID\smbguest /persistent:yes /savecred
   ```

> **Note**
>
> 在装载文件共享时，请注意事项：
>
> - 您可能会遇到 Amazon S3 存储桶中存在文件夹和对象并且名称相同的情况。在这种情况下，如果对象名称不包含尾部斜杠，则只有文件夹在文件网关中可见。例如，如果存储桶包含名为的对象`test`要么`test/`以及名为的文件夹`test/test1`，仅限`test/`和`test/test1`在文件网关中可见。
> - 除非您将文件共享连接配置为保存用户凭据并在系统重启期间持续存在，否则每次重新启动客户端系统时，您可能需要重新装载文件共享。

使用 Windows File Explorer 挂载 SMB 文件共享

1. 按 Windows 键并键入**File Explorer**中的搜索窗口框，或者按**Win+E**.
2. 在导航窗格中，选择此 PC，然后为计算机选项卡中的映射网络驱动器选择映射网络驱动器，如以下屏幕截图所示。



3. 在 Map Network Drive (映射网络驱动器) 对话框中，为 Drive (驱动器) 选择驱动器号。
4. 对于 Folder (文件夹)，键入 ***\\[File Gateway IP]\[SMB File Share Name]***，或者选择 Browse (浏览) 以从对话框中行您的 SMB 文件共享。
5. （可选）如果您希望装载点在重启后保留，请选择 Reconnect at sign-up (登录时重新连接)。
6. （可选）如果您希望用户输入 Microsoft AD 登录或来宾账户用户密码，请选择 Connect using different credentials (使用其他凭证连接)。
7. 选择 Finish (完成) 以完成您的装载点。

您可以通过 Storage Gateway 管理控制台编辑文件共享设置、编辑允许和拒绝的用户和组以及更改来宾访问密码。您还可以通过控制台刷新文件共享缓存中的数据和删除文件共享。

修改 SMB 文件共享的属性

1. 在中打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
2. 在导航窗格上，选择 File Shares (文件共享)。
3. 在 File Share (文件共享) 页面上，根据要修改的 SMB 文件共享选中复选框。
4. 对于 Actions (操作)，选择所需的操作：
   - 选择 Edit file share settings (编辑文件共享设置) 以修改共享访问。
   - 选择 Edit allowed/denied users (编辑允许/拒绝的用户) 以添加或删除用户和组，然后将允许和拒绝的用户和组键入到 Allowed Users (允许的用户)、Denied Users (拒绝的用户)、Allowed Groups (允许的组) 和 Denied Groups (拒绝的组) 框。使用 Add Entry (添加条目) 按钮创建新访问权限，使用 (X) 按钮删除访问权限。
5. 完成后，选择 Save。

   当您输入允许的用户和组时，您将创建一个允许列表。如果没有允许列表，所有经过身份验证的 Microsoft AD 用户都可以访问 SMB 文件共享。标记为 “被拒绝” 的任何用户和组都将被添加到拒绝列表并且无法访问 SMB 文件共享。在某个用户或组同时位于拒绝列表和允许列表中的情况下，拒绝列表的优先级将更高。

   您可以在 SMB 文件共享上启用访问控制列表 (ACL)。有关如何启用 ACL 的信息，请参阅使用 Microsoft Windows ACL 控制对 SMB 文件共享的访问。

下一步

测试 S3 文件网关

在具有预先存在的对象的存储桶上处理文件共享

您可以使用 NFS 或 SMB，借助在文件网关外部创建的对象导出 Amazon S3 存储桶上的文件共享。在网关外部创建的存储桶中的对象将显示为 NFS 或 SMB 文件系统中的文件（当文件系统客户端访问这些对象时）。标准可移植操作系统接口 (POSIX) 访问和权限将在文件共享中使用。当您将文件写回 Amazon S3 存储桶时，文件将采用您为其提供的属性和访问权限。

您可以随时将对象上传到 S3 存储桶。对于要将这些新添加的对象显示为文件的文件共享，您需要先刷新 S3 存储桶。有关更多信息，请参阅the section called “刷新您的 Amazon S3 存储桶中的对象”。

> **Note**
>
> 我们建议不要对一个 Amazon S3 存储桶使用多个写入器。如果要这样做，请务必阅读 “我是否能拥有多个写入器到我的 Amazon S3 存储桶的写入器？” 部分 中的Storage Gateway 常见问.

要将元数据默认值分配给使用 NFS 访问的对象，请参阅管理您的 Amazon S3 文件网关中的“编辑元数据默认值”。

对于 SMB，您可以使用预先存在的对象，借助 Amazon S3 存储桶的 Microsoft AD 或来宾访问导出共享。通过 SMB 文件共享导出的对象会继承其正上方的父目录中的 POSIX 所有权和权限。对于根文件夹下的对象，将继承根访问控制列表 (ACL)。对于根 ACL，所有者为 `smbguest`，文件的权限为 666，而且目录为 777。这适用于所有形式的经过身份验证的访问（Microsoft AD 和来宾）。

测试 S3 文件网关

您可以将文件和文件夹复制到映射驱动器。这些文件会自动上传到您的 Amazon S3 存储桶。

从 Windows 客户端上传文件到 Amazon S3

1. 在 Windows 客户端上，导航到您装载了文件共享的驱动器。驱动器名称前面是您的 S3 存储桶的名称。
2. 将文件或文件夹复制到该驱动器。
3. 在 Amazon S3 管理控制台上，导航到您映射的存储桶。您应该看到在您指定的 Amazon S3 存储桶中复制的文件和文件夹。

   您可以在中看到您在中创建的文件共享。文件共享在中的选项卡AWSStorage Gateway 管理控制台。

您的 NFS 或 SMB 客户端可以写入、读取、删除、重命名和截断文件。

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

请注意关于文件网关如何与 S3 协同工作的几个要点：

- 读取数据通过读通缓存提供。换句话说，如果数据不可用，将从 S3 中获取数据并添加到缓存中。
- 借助回写式缓存，通过经优化的分段上传将写入内容发送到 S3。
- 读取和写入操作经过了优化，因此仅在网络上传输所请求或已修改的部分。
- 从 S3 中删除对象。
- 使用与 Amazon S3 控制台中相同的语法，将目录作为 S3 中的文件夹对象进行管理。您可以重命名空目录。
- 递归文件系统操作性能 (例如 `ls -l`) 取决于存储桶中的对象数。

下一步

接下来该做什么？

接下来该做什么？

在前面的章节中，您创建并开始使用文件网关，包括装载文件共享和测试您的设置。

本指南的其他章节介绍如何进行如下操作：

- 要管理您的文件网关，请参阅管理您的 Amazon S3 文件网关。
- 要优化您的文件网关，请参阅优化网关性能。
- 如需排除网关问题，请参见 排查网关问题。
- 要了解 Storage Gateway 指标以及如何监控网关运行情况，请参阅。

清除不需要的资源

如果您作为示例练习或测试创建了网关，请考虑将其清除以避免产生意外或不必要的费用。

清除不需要的资源

1. 除非您计划继续使用网关，否则请将其删除。有关更多信息，请参阅使用 AWS Storage Gateway 控制台删除网关并清除相关资源。
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。

在 Virtual Private Cloud Cloud 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。然后，您可以使用软件设备将数据传输到AWS没有网关与之通信的存储AWS通过公共 Internet 提供存储服务。使用亚马逊 VPC 服务，您可以启动AWS自定义虚拟网络中的资源。可以使用 Virtual Private Cloud (VPC) 控制您的网络设置，例如 IP 地址范围、子网、路由表和网络网关。有关 VPC 的更多信息，请参阅Amazon VPC 是什么？中的Amazon VPC User Guide.

要将网关与 VPC 中的 Storage Gateway VPC 终端节点结合使用，请执行以下操作：

- 使用 VPC 控制台为 Storage Gateway 创建 VPC 终端节点并获取 VPC 终端节点 ID。在创建和激活网关时指定此 VPC 终端节点 ID。
- 如果您正在激活文件网关，请为 Amazon S3 创建 VPC 终端节点。为网关创建文件共享时指定此 VPC 终端节点。
- 如果您正在激活文件网关，则在文件网关 VM 本地控制台中设置和配置它。对于基于管理程序的本地文件网关，例如基于 VMware、Microsoft HyperV 和基于 Linux 内核的虚拟机 (KVM) 的文件网关，您需要此代理。在这些情况下，您需要代理才能使网关从 VPC 外部访问 Amazon S3 私有终端节点。有关如何配置 HTTP 代理的信息，请参阅配置 HTTP 代理。

> **Note**
>
> 必须在创建 VPC 终端节点的同一区域中激活您的网关。
> 对于文件网关，为文件共享配置的 Amazon S3 存储必须位于为 Amazon S3 创建 VPC 终端节点的同一区域中。

主题

为 Storage Gateway 创建 VPC 终端节点

按照这些说明创建 VPC 终端节点。如果您已有一个用于 Storage Gateway 的 VPC 终端节点，则可使用该终端节点。

为 Storage Gateway 创建 VPC 终端节点

1. 登录到 AWS Management Console，然后通过以下网址打开 Amazon VPC 控制台：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. 在存储库的创建终端节点页面上，选择AWS服务为了服务类别.
4. 对于 Service Name (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 Enable Private DNS Name (启用私有 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Create endpoint。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 DNS Names (DNS 名称) 部分中，使用第一个未指定可用区的 DNS 名称。您的 DNS 名称类似这样：`vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

现在，您有了 VPC 终端节点，可以创建您的网关。

> **Important**
>
> 如果您正在创建文件网关，则还需为 Amazon S3 创建终端节点。执行上面的 “为 Storage Gateway 创建 VPC 终端节点” 部分中所示的相同步骤，但选择`com.amazonaws.us-east-2.s3`而是在 “服务名称” 下。然后，选择您希望与 S3 终端节点关联的路由表，而不是子网/安全组。有关说明，请参阅创建网关终端节点.

设置和配置 HTTP 代理（仅限本地文件网关）

如果您正在激活文件网关，则需使用文件网关 VM 本地控制台设置和配置 HTTP 代理。本地文件网关需要此代理才能从 VPC 外部访问 Amazon S3 私有终端节点。如果您在 Amazon EC2 中已有一个 HTTP 代理，则可使用该代理。不过，您需要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

如果您没有 Amazon EC2 代理，请使用以下过程设置和配置 HTTP 代理。

设置代理服务器

1. 启动 Amazon EC2 Linux AMI。我们建议您使用经过网络优化的实例系列，例如 c5n.large。
2. 使用以下命令安装 squid：**`sudo yum install squid`**. 这样做会在中创建一个默认配置文件/`etc/squid/squid.conf`.
3. 将此配置文件的内容替换为以下内容。

```
#
# Recommended minimum configuration:
#

# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
acl localnet src 10.0.0.0/8             # RFC1918 possible internal network
acl localnet src 172.16.0.0/12       # RFC1918 possible internal network
acl localnet src 192.168.0.0/16    # RFC1918 possible internal network
acl localnet src fc00::/7       # RFC 4193 local private network range
acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machines

acl SSL_ports port 443
acl SSL_ports port 1026
acl SSL_ports port 1027
```

```
acl SSL_ports port 1028
acl SSL_ports port 1031
acl SSL_ports port 2222
acl CONNECT method CONNECT

#
# Recommended minimum Access Permission configuration:
#
# Deny requests to certain unsafe ports
http_access deny !SSL_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet
http_access allow localhost

# And finally deny all other access to this proxy
http_access deny all

# Squid normally listens to port 3128
http_port 3128

# Leave coredumps in the first cache dir
coredump_dir /var/spool/squid

#
# Add any of your own refresh_pattern entries above these.
#
refresh_pattern ^ftp:                    1440       20%        10080
refresh_pattern ^gopher:            1440       0%          1440
refresh_pattern -i (/cgi-bin/|\?) 0             0%          0
refresh_pattern .                              0              20%        4320
```

4. 如果您不需要锁定代理服务器，也不需要进行任何更改，请使用以下命令启用并启动代理服务器。这些命令会在服务器引导时启动服务器。

```
sudo chkconfig squid on
sudo service squid start
```

您现在可以为 Storage Gateway 配置 HTTP 代理以使用它。在配置网关以使用代理时，请使用默认 squid 端口 3128。生成的 squid.conf 文件默认涵盖以下必需的 TCP 端口：

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

使用 VM 本地控制台配置 HTTP 代理

1. 登录到网关的 VM 本地控制台。有关如何登录的信息，请参阅登录文件网关本地控制台。
2. 在主菜单中，选择 Configure HTTP proxy (配置 HTTP 代理)。
3. 在 Configuration (配置) 菜单中，选择 Configure HTTP proxy (配置 HTTP 代理)。
4. 提供代理服务器的主机名和端口。

有关如何配置 HTTP 代理的详细信息，请参阅配置 HTTP 代理。

允许流量到达 HTTP 代理中所需端口

如果您使用 HTTP 代理，请确保您允许流量从 Storage Gateway 到达以下列出的目的地和端口。

当通过公共终端节点进行通信时，它将与以下 Storage Gateway 服务进行通信。

```
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
storagegateway.region.amazonaws.com:443 (Required for making API calls)
s3.region.amazonaws.com (Required only for File Gateway)
```

> **Important**
>
> 取决于你的网关AWS地区，替换##在终端节点中与相应的区域字符串相应。例如，如果您在美国西部（俄勒冈）区域创建网关，则该终端节点如下所示：`storagegateway.us-west-2.amazonaws.com:443`.

当通过 VPC 终端节点进行通信时，它将与AWS通过 Storage Gateway VPC 终端节点上的多个端口和 Amazon S3 私有终端节点上的端口 443 提供服务。

- Storage Gateway VPC 终端节点上的 TCP 端口。
  - 443、1026、1027、1028、1031 和 2222
- S3 私有终端节点上的 TCP 端口
  - 443

管理您的 Amazon S3 文件网关

在下文中，您可以找到有关如何管理 Amazon S3 文件网关资源的信息。

主题

添加文件共享

在激活和运行 S3 文件网关后，您可以添加额外的文件共享并为其授予 Amazon S3 存储桶访问权。您可以授权访问的存储桶包括在不同的存储桶中AWS 账户比文件共享。有关如何添加文件共享的信息，请参阅创建文件共享。

主题

授予对 Amazon S3 存储桶的访问权限

创建文件共享时，文件网关需要访问将文件上传到 Amazon S3 存储桶，以及对用于连接到存储桶的任何接入点或虚拟私有云 (VPC) 终端节点执行操作的访问权限。要授予此访问权限，您的文件网关假定 AWS Identity and Access Management(IAM) 角色，该角色与授予此访问权限的 IAM 策略关联。

该角色需要此 IAM 策略以及与之有关的安全令牌服务 (STS) 信任关系。此策略确定了该角色可以执行的操作。此外，您的 S3 存储桶和任何关联的访问点或 VPC 终端节点都必须具有允许 IAM 角色访问它们的访问策略。

您可以自行创建该角色和访问策略，也可以让文件网关为您创建。如果文件网关为您创建该策略，该策略将包含 S3 操作列表。有关角色和权限的信息，请参阅。创建向AWS 服务中的IAM 用户指南.

下面是一个信任策略示例，该策略允许文件网关代入 IAM 角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "storagegateway.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

如果您不希望文件网关代表您创建策略，则可以创建自己的策略并将它附加到文件共享。有关此操作的详细信息，请参阅 创建文件共享。

以下示例策略允许文件网关执行策略中列出的所有 Amazon S3 操作。语句的第一部分允许对名为 `TestBucket` 的 S3 存储桶执行列出的所有操作。第二部分允许对 `TestBucket` 中的所有对象执行列出的操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetAccelerateConfiguration",
                "s3:GetBucketLocation",
                "s3:GetBucketVersioning",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:ListBucketMultipartUploads"
            ],
```

```
            "Resource": "arn:aws:s3:::TestBucket",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectVersion",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::TestBucket/*",
            "Effect": "Allow"
        }
    ]
}
```

以下示例策略与前面的示例策略类似，但允许您的文件网关执行通过访问点访问存储桶所需的操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectVersion",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:us-east-1:123456789:accesspoint/
TestAccessPointName/*",
            "Effect": "Allow"
        }
    ]
```

```
}
```

> **Note**
>
> 如果您需要通过 VPC 终端节点将文件共享连接到 S3 存储桶，请参阅Amazon S3 终端节点策略中的AWS PrivateLink用户指南.

跨服务混淆代理问题防范

混淆代理问题是一个安全性问题，即不具有操作执行权限的实体可能会迫使具有更高权限的实体执行该操作。在 AWS 中，跨服务模拟可能会导致混淆代理问题。当一项服务（调用服务）调用另一项服务（被调用服务）时，可能会发生跨服务模拟。可以操纵调用服务，使用其权限以在其他情况下该服务不应有访问权限的方式对另一个客户的资源进行操作。为防止这种情况，AWS 提供可帮助您保护所有服务的数据的工具，而这些服务中的服务委托人有权限访问账户中的资源。

我们建议使用资源策略中的 `aws:SourceArn` 和 `aws:SourceAccount` 全局条件上下文键，限制 AWS Storage Gateway 为另一项服务提供的资源访问权限。如果使用两个全局条件上下文键，在同一策略语句中使用时，`aws:SourceAccount` 值和 `aws:SourceArn` 值中的账户必须使用相同的账户 ID。

的价值`aws:SourceArn`必须是与文件共享关联的 Storage Gateway 的 ARN。

防范混乱的副手问题的最有效方法是使用`aws:SourceArn`具有资源的完整 ARN 的全局条件上下文键。如果您不知道资源的完整 ARN，或者您要指定多个资源，请使用`aws:SourceArn`带通配符的全局上下文条件键 (*) 对于 ARN 的未知部分。例如 `arn:aws:`*`servicename`*`::`*`123456789012`*`:*`。

以下示例显示如何使用`aws:SourceArn`和`aws:SourceAccount`Storage Gateway 中的全局条件上下文键，以防止混淆的副问题。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "storagegateway.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
```

```
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:storagegateway:us-east-1:123456789012:gateway/
sgw-712345DA"
        }
      }
    }
  ]
}
```

使用文件共享进行跨账户访问

跨账户当 Amazon Web Services 账户和该账户的用户获得了对属于其他 Amazon Web Services 账户的资源的访问权限时，访问权限便出现了。有了文件网关，您可以使用一个 Amazon Web Services 账户中的文件共享访问属于另一个 Amazon Web Services 账户的 Amazon S3 存储桶中的对象。

使用一个 Amazon Web Services 账户拥有的文件共享访问另一个 Amazon Web Services 账户中的 S3 存储桶

1. 确保 S3 存储桶拥有者授予 Amazon Web Services 账户访问您需要访问的 S3 存储桶和该存储桶中的对象的访问权限。有关如何授予此访问权限的信息，请参阅。示例 2：为了授予跨账户存储桶权限中的Amazon Simple Storage Service 用户指南. 有关所需权限的列表，请参阅授予对 Amazon S3 存储桶的访问权限。
2. 确保您的文件共享用来访问 S3 存储桶的 IAM 角色包含 `s3:GetObjectAcl` 和 `s3:PutObjectAcl` 等操作的权限。此外，确保 IAM 角色包括允许您的账户代入该 IAM 角色的信任策略。有关信任策略的示例，请参阅授予对 Amazon S3 存储桶的访问权限。

   如果您的文件共享使用现有角色来访问 S3 存储桶，您应包含 `s3:GetObjectAcl` 和 `s3:PutObjectAcl` 操作的权限。IAM 角色还需要一个允许您的帐户带入此角色的信任策略。有关信任策略的示例，请参阅授予对 Amazon S3 存储桶的访问权限。
3. 打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
4. 在配置文件共享设置对话框的对象元数据设置中，选择给予存储桶拥有者完全控制权限。

在为跨账户访问权限创建或更新文件共享并在本地挂载该文件共享后，我们强烈建议您测试设置。为此，您可以列出目录内容或者编写测试文件并确保这些文件在 S3 存储桶中显示为对象。

> **Important**
>
> 确保设置正确的策略以授予跨账户访问文件共享所使用的账户。如果您未这样做，则通过本地应用程序对文件所做的更新不能传播到您正在使用的 Amazon S3 存储桶。

Resources（资源）

有关访问策略和访问控制列表的更多信息，请参阅以下内容：

有关使用可用访问策略选项的准则中的Amazon Simple Storage Service 用户指南

访问控制列表 (ACL) 概述中的Amazon Simple Storage Service 用户指南

删除文件共享

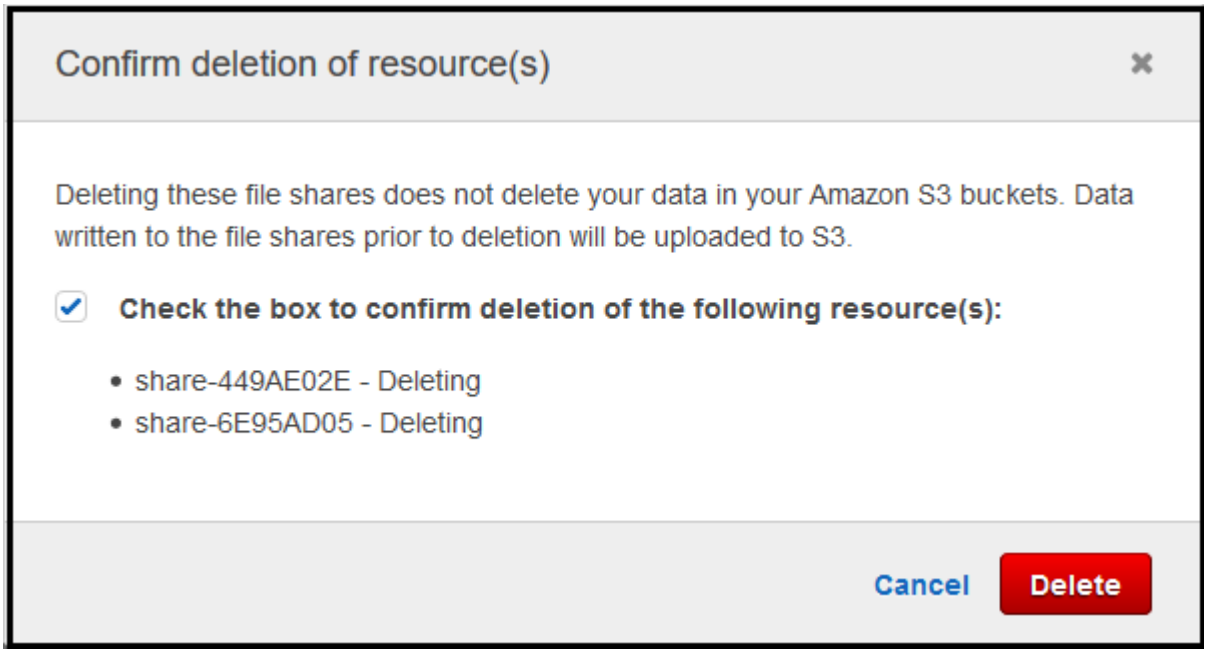
如果您不再需要某个文件共享，可以从 Storage Gateway 控制台将其删除。删除文件共享时，网关会从文件共享映射到的 Amazon S3 存储桶分离。但是，S3 存储桶及其内容不会被删除。

在删除文件共享时，如果网关正在向 S3 存储桶上传数据，则删除过程需要等到所有数据上传完之后才会完成。在数据完全上传之前，文件共享将具有 DELETING 状态。

如果您希望将数据完全上传，请执行紧跟着的删除文件共享步骤。如果您不想等到数据都上传完毕后再删除文件共享，则请参阅本主题稍后的强制删除文件共享步骤。

删除文件共享

1. 打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
2. 选择文件共享，然后选择要删除的文件共享。
3. 对于 Actions，选择 Delete file share。将出现以下确认对话框。



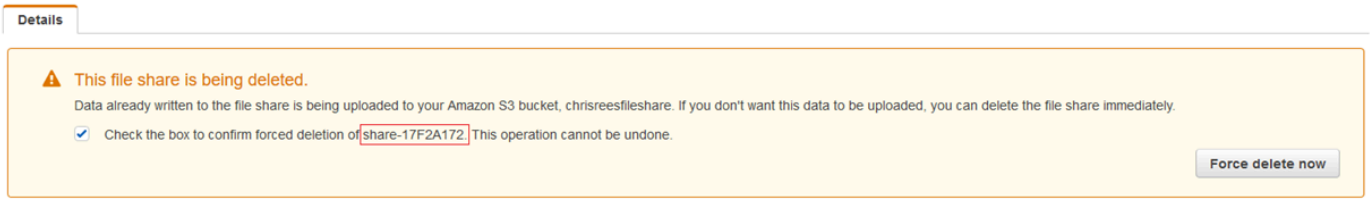
4. 在确认对话框中，选中要删除的文件共享对应的复选框，然后选择 Delete。

在某些情况下，您可能不想等到写入网络文件系统 (NFS) 文件共享上文件的所有数据都上传完毕后再删除文件共享。例如，您可能想要有意放弃已写入但尚未上传的数据。在另一个示例中，支持文件共享的 Amazon S3 存储桶或对象可能已被删除，这意味着无法再上传指定的数据。

在这些情况下，您可以通过使用强制删除文件共享。AWS Management Console或者`DeleteFileShare`API 操作。此操作会中止数据上传过程。执行此操作后，文件共享将进入 FORCE_DELETING 状态。要强制从控制台删除文件共享，请参阅以下过程。

强制删除文件共享

1. 打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
2. 选择文件共享，然后选择要强制删除的文件共享并等待几秒钟。删除消息会显示在 Details 选项卡中。



> **Note**
>
> 您无法撤消强制删除操作。

3. 在详细信息选项卡上显示的消息中，验证要强制删除的文件共享的 ID，选中确认框，然后选择立即强制删除。

您也可以使用 DeleteFileShare API 操作强制删除文件共享。

编辑 NFS 文件共享的设置

您可以编辑 Amazon S3 存储桶的存储类、文件共享名称、对象元数据、壁球级别、导出为和自动缓存刷新设置。

> **Note**
>
> 您无法编辑现有文件共享以指向新存储桶或访问点，也无法修改 VPC 终端节点设置。只有在创建新文件共享时，才能配置这些设置。

编辑文件共享设置

1. 打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
2. 选择 File shares，然后选择要更新的文件共享。
3. 适用于操作，选择编辑共享设置.
4. 执行以下一个或多个操作：
   - （可选）对于文件共享名中，输入文件共享的新名称。
   - 对于 Audit logs (审核日志)，请选择以下选项之一：
     - 选择Disable logging (禁用日志记录)以关闭日志记录。
     - 选择创建新的日志组以创建新的审核日志。
     - 选择使用现有日志组选择，然后从列表中选择现有的审核日志。

     有关审核日志的更多信息，请参阅了解文件网关审核日志。

- （可选）对于从 S3 自动刷新缓存中，选中该复选框，然后设置使用生存时间 (TTL) 刷新文件共享缓存的时间（以天、小时和分钟为单位）。TTL 是自上次刷新以来的时间长度。TTL 时间间隔过后，访问该目录会导致文件网关首先从 Amazon S3 存储桶刷新该目录的内容。
- （可选）对于文件上传通知中，选中 S3 文件网关将文件完全上传到 S3 时收到通知的复选框。设置安置时间以秒为单位来控制客户端在生成文件之前写入文件的最后一个时间点之后等待的秒数`ObjectUploaded`通知功能. 由于客户端可以对文件进行许多小写入，因此最好尽可能长时间设置此参数，以避免在较短的时间段内为同一文件生成多个通知。有关更多信息，请参阅获取文件上传通知。

  > **Note**
  >
  > 此设置不影响对象上传到 S3 的时间，仅影响通知的时间。

- 适用于新对象的存储类选择要用于在 Amazon S3 存储桶中创建的新对象的存储类：
  - 选择 S3 标准将您经常访问的对象数据冗余存储在地理上分开的多个可用区中。有关 S3 标准存储类的更多信息，请参阅。经常访问对象的存储类中的Amazon Simple Storage Service 用户指南.
  - 选择 S3 Intelligent-Tiering (S3 智能分层)，可通过自动将数据移动到最具成本效益的存储访问层来优化存储成本。有关 S3 智能分层存储类的更多信息，请参阅。可自动优化经常访问和不经常访问的对象的存储类中的Amazon Simple Storage Service 用户指南.
  - 选择 S3 标准 - IA 将您不常访问的对象数据冗余存储在地理上分开的多个可用区中。有关 S3 标准 — IA 存储类的更多信息，请参阅。不经常访问对象的存储类中的Amazon Simple Storage Service 用户指南.
  - 选择 S3 单区 - IA 将您不常访问的对象数据存储在单个可用区中。有关 S3 单区 — IA 存储类的更多信息，请参阅。不经常访问对象的存储类中的Amazon Simple Storage Service 用户指南.
- 对于对象元数据，选择要使用的元数据：
  - 选择猜测 MIME 访问类型，启用根据文件扩展名猜测已上传对象的 MIME 类型。
  - 选择 Give bucket owner full control (向存储桶拥有者授予完全控制权限) 以向 S3 存储桶拥有者授予完全控制权限，后者映射到文件的网络文件系统 (NFS) 或服务器消息块 (SMB) 文件共享。有关使用文件共享来访问其他账户拥有的存储桶中的对象的更多信息，请参阅使用文件共享进行跨账户访问。
  - 如果您在要求请求者或读取者（而不是存储桶拥有者）支付访问费用的存储桶上使用此文件共享，请选择启用申请方付款。有关更多信息，请参阅申请方付款存储桶。
- 对于 Squash 级别，选择 NFS 文件共享所需的 Squash 级别设置，然后选择保存。

> **Note**
>
> 您只能为 NFS 文件共享选择一个 Squash 级别设置。SMB 文件共享不使用 Squash 设置。

可能的值包括：

- Root squash (default) - 远程超级用户 (root 用户) 的访问权限将映射到 UID (65534) 和 GID (65534)。
- No root squash – 远程超级用户 (根用户) 以根用户身份接收访问权限。
- All squash – 所有用户访问权限将映射到 UID (65534) 和 GID (65534)。

“Squash level”的默认值为 Root squash。

- 适用于将导出为中，为文件共享选择一个选项。默认值为 Read-write。

> **Note**
>
> 对于安装在 Microsoft Windows 客户端上的文件共享，如果选择Read-only为了将导出为，您可能会看到有关某个意外错误正在阻止您创建文件夹的错误消息。此错误消息是 NFS 版本 3 的已知问题。您可以忽略此消息。

5. 选择 Save (保存)。

编辑 NFS 文件共享的元数据默认值

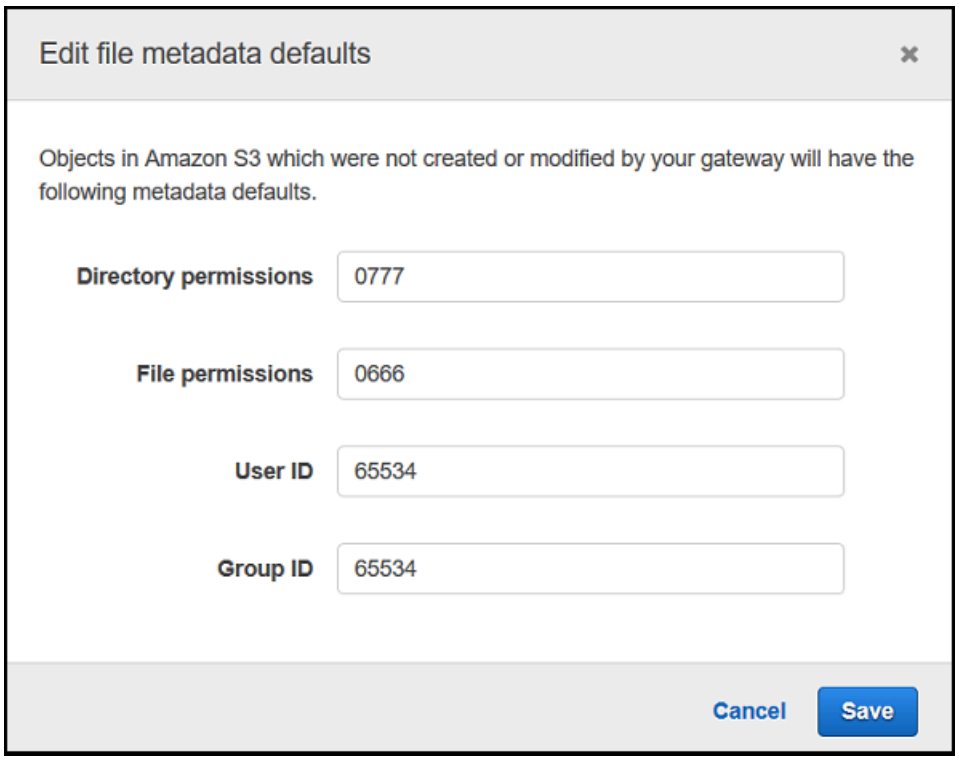
如果您没有为存储桶中的文件或目录设置元数据值，则 S3 文件网关将设置元数据默认值。这些值包括文件和文件夹的 Unix 权限。您可以在 Storage Gateway 控制台中编辑元数据默认值。

当 S3 文件网关在 Amazon S3 中存储文件和文件夹时，Unix 文件权限将存储在对象元数据中。当 S3 文件网关发现 S3 文件网关未存储的对象时，系统会为这些对象分配默认 Unix 文件权限。您可以在下表中找到默认 Unix 权限。

Metadata	描述
目录权限	“nnnn”形式的 Unix 目录模式。例如，“0666”表示文件共享中所有目录的访问模式。默认值是 0777。
文件权限	Unix 文件模式采用“nnnn”形式。例如，“0666”表示文件共享中的文件模式。默认值是 0666。
用户 ID	文件共享中文件的默认所有者 ID。默认值是 65534。
组 ID	文件共享的默认组 ID。默认值是 65534。

编辑元数据默认值

1. 打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
2. 选择 File shares，然后选择要更新的文件共享。
3. 对于 Action，选择 Edit file metadata defaults。
4. 在 Edit file metadata defaults 对话框中，提供元数据信息并选择 Save。



编辑 NFS 文件共享的访问设置

我们建议您为 NFS 文件共享更改允许的 NFS 客户端设置。如果您未这样做，则您网络上的任何客户端均可装载到您的文件共享。

编辑 NFS 访问设置

1. 打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
2. 选择文件共享，然后选择要编辑的 NFS 文件共享。
3. 对于操作，选择编辑共享访问设置。
4. 在编辑允许的客户对话框中，选择添加条目，为要允许的客户端提供 IP 地址或 CIDR 表示法，然后选择Save.

编辑网关的 SMB 设置

网关级 SMB 设置允许您配置网关上 SMB 文件共享的安全策略、Active Directory 身份验证、来宾访问、本地组权限和文件共享可见性。

编辑网关级别 SMB 设置

1. 打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
2. 选择网关选择，然后选择要编辑 SMB 设置的网关。
3. 来自操作选择下拉菜单，选择编辑 SMB 设置选择，然后选择要编辑的设置。

请参阅以下主题了解更多信息。

主题

- 为网关设置安全级别
- 使用 Active Directory 验证用户
- 提供访客访问您的文件共享权限
- 为网关配置本地组
- 设置文件共享可见性

为网关设置安全级别

通过使用 S3 文件网关，您可以指定网关的安全级别。通过指定此安全级别，您可以设置网关是否需要服务器消息块 (SMB) 签名或 SMB 加密，或者您是否要启用 SMB 版本 1。

配置安全级别

1. 打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
2. 选择网关选择，然后选择要编辑 SMB 设置的网关。
3. 来自操作选择下拉菜单，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**
>
> 此设置在 API 参考中称为 `SMBSecurityStrategy`。
> 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，S3 文件网关只允许来自已启用加密的 SMBv3 客户端的连接。对于处理敏感数据的环境，强烈建议使用此选项。此选项适用于 Microsoft Windows 8、Windows Server 2012 或更高版本上的 SMB 客户端。

- 强制签署— 如果选择此选项，S3 文件网关只允许来自已启用签名的 SMBv2 或 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。
- 协商客户端— 如果选择此选项，将根据客户端协商的内容建立请求。当您希望最大程度地提高环境中的各个客户端之间的兼容性时，建议使用此选项。

> **Note**
>
> 对于 2019 年 6 月 20 日之前激活的网关，默认安全级别为 Client negotiated (客户端协商)。
> 对于 2019 年 6 月 20 日及以后激活的网关，默认安全级别为 Enforce encryption (强制加密)。

5. 选择 Save (保存)。

使用 Active Directory 验证用户

要使用企业 Active Directory 对 SMB 文件共享进行经过身份验证的访问，请使用 Microsoft AD 域凭证编辑网关的 SMB 设置。这样做可以使网关加入 Active Directory 域并允许该域的成员访问 SMB 文件共享。

> **Note**
>
> 使用AWS Directory Service创建托管的 Active Directory 域服务AWS Cloud.

可以提供正确密码的任何人都将获得对 SMB 文件共享的来宾访问权限。

您也可以在 SMB 文件共享上启用访问控制列表 (ACL)。有关如何启用 ACL 的信息，请参阅使用 Microsoft Windows ACL 控制对 SMB 文件共享的访问。

启用 Active Directory 身份验证

1. 打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
2. 选择网关选择，然后选择要编辑 SMB 设置的网关。
3. 来自操作下拉菜单中，选择编辑 SMB 设置，然后选择Active Directory 设置.

4. 对于域名，提供您希望网关加入的域。您可以通过使用域的 IP 地址或其组织单位加入域。组织单位 是 Active Directory 细分，可以包含用户、组、计算机和其他组织单位。

> **Note**
>
> 如果您的网关无法加入 Active Directory 目录，请尝试通过 JoinDomain API 操作使用目录的 IP 地址加入。

> **Note**
>
> 当网关从未加入域时，Active Directory status (Active Directory 状态) 显示 Detached (已分离)。

5. 提供域用户名和域密码，然后选择保存。

   您的控制台的网关部分顶部的消息指示您的网关已成功加入您的 AD 域。

将文件共享访问权限限制到特定 AD 用户和组

1. 在 Storage Gateway 控制台中，选择要限制访问的文件共享。
2. 来自操作下拉菜单中，选择编辑文件共享访问设置.
3. 在用户和组文件共享访问权限部分中，选择您的设置。

   适用于允许的用户和组，选择添加允许的用户要么添加允许的组并输入要允许文件共享访问的 AD 用户或组。重复此过程可根据需要允许尽可能多的用户和组。

   适用于被拒绝的用户和组，选择添加拒绝的用户要么添加拒绝组并输入要拒绝文件共享访问的 AD 用户或组。重复此过程可根据需要拒绝尽可能多的用户和组。

> **Note**
>
> 这些区域有：用户和组文件共享访问权限仅在以下情况下才会Active Directory已选择。
> 仅输入 AD 用户或组名称。域名由网关加入的特定 AD 中的网关成员资格表示。
> 如果您未指定任何允许或拒绝的用户或组，任何经过身份验证的 AD 用户都可以导出文件共享。

4. 完成添加条目后，选择保存。

提供访客访问您的文件共享权限

如果您只希望提供来宾访问权限，您的 S3 文件网关不必是 Microsoft AD 域的一部分。您还可以使用作为 AD 域成员的 S3 文件网关来创建具有来宾访问权限的文件共享。在使用来宾访问创建文件共享之前，您需要更改默认密码。

更改来宾访问密码

1. 打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
2. 选择网关选择，然后选择要编辑 SMB 设置的网关。
3. 来自操作下拉菜单中，选择编辑 SMB 设置，然后选择访客访问设置.
4. 适用于访客密码，提供密码，然后选择Save.

为网关配置本地组

本地组设置允许您向 Active Directory 用户或组授予网关上 SMB 文件共享的特殊权限。

您可以使用本地组设置来分配网关管理员权限。网关管理员可以使用共享文件夹 Microsoft 管理控制台管理单元强制关闭已打开和锁定的文件。

> **Note**
>
> 必须至少添加一个网关管理员用户或组，然后才能将网关加入 Active Directory 域。

分配网关管理员

1. 打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
2. 选择网关选择，然后选择要编辑 SMB 设置的网关。
3. 来自操作选择下拉菜单，选择编辑 SMB 设置，然后选择本地组设置.
4. 在本地组设置部分中，选择您的设置。此部分仅适用于使用 Active Directory 的文件共享。

   适用于网关管理员中，添加要授予本地网关管理员权限的 Active Directory 用户和组。每行添加一个用户或组，包括域名。例如 **`corp\Domain Admins`**。要创建额外线，请选择添加新的网关管理员.

> **Note**
>
> 编辑网关管理员断开连接并重新连接所有 SMB 文件共享。

5. 选择保存更改，然后选择继续以确认出现的警告消息。

设置文件共享可见性

在向用户发布共享时，文件共享可见性控制网关上的共享是否可见。

设置文件共享可见性

1. 打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
2. 选择网关选择，然后选择要编辑 SMB 设置的网关。
3. 来自操作下拉菜单中，选择编辑 SMB 设置，然后选择文件共享可见性设置.
4. 适用于可见性状态中，选中该复选框可在向用户发布共享时显示此网关上的共享。将该复选框保持清除状态，以便在向用户发布共享时不会显示此网关上的共享。

编辑 SMB 文件共享的设置

创建 SMB 文件共享后，您可以编辑 Amazon S3 存储桶的存储类、对象元数据、区分大小写、基于访问的枚举、审核日志、自动缓存刷新和导出为文件共享的设置。

> **Note**
>
> 您无法编辑现有文件共享以指向新存储桶或访问点，也无法修改 VPC 终端节点设置。只有在创建新文件共享时，才能配置这些设置。

编辑 SMB 文件共享设置

1. 打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
2. 选择 File shares，然后选择要更新的文件共享。
3. 适用于操作，选择编辑共享设置.
4. 执行以下一个或多个操作：

- （可选）对于文件共享名中，输入文件共享的新名称。
- 对于 Audit logs (审核日志)，请选择以下选项之一：
  - 选择Disable logging (禁用日志记录)以关闭日志记录。
  - 选择创建新的日志组以创建新的审核日志。
  - 选择使用现有日志组选择，然后从列表中选择现有的审核日志。

  有关审核日志的更多信息，请参阅了解文件网关审核日志。
- （可选）对于之后从 S3 自动刷新缓存中，选中该复选框，然后设置使用生存时间 (TTL) 刷新文件共享缓存的时间（以天、小时和分钟为单位）。TTL 是自上次刷新以来的时间长度。TTL 时间间隔过后，访问该目录会导致文件网关首先从 Amazon S3 存储桶刷新该目录的内容。
- （可选）对于文件上传通知中，选中 S3 文件网关将文件完全上传到 S3 时收到通知的复选框。设置安置时间以秒为单位来控制客户端在生成文件之前写入文件的最后一个时间点之后等待的秒数`ObjectUploaded`通知功能. 由于客户端可以对文件进行许多小写入，因此最好尽可能长时间设置此参数，以避免在较短的时间段内为同一文件生成多个通知。有关更多信息，请参阅获取文件上传通知。

  > **Note**
  >
  > 此设置不影响对象上传到 S3 的时间，仅影响通知的时间。

- 适用于新对象的存储类选择要用于在 Amazon S3 存储桶中创建的新对象的存储类：
  - 选择 S3 标准将您经常访问的对象数据冗余存储在地理上分开的多个可用区中。有关 S3 标准存储类的更多信息，请参阅。经常访问对象的存储类中的Amazon Simple Storage Service 用户指南.
  - 选择 S3 Intelligent-Tiering (S3 智能分层)，可通过自动将数据移动到最具成本效益的存储访问层来优化存储成本。有关 S3 智能分层存储类的更多信息，请参阅。可自动优化经常访问和不经常访问的对象的存储类中的Amazon Simple Storage Service 用户指南.
  - 选择 S3 标准 - IA 将您不常访问的对象数据冗余存储在地理上分开的多个可用区中。有关 S3 标准 — IA 存储类的更多信息，请参阅。不经常访问对象的存储类中的Amazon Simple Storage Service 用户指南.
  - 选择 S3 单区 - IA 将您不常访问的对象数据存储在单个可用区中。有关 S3 单区 — IA 存储类的更多信息，请参阅。不经常访问对象的存储类中的Amazon Simple Storage Service 用户指南.
- 对于对象元数据，选择要使用的元数据：

- 选择猜测 MIME 访问类型，启用根据文件扩展名猜测已上传对象的 MIME 类型。
- 选择 Give bucket owner full control (向存储桶拥有者授予完全控制权限) 以向 S3 存储桶拥有者授予完全控制权限，后者映射到文件的网络文件系统 (NFS) 或服务器消息块 (SMB) 文件共享。有关使用文件共享访问其他账户拥有的存储桶中的对象的更多信息，请参阅使用文件共享进行跨账户访问.
- 如果您在要求请求者或读取者（而不是存储桶拥有者）支付访问费用的存储桶上使用此文件共享，请选择启用申请方付款。有关更多信息，请参阅申请方付款存储桶。

- 适用于将导出为中，为文件共享选择一个选项。默认值为 Read-write。

> **Note**
>
> 对于装载在 Microsoft Windows 客户端上的文件共享，如果选择Read-only为了将导出为，您可能会看到有关某个意外错误正在阻止您创建文件夹的错误消息。此错误消息是 NFS 版本 3 的已知问题。您可以忽略此消息。

- 对于 File/directory access controlled by (文件/目录访问控制方式)，选择下列选项之一：
  - 选择 Windows Access Control List (Windows 访问控制列表) 可为 SMB 文件共享中的文件和文件夹设置精细控制权限。有关更多信息，请参阅使用 Microsoft Windows ACL 控制对 SMB 文件共享的访问。
  - 选择 POSIX permissions (POSIX 权限) 可使用 POSIX 权限控制对通过 NFS 或 SMB 文件共享存储的文件和目录的访问。

  如果你的身份验证方法是Active Directory，对于管理员用户/组输入 AD 用户和组的逗号分隔列表。如果希望管理员用户有权更新文件共享中所有文件和文件夹的 ACL，请执行此操作。之后，这些用户和组将具有文件共享的管理员权限。组的前缀必须为@例如，角色，`@group1`.

- 适用于区分大小写中，选中该复选框以允许网关控制区分大小写，或清除该复选框以允许客户端控制区分大小写。

> **Note**
>
> - 如果选中此复选框，此设置将立即应用于新的 SMB 客户端连接。现有的 SMB 客户端连接必须断开与文件共享的连接，然后重新连接才能使设置生效。
> - 如果清除此复选框，此设置可能会导致您无法访问名称仅在大小写上不同的文件。

- 适用于基于访问权限的枚举中，选中该复选框以使共享中的文件和文件夹仅对具有读取权限的用户可见。保持清除该复选框，以使共享上的文件和文件夹在目录枚举期间对所有用户都可见。

> **Note**
>
> 基于访问的枚举是一种系统，它根据共享的访问控制列表 (ACL) 筛选 SMB 文件共享上的文件和文件夹枚举。

- 适用于机会主义锁（oplock），选择以下选项之一：
  - 选择Enabled (已启用)允许文件共享使用机会锁定来优化文件缓冲策略，这在大多数情况下提高了性能，特别是在 Windows 上下文菜单方面。
  - 选择Disabled以防止使用机会主义锁定。如果环境中的多个 Windows 客户端频繁同时编辑相同的文件，那么禁用机会锁定有时可以提高性能。

> **Note**
>
> 对于涉及在不同情况下访问同名文件的工作负载，建议不要对区分大小写的共享启用机会锁定。

5. 选择 Save changes（保存更改）。

刷新您的 Amazon S3 存储桶中的对象

在 NFS 或 SMB 客户端执行文件系统操作时，您的网关会在与文件共享关联的 S3 存储桶中维护一个对象清单。您的网关使用此缓存清单来减小 S3 请求的延迟和频率。此操作不会将文件导入 S3 文件网关缓存存储。它只更新缓存清单以反映 S3 存储桶中对象清单的变化。

要刷新文件共享的 S3 存储桶，您可以使用 Storage Gateway 控制台，RefreshCache在 Storage Gateway API 中进行操作，或者AWS Lambdafunction.

从控制台刷新 S3 存储桶中的对象

1. 打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
2. 选择 File shares，然后选择与要刷新的 S3 存储桶关联的文件共享。
3. 对于 Actions，选择 Refresh cache。

   刷新过程所需的时间取决于在网关上缓存的对象数以及在 S3 存储桶中添加或删除的对象数。

使用刷新 S3 存储桶中的对象AWS Lambda功能

1. 确定 S3 文件网关使用的 S3 存储桶。
2. 检查是否Event部分为空。它稍后会自动填充。
3. 创建 IAM 角色，并允许 Lambda 的信任关系`lambda.amazonaws.com`.
4. 使用以下策略。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "StorageGatewayPermissions",
            "Effect": "Allow",
            "Action": "storagegateway:RefreshCache",
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchLogsPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:CreateLogGroup",
                "logs:PutLogEvents"
            ],
            "Resource": "*"
        }
    ]
}
```

5. 从 Lambda 控制台创建 Lambda 函数。
6. 对您的 Lambda 任务使用以下函数。

```
import json
import boto3
client = boto3.client('storagegateway')
def lambda_handler(event, context):
    print(event)
    response = client.refresh_cache(
        FileShareARN='arn:aws:storagegateway:ap-southeast-2:672406774878:share/
share-E51FBD9C'
    )
```

```
    print(response)
    return 'Your FileShare cache has been refreshed'
```

7. 适用于执行角色中，选择您创建的 IAM 角色。
8. 可选：为 Amazon S3 添加触发器并选择事件ObjectCreated要么ObjectRemoved.

> **Note**
>
> RefreshCache在开始另一个过程之前需要完成一个过程 当您在存储桶中创建或删除许多对象时，性能可能会降低。因此，我们建议不要使用 S3 触发器。相反，请使用下面描述的 Amazon CloudWatch 规则。

9. 在 CloudWatch 控制台上创建 CloudWatch 规则并添加时间表。一般来说，我们推荐固定速率30分钟。但是，您可以在大型 S3 存储桶上使用 1-2 小时。
10. 为 CloudWatch 事件添加新的触发器，然后选择刚创建的规则。
11. 保存 Lambda 配置。选择测试。
12. 选择S3 把并根据您的要求自定义测试。
13. 测试应该会成功。如果没有，请根据您的要求修改 JSON 并重新测试。
14. 打开 Amazon S3 控制台，然后验证您创建的事件和 Lambda 函数 ARN 是否存在。
15. 使用 Amazon S3 控制台或将对象上传到 S3 存储桶。AWS CLI.

    CloudWatch 控制台将生成类似于以下内容的 CloudWatch 输出。

```
{
    u'Records': [
        {u'eventVersion': u'2.0', u'eventTime': u'2018-09-10T01:03:59.217Z',
 u'requestParameters': {u'sourceIPAddress': u'MY-IP-ADDRESS'},
        u's3': {u'configurationId': u'95a51e1c-999f-485a-b994-9f830f84769f',
 u'object': {u'sequencer': u'00549CC2BF34D47AED', u'key': u'new/filename.jpeg'},
        u'bucket': {u'arn': u'arn:aws:s3:::MY-BUCKET', u'name': u'MY-GATEWAY-
NAME', u'ownerIdentity': {u'principalId': u'A3OKNBZ72HVPP9'}}, u's3SchemaVersion':
 u'1.0'},
        u'responseElements': {u'x-amz-id-2':
 u'76tiugjhvjfyriugiug87t890nefevbck0iA3rPU9I/s4NY9uXwtRL75tCyxasgsdgfsq+IhvAg5M=',
 u'x-amz-request-id': u'651C2D4101D31593'},
        u'awsRegion': u'MY-REGION', u'eventName': u'ObjectCreated:PUT',
 u'userIdentity': {u'principalId': u'AWS:AROAI5LQR5JHFHDFHDFHJ:MY-USERNAME'},
 u'eventSource': u'aws:s3'}
    ]
```

```
}
```

Lambda 调用为您提供类似于以下内容的输出。

```
{
    u'FileShareARN': u'arn:aws:storagegateway:REGION:ACCOUNT-ID:share/MY-SHARE-
ID',
        'ResponseMetadata': {'RetryAttempts': 0, 'HTTPStatusCode': 200,
 'RequestId': '6663236a-b495-11e8-946a-bf44f413b71f',
            'HTTPHeaders': {'x-amzn-requestid': '6663236a-b495-11e8-946a-
bf44f413b71f', 'date': 'Mon, 10 Sep 2018 01:03:59 GMT',
                'content-length': '90', 'content-type': 'application/x-amz-
json-1.1'
        }
    }
}
```

您在客户端上挂载的 NFS 共享将反映此更新。

> **Note**
>
> 对于在包含数百万对象的大型存储桶中更新大型对象创建或删除的缓存，更新可能需要数小时。

16. 使用 Amazon S3 控制台手动删除对象，或AWS CLI.
17. 查看客户端上挂载的 NFS 共享。验证对象已消失（因为缓存已刷新）。
18. 查看您的 CloudWatch 日志以查看与事件一起删除的日志`ObjectRemoved:Delete`.

```
{
    u'account': u'MY-ACCOUNT-ID', u'region': u'MY-REGION', u'detail': {}, u'detail-
type': u'Scheduled Event', u'source': u'aws.events',
    u'version': u'0', u'time': u'2018-09-10T03:42:06Z', u'id':
 u'6468ef77-4db8-0200-82f0-04e16a8c2bdb',
    u'resources': [u'arn:aws:events:REGION:MY-ACCOUNT-ID:rule/FGw-RefreshCache-CW']
}
```

> **Note**
>
> 对于 cron 作业或计划任务，您的 CloudWatch 日志事件为`u'detail-type': u'Scheduled Event'`.

缓存刷新仅启动刷新操作。在缓存刷新完成时，这并不一定表示文件刷新完成。要确定在检查网关文件共享上的新文件之前已完成文件刷新操作，请使用 `refresh-complete` 通知。要做到这一点，您可以订阅通过 Amazon CloudWatch 事件在RefreshCache操作完成。有关更多信息，请参阅获得有关文件操作的通知。

将 S3 对象锁定与 Amazon S3 文件网关结合使用

Amazon S3 文件网关支持访问启用了 Amazon S3 对象锁定的 S3 存储桶。Amazon S3 对象锁定使您能够使用 “一次写入，多次读取” (WORM) 模式存储对象。使用 Amazon S3 对象锁定时，您可以防止删除或覆盖 S3 存储桶中的对象。Amazon S3 对象锁定与对象版本控制一起使用以保护您的数据。

如果启用 Amazon S3 对象锁定，您仍然可以修改对象。例如，可以通过 S3 文件网关上的文件共享写入、删除或重命名对象。以这种方式修改对象时，S3 文件网关放置新版本的对象，而不会影响以前的版本（即，锁定的对象）。

例如，如果您使用 S3 文件网关 NFS 或 SMB 接口删除文件并锁定了相应的 S3 对象，则网关放置 S3 删除标记以作为下一个对象版本并保留原始对象版本。同样，如果 S3 文件网关修改锁定的对象的内容或元数据，将上传包含更改的新对象版本，但原来的锁定对象版本保持不变。

有关 Amazon S3 对象锁定的更多信息，请参阅。使用 S3 对象锁定以锁定对象中的Amazon Simple Storage Service 用户指南.

了解文件共享状态

每个文件共享均有关联的状态，让您一目了然地了解文件共享的运行状态。状态大多数时候会显示文件共享运行正常，无需您采取任何行动。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 控制台中查看文件共享状态。对于网关中的每个文件共享，文件共享状态显示在 Status 列中。正常工作的文件共享的状态显示为 AVAILABLE。

在下表中，您可以找到各个文件共享状态的描述，以及基于状态，您是否需要采取行动和应在何时采取行动。在使用文件共享的所有或大部分时间，文件共享都应具有 AVAILABLE 状态。

状态	意义
AVAILABLE	文件共享已正确配置且可供使用。AVAILABLE 状态是文件共享的正常运行状态。
CREATING	正在创建该文件共享，因此尚不能使用它。CREATING (正在创建) 状态是过渡型状态。无需采取行动。如果文件共享停滞在此状态，这可能是因为网关 VM 丢失了与AWS.
UPDATING	文件共享配置正在更新。如果文件共享停滞在此状态，这可能是因为网关 VM 丢失了与的连接。AWS.
DELETING	正在删除文件共享。将不删除文件共享，直到所有数据上传到AWS. DELETING 状态是过渡型状态，无需执行任何操作。
FORCE_DELETING	正在强制删除文件共享。文件共享将被立即删除并上传到AWS已中止。FORCE_DELETING 状态是过渡性质的，无需执行任何操作。
UNAVAILABLE	文件共享处于不佳状态。某些问题会导致文件共享转为不佳状态。例如，角色策略错误或者文件共享映射到不存在的 Amazon S3 存储桶都会导致此问题。在解决导致状态不佳的问题后，文件将返回 AVAILABLE 状态。

文件共享最佳实践

在此部分中，您可以找到有关创建文件共享的最佳实践的信息。

主题

- 防止多个文件共享写入 Amazon S3 存储桶。
- 允许特定的 NFS 客户端挂载文件共享

防止多个文件共享写入 Amazon S3 存储桶。

在创建文件共享时，我们建议您配置 Amazon S3 存储桶，以便只有一个文件共享可以向其中写入内容。如果您将 S3 存储桶配置为由多个文件共享写入，则可能出现不可预测的结果。为了防止这种情况

发生，您可以创建一个 S3 存储桶策略，拒绝除用于文件共享的角色以外的所有角色在存储桶中放置或删除对象，然后将该策略附加到 S3 存储桶。

以下示例策略拒绝除创建存储桶的角色以外的所有角色写入到 S3 存储桶。将拒绝除 `s3:DeleteObject` 以外的所有角色的 `s3:PutObject` 和 `"TestUser"` 操作。该策略适用于 `"arn:aws:s3:::TestBucket/*"` 存储桶中的所有对象。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyMultiWrite",
         "Effect":"Deny",
         "Principal":"*",
         "Action":[
            "s3:DeleteObject",
            "s3:PutObject"
         ],
         "Resource":"arn:aws:s3:::TestBucket/*",
         "Condition":{
            "StringNotLike":{
               "aws:userid":"TestUser:*"
            }
         }
      }
   ]
}
```

允许特定的 NFS 客户端挂载文件共享

我们建议您更改文件共享允许的 NFS 客户端设置。如果您未这样做，则您网络上的任何客户端均可装载您的文件共享。有关如何编辑 NFS 客户端设置的信息，请参阅 编辑 NFS 文件共享的访问设置。

监控文件网关

您可以在中监控您的文件网关和相关资源。AWS Storage Gateway通过使用 Amazon CloudWatch 指标和文件共享审核日志。您还可以使用 CloudWatch Events 在文件操作完成时收到通知。有关文件网关类型指标的信息，请参阅监控文件网关。

主题

使用 CloudWatch 日志组获取文件网关健康日志

您可以使用 Amazon CloudWatch Logs 获取有关文件网关和相关资源的运行状况的信息。您可以使用日志来监控网关遇到的错误。此外，您可以使用 Amazon CloudWatch 订阅筛选器来实时自动处理日志信息。有关更多信息，请参阅 。使用订阅实时处理日志数据中的Amazon CloudWatch 用户指南。

例如，您可以将 CloudWatch 日志组配置为监控网关，并在文件网关无法将文件上传到 Amazon S3 存储桶时获得通知。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 S3 文件网关. 有关 CloudWatch 日志组的一般信息，请参阅。使用日志组和日志流中的Amazon CloudWatch 用户指南。

以下是文件网关报告的错误的示例。

```
{
    "severity": "ERROR",
    "bucket": "bucket-smb-share2",
    "roleArn": "arn:aws:iam::123456789012:role/my-bucket",
    "source": "share-E1A2B34C",
    "type": "InaccessibleStorageClass",
    "operation": "S3Upload",
    "key": "myFolder/myFile.text",
    "gateway": "sgw-B1D123D4",
    "timestamp": "1565740862516"
```

```
}
```

此错误意味着文件网关无法上传对象myFolder/myFile.text转换为 Amazon S3，因为它已从 Amazon S3 标准存储类转换为 S3 Glacier 灵活检索或 S3 Glacier Deep Archive 存储类。

在前面的网关运行状况日志中，这些项目指定了给定的信息：

- source: share-E1A2B34C 指示遇到此错误的文件共享。
- "type": "InaccessibleStorageClass" 指示所发生的错误的类型。在这种情况下，当网关尝试将指定的对象上传到 Amazon S3 或从 Amazon S3 读取时，会遇到此错误。但是，在这种情况下，对象转换为 Amazon S3 Glacier。"type" 的值可以是文件网关遇到的任何错误。有关可能错误的列表，请参阅 排查文件网关问题。
- "operation": "S3Upload"指示当网关尝试将该对象上传到 S3 时发生此错误。
- "key": "myFolder/myFile.text" 指示导致故障的对象。
- gateway": "sgw-B1D123D4 指示遇到此错误的文件网关。
- "timestamp": "1565740862516"指示发生错误的时间。

有关如何排查和修复此类错误的信息，请参阅排查文件网关问题。

在激活网关后配置 CloudWatch 日志组

以下过程显示了激活网关后如何配置 CloudWatch 日志组。

配置 CloudWatch 日志组以与文件网关一起使用

1. 登录到AWS Management Console然后打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
2. 在导航窗格中，选择网关，然后选择要为其配置 CloudWatch 日志组的网关。
3. 适用于操作，选择编辑网关信息. 或者，在详细信息选项卡，下Health 日志和未启用，选择配置日志组以打开编辑客户网关名称对话框。
4. 适用于网关运行状况日志组中，选择以下选项之一：

   - Disable logging (禁用日志记录)如果您不想使用 CloudWatch 日志组监控网关。
   - 创建新的日志组以创建新的 CloudWatch 日志组。
   - 使用现有日志组以使用已存在的 CloudWatch 日志组。

     从中选择日志组现有的日志组列表.

5. 选择 Save changes（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，选择网关，然后选择要为其配置 CloudWatch 日志组的网关。
    2. 选择详细信息选项卡和下Health 日志，选择CloudWatch Logs (CloudWatch 日志). 这些区域有：日志组详细信息页面将在 CloudWatch 控制台中打开。

配置 CloudWatch 日志组以与文件网关一起使用

1. 登录到AWS Management Console然后打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
2. 选择网关，然后选择要为其配置 CloudWatch 日志组的网关。
3. 适用于操作，选择编辑网关信息. 或者，在详细信息选项卡，旁边日志系统，在未启用，选择配置日志组以打开编辑网关信息对话框。
4. 适用于日志网关日志组，选择使用现有日志组，然后选择要使用的日志组。

    如果您没有日志组，请选择创建新日志组以创建日志组。您将被定向到 CloudWatch Logs 控制台，您可以在其中创建日志组。如果创建新的日志组，请选择刷新按钮以在下拉列表中查看新的日志组。
5. 完成此操作后，选择保存。
6. 要查看日志以了解您的网关，请选择该网关，然后选择详细信息选项卡。

有关如何排查错误的信息，请参阅排查文件网关问题。

使用 Amazon CloudWatch 指标

您可以使用AWS Management Console或 CloudWatch API。控制台将根据来自 CloudWatch API 的原始数据显示一系列图表。CloudWatch API 也可以通过其中一个AWS软件开发工具包要么Amazon CloudWatch API工具。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。

无论使用何种方法使用指标，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 的维度是`GatewayId`和`GatewayName`. 在 CloudWatch 控制台中，您可以使用`Gateway Metrics`视图以选择特定于网关的维度。有关维度的更多信息，请参阅。维度中的Amazon CloudWatch 用户指南.

- 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	描述
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 GatewayId 和 GatewayName 维度来标识要使用的文件网关。 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：

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

获得有关文件操作的通知

在文件操作完成时，Storage Gateway 可以启动 CloudWatch Event：

- 在网关完成将文件从文件共享异步上传到 Amazon S3 时，您可以获得通知。使用NotificationPolicy参数以请求文件上传通知。这将向 Amazon S3 发送每次已完成文件上传的通知。有关更多信息，请参阅获取文件上传通知。
- 在网关完成将工作文件集从文件共享到 Amazon S3 异步上传时，您可以获得通知。使用NotifyWhenUploaded用于请求工作文件集上传通知的 API 操作。在工作文件集中的所有文件上传到 Amazon S3 时，将发送通知。有关更多信息，请参阅获取工作文件集上传通知。
- 您可以在网关完成为 S3 存储桶刷新缓存后获得通知。当你调用RefreshCache通过 Storage Gateway 控制台或 API 进行操作完成后订阅通知。有关更多信息，请参阅获取刷新缓存通知。

在请求的文件操作完成后，Storage Gateway 将通过 CloudWatch Events 向您发送通知。您可以将 CloudWatch Events 配置为通过事件目标 (如 Amazon SNS、Amazon SQS 或AWS Lambdafunction. 例如，您可以将 Amazon SNS 目标配置为将通知发送给 Amazon SNS 使用者，例如电子邮件或短信。有关 CloudWatch 事件的信息，请参阅什么是 CloudWatch Events？

设置 CloudWatch Events 通知

1. 创建一个在触发您在 Storage Gateway 中请求的事件时调用的目标，例如 Amazon SNS 主题或 Lambda 函数。
2. 在 CloudWatch Events 控制台中创建一个根据 Storage Gateway 中的事件调用目标的规则。
3. 在该规则中，为事件类型创建一个事件模式。在事件与此规则模式匹配时将触发通知。
4. 选择目标并配置设置。

以下示例显示了一个规则，该规则将在指定网关和指定的网关中启动指定事件类型。AWS区域。例如，您可以指定 `Storage Gateway File Upload Event` 作为事件类型。

```
{
   "source":[
      "aws.storagegateway"
   ],
   "resources":[
      "arn:aws:storagegateway:AWS Region:account-id
                  :gateway/gateway-id"
   ],
   "detail-type":[
      "Event type"
   ]
}
```

有关如何使用 CloudWatch Event 来触发规则的信息，请参阅创建对事件触发的 CloudWatch Events 规则中的Amazon CloudWatch Events 用户指南.

获取文件上传通知

在两种使用案例中，您可以使用文件上传通知：

- 要自动完成在云中处理上传的文件，您可以调用`NotificationPolicy`参数然后找回通知 ID。在上传文件时触发的通知的通知 ID 与 API 返回的通知 ID 相同。如果映射该通知 ID 以跟踪您上传的文件列表，您可以在中触发上传的文件处理。AWS当生成具有相同 ID 的事件时。

- 对于内容分配使用案例，您可以有两个映射到同一 Amazon S3 存储桶的两个文件网关。网关 1 的文件共享客户端可能将新文件上传到 Amazon S3，然后网关 2 上的文件共享客户端读取这些文件。这些文件上传到 Amazon S3，但不会在网关 2 中显示这些文件，因为网关 2 使用 Amazon S3 中的本地缓存版本的文件。要使文件在 Gateway2 中可见，您可以使用`NotificationPolicy`参数请求网关 1 在上传文件完成后向您发送文件上传通知。然后，您可以使用 CloudWatch Events 自动发出RefreshCache在网关 2 上请求文件共享。当RefreshCache请求已完成，新文件在 Gateway2 中可见。

Example 示例-文件上传通知

以下示例显示了一个在事件与您创建的规则匹配 CloudWatch 发送给您的文件上传通知。此通知采用 JSON 格式。您可以将此通知配置为以文本消息的形式传输到目标。`detail-type` 为 `Storage Gateway Object Upload Event`。

```
{
    "version": "0",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway Object Upload Event",
    "source": "aws.storagegateway",
    "account": "123456789012",
    "time": "2020-11-05T12:34:56Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:storagegateway:us-east-1:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-1:123456789011:gateway/sgw-712345DA",
        "arn:aws:s3:::do-not-delete-bucket"
    ],
    "detail": {
        "object-size": 1024,
        "modification-time": "2020-01-05T12:30:00Z",
        "object-key": "my-file.txt",
        "event-type": "object-upload-complete",
        "prefix": "prefix/",
        "bucket-name": "my-bucket",
    }
}
```

字段名称	描述
版本	当前的 IAM 策略版本。

字段名称	描述
id	标识 IAM 策略的 ID。
detail-type	触发所发送的通知的事件的描述。
source	这些区域有：AWS作为请求和通知来源的服务。
账户	的 IDAWS从中生成请求和通知的账户。
time	将文件上传到 Amazon S3 的请求发出时间。
region	这些区域有：AWS从中发送请求和通知的区域。
resources	策略适用的存储网关资源。
Object size	数据元的大小 (以字节为单位)。
修改时间	客户端修改文件的时间。
Object key	文件的路径。
event-type	触发通知的 CloudWatch Events。
prefix	S3 存储桶的前缀名称。
bucket-name	S3 存储桶的名称。

获取工作文件集上传通知

有两个用例可以使用工作文件集上传通知：

- 要自动完成在云中处理上传的文件，您可以调用`NotifyWhenUploaded`API 然后找回通知 ID。在上传工作组文件时触发的通知的通知 ID 与 API 返回的通知 ID 相同。如果映射该通知 ID 以跟踪您上传的文件列表，您可以触发上传到的工作组文件处理。AWS当生成具有相同 ID 的事件时。
- 对于内容分配使用案例，您可以有两个映射到同一 Amazon S3 存储桶的两个文件网关。网关 1 的文件共享客户端可以将新文件上传到 Amazon S3，然后网关 2 上的文件共享客户端读取这些文件。这些文件上传到 Amazon S3，但不会在网关 2 中显示这些文件，因为网关 2 使用 S3 中的

本地缓存版本的文件。要使文件在 Gateway2 中可见，请使用NotifyWhenUploadedAPI 操作请求网关 1 在上传完成文件集时向您发送文件上传通知。然后，您可以使用 CloudWatch 事件自动发出RefreshCache在网关 2 上请求文件共享。当RefreshCache请求完成，新文件在网关 2 中可见。此操作不会将文件导入文件网关缓存存储。它只更新缓存清单以反映 S3 存储桶中对象清单的变化。

Example 示例-工作文件集上传通知

以下示例显示了一个工作文件集上传通知，在事件与您创建的规则匹配时，将通过 CloudWatch 向您发送该通知。此通知采用 JSON 格式。您可以将此通知配置为以文本消息的形式传输到目标。`detail-type` 为 `Storage Gateway File Upload Event`。

```
{
    "version": "2012-10-17",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway Upload Notification Event",
    "source": "aws.storagegateway",
    "account": "123456789012",
    "time": "2017-11-06T21:34:42Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:storagegateway:us-east-2:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-2:123456789011:gateway/sgw-712345DA"
    ],
    "detail": {
        "event-type": "upload-complete",
        "notification-id": "11b3106b-a18a-4890-9d47-a1a755ef5e47",
        "request-received": "2018-02-06T21:34:42Z",
        "completed": "2018-02-06T21:34:53Z"
    }
}
```

字段名称	描述
版本	当前的 IAM 策略版本。
id	标识 IAM 策略的 ID。
detail-type	触发所发送的通知的事件的描述。

字段名称	描述
source	这些区域有：AWS作为请求和通知来源的服务。
账户	的 IDAWS从中生成请求和通知的账户。
time	将文件上传到 Amazon S3 的请求发出时间。
region	这些区域有：AWS从中发送请求和通知的区域。
resources	策略适用的 Storage Gateway 资源。
event-type	触发通知的 CloudWatch Events。
notification-id	为发送的通知随机生成的 ID。该 ID 采用 UUID 格式。这是在调用 `NotifyWhenUploaded` 时返回的通知 ID。
request-received	网关收到 `NotifyWhenUploaded` 请求的时间。
completed	当工作集中的所有文件都上传到 Amazon S3 时。

获取刷新缓存通知

对于刷新缓存通知用例，您可以有两个映射到同一 Amazon S3 存储桶的文件网关，Gateway1 的 NFS 客户端会将新文件上传到 S3 存储桶。这些文件上传到 Amazon S3，但在您刷新缓存之前，它们不会出现在网关 2 中。这是因为 Gateway2 在 Amazon S3 中使用了本地缓存的文件版本。当刷新缓存完成时，您可能希望对 Gateway2 中的文件执行某项操作。大型文件可能需要一些时间才能在网关 2 中显示，因此您可能希望在缓存刷新完成时获得通知。您可以从 Gateway2 请求刷新缓存通知，以在所有文件都在 Gateway2 中可见时通知您。

Example 示例-刷新缓存通知

以下示例显示一个刷新缓存通知，在事件与您创建的规则匹配时，将通过 CloudWatch 向您发送该通知。此通知采用 JSON 格式。您可以将此通知配置为以文本消息的形式传输到目标。`detail-type` 为 `Storage Gateway Refresh Cache Event`。

```
{
    "version": "2012-10-17",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway Refresh Cache Event",
    "source": "aws.storagegateway",
    "account": "209870788375",
    "time": "2017-11-06T21:34:42Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:storagegateway:us-east-2:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-2:123456789011:gateway/sgw-712345DA"
    ],
    "detail": {
        "event-type": "refresh-complete",
        "notification-id": "1c14106b-a18a-4890-9d47-a1a755ef5e47",
        "started": "2018-02-06T21:34:42Z",
        "completed": "2018-02-06T21:34:53Z",
        "folderList": [
            "/"
        ]
    }
}
```

字段名称	描述
版本	当前的 IAM 策略版本。
id	标识 IAM 策略的 ID。
detail-type	触发所发送的通知的事件的类型描述。
source	这些区域有：AWS作为请求和通知来源的服务。
账户	的 IDAWS从中生成请求和通知的账户。

字段名称	描述
time	刷新工作集中的文件的请求的发出时间。
region	这些区域有：AWS从中发送请求和通知的区域。
resources	策略适用的 Storage Gateway 资源。
event-type	触发通知的 CloudWatch Events。
notification-id	为发送的通知随机生成的 ID。该 ID 采用 UUID 格式。这是在调用 `RefreshCache` 时返回的通知 ID。
started	当网关收到`RefreshCache` 请求并启动刷新。
completed	完成工作集刷新的时间。
folderList	在缓存中刷新的文件夹的逗号分隔路径列表。默认为 ["/"]。

了解网关指标

下表介绍了覆盖 S3 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特定于文件共享的指标同名。这些指标代表同类度量，但其范围限于网关，而非文件共享。

始终在使用特定指标时指定要使用网关还是文件共享。具体来说，在使用网关指标时，您必须指定`Gateway Name`对于要查看其指标数据的网关。有关更多信息，请参阅使用 Amazon CloudWatch 指标。

下表介绍了可用来获取有关您的信息的指标。S3 文件网关。

指标	描述
`AvailabilityNotifications`	此指标报告报告周期内网关生成的与可用性相关的运行状况通知数。 单位：计数

指标	描述
CacheFileSize	此指标用于跟踪网关缓存中文件的大小。 将此指标与Average统计数据来衡量网关缓存中文件的平均大小。将此指标与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	此指标会报告网关缓存中的可用字节数。 单位：字节
CacheHitPercent	应用程序从网关中读取的百分率，由缓存传送。样本在报告周期结束时采用。 在没有应用程序从网关进行读取时，该指标报告100%。 单位：百分比
CachePercentDirty	尚未持续到的网关缓存的总体百分率。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	此指标会报告网关缓存中使用的字节数。 单位：字节

指标	描述
CloudBytesDownloaded	网关上传到的总字节数AWS在本报告所述期间. 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每秒输入/输出操作次数 (IOPS)。 单位：字节
CloudBytesUploaded	网关从下载的总字节数AWS在本报告所述期间. 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
FilesFailingUpload	此指标跟踪未能上传到的文件的数量。AWS. 这些文件将生成包含有关该问题的更多信息的运行状况通知。 将此指标与Sum统计信息，显示当前无法上传到的文件数AWS. 单位：计数
FileSharesUnavailable	此指标提供了此网关上的文件共享数量，这些数目位于Unavailable状态。 如果此指标报告任何文件共享不可用，则网关可能存在问题，可能会导致您的工作流程中断。建议在此指标报告了非零值时创建警报。 单位：计数
FilesRenamed	此指标跟踪在报告时段内重命名的文件数。 单位：计数

指标	描述
HealthNotifications	此指标报告该网关在报告期内生成的运行状况通知的数量。 单位：计数
IoWaitPercent	此指标报告 CPU 等待本地磁盘响应的时间百分比。 单位：百分比
MemTotalBytes	此指标报告网关上的内存总量。 单位：字节
MemUsedBytes	此指标报告网关上已使用的内存量。 单位：字节
NfsSessions	此指标会报告在网关上处于活动状态的 NFS 会话数。 单位：计数
RootDiskFreeBytes	此指标会报告网关根磁盘上的可用字节数。 如果此指标报告小于 20 GB 可用，则应增加根磁盘的大小。 单位：字节
S3GetObjectRequestTime	此指标报告网关完成 S3 获取对象请求的时间。 单位：毫秒
S3PutObjectRequestTime	此指标报告网关完成 S3 放置对象请求的时间。 单位：毫秒

指标	描述
S3UploadPartRequestTime	此指标报告网关完成 S3 上传段请求的时间。 单位：毫秒
SmbV1Sessions	此指标会报告在网关上处于活动状态的 Smbv1 会话数。 单位：计数
SmbV2Sessions	此指标会报告在网关上处于活动状态的 Smbv2 会话数。 单位：计数
SmbV3Sessions	此指标会报告在网关上处于活动状态的 SmBv3 会话数。 单位：计数
TotalCacheSize	此指标报告缓存的总大小。 单位：字节
UserCpuPercent	此指标报告了在网关处理上花费的时间百分比。 单位：百分比

了解文件共享指标

您可以在下面找到有关包含文件共享的 Storage Gateway 指标的信息。每个文件共享均有与其关联的一组指标。某些特定于文件共享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，但其范围限于文件共享。

始终在使用指标前指定要使用网关还是文件共享指标。尤其是使用文件共享指标时，您必须指定标识希望查看其指标的文件共享的 `File share ID`。有关更多信息，请参阅使用 Amazon CloudWatch 指标。

下表描述了可用来获取文件共享信息的 Storage Gateway 指标。

指标	描述
CacheHitPercent	应用程序从缓存提供的文件共享中读取的百分率。样本在报告周期结束时采用。 在没有应用程序从文件共享获得时，该指标报告100%。 单位：百分比
CachePercentDirty	文件共享在未传送到的网关缓存的总体比例中的占比。AWS. 样本在报告周期结束时采用。 使用CachePercentDirty 以查看尚未持续到的网关缓存的总体比例。AWS. 单位：百分比
CachePercentUsed	文件共享对网关缓存存储空间的总体使用率占比。样本在报告周期结束时采用。 使用网关的 CachePercentUsed 指标来查看网关缓存存储空间的总体使用率。 单位：百分比
CloudBytesUploaded	网关上传到的总字节数AWS在本报告所述期间. 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	网关从下载的总字节数AWS在本报告所述期间. 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每秒输入/输出操作次数 (IOPS)。

指标	描述
	单位：字节
ReadBytes	报告周期内文件共享从场内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

了解文件网关审核日志

Amazon S3 文件网关 (S3 文件网关) 审计日志为您提供有关用户访问文件共享中的文件和文件夹的详细信息。您可以使用它们监控用户活动，并在识别到不当的活动模式时采取措施。

操作

下表介绍了文件网关审计日志文件访问操作。

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。
创建	创建新文件或文件夹。
重命名	重命名现有文件或文件夹。

操作名称	定义
删除	删除文件或文件夹。
写入属性	更新文件或文件夹元数据（ACL、拥有者、组、权限）。

属性

下表介绍了 S3 文件网关审计日志文件访问属性。

属性	定义
accessMode	对象的权限设置。
accountDomain （仅限中小型企业）	客户端账户所属的 Active Directory (AD) 域。
accountName （仅限中小型企业）	客户端的 Active Directory 用户名。
bucket	S3 存储桶名称。
clientGid （仅限 NFS）	访问对象的用户组的标识符。
clientUid （仅限 NFS）	访问对象的用户的标识符。
ctime	在此时间修改对象的内容或元数据，由客户端设置。
groupId	对象的组拥有者的标识符。
fileSizeInBytes	文件大小，以字节为单位，由客户端在文件创建时设置。
gateway	Storage Gateway ID。
mtime	在此时间修改对象的内容，由客户端设置。
newObjectName	新对象重命名后的完整路径。
objectName	对象的完整路径。

属性	定义
objectType	定义对象是文件还是文件夹。
operation	对象访问操作的名称。
ownerId	对象拥有者的标识符。
securityDescriptor （仅限中小型企业）	显示在对象上设置的自由访问控制列表 (DACL)，使用 SDDL 格式。
shareName	正在访问的共享的名称。
source	所审计的文件共享的 ID。
sourceAddress	文件共享客户端计算机的 IP 地址。
status	操作的状态。仅记录成功（记录失败，但由于权限被拒绝而引发的失败除外）。
timestamp	发生操作的时间，基于网关的操作系统时间戳。
version	审计日志格式的版本。

每个操作记录的属性

下表描述了在各个文件访问操作中记录的 S3 文件网关审计日志属性。

	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	写属性（更改 ACL）-仅限 SMB）	写属性（chown）	写属性 (chmod)	写属性 (chgrp)
access e			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	写属性（更改 ACL）-仅限 SMB）	写属性（chown）	写属性 (chmod)	写属性 (chgrp)
accoun main（仅限中小型企业）	X	X	X	X	X	X	X	X	X	X
accoun me（仅限中小型企业）	X	X	X	X	X	X	X	X	X	X
bucket	X	X	X	X	X	X	X	X	X	X
client （仅限 NFS）	X	X	X	X	X	X		X	X	X
client （仅限 NFS）	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	写属性（更改 ACL）-仅限 SMB）	写属性（chown）	写属性 (chmod)	写属性 (chgrp)
ctime			X	X						
groupI			X	X						
fileSi nBytes				X						
gatewa	X	X	X	X	X	X	X	X	X	X
mtime			X	X						
newObj Name					X					
object e	X	X	X	X	X	X	X	X	X	X
object e	X	X	X	X	X	X	X	X	X	X
operat	X	X	X	X	X	X	X	X	X	X
ownerI			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	写属性（更改 ACL）-仅限 SMB）	写属性（chown）	写属性 (chmod)	写属性 (chgrp)
securi escrip （仅限中小型企业）							X	X		
shareN	X	X	X	X	X	X	X	X	X	X
source	X	X	X	X	X	X	X	X	X	X
source ress	X	X	X	X	X	X	X	X	X	X
status	X	X	X	X	X	X	X	X	X	X
timest	X	X	X	X	X	X	X	X	X	X
versic	X	X	X	X	X	X	X	X	X	X

维护网关

维护网关包括配置缓存存储和上传缓冲区空间、执行常规维护和监控网关性能等任务。这些任务是所有网关类型的常见任务。

主题

关闭网关 VM

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。关闭虚拟机之前，您必须先停止网关。对于文件网关，您可以直接关闭虚拟机。虽然此部分的内容重点说明了使用 Storage Gateway 管理控制台启动和停止网关，不过您也可以使用虚拟机本地控制台或 Storage Gateway API 启动和停止网关。当您开启虚拟机时，请记住重新启动网关。

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。对于文件网关，您可以直接关闭虚拟机。而不需要关闭网关。虽然此部分的内容重点说明了使用 Storage Gateway 管理控制台启动和停止网关，不过您也可以使用虚拟机本地控制台或 Storage Gateway API 启动和停止网关。当您开启虚拟机时，请记住重新启动网关。

- 网关 VM 本地控制台 — 请参阅在本地控制台上执行维护任务.
- Storage Gateway API — 请参阅ShutdownGateway

管理 Storage Gateway 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 实例上创建的网关使用 Amazon EBS 卷作为本地磁盘。

主题

- 决定本地磁盘存储量
- 确定要分配的缓存存储空间的大小
- 添加缓存存储
- 将临时存储与 EC2 网关结合使用

决定本地磁盘存储量

要为网关分配的磁盘的数量和大小由您自己决定。网关需要以下额外存储：

文件网关至少需要一个磁盘用作缓存。下表为所部署的网关推荐了本地磁盘存储的大小。在设置网关后以及工作负载需求增大时，您可以添加更多本地存储。

本地存储	描述	网关类型
缓存存储空间	缓存存储空间用作等待向 Amazon S3 或文件系统上传的数据的本地持久存储。	• 文件网关

> **Note**
>
> 底层物理存储资源在 VMware 中表示为数据存储。部署网关 VM 时，您可选择用来存储 VM 文件的数据存储。预配置本地磁盘 (例如要用作缓存存储空间) 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其他数据存储中。
> 如果您有多个数据存储，强烈建议为缓存存储空间选择一个数据存储。仅由一个底层物理磁盘支持的数据存储在用于支持两个缓存存储空间的某些情况下可能导致性能不佳。这同样适用于备份是一个 RAID1 等低性能 RAID 配置的情况。

在初次配置和部署网关后，您可以通过添加用于缓存存储空间的磁盘来调整本地存储。

确定要分配的缓存存储空间的大小

您的网关使用其缓存存储来提供对最近访问数据的低延迟访问。缓存存储空间用作等待向 Amazon S3 或文件系统上传的数据的本地持久存储。有关如何估算缓存存储大小的更多信息，请参阅 管理 Storage Gateway 的本地磁盘。

您可以将此近似值用来初步为缓存存储空间预配置磁盘。然后，您可使用 Amazon CloudWatch 运行指标来监控缓存存储空间使用率并使用控制台根据需预配置更多存储空间。有关使用指标和设置警报的信息，请参阅 性能。

添加缓存存储

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。您可以向网关添加更多缓存空间，无需中断现有的网关功能。在添加更多存储容量时，可以在启动网关 VM 的情况下执行此操作。

> **Important**
>
> 在向现有网关添加缓存时，在主机 (管理程序或 Amazon EC2 实例) 中创建新磁盘至关重要。如果之前已将磁盘分配为缓存，请勿更改现有磁盘的大小。请勿删除已分配为缓存存储的缓存磁盘。

以下过程说明如何为网关配置或缓存存储。

添加和配置或缓存存储

1. 在主机（管理程序或 Amazon EC2 实例）中预置新磁盘。有关如何在管理程序中预置磁盘的信息，请参阅您的管理程序的用户手册。您将此磁盘配置为缓存存储。
2. 在打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
3. 在导航窗格中，选择 Gateways。
4. 在 Actions 菜单中，选择 Edit local disks。
5. 在“编辑本地磁盘”对话框中，标识您预配置的磁盘，然后确定将哪个磁盘用作缓存存储。

   如果您未看到自己的磁盘，请选择 Refresh 按钮。
6. 选择 Save 以保存您的配置设置。

将临时存储与 EC2 网关结合使用

本节介绍了您在选择临时磁盘作为网关缓存的存储空间时需要执行的用来防止数据丢失的步骤。

临时磁盘为 Amazon EC2 实例提供了临时性块级存储。临时磁盘非常适合用于临时存储频繁更改的数据，例如网关缓存存储空间中的数据。当您使用 Amazon EC2 Amazon 系统映像启动了网关并且您选择的实例类型支持短暂存储时，系统将自动列出磁盘，系统将自动列出磁盘，您可以选择其中一个磁盘

将数据存储在网关缓存中。有关更多信息，请参阅 。Amazon EC2 实例存储中的适用于 Linux 实例的 Amazon EC2 用户指南.

应用程序对磁盘的写入会同步存储在缓存中，然后以异步方式上传到 Amazon S3 中的持久性存储中。如果存储在短暂存储中的数据由于 Amazon EC2 实例在数据上传完成之前停止而丢失，那么仍然位于缓存中且尚未上传到 Amazon S3 的数据可能丢失。您可以在重新启动或停止承载网关的 EC2 实例之前执行这些步骤，以防止此类数据丢失。

> **Note**
>
> 如果您使用的是短暂存储，在您停止和启动您的网关时，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。没有方法可以解决此问题，因此您必须删除网关并在新的 EC2 实例上激活新的网关。

以下过程中的这些步骤特定于文件网关。

防止使用临时磁盘的文件网关中发生数据丢失

1. 停止正在写入到文件共享的所有进程。
2. 订阅以从 CloudWatch 事件接收通知。有关信息，请参阅 获得有关文件操作的通知。
3. 调用上传 API 时通知以便在短暂存储丢失之前一直被写入的数据在 Amazon S3 中持久存储时获得通知。
4. 等待 API 完成，您将收到一个通知 ID。

   您将收到一个具有相同的通知 ID 的 CloudWatch 事件。
5. 验证文件共享的 `CachePercentDirty` 指标是否为 0。这将确认您的所有数据都已写入到 Amazon S3。有关文件共享指标的信息，请参阅了解文件共享指标。
6. 您现在可以重新启动或停止文件网关而不用承担丢失任何数据的风险。

管理 Amazon S3 文件网关的带宽

您可以限制从网关到的上传吞吐量AWS以控制网关使用的网络带宽量。默认情况下，已激活的网关没有速率限制。

您可以使用AWS Management Console，一个AWS软件开发工具包 (SDK)，或AWS Storage GatewayAPI（请参阅更新带宽率限制时间表中的AWSStorage Gateway API 参考。）。使用带宽速

率限制计划，您可以将限制配置为在一天或一周内自动更改。有关更多信息，请参阅使用 Storage Gateway 控制台查看和编辑网关的带宽限制计划。

> **Note**
>
> Amazon FSx 文件网关类型目前不支持配置带宽速率限制和时间表。

主题

使用 Storage Gateway 控制台查看和编辑网关的带宽限制计划

本节介绍如何查看和编辑网关的带宽速率限制计划。

查看和编辑带宽速率限制计划

1. 在打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
2. 在左侧导航窗格中，选择网关，然后选择要管理的网关。
3. 适用于操作，选择编辑带宽速率限制计划.

   网关的当前带宽限制时间表显示在编辑带宽速率限制计划页. 默认情况下，新网关没有定义的带宽率限制。
4. （可选）选择添加新的带宽速率限制将新的可配置间隔添加到计划中。对于添加的每个间隔，输入以下信息：

   - 上传速率— 输入上传速率限制，以兆比特/秒 (Mbps) 为单位。最小值为 100 Mbps。
   - 星期几— 选择要应用时间间隔的每周的一天或几天。您可以在工作日（周一至周五）、周末（周六和周日）、一周中的每一天或每周的一个特定日期应用时间间隔。要在任何时候均匀、持续地应用带宽限制，请选择没有计划.
   - 开始时间— 输入带宽间隔的开始时间，使用 HH: MM 格式和网关与 UTC 的时区偏移量。

> **Note**
>
> 您的带宽速率限制间隔从您在此指定的分钟开始时开始。

- 结束时间— 输入带宽间隔的结束时间，使用 HH: MM 格式和网关与 GMT 之间的时区偏移量。

> **Important**
>
> 带宽速率限制间隔在此处指定的分钟结束时结束。要安排在一个小时结束的时间间隔，请输入**59**.
> 要安排连续的间隔，在小时开始时进行过渡，而不间隔之间的中断，请输入**59**在第一个时间间隔的最后一分钟。Enter**00**在接下来的时间间隔的开始分钟。

5. (可选) 根据需要重复之前的步骤，直到您的带宽速率限制计划完成。如果需要从计划中删除时间间隔，请选择Remove.

> **Important**
>
> 带宽速率限制间隔不能重叠。时间间隔的开始时间必须在前一个时间间隔的结束时间之后和下一个间隔的开始时间之前。

6. 完成后，选择保存更改.

使用更新网关带宽速率限制AWS SDK for Java

通过以编程方式更新带宽速率限制，您可以在一段时间内自动调整这些限制，例如，使用计划任务进行调整。以下示例展示了如何使用更新网关的带宽速率限制。AWS SDK for Java. 如需使用示例代码，您应该熟悉 Java 控制台应用程序的运行方式。有关更多信息，请参阅 。开始使用中的AWS SDK for Java开发人员指南.

Example ：使用更新网关带宽速率限制AWS SDK for Java

以下 Java 代码示例更新网关的带宽速率限制。要使用此示例代码，您必须提供服务终端节点、网关的 Amazon 资源名称 (ARN) 和上传限制。查看列表AWS可以与 Storage Gateway 一起使用的服务终端节点，请参阅AWS Storage Gateway终端节点和配额中的AWS一般参考.

```
    import java.io.IOException;
```

```
   import com.amazonaws.AmazonClientException;
   import com.amazonaws.auth.PropertiesCredentials;
   import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
   import com.amazonaws.services.storagegateway.model.
UpdateBandwidthRateLimitScheduleRequest;
   import com.amazonaws.services.storagegateway.model.
UpdateBandwidthRateLimitScheduleReturn;

   import java.util.Arrays;
   import java.util.Collections;
   import java.util.List;

   public class UpdateBandwidthExample {

       public static AWSStorageGatewayClient sgClient;

       // The gatewayARN
       public static String gatewayARN = "*** provide gateway ARN ***";

       // The endpoint
       static String serviceURL = "https://storagegateway.us-east-1.amazonaws.com";

       // Rates
       static long uploadRate = 100 * 1024 * 1024;  // Bits per second, minimum 100
Megabits/second

       public static void main(String[] args) throws IOException {

           // Create a storage gateway client
           sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(

UpdateBandwidthExample.class.getResourceAsStream("AwsCredentials.properties")));
           sgClient.setEndpoint(serviceURL);

           UpdateBandwidth(gatewayARN, uploadRate, null); // download rate not
supported by S3 File gateways

       }

       private static void UpdateBandwidth(String gatewayArn, long uploadRate, long
downloadRate) {
           try
           {
```

```
                BandwidthRateLimit bandwidthRateLimit = new
BandwidthRateLimit(downloadRate, uploadRate);
                BandwidthRateLimitInterval noScheduleInterval = new
BandwidthRateLimitInterval()
                    .withBandwidthRateLimit(bandwidthRateLimit)
                    .withDaysOfWeek(Arrays.asList(1, 2, 3, 4, 5, 6, 0))
                    .withStartHourOfDay(0)
                    .withStartMinuteOfHour(0)
                    .withEndHourOfDay(23)
                    .withEndMinuteOfHour(59);
                UpdateBandwidthRateLimitScheduleRequest
updateBandwidthRateLimitScheduleRequest =
                    new UpdateBandwidthRateLimitScheduleRequest()
                    .withGatewayARN(gatewayArn)
                    .with
BandwidthRateLimitIntervals(Collections.singletonList(noScheduleInterval));

                UpdateBandwidthRateLimitScheduleReturn
updateBandwidthRateLimitScheuduleResponse =
sgClient.UpdateBandwidthRateLimitSchedule(updateBandwidthRateLimitScheduleRequest);

                String returnGatewayARN =
updateBandwidthRateLimitScheuduleResponse.getGatewayARN();
                System.out.println("Updated the bandwidth rate limits of " +
returnGatewayARN);
                System.out.println("Upload bandwidth limit = " + uploadRate + " bits
per second");
            }
            catch (AmazonClientException ex)
            {
                System.err.println("Error updating gateway bandwith.\n" +
ex.toString());
            }
        }
    }
```

使用更新网关带宽速率限制AWS SDK for .NET

通过以编程方式更新带宽速率限制，您可以在一段时间内自动调整这些限制，例如，使用计划任务进行调整。以下示例展示了如何通过使用更新网关的带宽速率限制。AWS适用于 .NET 的软件开发工具包 (SDK)。如需使用示例代码，您应该熟悉 .NET 控制台应用程序的运行方式。有关更多信息，请参阅 。开始使用中的AWS SDK for .NET开发人员指南.

Example ：使用更新网关带宽速率限制AWS SDK for .NET

以下 C# 代码示例更新网关的带宽速率限制。要使用此示例代码，您必须提供服务终端节点、网关的 Amazon 资源名称 (ARN) 和上传限制。查看列表AWS可以与 Storage Gateway 一起使用的服务终端节点，请参阅AWS Storage Gateway终端节点和配额中的AWS一般参考.

```
    using System;
    using System.Collections.Generic;
    using System.Linq;
    using System.Text;
    using Amazon.StorageGateway;
    using Amazon.StorageGateway.Model;

    namespace AWSStorageGateway
    {
        class UpdateBandwidthExample
        {
            static AmazonStorageGatewayClient sgClient;
            static AmazonStorageGatewayConfig sgConfig;

            // The gatewayARN
            public static String gatewayARN = "*** provide gateway ARN ***";

            // The endpoint
            static String serviceURL = "https://storagegateway.us-
east-1.amazonaws.com";

            // Rates
            static long uploadRate = 100 * 1024 * 1024;  // Bits per second, minimum
 100 Megabits/second

            public static void Main(string[] args)
            {
                // Create a storage gateway client
                sgConfig = new AmazonStorageGatewayConfig();
                sgConfig.ServiceURL = serviceURL;
                sgClient = new AmazonStorageGatewayClient(sgConfig);

                UpdateBandwidth(gatewayARN, uploadRate, null);

                Console.WriteLine("\nTo continue, press Enter.");
                Console.Read();
            }
```

```
           public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
downloadRate)
           {
               try
               {
                  BandwidthRateLimit bandwidthRateLimit = new
BandwidthRateLimit(downloadRate, uploadRate);
                   BandwidthRateLimitInterval noScheduleInterval = new
BandwidthRateLimitInterval()
                    .withBandwidthRateLimit(bandwidthRateLimit)
                    .withDaysOfWeek(Arrays.asList(1, 2, 3, 4, 5, 6, 0))
                    .withStartHourOfDay(0)
                    .withStartMinuteOfHour(0)
                    .withEndHourOfDay(23)
                    .withEndMinuteOfHour(59);
                  List <BandwidthRateLimitInterval> bandwidthRateLimitIntervals = new
List<BandwidthRateLimitInterval>();
                  bandwidthRateLimitIntervals.Add(noScheduleInterval);
                  UpdateBandwidthRateLimitScheduleRequest
updateBandwidthRateLimitScheduleRequest =
                    new UpdateBandwidthRateLimitScheduleRequest()
                       .withGatewayARN(gatewayARN)
                       .with BandwidthRateLimitIntervals(bandwidthRateLimitIntervals);

                    UpdateBandwidthRateLimitScheduleReturn
updateBandwidthRateLimitScheuduleResponse =
sgClient.UpdateBandwidthRateLimitSchedule(updateBandwidthRateLimitScheduleRequest);
                    String returnGatewayARN =
updateBandwidthRateLimitScheuduleResponse.GatewayARN;
                    Console.WriteLine("Updated the bandwidth rate limits of " +
returnGatewayARN);
                    Console.WriteLine("Upload bandwidth limit = " + uploadRate + " bits
per second");
               }
               catch (AmazonStorageGatewayException ex)
               {
                   Console.WriteLine("Error updating gateway bandwith.\n" +
ex.ToString());
               }
           }
       }
   }
```

使用更新网关带宽速率限制AWS Tools for Windows PowerShell

通过以编程方式更新带宽速率限制，您可以在一段时间内自动调整这些限制，例如，使用计划任务进行调整。以下示例展示了如何使用更新网关的带宽速率限制。AWS Tools for Windows PowerShell. 如需使用示例代码，您应该熟悉 PowerShell脚本 控制台应用程序的运行方式。有关更多信息，请参阅《AWS Tools for Windows PowerShell 用户指南》中的入门。

Example ：使用更新网关带宽速率限制AWS Tools for Windows PowerShell

以下 PowerShell 脚本示例更新网关的带宽速率限制。要使用此示例脚本，您必须提供服务终端节点、网关的 Amazon 资源名称 (ARN) 和上传限制。

```
    <#
    .DESCRIPTION
        Update Gateway bandwidth limits schedule

    .NOTES
        PREREQUISITES:
        1) AWS Tools for PowerShell from https://aws.amazon.com/powershell/
        2) Credentials and region stored in session using Initialize-AWSDefault.
        For more info, see https://docs.aws.amazon.com/powershell/latest/userguide/
specifying-your-aws-credentials.html


    .EXAMPLE
        powershell.exe .\SG_UpdateBandwidth.ps1
    #>

    $UploadBandwidthRate = 100 * 1024 * 1024
    $gatewayARN = "*** provide gateway ARN ***"

    $bandwidthRateLimitInterval = New-Object
 Amazon.StorageGateway.Model.BandwidthRateLimitInterval
    $bandwidthRateLimitInterval.StartHourOfDay = 0
    $bandwidthRateLimitInterval.StartMinuteOfHour = 0
    $bandwidthRateLimitInterval.EndHourOfDay = 23
    $bandwidthRateLimitInterval.EndMinuteOfHour = 59
    $bandwidthRateLimitInterval.DaysOfWeek = 0,1,2,3,4,5,6
    $bandwidthRateLimitInterval.AverageUploadRateLimitInBitsPerSec =
 $UploadBandwidthRate

    #Update Bandwidth Rate Limits
    Update-SGBandwidthRateLimitSchedule -GatewayARN $gatewayARN `
```

```
                                        -BandwidthRateLimitInterval
@($bandwidthRateLimitInterval)

   $schedule =  Get-SGBandwidthRateLimitSchedule -GatewayARN $gatewayARN

   Write-Output("`nGateway: " + $gatewayARN);
   Write-Output("`nNew bandwidth throttle schedule: " +
$schedule.BandwidthRateLimitIntervals.AverageUploadRateLimitInBitsPerSec)
```

使用 AWS Storage Gateway 控制台管理网关更新

Storage Gateway 将定期发布针对您的网关的重要软件更新 您可以在 Storage Gateway 管理控制台上手动应用更新，也可以等待在配置的维护计划期间自动应用更新。尽管 Storage Gateway 每分钟检查一次更新，但仅在有更新时执行维护和重启。

Gateway 软件版本定期包括经过验证的操作系统更新和安全补丁AWS. 这些更新通常每六个月发布一次，并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。

> **Note**
>
> 您应将 Storage Gateway 设备视为托管嵌入式设备，不应尝试以任何方式访问或修改其安装。尝试使用普通网关更新机制之外的其他方法（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。

在将任何更新应用到网关之前，AWS在 SStorage Gateway ways 控制台上显示一条消息以及AWS Health Dashboard. 有关更多信息，请参阅AWS Health Dashboard。VM 不会重启，但网关在更新或重启期间暂时不可用。

部署并激活网关后，将设置默认的每周维护计划。您可以随时修改维护计划。在有更新可用时，Details (详细信息) 选项卡会显示维护消息。您可以在 Details (详细信息) 选项卡上查看上一次更新成功应用于您的网关的日期和时间。

修改维护计划

1. 在打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
2. 在导航窗格上，选择 Gateways (网关)，然后选择要为其修改更新计划的网关。
3. 对于 Actions (操作)，选择 Edit maintenance window (编辑维护时段)，以打开“Edit maintenance start time”(编辑维护起始时间) 对话框。

4. 对于 Schedule (日程安排)，选择 Weekly (每周) 或 Monthly (每月) 以安排更新。
5. 如果您选择 Weekly (每周)，请修改 Day of the week (星期) 和 Time (时间) 的值。

   如果您选择 Monthly (每月)，请修改 Day of the month (日期) 和 Time (时间) 的值。如果选择此选项，但收到错误，则表示您的网关是较旧版本，尚未升级到更新的版本。

   > **Note**
   >
   > 可以为每月第几天设置的最大值为 28。如果选择 28 个，则维护开始时间将在每个月的第 28 天。

   在您下次打开该网关的 Details (详细信息) 选项卡时，您的维护起始时间将会显示在 Details (详细信息) 选项卡上。

在本地控制台上执行维护任务

您可以使用主机的本地控制台执行以下维护任务。本地控制台可以在 VM 主机或 Amazon EC2 实例上执行。许多任务对不同的主机来说都具有共性，但也存在一些差异。

主题

- 在 VM 本地控制台（文件网关）上执行任务
- 在 Amazon EC2 本地控制台（文件网关）上执行任务
- 访问网关本地控制台
- 为网关配置网络适配器

在 VM 本地控制台（文件网关）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 VMware、Microsoft Hyper-V 和基于 Linux 内核的虚拟机 (KVM) 管理程序所共有的。

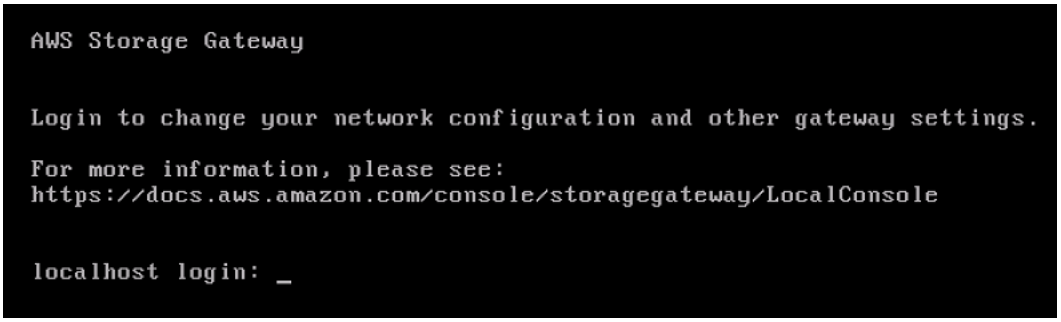
主题

- 登录文件网关本地控制台
- 配置 HTTP 代理
- 配置网关网络设置

- 测试网关的网络连接
- 查看网关系统资源状态
- 配置网关的网络时间协议 (NTP) 服务器
- 在本地控制台上运行存储网关命令
- 为网关配置网络适配器

登录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本地控制台，请使用默认用户名和密码登录。这些默认登录凭证可让您访问一些菜单，这些菜单可用来配置网关网络设置和从本地控制台更改密码。AWS Storage Gateway允许您从 Storage Gateway 控制台设置自己的密码，而不是从本地控制台更改密码。您无需知道默认密码就可以设置新密码。有关更多信息，请参阅登录文件网关本地控制台。



登录网关的本地控制台

- 如果这是您首次登录本地控制台，请使用默认凭证登录 VM。默认用户名为 admin，密码为 password。否则，请使用您的凭证登录。

> **Note**
>
> 我们建议您更改默认密码，方法为从本地控制台菜单（主菜单上的第 6 项）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存储网关命令。您还可以从 Storage Gateway 控制台设置密码。有关更多信息，请参阅登录文件网关本地控制台。

从 Storage Gateway 控制台设置本地控制台密码

在您首次登录本地控制台时，请使用默认凭证登录 VM。对于所有类型的网关，请使用默认凭证。此用户名为 admin，密码为 password。

我们建议您总是在创建新网关后立即设置新密码。如果愿意，您可以从 AWS Storage Gateway 控制台而不是本地控制台设置此密码。您无需知道默认密码就可以设置新密码。

在 Storage Gateway 控制台上设置本地控制台密码

1. 在打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
2. 在导航栏中，选择 Gateways (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)。

   您的新密码将替换默认密码。Storage Gateway 不保存密码，但会将其安全传输给 VM。

   > **Note**
   >
   > 密码可以由键盘上的任何字符组成，长度可以为 1—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 路由所有AWS通过您代理服务器的端点流量。即使使用 HTTP 代理，网关与终端之间的通信也是加密的。有关网关的网络要求的信息，请参阅网络和防火墙要求。

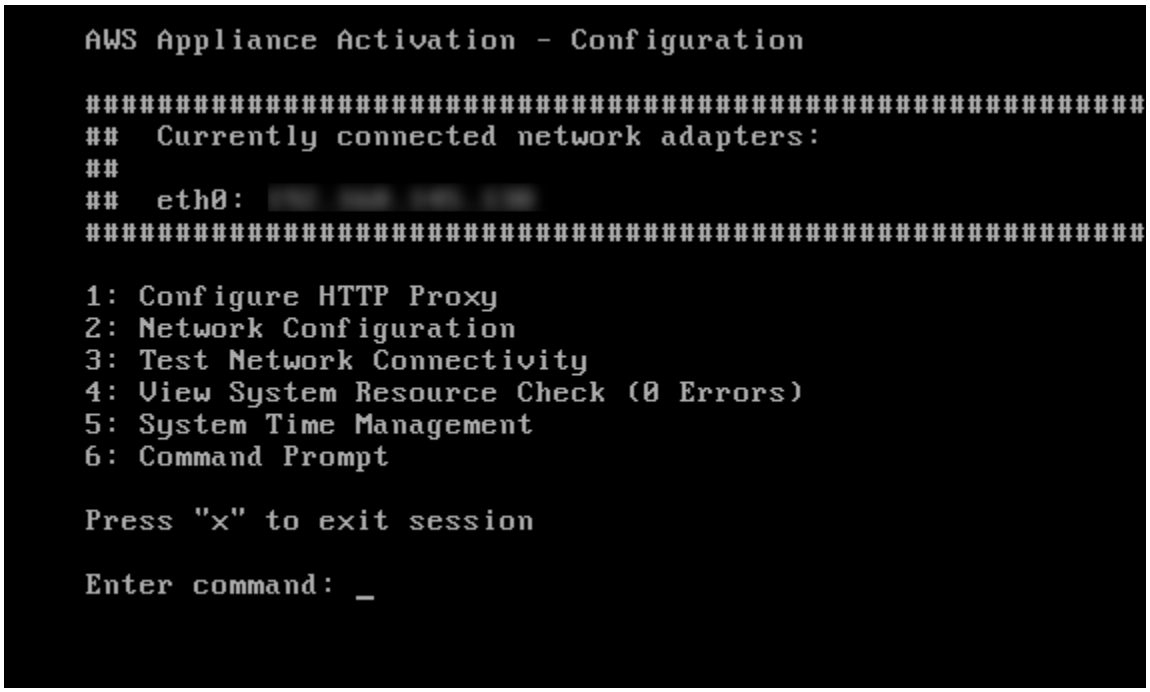
为文件网关配置 HTTP 代理

1. 登录到网关的本地控制台：

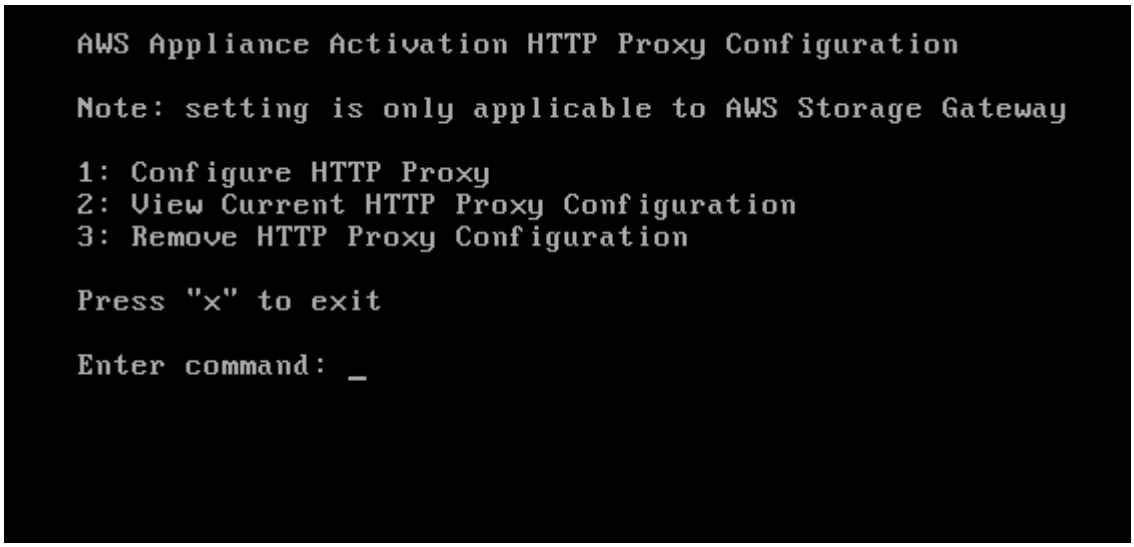
   - 有关登录到 VMware ESXi 本地控制台的更多信息，请参阅使用 VMware ESXi 访问网关本地控制台。

- 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 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. 在存储库的AWS设备激活-配置主菜单，输入**1**开始配置 HTTP 代理。



3. 在 HTTP Proxy Configuration (HTTP 代理配置) 菜单上，输入 **1** 并提供 HTTP 代理服务器的主机名。



您可以从该菜单配置其他 HTTP 设置，如下所示。

To	请执行该操作
配置 HTTP 代理	输入 **1**。 您需要提供主机名称和端口以完成配置。
查看当前的 HTTP 代理配置	输入 **2**。 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	输入 **3**。 消息 HTTP Proxy Configuration Removed 将会显示。

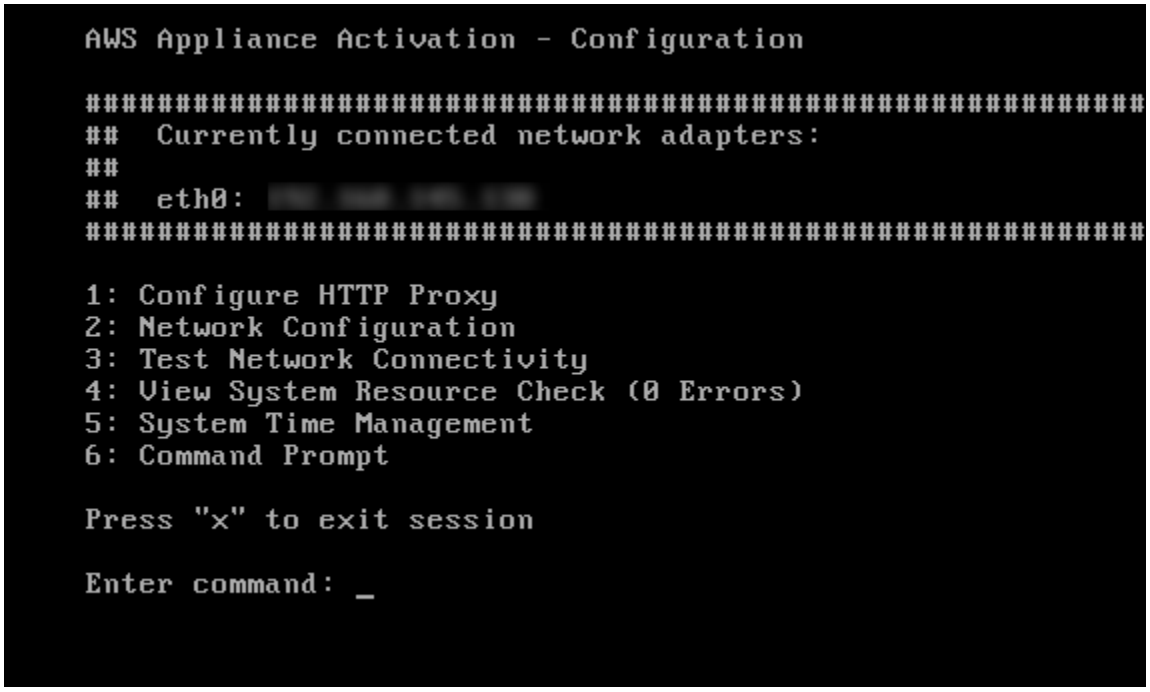
4. 重新启动 VM 以应用 HTTP 配置设置。

配置网关网络设置

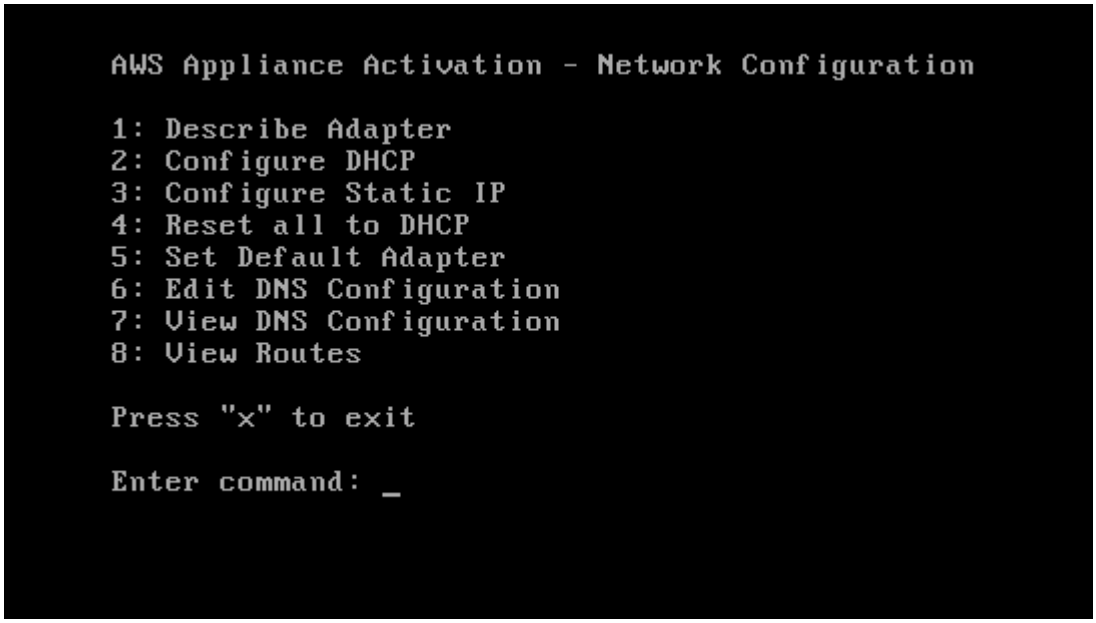
网关的默认网络配置是动态主机配置协议 (DHCP)。使用 DHCP，您的网关将被自动分配 IP 地址。在某些情况下，您可能需要手动将网关的 IP 地址分配为静态 IP 地址，如下所述。

如需将您的网关配置为使用静态 IP 地址。

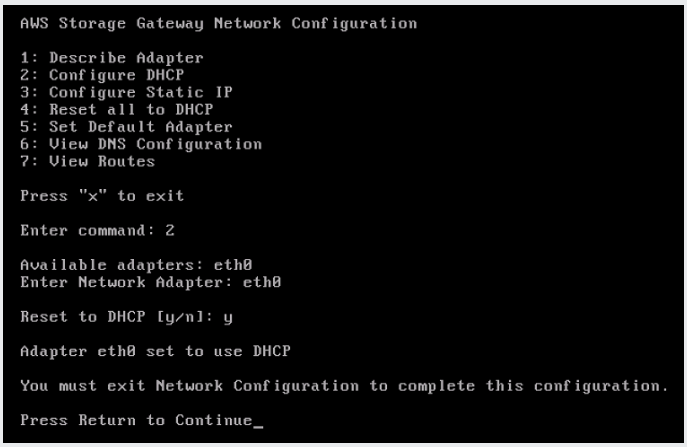
1. 登录到网关的本地控制台：
   - 有关登录到 VMware ESXi 本地控制台的更多信息，请参阅使用 VMware ESXi 访问网关本地控制台。
   - 有关登录到 Microsoft Hyper-V 本地控制台的更多信息，请参阅使用 Microsoft Hyper-V 访问网关本地控制台。
   - 有关登录到 KVM 本地控制台的更多信息，请参阅使用 Linux KVM 访问网关本地控制台。
2. 在存储库的AWS设备激活-配置主菜单，输入**2**开始配置网络。



3. 在 Network Configuration (网络配置) 菜单上，选择下列选项之一。



To	请执行该操作
获取有关网络适配器的信息	输入 **1**。 将显示一个适配器名称的列表，系统会提示您输入一个适配器名称，例如，**eth0**. 如果您指定的

To	请执行该操作
	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（选项）时，您可使用相同的适配器名称。3) 或设置网关的默认路由适配器（选项）时，5)。
配置 DHCP	输入 **2**。 系统将提示您将网络接口配置为使用 DHCP。 

To	请执行该操作
为网关配置静态 IP 地址	输入 **3**。 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，您必须从 Storage Gateway 控制台将其关闭，然后重启网关以便让设置生效。有关更多信息，请参阅关闭网关 VM。 如果网关使用一个以上的网络接口，您必须将所有启用的接口设置为使用 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，

To	请执行该操作
	则会禁用另一个接口。在这种情况下，如需启用此接口，您必须将其设置为静态 IP。 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。
将网关的所有网络配置重置为 DHCP	输入 **4**。 所有网络接口均设置为使用 DHCP。 **Important** 如果网关已激活，您必须从 Storage Gateway 控制台关停并重启网关以便让设置生效。有关更多信息，请参阅关闭网关 VM。
设置网关的默认路由适配器	输入 **5**。 将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 **6**。 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。

To	请执行该操作
查看网关的 DNS 配置	输入 **7**。 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 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 **8**。 网关的默认路由将会显示。

测试网关的网络连接

可使用网关的本地控制台测试网络连接。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：
   - 有关登录到 VMware ESXi 本地控制台的更多信息，请参阅使用 VMware ESXi 访问网关本地控制台。
   - 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 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. 来自AWS设备激活-配置主菜单中，输入相应的数字进行选择测试网络连接.

   如果您的网关已激活，则会立即开始连接测试。对于尚未激活的网关，必须指定终端节点类型和 AWS 区域如以下步骤所述。
3. 如果您的网关尚未激活，请输入相应的数字以选择网关的终端节点类型。

4. 如果选择了公共终端节点类型，请输入相应的数字以选择AWS 区域你想测试。对于支持AWS 区域列表AWS您可以用于 Storage Gateway 的服务终端节点，请参阅AWS Storage Gateway终端节点和配额中的AWS一般参考.

随着测试的进展，每个终端节点都会显示[PSED]要么[失败]，指示连接状态，如下所示：

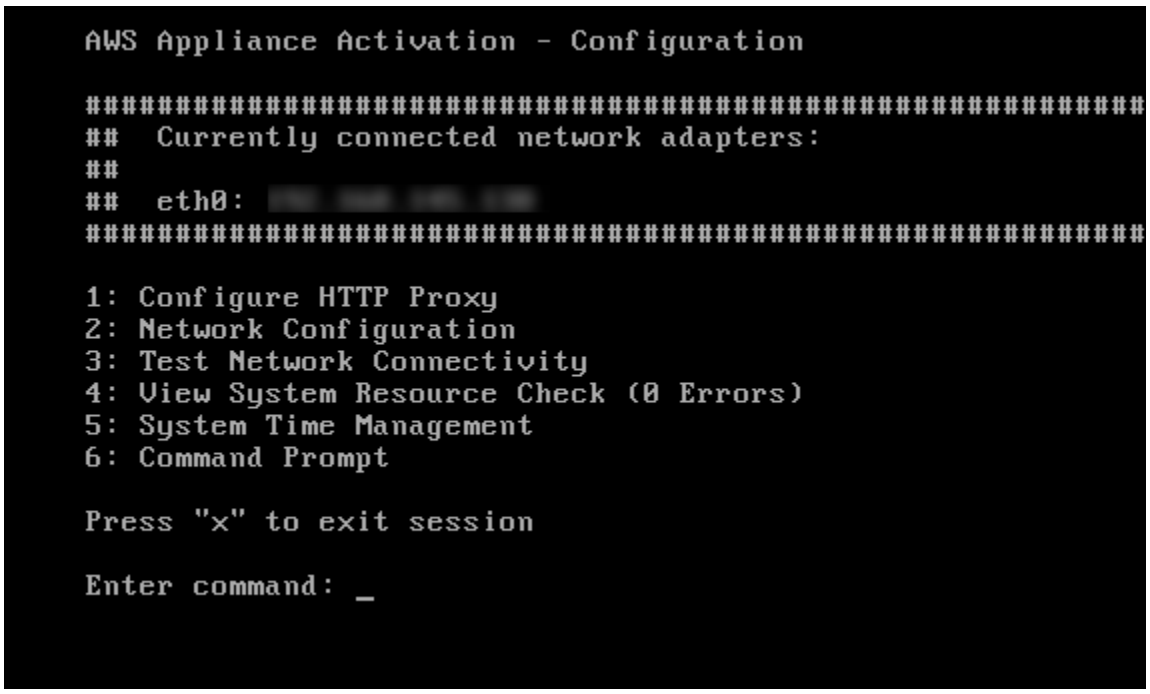
消息	描述
[PASSED]	Storage Gateway 具有网络连接。
[失败]	Storage Gateway 没有网络连接。

查看网关系统资源状态

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：
   - 有关登录到 VMware ESXi 控制台的更多信息，请参阅使用 VMware ESXi 访问网关本地控制台。
   - 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 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，输入**4**以查看系统资源检查的结果。



控制台为每个资源显示 [OK]、[WARNING] 或 [FAIL] 消息，如下表中所述。

消息	描述
[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，但您的网关可继续正常工作。Storage Gateway 显示一条消息以描述资源检查结果。
[FAIL]	资源不满足最低要求。网关可能无法正常工作。Storage Gateway 显示一条消息以描述资源检查结果。

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

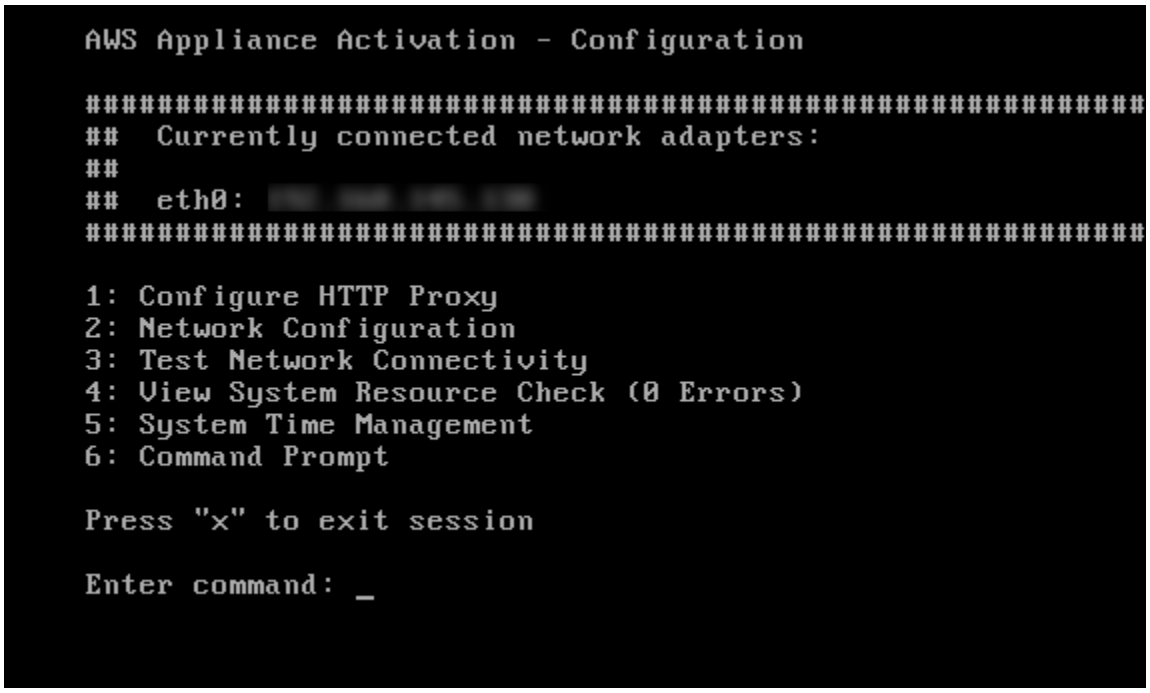
您可以使用管理程序主机查看和编辑网络时间协议 (NTP) 服务器配置并同步您网关上的 VM 时间。

管理系统时间

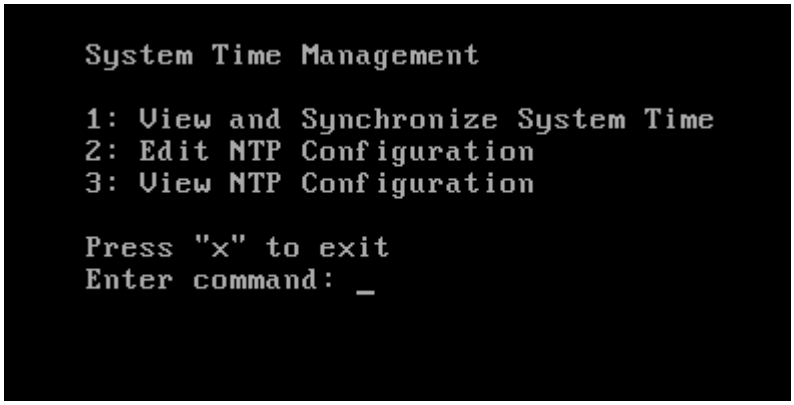
1. 登录到网关的本地控制台：

   - 有关登录到 VMware ESXi 本地控制台的更多信息，请参阅使用 VMware ESXi 访问网关本地控制台。
   - 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 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，输入**5**来管理系统的时间。



3. 在 System Time Management (系统时间管理) 菜单中，选择下列选项之一。



To	请执行该操作
查看 VM 时间并将其与 NTP 服务器时间同步。	输入 **1**。 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 VMware ESXi 上部署的网关，设置管理程序主机时间并将 VM 时间与主机同步，就足以避免时间偏差。有关更多信息，请参阅将 VM 时间与主机时间同步。 对于在 Microsoft Hyper-V 上部署的网关，您应定期查看 VM 的时间。有关更多信息，请参阅同步您的网关 VM 时间。 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 **2**。 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 **3**。 这将显示您的 NTP 服务器配置。

在本地控制台上运行存储网关命令

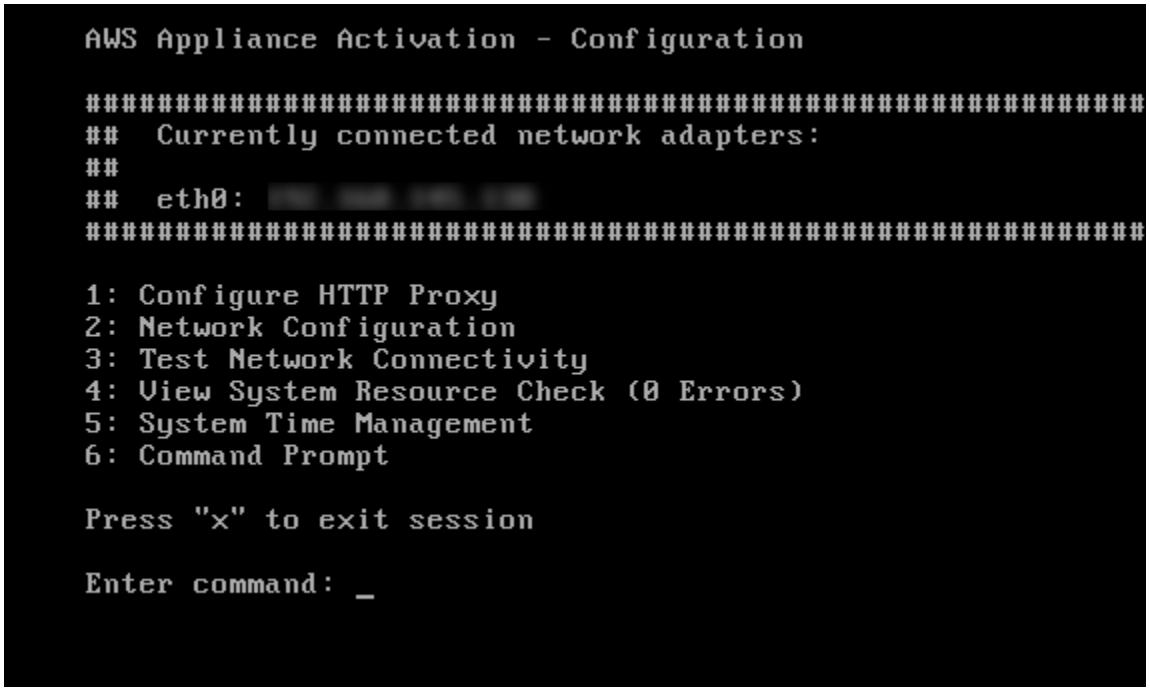
Storage Gateway 中的虚拟机本地控制台可帮助提供安全的环境来配置和诊断网关问题。通过使用本地控制台命令，您可以执行维护任务，例如，保存路由表、连接到 Amazon Web Services Services Support 等。

运行配置或诊断命令

1. 登录到网关的本地控制台：

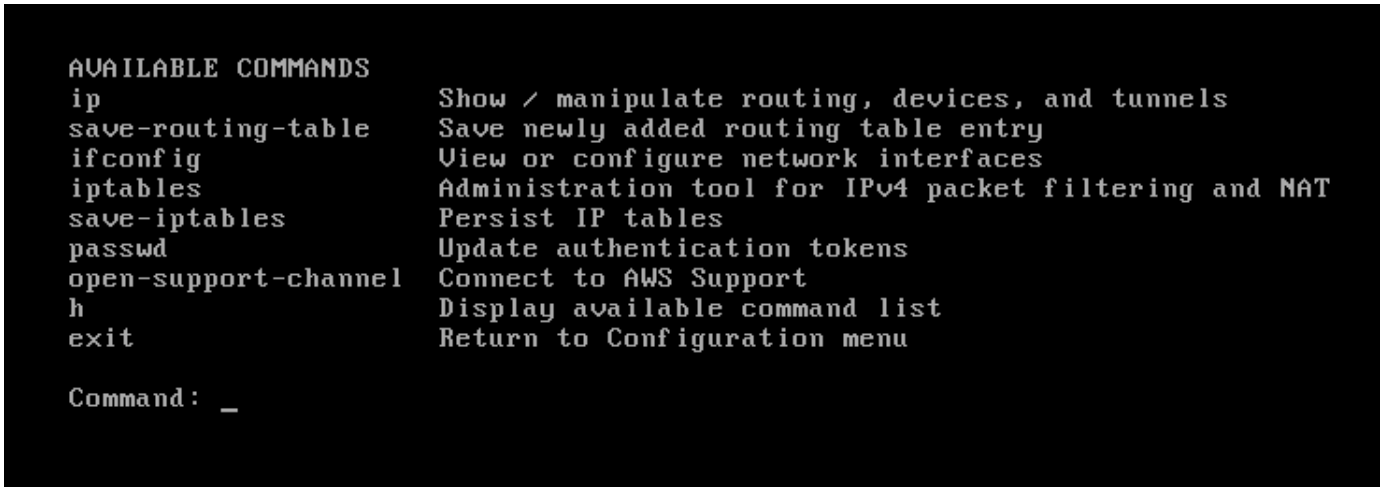
   - 有关登录到 VMware ESXi 本地控制台的更多信息，请参阅使用 VMware ESXi 访问网关本地控制台。
   - 有关登录到 Microsoft Hyper-V 本地控制台的更多信息，请参阅使用 Microsoft Hyper-V 访问网关本地控制台。
   - 有关登录到 KVM 本地控制台的更多信息，请参阅使用 Linux KVM 访问网关本地控制台。

2. 在存储库的AWS设备激活-配置主菜单，输入**6**为了命令提示符.



3. 在存储库的AWS设备激活-命令提示符控制台，输入**h**，然后按返回值键。

   控制台将显示 AVAILABLE COMMANDS (可用命令) 菜单与命令用途，如以下屏幕截图所示。



4. 在命令提示符处，输入要使用的命令并按说明操作。

要了解命令，请在命令提示符处输入命令名称。

为网关配置网络适配器

默认情况下，Storage Gateway 配置为使用 E1000 网络适配器类型，但您可以将您的网关重新配置为使用 VMXNET3 (10 GbE) 网络适配器。还可配置 Storage Gateway，以便能通过多个 IP 地址访问它。您可以通过将网关配置为使用多个网络适配器来完成此操作。

主题

- 将网关配置为使用 VMXNET3 网络适配器

将网关配置为使用 VMXNET3 网络适配器

Storage Gateway 在 VMware ESXi 和 Microsoft Hyper-V 管理程序主机中都支持 E1000 网络适配器类型。但是，VMXNET3 (10 GbE) 网络适配器类型仅在 VMware ESXi 管理程序主机中受支持。如果您的网关承载在 VMware ESXi 管理程序上，则可将网关重新配置为使用 VMXNET3 (10 GbE) 适配器输入。有关此适配器的更多信息，请参阅 VMware 网站。

对于 KVM 管理程序主机，Storage Gateway 支持使用`virtio`网络设备驱动程序。不支持为 KVM 主机使用 E1000 网络适配器类型。

> **Important**
>
> 要选择 VMXNET3，您的来宾操作系统输入必须是 Other Linux64 (其他 Linux64)。

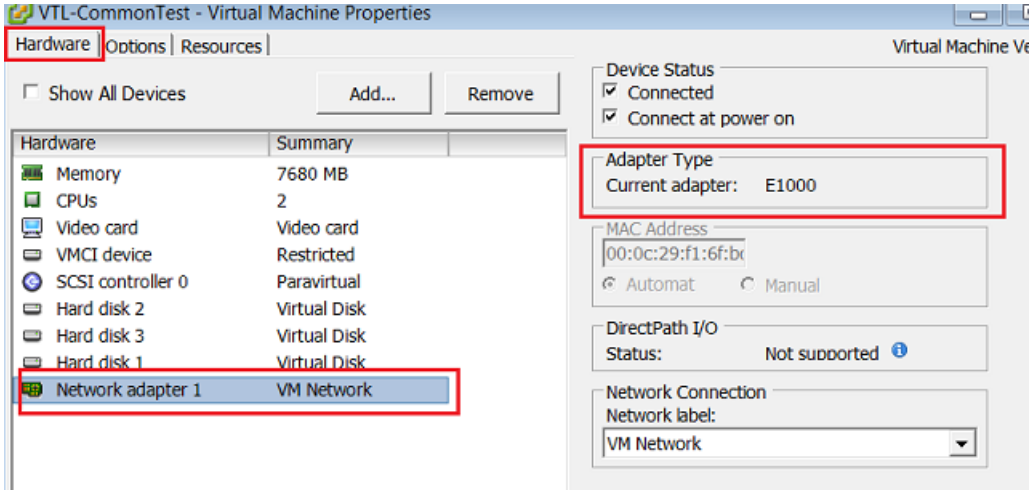
您可执行以下步骤将网关配置为使用 VMXNET3 适配器：

1. 删除默认的 E1000 适配器。
2. 添加 VMXNET3 适配器。
3. 重新启动网关。
4. 为网络配置适配器。

有关如何执行每个步骤的详细信息请参阅

删除默认的 E1000 适配器并将您的网关配置为使用 VMXNET3 适配器。

1. 在 VMware 中，打开网关的上下文（右键单击）菜单，然后选择编辑设置.
2. 在虚拟机属性窗口中，选择Hardware (硬件)选项卡。
3. 对于 Hardware，选择 Network adapter。请注意，当前适配器为 Adapter Enter (适配器输入) 部分中的 E1000。将此适配器替换为 VMXNET3 适配器。



4. 选择 E1000 网络适配器，然后选择 Remove。在此示例中，E1000 网络适配器为网络适配器 1.

> **Note**
>
> 尽管您可以同时在网关中运行 E1000 和 VMXNET3 网络适配器，但我们不建议这样做，因为这可能会导致网络问题。

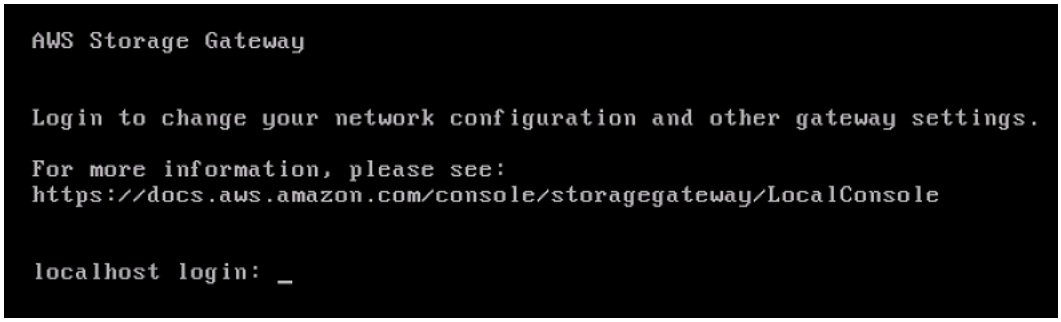
5. 选择Add以打开 “添加硬件” 向导。
6. 选择 Ethernet Adapter，然后选择 Next。
7. 在 “网络输入” 向导中，选择**VMXNET3**为了进入适配器，然后选择下一步.

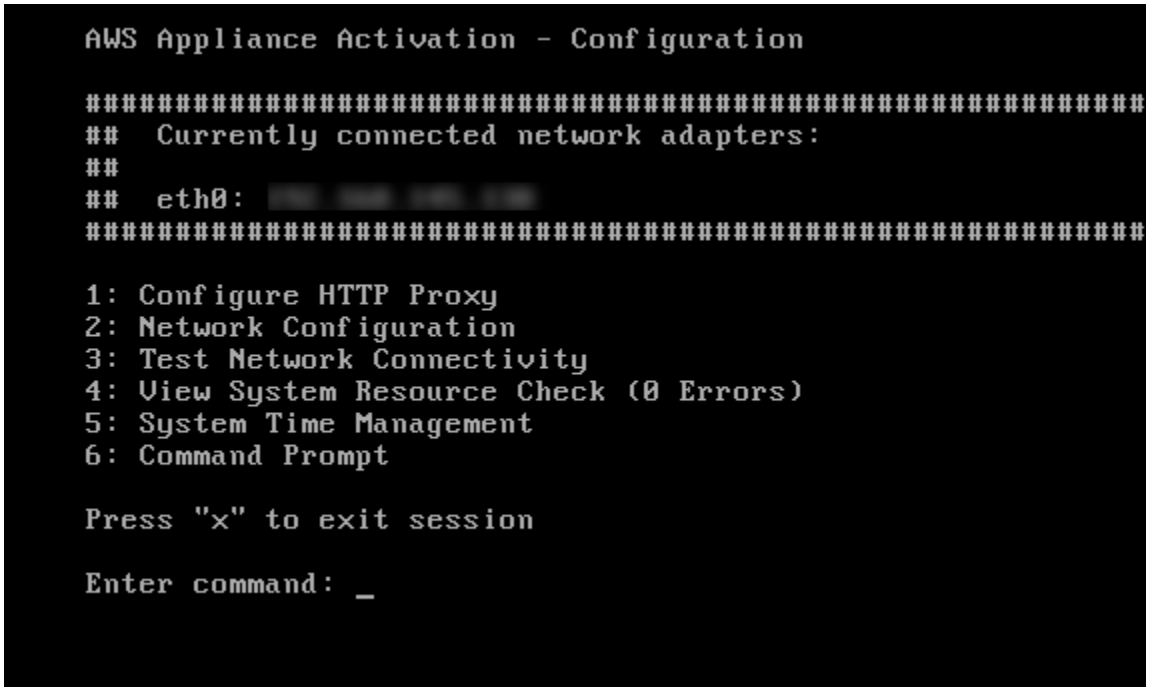
8. 在“Virtual Machine Properties (虚拟机属性)”向导中，验证 Adapter Enter (适配器输入) 部分中 Current Adapter (当前适配器) 是否设置为 VMXNET3，然后选择 OK (确定)。
9. 在 VMware VSphere 客户端中，关闭您的网关。
10. 在 VMware VSphere 客户端中，重新启动您的网关。

在网关重新启动后，重新配置刚添加的适配器以确保建立 Internet 网络连接。

为网络配置适配器

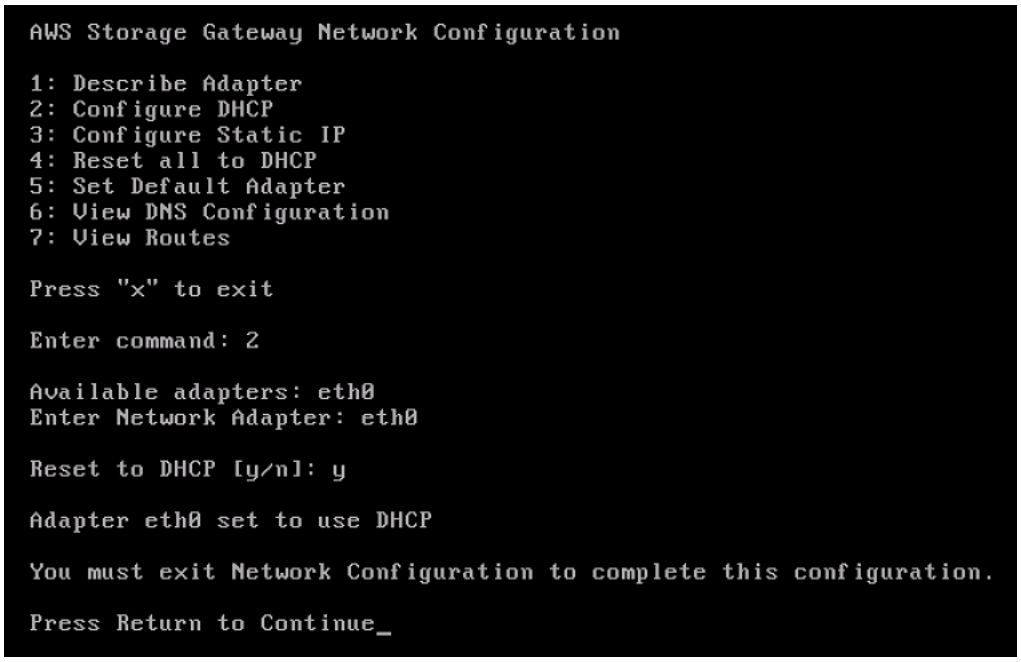
1. 在 VSphere 客户端中，选择 Console 选项卡以启动本地控制台。在本配置任务中，使用默认登录凭证登录网关的本地控制台。有关如何使用默认凭证登录的信息，请参阅登录文件网关本地控制台。





2. 在提示符处，输入 **2** 以选择 Network Configuration (网络适配器)，然后按 **Enter** 以打开网络配置菜单。

3. 在提示符处，输入 **4** 以选择 Reset all to DHCP (全部重置为 DHCP)，然后在命令提示符处输入 **y**（表示“是”）以将所有适配器重置为使用动态主机配置协议 (DHCP)。所有可用适配器均设置为使用 DHCP。



如果网关已激活，您必须从 Storage Gateway 管理控制台将其关闭，然后重启网关。在网关重新启动后，必须测试 Internet 网络连接。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。

在 Amazon EC2 本地控制台（文件网关）上执行任务

某些维护任务要求您在运行部署在 Amazon EC2 实例上的网关时登录到本地控制台。在本节中，您可以在找到有关如何登录到本地控制台并执行维护任务的信息。

主题

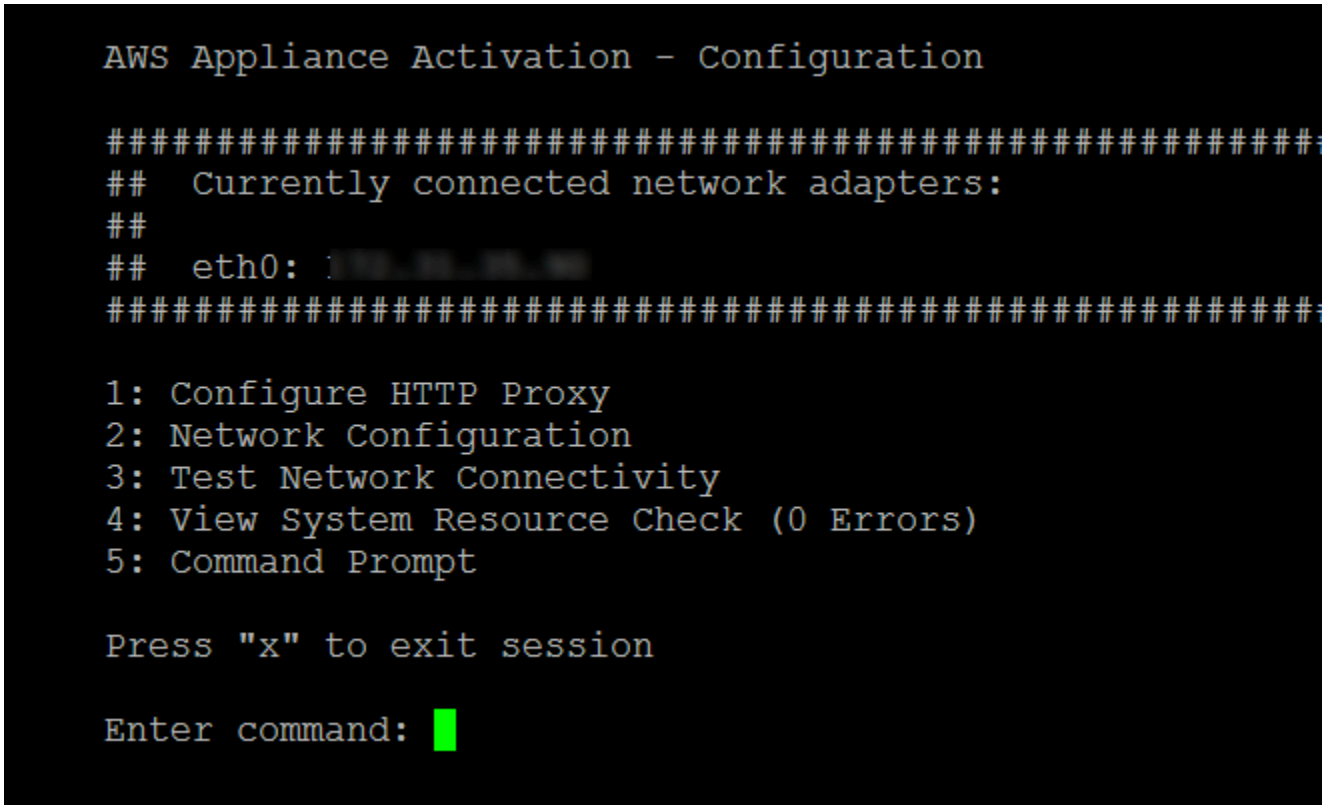
- 登录到您的 Amazon EC2 网关本地控制台
- 通过 HTTP 代理路由部署在 EC2 上的网关
- 配置网关网络设置
- 测试网关的网络连接
- 查看网关系统资源状态
- 在本地控制台上运行 Storage Gateway 命令

登录到您的 Amazon EC2 网关本地控制台

您可以使用安全外壳 (SSH) 客户端连接到 Amazon EC2 实例。有关详细信息，请参阅连接到您的实例中的Amazon EC2 用户指南. 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 密钥对中的Amazon EC2 用户指南。

登录网关本地控制台

1. 登录到本地控制台。如果要从 Windows 计算机连接到 EC2 实例，请以 admin 身份登录。
2. 登录后，会看到AWS设备激活-配置主菜单，如以下屏幕截图所示。



要了解相关内容	请参阅此主题
为网关配置 HTTP 代理	通过 HTTP 代理路由部署在 EC2 上的网关
为网关配置网络设置	测试网关的网络连接
测试网关连接性	测试网关的网络连接
查看系统资源检查	登录到您的 Amazon EC2 网关本地控制台.

要了解相关内容	请参阅此主题
运行 Storage Gateway 控制台命令	在本地控制台上运行 Storage Gateway 命令

要关闭网关，请输入 **0**。

要退出配置会话，请输入 **x** 以退出菜单。

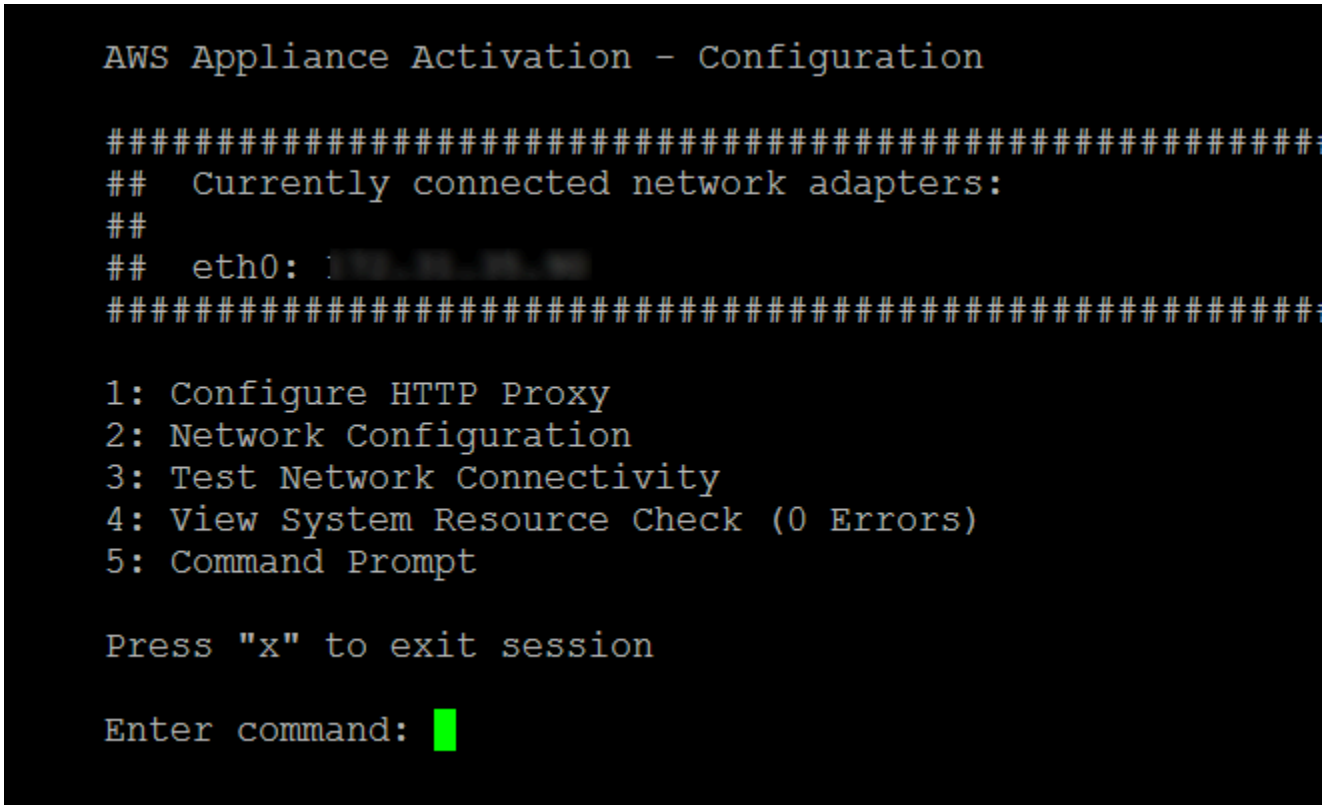
通过 HTTP 代理路由部署在 EC2 上的网关

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

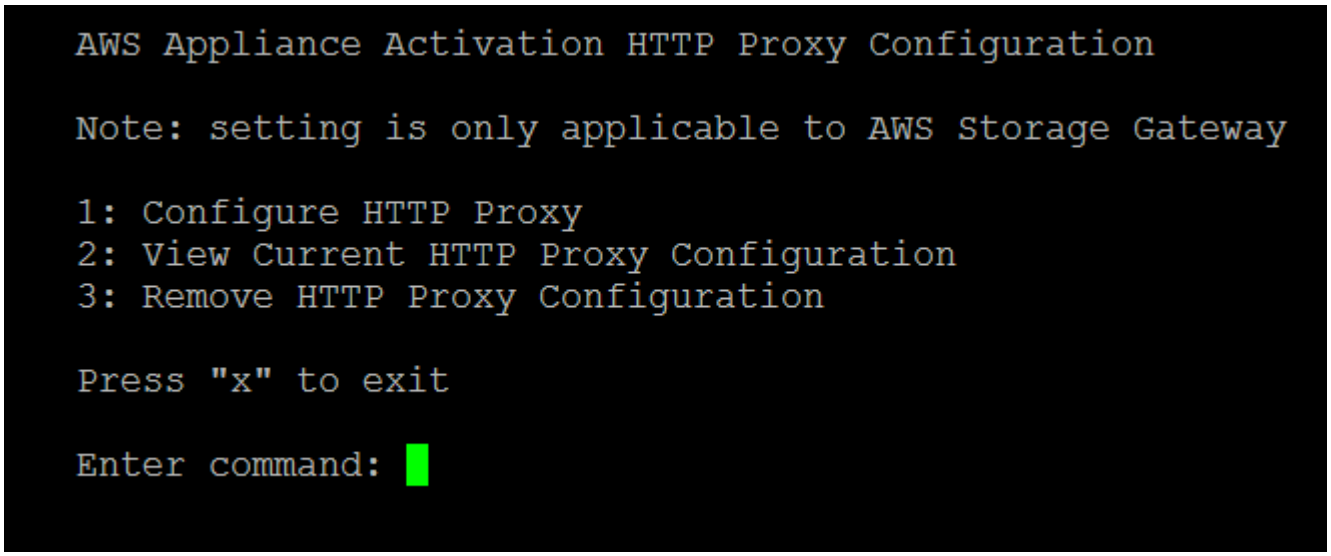
如果网关必须使用代理服务器与 Internet 通信，则需要为网关配置 HTTP 代理设置。为此，您可以为运行代理的主机指定 IP 地址和端口号。完成此操作后，Storage Gateway 路由所有AWS通过您代理服务器的端点流量。即使使用 HTTP 代理，网关与终端之间的通信也是加密的。

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 登录到您的 Amazon EC2 网关本地控制台。
2. 在存储库的AWS设备激活-配置主菜单，输入**1**开始配置 HTTP 代理。



3. 在AWS设备激活-配置HTTP 代理配置菜单。



To	请执行此操作
配置 HTTP 代理	输入 **1**。

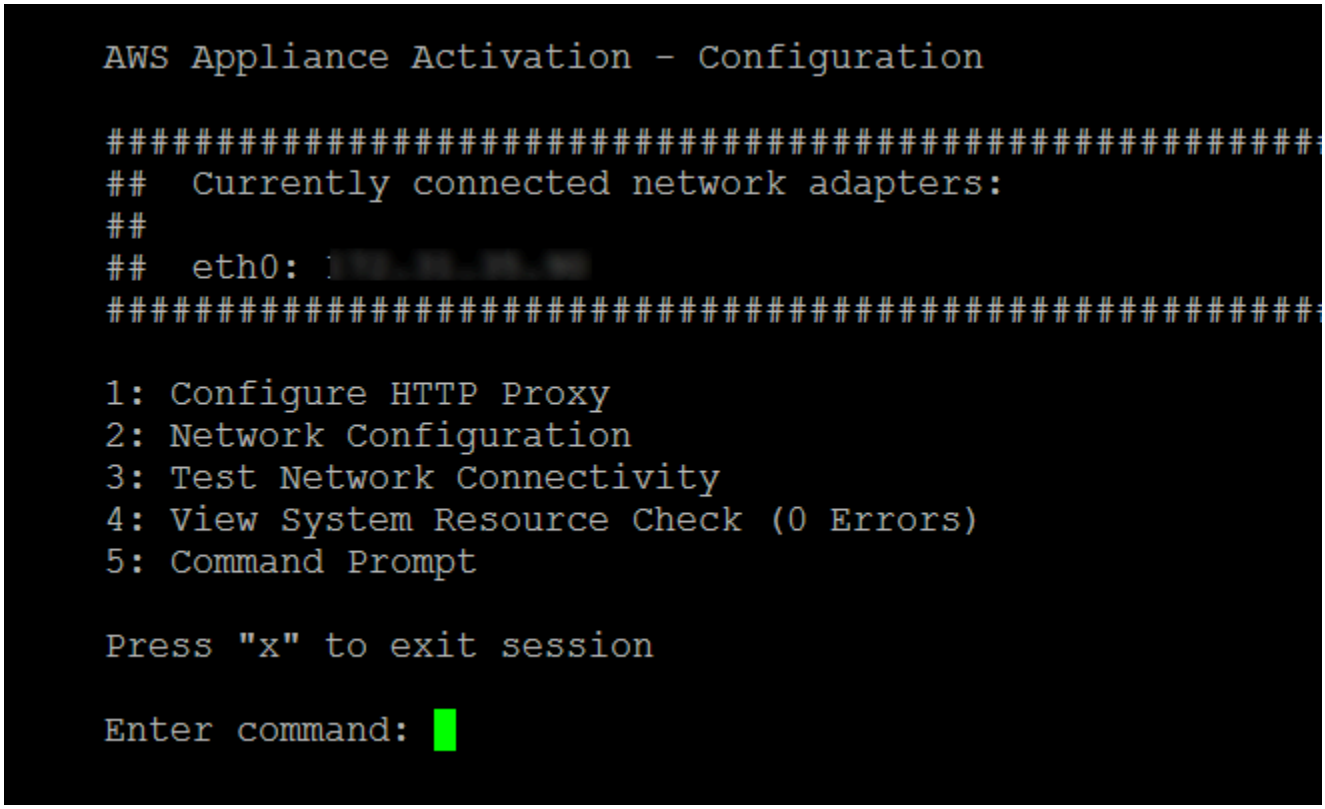
To	请执行此操作
	您需要提供主机名称和端口以完成配置。
查看当前的 HTTP 代理配置	输入 **2**。 如果未配置 HTTP 代理，则会显示消息 `HTTP Proxy not configured` 。如果 HTTP 代理已配置，则会显示代理的主机名称和端口。
移除 HTTP 代理配置	输入 **3**。 消息 `HTTP Proxy Configuration Removed` 将会显示。

配置网关网络设置

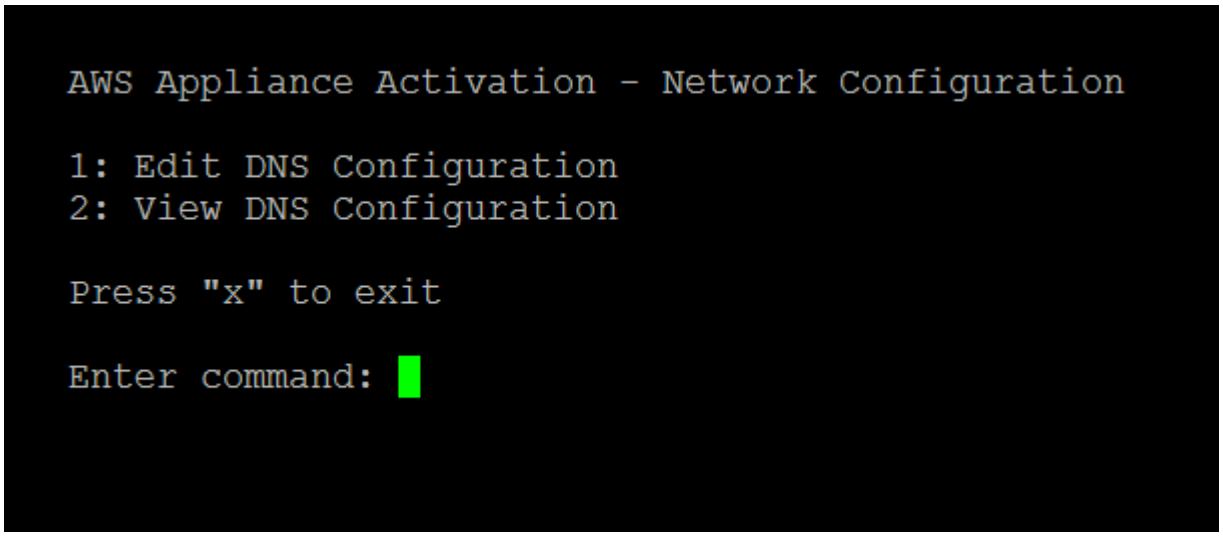
您可以通过本地控制台查看和配置域名服务器 (DNS) 设置。

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。有关说明，请参阅 登录到您的 Amazon EC2 网关本地控制台。
2. 在存储库的AWS设备激活-配置主菜单，输入**2**开始配置 DNS 服务器。



3. 在 Network Configuration (网络配置) 菜单上，选择下列选项之一。



To	请执行此操作
编辑网关的 DNS 配置	输入 **1**。

To	请执行此操作
	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。
查看网关的 DNS 配置	输入 **2**。 这将显示主 DNS 和备用 DNS 服务器的可用适配器。

测试网关的网络连接

可使用网关的本地控制台测试网络连接。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 登录到您的 Amazon EC2 网关本地控制台。
2. 来自AWS设备激活-配置主菜单中，输入相应的数字进行选择测试网络连接.

   如果您的网关已激活，则会立即开始连接测试。对于尚未激活的网关，必须指定终端节点类型和 AWS 区域如以下步骤所述。
3. 如果您的网关尚未激活，请输入相应的数字以选择网关的终端节点类型。
4. 如果选择了公共终端节点类型，请输入相应的数字以选择AWS 区域你想测试。对于支持AWS 区域列表AWS您可以用于 Storage Gateway 的服务终端节点，请参阅AWS Storage Gateway终端节点和配额中的AWS一般参考.

随着测试的进展，每个终端节点都会显示[PSED]要么[失败]，指示连接状态，如下所示：

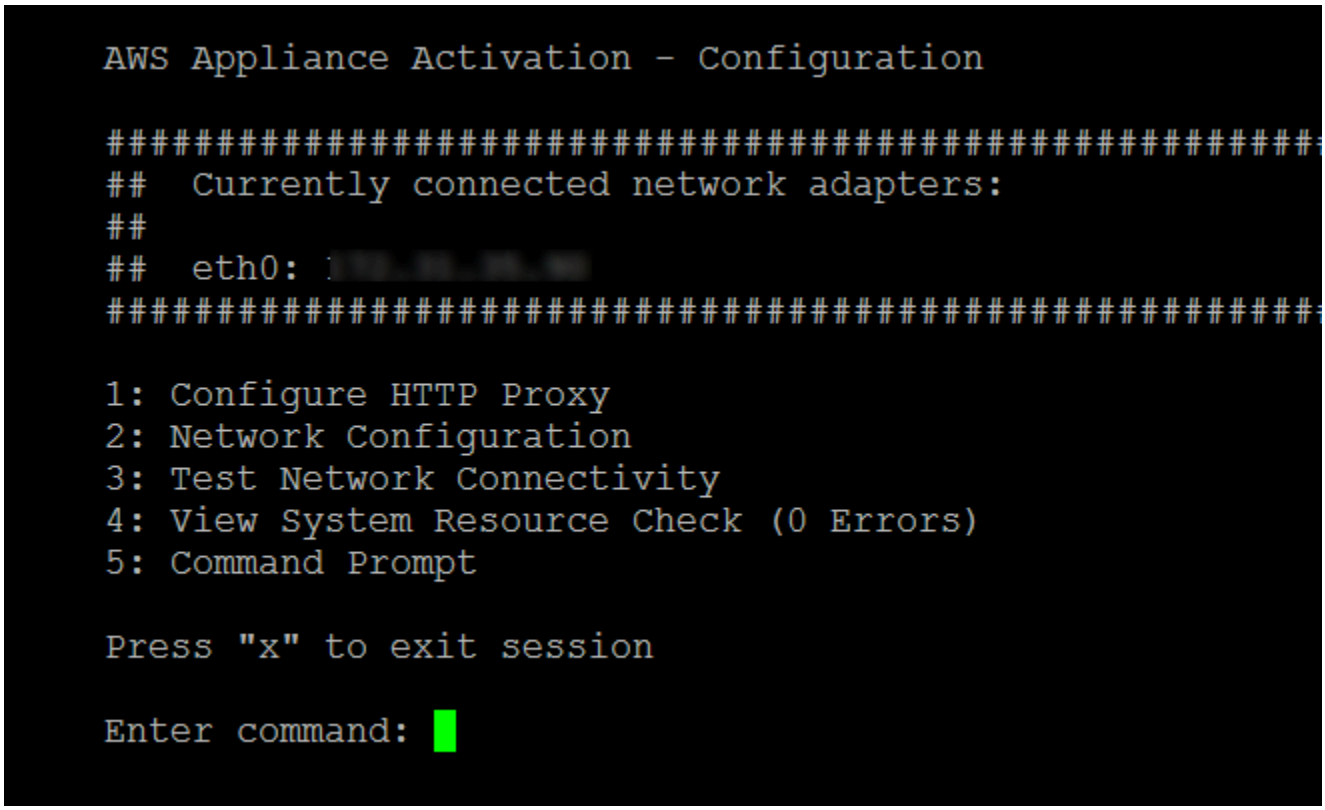
消息	描述
[PASSED]	Storage Gateway 具有网络连接。
[失败]	Storage Gateway 没有网络连接。

查看网关系统资源状态

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。有关说明，请参阅 登录到您的 Amazon EC2 网关本地控制台。
2. 在Storage Gateway 配置主菜单，输入**4**以查看系统资源检查的结果。



控制台为每个资源显示 [OK]、[WARNING] 或 [FAIL] 消息，如下表中所述。

消息	描述
[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，但您的网关可继续正常工作。Storage Gateway 显示一条消息以描述资源检查结果。

消息	描述
[FAIL]	资源不满足最低要求。网关可能无法正常工作。Storage Gateway 显示一条消息以描述资源检查结果。

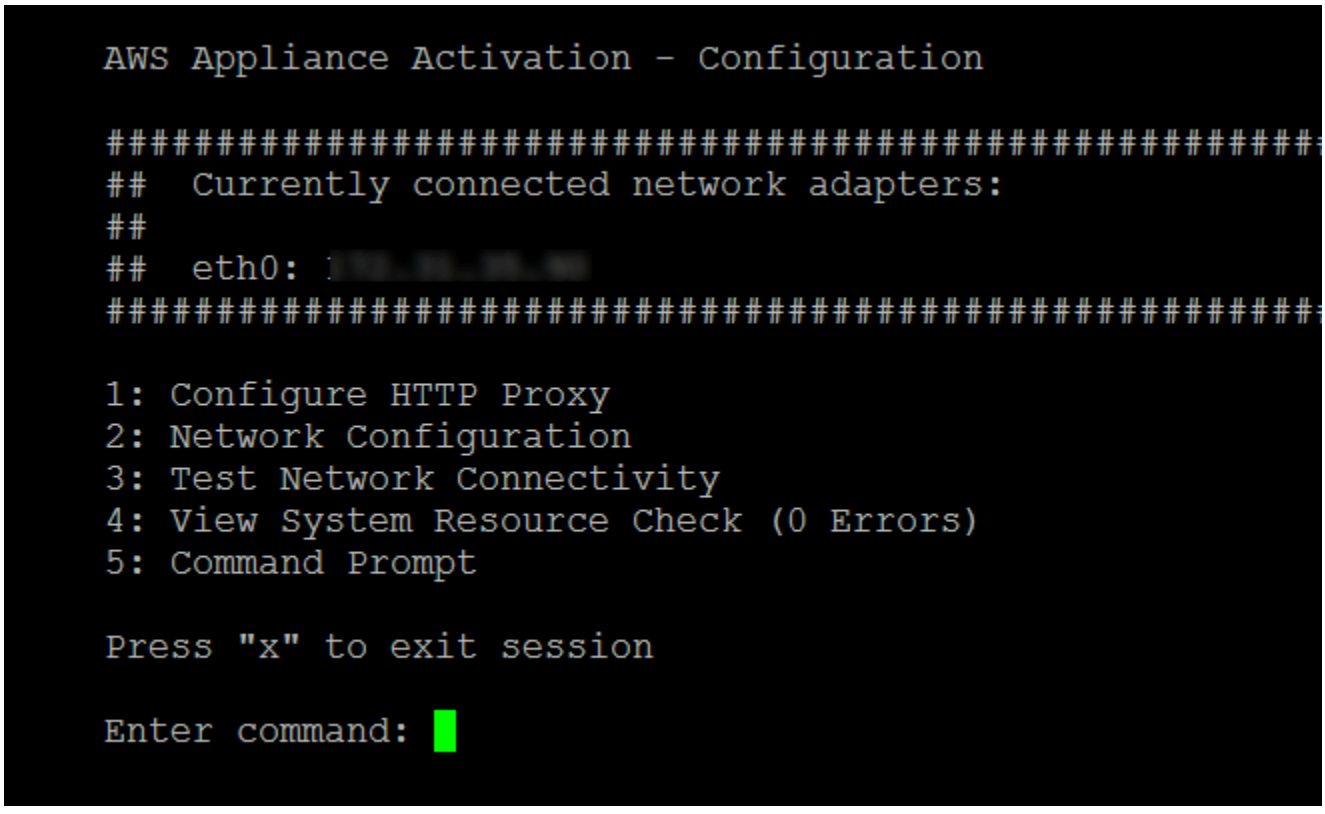
控制台还会在资源检查菜单选项旁边显示错误和警告的数量。

在本地控制台上运行 Storage Gateway 命令

AWS Storage Gateway 控制台可帮助提供安全的环境来配置和诊断网关问题。通过使用控制台命令，您可以执行维护任务，例如，保存路由表或连接到 Amazon Web Services Services Support。

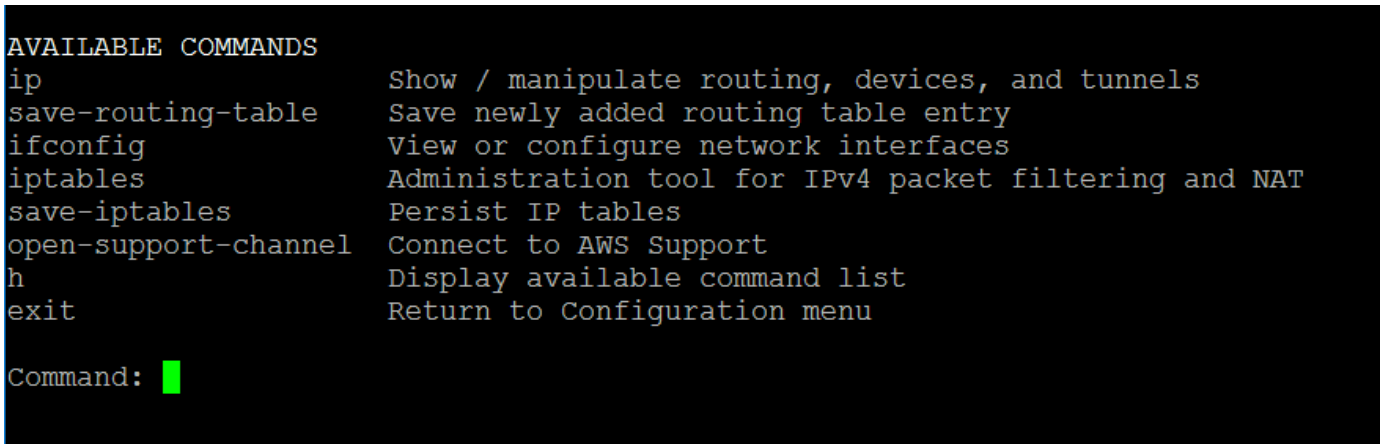
运行配置或诊断命令

1. 登录到网关的本地控制台。有关说明，请参阅 登录到您的 Amazon EC2 网关本地控制台。
2. 在AWS设备激活配置主菜单，输入**5**为了网关控制台.



3. 在命令提示符处，输入 **h**，然后按 Return 键。

控制台将显示包含可用命令的 AVAILABLE COMMANDS (可用命令) 菜单。该菜单后面将显示网关控制台提示，如以下屏幕截图所示。



4. 在命令提示符处，输入要使用的命令并按说明操作。

要了解命令，请在命令提示符处输入命令名称。

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，您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 VMware ESXi 访问网关本地控制台
- 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

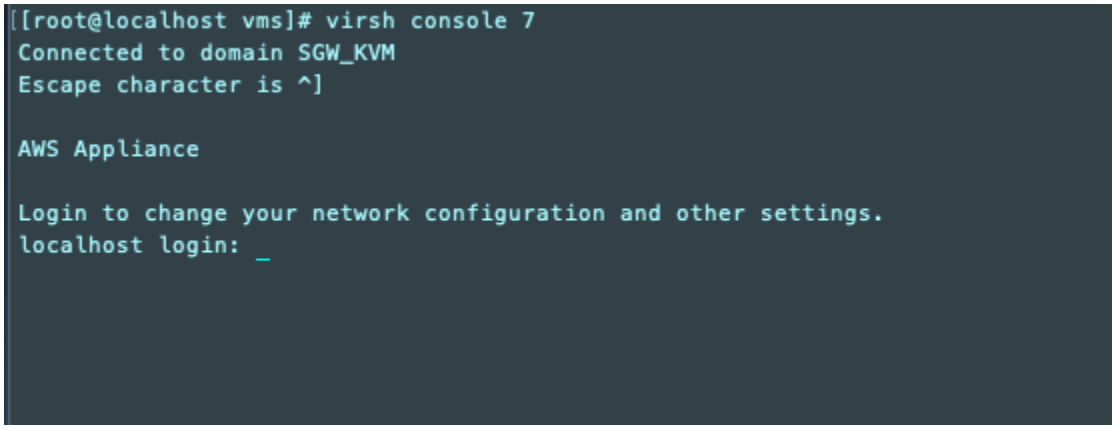
1. 使用以下命令列出 KVM 中当前可用的虚拟机。

```
# virsh list
```

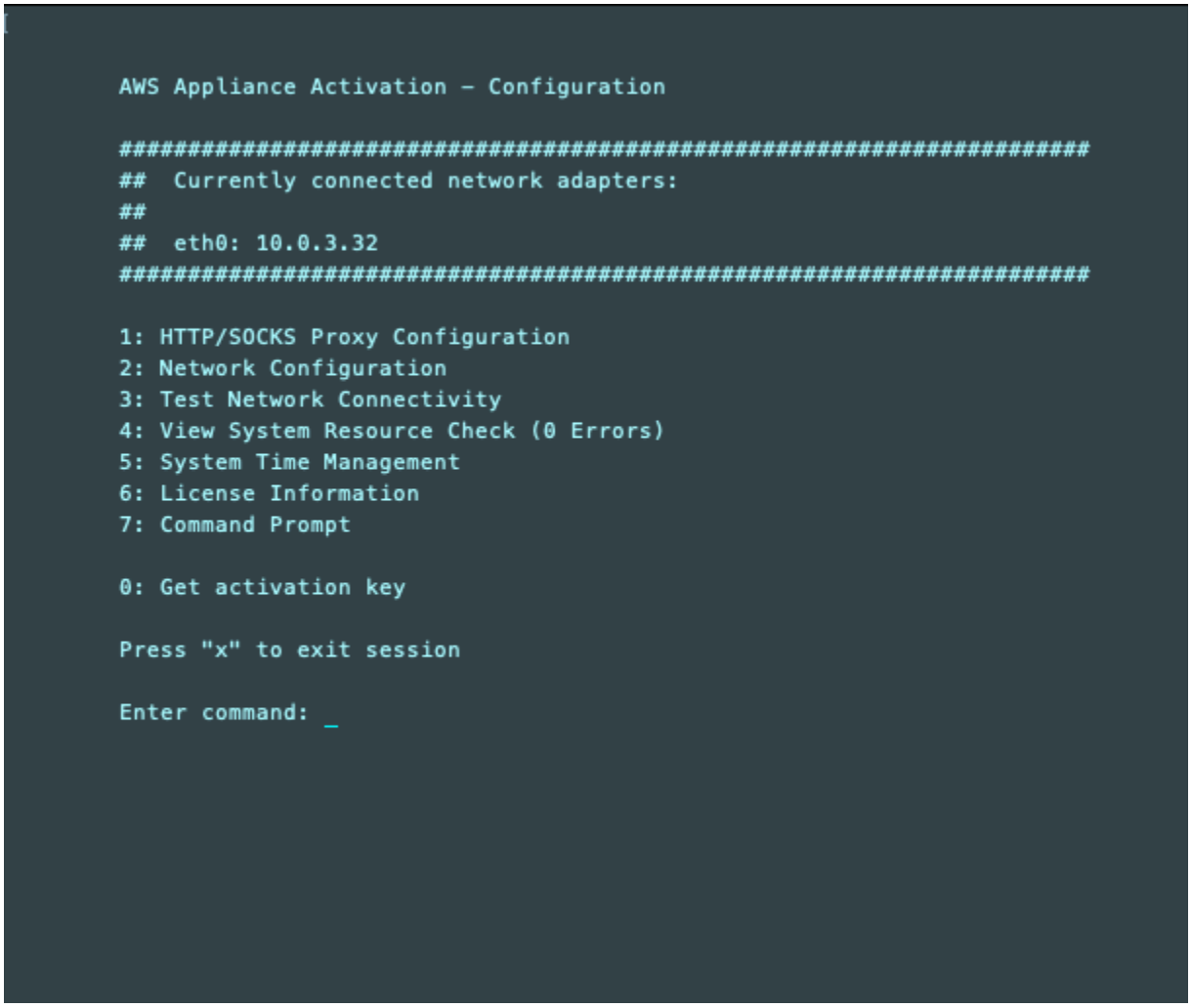
您可以按 Id 选择可用的虚拟机。

2. 使用以下命令访问本地控制台。

```
# virsh console VM_Id
```



3. 要获取用于登录本地控制台的默认凭证，请参阅登录文件网关本地控制台。
4. 登录后，您可以激活和配置网关。

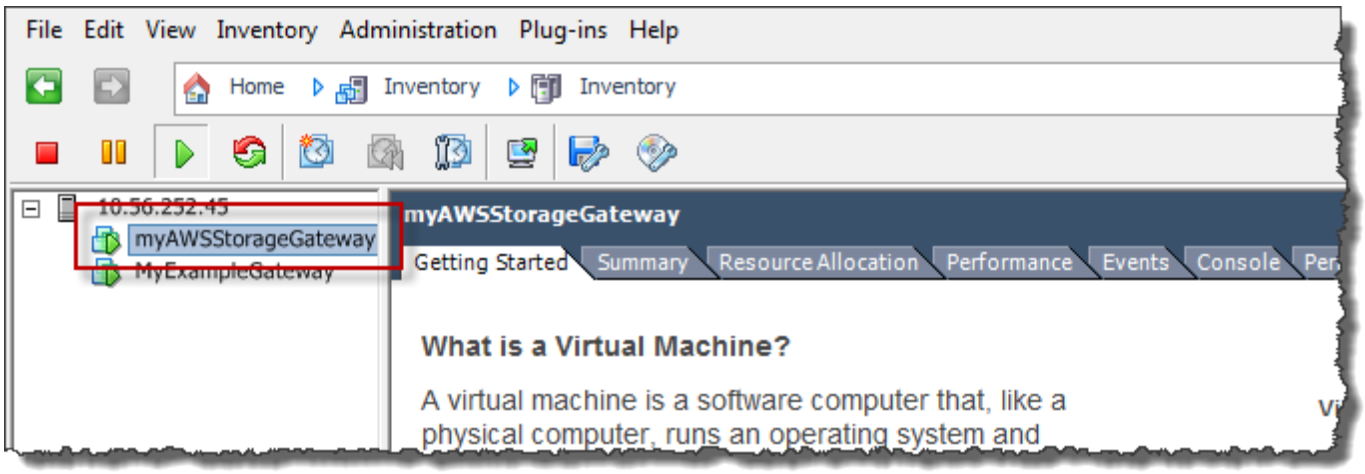


使用 VMware ESXi 访问网关本地控制台

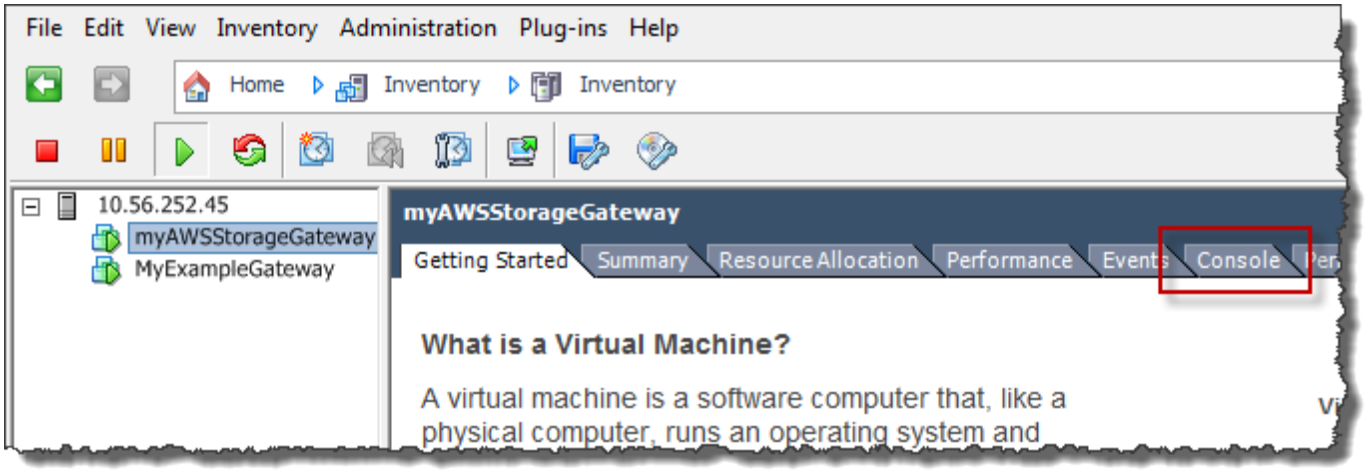
使用 VMware ESXi 访问网关的本地控制台

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

> **Note**
>
> 如果网关 VM 已开启，则有一个绿色箭头图标与 VM 图标一同显示，如以下屏幕截图所示。如果您的网关虚拟机未打开，则可以通过选择绿色来打开它开机上的图标工具栏菜单。

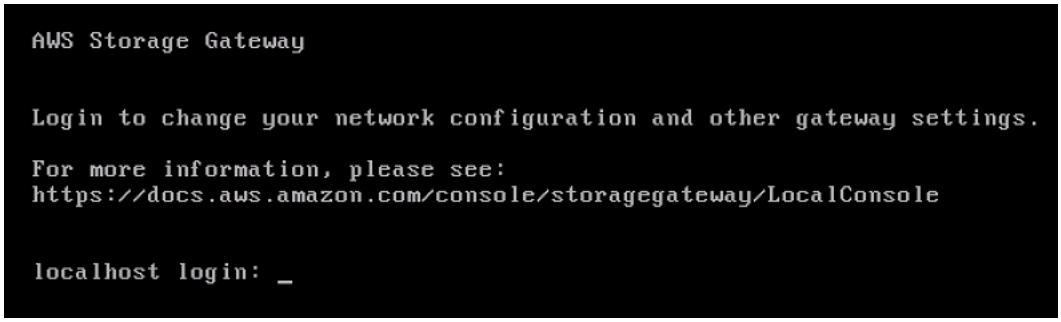


3. 选择 Console (控制台) 选项卡。



几分钟后，VM 就会准备就绪，供您登录了。

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



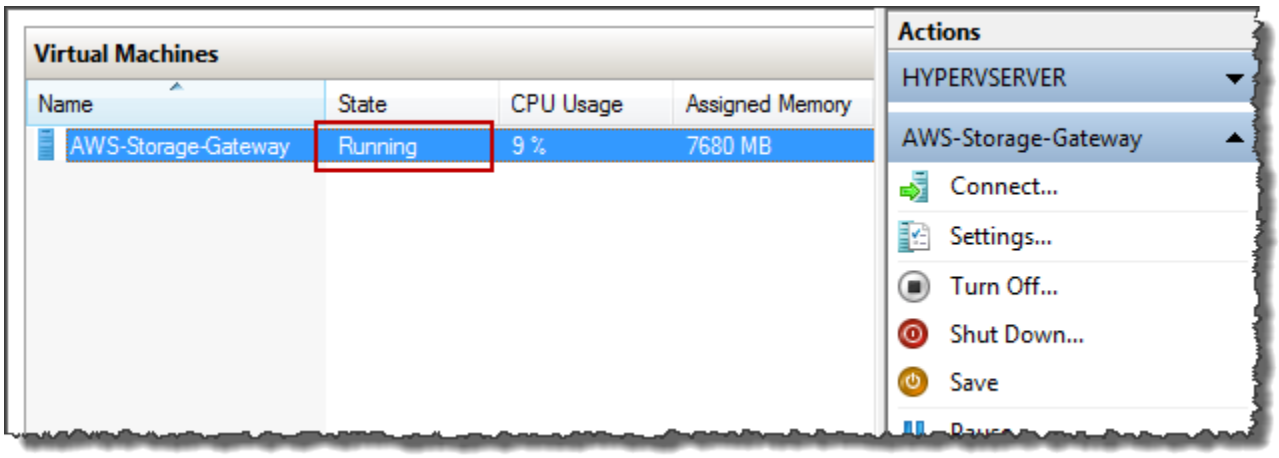
4. 要使用默认凭证登录，请继续执行过程登录文件网关本地控制台。

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)

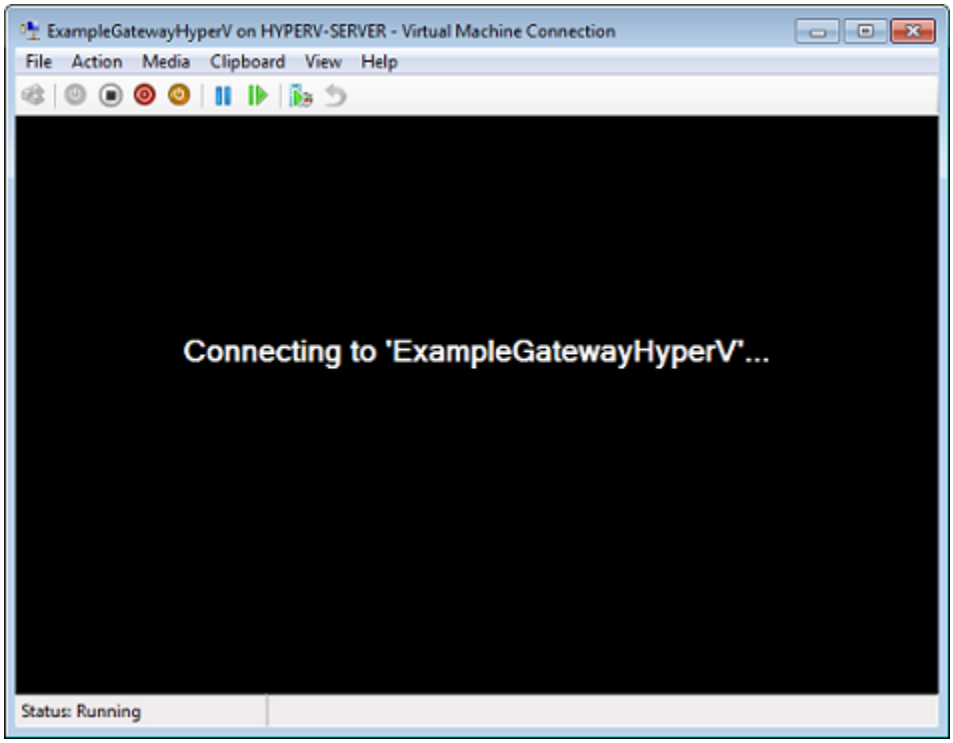
1. 在 Microsoft Hyper-V Manager 的 Virtual Machines (虚拟机) 列表中，选择您的网关 VM。
2. 确保网关已开启。

> **Note**
>
> 如果网关 VM 已开启，Running 会显示为 VM 的 State (状态)，如以下屏幕截图所示。如果您的网关虚拟机未打开，则可以通过选择以下方式将其打开启动中的操作窗格。



3. 在 Actions (操作) 窗格中，选择 Connect (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用户名称和密码。



几分钟后，VM 就会准备就绪，供您登录了。

4. 要使用默认凭证登录，请继续执行过程登录文件网关本地控制台。

为网关配置网络适配器

在本节中，您可以找到有关如何为您的网关配置多个网络适配器的信息。

主题

- 在 VMware ESXi 主机中为多个 NIC 配置您的网关

- 在 Microsoft Hyper-V 主机中为多个 NIC 配置您的网关

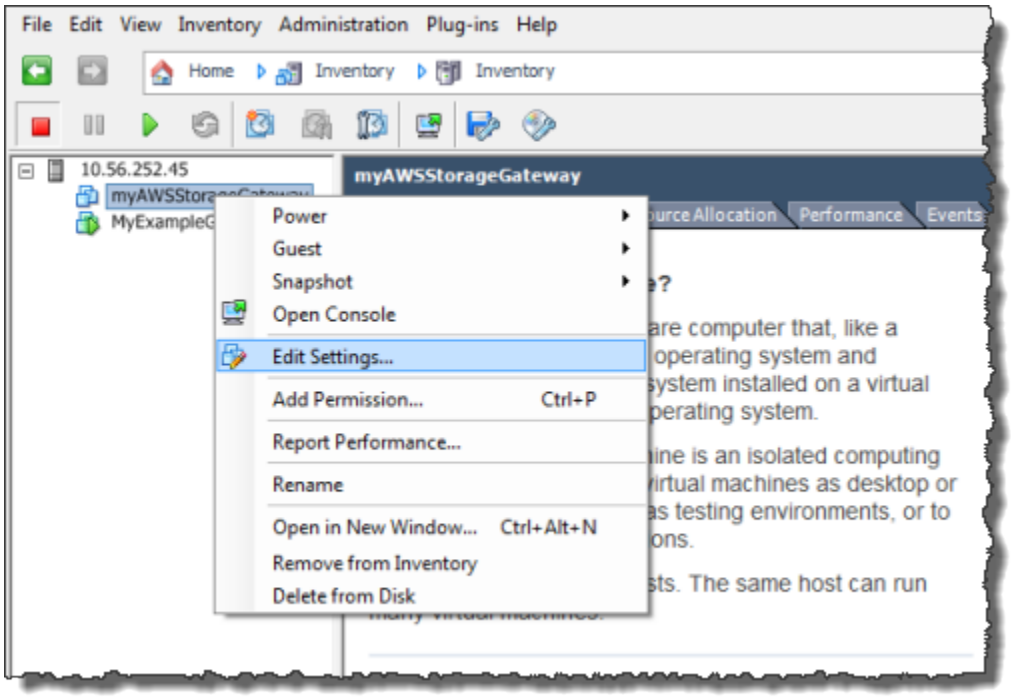
在 VMware ESXi 主机中为多个 NIC 配置您的网关

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。以下过程演示如何为 VMware ESXi 添加适配器。

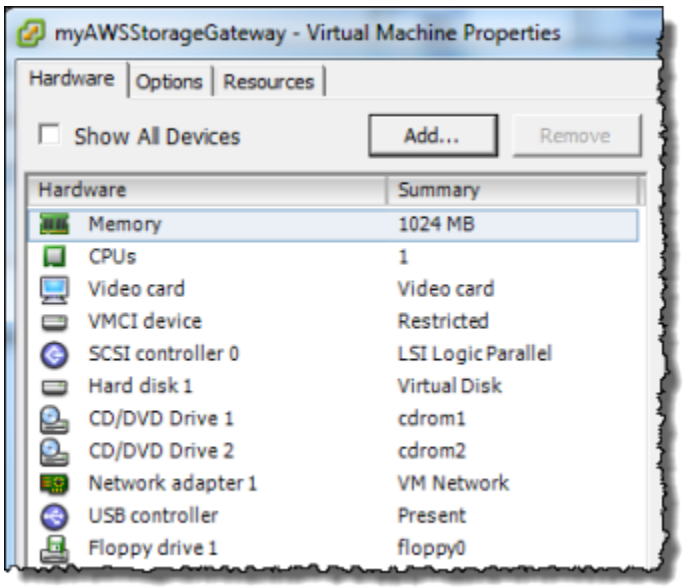
将网关配置为使用 VMware ESXi 主机中的另一个网络适配器

1. 关闭网关。
2. 在 VMware vSphere 客户端中，选择您的网关 VM。

   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)。

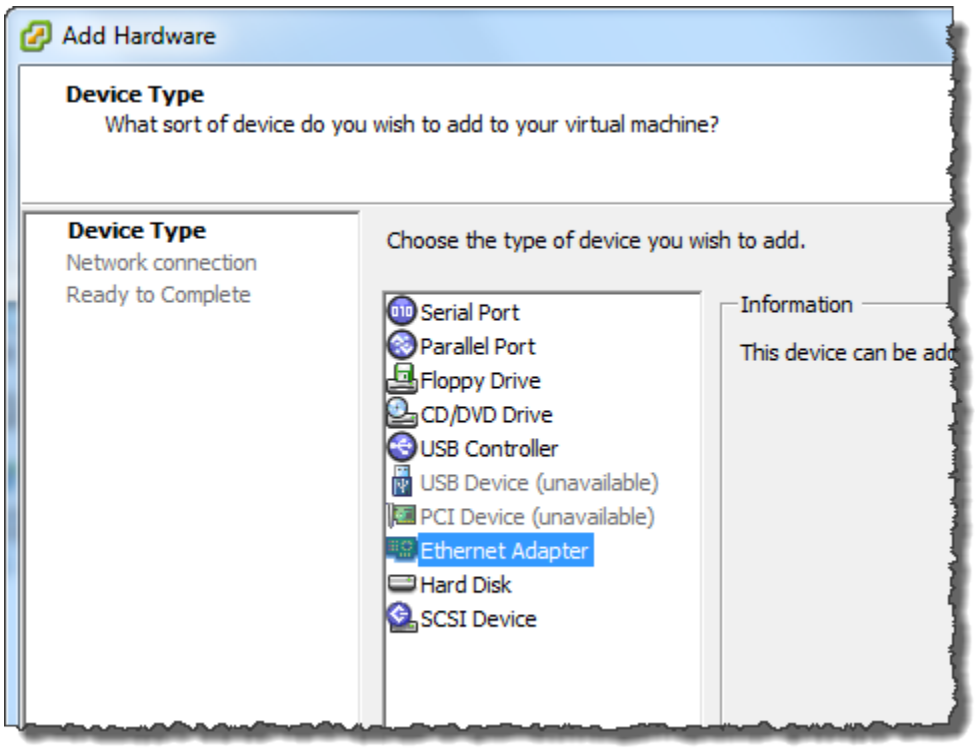


4. 在存储库的Hardware (硬件)选项卡虚拟机属性对话框中，选择Add添加设备。



5. 按 Add Hardware (添加硬件) 向导添加网络适配器。

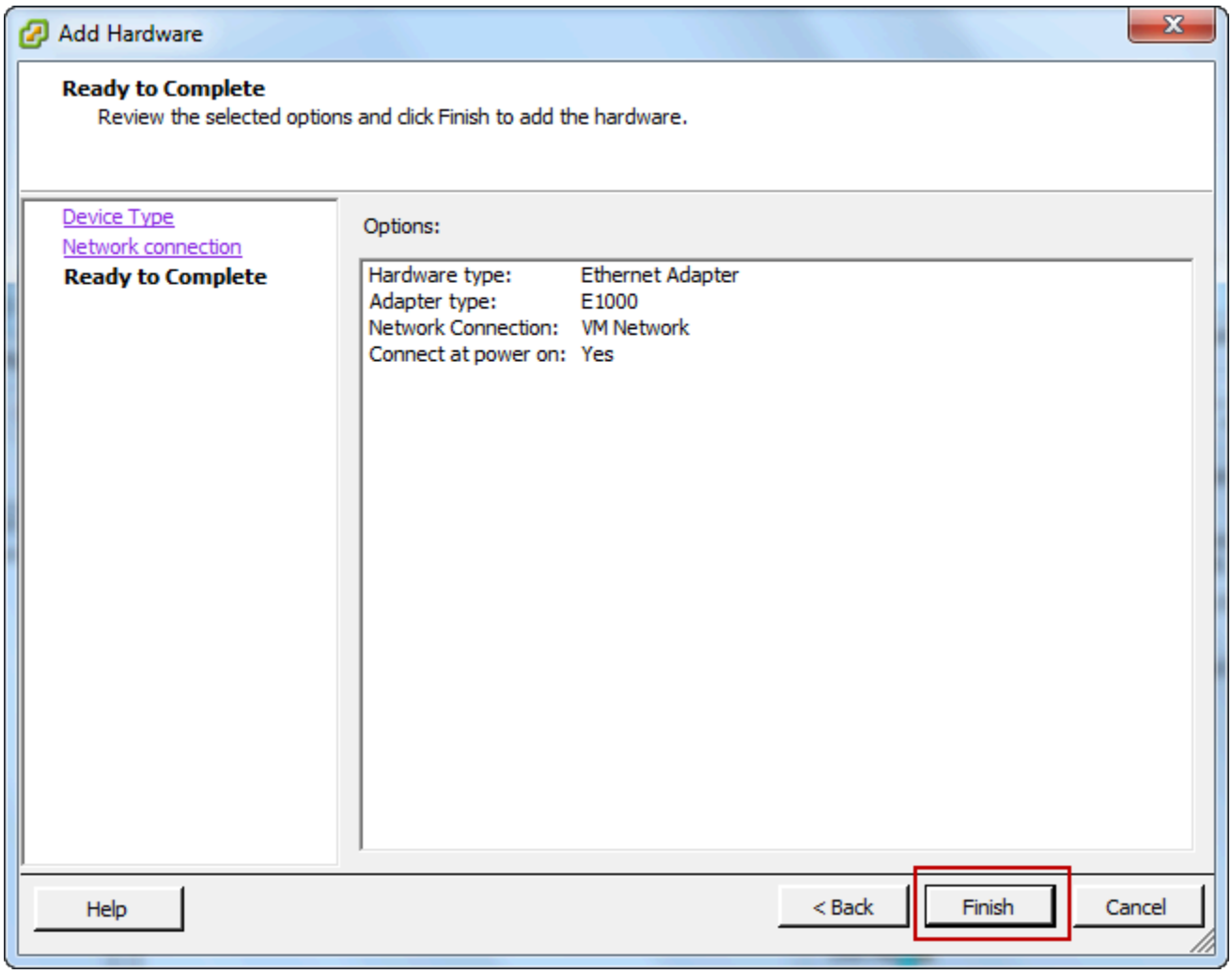
   a. 在 Device Type (设备类型) 窗格中，选择 Ethernet Adapter (以太网适配器) 以添加适配器，然后选择 Next (下一步)。



   b. 在网络类型窗格中，请确保开机时 Connect已选择类型，然后选择下一步.

我们建议您将 E1000 网络适配器与 Storage Gateway 一起使用。有关可能显示在适配器列表中的适配器类型的更多信息，请参阅 ESXi 和 vCenter 服务器文档中的“网络适配器类型”。

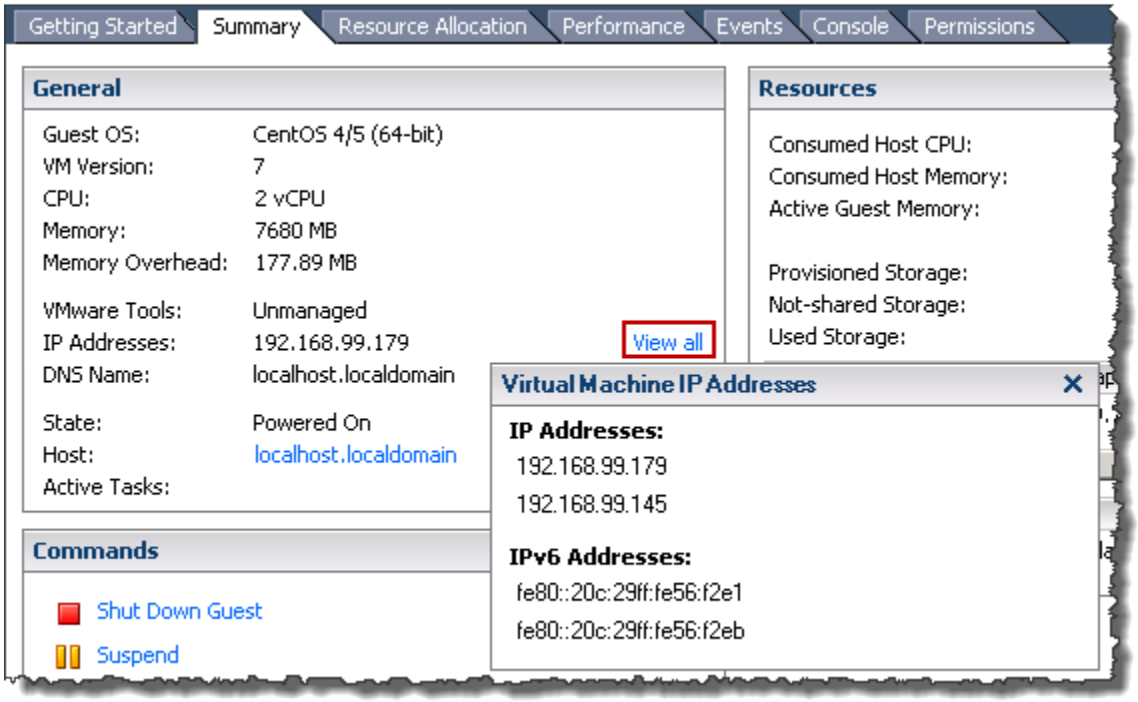
c. 在 Ready to Complete (已准备好完成) 窗格中，查看信息，然后选择 Finish (完成)。



6. 选择摘要虚拟机的选项卡，然后选择查看所有旁边IP 地址。Virtual Machine IP Addresses (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。

下图仅用于举例说明。在实际工作中，其中一个 IP 地址将是网关用来与 AWS 通信的地址，而另一个 IP 地址将是其他子网中的地址。



7. 在 Storage Gateway 控制台上，打开网关。
8. 在导航Storage Gateway 控制台的窗格中，选择网关然后选择要将适配器添加到的网关。确认 Details (详细信息) 选项卡中列出了第二个 IP 地址。

有关 VMware、Hyper-V 和 KVM 主机的常见本地控制台任务的信息，请参阅[在 VM 本地控制台（文件网关）上执行任务]

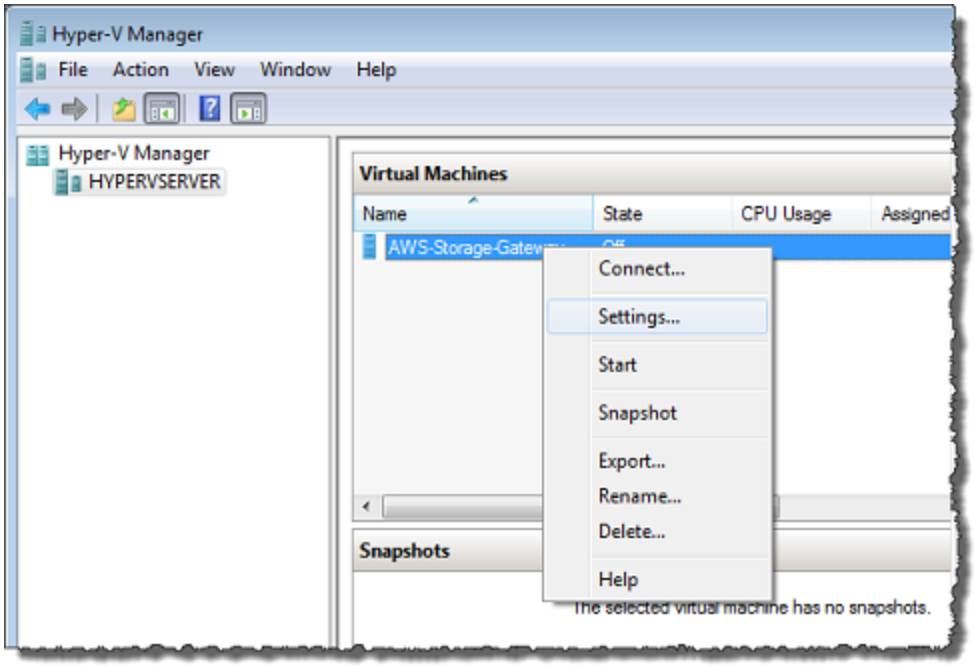
在 Microsoft Hyper-V 主机中为多个 NIC 配置您的网关

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

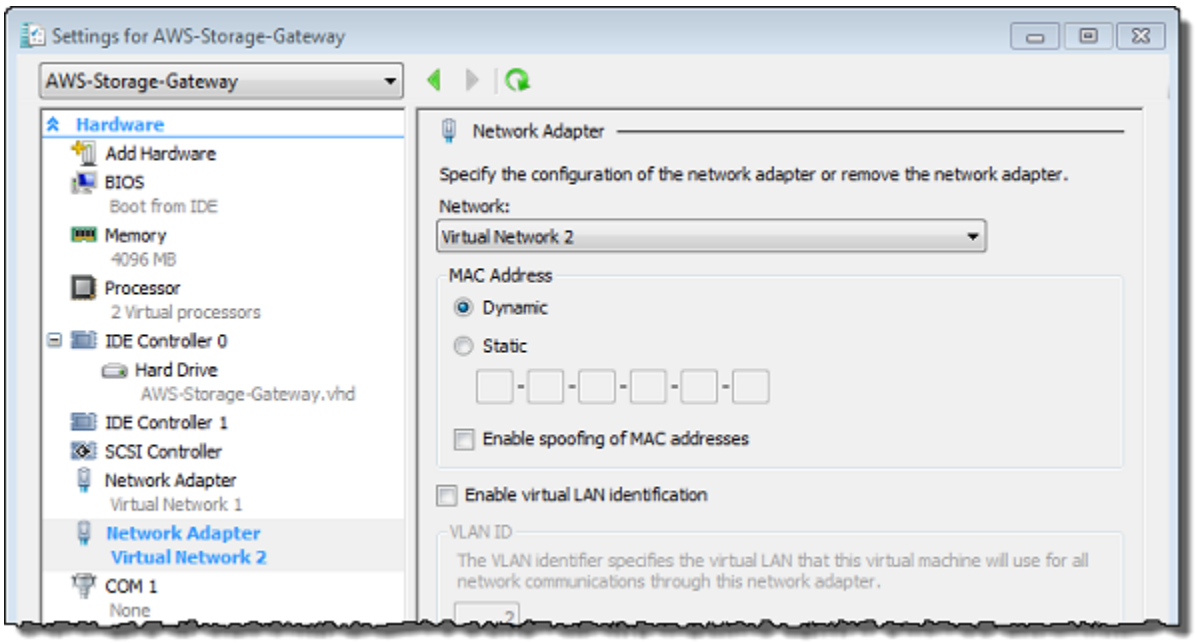
1. 在 Storage Gateway 控制台上，关闭网关。
2. 在 Microsoft Hyper-V Manager 中，选择您的网关 VM。
3. 如果 VM 已关闭，则打开网关的上下文（右键单击）菜单，然后选择 Turn Off (关闭)。

4. 在客户端中，打开网关 VM 的上下文菜单，然后选择 Settings (设置)。



5. 在 VM 的 Settings (设置) 对话框中，对于 Hardware (硬件)，选择 Add Hardware (添加硬件)。
6. 在 Add Hardware (添加硬件) 窗格中，选择 Network Adapter (网络适配器)，然后选择 Add (添加) 以添加设备。
7. 配置网络适配器，然后选择 Apply (应用) 以应用设置。

   在下例中，选择了 Virtual Network 2 (虚拟网络 2) 用于新适配器。



8. 在 Settings (设置) 对话框中，对于 Hardware (硬件)，确认已添加第二个适配器，然后选择 OK (确定)。
9. 在 Storage Gateway 控制台上，打开网关。
10. 在 Navigation (导航) 窗格中，选择 Gateways (网关)，然后选择要将适配器添加到的网关。确认 Details (详细信息) 选项卡中列出了第二个 IP 地址。

有关 VMware、Hyper-V 和 KVM 主机的常见本地控制台任务的信息，请参阅在 VM 本地控制台（文件网关）上执行任务

使用 AWS Storage Gateway 控制台删除网关并清除相关资源

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。

在删除后，网关不会再显示在 AWS Storage Gateway 管理控制台上，并且其与启动程序的 iSCSI 连接将关闭。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。

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 GatewayAPI 参考.

主题

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。

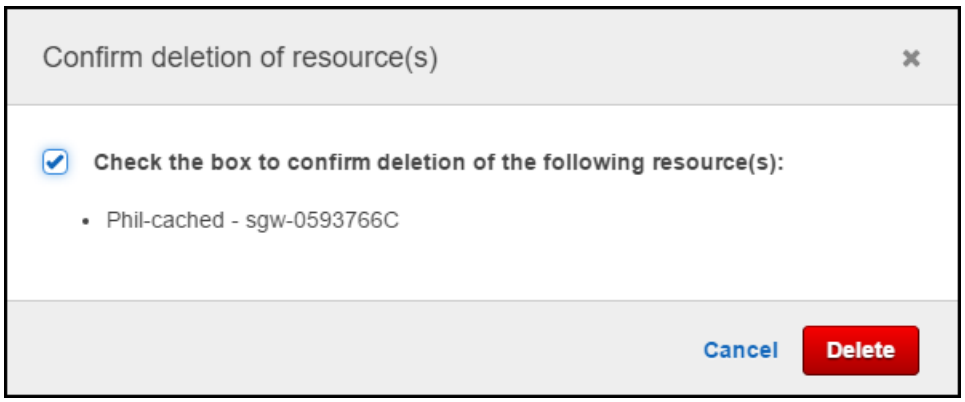
> **Note**
>
> 对于部署在 Amazon EC2 实例上的网关，实例将继续存在，直到您删除它。
> 对于部署在虚拟机 (VM) 上的网关，在您删除网关后，网关 VM 仍将存在于您的虚拟化环境中。要删除虚拟机，请使用 VMware vSphere 客户端、Microsoft Hyper-V Manager 或基于 Linux 内核的虚拟机 (KVM) 客户端连接到主机并删除虚拟机。请注意，您无法重复使用已删除的网关的 VM 来激活新网关。

如需删除网关

1. 在打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
2. 在导航窗格中，选择 Gateways，然后选择要删除的网关。
3. 对于 Actions (操作)，请选择 Delete gateway (删除网关)。
4.

> **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。
> 此外，网关删除后便无法恢复。

在显示的确认对话框中，选中复选框以确认删除。确保列出的网关 ID 指定了要删除的网关。然后选择 Delete (删除)。



Important

删除网关后，您就不用再为软件付费，但虚拟磁带、Amazon EBS Elastic Block Store (Amazon EBS) 快照和 Amazon EC2 实例等资源仍然存在。您将继续为这些资源付费。您可以选择通过取消 Amazon EC2 订阅来删除 Amazon EC2 实例和 Amazon EBS 快照。如果要保留 Amazon EC2 订阅，您可使用 Amazon EC2 控制台删除 Amazon EBS 快照。

从本地部署的网关中删除资源

您可按照下面的说明从本地部署的网关中移除资源。

从部署在 VM 上的卷网关中移除资源

如果要删除的网关部署在虚拟机 (VM) 上，我们建议您执行以下操作来清除资源：

- 删除网关。

从部署在 Amazon EC2 实例上的网关中删除资源

如果要删除部署在 Amazon EC2 实例上的网关，我们建议您清除AWS用于网关的资源，这样做可帮助避免产生非故意的使用费用。

从部署在 Amazon EC2 上的缓存卷中移除资源

如果您在 EC2 上部署了带有缓存卷的网关，我们建议您执行以下操作来删除网关并清除其资源：

1. 在 Storage Gateway 控制台中，按中所示删除网关。使用 Storage Gateway 控制台删除网关.

2. 在 Amazon EC2 控制台中，停止 EC2 实例（如果您打算再次使用该实例）。否则，终止该实例。如果您打算删除卷，请记下附加到该实例的块储存设备和设备的标识符，然后再终止该实例。您将需要这些标识符来标识要删除的卷。
3. 在 Amazon EC2 控制台中，删除附加到该实例的所有 Amazon EBS 卷（如果您不打算再次使用它们）。有关更多信息，请参阅 。清除您的实例和卷中的适用于 Linux 实例的 Amazon EC2 用户指南.

用新实例替换现有的文件网关

随着数据和性能需求的增长，或者如果您收到AWS通知迁移网关。如果要将网关移动到更好的主机平台或更新的 Amazon EC2 实例，或者刷新底层服务器硬件，则可能需要执行此操作。

有两种方法可以替换现有的文件网关。下表介绍了每种方法的优点和缺点。使用此信息，选择最适合您的网关环境的方法，然后参考以下相应部分中的过程步骤。

	方法 1：将缓存磁盘和网关 ID 迁移到替换实例	方法 2：使用空缓存磁盘和新的网关 ID 替换实例
缓存磁盘数据	缓存磁盘上的数据将被保留。如果您的网关有较大的缓存磁盘，或者您的应用程序对缓存不足读取操作造成的延迟敏感，则此方法非常有用。	缓存中的数据从AWS云。如果您的应用程序能够容忍由于缓存不足读取而造成的延迟，此方法对于写入大量工作负载来说
停机时间	在迁移过程中，您的网关将脱机 1-2 小时。	没有停机时间。现有网关可以与替换网关同时使用，直到您选择删除它。两个网关都在使用时，不支持多个写入器。
网关 ID	新网关从它替换的网关继承网关 ID。	现有网关和替换网关具有单独的唯一网关 ID。

> **Note**
>
> 数据只能在相同类型的网关之间移动。

方法 1：将缓存磁盘和网关 ID 迁移到替换实例

要将文件网关的缓存磁盘和网关 ID 迁移到替换实例，请执行以下操作：

1. 停止正在写入到现有文件网关的任何应用程序。
2. 确认`CachePercentDirty`上的指标监控现有文件网关的选项卡是`0`.

3. 通过使用虚拟机管理程序控件关闭主机虚拟机 (VM) 的电源，关闭现有文件网关。

   有关关闭 Amazon EC2 实例的更多信息，请参阅停止和启动您的实例中的Amazon EC2 用户指南.

   有关关闭 KVM、VMware 或 Hyper-V VM 的更多信息，请参阅虚拟机管理程序文档。

4. 从旧网关虚拟机中分离所有磁盘，包括根磁盘、缓存磁盘和上传缓冲区磁盘。

   > **Note**
   >
   > 记下根磁盘的卷 ID 以及与该根磁盘关联的网关 ID。在后面的步骤中，您需要将此磁盘从新的存储网关虚拟机管理程序中分离出来。

   如果您使用 Amazon EC2 实例作为文件网关的虚拟机，请参阅将 Amazon EBS 卷与 Windows 实例分离要么将 Amazon EBS 卷与 Linux 实例分离中的Amazon EC2 用户指南.

   有关从 KVM、VMware 或 Hyper-V VM 分离磁盘的信息，请参阅管理程序的文档。

5. 创建新的AWSStorage Gateway 虚拟机管理程序虚拟机实例，但不要将其作为网关激活。在后面的步骤中，这个新虚拟机将假设旧网关的标识。

   有关创建新 Storage Gateway 管理程序 VM 的更多信息，请参阅选择主机平台和下载 VM.

   > **Note**
   >
   > 不要为新虚拟机添加缓存磁盘。此虚拟机将使用与旧虚拟机使用的相同缓存磁盘。

6. 将新的 Storage Gateway 虚拟机配置为使用与旧虚拟机相同的网络设置。

   网关的默认网络配置是动态主机配置协议 (DHCP)。使用 DHCP，您的网关将被自动分配 IP 地址。

   如果您需要为网关 VM 手动配置静态 IP 地址，请参阅配置网关网络.

   如果您的网关 VM 必须使用 Socket Secure 版本 5 (SOCKS5) 代理连接到互联网，请参阅通过代理路由本地网关.

7. 启动新的 Storage Gateway 虚拟机。

8. 将从旧网关虚拟机分离的磁盘连接到新的网关 VM。不要从新的网关虚拟机中分离现有的根磁盘。

> **Note**
>
> 要成功迁移，所有磁盘都必须保持不变。更改磁盘大小或其他值会导致元数据不一致，从而阻碍成功迁移。

9. 通过使用以下格式的 URL 连接到新 VM 来启动网关迁移过程：

   http://*your-VM-IP-address*/migrate?gatewayId=*your-gateway-ID*

   对于新网关虚拟机，您可以使用与用于旧网关虚拟机的相同 IP 地址。您的 URL 应类似于以下示例：

   http://*198.51.100.123*/migrate?gatewayId=*sgw-12345678*

   从浏览器或使用 cURL 从命令行中使用此 URL。

   当网关迁移成功启动时，将显示以下消息：

   ```
   Successfully imported Storage Gateway information. Please refer to Storage Gateway
    documentation to perform the next steps to complete the migration.
   ```

10. 等待网关状态显示为正在运行中的AWSStorage Gateway 控制台。此过程最多可能需要 10 分钟，具体取决于可用带宽。
11. 停止新的 Storage Gateway 虚拟机。
12. 从新网关中分离旧网关的根磁盘（您之前记录的卷 ID）。
13. 启动新的 Storage Gateway 虚拟机。
14. 如果您的网关加入 Active Directory 域，请重新加入该域。有关说明，请参阅配置 Microsoft Active Directory 访问权限.

    > **Note**
    >
    > 即使文件网关的状态显示为已加入.

15. 确认您的共享在新网关虚拟机的 IP 地址上可用，然后删除旧的网关虚拟机。

    > **Warning**
    >
    > 网关删除后便无法恢复。

有关删除 Amazon EC2 实例的更多信息，请参阅终止实例中的Amazon EC2 用户指南. 有关删除 KVM、VMware 或 Hyper-V VM 的更多信息，请参阅管理程序的文档。

方法 2：使用空缓存磁盘和新的网关 ID 替换实例

要使用空缓存磁盘和新的网关 ID 设置替换文件网关实例，请执行以下操作：

1. 停止正在写入到现有文件网关的任何应用程序。确认CachePercentDirty上的指标监控“选项卡”0在新网关上设置文件共享之前。
2. 使用AWS Command Line Interface(AWS CLI) 通过执行以下操作来收集并保存有关现有文件网关和文件共享的配置信息：

   a. 保存文件网关的网关配置信息。

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

   此命令输出包含有关网关的元数据，如名称、网络接口、已配置的时区和状态（网关运行）。

   b. 保存文件网关的服务器消息块 (SMB) 设置。

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

   此命令输出一个 JSON 块，其中包含有关 SMB 文件共享的元数据，例如其域名、Microsoft Active Directory 状态、是否设置了来宾密码以及安全策略的类型。

   c. 为文件网关的每个 SMB 和网络文件系统 (NFS) 文件共享保存文件共享信息：

   - 对 SMB 文件共享使用以下命令。

     ```
     aws storagegateway describe-smb-file-shares --file-share-arn-list
      "arn:aws:storagegateway:us-east-2:123456789012:share/share-987A654B"
     ```

     此命令输出一个 JSON 块，其中包含有关 NFS 文件共享的元数据，例如其名称、存储类、状态、IAM 角色 Amazon Resource Name (ARN)、允许访问文件网关的客户端列表以及 SMB 客户端用于标识挂载点的路径。

- 对于 NFS 文件共享，请使用以下命令。

```
aws storagegateway  describe-nfs-file-shares --file-share-arn-list
 "arn:aws:storagegateway:us-east-2:123456789012:share/share-321A978B"
```

此命令输出一个 JSON 块，其中包含有关 NFS 文件共享的元数据，例如其名称、存储类、状态、IAM 角色 ARN、允许访问文件网关的客户端列表以及 NFS 客户端用于标识挂载点的路径。

3. 通过执行以下操作停止现有的文件网关：

   a. 停止正在写入到现有文件网关的任何应用程序。确认CachePercentDirty上的指标监控“选项卡”0在新网关上设置文件共享之前。

   b. 通过关闭托管网关的虚拟机 (VM) 的电源来停止现有的文件网关。

4. 创建新的文件网关。
5. 挂载在旧网关上配置的文件共享。
6. 确认新网关正常工作，然后从 Storage Gateway 控制台中删除旧网关。

> **Important**
>
> 删除网关之前，请确保当前没有应用程序正在写入到该文件网关的缓存。如果您在使用期间删除文件网关，则可能会发生数据丢失。

> **Warning**
>
> 网关删除后便无法恢复。

7. 删除旧的网关虚拟机或 EC2 实例。

性能

在本节中，您可以找到有关 Storage Gateway 性能的信息。

主题

- 文件网关的性能指南
- 优化网关性能
- 将 VMware vSphere 高可用性与 Storage Gateway 结合使用

文件网关的性能指南

在本部分中，您可以找到为文件网关 VM 预配置硬件的配置指南。表中列出的 Amazon EC2 实例大小和类型是示例，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。

在下表中，缓存命中率读取操作是从缓存提供的文件共享中读取。缓存错过读取操作是从 Amazon S3 提供的文件共享中读取。

> **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。

以下是文件网关配置示例。

Linux 客户端上的 S3 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	缓存错过读取吞吐量
根磁盘：80、GB io1、4,000 IOPS	NFSv3-1 个线程	110 MiB/ 秒（0.92 Gbps）	590 MiB/s (4.9 Gbps)	310 MiB/秒（2.6 Gbps）

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	缓存错过读取吞吐量
缓存磁盘：512 GiB 缓存，io1，1,500 预配置 IOPS 最低网络性能：10Gbps CPU：16 个 vCPU | RAM：32 GB 推荐用于 Linux 的 NFS 协议	NFSv3-8 个线程	160 MiB/s (1.3 Gbps)	590 MiB/s (4.9 Gbps)	335 MiB/s (2.8 Gbps)
	NFSv4-1 个线程	130 MiB/秒（1.1 Gbps）	590 MiB/s (4.9 Gbps)	295 MiB/s (2.5 Gbps)
	NFSv4-8 个线程	160 MiB/s (1.3 Gbps)	590 MiB/s (4.9 Gbps)	335 MiB/s (2.8 Gbps)
	SMBV3-1 个线程	115 MiB/s (1.0 Gbps)	325 兆比/秒（2.7 Gbps）	255 MiB/秒（2.1 Gbps）
	SMBV3-8 个线程	190 兆比/秒（1.6 Gbps）	590 MiB/s (4.9 Gbps)	335 MiB/s (2.8 Gbps)
存储网关硬件设备 最低网络性能：10Gbps	NFSv3-1 个线程	265 MiB/s (2.2 Gbps)	590 MiB/s (4.9 Gbps)	310 MiB/秒（2.6 Gbps）
	NFSv3-8 个线程	385 Mib/秒（3.1 Gbps）	590 MiB/s (4.9 Gbps)	335 MiB/s (2.8 Gbps)
	NFSv4-1 个线程	310 MiB/秒（2.6 Gbps）	590 MiB/s (4.9 Gbps)	295 MiB/s (2.5 Gbps)
	NFSv4-8 个线程	385 Mib/秒（3.1 Gbps）	590 MiB/s (4.9 Gbps)	335 MiB/s (2.8 Gbps)
	SMBV3-1 个线程	275 兆比/秒（2.4 Gbps）	325 兆比/秒（2.7 Gbps）	255 MiB/秒（2.1 Gbps）
	SMBV3-8 个线程	455 MiB/s (3.8 Gbps)	590 MiB/s (4.9 Gbps)	335 MiB/s (2.8 Gbps)

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	缓存错过读取吞吐量
根磁盘：80 GB，io1 SSD，4,000 IOPS 缓存磁盘：4 x 2 TB NVME 缓存磁盘 最低网络性能：10Gbps CPU：32 个 vCPU | RAM：244 GB 推荐用于 Linux 的 NFS 协议	NFSv3-1 个线程	300 MiB/s (2.5 Gbps)	590 MiB/s (4.9 Gbps)	325 兆比/秒（2.7 Gbps）
	NFSv3-8 个线程	585 MiB/s (4.9 Gbps)	590 MiB/s (4.9 Gbps)	580 MiB/s (4.8 Gbps)
	NFSv4-1 个线程	350 MiB/s (3.0 Gbps)	590 MiB/s (4.9 Gbps)	340 MiB/s (2.9 Gbps)
	NFSv4-8 个线程	575 MiB/s (4.8 Gbps)	590 MiB/s (4.9 Gbps)	575 MiB/s (4.8 Gbps)
	SMBV3-1 个线程	230 MiB/s (1.9 Gbps)	325 兆比/秒（2.7 Gbps）	245 MiB/s (2.0 Gbps)
	SMBV3-8 个线程	585 MiB/s (4.9 Gbps)	590 MiB/s (4.9 Gbps)	580 MiB/s (4.8 Gbps)

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	缓存错过读取吞吐量
根磁盘：80 GB io1，4,000 IOPS	SMBV3-1 个线程	150 MiB/s (1.3 Gbps)	180 MiB/s (1.5 Gbps)	20 MiB/s (0.2 Gbps)
缓存磁盘：512 GiB 缓存，io1，1,500 预配置 IOPS 最低网络性能：10 Gbps	SMBV3-8 个线程	190 兆比/秒（1.6 Gbps）	350 MiB/s (2.8 Gbps)	195 兆比/秒（1.6 Gbps）
	NFSv3-1 个线程	95 MiB/s (0.8 Gbps)	130 MiB/秒（1.1 Gbps）	20 MiB/s (0.2 Gbps)
	NFSv3-8 个线程	190 兆比/秒（1.6 Gbps）	330 MiB/s (2.8 Gbps)	190 兆比/秒（1.6 Gbps）

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	缓存错过读取吞吐量
CPU：16 个 vCPU | RAM：32 GB 建议用于 Windows 的中小型企业协议				
存储网关硬件设备 最低网络性能：10 Gbps	SMBV3-1 个线程	230 MiB/s (1.9 Gbps)	255 MiB/秒（2.1 Gbps）	20 MiB/s (0.2 Gbps)
	SMBV3-8 个线程	835 MiB/s (7.0 Gbps)	475 MiB/s (4.0 Gbps)	195 兆比/秒（1.6 Gbps）
	NFSv3-1 个线程	135 Mib/秒（1.1 Gbps）	185 MiB/秒（1.6 Gbps）	20 MiB/s (0.2 Gbps)
	NFSv3-8 个线程	545 MiB/ 秒（4.6 Gbps）	470 MiB/s (4.0 Gbps)	190 兆比/秒（1.6 Gbps）

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	缓存错过读取吞吐量
根磁盘：80 GB，io1 SSD，4,000 IOPS 缓存磁盘：4 x 2 TB NVME 缓存磁盘 最低网络性能：10 Gbps CPU：32 个 vCPU | RAM：244 GB 建议用于 Windows 的中小型企业协议	SMBV3-1 个线程	230 MiB/s (1.9 Gbps)	265 MiB/s (2.2 Gbps)	30 MiB/s (0.3 Gbps)
	SMBV3-8 个线程	835 MiB/s (7.0 Gbps)	780 MiB/s (6.5 Gbps)	250 MiB/秒（2.1 Gbps）
	NFSv3-1 个线程	135 Mib/秒 (1.1. Gbps)	220 MiB/s (1.8 Gbps)	30 MiB/s (0.3 Gbps)
	NFSv3-8 个线程	545 MiB/ 秒（4.6 Gbps）	570 MiB/s (4.8 Gbps)	240 MiB/s (2.0 Gbps)

> **Note**
>
> 您的性能可能因主机平台配置和网络带宽而异。

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，如固态硬盘 (SSD) 和 NVMe 控制器。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。更高的磁盘性能通常可带来更大的吞吐量和更多的每秒输入/输出操作 (IOPS) 次数。有关添加磁盘的信息，请参阅添加缓存存储.

要测量吞吐量，请使用`ReadBytes`和`WriteBytes`指标`Samples`Amazon CloudWatch 统计数据。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**
>
> 并非所有网关都可以使用 CloudWatch 指标。有关网关指标的信息，请参阅监控文件网关。

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，还要确认您没有超额预订主机服务器的 CPU。

在将额外的 CPU 添加到网关主机服务器时，将会增加网关的处理能力。通过执行该操作，您的网关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此数据上传到 Amazon S3 的过程。更多 CPU 还可帮助确保在主机与其他 VM 共享时您的网关获得足够的 CPU 资源。提供足够的 CPU 资源通常能取得增加吞吐量的效果。

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

- 24 个 CPU。
- 文件网关预留 RAM 的 16 GiB 预留 RAM
  - 16 GiB 的预留 RAM，用于缓存大小不超过 16 TiB 的网关
  - 32 GiB 的预留 RAM，用于缓存大小为 16 TiB 到 32 TiB 的网关
  - 48 GiB 的预留 RAM，用于缓存大小为 32 TiB 至 64 TiB 的网关
- 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 SSD。
- 磁盘 1 附加到半虚拟化控制器 2，将按如下方式用作网关上传缓冲区：

    - 使用 NVMe 控制器的 SSD。
- 磁盘 3 附加到半虚拟化控制器 2，将按如下方式用作网关上传缓冲区：
    - 使用 NVMe 控制器的 SSD。
- 在虚拟机网络 1 上配置网络适配器 1：
    - 使用 VM 网络 1 并添加 VMXnet3 (10 Gbps) 以用于提取。
- 在虚拟机网络 2 上配置网络适配器 2：
    - 使用 VM 网络 2 并添加 VMXnet3 (10 Gbps) 以用于连接到 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`ReadBytes`和`WriteBytes`用于衡量总数据吞吐量的网关指标。

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，则添加更多 CPU 可以帮助您的应用程序扩展其 I/O 负载。

将 VMware vSphere 高可用性与 Storage Gateway 结合使用

Storage Gateway 通过一组与 VMware vSphere High Availability (VMware HA) 集成的应用程序级运行状况检查，在 VMware 上提供高可用性。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。

通过此集成，部署在本地 VMware 环境中或 VMware Cloud on AWS 中的网关将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。

要将 VMware HA 与 Storage Gateway 结合使用，请执行下面列出的步骤。

主题

配置您的 vSphere VMware HA 集群

如果您尚未创建 VMware 集群，请先创建一个。有关如何创建 VMware 集群的信息，请参阅 VMware 文档中的创建 vSphere HA 集群。

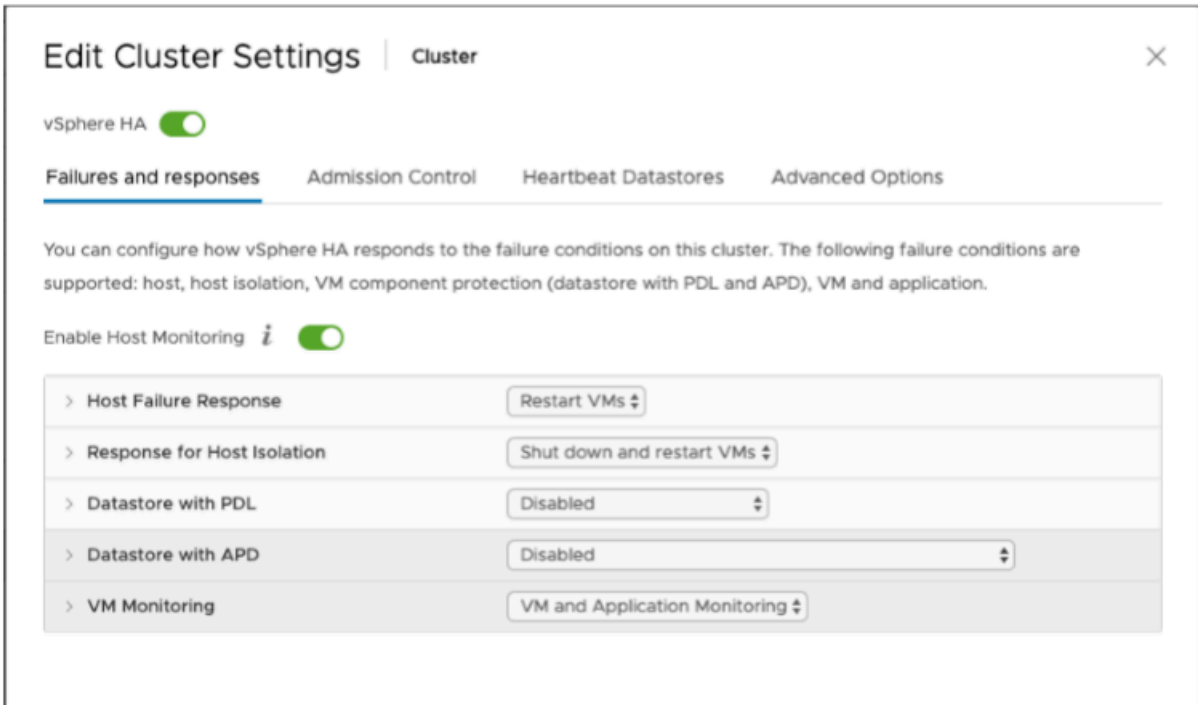
接下来，将 VMware 集群配置为与 Storage Gateway 结合使用。

配置 VMware 集群

1. 在 VMware vSphere 的 Edit Cluster Settings (编辑集群设置) 页面上，确保为 VM 和应用程序监控配置 VM 监控。为此，请设置下面列出的选项：

   - 主机故障响应：重新启动 VM
   - 对主机隔离的响应：关闭并重新启动 VM
   - PDL 的数据存储：Disabled (已禁用)
   - 具有 APD 的数据存储：Disabled (已禁用)
   - VM 监控：VM 和应用程序监控

有关示例，请参阅下面的屏幕截图。



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。
   - 最小的正常— 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。
   - 最长重置时段— 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

如果您在集群上运行了其他 VM，则可能需要专门为您的 VM 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）为集群上的其他 VM 添加覆盖选项。

下载适用于您的网关类型的 .ova 映像

使用以下过程可下载 .ova 映像。

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 —

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。

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。

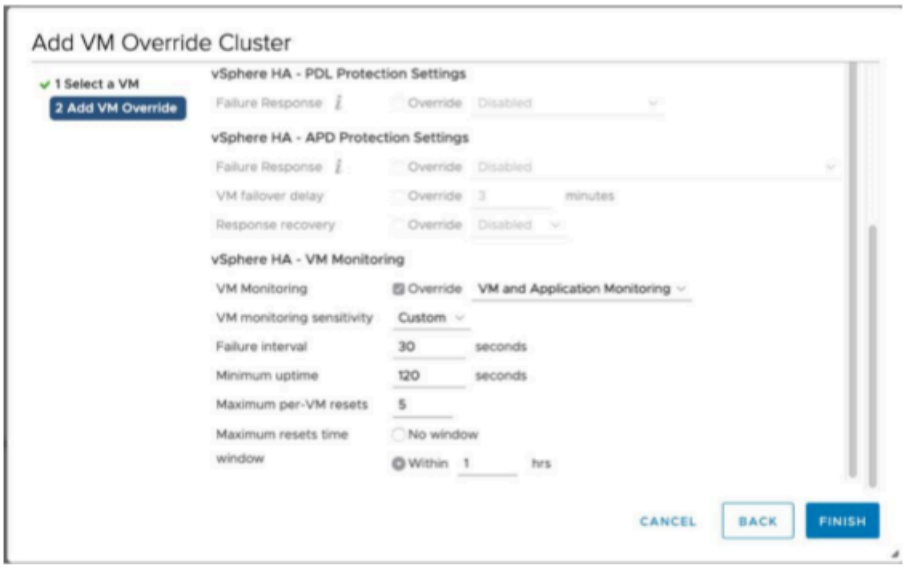
（可选）为集群上的其他 VM 添加覆盖选项

如果您在集群上运行了其他 VM，则可能需要专门为每个 VM 设置集群值。

为集群上的其他 VM 添加覆盖选项

1. 在 VMware vSphere 中的 Summary (摘要) 页面上，选择您的集群以打开集群页面，然后选择 Configure (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 覆盖选项以更改每个值。

   有关覆盖选项，请参阅下面的屏幕截图。



激活网关

在部署适用于网关的 .ova 后，激活网关。有关每个网关类型的不同之处的说明。

激活网关

- 根据您的网关类型选择激活说明：
  - 文件网关 —

测试您的 VMware High Availability 配置

激活网关后，请测试您的配置。

测试 VMware HA 配置

1. 在打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
2. 在导航窗格上，选择 Gateways (网关)，然后选择要针对 VMware HA 测试的网关。
3. 对于 Actions (操作)，请选择 Verify VMware HA (验证 VMware HA)。
4. 在显示的 Verify VMware High Availability Configuration (验证 VMware High Availability 配置) 框中，选择 OK (确定)。

> **Note**
>
> 测试 VMware HA 配置将重新启动网关 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. 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 CloudWatch 日志组获取文件网关健康日志。

中的安全性AWSStorage Gateway

AWS 的云安全性的优先级最高。作为 AWS 客户，您将从专为满足大多数安全敏感型企业的要求而打造的数据中心和网络架构中受益。

安全性是AWS和您的共同责任。责任共担模式将其描述为云的云的安全性和云中的安全性：

- 云的安全性 – AWS 负责保护在 AWS 云中运行 AWS 服务的基础设施。AWS 还向您提供可安全使用的服务。作为AWS合规性计划的一部分，第三方审计人员将定期测试和验证安全性的有效性。要了解适用于的合规性计划AWS请参阅 Storage GatewayAWS合规性计划范围内的服务.
- 云中的安全性 - 您的责任由您使用的 AWS 服务决定。您还需要对其它因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 Storage Gateway 时应用责任共担模式。以下主题说明如何配置 Storage Gateway 以实现您的安全性和合规性目标。你还将学习如何使用其他AWS有助于您监控和保护您的 Storage Gateway 资源的服务。

主题

- 中的数据保护AWSStorage Gateway
- Storage Gateway 的身份验证和访问控制
- AWS Storage Gateway 中的日志记录和监控
- 的合规性验证AWSStorage Gateway
- 中的故障恢复能力AWSStorage Gateway
- 中的基础设施安全性AWSStorage Gateway
- Storage Gateway 的安全最佳实践

中的数据保护AWSStorage Gateway

这些区域有：AWS 责任共担模式适用于中的数据保护AWSStorage Gateway。如该模式中所述，AWS 负责保护运行所有 AWS Cloud 的全球基础设施。您负责维护对托管在此基础设施上的内容的控制。此内容包括您所使用的 AWS 服务的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅AWS安全性博客上的AWS责任共担模式和 GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS Identity and Access Management (IAM) 设置单独的用户账户。这仅向每个用户授予履行其工作职责所需的权限。我们还建议您通过以下方式保护您的数据：

- 对每个账户使用 Multi-Factor Authentication (MFA)。
- 使用 SSL/TLS 与AWS资源进行通信。建议使用 TLS 1.2 或更高版本。
- 使用 AWS CloudTrail 设置 API 和用户活动日志记录。
- 使用AWS加密解决方案以及AWS服务中的所有默认安全控制。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的个人数据。
- 如果在通过命令行界面或 API 访问 AWS 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-2 版》。

我们强烈建议您切勿将机密信息或敏感信息（例如您客户的电子邮件地址）放入标签或自由格式字段（例如名称字段）。这包括使用 Storage Gateway 或其他时间。AWS使用控制台、API、AWS CLI，或者AWS开发工具包。您在用于名称的标签或自由格式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，我们强烈建议您不要在 URL 中包含凭证信息来验证您对该服务器的请求。

使用数据加密AWS KMS

Storage Gateway 使用 SSL/TLS（安全套接字层/传输层安全性）来加密在您的网关设备之间传输的数据，AWS存储。默认情况下，Storage Gateway 使用 Amazon S3 托管的加密密钥 (SSE-S3) 对其存储在 Amazon S3 中的所有数据进行服务器端加密。您可以选择使用 Storage Gateway API 将您的网关配置为使用服务器端加密以加密存储在云中的数据的选项。AWS Key Management Service(SSE-KMS) 客户主密钥 (CMK)。

> **Important**
>
> 当您使用AWS KMSCMK 用于服务器端加密，您必须选择对称 CMK。Storage Gateway 不支持非对称 CMK。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。

加密文件共享

对于文件共享，您可以将网关配置为加密对象AWS KMS— 使用 SSE-KMS 托管密钥。有关使用 Storage Gateway API 来加密写入文件共享的数据的信息，请参阅。CreateNFSFileShare中的AWS Storage GatewayAPI 参考.

加密文件系统

有关信息，请参阅亚马逊 FSx 中的数据加密中的Amazon FSx for Windows File Server 用户指南.

在使用 AWS KMS 加密您的数据时，请注意以下几点：

- 您的数据在云中静态加密。也就是说，在 Amazon S3 中对数据进行加密。
- IAM 用户必须有必需的权限才能调用AWS KMSAPI 操作。有关更多信息，请参阅 。将 IAM 策略与 AWS KMS中的AWS Key Management Service开发人员指南.
- 如果您删除或禁用 CMK 或撤销授权令牌，则将无法访问卷或磁带上的数据。有关更多信息，请参阅 。删除客户主密钥中的AWS Key Management Service开发人员指南.
- 如果从采用 KMS 加密的卷中创建快照，则将加密快照。快照将继承卷的 KMS 密钥。
- 如果从采用 KMS 加密的快照中创建新卷，则将加密卷。可以为新卷指定不同的 KMS 密钥。

> **Note**
>
> Storage Gateway 不支持从 KMS 加密卷或 KMS 加密快照的恢复点创建未加密卷。

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

Storage Gateway 的身份验证和访问控制

访问 AWS Storage Gateway 时需要可供 AWS 用来验证您的请求的凭证。这些凭证必须有权访问。AWS资源，例如网关、文件共享、卷或磁带。下面几节提供详细的信息来说明如何使用。AWS Identity and Access Management(IAM)和 Storage Gateway 通过控制可以访问您的资源的用户，从而帮助对这

- 身份验证
- 访问控制

身份验证

您可以以下面任一类型的身份访问 AWS：

- AWS 账户 根用户 – 当您首次创建 AWS 账户 账户时，最初使用的是一个对账户中所有 AWS 服务和资源有完全访问权限的单点登录身份。此身份称为AWS 账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。强烈建议您不使用根用户执行日常任务，即使是管理任务。相反，请遵循仅使用根用户创建您的第一个 IAM 用户的最佳实践。然后请妥善保存根用户凭证，仅用它们执行少数账户和服务管理任务。
- IAM 用户— 一个IAM 用户是你的身份AWS 账户它具有特定的自定义权限（例如，在 Storage Gateway 中创建网关的权限）。您可以使用 IAM 用户名和密码登录以保护 AWS 网页（如 AWS Management Console、AWS 开发论坛或 AWS Support 中心）。

  除了用户名和密码之外，您还可以为每个用户生成访问密钥。在通过AWS几个开发工具包之一或使用 AWS Command Line Interface (CLI) 以编程方式访问 服务时，可以使用这些密钥。SDK 和 CLI 工具使用访问密钥对您的请求进行加密签名。如果您不使用 AWS 工具，则必须自行对请求签名。支持 Storage Gateway签名版本 4这是用于对入站 API 请求进行身份验证的协议。有关验证请求的更多信息，请参阅 AWS 一般参考中的 Signature Version 4 签名流程。

- IAM 角色 – IAM 角色是可在账户中创建的一种具有特定权限的 IAM 身份。IAM 角色类似于 IAM 用户，因为它是一个 AWS 身份，具有确定其在 AWS 中可执行和不可执行的操作的权限策略。但是，角色旨在让需要它的任何人代入，而不是唯一地与某个人员关联。此外，角色没有关联的标准长期凭证（如密码或访问密钥）。相反，当您代入角色时，它会为您提供角色会话的临时安全凭证。具有临时凭证的 IAM 角色在以下情况下很有用：

  - 联合身份用户访问 – 您可以不创建 IAM 用户，而是使用来自 AWS Directory Service、您的企业用户目录或 Web 身份提供商的现有身份。这些用户称为联合身份用户。在通过身份提供商请求访问权限时，AWS 将为联合身份用户分配角色。有关联合身份用户的更多信息，请参阅 IAM 用户指南中的联合身份用户和角色。

  - AWS服务访问 – 服务角色是一个 IAM 角色，服务担任该角色以代表您在您的账户中执行操作。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。

- 在 Amazon EC2 上运行的应用程序 – 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时凭证。这优先于在 EC2 实例中存储访问密钥。要将 AWS 角色分配给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个附加到实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅 IAM 用户指南中的使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

访问控制

您可以使用有效的凭证来对自己的请求进行身份验证，但您还必须拥有权限才能创建或访问 Storage Gateway 例如，您必须有权限才能在 Storage Gateway 中创建网关。

下面几节介绍如何管理 Storage Gateway 的权限。我们建议您先阅读概述。

- 概述如何管理对 Storage Gateway 的访问。
- 基于身份的策略（IAM 策略）

概述如何管理对 Storage Gateway 的访问。

所有AWS资源归 Amazon Web Services 账户所有，创建和访问资源的权限由权限策略进行管理。账户管理员可以向 IAM 身份（即：用户、组和角色）附加权限策略，某些服务（如 AWS Lambda）也支持向资源附加权限策略。

> **Note**
>
> 账户管理员（或管理员用户）是具有管理员权限的用户。有关更多信息，请参阅 IAM 用户指南中的 IAM 最佳实践。

在授予权限时，您要决定谁获得权限，获得对哪些资源的权限，以及您允许对这些资源执行的具体操作。

主题

- Storage Gateway 资源和操作
- 了解资源所有权
- 管理对资源的访问
- 指定策略元素：操作、效果、资源和委托人
- 在策略中指定条件

Storage Gateway 资源和操作

在 Storage Gateway 中，主要资源是网关. Storage Gateway 还支持以下其他资源类型：文件共享、卷、虚拟磁带、iSCSI 目标和虚拟磁带库 (VTL) 设备。这些称为子资源，除非它们与网关关联，否则视为不存在。

这些资源和子资源具有与其关联的唯一 Amazon Resource Name (ARN)，如下表所示。

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`*

> **Note**
>
> Storage Gateway 资源 ID 采用大写形式。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。
>
> 2015 年 9 月 2 日前激活的网关的 ARN 包含网关名称而不是网关 ID。要获取网关的 ARN，请使用 `DescribeGatewayInformation` API 操作。

为授予执行特定 API 操作（如创建磁带）的权限，Storage Gateway 提供了一组 API 操作以创建和管理这些资源和子资源。有关 API 操作的列表，请参阅操作中的AWS Storage GatewayAPI 参考.

为授予执行特定 API 操作（如创建磁带）的权限，Storage Gateway 定义了一组您可以在权限策略中指定的操作，用于授予执行特定 API 操作的权限。一个 API 操作可能需要执行多个操作的权限。有关显示所有 Storage Gateway API 操作及其适用的资源的表，请参阅。Storage Gateway API 权限：操作、资源和条件参考.

了解资源所有权

一个资源拥有者是创建资源的 Amazon Web Services 账户。也就是说，资源所有者是的 Amazon Web Services 账户。主要实体(根账户、IAM 用户或 IAM 角色)，用于对创建资源的请求进行身份验证。以下示例说明了它的工作原理：

- 如果使用 Amazon Web Services 账户的根账户凭证激活网关，则您的 Amazon Web Services 账户即为该资源的所有者（在 Storage Gateway 中，资源为网关）。
- 如果您在 Amazon Web Services 账户中创建 IAM 用户并对`ActivateGateway`对该用户执行操作，则该用户可激活网关。但是，该用户所属的 Amazon Web Services 账户拥有这些网关资源的所有权。
- 如果您在您的 Amazon Web Services 账户中创建具有激活网关权限的 IAM 角色，则能够代入该角色的任何人都可以激活网关。角色所属的 Amazon Web Services 账户拥有网关资源。

管理对资源的访问

权限策略规定谁可以访问哪些内容。下一节介绍创建权限策略时的可用选项。

> **Note**
>
> 本节讨论如何在 Storage Gateway 范围内使用 IAM。这里不提供有关 IAM 服务的详细信息。有关完整的 IAM 文档，请参阅什么是 IAM中的IAM 用户指南。有关 IAM 策略语法和说明的信息，请参阅 IAM 用户指南中 AWS IAM 策略参考。

附加到 IAM 身份的策略称作基于身份 的策略（IAM 策略），附加到资源的策略称作基于资源 的策略。Storage Gateway 只支持基于身份的策略 (IAM 策略)。

主题

- 基于身份的策略（IAM 策略）
- 基于资源的策略

基于身份的策略（IAM 策略）

您可以向 IAM 身份附加策略。例如，可以：

- 将权限策略附加到账户中的用户或组— 账户管理员可以使用与特定用户关联的权限策略为该用户授予创建 Storage Gateway 资源（如网关、卷或磁带）的权限。
- 向角色挂载权限策略（授予跨账户权限）– 您可以向 IAM 角色挂载基于身份的权限策略，以授予跨账户的权限。例如，账户 A 中的管理员可以创建一个角色，以向其他 Amazon Web Services 账户（如账户 B）授予跨账户权限的角色。AWS服务如下：
  1. 账户 A 管理员可以创建一个 IAM 角色，然后向该角色附加授予其访问账户 A 中资源的权限策略。
  2. 账户 A 管理员可以向将账户 B 标识为能够代入该角色的委托人的角色附加信任策略。
  3. 之后，账户 B 管理员可以委派权限，指派账户 B 中的任何用户担任该角色。这样，账户 B 中的用户就可以创建或访问账户 A 中的资源了。如果您需要授予AWS 服务权限来担任该角色，则信任策略中的委托人也可以是 AWS 服务委托人。

  有关使用 IAM 委托权限的更多信息，请参阅 IAM 用户指南中的访问权限管理。

以下示例策略授予对所有资源执行所有 `List*` 操作的权限。此操作是只读操作。因此，该策略不允许用户更改资源的状态。

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "AllowAllListActionsOnAllResources",
            "Effect": "Allow",
            "Action": [
                "storagegateway:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

有关将基于身份的策略用于 Storage Gateway 的更多信息，请参阅对 Storage Gateway 使用基于身份的策略（IAM 策略）. 有关用户、组、角色和权限的更多信息，请参阅 IAM 用户指南中的身份（用户、组和角色）。

基于资源的策略

其他服务 (如 Amazon S3) 还支持基于资源的权限策略。例如，您可以将策略附加到 S3 存储桶以管理对该存储桶的访问权限。Storage Gateway 不支持基于资源的策略。

指定策略元素：操作、效果、资源和委托人

对于每个 Storage Gateway 资源（请参阅Storage Gateway API 权限：操作、资源和条件参考），该服务定义了一组 API 操作（请参阅）操作)。为授予这些 API 操作的权限，Storage Gateway 定义了一组您可以在策略中指定的操作。例如，对于 Storage Gateway 网关资源，定义了以下操作：`ActivateGateway`、`DeleteGateway`, 和`DescribeGatewayInformation`. 请注意，执行某项 API 操作可能需要执行多个操作的权限。

以下是最基本的策略元素：

- Resource（资源）- 在策略中，您可以使用 Amazon Resource Name (ARN) 标识策略应用到的资源。对于 Storage Gateway 资源，您随时可以使用通配符。(*)在 IAM 策略中。有关更多信息，请参阅Storage Gateway 资源和操作。
- 操作 – 您可以使用操作关键字标识要允许或拒绝的资源操作。例如，根据指定的`Effect`，`storagegateway:ActivateGateway`权限允许或拒绝执行 Storage Gateway 的用户权限。`ActivateGatewayoperation.`
- Effect（效果）— 您可以指定当用户请求特定操作（可以是允许或拒绝）时的效果。如果没有显式授予（允许）对资源的访问权限，则隐式拒绝访问。您也可显式拒绝对资源的访问，这样可确保用户无法访问该资源，即使有其他策略授予了访问权限的情况下也是如此。

- 委托人 – 在基于身份的策略（IAM 策略）中，附加了策略的用户是隐式委托人。对于基于资源的策略，您可以指定要接收权限的用户、账户、服务或其他实体 (仅适用于基于资源的策略)。Storage Gateway 不支持基于资源的策略。

有关 IAM 策略语法和描述的更多信息，请参阅 IAM 用户指南中的AWS IAM 策略参考。

有关显示所有 Storage Gateway API 操作的表，请参阅。Storage Gateway API 权限：操作、资源和条件参考.

在策略中指定条件

当您授予权限时，可使用 IAM 策略语言指定一些条件，这些条件规定在授予权限时策略何时生效。例如，您可能希望策略仅在特定日期后应用。有关使用策略语言指定条件的更多信息，请参阅 IAM 用户指南中的条件。

要表示条件，您可以使用预定义的条件键。没有特定于 Storage Gateway 的条件密钥。但有 AWS 范围内的条件密钥，您可以根据需要使用。有关 AWS 范围内的键的完整列表，请参阅 《IAM 用户指南》中的可用键。

对 Storage Gateway 使用基于身份的策略（IAM 策略）

本主题提供了基于身份的策略的示例，在这些策略中，账户管理员可以向 IAM 身份（即：用户、组和角色）附加权限策略。

> **Important**
>
> 我们建议您首先阅读以下介绍性主题，这些主题讲解了管理对 Storage Gateway 资源的访问权限的基本概念和选项。有关更多信息，请参阅概述如何管理对 Storage Gateway 的访问。。

本主题的各个部分涵盖以下内容：

- 使用 Storage Gateway 控制台所需的权限
- AWSStorage Gateway 的托管策略
- 客户管理的策略示例

下面介绍权限策略示例。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsSpecifiedActionsOnAllGateways",
            "Effect": "Allow",
            "Action": [
                "storagegateway:ActivateGateway",
                "storagegateway:ListGateways"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowsSpecifiedEC2ActionsOnAllGateways",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSnapshots",
                "ec2:DeleteSnapshot"
            ],
            "Resource": "*"
        }
    ]
}
```

该策略包含两个语句 (请注意两个语句中的 Action 和 Resource 元素) :

- 第一条语句授予两个 Storage Gateway 操作的权限（storagegateway:ActivateGateway和storagegateway:ListGateways) 在网关资源上。

  通配符 (*) 表示此语句可匹配任何资源。在这种情况下，该语句允许storagegateway:ActivateGateway和storagegateway:ListGateways任何网关上的操作。此处使用通配符是因为您在创建网关之前不知道资源 ID。有关如何在策略中使用通配符 (*) 的信息，请参阅示例 2：允许对网关进行只读访问。

  > **Note**
  >
  > ARN 唯一地标识AWS资源的费用。有关更多信息，请参阅 AWS 一般参考中的 Amazon Resource Name（ARN）和 AWS 服务命名空间。

  要将执行某个特定操作的权限限制为仅针对某个特定网关，请在策略中为该操作创建一个单独的语句并在该语句中指定网关 ID。

- 第二个语句授予执行 `ec2:DescribeSnapshots` 和 `ec2:DeleteSnapshot` 操作的权限。需要具有权限才能执行这些 Amazon Elastic Compute Cloud (Amazon EC2) 操作，因为从 Storage Gateway 生成的快照存储在 Amazon Elastic Block Store (Amazon EBS) 中并作为 Amazon EC2 资源进行管理，因此，它们需要执行相应的 EC2 操作。有关更多信息，请参阅 。操作中的Amazon EC2 API 参考. 由于这些 Amazon EC2 操作不支持资源级权限，因此该策略将指定通配符 (*) 作为`Resource`值而不是指定网关 ARN。

有关显示所有 Storage Gateway API 操作及其适用于的资源的表，请参阅Storage Gateway API 权限：操作、资源和条件参考.

使用 Storage Gateway 控制台所需的权限

要使用 Storage Gateway 控制台，您需要授予只读权限。如果您计划描述快照，则还需要授予执行其他操作的权限，如以下权限策略中所示：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsSpecifiedEC2ActionOnAllGateways",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        }
    ]
}
```

此额外权限之所以必需，因为从 Storage Gateway 生成的 Amazon EBS 快照将作为 Amazon EC2 资源进行管理。

要设置导航 Storage Gateway 控制台所需的最低权限，请参阅。示例 2：允许对网关进行只读访问.

AWSStorage Gateway 的托管策略

Amazon Web Services 通过提供由创建和管理的独立 IAM 策略来满足许多常用案例的要求。AWS. 托管策略可授予常用案例的必要权限，因此，您可以免去调查都需要哪些权限的工作。有关 的更多信息AWS请参阅托管策略AWS管理的策略中的IAM 用户指南.

以下AWS托管策略（您可以将它们附加到您的账户中的用户）是特定于 Storage Gateway 的：

- AWS 存储网关只读访问权限— 授予对的只读访问权限AWS Storage Gateway资源的费用。
- AWS 存储网关完全访问权限— 授予对的完全访问权限AWS Storage Gateway资源的费用。

> **Note**
>
> 您可以通过登录到 IAM 控制台并在该控制台中搜索特定策略来查看这些权限策略。

您还可以创建自定义 IAM 策略，以授予执行 AWS Storage Gateway API 操作的相关权限。您可以将这些自定义策略附加到需要这些权限的 IAM 用户或组。

客户管理的策略示例

本节的用户策略示例介绍如何授予各 Storage Gateway 操作的权限。在使用时，可使用这些策略。AWS开发工具包和AWS CLI. 当您使用控制台时，您需要授予特定于控制台的其他权限，使用 Storage Gateway 控制台所需的权限中对此进行了讨论。

> **Note**
>
> 所有示例都使用美国西部 (俄勒冈) 区域 (`us-west-2`) 并且包含虚构的账户 ID。

主题

- 示例 1：允许所有网关上的任何 Storage Gateway 操作
- 示例 2：允许对网关进行只读访问
- 示例 3：允许访问特定的网关
- 示例 4：允许用户访问特定卷
- 示例 5：允许对具有特定前缀的网关进行所有操作

示例 1：允许所有网关上的任何 Storage Gateway 操作

以下策略允许用户执行所有 Storage Gateway 操作。该策略还允许用户执行 Amazon EC2 操作 (DescribeSnapshots和DeleteSnapshot) 在从 Storage Gateway 生成的 Amazon EBS 快照上。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllAWSStorageGatewayActions",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {You can use Windows ACLs only with file shares that are enabled for Active
 Directory.
            "Sid": "AllowsSpecifiedEC2Actions",
            "Action": [
                "ec2:DescribeSnapshots",
                "ec2:DeleteSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

示例 2：允许对网关进行只读访问

以下策略允许对全部资源的 `List*` 和 `Describe*` 操作。请注意这些操作是只读操作。因此，该策略不允许用户更改任何资源的状态，也就是说，该策略不允许用户执行以下操作：`DeleteGateway`、`ActivateGateway`, 和`ShutdownGateway`.

该策略还允许 `DescribeSnapshots` Amazon EC2 操作。有关更多信息，请参阅 。DescribeSnapshots中的Amazon EC2 API 参考.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowReadOnlyAccessToAllGateways",
            "Action": [
                "storagegateway:List*",
                "storagegateway:Describe*"
            ],
```

```
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "AllowsUserToDescribeSnapshotsOnAllGateways",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

在上一策略中，除使用通配符 (*) 外，您也可以将该策略涵盖的资源范围限定到某个特定网关，如下例所示。然后，该策略将仅在该特定网关上允许这些操作。

```
"Resource": [
              "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
              "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
            ]
```

在网关内，您可以进一步将资源范围仅限制到网关卷，如下例所示：

```
"Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/volume/
*"
```

示例 3：允许访问特定的网关

下面的策略允许对具体网关的所有操作。该用户对您可能已部署的其他网关的访问受限制。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowReadOnlyAccessToAllGateways",
            "Action": [
                "storagegateway:List*",
                "storagegateway:Describe*"
            ],
```

```
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "AllowsUserToDescribeSnapshotsOnAllGateways",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "AllowsAllActionsOnSpecificGateway",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
            ]
        }
    ]
}
```

如果策略关联的用户使用 API 或AWS用于访问网关的 SDK。但是，如果用户要使用 Storage Gateway 控制台，则您还必须授予权限以允许`ListGateways`操作，如以下示例所示。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllActionsOnSpecificGateway",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
            ]
        },
        {
```

```
            "Sid": "AllowsUserToUseAWSConsole",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

示例 4：允许用户访问特定卷

以下策略允许用户对网关上的某个特定卷执行所有操作。由于用户在默认情况下没有任何权限，该策略会将用户限定为仅能访问某个特定的卷。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantsPermissionsToSpecificVolume",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/volume/volume-id"
        },
        {
            "Sid": "GrantsPermissionsToUseStorageGatewayConsole",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

如果策略关联的用户使用 API 或AWS用于访问卷的 SDK。但是，如果此用户要使用AWS Storage Gateway控制台，还必须授予权限才能允许`ListGateways`操作，如以下示例所示。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantsPermissionsToSpecificVolume",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-
id/volume/volume-id"
        },
        {
            "Sid": "GrantsPermissionsToUseStorageGatewayConsole",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

示例 5：允许对具有特定前缀的网关进行所有操作

以下策略允许用户对名称以开头的网关执行所有 Storage Gateway 操作。DeptX. 该策略还允许DescribeSnapshots如果您计划描述快照，则需要执行 Amazon EC2 操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsActionsGatewayWithPrefixDeptX",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/DeptX"
        },
        {
            "Sid": "GrantsPermissionsToSpecifiedAction",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
```

```
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

如果策略关联的用户使用 API 或AWS用于访问网关的 SDK。但是，如果此用户计划使用AWS Storage Gateway如所述，您必须授予其他权限。示例 3：允许访问特定的网关.

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，您可以根据标签使用 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。

```
{
  "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:region:account-id:*/*"
        }
    ]
}
```

根据 IAM 请求中的标签控制访问

要控制 IAM 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 IAM 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。**Department**和**Finance**. 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。

```
{
   "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"
            }
         }
      }
   ]
}
```

使用 Microsoft Windows ACL 控制对 SMB 文件共享的访问

Amazon S3 File Gateway 支持两种不同的方法，用于控制对通过 SMB 文件共享存储的文件和目录的访问权限：POSIX 权限或 Windows ACL。

在本节中，您可以找到有关如何在使用 Microsoft Active Directory (AD) 启用的 SMB 文件共享上使用 Microsoft Windows 访问控制列表 (ACL) 的信息。通过使用 Windows ACL，您可以为 SMB 文件共享中的文件和文件夹设置精细控制权限。

下面是 SMB 文件共享上的 Windows ACL 的一些重要特征：

- 当文件网关加入 Active Directory 域时，默认情况下，SMB 文件共享选择 Windows ACL。
- 启用 ACL 时，ACL 信息将保留在 Amazon S3 对象元数据中。
- 对于每个文件或文件夹，网关保留最多 10 个 ACL。
- 当您使用启用了 ACL 的 SMB 文件共享来访问在网关外创建的 S3 对象时，对象将从父文件夹继承 ACL 的信息。
- SMB 文件共享的默认根 ACL 为每个人提供完全访问权限，不过您可以更改根 ACL 的权限。您可以使用根 ACL 来控制对文件共享的访问。您可以设置谁可以挂载文件共享（映射驱动器）以及用户在文件共享中递归地获取文件和文件夹的哪些权限。但是，我们建议您在 S3 存储桶中的顶级文件夹上设置此权限，以便保留 ACL。

使用 CreateSMBFileShare API 操作创建新的 SMB 文件共享时，可以启用 Windows ACL。或者，您可以使用 UpdateSMBFileShare API 操作在现有 SMB 文件共享上启用 Windows ACL。

在新 SMB 文件共享上启用 Windows ACL

执行以下步骤以在新的 SMB 文件共享上启用 Windows ACL。

在创建新的 SMB 文件共享时启用 Windows ACL

1. 创建文件网关（如果您还没有）。有关更多信息，请参阅 。
2. 如果网关未加入域，请将其添加到域中。有关更多信息，请参阅 。
3. 创建 SMB 文件共享。
4. 通过 Storage Gateway 控制台在文件共享上启用 Windows ACL。

   要使用 Storage Gateway 控制台，请执行以下操作：

   a. 选择文件共享，然后选择 Edit file share (编辑文件共享)。
   b. 对于 File/directory access controlled by (文件/目录访问控制方式) 选项，选择 Windows Access Control List (Windows 访问控制列表)。
5. （可选）如果希望管理员用户有权更新文件共享中所有文件和文件夹的相关 ACL，请将管理员用户添加到 AdminUsersList。
6. 更新根文件夹下父文件夹的 ACL。为此，请使用 Windows 文件资源管理器在 SMB 文件共享中的文件夹上配置 ACL。

   > **Note**
   >
   > 如果在根目录而不是根目录下的父文件夹上配置 ACL，则 ACL 权限不会保留在 Amazon S3 中。

   我们建议在文件共享根目录下的顶级文件夹中设置 ACL，而不是直接在文件共享的根目录下设置 ACL。此方法将信息作为对象元数据保存在 Amazon S3 中。
7. 根据需要启用继承。

   > **Note**
   >
   > 您可以为 2019 年 5 月 8 日之后创建的文件共享启用继承。

如果启用继承并以递归方式更新权限，则 Storage Gateway 会更新 S3 存储桶中的所有对象。根据存储桶中的对象数量，更新可能需要一段时间才能完成。

在现有 SMB 文件共享上启用 Windows ACL

执行以下步骤以在具有 POSIX 权限的现有 SMB 文件共享上启用 Windows ACL。

使用 Storage Gateway 控制台在现有的 SMB 文件共享上启用 Windows ACL

1. 选择文件共享，然后选择 Edit file share (编辑文件共享)。
2. 对于 File/directory access controlled by (文件/目录访问控制方式) 选项，选择 Windows Access Control List (Windows 访问控制列表)。
3. 根据需要启用继承。

> **Note**
>
> 我们不建议在根级别设置 ACL，因为如果执行此操作并删除您的网关，则需要再次重置 ACL。

如果启用继承并以递归方式更新权限，则 Storage Gateway 会更新 S3 存储桶中的所有对象。根据存储桶中的对象数量，更新可能需要一段时间才能完成。

使用 ACL 时的限制

使用 Windows ACL 控制对 SMB 文件共享的访问时，请记住以下限制：

- 仅当使用 Windows SMB 客户端访问文件共享时，为 Active Directory 启用的文件共享上才支持 Windows ACL。
- 文件网关针对每个文件和目录最多支持 10 个 ACL 条目。
- 文件网关不支持`Audit`和`Alarm`条目，它们是系统访问控制列表 (SACL) 条目。文件网关支持 `Allow` 和 `Deny` 条目，它们是自由访问控制列表 (DACL) 条目。
- SMB 文件共享的根 ACL 设置仅针对该网关，并且设置将在网关更新和重新启动后保持不变。

> **Note**
>
> 如果在根目录而不是根目录下的父文件夹上配置 ACL，则 ACL 权限不会保留在 Amazon S3 中。

在给定以下条件的情况下，请确保执行以下操作：

- 如果将多个网关配置为访问同一个 Amazon S3 存储桶，请在每个网关上配置根 ACL 以保持权限一致。
- 如果您删除文件共享并在同一个 Amazon S3 存储桶上重新创建，请确保使用的是同一组根 ACL。

Storage Gateway API 权限：操作、资源和条件参考

在设置访问控制和编写可附加到 IAM 身份的权限策略（基于身份的策略）时，您可以将下表作为参考。此表列出了每个 Storage Gateway API 操作、您可为其授予执行该操作的权限的相应操作，以及AWS您可以授予权限的资源。您可以在策略的 `Action` 字段中指定这些操作，并在策略的 `Resource` 字段中指定资源值。

您可以使用AWS在您的 Storage Gateway 策略中用于表达条件。有关 AWS 范围内的键的完整列表，请参阅 《IAM 用户指南》 中的可用键。

> **Note**
>
> 要指定操作，请在 API 操作名称之前使用 `storagegateway:` 前缀 (例如，`storagegateway:ActivateGateway`)。对于每个 Storage Gateway 操作，您可以指定通配符 (*) 作为资源。

有关包含 ARN 格式的 Storage Gateway 资源的列表，请参阅。Storage Gateway 资源和操作.

以下是 Storage Gateway API 和所需的操作权限。

ActivateGateway

操作： `storagegateway:ActivateGateway`

资源： `*`

AddCache

操作： `storagegateway:AddCache`

资源： `arn:aws:storagegateway:region:account-id:gateway/gateway-id`

AddTagsToResource

操作： storagegateway:AddTagsToResource

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

或

arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

或

arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

AddUploadBuffer

操作： storagegateway:AddUploadBuffer

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

AddWorkingStorage

操作： storagegateway:AddWorkingStorage

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

CancelArchival

操作： storagegateway:CancelArchival

资源： arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

CancelRetrieval

操作： storagegateway:CancelRetrieval

资源： arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

CreateCachediSCSIVolume

操作： storagegateway:CreateCachediSCSIVolume

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

CreateSnapshot

操作： storagegateway:CreateSnapshot

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

CreateSnapshotFromVolumeRecoveryPoint

操作： storagegateway:CreateSnapshotFromVolumeRecoveryPoint

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

CreateStorediSCSIVolume

操作： storagegateway:CreateStorediSCSIVolume

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

CreateTapes

操作： storagegateway:CreateTapes

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteBandwidthRateLimit

操作： storagegateway:DeleteBandwidthRateLimit

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteChapCredentials

操作： storagegateway:DeleteChapCredentials

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/target/*iSCSItarget*

DeleteGateway

操作： storagegateway:DeleteGateway

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteSnapshotSchedule

操作： storagegateway:DeleteSnapshotSchedule

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DeleteTape

操作： storagegateway:DeleteTape

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteTapeArchive

操作： storagegateway:DeleteTapeArchive

资源： *

DeleteVolume

操作： storagegateway:DeleteVolume

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DescribeBandwidthRateLimit

操作： storagegateway:DescribeBandwidthRateLimit

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeCache

操作： storagegateway:DescribeCache

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeCachediSCSIVolumes

操作： storagegateway:DescribeCachediSCSIVolumes

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DescribeChapCredentials

操作： storagegateway:DescribeChapCredentials

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/target/*iSCSItarget*

DescribeGatewayInformation

操作： storagegateway:DescribeGatewayInformation

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeMaintenanceStartTime

操作： storagegateway:DescribeMaintenanceStartTime

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeSnapshotSchedule

操作： storagegateway:DescribeSnapshotSchedule

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DescribeStorediSCSIVolumes

操作： storagegateway:DescribeStorediSCSIVolumes

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DescribeTapeArchives

操作： storagegateway:DescribeTapeArchives

资源： *

DescribeTapeRecoveryPoints

操作： storagegateway:DescribeTapeRecoveryPoints

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeTapes

操作： storagegateway:DescribeTapes

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeUploadBuffer

操作： storagegateway:DescribeUploadBuffer

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeVTLDevices

操作： storagegateway:DescribeVTLDevices

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeWorkingStorage

操作： storagegateway:DescribeWorkingStorage

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DisableGateway

操作： storagegateway:DisableGateway

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ListGateways

操作： storagegateway:ListGateways

资源： *

ListLocalDisks

操作： storagegateway:ListLocalDisks

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ListTagsForResource

操作： storagegateway:ListTagsForResource

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

或

arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

或

arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

ListTapes

操作： storagegateway:ListTapes

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ListVolumeInitiators

操作： storagegateway:ListVolumeInitiators

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

ListVolumeRecoveryPoints

操作： storagegateway:ListVolumeRecoveryPoints

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ListVolumes

操作： storagegateway:ListVolumes

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

RemoveTagsFromResource

操作： storagegateway:RemoveTagsFromResource

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

或

arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

或

arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

ResetCache

操作： storagegateway:ResetCache

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

RetrieveTapeArchive

操作： storagegateway:RetrieveTapeArchive

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

RetrieveTapeRecoveryPoint

操作： storagegateway:RetrieveTapeRecoveryPoint

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ShutdownGateway

操作： storagegateway:ShutdownGateway

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

StartGateway

操作： storagegateway:StartGateway

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

UpdateBandwidthRateLimit

操作： storagegateway:UpdateBandwidthRateLimit

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

UpdateChapCredentials

操作： storagegateway:UpdateChapCredentials

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/target/*iSCSItarget*

UpdateGatewayInformation

操作： storagegateway:UpdateGatewayInformation

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

UpdateGatewaySoftwareNow

操作： storagegateway:UpdateGatewaySoftwareNow

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

UpdateMaintenanceStartTime

操作： storagegateway:UpdateMaintenanceStartTime

资源： arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

UpdateSnapshotSchedule

操作： storagegateway:UpdateSnapshotSchedule

资源： `arn:aws:storagegateway:region:account-id:gateway/gateway-id/volume/volume-id`

UpdateVTLDeviceType

操作： `storagegateway:UpdateVTLDeviceType`

资源： `arn:aws:storagegateway:region:account-id:gateway/gateway-id/device/vtldevice`

相关主题

- 访问控制
- 客户管理的策略示例

将服务相关角色用于 Storage Gateway

使用 Storage GatewayAWS Identity and Access Management(IAM)服务相关角色. 服务相关角色是一种与 Storage Gateway 直接关联的独特类型的 IAM 角色。服务相关角色由 Storage Gateway 预定义，并包含服务调用其他角色所需的所有权限。AWS服务代表您。

您可以使用服务相关角色轻松设置 Storage Gateway，因为您不必手动添加所需的权限。除非另外定义了其服务相关角色的权限，除非另外定义，否则只有 Storage Gateway 可以代入该角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其它 IAM 实体的权限策略。

有关支持服务相关角色的其它服务的信息，请参阅《使用 IAM 的 AWS 服务》并查找 Service-Linked Role（服务相关角色）列中显示为 Yes（是）的服务。选择 Yes (是) 和链接，查看该服务的服务相关角色文档。

Storage Gateway 的服务相关角色权限

使 Storage Gateway 名为的服务相关角色。存储网关的 AWS 服务角色— 存储网关的 AWS 服务角色。

AWSServiceRoleForStorageGateway 服务相关角色信任以下服务以担任该角色：

- `storagegateway.amazonaws.com`

角色权限策略允许 Storage Gateway 对指定资源完成以下操作：

- 操作：arn:aws:fsx:*:*:backup/* 上的 fsx:ListTagsForResource

您必须配置权限以允许 IAM 实体（如用户、组或角色）创建和编辑服务相关角色。有关更多信息，请参阅 IAM 用户指南中的服务相关角色权限。

为 Storage Gateway 创建服务相关角色

无需手动创建服务相关角色。当你创建 Storage Gateway 时AssociateFileSystem中的 API 调用 AWS Management Console，AWS CLI，或者AWSAPI、Storage Gateway 将为您创建服务相关角色。

> **Important**
>
> 如果您在其他使用此角色支持的功能的服务中完成某个操作，此服务相关角色可以出现在您的账户中。此外，如果您在 2021 年 3 月 31 日之前在 Storage Gateway 服务开始支持服务相关角色之前已在使用 Storage Gateway 服务，则存储网关会在您的账户中创建 AWSServiceRoleForStorageGateway 角色。要了解更多信息，请参阅我的 IAM 账户中出现新角色。

如果删除此服务相关角色，然后需要再次创建，可以使用相同流程在账户中重新创建此角色。当你创建 Storage Gateway 时AssociateFileSystemAPI 调用时，Storage Gateway 将再次为您创建服务相关角色。

您还可以使用 IAM 控制台通过存储网关的 AWS 服务角色使用案例。在 AWS CLI 或 AWS API 中，使用 storagegateway.amazonaws.com 服务名称创建服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的创建服务相关角色。如果您删除了此服务相关角色，则可以使用此相同过程再次创建角色。

编辑 Storage Gateway 的服务相关角色

Storage Gateway 不允许您编辑 AWSServiceRoleForStorageGateway 服务相关角色。创建服务相关角色后，将无法更改角色名称，因为可能有多个实体引用该角色。但是可以使用 IAM 编辑角色说明。有关更多信息，请参阅 IAM 用户指南中的编辑服务相关角色。

删除 Storage Gateway 的服务相关角色

Storage Gateway 不会自动删除 AWS ServiceRoleForStorageGateway 角色。要删除 AWS ServiceRole ForStorageGateWay 角色，您需要调用iam:DeleteSLRAPI。如果没有依赖于服务

相关角色的存储网关资源，则删除将成功，否则删除将失败。如果要删除服务关联角色，则需要使用 IAM APIiam:DeleteRole要么iam:DeleteServiceLinkedRole. 在这种情况下，您需要使用 Storage Gateway API 先删除账户中的任何网关或文件系统关联，然后通过使用删除服务链接角色iam:DeleteRole要么iam:DeleteServiceLinkedRoleAPI。当您使用 IAM 删除服务关联角色时，您需要使用 Storage GatewayDisassociateFileSystemAssociationAPI 首先删除账户中的所有文件系统关联。否则，删除操作将失败。

> **Note**
>
> 如果在您试图删除资源时 Storage Gateway 服务正在使用该角色，则删除操作可能会失败。如果发生这种情况，请等待几分钟后重试。

删除 AWS ServiceRoleForSStorage Gateway 所用的 StorageGateway 资源

1. 使用我们的服务控制台、CLI 或 API 调用清理资源并删除角色，或者使用 IAM 控制台、CLI 或 API 执行删除操作。在这种情况下，您需要使用 Storage Gateway API 首先删除账户中的任何网关和文件系统关联。
2. 如果您使用 IAM 控制台、CLI 或 API，请使用 IAM 删除服务相关角色。DeleteRole要么DeleteServiceLinkedRoleAPI。

使用 IAM 手动删除服务相关角色

使用 IAM 控制台AWS CLI，或者AWS删除服务相关角色的 AWS ServiceRole 的 API。有关更多信息，请参阅 IAM 用户指南中的删除服务相关角色。

服务相 Storage Gateway 角色支持的区域

Storage Gateway 支持在提供该服务的所有区域中使用服务相关角色。有关更多信息，请参阅AWS服务终端节点。

每个 Storage Gateway 不支持在提供该服务的每个区域中使用服务相关角色。您可以在以下区域中使用 AWS ServiceRoleForStorageGateway 角色。

区域名称	区域标识	Support Storage Gateway
US East (N. Virginia)	us-east-1	是

区域名称	区域标识	Support Storage Gateway
US East (Ohio)	us-east-2	是
US West (N. California)	us-west-1	是
US West (Oregon)	us-west-2	是
Asia Pacific (Mumbai)	ap-south-1	是
亚太地区（大阪）	ap-northeast-3	是
Asia Pacific (Seoul)	ap-northeast-2	是
亚太地区（新加坡）	ap-southeast-1	是
Asia Pacific (Sydney)	ap-southeast-2	是
Asia Pacific (Tokyo)	ap-northeast-1	是
Canada (Central)	ca-central-1	是
欧洲（法兰克福）	eu-central-1	是
Europe (Ireland)	eu-west-1	是
欧洲（伦敦）	eu-west-2	是
欧洲（巴黎）	eu-west-3	是
South America (São Paulo)	sa-east-1	是
AWS GovCloud (US)	us-gov-west-2	是

AWS Storage Gateway 中的日志记录和监控

Storage Gateway 与AWS CloudTrail，提供了用户、角色或所执行操作的记录的服务。AWSStorage Gateway 中的服务。CloudTrail 将 Storage Gateway 的所有 API 调用作为事件捕获。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。如果您创建跟踪，则可以使 CloudTrail 事件持续传送到 Amazon S3 存储桶（包括 Storage Gateway 的事件）。如果您

不配置跟踪记录，则仍可在 CloudTrail 控制台中的 Event history（事件历史记录）中查看最新事件。通过使用 CloudTrail 收集的信息，您可以确定向 Storage Gateway 发出了什么请求、发出请求的 IP 地址、何人发出的请求、请求的发出时间以及其他详细信息。

如需了解有关 CloudTrail 的更多信息，请参阅 AWS CloudTrail 用户指南。

CloudTrail 中的 Storage Gateway 信息

在您创建 AWS 账户时，将在该账户上启用 CloudTrail。当 Storage Gateway 中发生活动时，该活动将记录在 CloudTrail 事件中，并与其他活动一同保存AWS中的服务事件事件记录. 您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

要持续记录您的事件AWS账户（包括 Storage Gateway 的事件）创建跟踪。通过跟踪记录，CloudTrail 可将日志文件传送至 Amazon S3 存储桶。预设情况下，在控制台中创建跟踪时，此跟踪应用于所有 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 Bucket。此外，您可以配置其他 AWS 服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取行动。有关更多信息，请参阅下列内容：

- 创建跟踪记录概述
- CloudTrail 支持的服务和集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 从多个区域接收 CloudTrail 日志文件和从多个账户接收 CloudTrail 日志文件

记录所有 Storage Gateway 操作，中对这些操作进行了介绍。操作主题。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。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是 AWS Identity and Access Management (IAM) 用户凭证发出的。
- 请求是使用角色还是联合身份用户的临时安全凭证发出的。
- 请求是否由其他 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，可用于将事件作为日志文件传送到您指定的 Amazon S3 Bucket。CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

下面的示例显示了一个 CloudTrail 日志条目，该条目说明了 操作。

```
{ "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"
            }]
}
```

下面的示例显示了一个 CloudTrail 日志条目，该条目说明了 ListGateways way 操

```
{
 "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"
              }]
}
```

的合规性验证AWSStorage Gateway

第三方审计员评估的安全性和合规性AWSStorage Gateway 作为多个组成部分AWS合规性计划。这包括 SOC、PCI、ISO、FedRAMP、HIPAA、MTCS、C5、K-ISMS、ENS High、OSPAR 和 HITRUST CSF。

有关特定合规性计划范围内的 AWS 服务列表，请参阅合规性计划范围内的 AWS 服务。有关常规信息，请参阅AWS合规性计划。

您可以使用 AWS Artifact 下载第三方审计报告。有关更多信息，请参阅下载 AWS Artifact 中的报告。

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实现合规性：

- 安全性与合规性 Quick Start 指南 - 这些部署指南讨论了架构注意事项，并提供了在 AWS 上部署基于安全性和合规性的基准环境的步骤。
- 《设计符合 HIPAA 安全性和合规性要求的架构》白皮书 – 此白皮书介绍公司如何使用AWS创建符合 HIPAA 标准的应用程序。
- AWS合规性资源 – 此业务手册和指南集合可能适用于您的行业和位置。
- 《AWS Config 开发人员指南》中的使用规则评估资源 – 此 AWS Config 服务评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- AWS Security Hub – 此AWS服务提供了AWS中安全状态的全面视图，可帮助您检查是否符合安全行业标准和最佳实践。

中的故障恢复能力AWSStorage Gateway

AWS全球基础设施围绕AWS区域和可用区构建。AWS区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域和可用区的更多信息，请参阅 AWS 全球基础设施。

除了AWS全球基础设施，Storage Gateway 提供了多种功能以帮助支持您的数据弹性和备份需求。

- 使用 VMware vSphere 高可用性 (VMware HA) 帮助保护存储工作负载免受硬件、管理程序或网络故障的影响。有关更多信息，请参阅 。将 VMware vSphere 高可用性与 Storage Gateway 结合使用.
- 使用 AWS Backup 备份您的卷。有关更多信息，请参阅 。使用AWS Backup备份您的卷.

- 从恢复点克隆您的卷。有关更多信息，请参阅 。克隆卷.
- 在 Amazon S3 Glacier 中将虚拟磁带存档。有关更多信息，请参阅 。存档虚拟磁带.

中的基础设施安全性AWSStorage Gateway

作为托管服务，AWSStorage Gateway 受AWS中描述的全局网络安全程序Amazon Web Services：安全过程概述白皮书。

你用AWS发布 API 调用以通过网络访问 Storage Gateway。客户端必须支持传输层安全性 (TLS) 1.0 或更高版本。建议使用 TLS 1.2 或更高版本。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 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service (AWS STS) 生成临时安全凭证来对请求进行签名。

Storage Gateway 的安全最佳实践

AWSStorage Gateway 提供了在您开发和实施自己的安全策略时需要考虑的大量安全功能。以下最佳实践是一般指导原则，并不代表完整安全解决方案。这些最佳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.

排查网关问题

在下文中，您可以找到有关排查网关、文件共享、卷、虚拟磁带和快照相关问题的信息。本地网关问题排查信息涵盖 VMware ESXi 和 Microsoft Hyper-V 客户端上部署的网关。文件共享的问题排查信息适用于 Amazon S3 文件网关类型。卷的问题排查信息适用于卷网关类型。磁带的问题排查信息适用于磁带网关类型。网关问题的问题排查信息适用于使用 CloudWatch 指标。高可用性问题的疑难解答信息涵盖了在 VMware vSphere High Availability (HA) 平台上运行的网关。

主题

排查本地网关问题

您可以在下面找到有关您在使用场内网关时可能遇到的典型问题以及如何启用的信息。AWS Support 以帮助排查网关问题。

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	措施
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，可在 Summary (摘要) 选项卡上的 vSphere 客户端中找到 VM 的 IP 地址。 • 对于 Microsoft Hyper-V，可登录本地控制台查找 VM 的 IP 地址。

问题	措施
	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终端节点用于出站通信。AWS. 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。
当您单击时，网关的激活过程失败继续激活按钮在 Storage Gateway 管理控制台中。	• 检查网关 VM 是否可通过从客户端 ping 通。 • 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。有关同步管理程序主机和 VM 的时间的信息，请参阅 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 控制台和设置和激活网关向导。 • 检查您的 VM 至少有 7.5 GB 的 RAM。如果 RAM 少于 7.5 GB，网关分配就会失效。有关更多信息，请参阅文件网关设置要求。
您需要移除分配为上传缓冲区空间的磁盘。例如，您可能希望减少网关的上传缓冲区空间大小，或者可能需要替换已发生故障的用作上传缓冲区的磁盘。	

问题	措施
您需要提高网关和AWS.	您可以在网络适配器 (NIC) 上设置一个独立于您的应用程序和网关 VM 之间的连接的通往 AWS 的 Internet 连接，从而提高网关到 AWS 之间的带宽。在您拥有到 AWS 的高带宽连接并且希望避免带宽争用的情况下 (尤其是在快照还原期间)，采用此方法很有用。对于高吞吐量工作负载需求，您可以使用AWS Direct Connect在本地网关和间建立专用网络连接。AWS. 若要测量从网关到 AWS 的连接的带宽，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。提高 Internet 连接性能有助于确保您的上传缓冲区不被填满。

往返您网关的吞吐量将为零。	• 在存储库的网关在 Storage Gateway 控制台的选项卡中，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 管理器）看到的 IP 地址相同。如果您发现不一致，请从 Storage Gateway 控制台重启网关，如中所述。关闭网关 VM. 重启后，中的地址IP 地址Storage Gateway 控制台中的列表网关选项卡应与您从虚拟机管理程序客户端确定的网关的 IP 地址匹配。
	  • 对于 VMware ESXi，可在 Summary (摘要) 选项卡上的 vSphere 客户端中找到 VM 的 IP 地址。
	  • 对于 Microsoft Hyper-V，可登录本地控制台查找 VM 的 IP 地址。
	• 按测试网关的网络连接中所述，检查网关到 AWS 的连接。
	• 检查网关的网络适配器配置，同时确保要启用的所有网关接口均已启用。若要查看网关的网络适配器配置，请遵循 为网关配置网络适配器 中的说明并选择能够查看网关网络配置的选项。
	
	您可以从 Amazon CloudWatch 控制台查看往返网关的吞吐量。有关测量网关与 AWS 之间的吞吐量的更多信息，请参阅性能。

您在 Microsoft Hyper-V 上导入（部署）Storage Gateway 时遇到问题。	请参阅 排查 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。

问题	措施
你会收到一条消息说：“已写入网关卷中的数据未安全存储在AWS“。	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AWS Support.

启用AWS Support帮助排除本地托管的网关故障

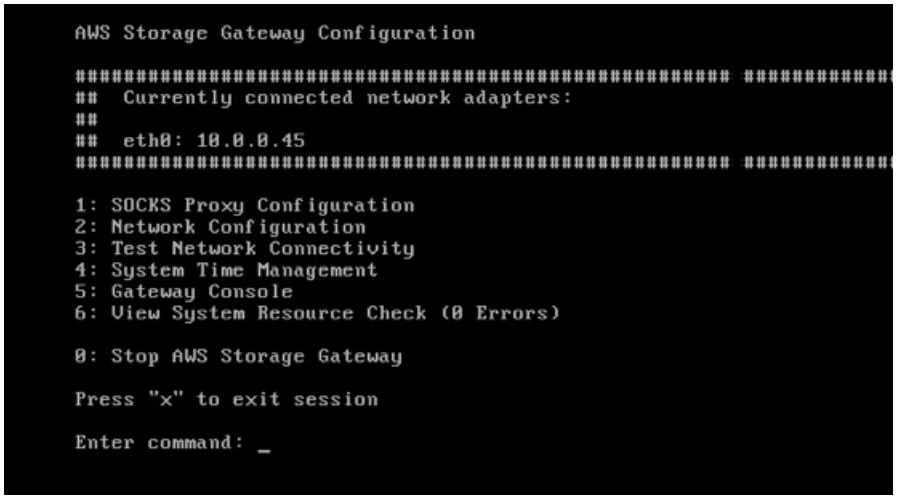
Storage Gateway 提供了一个本地控制台供您执行多个维护任务，包括启用AWS Support访问您的网关，以帮助您排查网关问题。默认情况下，AWS Support禁止访问您的网关。您可通过主机的本地控制台启用此访问。为了给予AWS Support要访问网关，您首先要登录到主机的本地控制台，导航到 Storage Gateway 的控制台，然后连接到支持服务器。

启用AWS Support访问网关

1. 登录到主机的本地控制台。

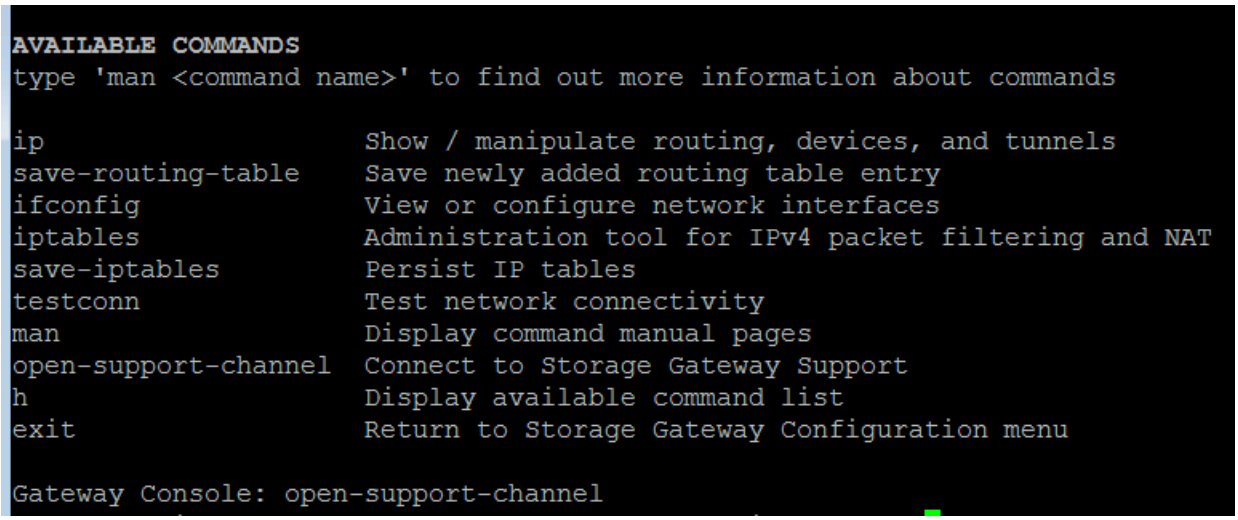
   - VMware ESXi — 有关更多信息，请参阅使用 VMware ESXi 访问网关本地控制台.
   - Microsoft Hyper-V — 有关更多信息，请参阅使用 Microsoft Hyper-V 访问网关本地控制台.

   本地控制台类似如下所示。

2. 出现提示时，输入**5**以打开AWS Support频道控制台。
3. 输入 **h** 以打开 AVAILABLE COMMANDS 窗口。
4. 请执行下列操作之一：

- 如果网关使用的是公共终端节点，请在可用命令窗口中，输入**open-support-channel**以连接到 Storage Gateway 的客户支持。允许 TCP 端口 22，以便您能打开以下网址的支持通道：AWS. 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 终端节点，请在 AVAILABLE COMMANDS 窗口中，输入 **open-support-channel**。如果未激活网关，请提供 VPC 终端节点或 IP 地址以连接到 Storage Gateway 的客户支持。允许 TCP 端口 22，以便您能打开以下网址的支持通道：AWS. 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。

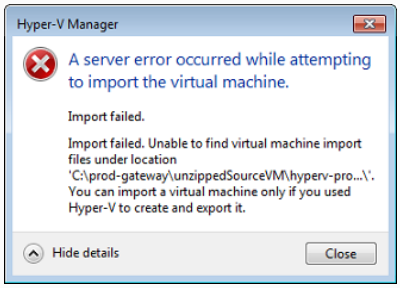
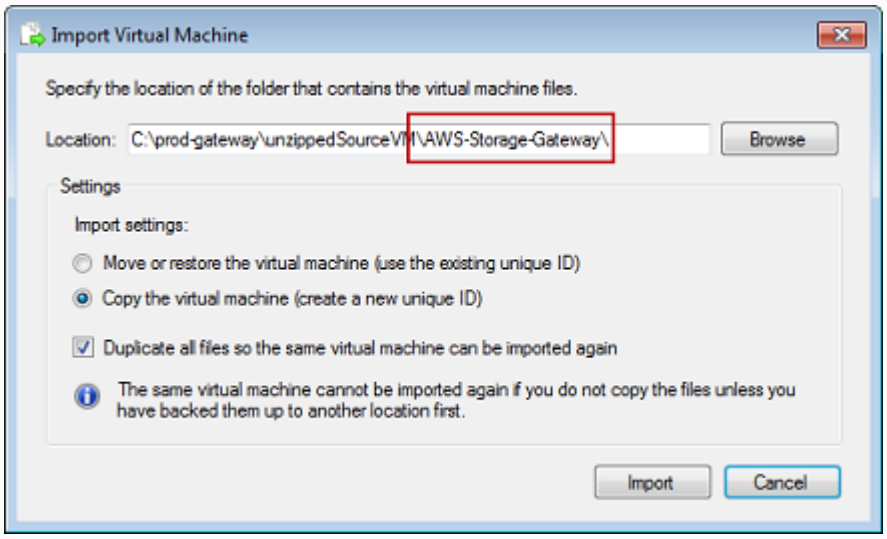
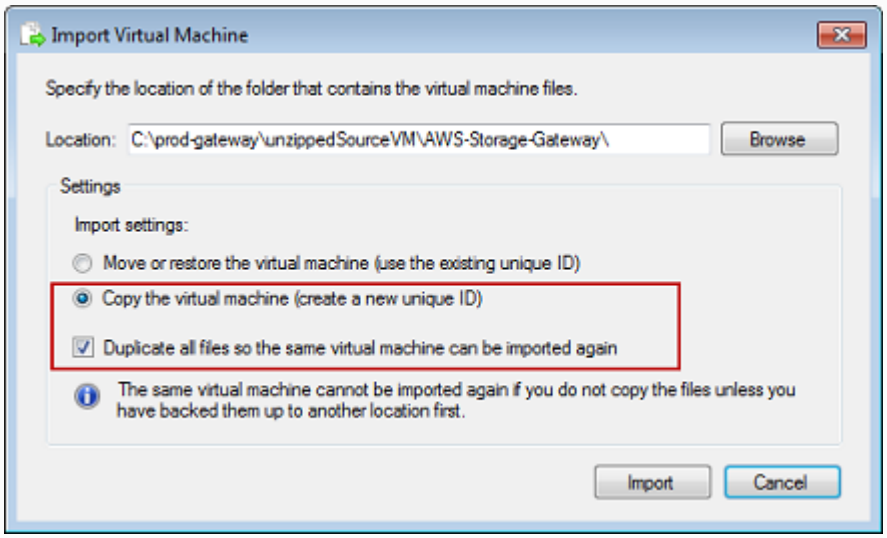


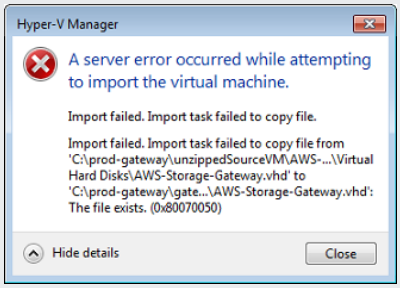
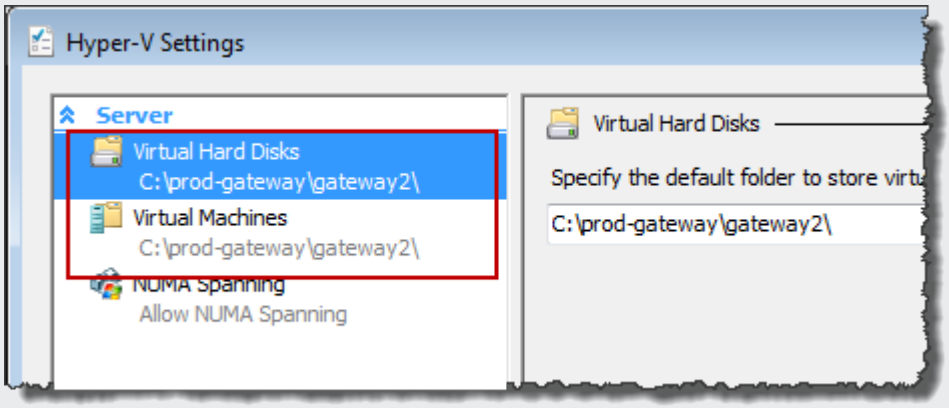
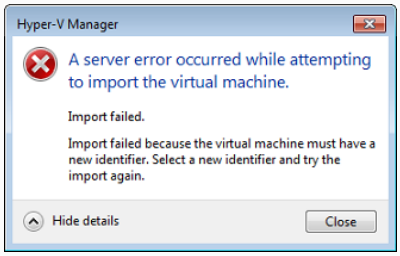
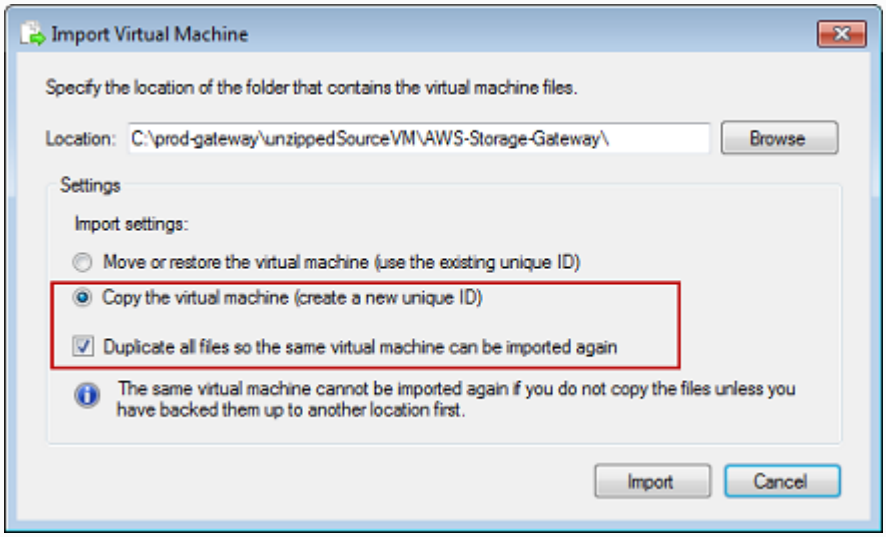
> **Note**
>
> 渠道号不是传输控制协议/用户数据报协议 (TCP/UDP) 端口号。相反，网关会与 Storage Gateway 服务器建立安全外壳 (SSH) (TCP 22) 连接，并提供用于连接的支持渠道。

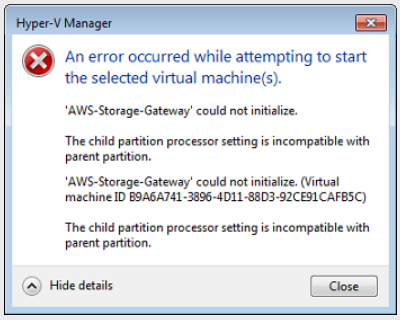
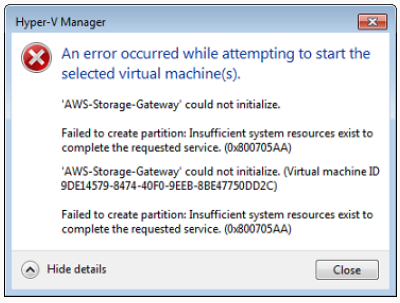
5. 建立支持通道后，为您的支持服务编号提供给AWS Support所以AWS Support可以提供故障排除帮助。
6. 在支持会话完成后，输入 **q** 以将其结束。在 Amazon Web Services Support 通知您支持会话已完成之前，不要关闭会话。
7. Enter**exit**以从 Storage Gateway 控制台注销。
8. 按照提示操作退出本地控制台。

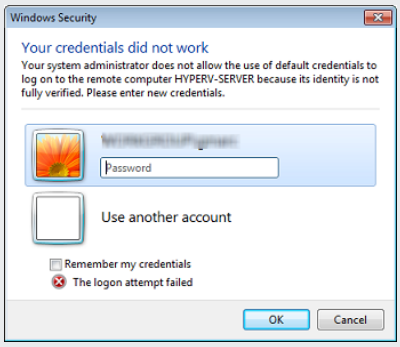
排查 Microsoft Hyper-V 设置

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	措施
您在尝试导入网关时会收到错误消息：“导入失败。Unable to find virtual machine import file under location ...”。 	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“Import Virtual Machine”对话框中所指定位置的最后一部分应该是“AWS-Storage-Gateway ”，如下例所示：  • 如果您已经部署了网关但没有选择复制虚拟机选项然后检查复制所有文件中的选项导入虚拟机对话框中，然后在已解压缩的网关文件的位置创建了虚拟机，您无法再次从此位置导入。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。下例介绍了您在计划从一个解压缩源文件位置创建多个网关的情况下必须选中的选项。 

问题	措施
您在尝试导入网关时会收到错误消息：“导入失败。Import task failed to copy file.” 	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 Settings 对话框中指定新的位置。 
您在尝试导入网关时会收到错误消息：“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，请确保选择复制虚拟机选项然后检查复制所有文件中的选项导入虚拟机对话框以为虚拟机创建新的唯一 ID。下例介绍了您应该使用的“Import Virtual Machine”对话框中的选项。 

问题	措施
您尝试启动网关 VM，但收到如下错误消息“The child partition processor setting is incompatible with parent partition.” 	此错误很可能是该网关所需的 CPU 和主机上可用的 CPU 之间的差异导致的。确保 VM 的 CPU 个数获得了底层管理程序的支持。 有关对 Storage Gateway 的要求的更多信息，请参阅。文件网关设置要求.
您尝试启动网关 VM，但收到一条错误消息 “创建分区失败：没有足够的资源来完成请求的服务。” 	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。 有关对 Storage Gateway 的要求的更多信息，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。
您必须将解压缩的 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。

问题	措施
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。

排查 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。有关本地网关和 Amazon EC2 中部署的网关之间的区别的详细信息，请参阅在 Amazon EC2 主机上部署文件网关.

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。

主题

- 过了几分钟之后你的网关激活尚未发生
- 在实例列表中找不到 EC2 网关实例
- 你想AWS Support帮助对 EC2 网关进行故障排除

过了几分钟之后你的网关激活尚未发生

在 Amazon EC2 控制台中检查以下内容：

- 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。添加安全组规则中的适用于 Linux 实例的 Amazon EC2 用户指南.
- 网关实例会标记为“running”。在 Amazon EC2 控制台中，州应该是 RUNNING (正在运行)。
- 确保您的 Amazon EC2 实例类型满足最低要求，如中所述。存储需求.

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。

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 的实例应以文本开头。**`aws-storage-gateway-ami`**.
- 如果您有几个实例基于 Storage Gateway AMI，请查看实例启动时间以寻找正确的实例。

你想AWS Support帮助对 EC2 网关进行故障排除

Storage Gateway 提供了一个本地控制台供您执行多个维护任务，包括启用AWS Support访问您的网关，以帮助您排查网关问题。默认情况下，AWS Support禁止访问您的网关。可通过 Amazon EC2 本地控制台启用此访问。可通过安全 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 安全组中的Amazon EC2 用户指南.

为了让AWS Support要连接到网关，您首先要登录到 Amazon EC2 实例的本地控制台，导航到 Storage Gateway 的控制台，然后提供该访问权限。

启用AWS Support访问 Amazon EC2 实例上部署的网关

1. 登录到 Amazon EC2 实例的本地控制台。有关说明，请转到连接到您的实例中的Amazon EC2 用户指南.

   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**
   >
   > 这些区域有：*####*是.pem文件中包含用来启动 Amazon EC2 实例的 EC2 key pair 的私有证书。有关更多信息，请参阅 。检索密钥对的公有密钥中的Amazon EC2 用户指南.

这些区域有：*##-##DNS-##*是运行网关的 Amazon EC2 实例的公共域名系统 (DNS) 名称。可通过选择 EC2 控制台中的 Amazon EC2 实例并单击说明选项卡。

2. 出现提示时，输入**6 - Command Prompt**以打开AWS Support频道控制台。
3. 输入 **h** 以打开 AVAILABLE COMMANDS 窗口。
4. 请执行下列操作之一：

   - 如果网关使用的是公共终端节点，请在可用命令窗口中，输入**open-support-channel**以连接到 Storage Gateway 的客户支持。允许 TCP 端口 22，以便您能打开以下网址的支持通道：AWS. 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 终端节点，请在 AVAILABLE COMMANDS 窗口中，输入 **open-support-channel**。如果未激活网关，请提供 VPC 终端节点或 IP 地址以连接到 Storage Gateway 的客户支持。允许 TCP 端口 22，以便您能打开以下网址的支持通道：AWS. 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**
   >
   > 渠道号不是传输控制协议/用户数据报协议 (TCP/UDP) 端口号。相反，网关会与 Storage Gateway 服务器建立安全外壳 (SSH) (TCP 22) 连接，并提供用于连接的支持渠道。

5. 建立支持通道后，为您的支持服务编号提供给AWS Support所以AWS Support可以提供故障排除帮助。
6. 在支持会话完成后，输入 **q** 以将其结束。在 Amazon Web Services Support 通知您支持会话已完成之前，不要关闭会话。
7. Enter**exit**以退出 Storage Gateway 控制台。
8. 通过控制台菜单操作来注销 Storage Gateway 实例。

排查硬件设备问题

以下主题将讨论 Storage Gateway 硬件设备可能遇到的问题以及有关排查这些问题的建议。

你无法确定服务 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)。

您如何执行出厂设置重置？

如果您需要在设备上执行出厂重置，请联系 Storage Gateway 硬件设备团队以获得 Support，如后面的 “支持” 部分中所述。

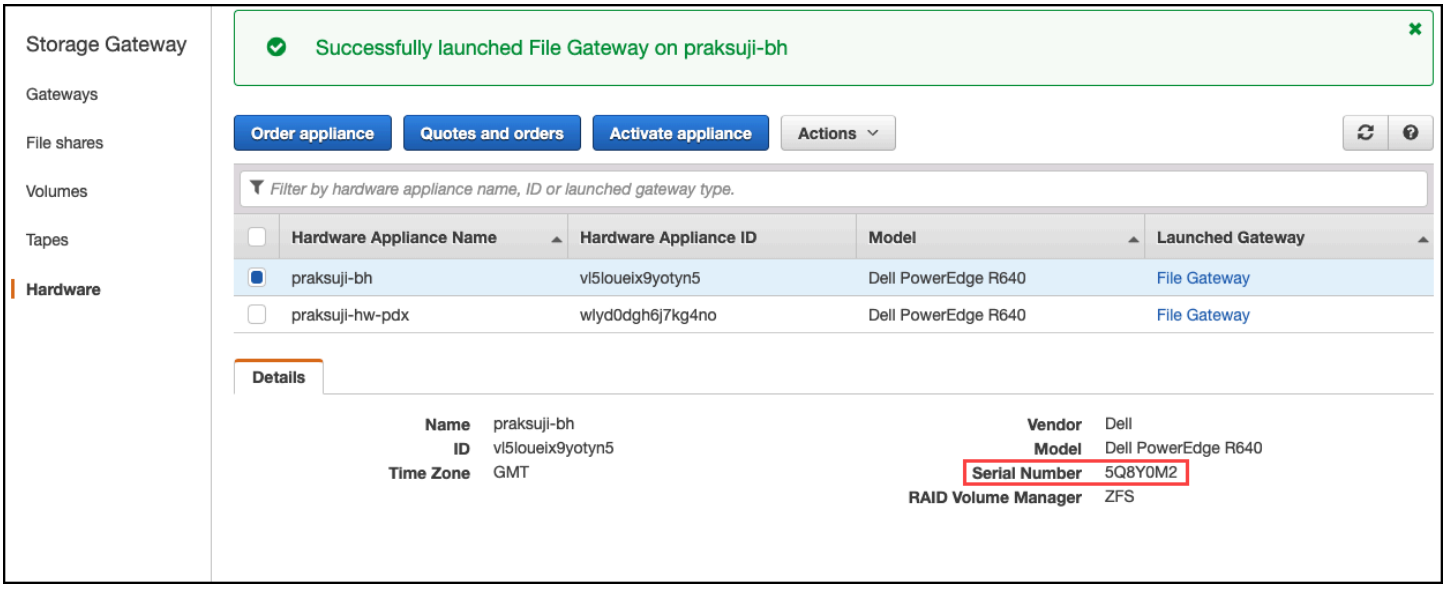
你从哪里获得戴尔 iDRAC 支持？

Dell PowerEdge R640 服务器带有 Dell iDRAC 管理界面。我们建议执行下列操作：

- 如果使用 iDRAC 管理界面，则应更改默认密码。有关 iDRAC 凭据的更多信息，请参阅Dell PowerEdge-iDRAC 的默认用户名和密码是什么？.
- 确保固件是最新的以防止安全漏洞。
- 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。

你找不到硬件设备序列号

要查找硬件设备的序列号，请转到Hardware (硬件)页面在 Storage Gateway 控制台中，如下所示。



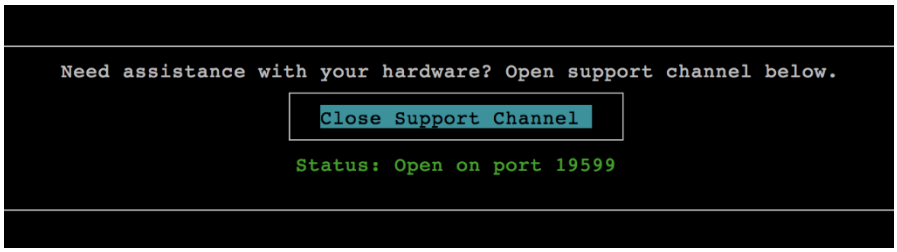
在哪里获得硬件设备支持

要联系 Storage Gateway 硬件设备支持，请参阅AWS Support.

这些区域有：AWS Support团队可能要求您激活支持渠道以远程排查您的网关问题。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。

打开支持通道AWS

1. 打开硬件控制台。
2. 选择 Open Support Channel (打开支持渠道)，如下所示。



   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。
3. 请记下端口号并将其提供给AWS Support.

排查文件网关问题

在运行 VMware vSphere 高可用性 (HA) 时，您可以使用 Amazon CloudWatch 日志组来配置文件网关。如果您执行此操作，则会收到有关文件网关的运行状况以及文件网关遇到的错误的通知。您可在 CloudWatch Logs 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

Error: InaccessibleStorageClass

你可以得到`InaccessibleStorageClass`当对象从 Amazon S3 标准存储类中移出时出现错误。

在此处，当文件网关尝试将指定的对象上传到 S3 存储桶或从 S3 存储桶读取对象时，通常会遇到错误。遇到此错误，对象通常已移至 Amazon S3 Glacier 或 S3 Glacier Deep Archive 存储类中。

解决 InaccessibleStorageClass 错误

- 将对象从 S3 Glacier 或 S3 Glacier Deep Archive 存储类移回 S3。

  如果将对象移至 S3 存储桶来纠正上传错误，则最终将上传文件。如果将对象移至 S3 存储桶来纠正读取错误，则文件网关的 SMB 或 NFS 客户端随后可以读取该文件。

Error: S3 访问被拒绝

你可以得到`S3AccessDenied`对于文件共享的 Amazon S3 存储桶访问错误AWS Identity and Access Management(IAM) 角色。在这种情况下，由指定的 S3 存储桶访问 IAM 角色。`roleArn`错误中的不允许涉及的操作。由于 Amazon S3 前缀指定的目录中的对象的权限，不允许执行此操作。

要解决 S3AccessDenied 错误

- 修改附加到的 Amazon S3 访问策略`roleArn`在文件网关运行状况日志中，以允许 Amazon S3 操作的权限。请确保访问策略允许针对导致错误的操作的权限。此外，允许针对 `prefix` 的日志中指定的目录的权限。有关 Amazon S3 权限的信息，请参阅在策略中指定权限在Amazon Simple Storage Service 用户指南。

  这些操作可能会导致出现 `S3AccessDenied` 错误。

  - `S3HeadObject`
  - `S3GetObject`
  - `S3ListObjects`
  - `S3DeleteObject`
  - `S3PutObject`

Error: InvalidObjectState

你可以得到InvalidObjectState当指定文件网关以外的写入器修改指定 S3 存储桶中的指定文件时，会出现错误。因此，文件网关文件的状态与其在 Amazon S3 中的状态不匹配。任何后续的文件上传到 Amazon S3 或从 Amazon S3 检索文件都会失败。

要解决 InvalidObjectState 错误

如果修改文件的操作为S3Upload要么S3GetObject中，执行以下操作：

1. 将文件的最新副本保存到 SMB 或 NFS 客户端的本地文件系统中 (在步骤 4 中您需要此文件副本)。如果 Amazon S3 中的该文件的版本是最新的，请下载该版本。您可以使用 AWS Management Console或 AWS CLI 执行此操作。
2. Amazon S3 用AWS Management Console要么AWS CLI.
3. 使用您的 SMB 或 NFS 客户端从文件网关中删除该文件。
4. 使用您的 SMB 或 NFS 客户端将步骤 1 中保存的该文件的最新版本复制到 Amazon S3。通过文件网关执行此操作。

Error: ObjectMissing

你可以得到ObjectMissing当指定文件网关以外的写入器从 S3 存储桶中删除指定文件时，会出现错误。任何后续的上传到 Amazon S3 或从 Amazon S3 检索对象都会失败。

要解决 ObjectMissing 错误

如果修改文件的操作为S3Upload要么S3GetObject中，执行以下操作：

1. 将文件的最新副本保存到 SMB 或 NFS 客户端的本地文件系统中 (在步骤 3 中您需要此文件副本)。
2. 使用您的 SMB 或 NFS 客户端从文件网关中删除该文件。
3. 使用您的 SMB 或 NFS 客户端复制在步骤 1 中保存的该文件的最新版本。通过文件网关执行此操作。

：Notification 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。

：Notification 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，通过 vSphere High Availability 应用程序监控进行重置会触发此事件。

当网关在此类环境中运行时，请检查是否存在 HealthCheckFailure 通知并查看 VM 的 VMware 事件日志。

：Notification HealthCheckFailure

对于 VMware vSphere HA 上的网关，当运行状况检查失败并请求重新启动 VM 时，您会收到 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。

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AWS Support.

：Notification AvailabilityMonitorTest

你会得到AvailabilityMonitorTest当你发出通知运行测试的可用性和应用监控系统在 VMware vSphere HA 平台上运行的网关上。

Error: RoleTrustRelationshipInvalid

当文件共享的 IAM 角色具有配置错误的 IAM 信任关系（即，IAM 角色不信任名为的 Storage Gateway 委托人）时，您会收到此错误。storagegateway.amazonaws.com)。因此，文件网关将无法获得凭证来在支持文件共享的 S3 存储桶上运行任何操作。

要解决 RoleTrustRelationshipInvalid 错误

- 使用 IAM 控制台或 IAM API 包含storagegateway.amazonaws.com作为受文件共享的 iAMRole 信任的委托人。有关 IAM 角色的信息，请参阅教程：委托访问权限AWS使用 IAM 角色的账户.

使用 CloudWatch 指标排除

您可以在下面找到有关将 Amazon CloudWatch 指标用于 Storage Gateway 时需执行的操作的信息。

主题

浏览目录时，网关反应缓慢

如果您在运行时，文件网关的反应较慢ls命令或浏览目录，请检查IndexFetch和IndexEviction：CloudWatch 指标：

- 如果IndexFetch运行时指标大于 0ls命令或浏览目录时，文件网关在启动时没有有关受影响的目录内容的信息，并且必须访问 Amazon S3。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，则表示您的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。如果此情况经常发生，并且对性能有影响，请联系AWS Support.

  和开发AWS Support相关 S3 存储桶的内容以及根据您的使用案例提出改进性能的建议。

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。此指标显示当存在未完成磁盘 I/O 请求时 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，可能会被缓慢的根磁盘阻塞。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指标等于或几乎与MemTotalBytes指标，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文件网关添加更多 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，您可能需要为文件网关添加更多 RAM。

您的网关向 Amazon S3 传输数据的速度较慢

如果文件网关向 Amazon S3 传输数据的速度较慢，请执行以下操作：

- 如果CachePercentDirty指标为 80 或更高，文件网关将数据写入磁盘的速度快于将数据上传到 Amazon S3 的速度。考虑增加从文件网关上载的带宽、添加一个或多个缓存磁盘或减慢客户端写入速度。
- 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。我们建议您为缓存使用本地固态驱动器 (SSD) 磁盘，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。
- 如果S3PutObjectRequestTime、S3UploadPartRequestTime，或者S3GetObjectRequestTime很高，可能存在网络瓶颈。尝试分析您的网络以验证网关是否具有预期的带宽。

您的网关执行的 Amazon S3 操作比预期的多

如果您的文件网关执行的 Amazon S3 操作比预期的多，请检查FilesRenamed指标。在 Amazon S3 中执行重命名操作非常昂贵。优化工作流程以尽量减少重命名操作的数量。

您在 Amazon S3 存储桶中看不到文件

如果您注意到网关上的文件未反映在 Amazon S3 存储桶中，请检查FilesFailingUpload指标。如果指标报告某些文件上传失败，请检查您的运行状况通知。当文件上传失败时，网关将生成包含有关该问题的更多详细信息的运行状况通知。

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，文件网关无法接受对磁盘的新写入操作，因为缓存磁盘上没有足够的可用空间。要查看您的文件网关上传到 Amazon FSx 或 Amazon S3 的速度，请查看CloudBytesUploaded指标。将该指标与WriteBytes指标，该指标显示客户端将文件写入文件

网关的速度。如果文件网关的写入速度快于上传到 Amazon FSx 或 Amazon S3 的速度，请添加更多缓存磁盘以至少覆盖备份作业的大小。或者，增加上传带宽。

- 如果备份作业失败但CachePercentDirty指标低于 80%，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` 增大此超时。运行此命令会将超时设置为 300 秒。

  对于 NFS，请确保使用硬装载而非软装载来装载客户端。

排查文件共享问题

您可以在下面找到有关您遇到文件共享意外问题时要采取的措施的信息。

主题

您的文件共享卡在创建状态

当您创建文件共享时，状态为 CREATING。创建文件共享之后，状态变为 AVAILABLE。如果文件共享陷入 CREATING 状态，请执行以下操作：

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 确保文件共享映射的 S3 存储桶存在。如果此存储桶不存在，则创建存储桶。创建存储桶之后，文件共享状态变为 AVAILABLE。有关如何创建 S3 存储桶的信息，请参阅创建存储桶中的Amazon Simple Storage Service 用户指南.

3. 确保您的存储桶名称符合 Amazon S3 中的存储桶命名规则。有关更多信息，请参阅 Amazon Simple Storage Service 用户指南中的存储桶命名规则。
4. 确保用于访问 S3 存储桶的 IAM 角色具有正确的权限，并验证 S3 存储桶是否在 IAM 策略中被列为资源。有关更多信息，请参阅授予对 Amazon S3 存储桶的访问权限。

您无法创建文件共享

1. 如果由于文件共享陷入 CREATING 状态而无法创建文件共享，请验证文件共享映射的 S3 存储桶是否存在。有关如何执行此操作的信息，请参阅上述的 您的文件共享卡在创建状态。
2. 如果 S3 存储桶存在，请验证AWS Security Token Service在创建文件共享的区域中启用。如果安全令牌未启用，则应启用安全令牌。有关如何使用以下方式启用令牌的信息。AWS Security Token Service，请参阅激活和停用AWS在 STSAWS区域中的IAM 用户指南.

SMB 文件共享不允许多种不同的访问方法。

SMB 文件共享具有以下限制：

1. 当同一客户端尝试安装 Active Directory 和来宾访问 SMB 文件共享时，将显示以下错误消息：`Multiple connections to a server or shared resource by the same user, using more than one user name, are not allowed. Disconnect all previous connections to the server or shared resource and try again.`
2. 一个 Windows 用户不能保持与两个来宾访问 SMB 文件共享的连接，并且在新的来宾访问连接建立后可能会断开连接。
3. Windows 客户端无法同时安装由同一网关导出的来宾访问和 Active Directory SMB 文件共享。

多个文件共享无法写入映射的 S3 存储桶

我们不建议将 S3 存储桶配置为允许多个文件共享写入到一个 S3 存储桶。此方法可能导致无法预测的结果。

相反，我们建议您只允许一个文件共享写入到每个 S3 存储桶。您可以创建存储桶策略，仅允许与文件共享相关联的角色写入到存储桶。有关更多信息，请参阅文件共享最佳实践。

无法将文件上传到 S3 存储桶

如果无法将文件上传到 S3 存储桶，请执行以下操作：

1. 确保您已为 Amazon S3 文件网关授予必要的访问权限，以将文件上传到 S3 存储桶。有关更多信息，请参阅授予对 Amazon S3 存储桶的访问权限。
2. 确保创建存储桶的角色有权写入到 S3 存储桶。有关更多信息，请参阅文件共享最佳实践。
3. 如果您的文件网关使用 SSE-KMS 进行加密，请确保与文件共享关联的 IAM 角色包括kms:Encrypt、kms:Decrypt、KMS：重新加密、kms:GenerateDataKey, 和kms:DescribeKey权限。有关更多信息，请参阅 。为 Storage Gateway 使用基于身份的策略（IAM 策略）.

无法更改默认加密以使用 SSE-KMS 加密存储在我的 S3 存储桶中存储的对象

如果更改默认加密并使用 SSE-KMS (服务器端加密)AWS KMS— 托管密钥）S3 存储桶的默认值，Amazon S3 文件网关存储在存储桶中存储的对象不会使用 SSE-KMS 加密。默认情况下，S3 文件网关在将数据写入 S3 存储桶时会使用 Amazon S3 (SSE-S3) 托管的服务器端加密。更改默认值不会自动更改您的加密。

要将加密更改为将 SSE-KMS 与您自己的 AWS KMS 密钥结合使用，则必须启用 SSE-KMS 加密。为此，您需要在创建文件共享时提供 KMS 密钥的 Amazon 资源名称 (ARN)。您也可以通过使用 `UpdateNFSFileShare` 或 `UpdateSMBFileShare` API 操作来更新文件共享的 KMS 设置。更新后，此更新应用于存储在 S3 存储桶中的对象。有关更多信息，请参阅使用数据加密AWS KMS。

在启用对象版本控制的 S3 存储桶中直接进行的更改可能会影响您在文件共享中看到的内容

如果 S3 存储桶具有由其他客户端写入它的对象，则由于 S3 存储桶对象版本控制，S3 存储桶的视图可能不是最新的。您应始终先刷新缓存，然后再查看感兴趣的文件。

对象版本控制 是一项可选的 S3 存储桶功能，通过存储同名对象的多个副本来帮助保护数据。例如，每个副本都有单独的 ID 值，`file1.jpg：ID="xxx"`和`file1.jpg：ID="yyy"`. 同名对象数及其生命周期由 Amazon S3 生命周期策略控制。有关 Amazon S3 概念的更多详细信息，请参阅使用版本控制和对象生命周期管理中的Amazon S3 开发人员指南。

在删除受版本控制的对象时，会使用删除标记来标记该对象，但保留该对象。只有 S3 存储桶拥有者才能永久删除启用了版本控制的对象。

在 S3 File Gateway 中，所显示的文件是获取对象或刷新缓存时 S3 存储桶中的对象的最新版本。S3 文件网关会忽略任何较旧版本或标记为删除的任何对象。在读取文件时，您从最新版本读取数据。在您编写文件共享中的文件时，S3 File Gateway 将创建具有您所做更改的命名对象的新版本，并且该版本将成为最新版本。

如果新版本添加到了您的应用程序之外的 S3 存储桶中，则您的 S3 文件网关将继续从较早版本读取，并且您所做的更新将基于较早版本。要读取对象的最新版本，请使用 RefreshCache API 操作或从控制台刷新，如刷新您的 Amazon S3 存储桶中的对象中所述。

> **Important**
>
> 我们不建议对象或文件从文件共享之外写入 S3 File Gateway S3 存储桶中。

当写入启用对象版本控制的 S3 存储桶时，Amazon S3 文件网关可能会创建一个 S3 对象的多个版本

启用对象版本控制后，您可能会在每次从 NFS 或 SMB 客户端更新文件时在 Amazon S3 中创建对象的多个版本。以下是可能导致 S3 存储桶中创建对象的多个版本的情况：

- 当文件上传到 Amazon S3 后，NFS 或 SMB 客户端在 Amazon S3 文件网关中进行修改时，S3 文件网关会上传新的或修改的数据，而不是上传整个文件。修改文件会导致创建新版本的 Amazon S3 对象。
- 当 NFS 或 SMB 客户端将文件写入 S3 文件网关时，S3 文件网关会将文件的数据上传到 Amazon S3，然后是其元数据（所有权、时间戳等）。上传文件数据将创建 Amazon S3 对象，上传文件的元数据将更新 Amazon S3 对象的元数据。此过程将创建对象的另一个版本，从而生成对象的两个版本。
- S3 File Gateway 上传较大的文件时，可能需要在客户端完成写入文件网关之前上传较小的文件块。造成这种情况的一些原因包括释放缓存空间或高写入文件的速率。这可能会导致 S3 存储桶中的对象的多个版本。

在设置生命周期策略将对象移动到不同的存储类之前，您应监控 S3 存储桶以确定存在多少版本的对象。您应该为之前的版本配置生命周期过期，以尽量减少 S3 存储桶中对象的版本数。在 S3 存储桶之间使用同区复制 (SRR) 或跨区域复制 (CRR) 将增加使用的存储空间。有关复制的更多信息，请参阅复制.

> **Important**
>
> 在您了解启用对象版本控制时使用了多少存储空间之前，不要配置 S3 存储桶之间的复制。

使用受版本控制的 S3 存储桶会大大增加 Amazon S3 中的存储量，因为对文件进行的每个修改都会创建 S3 对象的新版本。默认情况下，Amazon S3 将继续存储所有这些版本，除非您专门创建策略来覆盖此行为并限制保留的版本数。如果您注意到启用对象版本控制后存储使用量异常大，请检查您是否正确设置了存储策略。浏览器请求的 HTTP 503-slow down 响应数的增加也可能是由于对象版本控制问题。

如果您在安装 S3 文件网关后启用了对象版本控制，则将保留所有唯一对象 (ID="NULL") 您可以在文件系统中看到它们。将为对象的新版本分配唯一 ID (保留较旧版本) 。基于对象的时间戳，仅最新版本的对象可在 NFS 文件系统中查看。

在您启用对象版本控制后，您的 S3 存储桶将无法返回到不受版本控制的状态。但是，您可以暂停版本控制。在暂停版本控制时，会为新对象分配一个 ID。如果存在具有 ID="NULL" 值的同名对象，则将覆盖较旧版本。但是，将保留包含非 NULL ID 的任何版本。时间戳将新对象标识为最新对象，并且这是显示在 NFS 文件系统中的对象。

对 S3 存储桶的更改不会反映在 Storage Gateway 中

当您使用文件共享本地将文件写入缓存时，Storage Gateway 会自动更新文件共享缓存。但是，当您将文件直接上传到 Amazon S3 时，Storage Gateway 不会自动更新缓存。当您执行此操作时，您必须执行RefreshCache操作以查看文件共享的更改。如果您有多个文件共享，那么您必须运行RefreshCache对每个文件共享进行操作。

您可以使用 Storage Gateway 控制台和AWS Command Line Interface(AWS CLI):

- 要使用 Storage Gateway 控制台刷新缓存，请参阅刷新 Amazon S3 存储桶中的对象。
- 使用刷新缓存AWS CLI：
  1. 运行命令aws storagegateway list-file-shares
  2. 将文件共享的 Amazon 资源编号 (ARN) 复制到您要刷新的缓存中。
  3. 运行refresh-cache以您的 ARN 作为值的命令--file-share-arn：

     ```
     aws storagegateway refresh-cache --file-share-arn
     arn:aws:storagegateway:eu-west-1:12345678910:share/share-FFDEE12
     ```

要自动化RefreshCache操作，请参阅如何在 Storage Gateway 上自动执行 ReRefreshCache 操作？

ACL 权限不符合预期

如果访问控制列表 (ACL) 权限未按预期与 SMB 文件共享一起运行，则您可以执行测试。

为此，请首先测试 Microsoft Windows 文件服务器或本地 Windows 文件共享上的权限。然后，将行为与您网关的文件共享进行比较。

执行递归操作后，网关性能下降

在某些情况下，您可能会执行递归操作（例如重命名目录或启用 ACL 的继承），并强制沿树向下执行递归操作。如果您执行此操作，S3 文件网关会递归地将该操作应用于文件共享中的所有对象。

例如，假设您将继承应用于 S3 存储桶中的现有对象。您的 S3 文件网关以递归方式将继承应用于存储桶中的所有对象。此类操作可能会导致网关性能下降。

高可用性运行状况通知

在 VMware vSphere High Availability (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，请参阅排查高可用性问题。

排查高可用性问题

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 Health：
- 指标

运行 Health：

在 VMware vSphere HA 上运行网关时，所有网关都会向配置的 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

- ：Notification 重启
- ：Notification HardReboot
- ：Notification HealthCheckFailure
- ：Notification AvailabilityMonitorTest

：Notification 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。

：Notification 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，通过 vSphere High Availability 应用程序监控进行重置会触发此事件。

措施

当网关在此类环境中运行时，请检查是否存在 `HealthCheckFailure` 通知并查看 VM 的 VMware 事件日志。

：Notification HealthCheckFailure

对于 VMware vSphere HA 上的网关，当运行状况检查失败并请求重新启动 VM 时，您会收到 `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AWS Support.

：Notification AvailabilityMonitorTest

对于 VMware vSphere HA 上的网关，您可以获得`AvailabilityMonitorTest`当你发出通知运行测试的可用性和应用监控VMware 中的系统。

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，请咨询配置的 CloudWatch 日志组。

恢复数据的最佳实践

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 Amazon 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。

主题

从意外的虚拟机关闭中恢复

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。
- 如果您的网关发生故障并且您的卷或磁带因意外关闭而出现问题，您可以恢复您的数据。有关如何恢复数据的信息，请参阅以下适用于您的情况的内容。

从发生故障的缓存磁盘中恢复数据

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。
- 如果缓存磁盘受损或无法访问，则关闭网关，重置缓存磁盘，重新为缓存存储配置磁盘，然后重新启动网关。

有关详细信息，请参阅从发生故障的缓存磁盘中恢复数据。

从不可访问的数据中心中恢复数据

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。

从不可访问的数据中心内的文件网关恢复数据

对于文件网关，可将新文件共享映射到包含您要恢复的数据的 Amazon S3 存储桶。

1. 在 Amazon EC2 主机上创建并激活新的文件网关。有关更多信息，请参阅在 Amazon EC2 主机上部署文件网关。
2. 在您创建的 EC2 网关上创建一个新的文件共享。有关更多信息，请参阅 。创建文件共享.
3. 将文件共享装载到您的客户端上并将其映射到包含您要恢复的数据的 S3 存储桶。有关更多信息，请参阅 。装载和使用文件共享.

其他 Storage Gateway 资源

在本节中，您可以找到有关的信息AWS以及可帮助您设置或管理网关的第三方软件、工具和资源，以及有关 Storage Gateway 配额的信息。

主题

主机设置

主题

为 Storage Gateway 配置 VMware

在为 Storage Gateway 配置 VMware 时，应确保将 VM 时间与主机时间同步，将 VM 配置为在预配置存储时使用半虚拟化磁盘控制器，并在支持网关 VM 的基础设施层提供故障保护措施。

主题

- 将 Storage Gateway 与 VMware 高可用性配合使

将 VM 时间与主机时间同步

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。

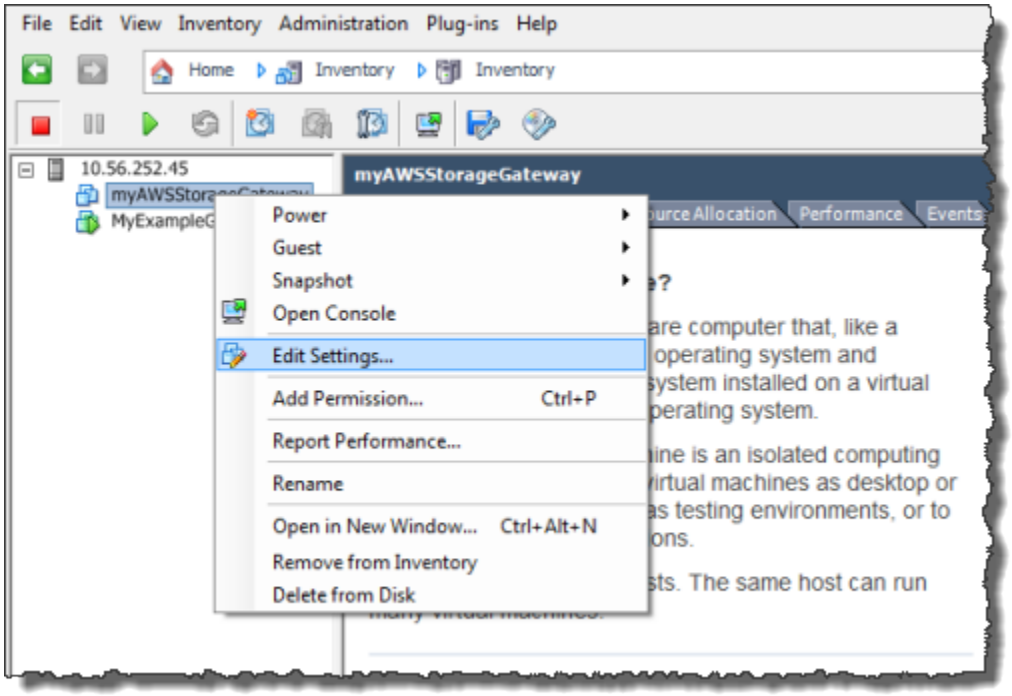
> **Important**
>
> 要成功激活网关，就需要同步 VM 时间和主机时间。

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，打开网关 VM 的上下文 (右键单击) 菜单，然后选择 Edit Settings。

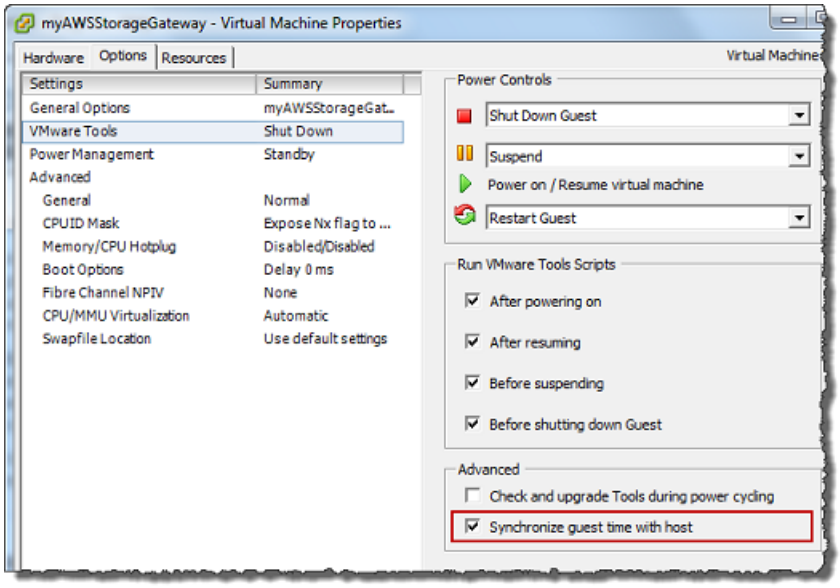
   “Virtual Machine Properties”对话框打开。



   b. 选择 Options 选项卡，然后选择选项列表中的 VMware Tools。

   c. 选中 Synchronize guest time with host 选项，然后选择 OK。

VM 时间与主机进行同步。



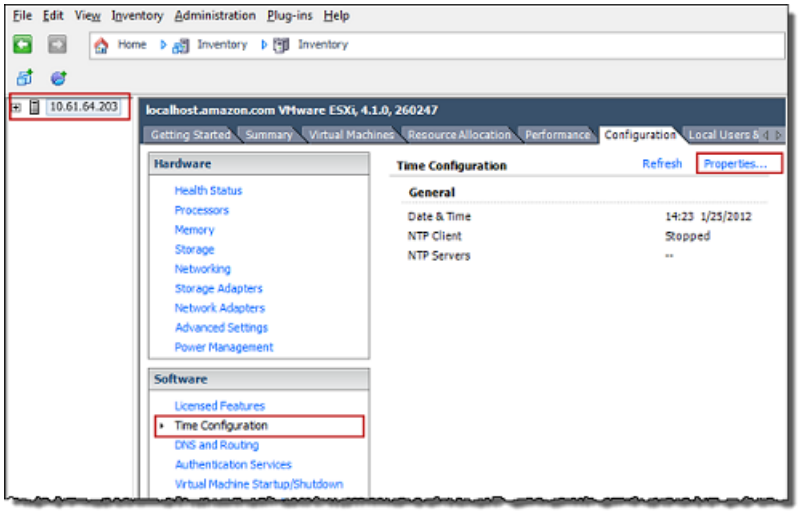
2. 配置主机时间。

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。

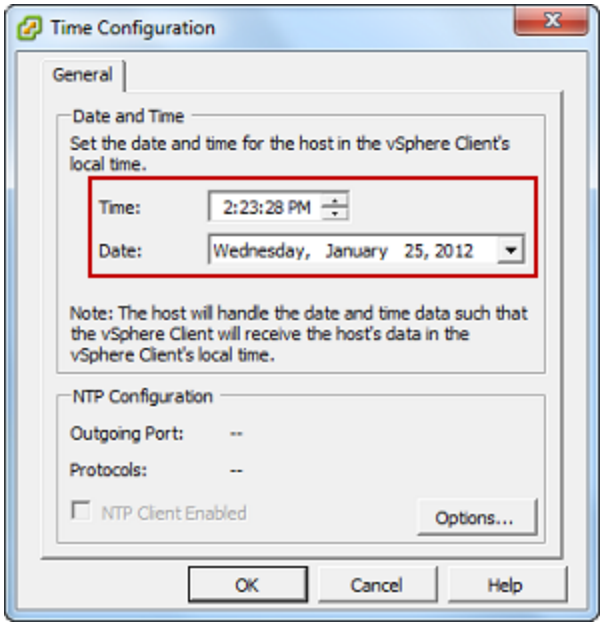
a. 在 VMware vSphere 客户端中，选择左侧窗格中的 vSphere 主机节点，然后选择 Configuration 选项卡。

b. Select时间配置中的软件面板，然后选择属性链接。

“Time Configuration”对话框显示。

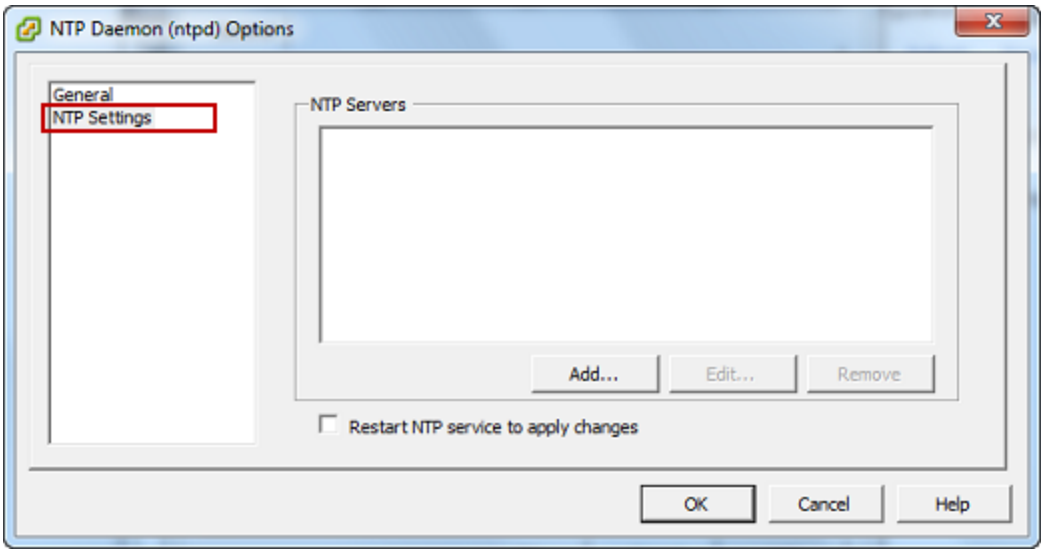


c. 在 Date and Time (日期和时间) 面板中，设置日期和时间。



d. 将主机配置为自动将其时间与 NTP 服务器同步。

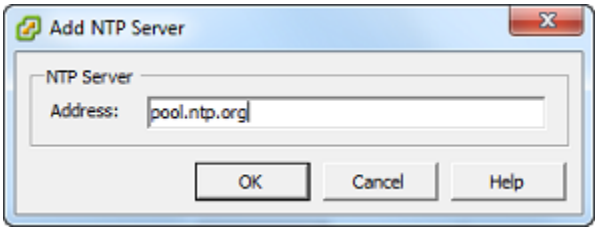
i. 选择选项中的时间配置对话框，然后在NTP 守护程序 (ntpd) 选项对话框中，选择NTP 设置在左侧窗格中。



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。

您可使用 `pool.ntp.org`，如以下示例所示。



iv. 在 NTP Daemon (ntpd) Options 对话框中的左侧窗格中选择 General。

v. 在 Service Commands 窗格中，选择 Start 以启动服务。

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。

将 Storage Gateway 与 VMware 高可用性配合使

VMware High Availability (HA) 是一种 vSphere 组件，可以在支持网关 VM 的基础设施层提供故障防护。VMware HA 做到这点的机制是：使用配置为群集的多个主机，这样，当运行网关 VM 的一个主机发生故障时，网关 VM 会在群集内的另一个主机上自动重新启动。有关 VMware HA 的更多信息，请参阅VMware HA：概念和最佳实践在 VMware 网站上。

要将 Storage Gateway 与 VMware HA 结合使用，建议执行下列操作：

- 部署 VMware ESX.ova仅在集群中的一台主机上包含 Storage Gateway VM 的可下载程序包。

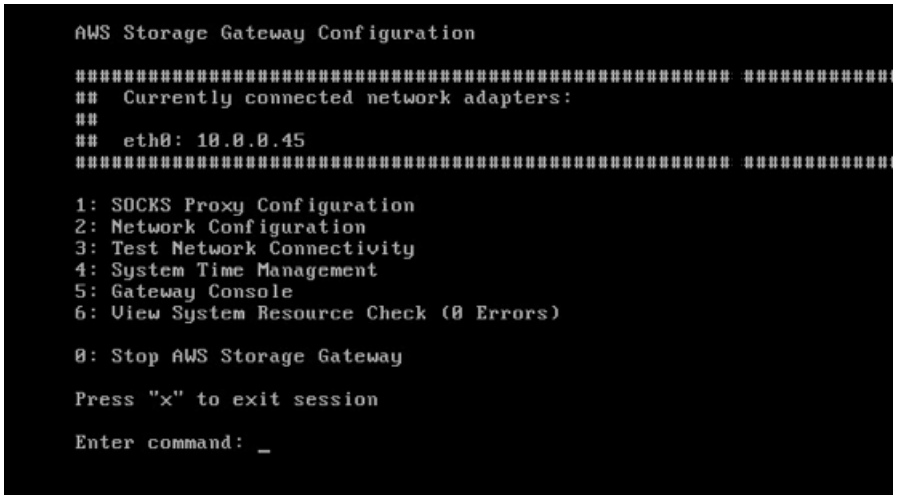
- 在部署 .ova 程序包时，选择一个不在主机本地的数据存储。而是使用一个可供群集的所有主机访问的数据存储。如果您选择的是主机本地数据存储，而主机发生了故障，则群集中的其他主机可能无法访问该数据源，并且可能无法成功地故障转移到另一台主机。
- 利用群集化，如果您将 .ova 程序包部署到群集，请在系统提示您这样做时选择一台主机。或者您也可以直接部署到群集中的主机里。

同步您的网关 VM 时间

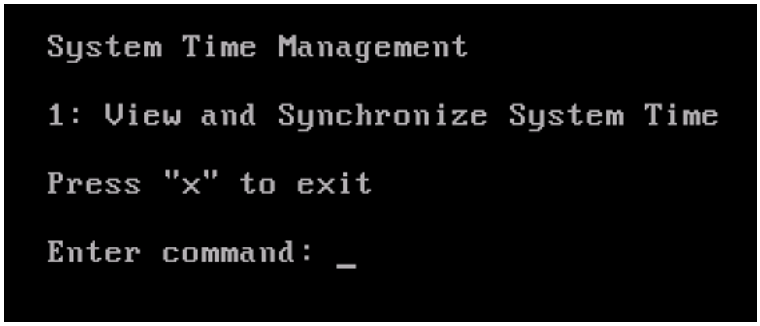
对于 VMware ESXi 上部署的网关，设置管理程序主机时间并将 VM 时间与主机同步，就足以避免时间偏差。有关更多信息，请参阅将 VM 时间与主机时间同步。对于 Microsoft Hyper-V 上部署的网关，您应该定期使用下面介绍的步骤查看 VM 的时间。

查看管理程序网关 VM 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 VMware ESXi 本地控制台的更多信息，请参阅使用 VMware ESXi 访问网关本地控制台。
   - 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. 在存储库的Storage Gateway 配置输入主菜单**4**为了系统时间管理.



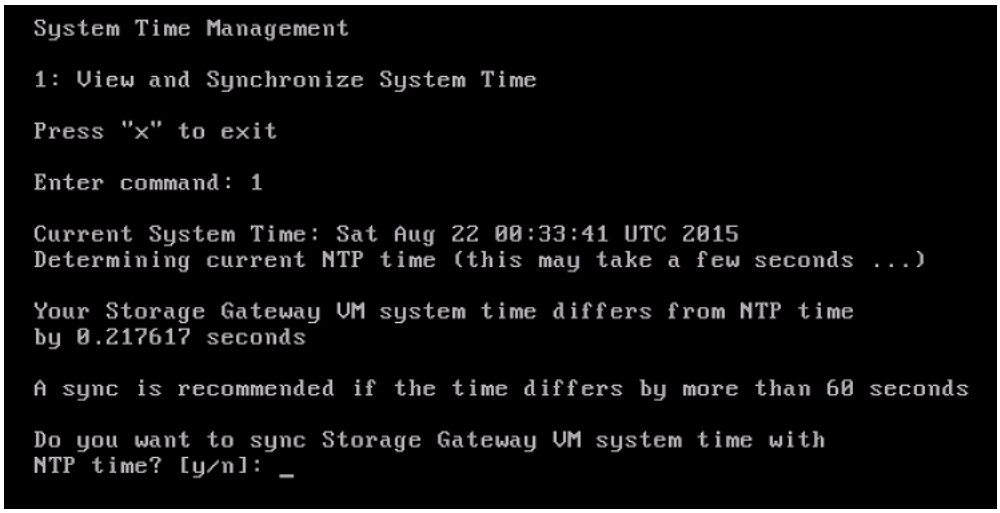
3. 在存储库的系统时间管理菜单中，输入**1**为了查看和同步系统时间.



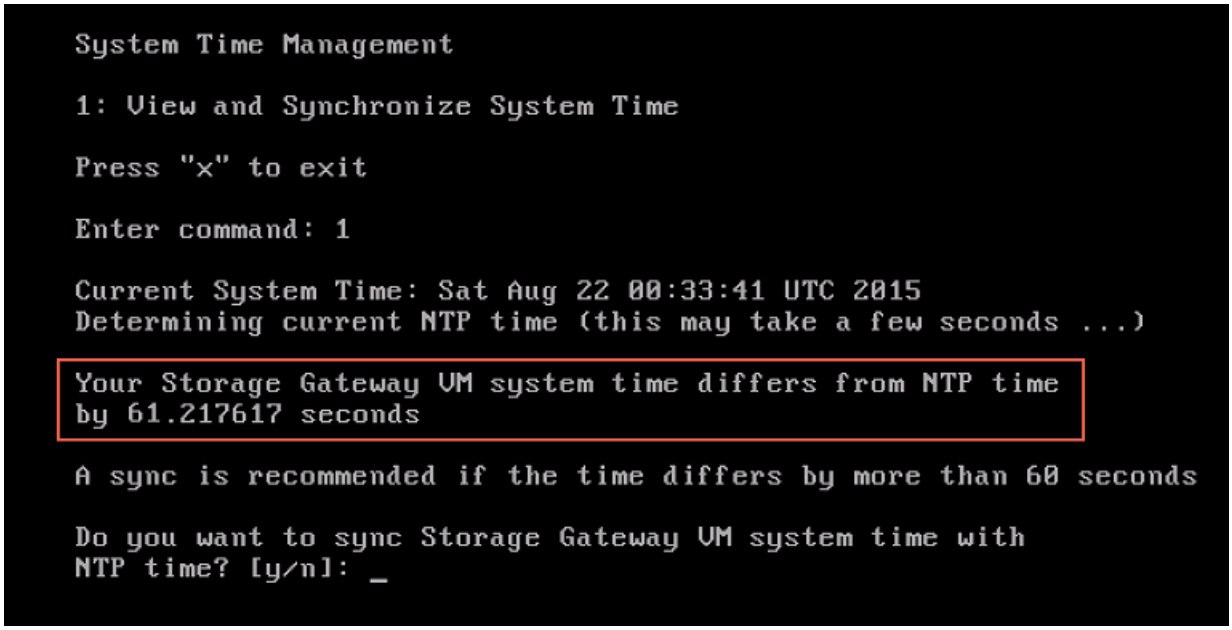
4. 如果结果指示您应该将 VM 的时间与 NTP 时间同步，请输入 **y**。否则，请输入 **n**。

   如果输入 **y** 进行同步，则同步可能需要消耗一段时间。

   以下屏幕截图显示了不需要进行时间同步的 VM。



   以下屏幕截图显示了需要进行时间同步的 VM。



在 Amazon EC2 主机上部署文件网关

您可以在 Amazon Elastic Compute Cloud (Amazon EC2) 实例上部署和激活文件网关。文件网关 Amazon 系统映像 (AMI) 以社区 AMI 形式提供。

在 Amazon EC2 实例上部署网关

1. 在选择主机平台页面上，选择 Amazon EC2。
2. 选择 Launch instance (启动实例) 启动存储网关 EC2 AMI。您将会重定向到可在其中选择实例类型的 Amazon EC2 控制台。
3. 在存储库的步骤 2: 选择一个实例类型页面上，选择您的实例的硬件配置。在满足特定最低要求的实例类型上支持 Storage Gateway。我们建议您首先使用 m4.xlarge 实例类型，它满足网关正常运行所需的最低要求。有关更多信息，请参阅本地 VM 的硬件要求。

   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 。调整实例大小中的适用于 Linux 实例的 Amazon EC2 用户指南.

   > **Note**
   >
   > 某些实例类型，尤其是 i3 EC2，使用的是 NVMe SSD 磁盘。这些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，并且仅在该参数为时才启动或停止系统。`0`. 要了解有关监控网关指标的更多信息，请参阅Storage Gateway 指标和维度在

CloudWatch 文档中。有关 Amazon EC2 实例类型要求的更多信息，请参阅。the section called “Amazon EC2 实例类型要求”.

4. 选择 Next:。配置实例详细信息.
5. 在存储库的步骤 3: 配置实例详细信息页面上，选择的值自动分配公有 IP. 如果您的实例应可从公共 Internet 进行访问，请验证 Auto-assign Public IP (自动分配公有 IP) 是否已设置为 Enable (启用)。如果您的实例不应可从 Internet 访问，请为 Auto-assign Public IP (自动分配公有 IP) 选择 Disable (禁用)。
6. 适用于IAM 角色，选择AWS Identity and Access Management您希望为网关使用的 (IAM) 角色。
7. 选择 Next:。添加存储.
8. 在存储库的步骤 4: 添加存储页面上，选择添加新卷将存储添加到文件网关实例。您至少需要为缓存存储配置一个 Amazon EBS 卷。

   推荐的磁盘大小：缓存（最小值）150 GiB 和缓存（最大值）64 TiB
9. 在存储库的第 5 步：添加标签页面上，您可以向实例添加可选标签。接下来，选择 Next (下一步)：配置安全组.
10. 在存储库的步骤 6：配置安全组页面上，向传输到实例的特定流量添加防火墙规则。您可以创建新安全组或者选择现有安全组。

    Important

    除了 Storage Gateway 激活和安全外壳 (SSH) 访问端口，NFS 客户端还需要访问其他端口。有关详细信息，请参阅网络和防火墙要求。
11. 选择 Review and Launch (查看和启动) 查看您的配置。
12. 在存储库的步骤 7：核查实例启动页面上，选择启动.
13. 在 Select an existing key pair or create a new key pair (选择现有密钥对或创建新密钥对) 对话框中，选择 Choose an existing key pair (选择现有密钥对)，然后选择您在开始设置时创建的密钥对。准备好后，选择确认框，然后选择 Launch Instances (启动实例)。

    这将显示一个确认页，告知您实例正在启动。
14. 选择 View Instances 以关闭确认页面并返回控制台。在 Instances (实例) 屏幕上，您可以查看您实例的状态。启动实例只需很短的时间。当您启动实例时，其初始状态为 pending (待处理)。实例启动后，其状态变为 running (正在运行)，并且会收到一个公有 DNS 名称。
15. 在中选择您的实例，记下中的公有 IP 地址说明标签，然后返回连接到AWS页面中的 Storage Gateway 控制台以继续您的网关设置。

您可以使用 Storage Gateway 控制台或通过查询AWS Systems Manager参数存储区。

确定 AMI ID

1. 登录到AWS Management Console然后打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
2. 依次选择 Create gateway (创建网关)、File gateway (文件网关) 和 Next (下一步)。
3. 在 Choose host platform (选择主机平台) 页面上，选择 Amazon EC2。
4. 选择启动实例启动 Storage Gateway EC2 AMI。您将被重定向到 EC2 社区 AMI 页面，在此页面上，您可以在其中看到适用于您的 AMI ID。AWSURL 中的区域。

   或者，您可以查询 Systems Manager 参数存储。您可以使用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_S3/latest`. 例如，使用以下 CLI 命令返回当前 AMI 在当前 AMI 的 ID。AWS区域。

   ```
   aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/
   FILE_S3/latest
   ```

   该 CLI 命令会返回类似以下内容的输出：

   ```
   {
       "Parameter": {
           "Type": "String",
           "LastModifiedDate": 1561054105.083,
           "Version": 4,
           "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/
   FILE_S3/latest",
           "Name": "/aws/service/storagegateway/ami/FILE_S3/latest",
           "Value": "ami-123c45dd67d891000"
       }
   }
   ```

获取网关的激活密钥

要获取网关的激活密钥，需要向网关 VM 发出一个 Web 请求，它会返回一个包含激活密钥的重定向。此激活密钥作为一个参数传递到 `ActivateGateway` API 操作以指定网关的配置。有关更多信息，请参阅 。ActivateGateway中的Storage Gateway API 参考.

您向网关 VM 发出的请求包含AWS激活发生的区域。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*。

主题

- AWS CLI
- Linux (bash/zsh)
- Microsoft Windows PowerShell

AWS CLI

如果您尚未安装和配置 AWS CLI，则必须先执行此操作。为此，请按照 AWS Command Line Interface 用户指南中的这些指示操作：

- 安装AWS Command Line Interface
- 配置AWS Command Line Interface

以下示例说明了如何使用AWS CLI要获取 HTTP 响应，请分析 HTTP 标头并获取激活密钥。

```
wget 'ec2_instance_ip_address/?activationRegion=eu-west-2' 2>&1 | \
grep -i location | \
grep -i key | \
cut -d'=' -f2 |\
cut -d'&' -f1
```

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 "$activation_region" ]]; then
    echo "Usage: get-activation-key ip_address activation_region"
    return 1
  fi
  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region"); then
```

```
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
    echo "$activation_key_param" | cut -f2 -d=
  else
    return 1
  fi
}
```

Microsoft Windows PowerShell

以下示例显示如何使用 Microsoft Windows PowerShell 获取 HTTP 响应、分析 HTTP 标头以及获取激活密钥。

```
function Get-ActivationKey {
  [CmdletBinding()]
  Param(
    [parameter(Mandatory=$true)][string]$IpAddress,
    [parameter(Mandatory=$true)][string]$ActivationRegion
  )
  PROCESS {
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion" -MaximumRedirection 0 -ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

使用AWS Direct Connect使用 Storage Gateway

AWS Direct Connect会将您的内部网络链接到 Amazon Web Services Cloud。使用AWS Direct Connect通过 Storage Gateway，您可以针对高吞吐量工作负载需求创建一个连接，从而提供本地网关与AWS.

Storage Gateway 使用了公用终端节点 有了AWS Direct Connect建立连接后，您可以创建一个公共虚拟接口来将流量路由到 Storage Gateway 终端节点。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 服务公共终端节点可以位于同一个AWS区域作为AWS Direct Connect 位置，或者可以在不同的地方AWS区域。

下图显示了一个示例，说明了如何AWS Direct Connect与 Storage Gateway 配合使用。

以下过程假定您已创建正常运行的网关。

使用AWS Direct Connect使用 Storage Gateway

1. 创建并建立AWS Direct Connect您的本地数据中心和 Storage Gateway 终端节点之间的连接 有关如何创建连接的更多信息，请参阅。入门AWS Direct Connect中的AWS Direct Connect用户指南。
2. 将您的本地 Storage Gateway 设备 Connect 到AWS 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 。创建虚拟接口中的AWS Direct Connect用户指南。

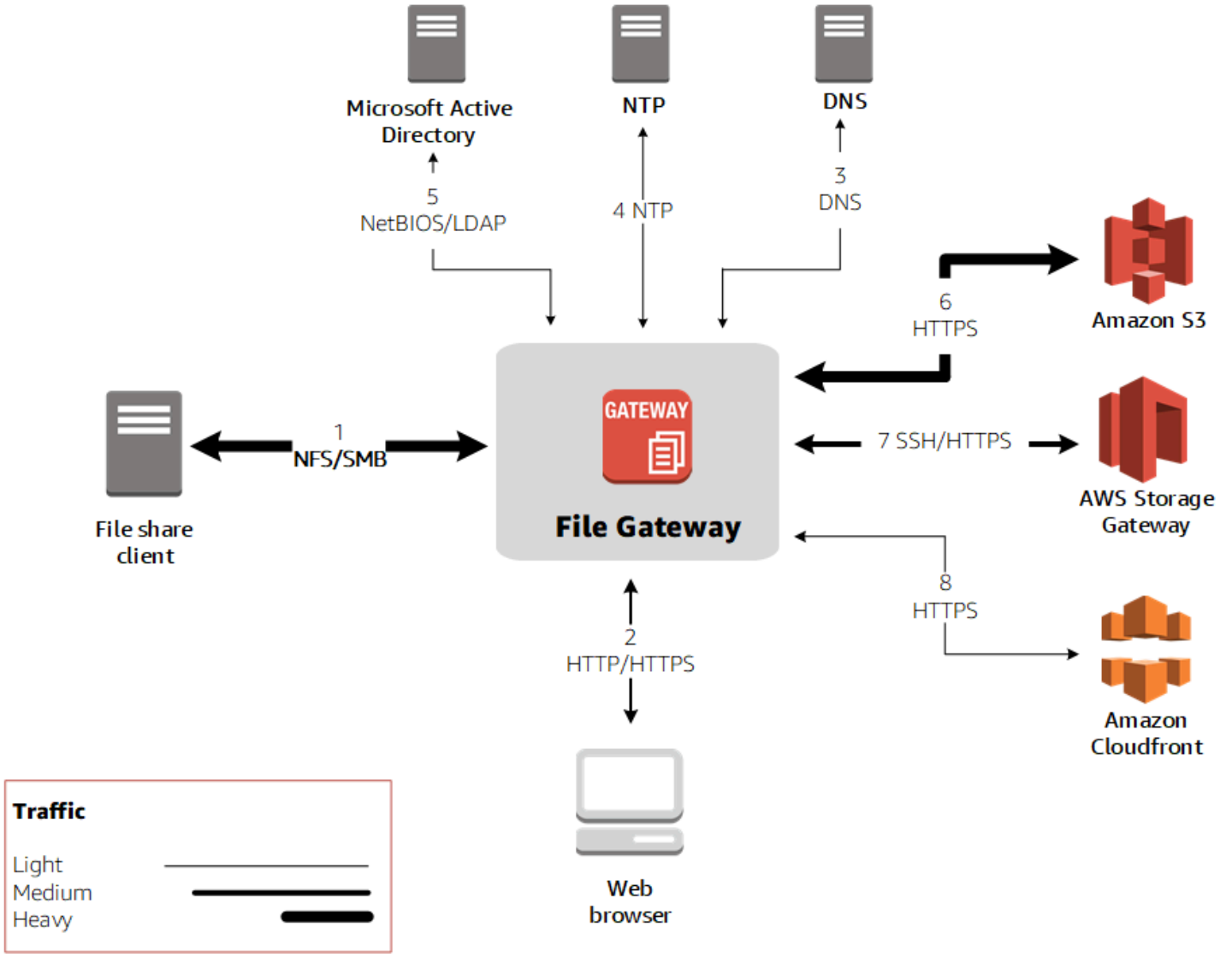
有关详细信息AWS Direct Connect请参阅是什么AWS Direct Connect?中的AWS Direct Connect用户指南.

端口要求

Storage Gateway 需要使用以下端口才能正常运行。部分端口是所有网关类型的通用端口，是所有网关类型所需要的。其他端口则是特定网关类型所需要的。在本节中，您可以查找所需端口的示意图以及每种网关类型所需的端口的列表。

文件网关

下图显示了要为文件网关操作开放的端口。



下列端口是所有网关类型的通用端口，是所有网关类型所需要的。

From	To	协议	端口	如何使用	
Storage Gateway VM	Amazon Web Services	传输控制协议 (TCP)	443 (HTTPS)	适用于从 Storage Gateway VM 到AWS服务终端节点。有关服务终端节点的信息，请参阅允许通	

From	To	协议	端口	如何使用	
				过防火墙和路由器进行 AWS Storage Gateway 访问。	
您的 Web 浏览器	Storage Gateway VM	TCP	80 (HTTP)	由本地系统用于获取 Storage Gateway 激活密钥。端口 80 仅在激活 Storage Gateway 设备期间使用。 Storage Gateway 虚拟机不要求可公开访问端口 80。所需的端口 80 访问级别取决于网络配置。如果从 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。	

From	To	协议	端口	如何使用	
Storage Gateway VM	域名服务 (DNS) 服务器	用户数据报协议 (UDP)/ UDP	53 (DNS)	用于在 Storage Gateway VM 和 DNS 服务器之间进行通信。	
Storage Gateway VM	Amazon Web Services	TCP	22 (支持渠道)	允许 Amazon Web Services Services Services Support 访问您的网关，以帮助您排网关问题。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。	

From	To	协议	端口	如何使用	
Storage Gateway VM	网络时间协议 (NTP) 服务器	UDP	123 (NTP)	由本地系统使用以将 VM 时间同步到主机时间。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	
存储网关硬件设备	超文本传输协议 (HTTP) 代理	TCP	8080 (HTTP)	在激活时暂时需要。	

下表列出了必须为使用网络文件系统 (NFS) 或服务器消息块 (SMB) 协议的文件网关开放的必需端口。这些端口规则是安全组定义的一部分。

Ru	网络元素	文件共享类型	协议	端口	入站	出站	必填？	备注
1	文件共享客户端	NFS	TCP/UDP 数据	111	✓	✓	✓	文件共享数据传输（仅针对 NFS）
			TCP/UDP NFS	2049	✓	✓	✓	文件共享数据传输（仅针对 NFS）
			TCP/UDP NFSv3	2004	✓	✓	✓	文件共享数据传输（仅针对 NFS）
		SMB	TCP/UDP SMBv2	139	✓	✓	✓	文件共享数据传输会话服务（仅针对 SMB）；取代了 Microsoft Windows NT 及更高版本的端口 137—139
			TCP/UDP SMBv3	445	✓	✓	✓	文件共享数据传输会话服务（仅针对 SMB）；取代了 Microsoft Windows NT 及更高版本的端口 137—139
2	Web 浏览器	NFS 和 SMB	TCP HTTP	80	✓	✓	✓	Amazon Web Services 管理控制台（仅限激活）
			TCP HTTPS	443	✓	✓	✓	Amazon Web Services 管理控制台（所有其他操作）
3	DNS	NFS 和 SMB	TCP/UDP DNS	53	✓	✓	✓	IP 名称解析

Ru	网络元素	文件共享类型	协议	端口	入站	出站	必填？	备注
4	NTP	NFS 和 SMB	UDP NTP	123	✓	✓	✓	时间同步服务
5	Microsoft Active Directory	SMB	UDP NetBIOS	137	✓	✓	✓	名称服务（不用于 NFS）
			UDP NetBIOS	138	✓	✓	✓	数据报服务
			TCP LDAP	389	✓	✓		目录系统代理 (DSA)；客户端连接
			TCP LDAPS	636	✓	✓		LDAP — 基于安全套接字层 (SSL) 的轻量目录访问协议 (LDAP)。
6	Amazon S3	NFS 和 SMB	HTTPS 数据	443	✓	✓	✓	存储数据传输
7	Storage Gateway	NFS 和 SMB	TCP SSH	22	✓	✓	✓	支持渠道
			TCP HTTPS	443	✓	✓	✓	管理控制台
8	Amazon CloudFront	NFS 和 SMB	TCP HTTPS	443	✓	✓	✓	用于激活

连接到网关

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，您还可以从 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 主机：使用 VMware ESXi 访问网关本地控制台
- 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 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 。

您还可以从 Amazon EC2 管理控制台获取该 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。

过程 1：使用公有 IP 地址连接到网关

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 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 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。

过程 2：使用弹性 IP 地址连接到网关

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 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 Storage Gateway 控制台并键入该弹性 IP 地址。
4. 激活网关之后，选择刚刚激活的网关，然后选择底部面板中的 VTL devices (VTL 设备) 选项卡。
5. 获取您的所有 VTL 设备的名称。

6. 对于每个目标，运行以下命令以配置目标。

```
iscsiadm -m node -o new -T [$TARGET_NAME] -p [$Elastic_IP]:3260
```

7. 对于每个目标，运行以下命令以登录。

```
iscsiadm -m node -p [$ELASTIC_IP]:3260 --login
```

您的网关现已使用 EC2 实例的弹性 IP 地址连接。

了解 Storage Gateway 资源和资源 ID

在 Storage Gateway 中，主要资源为网关但是其他资源类型包括：卷、虚拟磁带、iSCSI 目标, 和vtl 设备. 这些称为子资源，除非它们与网关关联，否则视为不存在。

这些资源和子资源具有与其关联的唯一 Amazon Resource Name (ARN)，如下表所示。

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*
卷 ARN	arn:aws:storagegateway: *region*:*account-id* :gateway/ *gateway-id* /volume/*volume-id*
磁带 ARN	arn:aws:storagegateway: *region*:*account-id* :tape/*tapebarcode*
目标 ARN (iSCSI 目标)	arn:aws:storagegateway: *region*:*account-id* :gateway/ *gateway-id* /target/*iSCSItarget*
VTL 设备 ARN	arn:aws:storagegateway: *region*:*account-id* :gateway/ *gateway-id* /device/*vtldevice*

Storage Gateway 还支持使用 EC2 实例以及 EBS 卷和快照。这些资源是 Storage Gateway 中使用的 Amazon EC2 资源。

使用资源 ID

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。卷 ID 的格式为 `vol-3344CCDD`，其中 `vol` 是卷的资源标识符。

对于虚拟磁带，可以为条码 ID 追加最多 4 字符前缀，以帮助您整理磁带。

Storage Gateway 资源 ID 采用大写形式。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**
>
> 从网关卷创建的 Storage Gateway 卷和 Amazon EBS 快照的 ID 将改为采用加长格式。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。自 2016 年 4 月起，您将能够使用这些加长格式的 ID，以便使用新格式测试您的系统。有关更多信息，请参阅加长的 EC2 和 EBS 资源 ID。
>
> 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`。
>
> 有关更多信息，请参阅 。公告：正视 — 2016 年将采用更长的 Storage Gateway 卷和快照 ID。.

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。
- 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). 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. 在中打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
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. 在中打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
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. 在中打开 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home.
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。

另请参阅

使用标签控制对网关和资源的访问

使用开源组件AWS Storage Gateway

在此部分中，您可以找到有关我们提供 Storage Gateway 功能所依赖的第三方工具和许可证的信息。

主题

- Storage Gateway 的开源组件
- 适用于 Amazon S3 文件网关的开源组件

Storage Gateway 的开源组件

多种第三方工具和许可证用于提供卷网关、磁带网关和 Amazon S3 文件网关的功能。

使用以下链接下载附带的某些开源软件组件的源代码：AWS Storage Gateway软件：

- 对于 VMware ESXi 上部署的网关：sources.tar
- 对于 Microsoft Hyper-V 上部署的网关：sources_hyperv.tar
- 对于在基于 Linux 内核的虚拟机 (KVM) 上部署的网关：sources_KVM.tar

该产品包括 OpenSSL Project 为在 OpenSSL Toolkit 中使用而开发的软件 (http://www.openssl.org/)。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.

适用于 Amazon S3 文件网关的开源组件

多种第三方工具和许可证用于提供 Amazon S3 文件网关（S3 文件网关）功能。

使用以下链接下载 S3 File Gateway 软件附带的某些开源软件组件的源代码：

- 对于 Amazon S3 文件网关：sgw-file-s3 开源 .tgz

该产品包括 OpenSSL Project 为在 OpenSSL Toolkit 中使用而开发的软件 (http://www.openssl.org/)。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.

配额

文件共享的配额

下表列出了文件共享的配额。

描述	文件网关
每个 Amazon S3 存储桶的最大文件共享数。文件共享和 S3 存储桶之间存在一对一映射	1
每个网关的最大文件共享数	10
单个文件的最大大小，即 Amazon S3 中单个对象的最大大小。 **Note** 如果您写入文件的大小超过 5 TB，则会收到“文件太大”错误消息，并且只上传文件的前 5 TB。	5 TB
最大路径长度	1024 字节

描述	文件网关
Note 客户端不得创建超过此长度的路径，否则会导致错误。此限制适用于文件网关支持的 NFS 和 SMB 协议。	

为网关推荐的本地磁盘大小

下表为所部署的网关推荐了本地磁盘存储的大小。

网关类型	缓存（最小值）	缓存（最大值）	其他所需的本地磁盘
S3 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，最大容量。
在向现有网关添加缓存时，在主机 (管理程序或 Amazon EC2 实例) 中创建新磁盘至关重要。
如果之前已将磁盘分配为缓存，请勿更改现有磁盘的大小。

使用存储类

Storage Gateway 支持 Amazon S3 标准、Amazon S3 标准 — 不频繁访问、Amazon S3 智能分层以及 S3 Glacier 存储类。有关存储类的更多信息，请参阅Amazon S3 存储类中的Amazon Simple Storage Service 用户指南.

主题

- 将存储类与文件网关结合使用
- 将 GLACIER 存储类用于文件网关

将存储类与文件网关结合使用

当您创建或更新文件共享时，您可以为对象选择您的存储类。您可以选择 Amazon S3 标准存储类别，或任何 S3 标准 — IA、S3 单区 — IA 或 S3 智能分层存储类。存储在任一这些存储类中的对象可以通过生命周期策略转换到 GLACIER 中。

Amazon S3 存储类	注意事项
标准	选择“Standard”(标准) 将您经常访问的文件冗余存储在地理上分开的多个可用区中。这是默认存储类。有关更多信息，请参阅 Amazon S3 定价。
S3 Intelligent-Tiering	选择“Intelligent-Tiering”(智能分层) 可通过自动将数据移动到最具成本效益的存储访问层来优化存储成本。 存储在 “Intelligent-Tiering” (智能分层) 存储类别中的对象可能会因在 30 天内覆盖、删除、请求或转换存储类别之间的对象而产生额外费用。存储时间最短为 30 天，在 30 天之前删除的对象将按比例收取相当于剩余天数的存储费用。考虑这些对象的更改频率，计划保留这些对象的时间以及需要访问的频率。小于 128 KB 的对象无法在 “智能分层” (智能分层) 存储类别中进行自动分层。这些对象按频繁访问套餐费率收费，并收取提前删除费用。 S3 智能分层现在支持存档访问层和深度存档访问层。S3 智能分层会自动将 90 天未访问的对象移动到存档访问层，然后在 180 天未访问后将其移动到 Deep Archive 访问层。无论何时还原其中一个存档访问层中的对象，该对象都会在几个小时内移动到 “频繁访问” 层，并准备好进行检索。如果试图通过文件共享访问文件的用户或应用程序只存在于两个存档层中的一个存档层中，这会导致超时错误。如果您的应用程序通过

Amazon S3 存储类	注意事项
	文件网关提供的文件共享访问文件，请勿将存档层与 S3 智能分层结合使用。 对文件网关管理的文件执行更新元数据（例如所有者、时间戳、权限和 ACL）的文件操作时，将删除现有对象，并在此 Amazon S3 存储类中创建新版本的对象。在生产环境中使用此存储类之前，应验证文件操作如何影响对象创建，因为需要支付提前删除费 有关更多信息，请参阅 Amazon S3 定价。
S3 Standard-IA	选择“Standard-IA”(标准 - IA) 将您不常访问的文件冗余存储在地理上分开的多个可用区中。 存储在 “Standandard-IA” (标准-IA) 存储类别中的对象可能会因在 30 天内覆盖、删除、请求、检索或转换存储类别之间的对象而产生额外费用。最少存储时间为 30 天。30 天之前删除的对象将产生相当于剩余天数的存储费用的按比例计算。考虑这些对象的更改频率，计划保留这些对象的时间以及需要访问的频率。小于 128 KB 的对象需支付 128 KB 的费用，并收取提前删除费用。 对文件网关管理的文件执行更新元数据（例如所有者、时间戳、权限和 ACL）的文件操作时，将删除现有对象，并在此 Amazon S3 存储类中创建新版本的对象。在生产环境中使用此存储类之前，应验证文件操作如何影响对象创建，因为需要支付提前删除费 有关更多信息，请参阅 Amazon S3 定价。

Amazon S3 存储类	注意事项
S3 One Zone-IA	选择单区-IA 将您不常访问的文件存储在单个可用区中。 存储在 “One Zone-IA” (单区-IA) 存储类别中的对象可能会因在 30 天内覆盖、删除、请求、检索或转换存储类别之间的对象而产生额外费用。存储时间最短为 30 天，在 30 天之前删除的对象将按比例收取相当于剩余天数的存储费用。考虑这些对象的更改频率，计划保留这些对象的时间以及需要访问的频率。小于 128 KB 的对象需支付 128 KB 的费用，并收取提前删除费用。 对文件网关管理的文件执行更新元数据（例如所有者、时间戳、权限和 ACL）的文件操作时，将删除现有对象，并在此 Amazon S3 存储类中创建新版本的对象。在生产环境中使用此存储类之前，应验证文件操作如何影响对象创建，因为需要支付提前删除费 有关更多信息，请参阅 Amazon S3 定价。

尽管您可以将对象从文件共享直接写入 S3 标准 — IA、S3-One Zone-IA 或 S3 智能分层存储类别，但我们建议您使用生命周期策略转换对象而不是直接从文件共享写入，尤其是如果您希望更新或删除对象存档后 30 天内。有关生命周期策略信息，请参阅对象生命周期管理.

将 GLACIER 存储类用于文件网关

如果您通过 Amazon S3 生命周期策略将某个文件转换到 S3 Glacier，且该文件通过缓存呈现给您的文件共享客户端，您在更新该文件时将遇到 I/O 错误。我们建议将 CloudWatch Events 设置为在这些 I/O 错误发生时接收通知，然后使用该通知采取措施。例如，您可以采取措施以将已存档对象还原到 Amazon S3 中。在对象还原到 S3 后，您的文件共享客户端可以通过文件共享成功地访问和更新它们。

有关如何还原已存档对象的信息，请参阅。还原存档对象中的Amazon Simple Storage Service 用户指南.

Storage Gateway 的 API 参考

除使用控制台外，您还可以使用 AWS Storage Gateway API，以编程方式配置并管理网关。本部分描述 AWS Storage Gateway 操作、为身份验证进行的请求签名和错误处理。有关可用于 Storage Gateway 的区域和终端节点的信息，请参阅AWS Storage Gateway终端节点和配额中的AWS一般参考.

> **Note**
>
> 您也可以使用AWS使用 Storage Gateway 开发应用程序时使用 SDK 这些区域有：AWS适用于 Java、.Net 和 PHP 的开发工具包包含底层的 Storage Gateway API，从而简化您的编程任务。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必需的请求标头

本部分描述您每次向其发送 POST 请求时必须使用的标头。AWS Storage Gateway. 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。

下例展示在 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
```

以下是必须包含在 POST 请求中的标头AWS Storage Gateway. 以下所示标头以 “x-amz” 为开头AWS 具体的标头。列出的其他所有标头均为 HTTP 事务中使用的普通标头。

标头	描述
`Authorization`	授权标头包含有关启用的请求的数种信息。AWS Storage Gateway以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，您指定YourAccessKey，年份、月份和日期，(yyyymmdd)、区域 和 CalculatedSignature。授权标头的格式由AWSV4 签名过程。签名的详细信息在主题 签名请求 中进行讨论。
`Content-Type`	使用`application/x-amz-json-1.1` 作为所有请求的内容类型AWS Storage Gateway. `Content-Type: application/x-amz-json-1.1`
`Host`	使用主机标头来指定AWS Storage Gateway发送请求的终端节点。例如，`storagegateway.us-east-2.amazonaws.com` 是美国东部 (俄亥俄) 区域的终端节点。有关可用于的终端节点的更多信息AWS Storage Gateway请参阅AWS Storage Gateway终端节点和配额中的AWS 一般参考. `Host: storagegateway. region.amazonaws.com`

标头	描述
x-amz-date	您必须在 HTTP 中提供时间戳Date标题或 AWSx-amz-date 标头。(部分 HTTP 客户端库文件不允许您设置Date标头。) 当x-amz-date 标头存在，AWS Storage Gateway忽略任何Date请求身份验证期间的标头。x-amz-date 格式必须为 YYYYMMDD'T'HHMMSS'Z' 格式的 ISO8601 Basic。如果同时使用了Date和x-amz-date 标头，日期标头的格式就不必是 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` 这些区域有：OoperationName值（例如 “ActivateGateway”）可从以下 API 列表中找到：Storage Gateway 的 API 参考.

签名请求

Storage Gateway 要求通过对请求进行签名，来验证所发送的每个请求 您使用加密哈希函数计算数字签名，从而对请求签名。加密哈西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。

收到您的请求后，Storage Gateway 将使用对该请求进行签名的相同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 将处理该请求。否则，请求将被拒绝。

使用 Storage Gateway 支持使AWS签名版本 4. 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 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，以您的秘密访问密钥为开始并使用凭证范围字符串来创建基于哈西的消息验证码 (HMAC)。

实例签名计算

下例演练为 ListGateways 创建签名的详细步骤。该示例可用作核查您的签名计算方法的参考。其他参考计算方法包含在 Amazon Web Services 词汇表的签名版本 4 测试套件中。

示例假定以下各项：

- 请求的时间戳为“Mon, 10 Sep 2012 00:00:00”GMT。
- 终端节点为美国东部 (俄亥俄) 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 API）没有查询参数。

这些区域有：待签字符串为了任务 2：创建待签字符串是：

```
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：AKIAIOSFODNN7EXAMPLE

```
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

本部分提供有关 AWS Storage Gateway 错误的引用信息。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，仅为 `ActivationKeyInvalid`ActivateGateway API 返回操作错误代码。

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 例外。当 AWS Storage Gateway 操作返回错误响应时，响应正文中会包含这些例外之一。`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	消息	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`	X.509 证书或AWS我们的记录中没有所提供的访问密钥 ID。	403 禁止访问

例外	消息	HTTP 状态代码
InvalidGatewayRequestException	操作错误代码 中的操作错误代码消息之一。	400 错误请求
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	请求中必须包含有效的（已注册）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	这些区域有：AWS访问密钥 Id 需要订阅服务。	400 错误请求
ThrottlingException	费率已超。	400 错误请求
UnknownOperationException	指定了未知操作。Storage Gateway 中的操作 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

下表显示的是 AWS Storage Gateway 操作错误代码和返回这些代码的 API 之间的映射。返回所有操作错误代码，其中包括两个常规例外情况之一—InternalServerError和InvalidGatewayRequestException中介绍了异常.

操作错误代码	消息	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	消息	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
文件系统关联终端点配置冲突	现有的文件系统关联端点配置与指定的配置冲突。	关联文件系统
文件系统关联端点 IP 地址已在使用中	指定的端点 IP 地址已在使用中。	关联文件系统
文件系统关联端点 IP 地址丢失	缺少文件系统关联端点 IP 地址。	关联文件系统
找不到文件系统关联	找不到指定的文件系统关联。	更新文件系统协会 取消关联文件系统 描述文件系统关联
找不到文件系统	找不到指定的文件系统。	关联文件系统

操作错误代码	消息	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	消息	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	消息	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	消息	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	消息	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	消息	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	消息	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	消息	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	消息	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	消息	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	消息	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	消息	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	消息	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	消息	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	消息	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	消息	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	消息	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	消息	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：application/x-amz-json-1.1
- 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 DescribeStorediSCSIVolumes API 并指定不存在的网关 ARN 请求输入，那么会返回以下 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 中的操作

有关 Storage Gateway 操作的列表，请参阅操作中的AWS Storage GatewayAPI 参考.

的文档历史记录AWSStorage Gateway

- API 版本：2013-06-30
- 最新文档更新：2021 年 10 月 12 日

下表介绍每一个发行版中的重大更改。AWSStorage Gateway 用户指南2018 年 4 月之后。如需对此文档更新的通知，您可以订阅 RSS 源。

更新-历史记录-更改	update-history-description	update-history-date
更新了网关创建程序	更新了创建新网关的程序，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
Support SMB 文件共享上的强制关闭文件	现在，您可以使用本地组设置来分配网关管理员权限。网关管理员可以使用共享文件夹 Microsoft 管理控制台管理单元强制关闭在 SMB 文件共享上打开和锁定的文件。有关更多信息，请参阅 。为网关配置本地组.	2021 年 10 月 12 日
对 NFS 文件共享的审核日志支持	现在，您可以配置 NFS 文件共享以生成审计日志，以提供有关用户访问文件共享中的文件和文件夹的详细信息。您可以使用这些日志监控用户活动，并在识别到不当的活动模式时采取措施。有关更多信息，请参阅 。了解文件网关审核日志.	2021 年 10 月 12 日
接入点别名	文件网关文件共享现在可以使用存储桶风格的接入点别名连	2021 年 10 月 12 日

	接到 Amazon S3 存储。有关更多信息，请参阅 。创建文件共享.	
VPC 终端节点和接入点支持	文件网关文件共享现在可以通过 VPC 中的接入点或接口终端节点连接到 S3 存储桶AWS PrivateLink. 有关更多信息，请参阅 。创建文件共享.	2021 年 7 月 7 日
支持机会主义锁	文件网关文件共享现在可以使用机会锁定来优化其文件缓冲策略，这在大多数情况下提高了性能，特别是在 Windows 上下文菜单方面。有关更多信息，请参阅 。创建 SMB 文件共享.	2021 年 7 月 7 日
FedRAMP 合规性	Storage Gateway 现在符合 FedRAMP 标准。有关更多信息，请参阅 。的合规 Storage Gateway 验证.	2020 年 11 月 24 日
基于计划的带宽限制	Storage Gateway 现在支持基于日程安排的磁带和卷网关进行带宽限制。有关更多信息，请参阅 。使用 Storage Gateway 控制台安排带宽限制.	2020 年 11 月 9 日
文件网关的文件上传通知	文件网关现在提供文件上传通知，当文件网关已将文件完全上传到 Amazon S3 时，该通知您。有关更多信息，请参阅 。获取文件上传通知.	2020 年 11 月 9 日

针对文件网关的基于访问的枚举	文件网关现在提供基于访问的枚举，它根据共享的 ACL 过滤 SMB 文件共享上的文件和文件夹枚举。有关更多信息，请参阅 。创建 SMB 文件共享.	2020 年 11 月 9 日
文件网关迁移	文件网关现在提供了用新文件网关替换现有文件网关的记录过程。有关更多信息，请参阅 。用新的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了 4 倍。有关更多信息，请参阅 。文件网关的性能指南.	2020 年 8 月 31 日
通过控制台订购硬件设备	您现在可以通过AWSStorage Gateway 控制台。有关更多信息，请参阅 。使用 Storage Gateway 硬件设备.	2020 年 8 月 12 日
Support 美国联邦信息处理标准 (FIPS) 终端节点AWS区域	现在，您可以在美国东部（俄亥俄）、美国西部（加利福尼亚北部）、美国西部（加利福尼亚北部）、美国西部（俄勒冈）和加拿大（中部）区域激活网关。有关更多信息，请参阅 。AWSStorage Gateway 终端节点和配额中的AWS一般参考.	2020 年 7 月 31 日

Support 附加到单个 Amazon S3 存储桶的多个文件共享	文件网关现在支持为单个 S3 存储桶创建多个文件共享，并根据目录访问频率将文件网关的本地缓存与存储桶同步。您可以限制管理在文件网关上创建的文件共享所需的存储桶数量。您可以为 S3 存储桶定义多个 S3 前缀，然后将单个 S3 前缀映射到单个网关文件共享。您还可以将网关文件共享名称定义为独立于存储桶名称，以适应本地文件共享命名约定。有关更多信息，请参阅 。创建 NFS 文件共享要么创建 SMB 文件共享.	2020 年 7 月 7 日
文件网关本地缓存存储空间增加 4 倍	Storage Gateway 现在支持文件网关的本地缓存高达 64 TB，通过提供对较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 。为网关推荐的本地磁盘大小中的Storage Gateway 用户指南.	2020 年 7 月 7 日
在 Storage Gateway 控制台中查看 Amazon CloudWatch 警报	您现在可以在 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) 终端节点	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 终端节点，请参阅选择服务终端节点。要为卷网关选择 FIPS 终端节点，请参阅选择服务终端节点。要为磁带网关选择 FIPS 终端节点，请参阅选择服务终端节点。	2020 年 5 月 22 日
NewAWS区域	Storage Gateway 现已在非洲（开普敦）和欧洲（米兰）区域提供。有关更多信息，请参阅 。AWSStorage Gateway 终端节点和配额中的AWS一般参考.	2020 年 5 月 7 日
对 S3 智能分层存储类的支持	Storage Gateway 现在支持 S3 智能分层存储类。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 。可自动优化经常访问和不经常访问的对象的存储类中的Amazon Simple Storage Service 用户指南.	2020 年 4 月 30 日
NewAWS区域	现于中可用 Storage GatewayAWSGovCloud（美国东部）区域。有关更多信息，请参阅 。AWSStorage Gateway 终端节点和配额中的AWS一般参考.	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 。支持的管理程序和主机要求中的Storage Gateway 用户指南.	2020 年 2 月 4 日
对 VMware vSphere 高可用性的支持	现在支持 VMware 高可用性，以帮助保护存储工作负载免受硬件、管理程序或网络故障的影响。有关更多信息，请参阅 。将 VMware vSphere High Availability 与 Storage Gateway 结合使中的Storage Gateway 用户指南. 此版本还包含性能改进。有关更多信息，请参阅 。性能中的Storage Gateway 用户指南.	2019 年 11 月 20 日
NewAWS 区域用于磁带网关	磁带网关现已在南美洲（圣保罗）区域提供。有关更多信息，请参阅 。AWSStorage Gateway 终端节点和配额中的AWS一般参考.	2019 年 9 月 24 日
Support Amazon CloudWatch Logs	现在，您可以使用 Amazon CloudWatch 日志组配置文件网关，以获取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 。通过 Amazon CloudWatch 日志组获取有关网关 Health 和错误的通知中的Storage Gateway 用户指南。	2019 年 9 月 4 日

NewAWS 区域	Storage Gateway 现已在亚太地区（香港）区域提供。有关更多信息，请参阅 。AWSStorage Gateway 终端节点和配额中的AWS一般参考.	2019 年 8 月 14 日
NewAWS 区域	Storage Gateway 现已在中东（巴林）区域提供。有关更多信息，请参阅 。AWSStorage Gateway 终端节点和配额中的AWS一般参考.	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
Microsoft Windows ACL 的 SMB 文件共享支持	对于文件网关，您现在可以使用 Microsoft Windows 访问控制列表 (ACL) 控制对服务器消息块 (SMB) 文件共享的访问。有关更多信息，请参阅使用 Microsoft Windows ACL 控制对 SMB 文件共享的访问。	2019 年 5 月 8 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

欧洲 Storage Gateway 硬件设备的可用性	现已在欧洲使用 Storage Gateway 硬件设备。有关更多信息，请参阅 。AWSStorage Gateway 硬件设备区域中的AWS一般参考. 此外，您现在还可以将 Storage Gateway 硬件设备上的可用存储从 5 TB 增加到 12 TB，并将安装的铜缆网络网卡更换为 10 Gb 以太网光纤网卡。有关更多信息，请参阅设置您的硬件设备。	2019 年 2 月 25 日
Support Storage Gateway 硬件设备	Storage Gateway 硬件设备包含预安装在第三方服务器上的 Storage Gateway 软件。您可以从 AWS Management Console管理设备。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
对服务器消息块 (SMB) 协议的支持	文件网关向文件共享添加了对服务器消息块 (SMB) 协议的支持。有关更多信息，请参阅创建文件共享。	2018 年 6 月 20 日

早期更新

下表介绍每一个发行版中的重大更改。AWSStorage Gateway 用户指南2018 年 5 月之前。

更改	说明	更改日期
Support S3 单区-IA 存储类别	对于文件网关，您现在可以选择 S3 单区-IA 作为文件共享的默认存储类别。使用此存储类别，您可以在 Amazon S3 内的单个可用区中存储对象数据。有关更多信息，请参阅创建文件共享。	2018 年 4 月 4 日

更改	说明	更改日期
新的 AWS 区域	磁带网关现已在亚太地区（新加坡）区域提供。有关详细信息，请参阅支持的 AWS 区域。	2018 年 4 月 3 日
Support 刷新缓存通知、申请方付款和适用于 Amazon S3 存储桶的标准 ACL	使用文件网关，您现在可以在网关完成为 Amazon S3 存储桶刷新缓存后获得通知。有关更多信息，请参阅 。RefreshCache.html中的Storage Gateway API 参考. 对于文件网关，您现在可以指定申请方或读取者支付访问费用，而不是存储桶拥有者支付。 使用文件网关，您现在可以向映射到 NFS 文件共享的 S3 存储桶的所有者授予完全控制权限。 有关更多信息，请参阅创建文件共享。	2018 年 3 月 1 日
新的 AWS 区域	Storage Gateway 现已在欧洲（巴黎）区域提供。有关详细信息，请参阅支持的 AWS 区域。	2017 年 12 月 18 日
支持文件上传通知和 MIME 类型猜测	文件网关现在使您能够在写入 NFS 文件共享的所有文件均已上传至 Amazon S3 后获得通知。有关更多信息，请参阅 。NotifyWhenUploaded中的Storage Gateway API 参考. 文件网关现在可根据文件扩展名猜测已上传对象的 MIME 类型。有关更多信息，请参阅创建文件共享。	2017 年 11 月 21 日
支持 VMware ESXi 虚拟机监控程序版本 6.5	AWSStorage Gateway 现在支持 VMware ESXi 虚拟机监控程序版本 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
Microsoft Hyper-V 管理程序的文件网关支持	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

更改	说明	更改日期
新的 AWS 区域	Storage Gateway 现已在亚太地区（孟买）区域提供。有关详细信息，请参阅支持的 AWS 区域。	2017 年 5 月 02 日
对文件共享设置的更新 对文件共享的缓存刷新的支持	文件网关现在将挂载选项添加到文件共享设置。您现在可以为文件共享设置 squash 和只读选项。有关更多信息，请参阅创建文件共享。 文件网关现在可以在 Amazon S3 存储桶中查找自网关上次列出存储桶内容并缓存结果后添加或删除的对象。有关更多信息，请参阅 API 参考中的 RefreshCache。	2017 年 3 月 28 日
支持 Amazon EC2 上的文件网关	AWSStorage Gateway 现在可将文件网关部署在 Amazon EC2 中。您可以使用现在以社区 AMI 形式提供的 Storage Gateway（AMI）在 Amazon EC2 中启动文件网关。有关如何创建文件网关并将它部署到 EC2 实例的信息，请参阅创建并激活 Amazon S3 文件网关。有关如何启动文件网关 AMI 的信息，请参阅 在 Amazon EC2 主机上部署文件网关。 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 代理路由部署在 EC2 上的网关。	2017 年 2 月 8 日
新的 AWS 区域	Storage Gateway 现已在欧洲（伦敦）区域提供。有关详细信息，请参阅支持的 AWS 区域。	2016 年 12 月 13 日
新的 AWS 区域	Storage Gateway 现已在加拿大（中部）区域提供。有关详细信息，请参阅支持的 AWS 区域。	2016 年 12 月 8 日
支持文件网关	除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

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。