aws

卷网关用户指南

AWS Storage Gateway

API 版本 2013-06-30

AWS Storage Gateway: 卷网关用户指南

Table of Contents

..... x
什么是卷网关？ 1
卷网关 1
您是 Storage Gateway 的新用户吗？ 2
卷网关的工作原理 2
卷网关 2
定价 6
规划网关部署 6
入门 8
报名参加 AWS Storage Gateway 8
AWS 区域 8
要求 9
硬件和存储要求 9
网络和防火墙要求 11
受支持的管理程序和主机要求 20
受支持的 iSCSI 启动程序 21
正在访问 AWS Storage Gateway 22
使用硬件设备 23
支持的 AWS 区域 23
设置硬件设备 23
在机架上安装硬件设备并连接到电源 25
硬件设备尺寸 25
配置网络参数 29
激活硬件设备 32
创建网关 33
为网关配置 IP 地址 33
配置网关 35
删除网关 35
删除硬件设备 36
创建网关 37
概述 - 网关激活 37
设置网关 37
连接到 AWS 37
检查并激活 37

概述 - 网关配置 37
概述 - 存储资源 38
创建卷网关 38
创建网关 38
创建卷 43
使用卷 46
备份您的卷 54
在 Virtual Private Cloud 中激活网关 59
为 Storage Gateway 创建 VPC 端点 60
管理您的网关 62
管理卷网关 62
编辑网关信息 63
添加卷 64
扩展卷的大小 64
克隆卷 64
查看卷使用率 68
减少卷上的计费存储量 68
删除卷 68
将您的卷迁移至不同的网关 69
创建一次性快照 71
编辑快照计划 71
删除快照 72
了解卷状态和转换 84
将数据移至新网关 92
将存储卷移至新的存储卷网关 93
将缓存卷移至新的缓存卷网关虚拟机。 95
监控 Storage Gateway 98
了解网关指标 98
Storage Gateway 指标的维度 102
监控上传缓冲区 103
监控缓存存储 105
了解 CloudWatch 警报 107
创建推荐的 CloudWatch 警报 108
创建自定义 CloudWatch 警报 109
监控卷网关 110
获取卷网关运行状况日志 111

使用亚马逊 CloudWatch 指标 112
衡量您的应用程序和网关间的性能。 113
衡量网关与 AWS间的性能 115
了解卷指标 118
维护网关 123
关闭网关虚拟机 123
启动和停止卷网关 124
管理本地磁盘 124
确定本地磁盘存储量 125
调整上传缓冲区大小 126
调整缓存存储大小 127
添加上传缓冲区或缓存存储 128
管理带宽 128
使用 Storage Gateway 控制台更改带宽限制 129
计划带宽限制 130
使用 AWS SDK for Java 131
使用 AWS SDK for .NET 133
使用 AWS Tools for Windows PowerShell 135
管理网关更新 136
打开或关闭维护更新 137
修改网关维护时段计划 137
在本地控制台上执行维护任务 138
在 虚拟机本地控制台上执行任务 138
在 EC2 本地控制台上执行任务 153
访问网关本地控制台 157
为网关配置网络适配器 162
删除网关和清除资源 166
使用 Storage Gateway 控制台删除网关 166
从本地部署的网关中删除资源 167
从部署在 Amazon EC2 实例上的网关中移除资源 168
Performance 169
优化网关性能 169
建议的配置 169
在网关中添加资源 169
优化 iSCSI 设置 172
向应用程序环境添加资源 172

将 VMware High Availability 与 Storage Gateway 结合使用 173
配置您的 vSphere VMware HA 集群 174
从 Storage Gateway 控制台下载 .ova 映像 175
部署网关 175
（可选）为集群上的其他 VM 添加覆盖选项 176
激活网关 176
测试您的 VMware High Availability 配置 177
安全性 178
数据保护 178
数据加密 179
配置 CHAP 身份验证 180
Identity and Access Management 182
受众 183
使用身份进行身份验证 183
使用策略管理访问 186
Stor AWS age Gateway 如何与 IAM 协作 187
基于身份的策略示例 194
故障排除 196
日志记录和监控 198
Storage Gateway 信息位于 CloudTrail 198
了解 Storage Gateway 日志文件条目 199
合规性验证 201
韧性 201
基础设施安全性 202
AWS 安全最佳实践 202
排查网关问题 203
故障排除：网关离线问题 203
检查关联的防火墙或代理 204
检查是否正在对网关流量进行 SSL 检查或深度数据包检查 204
检查虚拟机管理程序主机上是否出现停电或硬件故障 204
检查关联的缓存磁盘是否有问题 204
故障排除：网关激活问题 205
解决使用公共终端节点激活网关时出现的错误 205
解决使用 Amazon VPC 终端节点激活网关时出现的错误 208
解决使用公有终端节点激活网关且同一 VPC 中有 Storage Gateway VPC 终端节点时出现的错误 211

排查本地网关问题 212
激活 AWS Support 以帮助排除网关故障 214
排查 Microsoft Hyper-V 设置问题 215
排查 Amazon EC2 网关问题 219
过了一会儿网关并未激活 220
在实例列表中找不到 EC2 网关实例 220
无法将 Amazon EBS 卷附加到 EC2 网关实例 220
不能将启动程序挂载到 EC2 网关的卷目标 220
您在添加存储卷时收到一条消息，指出“无可用磁盘” 220
如何删除分配为上传缓冲区空间的磁盘，从而减少上传缓冲区空间 221
进出 EC2 网关的吞吐量降为零 221
激活 AWS Support 以帮助排除网关故障 221
使用串行控制台连接到 Amazon EC2 网关 223
排查硬件设备问题 223
如何确定服务 IP 地址 223
如何执行出厂重置 223
如何执行远程重启 223
如何获得 Dell iDRAC 支持 223
如何找到硬件设备序列号 223
如何获得硬件设备支持 224
排查卷问题 225
控制台显示您的卷未配置 225
控制台显示您的卷无法恢复 225
您的缓存网关无法访问，您希望恢复数据 226
控制台显示您的卷处于 PASS THROUGH 状态 226
您要验证卷的完整性并修复可能的错误 227
您的卷的 iSCSI 目标未在 Windows 磁盘管理控制台中显示 227
您要更改卷的 iSCSI 目标名称 227
您计划的卷快照未创建 227
您需要移除或更换出现故障的磁盘 227
从应用程序到卷的吞吐量降为零 227
您网关中的一个缓存磁盘遇到了故障 228
卷快照处于 PENDING 状态的时间长于预期时间 228
高可用性运行状况通知 229
排查高可用性问题 229
运行状况通知 229

指标 230
恢复您的数据：最佳实践 230
从虚拟机意外关闭中恢复 231
从故障网关或 VM 恢复您的数据 231
从不可恢复卷恢复数据 232
从出现故障的缓存磁盘恢复数据 232
从受损文件系统恢复数据 232
从不可访问的数据中心恢复数据 233
其他资源 235
主机设置 235
为 Storage Gateway 配置 VMware 235
同步您的网关 VM 时间 242
为磁带网关部署 Amazon EC2 主机 244
使用默认设置部署 Amazon EC2 247
修改 Amazon EC2 实例元数据选项 249
卷网关 249
从网关中移除磁盘 250
EC2 网关的 EBS 卷 254
获取激活密钥 255
Linux (curl) 255
Linux (bash/zsh) 256
微软 Windows PowerShell 257
使用本地控制台 257
连接 iSCSI 启动程序 258
将卷连接到 Windows 客户端 259
将卷或 VTL 设备连接到 Linux 客户端 264
自定义 iSCSI 设置 266
配置 CHAP 身份验证 273
AWS Direct Connect 与 Storage Gateway 一起使用 280
端口要求 281
连接到网关 285
从 Amazon EC2 主机获取 IP 地址 285
了解资源和资源 ID 286
使用资源 ID 287
为资源添加标签 287
使用标签 288

开源组件 289
Storage Gateway 配额 289
卷的配额 290
为网关建议的本地磁盘大小 290
API 参考 292
必需的请求标头 292
对请求进行签名 294
实例签名计算 295
错误响应 296
异常 297
操作错误代码 298
错误响应 318
操作 320
文档历史记录 321
早期更新 332
发布说明 346

Amazon S3 文件网关文档已移至什么是 Amazon S3 文件网关？

Amazon FSx 文件网关文档已移至什么是 Amazon FSx 文件网关？

磁带网关文档已移至什么是磁带网关？

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。

什么是卷网关？

AWS Storage Gateway 将本地软件设备与基于云的存储设备相连接，从而在您的本地 IT 环境和 AWS 存储基础架构之间提供与数据安全功能的无缝集成。您可以使用此服务将数据存储到 Amazon Web Services 云，利用经济高效的可扩展存储来帮助保持数据安全性。

AWS Storage Gateway 提供基于文件的文件网关（Amazon S3 文件和 Amazon FSx 文件）、基于卷（缓存和存储）和基于磁带的存储解决方案。

主题

- 卷网关
- 您是 Storage Gateway 的新用户吗？
- 卷网关的工作原理（架构）
- Storage Gateway 定价
- 规划 Storage Gateway 部署

卷网关

卷网关 - 卷网关提供了支持云的存储卷，可以从本地应用程序服务器将该存储卷作为 Internet 小型计算机系统接口 (iSCSI) 设备来装载。

您可以在本地将卷网关部署为在 VMware ESXi、KVM 或 Microsoft Hyper-V 管理程序上运行的虚拟机设备，可以作为硬件设备来部署，也可以在 AWS 中作为 Amazon EC2 实例来部署。

该网关支持以下卷配置：

- 缓存卷 - 将数据存储在 Amazon Simple Storage Service (Amazon S3) 中并在本地保留经常访问的数据子集的副本。缓存卷不仅有助于节省大量主存储成本，而且最大程度地减小了本地扩展存储的需求。您还可以保留对经常访问的数据的低延迟访问。
- 存储卷 – 如果需要对整个数据集进行低延迟访问，请首先将本地网关配置为将所有数据存储在本地。然后将这些数据的 point-in-time 快照异步备份到 Amazon S3。此配置提供了经久、价格低廉且可以恢复到本地数据中心或 Amazon Elastic Compute Cloud (Amazon EC2) 的场外备份。例如，如果您出于灾难恢复目的而需要替代容量，则可以将备份恢复到 Amazon EC2。

文档：有关卷网关文档，请参阅创建卷网关。

您是 Storage Gateway 的新用户吗？

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：

- 创建卷网关介绍如何创建和使用卷网关。其中介绍了如何创建存储卷以及将数据备份到卷。
- 管理您的网关介绍如何为网关及其资源执行管理任务。

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 AWS Storage Gateway API 参考。

卷网关的工作原理（架构）

接下来，您可以找到卷网关解决方案的架构概述。

卷网关

对于卷网关，您可以使用缓存卷或存储卷。

主题

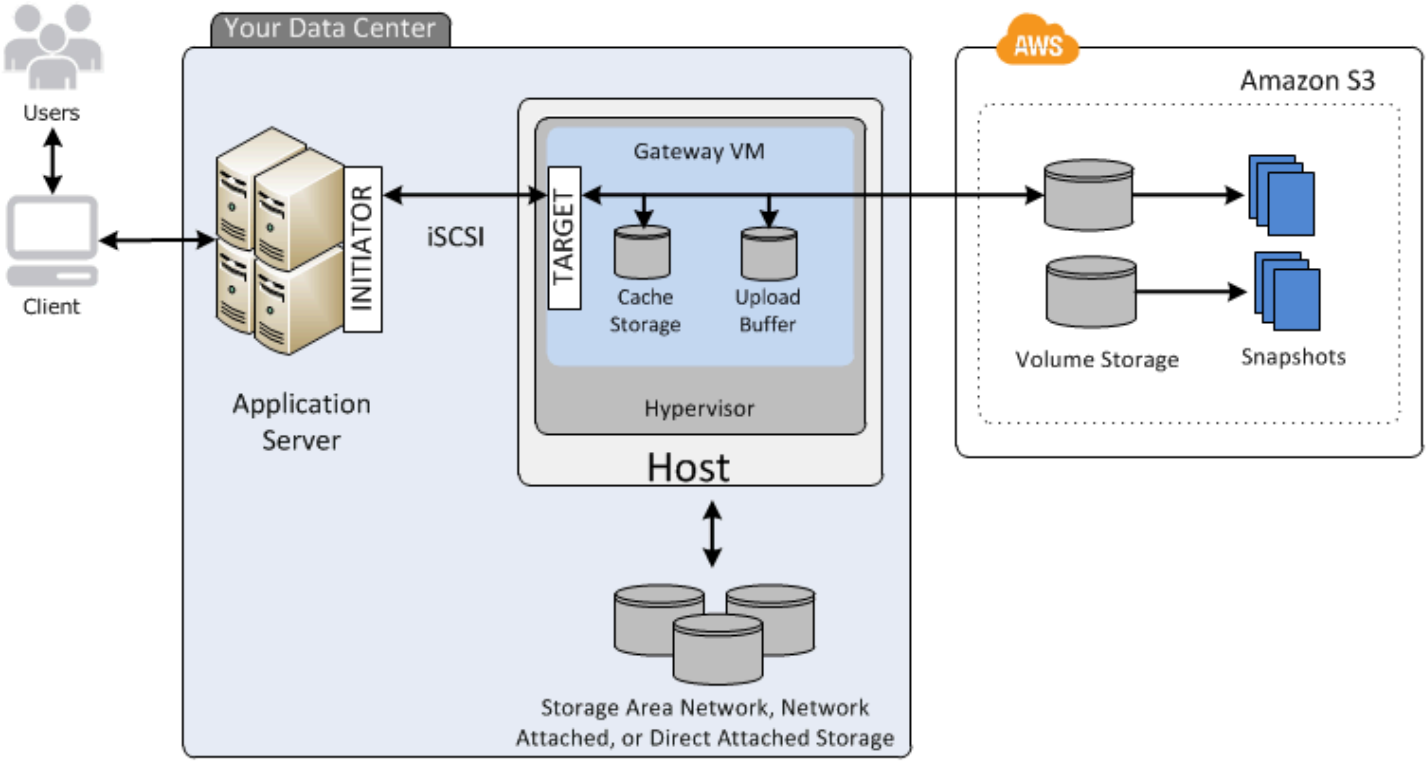
- 缓存卷架构
- 存储卷架构

缓存卷架构

通过使用缓存卷，您可以将 Amazon S3 用作主要数据存储，同时将经常访问的数据在 Storage Gateway 中本地保留。缓存卷可帮助您尽量避免扩展内部存储基础设施，同时为您的应用程序提供对其常用数据的低延迟访问。您可以创建容量高达 32 TiB 的存储卷，并从本地应用程序服务器将其附加为 iSCSI 设备。网关将写入这些卷中的数据存储在 Amazon S3 中，并将最近读取的数据保留在本地 Storage Gateway 的缓存和上传缓冲区存储中。

缓存卷的大小范围可以是 1 GiB 到 32 TiB，并且必须四舍五入到最接近的 GiB 值。为缓存卷配置的每个网关可以支持最多 32 个卷，总的最大存储卷大小为 1024 TiB (1 PiB)。

在缓存卷解决方案中，Storage Gateway 将所有本地应用程序数据保存在 Amazon S3 的存储卷中。以下示意图提供了缓存卷部署的概览。



在数据中心的主机上安装 Storage Gateway 软件设备（虚拟机）并将其激活后，您可以使用 AWS Management Console 来配置由 Amazon S3 支持的存储卷。您还可以使用 Storage Gateway API 或 AWS SDK 库以编程方式配置存储卷。您然后将这些存储卷作为 iSCSI 设备安装到场内应用程序服务器。

您还在场内为该 VM 分配磁盘。这些场内磁盘服务于下列目的：

- 网关用作缓存存储空间的磁盘 — 当您的应用程序向中的存储卷写入数据时 AWS，网关会首先将数据存储在用于缓存存储的本地磁盘上。然后网关将数据上传到 Amazon S3。缓存存储空间用作等待从上传缓冲区上传到 Amazon S3 的数据的本地持久存储器。

  缓存存储空间还让您的网关能够在本地存储您的应用程序的最近访问数据，以实现低延迟访问。如果您的应用程序请求数据，网关在检查 Amazon S3 前会先检查缓存存储中的数据。

  您可以使用以下准则确定可以为缓存存储空间分配的磁盘空间量。通常，您应该至少分配现有文件存储大小的 20% 作为缓存存储空间。缓存存储空间还应该大于上传缓冲区。此指引有助于确保缓存存储具有足够的大小来持续承载上传缓冲区中尚未上传到 Amazon S3 的所有数据。
- 网关用作上传缓冲区的磁盘 - 为了做好上传到 Amazon S3 的准备，您的网关还会将传入数据存储在一个暂存区域中（称为上传缓冲区）。您的网关通过加密的安全套接字层 (SSL) 连接将这些缓冲数据上传到 AWS，然后将其加密存储在 Amazon S3 中。

您可以对 Amazon S3 中的存储卷创建增量备份，也称为快照。这些 point-in-time 快照还作为亚马逊 EBS 快照存储在 Amazon S3 中。拍摄新的快照时，只有从上次快照拍摄以来发生变化的数据才会存储。创建快照后，网关会将更改上传到快照点，然后使用 Amazon EBS 创建新快照。您可以采用预定或一次性方式启动快照的拍摄。单个卷支持快速连续对多个快照进行排队，但每个快照都必须完成创建后才能创建下一个快照。删除快照时，只会移除其他任何快照不需要的数据。有关 Amazon EBS 快照的信息，请参阅 Amazon EBS 快照。

如果需要恢复数据的备份，则可以将 Amazon EBS 快照还原到网关存储卷。另外，对于大小高达 16 TiB 的快照，可以将快照用作新的 Amazon EBS 卷的起点。然后，您可以将这个新的 Amazon EBS 卷附加到 Amazon EC2 实例。

缓存卷的所有网关数据和快照数据均存储在 Amazon S3 中，并使用服务器端加密 (SSE) 进行静态加密。不过，您不能使用 Amazon S3 API 或其他工具（如 Amazon S3 管理控制台）访问这些数据。

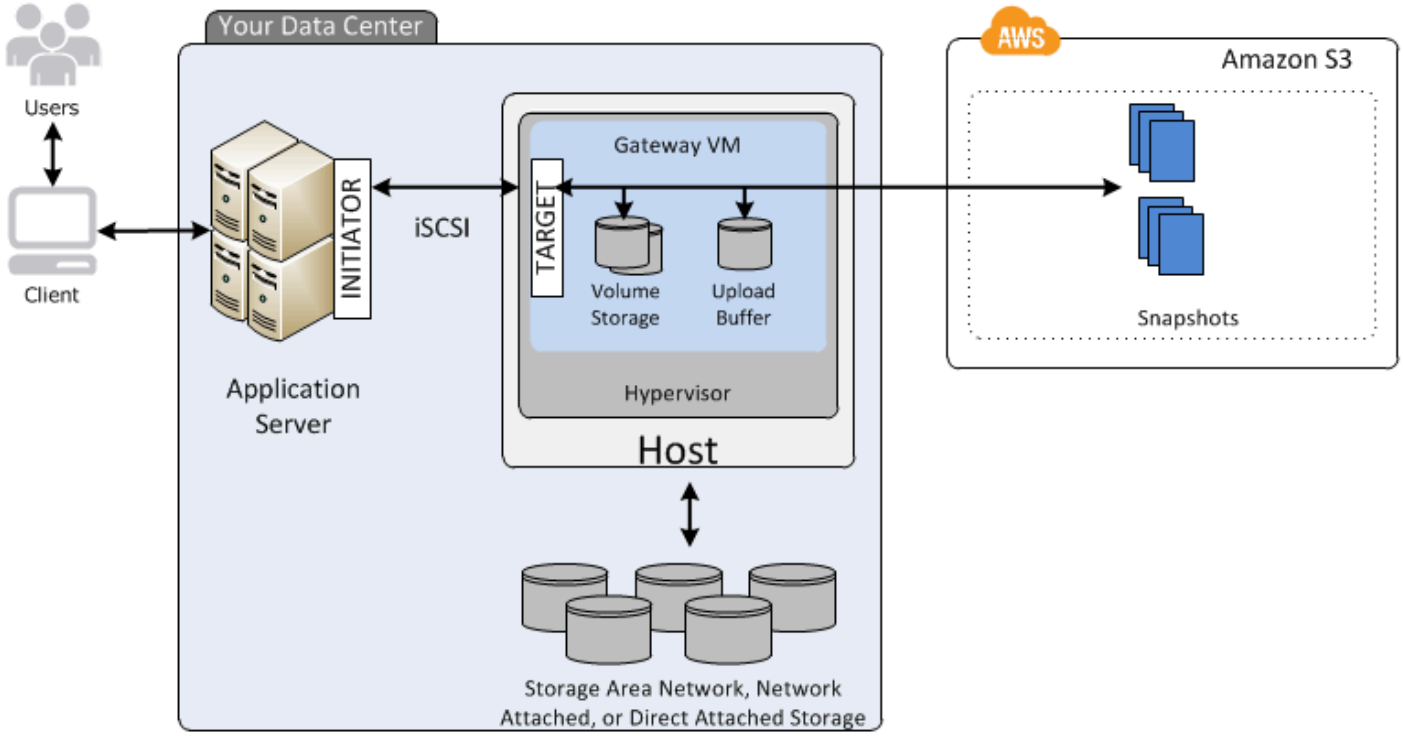
存储卷架构

通过使用存储卷，您可以将主要数据存储在本地，同时将这些数据异步备份到 AWS。存储卷为您的本地应用程序提供对整个数据集的低延迟访问。同时，它们可提供持久的场外备份。您可以创建存储卷，并从本地应用程序服务器将它们作为 iSCSI 设备挂载。写入到您的存储卷的数据保存在本地存储硬件中。此数据以 Amazon Elastic Block Store (Amazon EBS) 快照的形式异步备份到 Amazon S3。

存储卷的大小范围可以是 1 GiB 到 16 TiB，并且必须四舍五入到最接近的 GiB 值。为存储卷配置的每个网关可以支持最多 32 个卷、总共 512 TiB (0.5 PiB) 的卷存储。

使用存储卷，您可在数据中心本地维护卷存储。亦即，您将所有的应用程序场内保存在存储硬件中。然后，使用有助于保持数据安全性的功能，网关将数据上传到 Amazon Web Services 云，从而实现经济高效的备份和快速灾难恢复。如果您希望将数据保存在本地，这个解决方案就很适合，因为您需要对所有数据进行低延迟访问并在 AWS中维护备份。

下图概述了存储卷的部署情况。



在数据中心的主机上安装并激活 Storage Gateway 软件设备 (VM) 后，您可以创建网关存储卷。然后将它们映射到本地直连式存储 (DAS) 或存储区域网络 (SAN) 磁盘。您可以从新磁盘或已存有数据的磁盘开始着手。您然后可以将这些存储卷作为 iSCSI 设备安装到场内应用程序服务器。场内应用程序从/向网关存储卷读写数据的同时，这些数据从卷的已分配磁盘存储并检索。

为了准备要上传到 Amazon S3 的数据，网关还将传入数据存储在称为上传缓冲区的暂存区域中。您可以将场内 DAS 或 SAN 磁盘用作工作存储空间。您的网关通过加密的安全套接字层 (SSL) 连接，将数据从上传缓冲区上传到在 Amazon Web Services 云中运行的 Storage Gateway 服务。该服务随后将数据加密存储在 Amazon S3 中。

您可以对存储卷拍摄增量备份，亦即快照。网关将这些快照以 Amazon EBS 快照的形式存储在 Amazon S3 中。拍摄新的快照时，只有从上次快照拍摄以来发生变化的数据才会存储。创建快照后，网关会将更改上传到快照点，然后使用 Amazon EBS 创建新快照。您可以采用预定或一次性方式启动快照的拍摄。单个卷支持快速连续对多个快照进行排队，但每个快照都必须完成创建后才能创建下一个快照。删除快照时，只会删除其他快照都不需要的数据。

如果需要恢复数据的备份，则可以将 Amazon EBS 快照还原为本地网关存储卷。您还可以将快照用作新 Amazon EBS 卷的起点，并可在随后将该卷连接到 Amazon EC2 实例。

Storage Gateway 定价

有关定价的最新信息，请参阅 AWS Storage Gateway 详情页面上的定价。

规划 Storage Gateway 部署

通过使用 Storage Gateway 软件设备，您可以将现有的本地应用程序基础设施与提供数据安全功能的可扩展、经济实惠的 AWS 云存储连接起来。

要部署 Storage Gateway，您首先需要确定以下两项：

1. 您的网关类型 - 本指南介绍以下网关类型：
   - 卷网关 - 利用卷网关，您可以在 Amazon Web Services 云中创建存储卷。本地应用程序可将这些作为 Internet 小型计算机系统接口 (iSCSI) 目标进行访问。有两个选项 – 缓存卷和存储卷。
     - 使用缓存卷，您可以将卷数据存储在中 AWS，而最近访问的数据的一小部分则存储在本地缓存中。此方法实现了对经常访问的数据集进行低延迟访问。它还提供对存储在中的整个数据集的无缝访问 AWS。通过使用缓存卷，您可以扩展存储资源，而无需预配置其他硬件。
     - 使用存储卷，您可以将整组卷数据存储在本地，并在其中存储定期 point-in-time 备份（快照）AWS。在此模型中，您的本地存储是主存储，可提供对整个数据集的低延迟访问。 AWS 存储是在数据中心发生灾难时可以恢复的备份。

     对于缓存卷和存储卷，您可以以 Amazon EBS point-in-time 快照的形式拍摄卷网关卷的快照。您可以使用卷的快照作为新 Amazon EBS 卷的起点，并可在随后将该卷连接到 Amazon EC2 实例。通过这种方法，如果您需要额外的按需计算容量来进行数据处理或需要替换容量以用于灾难恢复，则可以将本地应用程序中的数据提供给在 Amazon EC2 上运行的应用程序。这使您可以为卷制作节省空间的版本控制副本，来满足数据保护、恢复、迁移和其他各种数据传输需求。

     有关基于 Amazon EBS 快照创建卷的信息，请参阅创建卷。

     有关卷网关的架构概述，请参阅缓存卷架构和存储卷架构。
2. 托管选项 — 您可以在本地将 Storage Gateway 作为虚拟机设备或硬件设备运行，也可以在本地以 Amazon EC2 实例的 AWS 形式运行。有关更多信息，请参阅要求。如果数据中心脱机且没有可用主机，则可在 EC2 实例上部署网关。Storage Gateway 提供了一个包含网关 VM 映像的 Amazon 系统映像 (AMI)。

此外，在配置主机以部署网关软件设备时，您需要为网关 VM 分配足够的存储。

在继续下一步之前，请确保您已完成以下操作：

- 对于本地部署的网关，选择 VM 主机的类型并进行设置。您的选项是 VMware ESXi 管理程序、Microsoft Hyper-V 和基于 Linux 内核的虚拟机 (KVM)。如果您在防火墙后部署网关，请确保网关 VM 能够访问端口。有关更多信息，请参阅 要求。

入门

在此部分中，您可以找到有关如何开始使用 Storage Gateway 的说明。要开始使用，您首先要注册 AWS。如果您是新用户，我们建议您阅读区域和要求部分。

主题

- 报名参加 AWS Storage Gateway
- AWS 区域
- 要求
- 正在访问 AWS Storage Gateway

报名参加 AWS Storage Gateway

要使用 Storage Gateway，您需要一个 Amazon Web Services 账户，以使您有权访问所有 AWS 资源、论坛、支持和使用率报告。任何服务只会在使用后才需要付费。如果您已有 Amazon Web Services 账户，则可跳过本步骤。

注册 Amazon Web Services 账户

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

   在注册时，将接到一通电话，要求使用电话键盘输入一个验证码。

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

有关定价的信息，请参阅 Storage Gateway 详情页面上的定价。

AWS 区域

Storage Gateway 在激活网关的 AWS 区域中存储卷、快照、磁带和文件数据。文件数据存储在您的 Amazon S3 存储桶所在的 AWS 区域。在开始部署网关之前，您需要在 Storage Gateway 管理控制台的右上角选择一个 AWS 区域。

- 存储网关-有关支持的 AWS 区域和可用于 Storage Gateway 的 AWS 服务终端节点列表，请参阅中的AWS Storage Gateway 终端节点和配额。AWS 一般参考
- Storage Gateway 硬件设备—有关硬件设备可以使用的支持 AWS 区域，请参阅中的AWS Storage Gateway 硬件设备区域。AWS 一般参考

要求

除非另有说明，否则所有网关配置都需要满足以下要求。

主题

- 硬件和存储要求
- 网络和防火墙要求
- 受支持的管理程序和主机要求
- 受支持的 iSCSI 启动程序

硬件和存储要求

本节介绍网关的最低硬件和设置要求，以及为所需存储分配的最小磁盘空间量。

虚拟机硬件要求。

在部署网关时，您必须确保部署网关虚拟机的基础硬件能够分配以下最少资源：

- 分配给 VM 的四个虚拟处理器。
- 对于卷网关，您的硬件应使用以下数量的 RAM：
  - 对于缓存大小不超过 16 TiB 的网关，预留 16 GiB 的 RAM
  - 对于缓存大小为 16 TiB 至 32 TiB 的网关，预留 32 GiB 的 RAM
  - 对于缓存大小为 32 TiB 至 64 TiB 的网关，预留 48 GiB 的 RAM
- 80 GiB 磁盘空间，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 AWS Storage Gateway 配额。

对 Amazon EC2 实例类型的要求

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

对于卷网关，您的 Amazon EC2 实例应根据您计划用于网关的缓存大小使用以下数量的 RAM：

- 对于缓存大小不超过 16 TiB 的网关，预留 16 GiB 的 RAM
- 对于缓存大小为 16 TiB 至 32 TiB 的网关，预留 32 GiB 的 RAM
- 对于缓存大小为 32 TiB 至 64 TiB 的网关，预留 48 GiB 的 RAM

使用为您的网关类型推荐的以下实例类型之一。

建议用于缓存卷和磁带网关类型

- 通用型实例系列 – m4、m5 或 m6 实例类型。

> **Note**
>
> 建议不要使用 m4.16xlarge 实例类型。

- 计算优化型实例系列 - c4、c5 或 c6 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、r5 或 r6 实例类型。
- 存储优化型实例系列 - i3 或 i4 实例类型。

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。

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）	上传缓冲区（最小值）	上传缓冲区（最大值）	其他必需的本地磁盘
缓存卷网关	150 GiB	64 TiB	150 GiB	2 TiB	—

网关类型	缓存（最小值）	缓存（最大值）	上传缓冲区（最小值）	上传缓冲区（最大值）	其他必需的本地磁盘
存储卷网关	—	—	150 GiB	2 TiB	一个或多个，用于存储卷

> **Note**
>
> 您可以为缓存和上传缓冲区配置一个或多个不超过最大容量的本地驱动器。
> 在向现有网关添加缓存或上传缓冲区时，在主机（管理程序或 Amazon EC2 实例）中创建新磁盘，这很重要。如果之前已将磁盘分配为缓存或上传缓冲区，请勿更改现有磁盘的大小。

有关网关配额的信息，请参阅AWS Storage Gateway 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。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 Storage Gateway，或者使用其他类型的部署（包括本地）和限制 AWS IP 地址范围的网络安全策略。在这些情况下，当 AWS IP 范围值发生变化时，您的网关可能会遇到服务连接问题。您需要使用的 AWS IP 地址范围值位于您激活网关的 AWS 区域的 Amazon 服务子集中。有关当前 IP 范围值，请参阅《AWS 一般参考》中的 AWS IP 地址范围。

> **Note**
>
> 网络带宽要求因网关上传和下载的数据量而异。成功下载、激活和更新网关至少需要 100Mbps。您的数据传输模式将决定支持您的工作负载所需的带宽。在某些情况下，您可以在 Amazon EC2 上部署 Storage Gateway 或使用其他类型的部署

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。

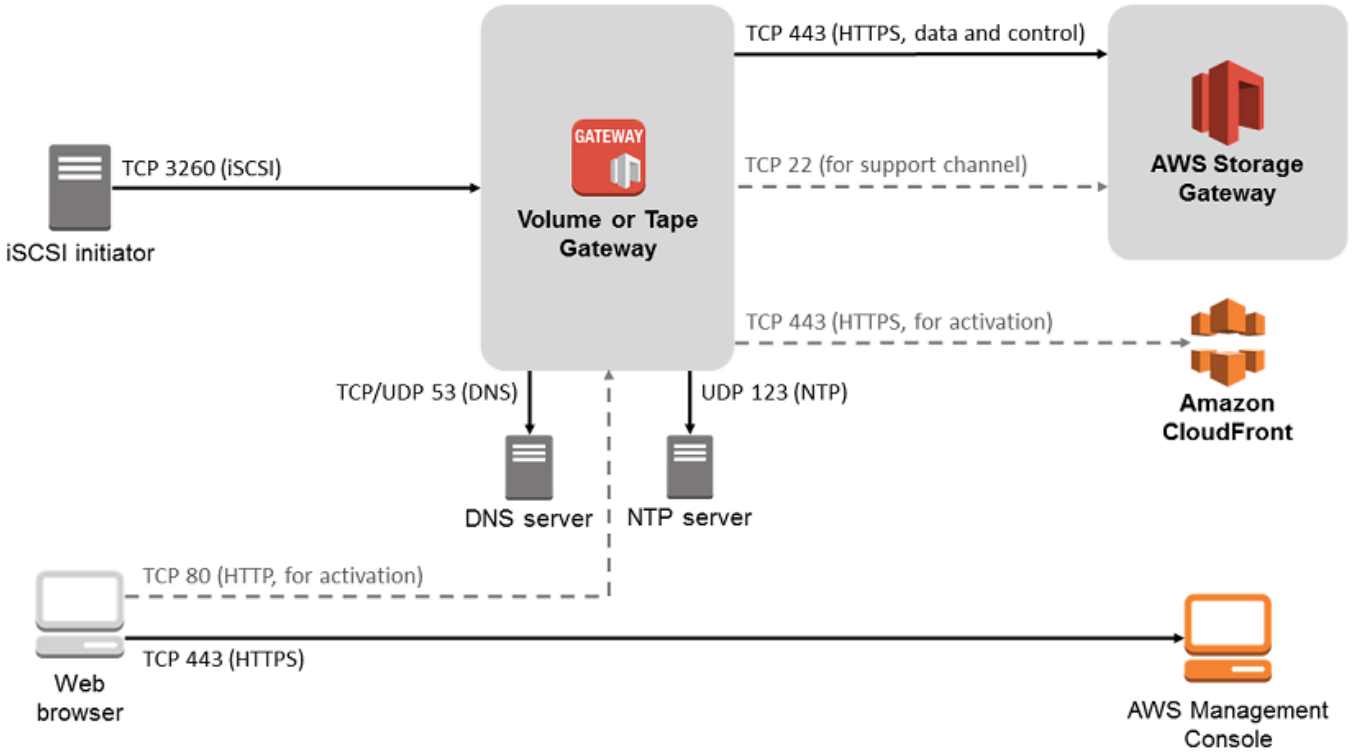
协议	端口	方向	来源	目标位置	如何使用
TCP	443（HTTPS）	出站	Storage Gateway	AWS	用于从 Storage Gateway 到 AWS 服务端点的通信。有关服务端点的信息，请参阅允许通过防火墙和路由器进行 AWS Storage Gateway 访问。
TCP	80 (HTTP)	入站	您从中连接到 AWS 管理控制台的主机。	Storage Gateway	由本地系统用于获取 Storage Gateway 激活密钥。仅在

协议	端口	方向	来源	目标位置	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。端口 80 所需的访问级别取决于网络配置。如果您从 Storage Gateway 管理控制台激活了网关，则您连接到控制台所用的主机必须对网关端口 80 具有访问权限。
TCP/UDP	53 (DNS)	出站	Storage Gateway	域名服务 (DNS) 服务器	用于 Storage Gateway 和 DNS 服务器之间的通信。

协议	端口	方向	来源	目标位置	如何使用
TCP	22 (支持渠道)	出站	Storage Gateway	AWS Support	AWS Support 允许访问您的网关以帮助您解决网关问题。您无需打开此端口即可实现网关的正常操作，但在进行问题排查时需要如此。
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。

卷网关和磁带网关的端口

下图显示了要为卷网关开放的端口。



除了通用端口之外，卷网关还需要下列端口。

协议	端口	方向	来源	目标位置	如何使用
TCP	3260 (iSCSI)	入站	iSCSI 启动程序	Storage Gateway	由本地系统用于连接由网关公开的 iSCSI 目标。

有关端口要求的详细信息，请参阅其他 Storage Gateway 资源部分中的端口要求。

Storage Gateway 硬件设备的网络和防火墙要求

每个 Storage Gateway 硬件设备都需要以下网络服务：

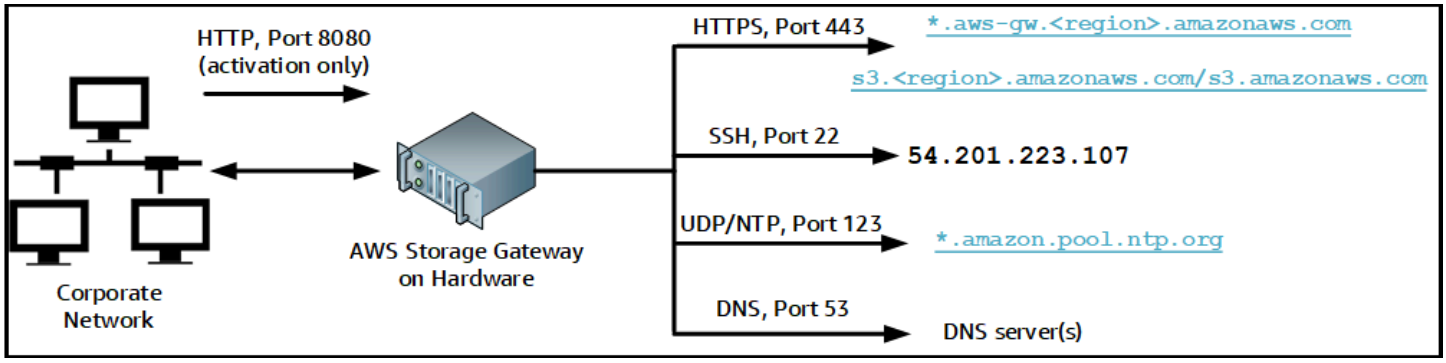
- Internet 访问 - 通过服务器上的任何网络接口实现与 Internet 的永久性网络连接。
- DNS 服务 - 用于硬件设备和 DNS 服务器之间的通信的 DNS 服务。
- 时间同步 - 必须可访问自动配置的 Amazon NTP 时间服务。

- IP 地址 - 已分配的 DHCP 或静态 IPv4 地址。您无法分配 IPv6 地址。

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

1. iDRAC
2. em1
3. em2
4. em3
5. em4

您可以使用 iDRAC 端口进行远程服务器管理。



硬件设备需要以下端口才能运行。

协议	端口	方向	来源	目标位置	如何使用
SSH	22	出站	硬件设备	54.201.223.107	支持渠道
DNS	53	出站	硬件设备	DNS 服务器	名称解析
UDP/NTP	123	出站	硬件设备	*.amazon.pool.ntp.org	时间同步
HTTPS	443	出站	硬件设备	*.amazonaws.com	数据传输

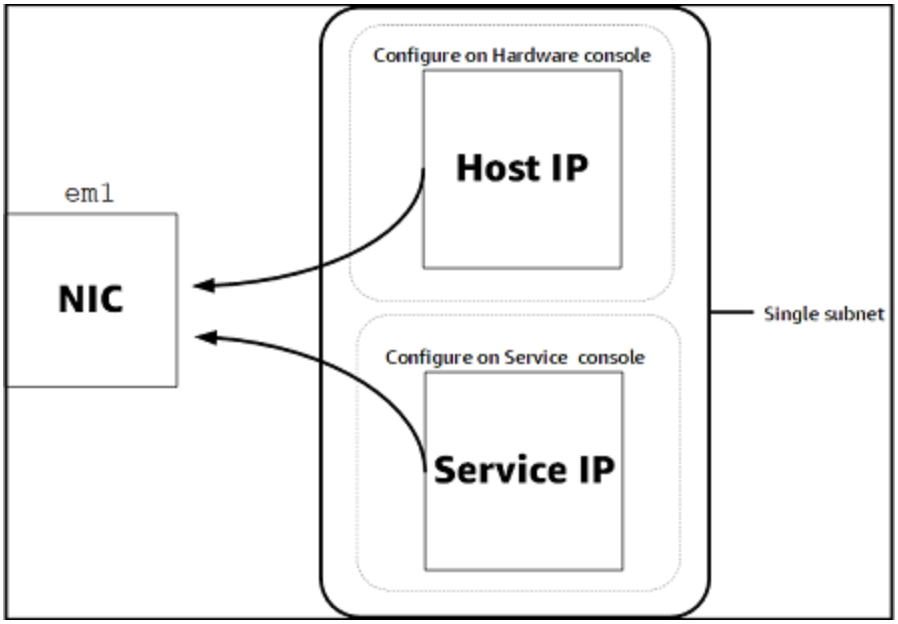
协议	端口	方向	来源	目标位置	如何使用
HTTP	8080	入站	AWS	硬件设备	激活（仅短时）

要按设计的方式运行，硬件设备需要下面所示的网络和防火墙设置：

- 在硬件控制台中配置所有连接的网络接口。
- 确保每个网络接口都位于唯一的子网中。
- 为所有连接的网络接口提供对上图中列出的端点的出站访问权限。
- 配置至少一个网络接口以支持硬件设备。有关更多信息，请参阅配置网络参数。

> **Note**
>
> 有关显示服务器背面及其端口的图示，请参阅在机架上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才能与之通信 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端点与 AWS进行出站通信。

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

> **Important**
>
> 根据网关的 AWS 区域，将服务终端节点中的*##*替换为正确的区域字符串。

所有网关都需要以下服务端点才能执行 head-bucket 操作。

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

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

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

调用 API 需要使用以下网关服务端点。

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

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

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

只有文件网关使用下面显示的 Amazon S3 服务端点。文件网关需要此端点才能访问文件共享映射到的 S3 存储桶。

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

以下示例是美国东部（俄亥俄州）区域 (us-east-2) 中的 S3 服务端点。

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

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

以下是 AWS GovCloud (US) 区域的 S3 服务端点。

```
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 AWS GovCloud （美国西部）区域中 S3 存储桶的 FIPS 服务终端节点。

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

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-有关支持的 AWS 区域和可用于 Storage Gateway 的 AWS 服务终端节点列表，请参阅中的AWS Storage Gateway 终端节点和配额。AWS 一般参考
- Storage Gateway 硬件设备—有关可与硬件设备配合使用的支持 AWS 区域，请参阅中的 Storage Gateway 硬件设备区域。AWS 一般参考

配置 Amazon EC2 网关实例的安全组

安全组会控制发往 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。
- 若要从网关的安全组外部的 Amazon EC2 主机激活您的网关，则需要允许从该主机的 IP 地址通过端口 80 进行传入连接。如果您不能确定激活主机的 IP 地址，则可以打开端口 80、激活网关，然后在完成激活后关闭端口 80 上的访问。
- 仅当使用端口 22 AWS Support 进行故障排除时，才允许访问。有关更多信息，请参阅您 AWS Support 想帮忙排除 EC2 网关故障。

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，也可以 AWS 作为 Amazon EC2 实例运行。

> **Note**
>
> 当制造商结束对某个管理程序版本的一般支持时，Storage Gateway 也将结束对该版本的支持。有关支持特定版本管理程序的详细信息，请参阅制造商的文档。

Storage Gateway 支持以下管理程序版本和主机：

- VMware ESXi Hypervisor（版本 7.0 或 8.0）– 可从 VMware 网站上获取免费 VMware 版本。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、2016、2019 或 2022）- Hyper-V 的免费独立版本可从 Microsoft 下载中心获取。对于此设置，您需要 Microsoft Windows 客户端计算机上的 Microsoft Hyper-V Manager 才能连接到主机。
- 基于 Linux 内核的虚拟机 (KVM) - 免费的开源虚拟化技术。Linux 2.6.20 及更高版本中都包括了 KVM。Storage Gateway 已通过测试，并受到 CentOS/RHEL 7.7、Ubuntu 16.04 LTS 和 Ubuntu

18.04 LTS 发行版的支持。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)。在 Amazon EC2 上只能部署文件、缓存卷和磁带网关类型。有关如何在 Amazon EC2 上部署网关的信息，请参阅部署 Amazon EC2 实例来托管卷网关。
- Storage Gateway 硬件设备 - 对于具有有限虚拟机基础架构的位置，Storage Gateway 提供了物理硬件设备来作为本地部署选项。

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

受支持的 iSCSI 启动程序

部署缓存卷或存储卷网关时，可以在网关上创建 iSCSI 存储卷。

为了连接到这些 iSCSI 设备，Storage Gateway 支持以下 iSCSI 启动程序：

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows 10
- Windows 8.1
- Red Hat Enterprise Linux 5
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7
- VMware ESX 启动程序，它提供一种在 VM 的来宾操作系统中使用启动程序的替代方法

> **Important**
>
> Storage Gateway 不支持来自 Windows 客户端的 Microsoft Multipath I/O (MPIO)。

如果主机使用 Windows Server 失效转移集群 (WSFC) 协调访问，Storage Gateway 支持将多个主机与同一个卷关联。但是，若未使用 WSFC，则不能将多个主机连接到同一个卷 (例如，共享非群集 NTFS/ext4 文件系统)。

正在访问 AWS Storage Gateway

您可以使用 Storage Gateway 管理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。

要允许浏览器访问 Storage Gateway 控制台，请确保您的浏览器可以访问 Storage Gateway API 端点。有关更多信息，请参阅《AWS 一般参考》中的 Storage Gateway 端点和配额。

此外，您还可以使用 AWS Storage Gateway API 以编程方式配置和管理您的网关。有关该 API 的更多信息，请参阅Storage Gateway 的 API 参考。

您还可以使用软件开发 AWS 工具包开发与 Storage Gateway 交互的应用程序。适用于 Java、.Net 和 PHP 的 AWS 软件开发工具包包含底层的 Storage Gateway API，简化了编程任务。有关下载开发工具包库的信息，请参阅示例代码库。

使用 Storage Gateway 硬件设备

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

硬件设备是一个高性能的 1U 服务器，您可以将其部署在您的数据中心或企业防火墙内的本地位置。在购买并激活您的硬件设备时，激活过程会将硬件设备与您的 Amazon Web Services 账户关联。在激活后，您的硬件设备在控制台的硬件设备概述页面中显示为网关。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。

在以下几节中，您可以找到有关如何订购、设置、配置、激活、启动和使用 Storage Gateway 硬件设备的说明。

主题

- 支持的 AWS 区域
- 设置硬件设备
- 在机架上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
- 创建网关
- 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

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

设置硬件设备

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与设备的始终在线连接 AWS 并激活设备。激活会将您的设备与在激活过程中使用的 Amazon Web Services 账户关联。在激活设备后，您可以在 Storage Gateway 控制台中启动文件、卷或磁带网关。

> **Note**
>
> 您有责任确保硬件设备固件完好无损 up-to-date。

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，请参阅在机架上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. 在您选择的 AWS 区域的主机硬件设备概述页面上激活硬件设备。有关更多信息，请参阅激活硬件设备。
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。这样做可以为低延迟访问中的数据提供更大的缓存 AWS。如果您订购的是 5 TB 型号，则可以购买五个 1.92 TB SSD（固态硬盘），将可用存储增加到 12 TB。

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

1. 将硬件设备重置为出厂设置。有关如何执行该操作的说明，请联系 Amazon Web Services 支持。
2. 将五个 1.92 TB SSD 添加到设备中。

网络接口卡选项

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

- 10G-Base-T NIC 配置：
  - 对于 10G，使用 CAT6 线缆；对于 1G，使用 CAT5(e) 线缆
- 10G DA/SFP+ NIC 配置：

- 使用最长 5 米的 Twinax 铜质直连线缆
- 戴尔/英特尔兼容 SFP+ 光学模块（SR 或 LR）
- 适用于 1G-Base-T 或 10G-Base-T 的 SFP/SFP+ 铜质收发器

在机架上安装硬件设备并将其连接到电源

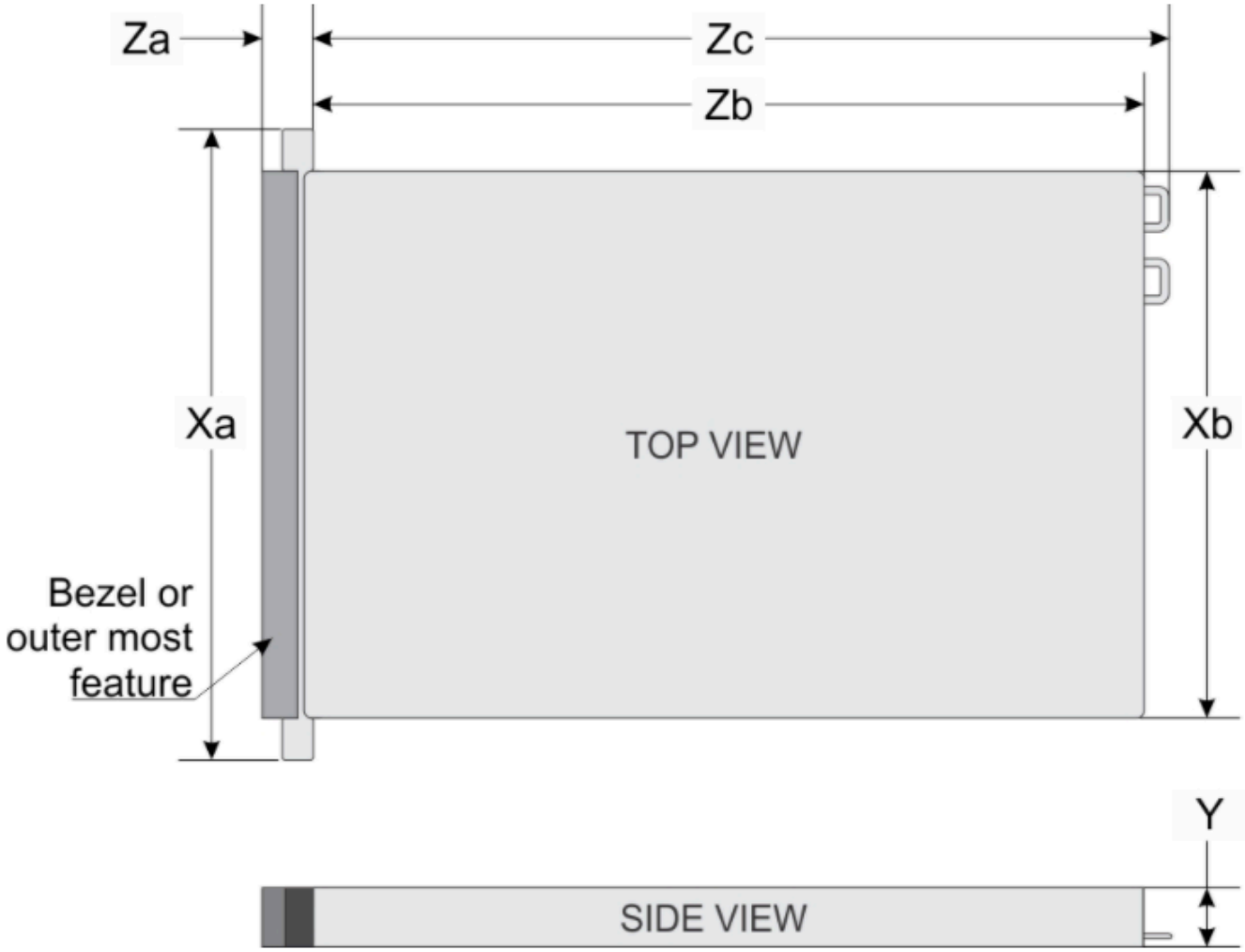
在拆开 Storage Gateway 硬件设备的包装后，请按照箱内包含的说明操作，在机架上安装服务器。您的设备具有 1U 外形规格，可安装在符合国际电工委员会 (IEC) 标准的 19 英寸机架中。

要安装您的硬件设备，需要以下组件：

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

硬件设备尺寸

硬件设备尺寸，包括安装支架和挡板。



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)

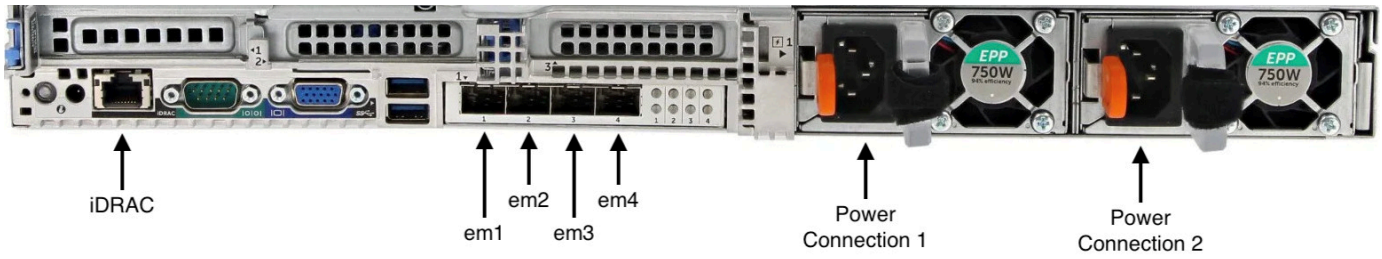
硬件设备尺寸，包括安装支架和挡板。

将硬件设备连接至电源

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

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。
   带有网络和电源连接器标签的硬件设备背面。

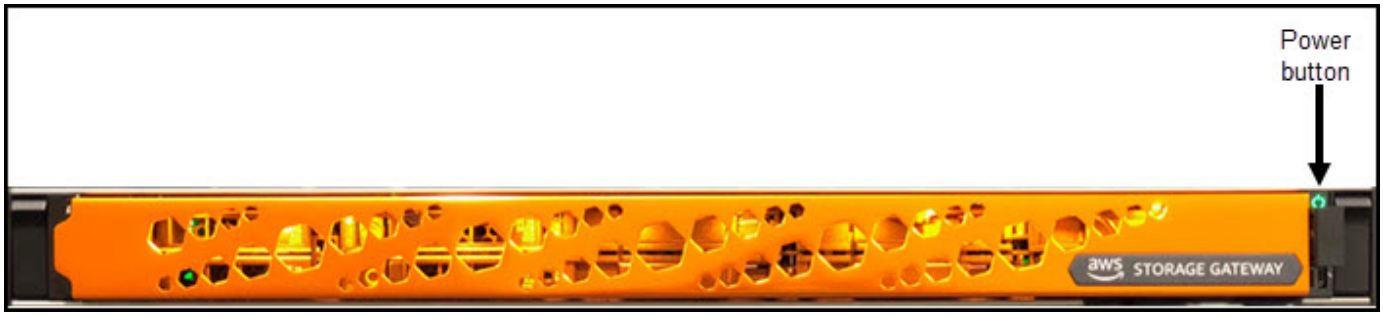
   带有网络和电源连接器标签的硬件设备背面。

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。将用于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。
   带有电源按钮标签的硬件设备正面。

   带有电源按钮标签的硬件设备正面。

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专用于 AWS 配置初始网络参数的用户界面。您可以配置这些参数来将设备连接到 AWS 并开启支持渠道，以便 Amazon Web Services 支持人员可以进行故障排除。

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)。

硬件设备控制台“设置密码”对话框屏幕。

硬件设备控制台“设置密码”对话框屏幕。

此时您位于硬件控制台中，如下所示。
硬件设备控制台主菜单，其中显示了连接和菜单选项。

硬件设备控制台主菜单，其中显示了连接和菜单选项。

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[在机架上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，让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。
   硬件设备控制台配置网络屏幕。

硬件设备控制台配置网络屏幕。

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，请在 em1 部分中选择静态，然后按 Enter 键来查看如下所示的“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**
   >
   > 如果您配置任何其他接口，则该接口必须为要求中列出的 AWS 端点提供相同的始终在线连接。

硬件设备控制台“将 NIC 配置为静态 IP”屏幕。

硬件设备控制台“将 NIC 配置为静态 IP”屏幕。

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

配置 IP 地址后，您可以在 AWS Storage Gateway 控制台的 “硬件” 页面上输入此 IP 地址以激活您的硬件设备。激活过程会验证您的硬件设备是否具有适当的安全凭证并将其注册到您的 AWS 账户。

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

激活 Storage Gateway 硬件设备

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

   > **Note**
   >
   > 如果只激活，必须满足以下条件：
   >
   > - 您的浏览器必须与您的硬件设备位于同一网络上。
   > - 您的防火墙必须允许在 8080 端口上对设备的入站流量进行 HTTP 访问。

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

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

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

此时，硬件设备概览页面上会出现一个横幅，指示硬件设备已成功激活。

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

下一步

创建网关

创建网关

您可以在硬件设备上创建 S3 文件网关、FSx 文件网关、磁带网关或卷网关。

在硬件设备上创建网关

1. 登录 AWS Management Console 并打开 Storage Gateway 控制台，网址为 https://console.aws.amazon.com/storagegateway/home。
2. 选择 Hardware (硬件)。
3. 选择要在其上创建网关的已激活硬件设备，然后选择创建网关。
4. 按照创建网关中所述的程序设置、连接和配置所选的网关类型。

在 Storage Gateway 控制台中完成网关创建后，Storage Gateway 软件会自动在硬件设备上开始安装。需要等待 5-10 分钟，网关才会在控制台中显示为在线。

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

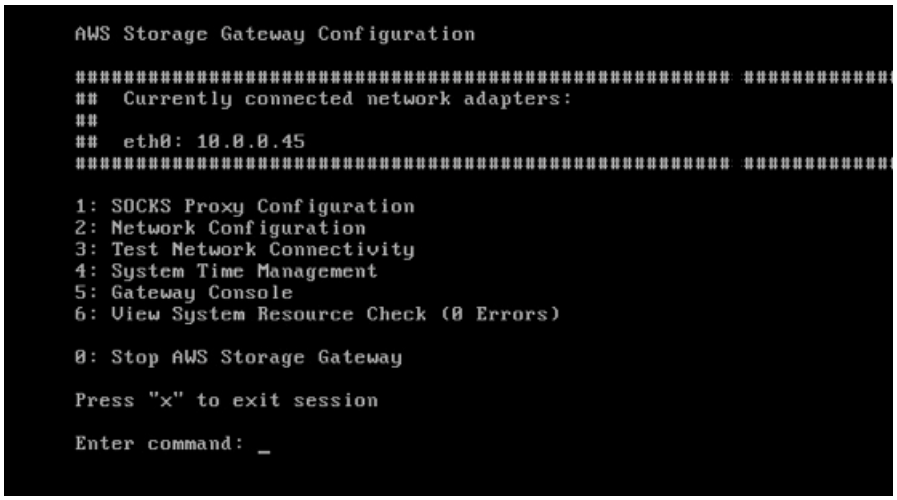
为网关配置 IP 地址

在激活硬件设备之前，为其物理网络接口分配一个 IP 地址。您已激活设备并在设备上启动了 Storage Gateway，现在您需要为在硬件设备上运行的 Storage Gateway 虚拟机分配另一个 IP 地址。要向已安装在您的硬件设备上的网关分配静态 IP 地址，请从该网关的本地控制台配置 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the section called “从 Storage Gateway 控制台设置本地控制台密码”：
5. 导航到网关本地控制台的网络设置页面，如下所示。
   网关本地控制台配置页面，其中显示了网络配置选项。



   网关本地控制台配置页面，其中显示了网络配置选项。
6. 键入 2 以转到如下所示的 Network Configuration (网络配置) 页面。
   网关本地控制台网络配置页面，其中显示了 DHCP 和静态 IP 选项。

   网关本地控制台网络配置页面，其中显示了 DHCP 和静态 IP 选项。

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，从而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。在您的网关类型对应的配置网关页面上继续安装。有关说明，请参阅配置您的卷网关。

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. 在 Storage Gateway 控制台的硬件页面上，选择要删除的硬件设备。
2. 对于 Actions (操作)，选择 Remove Gateway (删除网关)。此时会显示确认对话框。
3. 确认要从指定的硬件设备中删除网关软件，然后在确认框中键入单词 remove 并选择删除。

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

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

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

删除硬件设备

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

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

创建网关

本页上的概述主题简要介绍了 Storage Gateway 创建过程的工作原理。有关使用 Storage Gateway 控制台创建特定类型网关的 step-by-step 过程，请参阅创建卷网关。

概述 - 网关激活

网关激活包括设置网关，将其连接到 AWS，然后查看您的设置并激活它。

设置网关

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

连接到 AWS

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

检查并激活

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

概述 - 网关配置

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

概述 - 存储资源

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

创建卷网关

在此部分中，您可以找到有关如何创建和使用卷网关的说明。

主题

- 创建网关
- 创建卷
- 使用卷
- 备份您的卷

创建网关

在此部分中，您可以找到有关如何下载、部署和激活卷网关的说明。

主题

- 设置卷网关
- 将卷网关连接到 AWS
- 检查设置并激活卷网关
- 配置卷网关

设置卷网关

设置新的卷网关

1. 打开 AWS Management Console https://console.aws.amazon.com/storagegateway/home/，然后选择要创建网关 AWS 区域 的位置。
2. 选择创建网关来打开设置网关页面。
3. 在网关设置部分，执行以下操作：

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

b. 对于网关时区，选择要在其中部署网关的地区的本地时区。

4. 在网关选项部分中，对于网关类型，选择卷网关，然后选择您的网关要使用的卷类型。可从以下选项中进行选择：

   - 缓存卷 - 将您的主数据存储在 Amazon S3 中，并在高速缓存中本地保留经常访问的数据，以便更快地访问。
   - 存储卷 - 将您的所有数据存储在本地，同时也将数据异步备份到 Amazon S3。使用这种卷类型的网关无法部署在 Amazon EC2 上。

5. 在平台选项部分中，执行以下操作：

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

      - VMware ESXi - 使用 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 Linux KVM 下载、部署和配置网关虚拟机。
      - Amazon EC2 - 配置并启动用于托管网关的 Amazon EC2 实例。此选项不适用于存储卷网关。
      - 硬件设备-订购专用的物理硬件设备 AWS 来托管您的网关。

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

6. 选择下一步以继续。

现在，您的网关已设置完毕，您需要选择您想要的网关连接和通信方式 AWS。有关说明，请参阅将您的卷网关连接到 AWS。

将卷网关连接到 AWS

将新的卷网关连接到 AWS

1. 如果您尚未完成设置卷网关中所述的步骤，请完成这些步骤。完成后，选择下一步，在 Storage Gateway 控制台中打开连接到 AWS 页面。

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

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

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

   - VPC 托管 - 您的网关通过与 VPC 的私有连接与 AWS 进行通信，从而使您可以控制自己的网络设置。如果选择此选项，则必须指定现有 VPC 端点，方法是从下拉菜单中选择其 VPC 端点 ID，或者提供其 VPC 端点 DNS 名称或 IP 地址。

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

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

     您可以通过从虚拟机管理程序客户端登录到网关的本地控制台来获取网关 IP 地址，或从 Amazon EC2 实例详情页面复制网关 IP 地址。

   - 激活密钥 - 在相应字段中提供网关的激活密钥。您可以使用网关的本地控制台来生成激活密钥。如果网关的 IP 地址不可用，请选择此选项。

4. 选择下一步以继续。

既然您已经选择了网关的连接方式 AWS，那么您需要激活网关。有关说明，请参阅查看设置并激活您的卷网关。

检查设置并激活卷网关

激活新的卷网关

1. 如果尚未完成以下主题中所述的程序，请先完成这些程序：

   - 设置卷网关

- 将您的卷网关连接到 AWS

完成后，选择下一步，在 Storage Gateway 控制台中打开检查并激活页面。

2. 查看页面上每个部分的初始网关详细信息。
3. 如果某个部分包含错误，请选择编辑来返回到相应的设置页面并进行更改。

> **Note**
>
> 创建网关后，您无法修改网关选项或连接设置。

4. 选择激活网关以继续。

您已经激活了网关，现在需要进行首次配置，以便分配本地存储磁盘和配置日志记录。有关说明，请参阅配置卷网关。

配置卷网关

对新的卷网关执行首次配置

1. 如果尚未完成以下主题中所述的程序，请先完成这些程序：

   - 设置卷网关
   - 将您的卷网关连接到 AWS
   - 检查设置并激活卷网关

   完成后，选择下一步，在 Storage Gateway 控制台中打开配置网关页面。

2. 在配置存储部分，使用下拉菜单为 CACHE STORAGE 至少分配一个容量至少为 165 GiB 的磁盘，为 UPLOAD BUFFER 至少分配一个容量至少为 150 GiB 的磁盘。本节中列出的本地磁盘对应于您在主机平台上预配置的物理存储。
3. 在CloudWatch 日志组部分，选择如何设置 Amazon CloudWatch Logs 以监控网关的运行状况。可从以下选项中进行选择：

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

> **Note**
>
> 要接收 Storage Gateway 运行状况日志，您的日志组资源策略中必须包含以下权限。将*#########*替换为您部署的特定日志组 resourceArn 信息。
>
> ```
> "Sid": "AWSLogDeliveryWrite20150319",
>       "Effect": "Allow",
>       "Principal": {
>         "Service": [
>           "delivery.logs.amazonaws.com"
>         ]
>       },
>       "Action": [
>         "logs:CreateLogStream",
>         "logs:PutLogEvents"
>       ],
>       "Resource": "arn:aws:logs:eu-west-1:1234567890:log-group:/foo/bar:log-stream:*"
> ```
>
> 仅当您希望权限明确应用于单个日志组时，才需要 “资源” 元素。

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

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

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

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

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

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

您已经创建了网关，现在您需要创建一个供网关使用的卷。有关说明，请参阅创建卷。

创建卷

之前，您已分配添加到 VM 缓存存储和上传缓冲区的本地磁盘。您现在创建应用程序将向其读取和写入数据的存储卷。网关将在缓存存储中本地保留卷的最近访问的数据，并将数据异步传输到 Amazon S3。对于存储卷，您已分配添加到 VM 上传缓冲区的本地磁盘和应用程序数据。

> **Note**
>
> 您可以使用 AWS Key Management Service (AWS KMS) 对写入缓存卷并存储在 Amazon S3 中的数据进行加密。目前，您可以按照《AWS Storage Gateway API 参考》来执行此操作。有关更多信息，请参阅 CreateCachedisciVol ume 或。create-cached-iscsi-volume

创建卷

1. 打开 Storage Gateway 控制台，网址为 https://console.aws.amazon.com/storagegateway/home。
2. 在 Storage Gateway 控制台中，选择创建卷。
3. 在 Create volume (创建卷) 对话框中，为 Gateway (网关) 选择网关。
4. 对于缓存卷，在容量中输入容量。

   对于存储卷，从列表中选择 Disk ID (磁盘 ID) 值。
5. 对于卷内容，您的选择取决于您正为其创建卷的网关的类型。

   对于缓存卷，您可使用以下选项：

- 创建新的空卷。
- 基于 Amazon EBS 快照创建卷。如果选择此选项，请为 EBS snapshot ID (EBS 快照 ID) 提供一个值。

> **Note**
>
> Storage Gateway 不支持根据 AWS Marketplace 卷的快照来创建缓存卷。

- 从上次卷恢复点克隆。如果选择此选项，请为 Source volume (源卷) 选择一个卷 ID。如果区域中没有任何卷，则不会显示此选项。

对于存储卷，您可使用以下选项：

- 创建新的空卷。
- 基于快照创建卷。如果选择此选项，请为 EBS snapshot ID (EBS 快照 ID) 提供一个值。
- 在磁盘上保留现有数据

6. 在 iSCSI 目标名称 中输入名称。

   目标名称可包含小写字母、数字句点 (.) 和连词符 (-)。发现后，此目标名称显示为 iSCSI Microsoft 启动程序 UI 的目标选项卡中的 iSCSI 目标节点名称。例如，名称 `target1` 将显示为 `iqn.1007-05.com.amazon:target1`。确保目标名称在存储区域网络 (SAN) 内具有全局唯一性。

7. 验证 Network interface (网络接口) 设置是否已选择 IP 地址，或者为 Network interface (网络接口) 选择 IP 地址。对于 Network interface (网络接口)，为网关 VM 配置的每个适配器分别显示一个 IP 地址。如果网关 VM 配置为仅使用一个网络适配器，则不会显示Network interface (网络接口) 下拉列表，因为只有一个 IP 地址。

   您的 iSCSI 目标将在您选择的网络适配器上可用。

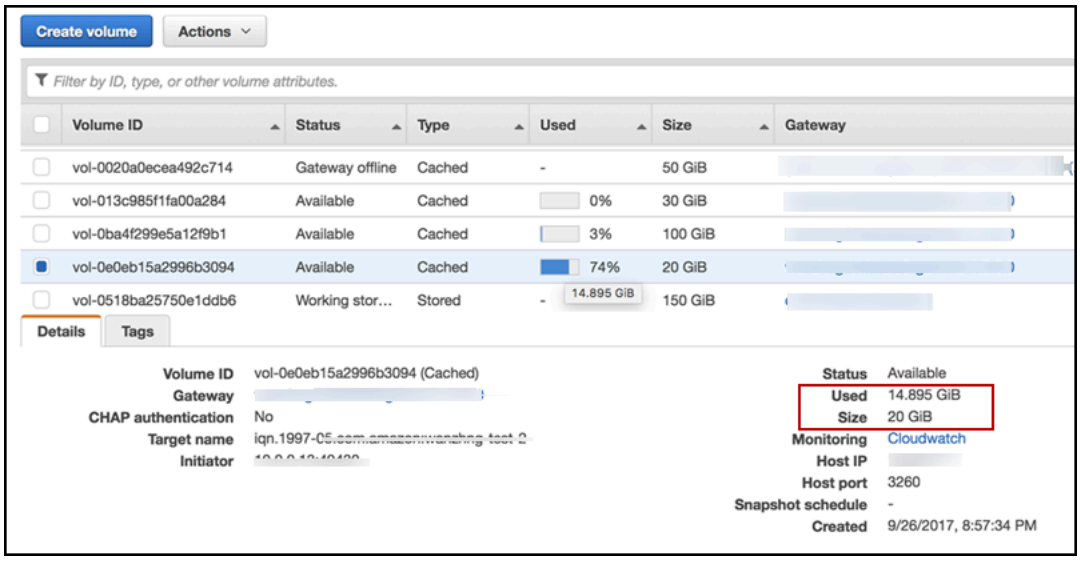
   如果已将网关定义为使用多个网络适配器，请选择存储应用程序应该用于访问卷的 IP 地址。有关配置多个网络适配器的信息，请参阅将网关配置为使用多个 NIC。

   > **Note**
   >
   > 选择网络适配器后，将无法再更改此设置。

8. （可选）对于 Tags (标签)，输入键和值以将标签添加到您的卷。标签是帮助您管理、筛选和搜索卷的区分大小写的键/值对。
9. 选择创建卷。

   如果您之前已在此区域中创建了卷，则会看到它们在 Storage Gateway 控制台中列出。

   此时将显示 Configure CHAP Authentication (配置 CHAP 身份验证) 对话框。此时，您可以为卷配置质询握手身份验证协议 (CHAP)，也可以选择取消并稍后配置 CHAP。有关 CHAP 设置的更多信息，请参阅为您的卷配置 CHAP 身份验证。



如果不想设置 CHAP，请开始使用您的卷。有关更多信息，请参阅使用卷。

为您的卷配置 CHAP 身份验证

CHAP 通过要求进行身份验证才能访问存储卷目标来预防反演攻击。在 Configure CHAP Authentication (配置 CHAP 身份验证) 对话框中，提供相应的信息以便为您的卷配置 CHAP。

配置 CHAP

1. 选择要配置 CHAP 的卷。
2. 对于 Actions (操作)，选择 Configure CHAP authentication (配置 CHAP 身份验证)。
3. 对于启动程序名称，请输入启动程序的名称。
4. 对于启动程序密钥，请输入用于验证 iSCSI 启动程序身份的密码。
5. 对于目标密钥，请输入用于验证双向 CHAP 目标身份的密码。
6. 选择保存来保存您的输入。

有关设置 CHAP 身份验证的更多信息，请参阅 为 iSCSI 目标配置 CHAP 身份验证。

下一步

使用卷

使用卷

在下文中，您可以找到有关如何使用卷的说明。要使用卷，应首先将卷作为 iSCSI 目标连接到客户端，然后将卷初始化和格式化。

主题

- 将卷连接到客户端
- 将卷初始化和格式化
- 测试网关
- 我从这里可以继续进行哪些内容？

将卷连接到客户端

使用客户端中的 iSCSI 启动程序来连接到卷。在以下过程结束时，这些卷将成为 客户端上的本地设备。

> **Important**
>
> 如果主机使用 Windows Server 失效转移集群 (WSFC) 协调访问，您可以使用 Storage Gateway 将多个主机连接到同一个卷。若未使用 WSFC，则不能将多个主机连接到同一个卷，例如，通过共享非群集 NTFS/ext4 文件系统。

主题

- 连接到 Microsoft Windows 客户端
- 连接到 Red Hat Enterprise Linux 客户端

连接到 Microsoft Windows 客户端

以下过程显示连接到 Windows 客户端时需要遵循的步骤摘要。有关更多信息，请参阅连接 iSCSI 启动程序。

连接到 Windows 客户端

1. 启动 iscsicpl.exe。
2. 在 iSCSI Initiator Properties (iSCSI 发起程序属性) 对话框中，选择 Discovery (发现) 选项卡，然后选择 Discovery Portal (发现门户)。
3. 在 Discover Target Portal (发现目标门户) 对话框中，对于“IP address or DNS name (IP 地址或 DNS 名称)”，键入 iSCSI 目标的 IP 地址。
4. 将新的目标门户连接到网关上的存储卷目标。
5. 选择该目标，然后选择 Connect (连接)。
6. 在 Targets (目标) 选项卡中，确保目标状态的值为 Connected (已连接)（表示已连接目标），然后单击 OK (确定)。

连接到 Red Hat Enterprise Linux 客户端

以下过程显示连接到 Red Hat Enterprise Linux (RHEL) 客户端时需要遵循的步骤摘要。有关更多信息，请参阅连接 iSCSI 启动程序。

将 Linux 客户端连接到 iSCSI 目标

1. 安装 iscsi-initiator-utils RPM 软件包。

   您可以使用下面的命令来安装该包。

   ```
   sudo yum install iscsi-initiator-utils
   ```

2. 确保 iSCSI 守护进程正在运行。

   对于 RHEL 5 或 RHEL 6，请使用以下命令。

   ```
   sudo /etc/init.d/iscsi status
   ```

   对于 RHEL 7，请使用以下命令。

```
sudo service iscsid status
```

3. 发现为网关定义的卷或 VTL 设备目标。使用以下发现命令。

```
sudo /sbin/iscsiadm --mode discovery --type sendtargets --portal [GATEWAY_IP]:3260
```

发现命令的输出内容应类似如下示例输出内容。

对于卷网关：*[GATEWAY_IP]*:3260, 1 iqn.1997-05.com.amazon:myvolume

对于磁带网关：iqn.1997-05.com.amazon:*[GATEWAY_IP]*-tapedrive-01

4. 连接到目标。

确保在连接命令中指定正确的 *[GATEWAY_IP]* 和 IQN。

使用以下命令。

```
sudo /sbin/iscsiadm --mode node --targetname
 iqn.1997-05.com.amazon:[ISCSI_TARGET_NAME] --portal [GATEWAY_IP]:3260,1 --login
```

5. 验证卷是否已附加到客户端机器 (启动程序)。为此，请使用以下命令。

```
ls -l /dev/disk/by-path
```

命令的输出内容应类似如下示例输出内容。

lrwxrwxrwx. 1 root root 9 Apr 16 19:31 ip-*[GATEWAY_IP]*:3260-iscsi-iqn.1997-05.com.amazon:myvolume-lun-0 -> ../../sda

设置启动程序后，我们强烈建议您按自定义您的 Linux iSCSI 设置中介绍的方式自定义 iSCSI 设置。

将卷初始化和格式化

使用客户端中的 iSCSI 启动程序连接到卷之后，将卷初始化并格式化。

主题

- 在 Microsoft Windows 中初始化并格式化卷

- 在 Red Hat Enterprise Linux 中初始化并格式化卷

在 Microsoft Windows 中初始化并格式化卷

使用以下过程在 Windows 中初始化并格式化卷。

初始化并格式化存储卷

1. 启动 **diskmgmt.msc** 以打开 Disk Management (磁盘管理) 控制台。
2. 在 Initialize Disk (初始化磁盘) 对话框中，将卷作为 MBR (Master Boot Record) (MBR (主启动记录)) 分区进行初始化。选择分区格式时，您应该考虑所连接卷的类型（缓存卷或存储卷），如下表所示。

分区形式	用于以下情况
MBR (主启动记录)	• 如果网关是一个存储卷且存储卷的大小限制为 1 TiB。 • 如果网关是一个缓存卷且存储卷的大小小于 2 TiB。
GPT (GUID 分区表)	如果网关的存储卷为 2 TiB 或者大小更大。

3. 创建简单卷：
   a. 使卷处于联机状态，以将其初始化。所有可用的卷均显示在磁盘管理控制台中。
   b. 打开磁盘的上下文（右键单击）菜单，然后选择 New Simple Volume (新建简单卷)。

      > **Important**
      >
      > 请谨慎处理，避免错误地将其他磁盘格式化。检查并确保您正在格式化的磁盘匹配您分配给网关 VM 的本地磁盘大小，并且其状态为 Unallocated (未分配)。

   c. 指定磁盘的最大大小。
   d. 为卷分配驱动器盘符或路径，然后通过选择 Perform a quick format (执行快速格式化) 来将卷格式化。

> **Important**
>
> 我们强烈建议您对缓存卷使用 Perform a quick format (执行快速格式化)。这样做可减少初始化 I/O、减小初始快照大小并使卷尽快可用。它还可避免因完全格式化过程而使用缓存卷空间。

> **Note**
>
> 格式化卷所需的时间取决于卷的大小。该过程可能需要几分钟才能完成。

在 Red Hat Enterprise Linux 中初始化并格式化卷

使用以下过程在 Red Hat Enterprise Linux (RHEL) 中初始化并格式化卷。

初始化并格式化存储卷

1. 将目录更改为 `/dev` 文件夹。
2. 运行 `sudo cfdisk` 命令。
3. 使用以下命令识别新卷。要查找新卷，您可以列出卷的分区布局。

   ```
   $ lsblk
   ```

   对于未分区的新卷，系统会显示“unrecognized volumes label”(无法识别卷标签) 错误。
4. 将新卷初始化。选择分区格式时，您应该考虑所连接卷的大小和类型 (缓存或存储)，如下表所示。

分区形式	用于以下情况
MBR (主启动记录)	• 如果网关是一个存储卷且存储卷的大小限制为 1 TiB。 • 如果网关是一个缓存卷且存储卷的大小小于 2 TiB。
GPT (GUID 分区表)	如果网关的存储卷为 2 TiB 或者大小更大。

对于 MBR 分区，使用以下命令：`sudo parted /dev/`*`your volume`* `mklabel msdos`

对于 GPT 分区，使用以下命令：`sudo parted /dev/`*`your volume`* `mklabel gpt`

5. 使用以下命令创建分区。

   ```
   sudo parted -a opt /dev/your volume mkpart primary file system 0% 100%
   ```

6. 使用以下命令为分区分配驱动器盘符并创建文件系统。

   ```
   sudo mkfs -L datapartition /dev/your volume
   ```

7. 使用以下命令装载文件系统。

   ```
   sudo mount -o defaults /dev/your volume /mnt/your directory
   ```

测试网关

可通过执行以下任务来测试卷网关设置：

1. 将数据写入卷。
2. 拍摄快照。
3. 将快照还原到另一个卷。

您可以通过对卷进行快照备份并将快照存储在中来验证网关的设置 AWS。然后将此快照还原到新卷。您的网关将指定快照中的数据复制 AWS 到新卷中。

> **Note**
>
> 不支持从加密的 Amazon Elastic Block Store (Amazon EBS) 卷还原数据。

在 Microsoft Windows 上创建存储卷的 Amazon EBS 快照

1. 在 Windows 计算机上，将一些数据复制到您的映射存储卷上。

   复制的数据量对于本示范无关紧要。一个小文件即足够用来展示还原过程。

2. 在 Storage Gateway 控制台的“导航”窗格中，选择卷。
3. 选择为网关创建的存储卷。

   此网关应仅有一个存储卷。选择卷时，会显示它的属性。

4. 对于 Actions (操作)，选择 Create EBS snapshot (创建 EBS 快照) 以创建卷的快照。

根据磁盘上的数据量以及上传带宽的大小，完成快照可能需要几秒钟的时间。记录您从中创建快照的卷的 ID。您将使用该 ID 来查找该快照。

5. 在 Create EBS Snapshot (创建 EBS 快照) 对话框中，提供快照的描述。
6. （可选）对于 Tags (标签)，输入键和值以将标签添加到快照。标签是帮助您管理、筛选和搜索快照的区分大小写的键/值对。
7. 选择创建快照。您的快照存储为 Amazon EBS 快照。请记下您的快照 ID。快照列中显示为您的卷创建的快照数目。
8. 在 EBS 快照列中，选择为其创建快照的卷的链接，以便在 Amazon EC2 控制台上查看您的 EBS 快照。

将快照还原到另一个卷

请参阅 创建卷。

我从这里可以继续进行哪些内容？

在前面的章节中，您创建和预配置了网关，并将主机连接到了网关的存储卷。您将数据添加到了网关的 iSCSI 卷，拍摄了卷的快照，将快照还原成了新卷，连接到了新卷，并且验证了数据显示在新卷上。

完成本练习后，请考虑以下各项：

- 如果您计划继续使用网关，则应阅读针对实际工作负载配置更恰当的上传缓冲区大小的相关内容。有关更多信息，请参阅针对实际工作负载调整卷网关存储的大小。
- 如果您不打算继续使用网关，请考虑删除网关以避免产生任何费用。有关更多信息，请参阅清除不需要的资源。

本指南的其他章节介绍如何进行如下操作：

- 要详细了解存储卷以及如何管理这些卷，请参阅管理您的网关。
- 如需排除网关问题，请参见 排查网关问题。
- 要优化网关，请参阅优化网关性能。
- 要了解 Storage Gateway 指标以及如何监控网关运行情况，请参阅监控 Storage Gateway。
- 要了解有关配置网关的 iSCSI 目标以存储数据的更多信息，请参阅将卷连接到 Windows 客户端。

要了解如何针对实际工作负载调整卷网关存储的大小并清除不需要的资源，请参阅以下各节。

针对实际工作负载调整卷网关存储的大小

此时，您就有了一个可以运行的简单网关。不过，用来创建网关的假定不适合实际工作负载。如果要将此网关用于实际工作负载，则需要执行两项操作：

1. 适当设置上传缓冲区的大小。
2. 如果尚未为上传缓冲区设置监控，请进行设置。

随后，您可以了解如何完成这两个任务。如果已激活缓存卷的网关，您还需要针对实际工作负载设置缓存存储空间的大小。

如需为网关缓存设置配置上传缓冲区和缓存存储空间的大小

- 使用 确定要分配的上传缓冲区的大小 中显示的用于配置上传缓冲区大小的公式。我们强烈建议您至少分配 150 GiB 的上传缓冲区。如果上传缓冲区公式得出了小于 150 GiB 的值，请使用 150 GiB 作为您分配的上传缓冲区。

  上传缓冲区公式考虑了从应用程序到网关的吞吐量与从网关到 AWS网关的吞吐量之间的差异乘以您预计写入数据的时间。例如，假定您的应用程序每天 12 个小时以每秒 40 MB 的速度向网关写入文本数据并且您的网络吞吐量为 12 MB 每秒。假定文本数据压缩系数为 2:1，公式就会指定您大约需要分配 675 GiB 的上传缓冲区空间。

为存储设置配置上传缓冲区的大小

- 使用 确定要分配的上传缓冲区的大小 中讨论的公式。我们强烈建议您至少分配 150 GiB 的上传缓冲区。如果上传缓冲区公式得出了小于 150 GiB 的值，请使用 150 GiB 作为您分配的上传缓冲区。

  上传缓冲区公式考虑了从应用程序到网关的吞吐量与从网关到 AWS网关的吞吐量之间的差异乘以您预计写入数据的时间。例如，假定您的应用程序每天 12 个小时以每秒 40 MB 的速度向网关写入文本数据并且您的网络吞吐量为 12 MB 每秒。假定文本数据压缩系数为 2:1，公式就会指定您大约需要分配 675 GiB 的上传缓冲区空间。

如需监控您的上传缓冲区

1. 打开 Storage Gateway 控制台，网址为 https://console.aws.amazon.com/storagegateway/home。

2. 选择网关选项卡，选择详细信息选项卡，然后查找上传缓冲区已用容量字段，以查看网关的当前上传缓冲区。
3. 设置一个或多个警报以通知您有关上传缓冲区使用率的信息。

   我们强烈建议您在 Amazon CloudWatch 控制台中创建一个或多个上传缓冲区警报。例如，您可以根据需要设置使用量报警，并设置超出某使用量便触发操作的报警。此操作可能会添加更多上传缓冲区空间。有关更多信息，请参阅如需为网关的上传缓冲区设置上阈值警报。

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. 删除任何快照。有关说明，请参阅删除快照。
2. 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。
3. 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。

备份您的卷

使用 Storage Gateway 有助于保护使用 Storage Gateway 卷进行云端备份存储的本地业务应用程序。在 Storage Gateway 或 AWS Backup中，您可以使用本机快照计划程序来备份本地 Storage Gateway 卷。在这两种情况下，Storage Gateway 卷备份都以 Amazon EBS 快照形式存储在 Amazon Web Services 中。

主题

- 使用 Storage Gateway 来备份卷
- AWS Backup 使用备份您的卷

使用 Storage Gateway 来备份卷

您可以使用 Storage Gateway 管理控制台，通过创建 Amazon EBS 快照并将快照存储在 Amazon Web Services 中来备份您的卷。您可以创建一次性快照或者设置由 Storage Gateway 管理的快照计划。您可以在以后使用 Storage Gateway 控制台将快照还原到新卷。有关如何从 Storage Gateway 备份和管理备份的信息，请参阅以下主题：

- 测试网关
- 创建一次性快照
- 克隆卷

AWS Backup 使用备份您的卷

AWS Backup 是一项集中式备份服务，可让您轻松且经济实惠地在 Amazon Web Services Cloud 和本地 AWS 服务中跨服务备份应用程序数据。这样做可以帮助您满足业务和监管备份合规性要求。 AWS Backup 通过提供一个可以执行以下操作的中心位置，使保护 AWS 存储卷、数据库和文件系统变得简单：

- 配置和审核要备份的 AWS 资源。
- 计划自动备份。
- 设置保留策略。
- 监控所有最近的备份和还原活动。

由于 Storage Gateway 与集成 AWS Backup，因此它允许客户使用 AWS Backup 备份使用 Storage Gateway 卷进行云支持的存储的本地业务应用程序。 AWS Backup 支持缓存卷和存储卷的备份和恢复。有关的信息 AWS Backup，请参阅 AWS Backup 文档。有关的信息 AWS Backup，请参阅什么是 AWS Backup？ 在《AWS Backup 用户指南》中。

您可以使用来管理 Storage Gateway 卷的备份 AWS Backup 和恢复操作，无需创建自定义脚本或手动管理 point-in-time 备份。借 AWS Backup助，您还可以通过单个 AWS Backup 仪表板监控本地卷备份以及云端 AWS 资源。您可以使用 AWS Backup 创建一次性按需备份，也可以定义在中管理的备份计划 AWS Backup。

从中获取 AWS Backup 的 Storage Gateway 卷备份作为亚马逊 EBS 快照存储在亚马逊 S3 中。您可以从 AWS Backup 控制台或 Amazon EBS 控制台查看 Storage Gateway 卷备份。

您可以轻松地将通过管理的 Storage Gateway 卷恢复 AWS Backup 到任何本地网关或云内网关。您也可以将此类卷还原到 Amazon EBS 卷，以便与 Amazon EC2 实例结合使用。

使用备份 Storag AWS Backup e Gateway 卷的好处

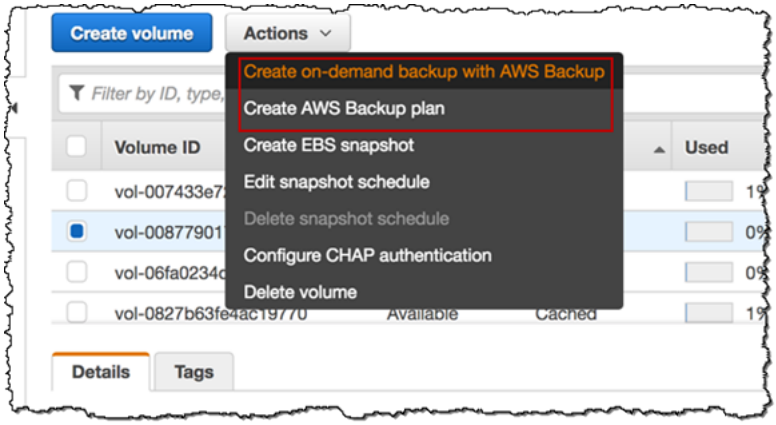
使用 AWS Backup 备份 Storage Gateway 卷的好处是，您可以满足合规性要求，避免操作负担并集中备份管理。 AWS Backup 允许您执行以下操作：

- 设置可自定义的计划备份策略来满足您的备份需求。
- 设置备份保留和过期规则，这样您就不再需要开发自定义脚本或手动管理卷的 point-in-time 备份。
- 从中央视图管理和监控跨多个网关和其他 AWS 资源的备份。

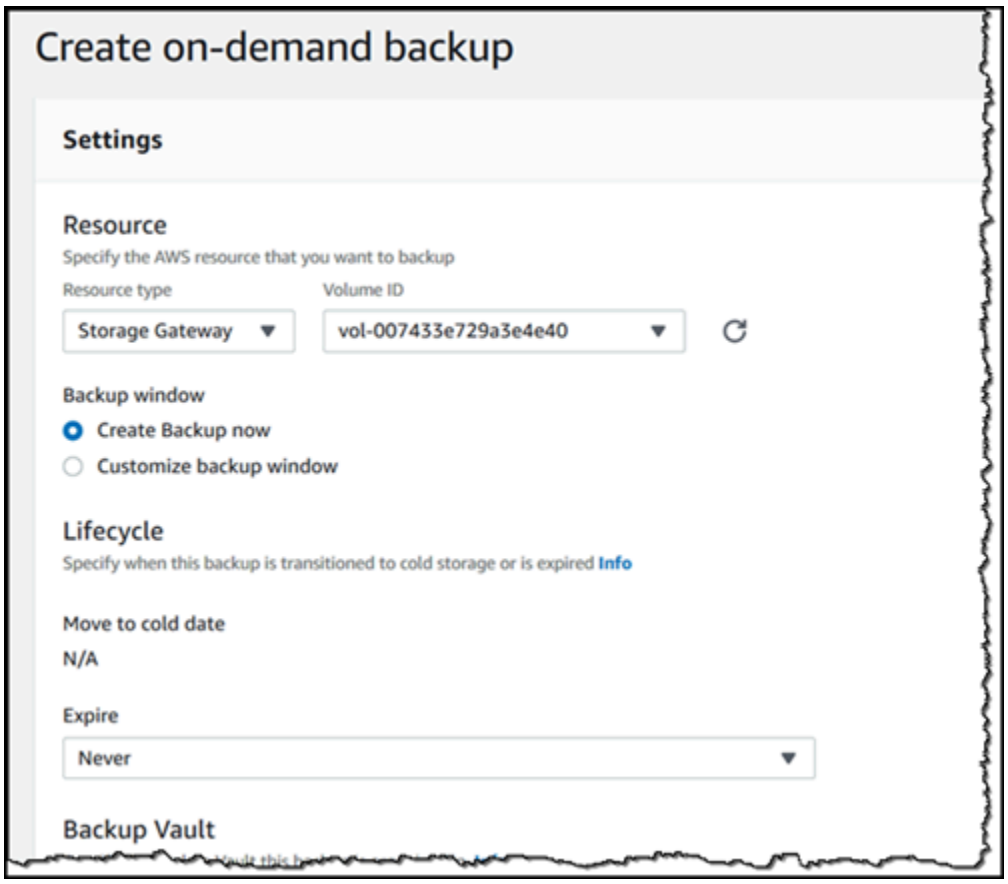
AWS Backup 用于创建卷的备份

> **Note**
>
> AWS Backup 要求您选择一个使用的 AWS Identity and Access Management (IAM) 角色 AWS Backup 。你需要创建这个角色，因为它 AWS Backup 不是为你创建的。您还需要在 AWS Backup 和此 IAM 角色之间创建信任关系。有关如何执行此操作的信息，请参阅《AWS Backup 用户指南》。有关如何执行此操作的信息，请参阅《AWS Backup 用户指南》中的创建备份计划。

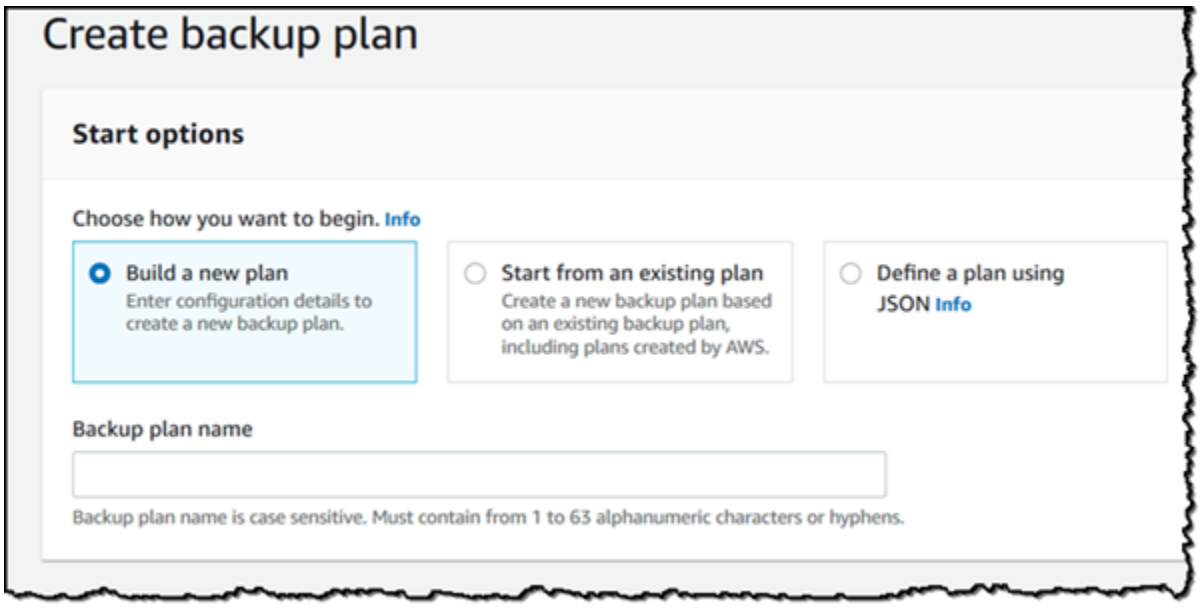
1. 打开 Storage Gateway 控制台，然后在左侧导航窗格中选择卷。
2. 在 “操作” 中，选择 “使用创建按需备份” AWS Backup 或 “创建 AWS 备份计划”。



如果要创建 Storage Gateway 卷的按需备份，请选择使用创建按需备份 AWS Backup。您将被引导进入 AWS Backup 控制台。



如果要创建新 AWS Backup 计划，请选择创建 AWS 备份计划。您将被定向到 AWS Backup 控制台。



在 AWS Backup 控制台上，您可以创建备份计划、为备份计划分配 Storage Gateway 卷以及创建备份。您也可以执行日常备份管理任务。

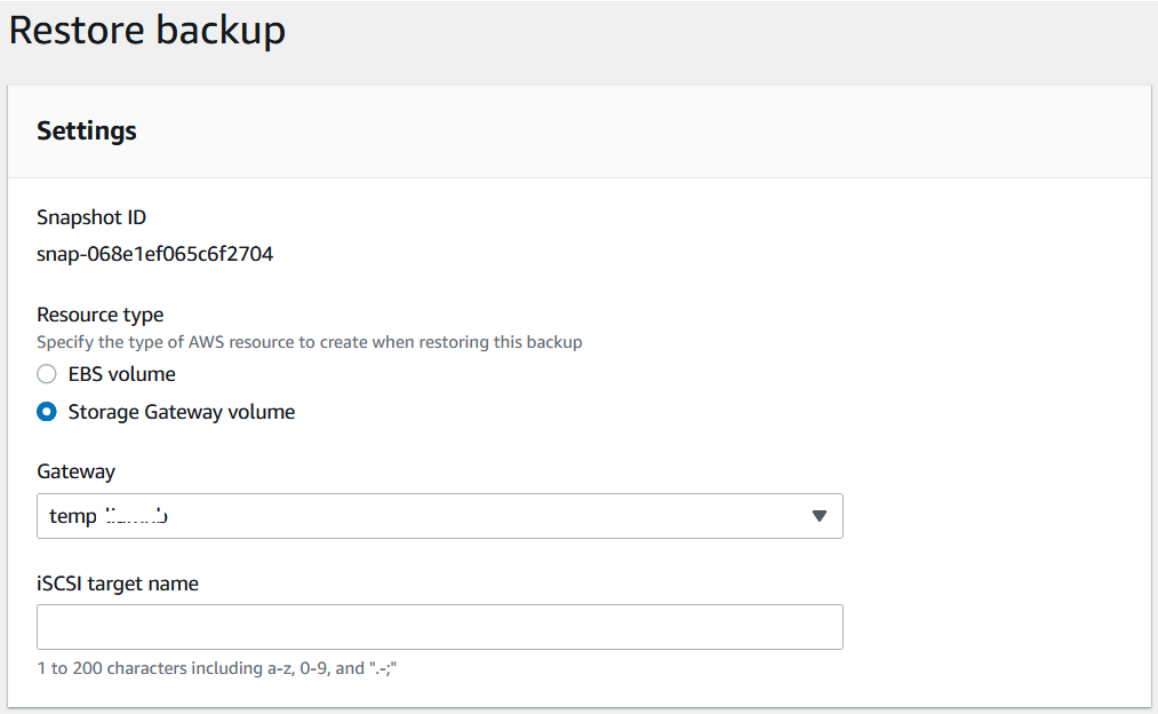
从 AWS Backup查找和还原卷

您可以从 AWS Backup 控制台找到并恢复备份的 Storage Gateway 卷。有关更多信息，请参阅 AWS Backup 用户指南。有关更多信息，请参阅《AWS Backup 用户指南》中的恢复点。

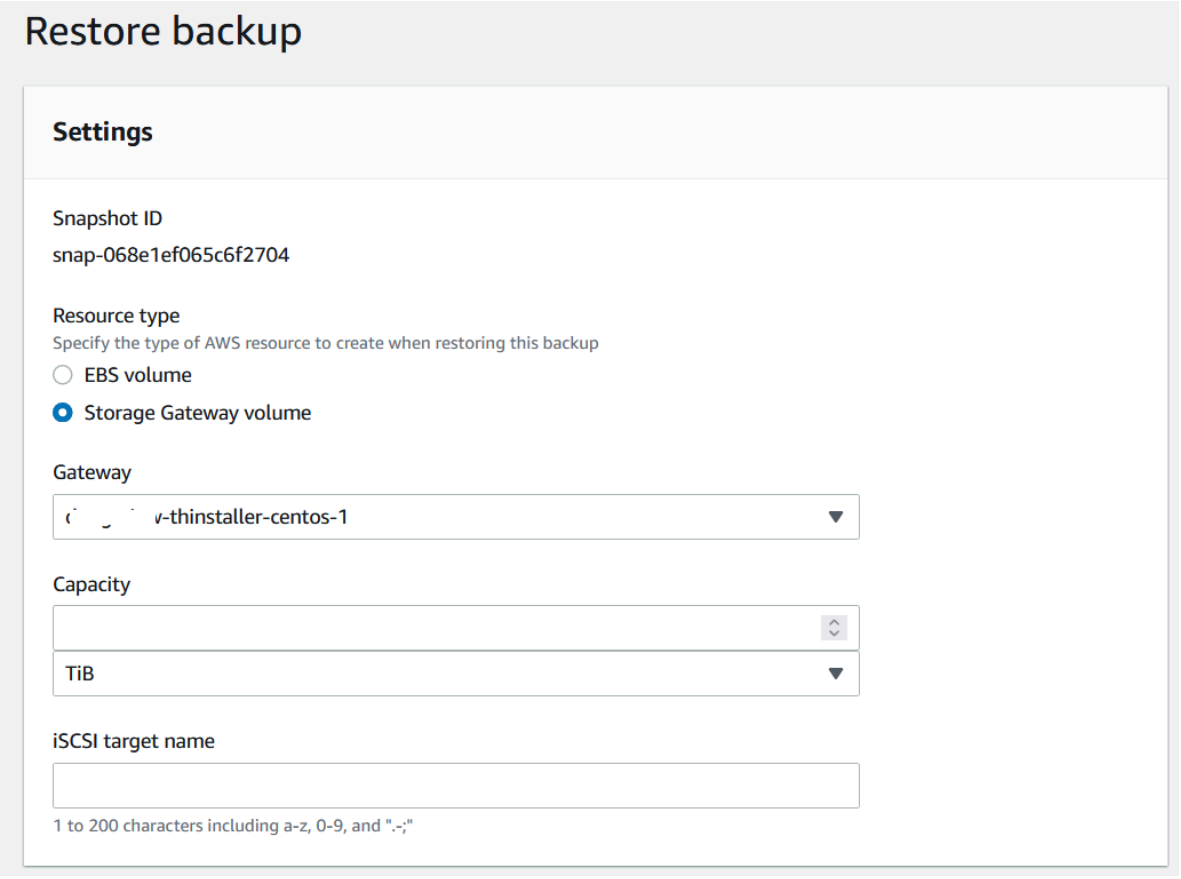
查找和还原您的卷

1. 打开 AWS Backup 控制台，找到要恢复的 Storage Gateway 卷备份。您可以将 Storage Gateway 卷备份还原到 Amazon EBS 卷或 Storage Gateway 卷。根据您的还原要求选择合适的选项。
2. 对于还原类型，请选择还原已存储或已缓存的 Storage Gateway 卷，并提供所需信息：

   - 对于存储卷，请提供 Gateway name (网关名称)、Disk ID (磁盘 ID) 和 iSCSI target name (iSCSI 目标名称)。



   - 对于缓存卷，请提供 Gateway name (网关名称)、Capacity (容量) 和 iSCSI target name (iSCSI 目标名称)。



3. 选择 Restore resource (还原资源) 以还原您的卷。

> **Note**
>
> 您无法使用 Amazon EBS 控制台删除由 AWS Backup创建的快照。

在 Virtual Private Cloud 中激活网关

您可以在本地网关设备和基于云的存储基础设施之间创建私有连接。您可以使用此连接激活您的网关，并允许其将数据传输到 AWS 存储服务，而无需通过公共 Internet 进行通信。使用 Amazon VPC 服务，您可以在自定义虚拟私有云 (VPC) 中启动 AWS 资源，包括私有网络接口终端节点。您可以使用 VPC 来控制网络设置，例如 IP 地址范围、子网、路由表和网络网关。有关 VPC 的更多信息，请参阅《Amazon VPC 用户指南》中的什么是 Amazon VPC？。

要在 VPC 中激活您的网关，请使用 Amazon VPC 控制台为 Storage Gateway 创建 VPC 端点并获取 VPC 端点 ID，然后在创建和激活网关时指定此 VPC 端点 ID。有关更多信息，请参阅 将卷网关连接到 AWS。

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

主题

- 为 Storage Gateway 创建 VPC 端点

为 Storage Gateway 创建 VPC 端点

按照这些说明创建 VPC 终端节点。如果您已经有用于 Storage Gateway 的 VPC 端点，则可以使用它来激活您的网关。

为 Storage Gateway 创建 VPC 端点

1. 登录 AWS Management Console 并打开亚马逊 VPC 控制台，网址为 https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints (终端节点)，然后选择 Create Endpoint (创建终端节点)。
3. 在创建端点页面上，为服务类别选择 AWS 服务。
4. 对于 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. 选择创建端点。终端节点的初始状态为 pending (待处理)。创建终端节点时，记下您刚创建的 VPC 终端节点的 ID。
9. 在创建终端节点时，选择 Endpoints (终端节点)，然后选择新的 VPC 终端节点。

10. 在所选存储网关端点的详细信息选项卡中，在 DNS 名称下，使用第一个未指定可用区的 DNS 名称。您的 DNS 名称类似这样：`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。有关更多信息，请参阅创建网关。

管理您的网关

管理网关包括配置缓存存储和上传缓冲区空间、使用卷或虚拟磁带、进行常规维护等任务。如果您尚未创建网关，请参阅入门。

定期发布的 Storage Gateway 软件版本包括经过验证的操作系统更新和安全补丁。在定期维护时段内的定期网关更新过程应用这些更新，并且通常会每六个月发布一次。注意：用户应将 Storage Gateway 设备视为托管虚拟机，并且不应尝试访问或修改 Storage Gateway 设备实例。尝试使用正常网关更新机制以外的方法（例如 SSM 或虚拟机管理程序工具）安装或更新任何软件包可能会中断网关的正常运行。

主题

- 管理卷网关
- 将数据移至新网关

管理卷网关

在下文中，您可以找到有关如何管理卷网关资源的信息。

缓存卷是 Amazon Simple Storage Service (Amazon S3) 中作为 iSCSI 目标公开的卷，您可以使用这些卷存储应用程序数据。您可以在下面找到有关如何为缓存设置添加和移除卷的信息。您还可以了解如何在 Amazon EC2 网关中添加和删除 Amazon Elastic Block Store (Amazon EBS) 卷。

主题

- 编辑基本网关信息
- 添加卷
- 扩展卷的大小
- 克隆卷
- 查看卷使用率
- 减少卷上的计费存储量
- 删除卷
- 将您的卷迁移至不同的网关
- 创建一次性快照
- 编辑快照计划

- 删除快照
- 了解卷状态和转换

> **Important**
>
> 如果缓存卷将您的主要数据保存在 Amazon S3 中，您应该避免在整个卷上读取或写入所有数据。例如，我们建议不要使用扫描整个缓存卷的病毒扫描软件。此类扫描（无论是按需执行还是按计划执行）都会导致存储在 Amazon S3 中的所有数据为了扫描而进行本地下载，从而导致高带宽使用率。您可以使用实时病毒扫描，而不是进行全盘扫描，也就是说，在从缓存卷读取数据或向缓存卷写入数据时扫描数据。

不支持重新配置卷的大小。要更改某个卷的大小，请创建该卷的快照，然后从该快照创建新的缓存卷。新卷可大于快照所从创建的卷。有关描述如何移除卷的步骤，请参阅删除卷。有关描述如何添加卷和保存现有数据的步骤，请参阅删除卷。

所有缓存卷数据和快照数据均存储在 Amazon S3 中，并使用服务器端加密 (SSE) 进行静态加密。不过，您不能使用 Amazon S3 API 或其他工具（如 Amazon S3 管理控制台）访问这些数据。

编辑基本网关信息

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

编辑现有网关的基本信息

1. 打开 Storage Gateway 控制台，网址为 https://console.aws.amazon.com/storagegateway/home。
2. 选择网关，然后选择要为其编辑基本信息的网关。
3. 从操作下拉菜单中，选择编辑网关信息。
4. 修改要更改的设置，然后选择保存更改。

> **Note**
>
> 更改网关名称将断开为监控网关而设置的所有 CloudWatch 警报。要重新连接警报，请在 CloudWatch 控制台中GatewayName更新每个警报的。

添加卷

随着应用程序需求增长，您可能需要向网关添加更多卷。添加更多卷时，您必须考虑分配给网关的缓存存储和上传缓冲区的大小。网关必须有供新卷使用的充足缓冲区和缓存空间。有关更多信息，请参阅确定要分配的上传缓冲区的大小。

您可以使用 Storage Gateway 控制台或 Storage Gateway API 来添加卷。有关使用 Storage Gateway API 添加卷的信息，请参阅 CreateCachedisci Volume。有关使用 Storage Gateway 控制台添加卷的说明，请参阅创建卷。

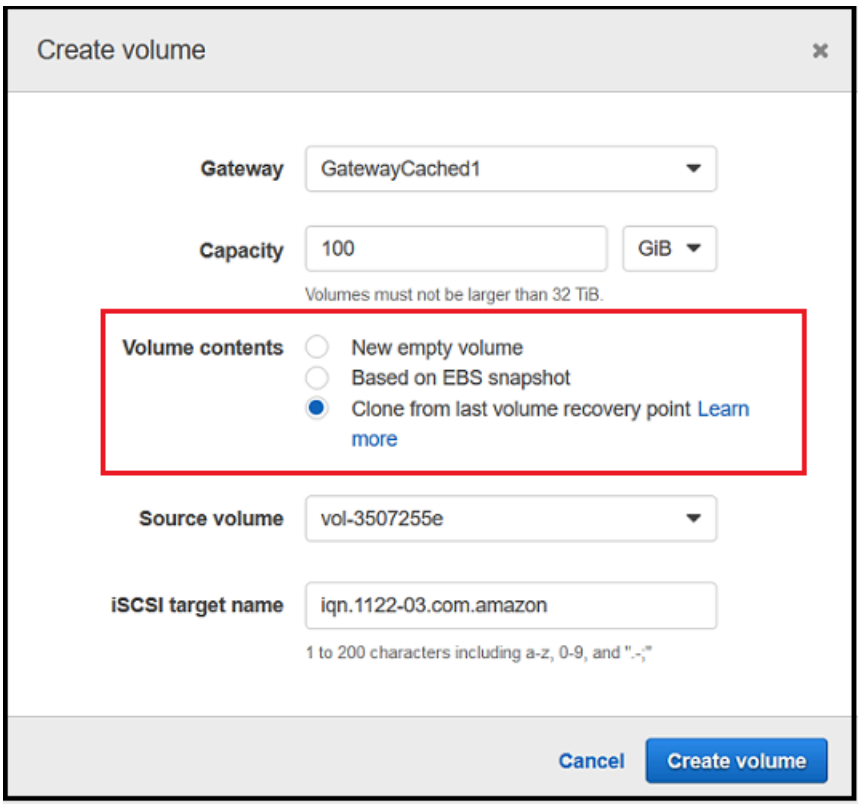
扩展卷的大小

随着应用程序需求增长，您可能希望扩展卷而不是将更多卷添加到网关。在这种情况下，您可以执行下列操作之一：

- 创建您想要扩展的卷的快照，然后使用此快照创建更大的新卷。有关如何创建快照的信息，请参阅创建一次性快照。有关如何使用快照创建新卷的信息，请参阅创建卷。
- 使用您想要扩展的已缓存卷克隆更大的新卷。有关如何克隆卷的信息，请参阅克隆卷。有关如何创建卷的信息，请参阅创建卷。

克隆卷

您可以从同一 AWS 区域中的任何现有缓存卷中创建新卷。将从选定卷的最新恢复点创建新卷。卷恢复点 是一个卷的所有数据都保持一致的时间点。要克隆卷，请在创建卷对话框中选择从上一个恢复点克隆选项，然后选择要用作源的卷。以下屏幕截图显示 Create volume 对话框。



与创建 Amazon EBS 快照相比，从现有卷克隆的方式会更快速、更经济高效。克隆使用源卷的最新恢复点，将数据从源卷 byte-to-byte 复制到新卷。Storage Gateway 会自动为缓存卷创建恢复点。要查看最后一个恢复点的创建时间，请查看 Amazon 中的`TimeSinceLastRecoveryPoint`指标 CloudWatch。

克隆的卷独立于源卷。也就是说，在克隆后对任一卷的更改将不会影响另一个卷。例如，如果您删除源卷，并不会影响克隆的卷。您可以在启动程序已连接且正在使用时克隆源卷。这样做不会影响源卷的性能。有关如何克隆卷的信息，请参阅创建卷。

您也可以在恢复方案中使用克隆过程。有关更多信息，请参阅您的缓存网关无法访问，您希望恢复数据。

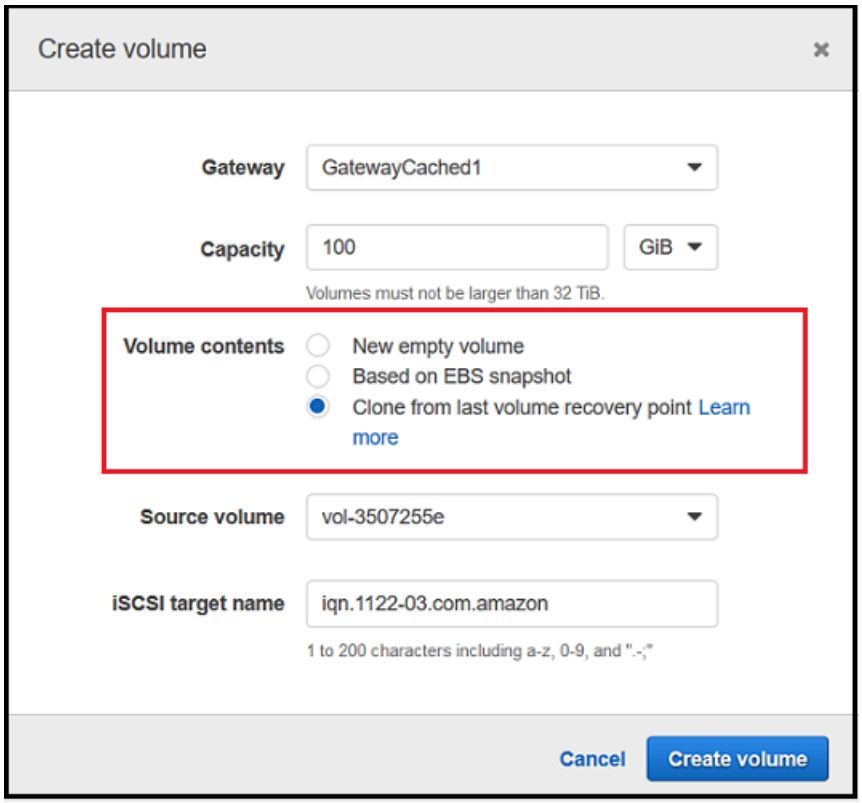
从卷恢复点进行克隆

以下过程介绍如何从卷恢复点克隆一个卷并使用该卷。

从无法访问的网关克隆并使用卷

1. 打开 Storage Gateway 控制台，网址为 https://console.aws.amazon.com/storagegateway/home。
2. 在 Storage Gateway 控制台中，选择创建卷。

3. 在 Create volume (创建卷) 对话框中，为 Gateway (网关) 选择网关。
4. 对于容量，键入卷的容量。此容量必须至少与源卷的大小相同。
5. 选择 Clone from last recovery point，然后为 Source volume 选择卷 ID。源卷可以是选定 AWS 区域中的任何缓存卷。



6. 为 iSCSI target name (iSCSI 目标名称) 键入名称。

   目标名称可包含小写字母、数字句点 (.) 和连词符 (-)。发现后，此目标名称显示为 iSCSI Microsoft 启动程序 UI 的目标选项卡中的 iSCSI 目标节点名称。例如，名称 `target1` 将显示为 `iqn.1007-05.com.amazon:target1`。确保目标名称在存储区域网络 (SAN) 内具有全局唯一性。

7. 验证 Network interface 设置是否为网关的 IP 地址，或者为 Network interface 选择 IP 地址。

   如果您已将网关定义为使用多个网络适配器，则选择存储应用程序将用于访问卷的 IP 地址。为网关定义的每个网络适配器代表您可以选择的一个 IP 地址。

   如果网关 VM 是针对多个网络适配器配置的，则创建卷对话框对于网络接口将显示一个列表。在该列表中，一个 IP 地址对应一个为网关 VM 配置的适配器。如果网关 VM 只是为一个网络适配器配置的，则不会显示列表，因为只有一个 IP 地址。

8. 选择创建卷。此时将显示 Configure CHAP Authentication (配置 CHAP 身份验证) 对话框。您稍后可以配置 CHAP。有关信息，请参阅 为 iSCSI 目标配置 CHAP 身份验证。

下一步是将卷连接到客户端。有关更多信息，请参阅将卷连接到客户端。

创建恢复快照

以下过程说明如何从卷恢复点创建一个快照并使用该快照。您可以拍摄一次性快照、临时快照或者为卷设置快照计划。

从无法访问的网关创建并使用卷的恢复快照

1. 打开 Storage Gateway 控制台，网址为 https://console.aws.amazon.com/storagegateway/home。
2. 在导航窗格中，选择 网关。
3. 选择无法访问的网关，然后选择 Details 选项卡。

   此时选项卡上会显示恢复快照消息。

4. 选择 Create recovery snapshot 以打开 Create recovery snapshot 对话框。
5. 从显示的卷列表中，选择要恢复的卷，然后选择 Create snapshots。

   Storage Gateway 启动快照过程。
6. 查找并还原快照。

查看卷使用率

当您将数据写入卷时，可以在 Storage Gateway 管理控制台中查看卷上存储的数据量。每个卷的 Details 选项卡显示卷使用率信息。

查看写入到卷中的数据量

1. 打开 Storage Gateway 控制台，网址为 https://console.aws.amazon.com/storagegateway/home。
2. 在导航窗格中，选择 Volumes，然后选择您感兴趣的卷。
3. 选择详细信息选项卡。

   以下字段提供有关卷的信息：

   - Size：所选卷的总容量。
   - Used：卷上存储的数据量。

   > **Note**
   >
   > 这些值不适用于在 2015 年 5 月 13 日之前创建的卷，除非您在卷上存储数据。

减少卷上的计费存储量

从文件系统中删除文件不一定会从底层块储存设备删除数据或减少卷上存储的数据量。如果您要减少卷上的计费存储量，我们建议用零来覆盖您的文件，从而将存储压缩到极小的实际存储量。Storage Gateway 基于压缩的存储收取卷用量费用。

> **Note**
>
> 如果您使用删除工具，该工具用随机数据来覆盖卷上的数据，则您的用量不会减少。这是因为随机数据是不可压缩的。

删除卷

当应用程序需求改变时（例如，如果您迁移应用程序来使用更大的存储卷），您可能需要删除卷。删除某个卷前，请确保当前没有应用程序正在写入该卷。另外，请确保该卷没有正在拍摄的快照。如果为卷

定义了快照计划，则可以在 Storage Gateway 控制台的快照计划选项卡上进行查看。有关更多信息，请参阅编辑快照计划。

您可以使用 Storage Gateway 控制台或 Storage Gateway API 来删除卷。有关使用 Storage Gateway API 删除卷的信息，请参阅删除卷。以下过程展示如何使用控制台。

在删除卷之前，备份您的数据或拍摄关键数据的快照。对于存储卷，您的本地磁盘不会被擦除。删除的卷将无法恢复。

删除卷

1. 打开 Storage Gateway 控制台，网址为 https://console.aws.amazon.com/storagegateway/home。
2. 选择卷，然后选择一个或多个要删除的卷。
3. 在操作中选择删除卷。此时会显示确认对话框。
4. 确认要删除指定的卷，然后在确认框中键入单词 delete 并选择删除。

将您的卷迁移至不同的网关

随着数据和性能需求的增长，您可能希望将卷移动到不同的卷网关。要执行此操作，您可以使用 Storage Gateway 控制台或 API 分离和附加卷。

通过分离并附加卷，您可以实现：

- 将卷移动到更好的主机平台或者较新的 Amazon EC2 实例。
- 刷新服务器的底层硬件。
- 在不同管理程序类型之间移动卷类型。

在分离卷时，网关会上传卷数据和元数据并存储到 AWS的 Storage Gateway 服务中。以后，您可以轻松地将分离的卷附加到任何支持的主机平台。

> **Note**
>
> 已分离的卷按照标准卷存储费率计费，直至您删除它。有关如何减少账单的信息，请参阅减少卷上的计费存储量。

> **Note**
>
> 附加和分离卷有一些限制：
>
> - 分离卷可能需要较长的时间。分离卷时，网关会在分离卷 AWS 之前将该卷上的所有数据上传到该卷上。完成上传所需的时间取决于需要上传的数据量以及您的网络与 AWS的连接。
> - 如果分离缓存卷，则您无法将其作为存储卷重新附加。
> - 如果分离存储卷，则您无法将其作为缓存卷重新附加。
> - 已分离的卷在附加到网关之前无法使用。
> - 在您附加存储卷时，该卷需要完全恢复之后才能附加到网关。
> - 当您开始附加或分离卷时，需要等待直至操作完成，然后才能使用卷。
> - 目前，只有 API 中支持强制删除卷。
> - 如果有卷正在从网关中分离而您删除了该网关，则会导致数据丢失。请等待直至卷分离操作完成，然后再删除网关。
> - 如果存储网关存储正在还原的状态，您无法从其中分离卷。

以下步骤演示如何使用 Storage Gateway 控制台分离和附加卷。有关使用 API 执行此操作的更多信息，请参阅 AWS Storage Gateway API 参考AttachVolume中的DetachVolume或。

从网关分离卷

1. 打开 Storage Gateway 控制台，网址为 https://console.aws.amazon.com/storagegateway/home。
2. 选择卷，然后选择一个或多个要分离的卷。
3. 对于操作，选择分离卷。此时会显示确认对话框。
4. 确认要分离指定的卷，然后在确认框中键入单词 detach 并选择分离。

> **Note**
>
> 如果您要分离的卷有大量数据，则其状态会从已附加转变为正在分离，直至完成上传所有数据。然后，状态更改为已分离。如果只有少量数据，您可能无法看到正在分离状态。如果卷上没有数据，则状态从已附加更改为已分离。

现在，您可以将此卷附加到其他网关。

将卷附加到网关

1. 打开 Storage Gateway 控制台，网址为 https://console.aws.amazon.com/storagegateway/home。
2. 在导航窗格中，选择卷。已分离的各个卷的状态显示为已分离。
3. 从已分离卷列表中，选择要附加的卷。一次只能附加一个卷。
4. 对于操作，选择附加卷。
5. 在附加卷对话框中，选择要将卷附加到的网关，然后输入要将卷连接到的 iSCSI 目标。

   如果您在附加存储卷，请为磁盘 ID 输入其磁盘标识符。
6. 选择附加卷。如果您连接的卷上有大量数据，则在 `AttachVolume` 操作成功后，卷的状态将从已分离转换为已附加。
7. 在显示的配置 CHAP 身份验证向导中，在各自的框中提供启动程序名称、启动程序密钥和目标密钥，然后选择保存。有关使用质询握手身份验证协议 (CHAP) 身份验证的更多信息，请参阅为 iSCSI 目标配置 CHAP 身份验证。

创建一次性快照

除了计划快照外，对于卷网关，您还可以拍摄一次性的临时快照。这样一来，您可以立即备份存储卷，而无需等待下次预定快照。

拍摄存储卷的一次性快照

1. 打开 Storage Gateway 控制台，网址为 https://console.aws.amazon.com/storagegateway/home。
2. 在导航窗格中，选择 Volumes，然后选择要从中创建快照的卷。
3. 对于操作，选择创建快照。
4. 在 Create snapshot 对话框中，键入快照描述，然后选择 Create snapshot。

   您可以验证是否已使用控制台创建快照。

您的快照在与卷位于相同行的 Snapshots 中列出。

编辑快照计划

对于存储的卷， AWS Storage Gateway 创建每天一次的默认快照计划。

> **Note**
>
> 您无法删除默认快照计划。存储卷需要至少一个快照计划。但是，您可以通过指定快照每天发生的时间和/或频率 (每 1、2、4、8、12 或 24 个小时) 来更改快照计划。

对于缓存卷， AWS Storage Gateway 不会创建默认的快照计划。不会创建默认计划，因为您的数据存储在 Amazon S3 中，所以，您无需快照或快照计划以用于灾难恢复目的。不过，您可以在需要时随时设置快照计划。为缓存卷创建快照提供了另一种在必要时恢复数据的方法。

通过使用以下步骤，您可以编辑卷的快照计划。

编辑卷的快照计划

1. 打开 Storage Gateway 控制台，网址为 https://console.aws.amazon.com/storagegateway/home。
2. 在导航窗格中，选择 Volumes，然后选择已从中创建快照的卷。
3. 对于 Actions (操作)，选择 Edit snapshot schedule (编辑快照计划)。
4. 在 Edit snapshot schedule 对话框中，修改计划，然后选择 Save。

删除快照

可以删除存储卷的快照。例如，当您在一段时间内拍摄了存储卷的许多快照而不再需要较旧的快照时，您可能想要删除快照。由于快照是增量备份，因此删除某个快照的操作仅会删除其他快照不需要的数据。

主题

- 使用适用于 Java 的 AWS 软件开发工具包删除快照
- 使用适用于 .NET 的 AWS 软件开发工具包删除快照
- 使用 AWS Tools for Windows PowerShell删除快照

在 Amazon EBS 控制台中，您可以一次删除一个快照。有关如何使用 Amazon EBS 控制台删除快照的信息，请参阅《Amazon EC2 用户指南》中的删除 Amazon EBS 快照。

要一次删除多个快照，您可以使用其中一个支持 Storage Gateway 操作的 AWS 软件开发工具包。有关示例，请参阅 使用适用于 Java 的 AWS 软件开发工具包删除快照、使用适用于 .NET 的 AWS 软件开发工具包删除快照 和 使用 AWS Tools for Windows PowerShell删除快照。

使用适用于 Java 的 AWS 软件开发工具包删除快照

如需删除与卷关联的多个快照，您可以使用编程方法。以下示例演示如何使用适用于 Java 的 AWS 软件开发工具包删除快照。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《适用于 Java 的AWS 软件开发工具包开发人员指南》中的入门。如果您只需删除少量快照，请按 删除快照 中所述使用控制台。

Example : 使用适用于 Java 的 AWS SDK 删除快照

以下 Java 代码示例列出了网关各个卷的快照以及快照起始日期是在指定日期前还是之后。它使用适用于 Storage Gateway 和 Amazon EC2 的 Java AWS 开发工具包 API。Amazon EC2 API 包括数种处理快照的操作。

更新代码以提供服务终端节点、您的网关的 Amazon 资源名称 (ARN) 和您想要保存快照的回溯天数。此截止日期之前拍摄的快照都将被删除。您还需要指定布尔值 `viewOnly`，该值表明是要查看要删除的快照还是实际执行快照删除。先只带 view 选项 (即将 `viewOnly` 设置为 `true`) 运行代码，看看代码会删除什么。有关可以与 Storage Gateway 配合使用的 AWS 服务终端节点列表，请参阅中的AWS Storage Gateway 终端节点和配额AWS 一般参考。

```
import java.io.IOException;
import java.util.ArrayList;
import java.util.Calendar;
import java.util.Collection;
import java.util.Date;
import java.util.GregorianCalendar;
import java.util.List;

import com.amazonaws.auth.PropertiesCredentials;
import com.amazonaws.services.ec2.AmazonEC2Client;
import com.amazonaws.services.ec2.model.DeleteSnapshotRequest;
import com.amazonaws.services.ec2.model.DescribeSnapshotsRequest;
import com.amazonaws.services.ec2.model.DescribeSnapshotsResult;
import com.amazonaws.services.ec2.model.Filter;
import com.amazonaws.services.ec2.model.Snapshot;
import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
import com.amazonaws.services.storagegateway.model.ListVolumesRequest;
import com.amazonaws.services.storagegateway.model.ListVolumesResult;
import com.amazonaws.services.storagegateway.model.VolumeInfo;

public class ListDeleteVolumeSnapshotsExample {

    public static AWSStorageGatewayClient sgClient;
```

```
    public static AmazonEC2Client ec2Client;
    static String serviceURLSG = "https://storagegateway.us-east-1.amazonaws.com";
    static String serviceURLEC2 = "https://ec2.us-east-1.amazonaws.com";

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

    // The number of days back you want to save snapshots. Snapshots before this cutoff
are deleted
    // if viewOnly = false.
    public static int daysBack = 10;

    // true = show what will be deleted; false = actually delete snapshots that meet
the daysBack criteria
    public static boolean viewOnly = true;

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

        // Create a Storage Gateway and amazon ec2 client
        sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(

ListDeleteVolumeSnapshotsExample.class.getResourceAsStream("AwsCredentials.properties")));

        sgClient.setEndpoint(serviceURLSG);

        ec2Client = new AmazonEC2Client(new PropertiesCredentials(

ListDeleteVolumeSnapshotsExample.class.getResourceAsStream("AwsCredentials.properties")));
        ec2Client.setEndpoint(serviceURLEC2);

        List<VolumeInfo> volumes = ListVolumesForGateway();
        DeleteSnapshotsForVolumes(volumes, daysBack);

    }
    public static List<VolumeInfo> ListVolumesForGateway()
    {
        List<VolumeInfo> volumes = new ArrayList<VolumeInfo>();

        String marker = null;
        do {
            ListVolumesRequest request = new
ListVolumesRequest().withGatewayARN(gatewayARN);
            ListVolumesResult result = sgClient.listVolumes(request);
            marker = result.getMarker();
```

```
            for (VolumeInfo vi : result.getVolumeInfos())
            {
                volumes.add(vi);
                System.out.println(OutputVolumeInfo(vi));
            }
        } while (marker != null);

        return volumes;
    }
    private static void DeleteSnapshotsForVolumes(List<VolumeInfo> volumes,
            int daysBack2) {

        // Find snapshots and delete for each volume
        for (VolumeInfo vi : volumes) {

            String volumeARN = vi.getVolumeARN();
            String volumeId =
volumeARN.substring(volumeARN.lastIndexOf("/")+1).toLowerCase();
            Collection<Filter> filters = new ArrayList<Filter>();
            Filter filter = new Filter().withName("volume-id").withValues(volumeId);
            filters.add(filter);

            DescribeSnapshotsRequest describeSnapshotsRequest =
                new DescribeSnapshotsRequest().withFilters(filters);
            DescribeSnapshotsResult describeSnapshotsResult =
                ec2Client.describeSnapshots(describeSnapshotsRequest);

            List<Snapshot> snapshots = describeSnapshotsResult.getSnapshots();
            System.out.println("volume-id = " + volumeId);
            for (Snapshot s : snapshots){
                StringBuilder sb = new StringBuilder();
                boolean meetsCriteria = !CompareDates(daysBack, s.getStartTime());
                sb.append(s.getSnapshotId() + ", " + s.getStartTime().toString());

                sb.append(", meets criteria for delete? " + meetsCriteria);
                sb.append(", deleted? ");
                if (!viewOnly & meetsCriteria) {
                    sb.append("yes");
                    DeleteSnapshotRequest deleteSnapshotRequest =
                        new DeleteSnapshotRequest().withSnapshotId(s.getSnapshotId());
                    ec2Client.deleteSnapshot(deleteSnapshotRequest);
                }
                else {
```

```
                    sb.append("no");
                }
                System.out.println(sb.toString());
            }
        }
    }

    private static String OutputVolumeInfo(VolumeInfo vi) {

        String volumeInfo = String.format(
                 "Volume Info:\n" +
                 "  ARN: %s\n" +
                 "  Type: %s\n",
                 vi.getVolumeARN(),
                 vi.getVolumeType());
        return volumeInfo;
     }

    // Returns the date in two formats as a list
    public static boolean CompareDates(int daysBack, Date snapshotDate) {
        Date today = new Date();
        Calendar cal = new GregorianCalendar();
        cal.setTime(today);
        cal.add(Calendar.DAY_OF_MONTH, -daysBack);
        Date cutoffDate = cal.getTime();
        return (snapshotDate.compareTo(cutoffDate) > 0) ? true : false;
    }

}
```

使用适用于 .NET 的 AWS 软件开发工具包删除快照

如需删除与卷关联的多个快照，您可以使用编程方法。以下示例演示如何使用适用于 .NET 的 AWS 软件开发工具包版本 2 和 3 删除快照。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《适用于 .NET 的AWS 软件开发工具包开发人员指南》中的入门。如果您只需删除少量快照，请按 删除快照 中所述使用控制台。

Example : 使用适用于.NET 的 AWS SDK 删除快照

在以下 C# 代码示例中， AWS Identity and Access Management 用户可以列出网关每个卷的快照。然后，该用户可以判断快照的起始时间是在指定日期 (保留期) 之前还是之后，并删除过了保留期的快照。该示例为 Storage Gateway 和 Amazon EC2 使用适用于 .NET 的 AWS 软件开发工具包 API。Amazon EC2 API 包括数种处理快照的操作。

以下代码示例使用适用于.NET 的 AWS SDK 版本 2 和 3。您可以将旧版本的 .NET 迁移到新版本。有关更多信息，请参阅将您的代码迁移到最新版本的 AWS SDK for .NET。

更新代码以提供服务终端节点、您的网关的 Amazon 资源名称 (ARN) 和您想要保存快照的回溯天数。此截止日期之前拍摄的快照都将被删除。您还需要指定布尔值 `viewOnly`，该值表明是要查看要删除的快照还是实际执行快照删除。先只带 view 选项 (即将 `viewOnly` 设置为 `true`) 运行代码，看看代码会删除什么。有关可以与 Storage Gateway 配合使用的 AWS 服务终端节点列表，请参阅中的AWS Storage Gateway 终端节点和配额AWS 一般参考。

首先，创建一个用户并将最小 IAM 策略附加到该用户。然后为您的网关制定自动快照计划。

以下代码创建允许用户删除快照的最小权限策略。在本示例中，策略的名称为 **`sgw-delete-snapshot`**。

```
{
      "Version": "2012-10-17",
      "Statement": [
          {
              "Sid": "StmtEC2Snapshots",
              "Effect": "Allow",
              "Action": [
                  "ec2:DeleteSnapshot",
                  "ec2:DescribeSnapshots"
              ],
              "Resource": [
                  "*"
              ]
          },
          {
              "Sid": "StmtSgwListVolumes",
              "Effect": "Allow",
              "Action": [
                  "storagegateway:ListVolumes"
              ],
              "Resource": [
                  "*"
              ]
          }
      ]
  }
```

以下 C# 代码在指定网关中查找与卷和指定截止期匹配的所有快照并将其删除。

```
using System;
using System.Collections.Generic;
using System.Text;
using Amazon.EC2;
using Amazon.EC2.Model;
using Amazon.StorageGateway.Model;
using Amazon.StorageGateway;

namespace DeleteStorageGatewaySnapshotNS
{
    class Program
    {
        /*
         * Replace the variables below to match your environment.
         */

         /* IAM AccessKey */
        static String AwsAccessKey = "AKIA...............";

        /* IAM SecretKey */
        static String AwsSecretKey = "******************************";

        /* Account number, 12 digits, no hyphen */
        static String OwnerID = "123456789012";

        /* Your Gateway ARN. Use a Storage Gateway ID, sgw-XXXXXXXX* */
        static String GatewayARN = "arn:aws:storagegateway:ap-
southeast-2:123456789012:gateway/sgw-XXXXXXXX";

        /* Snapshot status: "completed", "pending", "error" */

        static String SnapshotStatus = "completed";

        /* Region where your gateway is activated */
        static String AwsRegion = "ap-southeast-2";

        /* Minimum age of snapshots before they are deleted (retention policy) */
        static int daysBack = 30;

        /*
         * Do not modify the four lines below.
         */
        static AmazonEC2Config ec2Config;
```

```
        static AmazonEC2Client ec2Client;
        static AmazonStorageGatewayClient sgClient;
        static AmazonStorageGatewayConfig sgConfig;

        static void Main(string[] args)
        {
            // Create an EC2 client.
            ec2Config = new AmazonEC2Config();
            ec2Config.ServiceURL = "https://ec2." + AwsRegion + ".amazonaws.com";
            ec2Client = new AmazonEC2Client(AwsAccessKey, AwsSecretKey, ec2Config);

            // Create a Storage Gateway client.
            sgConfig = new AmazonStorageGatewayConfig();
            sgConfig.ServiceURL = "https://storagegateway." + AwsRegion +
".amazonaws.com";
            sgClient = new AmazonStorageGatewayClient(AwsAccessKey, AwsSecretKey,
sgConfig);

            List<VolumeInfo> StorageGatewayVolumes = ListVolumesForGateway();
            List<Snapshot> StorageGatewaySnapshots =
ListSnapshotsForVolumes(StorageGatewayVolumes,
                                                    daysBack);
            DeleteSnapshots(StorageGatewaySnapshots);
        }

        /*
         * List all volumes for your gateway
         * returns: A list of VolumeInfos, or null.
         */
        private static List<VolumeInfo> ListVolumesForGateway()
        {
            ListVolumesResponse response = new ListVolumesResponse();
            try
            {
                ListVolumesRequest request = new ListVolumesRequest();
                request.GatewayARN = GatewayARN;
                response = sgClient.ListVolumes(request);

                foreach (VolumeInfo vi in response.VolumeInfos)
                {
                    Console.WriteLine(OutputVolumeInfo(vi));
                }
            }
            catch (AmazonStorageGatewayException ex)
```

```
            {
                Console.WriteLine(ex.Message);
            }
            return response.VolumeInfos;
        }

        /*
         * Gets the list of snapshots that match the requested volumes
         * and cutoff period.
         */
        private static List<Snapshot> ListSnapshotsForVolumes(List<VolumeInfo> volumes,
int snapshotAge)
        {
            List<Snapshot> SelectedSnapshots = new List<Snapshot>();
            try
            {
                foreach (VolumeInfo vi in volumes)
                {
                    String volumeARN = vi.VolumeARN;
                    String volumeID = volumeARN.Substring(volumeARN.LastIndexOf("/") +
1).ToLower();

                    DescribeSnapshotsRequest describeSnapshotsRequest = new
DescribeSnapshotsRequest();

                    Filter ownerFilter = new Filter();
                    List<String> ownerValues = new List<String>();
                    ownerValues.Add(OwnerID);
                    ownerFilter.Name = "owner-id";
                    ownerFilter.Values = ownerValues;
                    describeSnapshotsRequest.Filters.Add(ownerFilter);

                    Filter statusFilter = new Filter();
                    List<String> statusValues = new List<String>();
                    statusValues.Add(SnapshotStatus);
                    statusFilter.Name = "status";
                    statusFilter.Values = statusValues;
                    describeSnapshotsRequest.Filters.Add(statusFilter);

                    Filter volumeFilter = new Filter();
                    List<String> volumeValues = new List<String>();
                    volumeValues.Add(volumeID);
                    volumeFilter.Name = "volume-id";
                    volumeFilter.Values = volumeValues;
```

```
                    describeSnapshotsRequest.Filters.Add(volumeFilter);

                    DescribeSnapshotsResponse describeSnapshotsResponse =
                      ec2Client.DescribeSnapshots(describeSnapshotsRequest);

                    List<Snapshot> snapshots = describeSnapshotsResponse.Snapshots;
                    Console.WriteLine("volume-id = " + volumeID);
                    foreach (Snapshot s in snapshots)
                    {
                        if (IsSnapshotPastRetentionPeriod(snapshotAge, s.StartTime))
                        {
                            Console.WriteLine(s.SnapshotId + ", " + s.VolumeId + ",
                               " + s.StartTime + ", " + s.Description);
                            SelectedSnapshots.Add(s);
                        }
                    }
                }
            }
            catch (AmazonEC2Exception ex)
            {
                Console.WriteLine(ex.Message);
            }
            return SelectedSnapshots;
        }

        /*
         * Deletes a list of snapshots.
         */
        private static void DeleteSnapshots(List<Snapshot> snapshots)
        {
            try
            {
                foreach (Snapshot s in snapshots)
                {

                    DeleteSnapshotRequest deleteSnapshotRequest = new
DeleteSnapshotRequest(s.SnapshotId);
                    DeleteSnapshotResponse response =
ec2Client.DeleteSnapshot(deleteSnapshotRequest);
                    Console.WriteLine("Volume: " +
                              s.VolumeId +
                              " => Snapshot: " +
                              s.SnapshotId +
                              " Response: "
```

```
                                + response.HttpStatusCode.ToString());
                }
            }
            catch (AmazonEC2Exception ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /*
         * Checks if the snapshot creation date is past the retention period.
         */
        private static Boolean IsSnapshotPastRetentionPeriod(int daysBack, DateTime
 snapshotDate)
        {
            DateTime cutoffDate = DateTime.Now.Add(new TimeSpan(-daysBack, 0, 0, 0));
            return (DateTime.Compare(snapshotDate, cutoffDate) < 0) ? true : false;
        }

        /*
         * Displays information related to a volume.
         */
        private static String OutputVolumeInfo(VolumeInfo vi)
        {
            String volumeInfo = String.Format(
                "Volume Info:\n" +
                "  ARN: {0}\n" +
                "  Type: {1}\n",
                vi.VolumeARN,
                vi.VolumeType);
            return volumeInfo;
        }
    }
}
```

使用 AWS Tools for Windows PowerShell删除快照

如需删除与卷关联的多个快照，您可以使用编程方法。以下示例演示如何使用 AWS Tools for Windows PowerShell删除快照。要使用示例脚本，您应该熟悉如何运行PowerShell 脚本。有关更多信息，请参阅 https://docs.aws.amazon.com/powershell/latest/userguide/pstools-getting-started.html 中的AWS Tools for Windows PowerShell入门。如果您只需要删除少量快照，请按 删除快照 中所述使用控制台。

Example : 使用删除快照 AWS Tools for Windows PowerShell

以下 PowerShell 脚本示例列出了网关每个卷的快照以及快照开始时间是在指定日期之前还是之后。它使用 Storage Gateway 和 Amazon EC2 的 AWS Tools for Windows PowerShell cmdlet。Amazon EC2 API 包括数种处理快照的操作。

您需要更新脚本并提供您的网关的 Amazon 资源名称 (ARN) 和想要保存快照的回溯天数。此截止日期之前拍摄的快照都将被删除。您还需要指定布尔值 `viewOnly`，该值表明是要查看要删除的快照还是实际执行快照删除。先只带 view 选项 (即将 `viewOnly` 设置为 `true`) 运行代码，看看代码会删除什么。

```
<#
.DESCRIPTION
    Delete snapshots of a specified volume that match given criteria.

.NOTES
    PREREQUISITES:
    1) AWS Tools for Windows PowerShell from https://aws.amazon.com/powershell/
    2) Credentials and AWS 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_DeleteSnapshots.ps1
#>

# Criteria to use to filter the results returned.
$daysBack = 18
$gatewayARN = "*** provide gateway ARN ***"
$viewOnly = $true;

#ListVolumes
$volumesResult = Get-SGVolume -GatewayARN $gatewayARN
$volumes = $volumesResult.VolumeInfos
Write-Output("`nVolume List")
foreach ($volumes in $volumesResult)
  { Write-Output("`nVolume Info:")
    Write-Output("ARN:  " + $volumes.VolumeARN)
    write-Output("Type: " + $volumes.VolumeType)
  }

Write-Output("`nWhich snapshots meet the criteria?")
foreach ($volume in $volumesResult)
```

```
  {
    $volumeARN = $volume.VolumeARN

    $volumeId = ($volumeARN-split"/")[3].ToLower()

    $filter = New-Object Amazon.EC2.Model.Filter
    $filter.Name = "volume-id"
    $filter.Value.Add($volumeId)

    $snapshots = get-EC2Snapshot -Filter $filter
    Write-Output("`nFor volume-id = " + $volumeId)
    foreach ($s in $snapshots)
    {
       $d = ([DateTime]::Now).AddDays(-$daysBack)
       $meetsCriteria = $false
       if ([DateTime]::Compare($d, $s.StartTime) -gt 0)
       {
            $meetsCriteria = $true
       }

       $sb = $s.SnapshotId + ", " + $s.StartTime + ", meets criteria for delete? " +
$meetsCriteria
       if (!$viewOnly -AND $meetsCriteria)
       {
           $resp = Remove-EC2Snapshot -SnapshotId $s.SnapshotId
           #Can get RequestId from response for troubleshooting.
           $sb = $sb + ", deleted? yes"
       }
       else {
           $sb = $sb + ", deleted? no"
       }
       Write-Output($sb)
    }
  }
```

了解卷状态和转换

每个卷均有关联的状态，让您一目了然地了解卷的运行状态。状态大多数时候会显示卷运行正常，无需您采取任何行动。在某些情况下，状态显示卷有问题，可能需要您执行相关操作，也可能不需要。您可以找到以下信息以帮助您决定何时需要采取行动。[你可以在 Storage Gateway 控制台上查看卷状态，也可以使用 Storage Gateway API 操作之一，例如 DescribeCachedisciVolumes 或 DescribeStoredisciVol umes。]

主题

- 理解卷状态
- 了解连接状态
- 了解缓存卷状态转换
- 了解存储卷状态转换

理解卷状态

下表显示了 Storage Gateway 控制台中的卷状态。卷状态显示在网关中各个存储卷的 Status (状态) 一栏中。正常工作的卷的状态显示为可用。

在下表中，您可以找到各个存储卷状态的描述，以及基于每种状态，您是否需要采取行动和应在何时采取行动。可用状态是卷的正常状态。在使用卷的所有或大部分时间，卷都应具有此状态。

Status	含义
Available	卷可供使用。此状态是卷的正常运行状态。 当正在引导阶段完成后，卷将恢复为可用状态。即，网关已同步自卷首次进入传递状态以来对卷所做的任何更改。
正在引导	网关正在本地将数据与存储在中的 AWS数据副本进行同步。您通常不需要针对该状态采取任何行动，因为大多情况下，存储卷将自动显示为可用状态。 以下是卷状态为正在引导的场景： • 网关意外关闭。 • 超出了网关的上传缓冲区容量。在这种情况下，当您的卷处于传递状态并且自由上传缓冲区空间充分增加时，将发生引导。您可以提供额外的上传缓冲区空间，作为提高自由上传缓冲区空间百分比的一种方式。在此特殊的情况下，存储卷从传递转为正在引导，再转为可用状态。您可在引导期间继续使用此卷。但此时您不能拍摄卷的快照。 • 您正在创建存储卷网关并保留现有磁盘数据。在这种情况下，您的网关开始将所有数据上传到 AWS。在本地磁盘上的所有数据都被复制到之

Status	含义
	前，该卷一直处于 Bootstrapping 状态。 AWS您可在引导期间继续使用此卷。但此时您不能拍摄卷的快照。
Creating	目前正在创建卷，因此尚不能使用它。正在创建状态是过渡型状态。无需采取行动。
Deleting	卷当前正在删除。正在删除状态是过渡型状态。无需采取行动。
无法恢复	发生错误，卷无法从其还原。有关在此情况下采取何种措施的信息，请参见 排查卷问题。

Status	含义
传递	本地维护的数据与存储在中的数据不同步 AWS。对处于传递状态的卷写入的数据将保持在缓存中，直至卷的状态成为正在引导。此数据开始上传到引导状态开始 AWS 时。 传递状态可因多种原因而出现，如下面所列： • 如果网关已用完上传缓冲区空间，则将出现传递状态。当卷均处于传递状态时，您的应用程序可继续在其中读取和写入数据。但是，网关不会向其上传缓冲区写入您的任何卷数据，也不会将任何此类数据上传到 AWS。 网关将继续上传在卷进入传递状态之前写入卷的任何数据。当卷处于传递状态时，存储卷的任何待处理或计划快照均会失败。有关因超出上传缓冲区容量而导致存储卷处于传递状态的情况下应执行的操作的信息，请参阅排查卷问题。 要返回“活动”状态，处于传递状态的卷必须完成正在引导阶段。在 Bootstrap ping 期间，该卷在内部重新建立同步 AWS，这样它就可以恢复对卷的更改的记录（日志），并激活功能。CreateSnapshot 在正在引导状态期间，写入到卷的内容记录在上传缓冲空间。 • 一次存在多个存储卷引导时，将出现传递状态。同一时间只能有一个存储卷进行自举。例如，假设您创建两个存储卷并选择保存两个存储卷上的现有数据。在这种情况下，第二个存储卷就会显示传递状态，直至第一个存储卷完成引导。在这种情况下，您不需要采取行动。各个存储卷将会在创建完成后自动转为可用状态。您可以在存储卷处于传递或正在引导状态时对其进行读写操作。 • 传递状态偶尔可能表示为上传缓冲区使用分配的磁盘已失效。有关在此场景中应采取何种行动的信息，请参阅 排查卷问题。 • 当卷处于活动或正在引导状态时，会出现传递状态。在这种情况下，卷收到一个写入，但上传缓冲区没有足够容量来记录该写入。 •

Status	含义
	当卷处于任何状态并且网关未完全关闭时，发生传递状态。发生这种类型的关闭的原因一是软件崩溃，二是 VM 关闭。在这种情况下，处于任意状态的卷都将进入传递状态。
Restoring (还原)	卷正在从现有快照还原。此状态仅适用于存储卷。有关更多信息，请参阅卷网关的工作原理（架构）。 如果您同时还原两个存储卷，则两个存储卷均会显示还原状态。各个存储卷将会在创建完成后自动转为可用状态。您可以在存储卷处于还原状态时对其进行读写操作并拍摄快照。
Restoring Pass Through (还原传递)	该卷正在从现有快照还原，并且遇到了上传缓冲区问题。此状态仅适用于存储卷。有关更多信息，请参阅卷网关的工作原理（架构）。 导致 Restoring Pass Through (还原传递) 状态的一个原因是您的网关已用完上传缓冲区空间。当存储卷处于 Restoring Pass Through (还原传递) 状态时，您的应用程序可继续在其中读取和写入数据。但是，在 Restoring Pass Through (还原传递) 状态期间，您无法拍摄存储卷的任何快照。有关存储卷因超出上传缓冲区容量而处于 Restoring Pass Through (还原传递) 状态时应采取操作的信息，请参阅排查卷问题。 Restoring Pass Through (还原传递) 状态偶尔也可能表示为上传缓冲区分配的磁盘失效。有关在此场景中应采取何种行动的信息，请参阅 排查卷问题。
Upload Buffer Not Configured (上传缓冲区未配置)	由于网关未配置上传缓冲区，因此您无法创建或使用卷。有关如何为缓存卷设置中的卷添加上传缓冲区容量的信息，请参阅确定要分配的上传缓冲区的大小。有关如何为存储卷设置中的卷添加上传缓冲区容量的信息，请参阅确定要分配的上传缓冲区的大小。

了解连接状态

您可以使用 Storage Gateway 控制台或 API，从网关分离卷或者将卷附加到网关。下表显示了 Storage Gateway 控制台中的卷附加状态。卷连接状态显示在网关中各个存储卷的连接状态列中。例如，已从网关中分离的卷具有已分离状态。有关如何附加和分离卷的信息，请参阅将您的卷迁移至不同的网关。

Status	含义
Attached (已附加)	卷已附加到网关。
Detached	卷已从网关上分离。
正在分离	卷正在从网关上分离。当您分离某个卷且该卷上没有数据时，可能不会看到此状态。

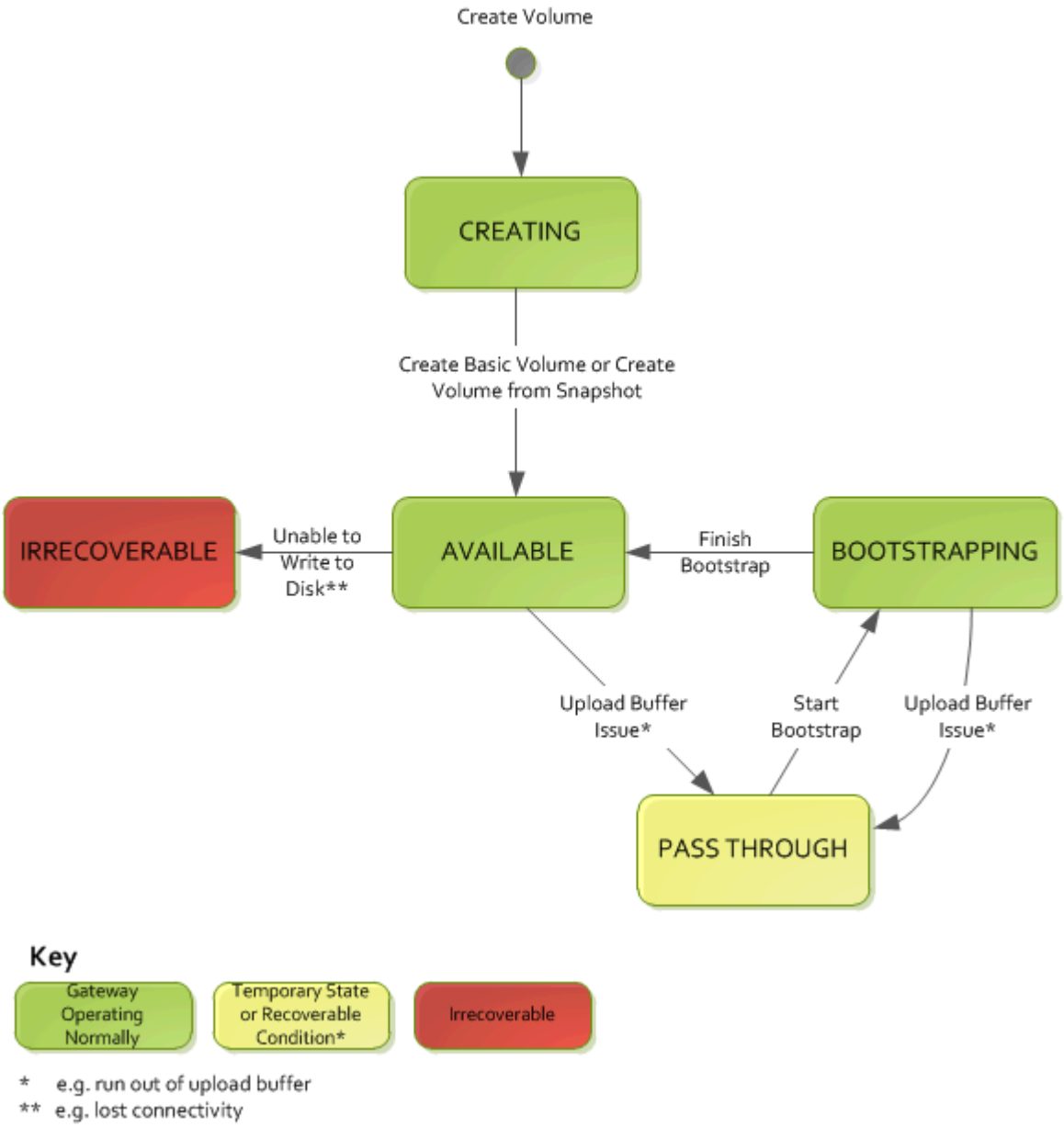
了解缓存卷状态转换

通过以下状态示意图了解缓存网关中卷状态之间的最常见转换。您无需详细了解该示意图就能有效使用网关。不过，如果您有兴趣进一步了解卷网关的工作方式，该示意图提供了详细的信息。

该示意图没有显示 Upload Buffer Not Configured (上传缓冲区未配置) 状态，也没有显示正在删除 状态。示意图中的卷状态以绿色、黄色和红色框的形式呈现。各种颜色的具体含义如下。

颜色	卷状态
Green	网关运行正常。卷状态为可用，或者最终变为可用。
黄色	卷处于传递状态，这表示存储卷具有潜在问题。如果该状态是由于上传缓冲区空间已满所致，那么在某些情况下，缓冲区空间可能变得再次可用。此时，存储卷将自动更正为可用状态。在其他情况下，您可能需要向网关添加更多上传缓冲区空间，以使存储卷状态转为可用。有关在超出上传缓冲区容量的情况下如何进行故障排除的信息，请参阅 排查卷问题。有关如何添加上传缓冲区容量的信息，请参阅 确定要分配的上传缓冲区的大小。
红光	存储卷处于无法恢复状态。在这种情况下，您应删除卷。有关如何执行此操作的信息，请参阅 删除卷。

在示意图中，两种状态之间的转换使用标记线表示。例如，从正在创建状态到可用状态的转换被标记为创建基本卷或从快照中创建卷。此转换表示正在创建缓存卷。有关创建存储卷的更多信息，请参阅添加卷。



> **Note**
>
> 卷状态传递在该示意图中显示为黄色。但是，这与 Storage Gateway 控制台的状态框中的此状态图标颜色不匹配。

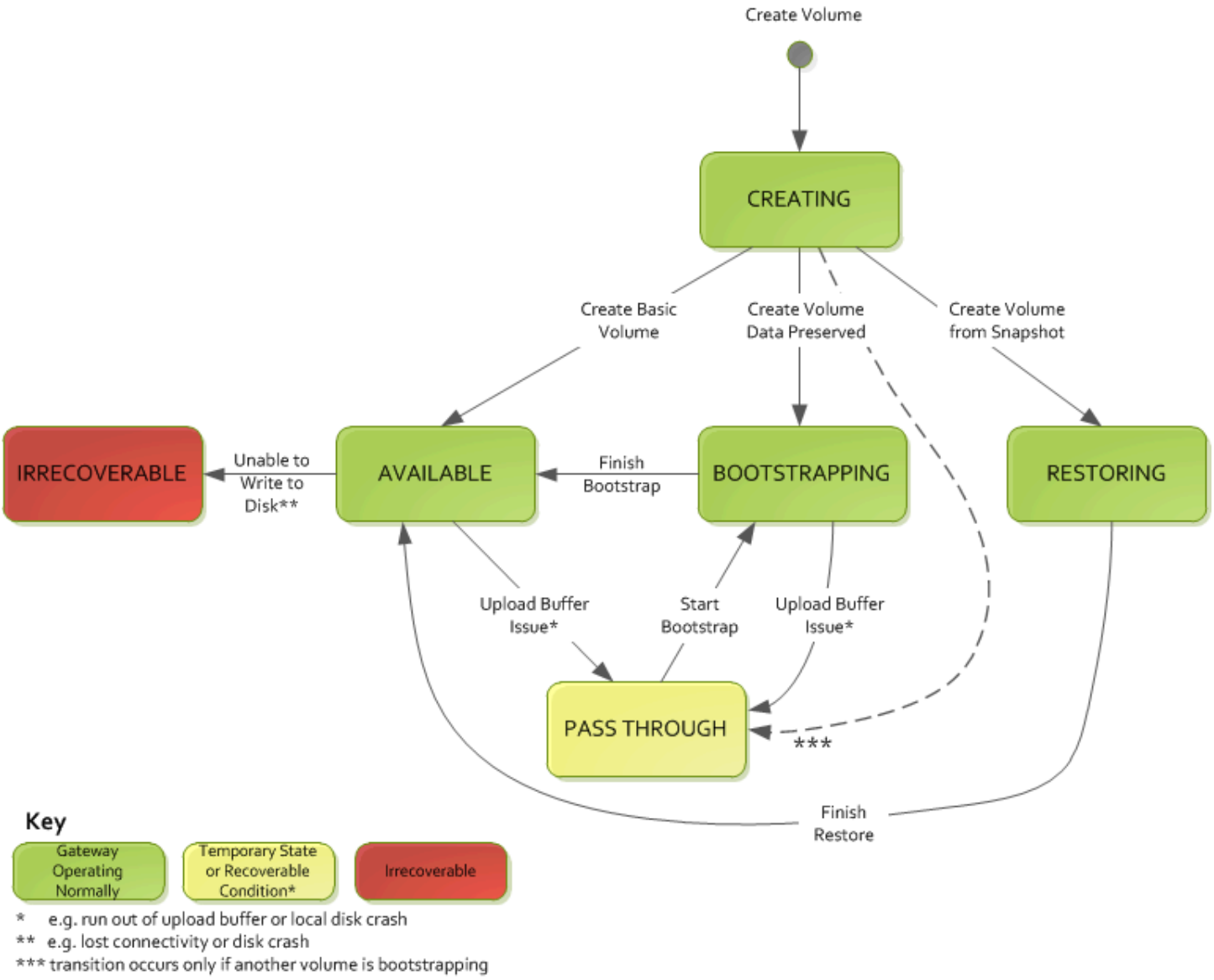
了解存储卷状态转换

通过以下状态示意图了解存储网关中卷状态之间的最常见转换。您无需详细了解该示意图就能有效使用网关。示意图只是在您希望详细了解卷网关的工作方式的情况下，为您提供详细信息。

该示意图没有显示 Upload Buffer Not Configured (上传缓冲区未配置) 状态，也没有显示正在删除 状态。示意图中的卷状态以绿色、黄色和红色框的形式呈现。各种颜色的具体含义如下。

颜色	卷状态
Green	网关运行正常。卷状态为可用，或者最终变为可用。
黄色	在您创建存储卷并保存数据时，如果另一个卷进行引导，则将出现从正在创建状态到传递状态的路径。在这种情况下，如果第一个卷完成引导，则处于传递状态的卷将转为正在引导状态再转为可用状态。除了所述具体情况外，黄色（传递状态）表示存储卷可能存在问题，最常见的一个问题是上传缓冲区问题。如果超出了上传缓冲区容量，则某些情况下缓冲区空间将变得再次可用。此时，存储卷将自动更正为可用状态。在其他情况下，您可能需要向网关添加更多上传缓冲区容量，以使存储卷返回可用状态。有关在超出上传缓冲区容量的情况下如何进行故障排除的信息，请参阅 排查卷问题。有关如何添加上传缓冲区容量的信息，请参阅 确定要分配的上传缓冲区的大小。
红光	存储卷处于无法恢复状态。在这种情况下，您应删除卷。有关如何执行此操作的信息，请参阅 删除卷。

在下面的示意图中，两种状态之间的转换用标记线表示。例如，从正在创建状态到可用状态的转换被标记为创建基本卷。此转换表示在不保存数据的情况下创建存储卷或者从快照创建卷。



> **Note**
>
> 卷状态传递在该示意图中显示为黄色。但是，这与 Storage Gateway 控制台的状态框中的此状态图标颜色不匹配。

将数据移至新网关

随着数据和性能需求的增长，或者收到迁移网关的 AWS 通知，您可以在网关之间移动数据。以下是要移动数据的一些原因：

- 将数据移动到更好的主机平台或者较新的 Amazon EC2 实例。
- 刷新服务器的底层硬件。

将数据移至新网关所遵循的步骤取决于您的网关类型。

> **Note**
>
> 数据只能在相同类型的的网关之间移动。

将存储卷移至新的存储卷网关

将存储卷移至新的存储卷网关

1. 停止正在写入旧存储卷网关的所有应用程序。
2. 按照以下步骤创建卷的快照，然后等待快照完成。

   a. 打开 Storage Gateway 控制台，网址为 https://console.aws.amazon.com/storagegateway/home。

   b. 在导航窗格中，选择卷，然后选择要从中创建快照的卷。

   c. 对于操作，选择创建快照。

   d. 在创建快照对话框中，输入快照描述，然后选择创建快照。

   您可以验证是否已使用控制台创建快照。如果数据仍在上传到该卷，请等到上传完成，然后再执行下一步操作。要查看快照状态并确认没有快照处于待处理状态，请选择卷上的快照链接。
3. 按照以下步骤停止旧的存储卷网关：

   a. 在导航窗格中，选择网关，然后选择要停止的旧存储卷网关。网关处于 Running 状态。

   b. 在操作部分，选择停止网关。验证对话框中的网关 ID，然后选择停止网关。

   在网关停止时，您可能会看到指示网关状态的消息。当网关关闭时，详细信息选项卡中会显示一条消息和启动网关按钮。当网关关闭时，网关的状态为关闭。

   c. 使用管理程序控件关闭 VM。

   有关停止网关的更多信息，请参阅启动和停止卷网关。
4. 将与您的存储卷关联的存储磁盘与网关 VM 分离。这不包括 VM 的根磁盘。

5. 使用 Storage Gateway 控制台提供的新管理程序 VM 映像来激活新的存储卷网关，网址为 https://console.aws.amazon.com/storagegateway/home。
6. 连接您在步骤 5 中从旧的存储卷网关 VM 中分离的物理存储磁盘。
7. 要保留磁盘上的现有数据，请按照以下步骤来创建存储卷。

   a. 在 Storage Gateway 控制台中，选择创建卷。

   b. 在创建卷对话框中，选择您在步骤 5 中创建的存储卷网关。

   c. 从列表中选择一个磁盘 ID 值。

   d. 对于卷内容，选择保留磁盘上的现有数据选项。

   有关创建卷的更多信息，请参阅创建卷。
8. （可选）在出现的配置 CHAP 身份验证向导中，在各自的框中输入启动程序名称、启动程序密钥和目标密钥，然后选择保存。

   有关使用质询握手身份验证协议 (CHAP) 身份验证的更多信息，请参阅为 iSCSI 目标配置 CHAP 身份验证。
9. 启动写入存储卷的应用程序。
10. 确认新的存储卷网关运行正常后，可以删除旧的存储卷网关。

> **Important**
>
> 删除网关之前，请确保当前没有应用程序正在写入到网关的卷。如果您在网关使用期间删除网关，则会造成数据丢失。

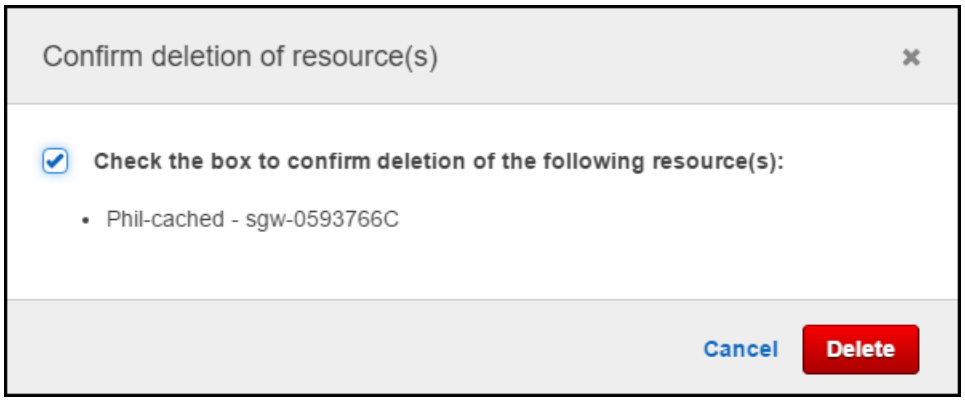
按照以下步骤删除旧的存储卷网关：

> **Warning**
>
> 删除网关后便无法恢复。

a. 在导航窗格中，选择网关，然后选择要删除的旧存储卷网关。

b. 对于 Actions (操作)，请选择 Delete gateway (删除网关)。

c. 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 指定了要删除的旧存储卷网关。然后选择删除。



11. 删除旧的网关 VM。有关删除 VM 的信息，请参阅管理程序的文档。

将缓存卷移至新的缓存卷网关虚拟机。

将缓存卷移至新的缓存卷网关虚拟机 (VM)

1. 停止正在写入旧缓存卷网关的所有应用程序。
2. 卸载 iSCSI 卷或断开与任何正在使用 iSCSI 卷的客户端的连接。由于可以防止客户端更改数据或向这些卷添加数据，从而有助于使这些卷上的数据保持一致。
3. 按照以下步骤创建卷的快照，然后等待快照完成。

   a. 打开 Storage Gateway 控制台，网址为 https://console.aws.amazon.com/storagegateway/home。

   b. 在导航窗格中，选择卷，然后选择要从中创建快照的卷。

   c. 对于操作，选择创建快照。

   d. 在创建快照对话框中，输入快照描述，然后选择创建快照。

   您可以验证是否已使用控制台创建快照。如果数据仍在上传到该卷，请等到上传完成，然后再执行下一步操作。要查看快照状态并确认没有快照处于待处理状态，请选择卷上的快照链接。

   有关在控制台中检查卷状态的更多信息，请参阅了解卷状态和转换。有关缓存卷状态的信息，请参阅了解缓存卷状态转换 。

4. 按照以下步骤停止旧的缓存卷网关：

   a. 在导航窗格中，选择网关，然后选择要停止的旧缓存卷网关。网关处于 Running 状态。

b. 在操作部分，选择停止网关。验证对话框中的网关 ID，然后选择停止网关。请记录网关 ID，因为在后面的步骤中需要用到。

   在旧网关停止时，您可能会看到指示网关状态的消息。当旧网关关闭时，详细信息选项卡中会显示一条消息和启动网关按钮。当网关关闭时，网关的状态为关闭。

c. 使用管理程序控件关闭旧 VM。有关关闭 Amazon EC2 实例的更多信息，请参阅 Amazon EC2 用户指南中的停止和启动您的实例。有关关闭 KVM、VMware 或 Hyper-V VM 的更多信息，请参阅管理程序文档。

有关停止网关的更多信息，请参阅启动和停止卷网关。

5. 将所有磁盘（包括根磁盘、缓存磁盘和上传缓冲区磁盘）与旧网关 VM 分离。

> **Note**
>
> 记下根磁盘的卷 ID 以及与该根磁盘关联的网关 ID。您将在稍后的步骤中将此磁盘与新的 Storage Gateway 管理程序分离。（请参阅步骤 11。）

如果您使用亚马逊 EC2 实例作为缓存卷网关的虚拟机，请参阅 Amazon EC2 用户指南中的将 Amazon EBS 卷与 Linux 实例分离。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。

6. 创建新的 Storage Gateway 管理程序 VM 实例，但不要将其作为网关激活。有关创建新的 Storage Gateway 管理程序 VM 的更多信息，请参阅设置卷网关。这个新网关将代入旧网关的身份。

> **Note**
>
> 请勿向新 VM 添加用作缓存或上传缓冲区的磁盘。您的新 VM 将使用与旧 VM 相同的缓存磁盘和上传缓冲区磁盘。

7. 您的新 Storage Gateway 管理程序 VM 实例应使用与旧 VM 相同的网络配置。网关的默认网络配置是动态主机配置协议 (DHCP)。使用 DHCP 时，系统会为您的网关自动分配 IP 地址。

   如果您需要为新 VM 手动配置静态 IP 地址，请参阅配置网关网络，了解更多详细信息。如果您的网关必须使用 Socket Secure 版本 5 (SOCKS5) 代理才能连接到 Internet，请参阅通过代理路由本地网关，了解更多详细信息。

8. 启动新 VM。

9. 将您在步骤 5 中从旧的缓存卷网关 VM 中分离的磁盘连接到新的缓存卷网关。按照与旧网关 VM 相同的顺序将它们连接到新网关 VM。

   所有磁盘都必须使转换保持不变。请勿更改卷大小，因为这会导致元数据变得不一致。

10. 通过使用以下格式的 URL 连接到新 VM，启动网关迁移过程。

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

    您可以为新网关 VM 重复使用与旧网关 VM 相同的 IP 地址。您的 URL 应类似于以下示例。

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

    在浏览器中或在命令行中通过 `curl` 来使用此 URL，启动迁移过程。

    成功启动网关迁移过程后，您会看到以下消息：

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

11. 分离旧网关的根磁盘，您在步骤 5 中记下了该磁盘的卷 ID。
12. 启动网关。

    按照以下步骤启动新的缓存卷网关：

    a. 打开 Storage Gateway 控制台，网址为 https://console.aws.amazon.com/storagegateway/home。
    b. 在导航窗格中，选择网关，然后选择要启动的新网关。网关处于 Shutdown 状态。
    c. 选择详细信息，然后选择启动网关。

    有关启动网关的更多信息，请参阅启动和停止卷网关。

13. 现在，您的应用程序应该可以使用新网关 VM 的 IP 地址来访问您的卷。
14. 确认您的卷可用，然后删除旧网关 VM。有关删除 VM 的信息，请参阅管理程序的文档。

监控 Storage Gateway

本节介绍如何使用 Amazon 监控网关，包括监控与网关关联的资源 CloudWatch。您可以监控网关的上传缓冲区和缓存存储。使用 Storage Gateway 控制台来查看网关的指标和警报。例如，您可以查看读写操作中使用的字节数、读写操作耗费的时间以及从 Amazon Web Services 云检索数据耗费的时间。借助指标，您可以跟踪网关的运行状况并设置警报，以便在一个或多个指标超出定义的阈值时通知您。

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

主题

- 了解网关指标
- Storage Gateway 指标的维度
- 监控上传缓冲区
- 监控缓存存储
- 了解 CloudWatch 警报
- 为您的网关创建推荐的 CloudWatch 警报
- 为您的网关创建自定义 CloudWatch 警报
- 监控卷网关

了解网关指标

在本主题的讨论中，我们将网关指标定义为限定在网关范围内的指标，也就是说，这些指标衡量网关的某方面性能。由于一个网关包含一个或多个卷，因此网关特定的指标代表网关上的所有卷。例如，`CloudBytesUploaded` 指标是网关在报告期间发送给云的字节的总数。该指标包括网关上所有卷的活动。

使用网关指标数据时，应指定您希望查看其指标的网关的唯一标识。为此，您可指定 `GatewayId` 和 `GatewayName` 值。希望使用网关的指标时，您在指标命名空间中指定网关维度，该维度将网关专属的指标从卷专属的指标区分开。有关更多信息，请参阅使用亚马逊 CloudWatch 指标。

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

指标	描述
AvailabilityNotifications	网关生成的与可用性相关的运行状况通知数。 将此指标与 Sum 统计数据结合使用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，请查看您配置的 CloudWatch 日志组。 单位：数字
CacheHitPercent	缓存传送的应用程序读取率。样本在报告周期结束时采用。 单位：百分比
CacheUsed	网关的缓存存储中正在使用的字节总数。样本在报告周期结束时采用。 单位：字节
IoWaitPercent	网关等待本地磁盘响应的时间百分比。 单位：百分比
MemTotalBytes	为网关 VM 预配置的 RAM 量，以字节为单位。 单位：字节

指标	描述	
MemUsedBytes	网关 VM 当前正在使用的 RAM 量，以字节为单位。 单位：字节	
QueuedWrites	等待写入的字节数 AWS，在报告周期结束时对网关中所有卷进行采样。这些字节保存在网关的工作存储空间中。 单位：字节	
ReadBytes	报告周期内网关中的所有卷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	
ReadTime	报告周期内网关中所有卷从本地应用程序进行读取操作所耗费的总毫秒数。 将该指标与 Average 统计数据结合使用可测量延迟。 单位：毫秒	
TimeSinceLastRecoveryPoint	自上次可用还原点以来的时间。有关更多信息，请参阅[您的缓存网关无法访问，您希望恢复数据]。 单位：秒	

指标	描述
TotalCacheSize	以字节为单位的缓存总大小。样本在报告周期结束时采用。 单位：字节
UploadBufferPercentUsed	网关上传缓冲区的使用率。样本在报告周期结束时采用。 单位：百分比
UploadBufferUsed	网关的上传缓冲区正在使用的总字节数。样本在报告周期结束时采用。 单位：字节
UserCpuPercent	网关处理所花 CPU 时间的百分比，在所有核心上平均计算。 单位：百分比
WorkingStorageFree	网关的工作存储空间中未使用的总空间量。样本在报告周期结束时采用。 单位：字节
WorkingStoragePercentUsed	网关上传缓冲区的使用率。样本在报告周期结束时采用。 单位：百分比
WorkingStorageUsed	网关的上传缓冲区正在使用的总字节数。样本在报告周期结束时采用。 单位：字节

指标	描述
WriteBytes	报告周期内网关中所有卷写入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
WriteTime	报告周期内网关中所有卷从本地应用程序进行写入操作所耗费的总毫秒数。 将该指标与 Average 统计数据结合使用可测量延迟。 单位：毫秒

Storage Gateway 指标的维度

Storage Gateway 服务的 CloudWatch 命名空间是AWS/StorageGateway。数据在 5 分钟期间内自动可用，无需收费。

维度	描述
GatewayId ，GatewayName	这些维度会将您请求的数据筛选为特定于网关的指标。您可以通过 GatewayId 或 GatewayName 的值标识要工作的网关。如果在您需要查看指标的这段时间范围内，网关的名称发生了变化，则请使用 GatewayId 。 网关的吞吐量和延迟数据基于网关的所有卷。有关使用网关指标的信息，请参阅衡量网关和之间的性能 AWS。

维度	描述
VolumeId	该维度会将您请求的数据限定为特定于卷的指标。通过要使用的存储卷的 VolumeId 值标识该存储卷。有关使用卷指标的信息，请参阅测量应用程序与网关之间的性能。

监控上传缓冲区

您可以在下面找到有关如何监控网关的上传缓冲区以及如何创建警报以便您在缓冲区超出指定阈值时收到通知的信息。通过使用此方法，您可以在缓冲区存储空间充满并且存储应用程序停止备份到 AWS 前，向网关添加缓冲区存储。

在缓存卷和磁带网关架构中以相同的方式监控上传缓冲区。有关更多信息，请参阅卷网关的工作原理（架构）。

> **Note**
>
> 在 Storage Gateway 中的缓存卷功能发布前，WorkingStoragePercentUsed、WorkingStorageUsed 和 WorkingStorageFree 指标仅适用于存储卷的上传缓冲区。现在，请使用等效上传缓冲区指标 UploadBufferPercentUsed、UploadBufferUsed 和 UploadBufferFree。这些指标适用于两种网关架构。

关注项	如何测量
上传缓冲区使用率	将 UploadBufferPercentUsed 、UploadBufferUsed 和 UploadBufferFree 指标与 Average 统计数据结合使用。例如，将 UploadBufferUsed 与 Average 结合使用，以分析一段时间内的存储使用率。

测量使用的上传缓冲区的百分比

1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 选择 StorageGateway：网关指标维度，然后找到要使用的网关。

3. 选择 UploadBufferPercentUsed 指标。
4. 对于 Time Range，请选择一个值。
5. 选择 Average 统计数据。
6. 对于 Period，请选择值 5 分钟以匹配默认报告时间。

得出的按时间排序的数据点集包含上传缓冲区的使用率。

按照以下步骤，您可以使用 CloudWatch 控制台创建警报。要了解有关警报和阈值的更多信息，请参阅 Amazon CloudWatch 用户指南中的创建 CloudWatch 警报。

如需为网关的上传缓冲区设置上阈值警报

1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 选择 Create Alarm (创建警报) 可启动“Create Alarm (创建警报)”向导。
3. 为您的警报指定指标：
   a. 在创建警报向导的选择指标页面上 GatewayId，选择AWS/StorageGateway:，GatewayName 维度，然后找到要使用的网关。
   b. 选择 UploadBufferPercentUsed 指标。使用 Average 统计数据和 5 分钟的周期。
   c. 选择继续。
4. 定义警报名称、描述和阈值：
   a. 在“Create Alarm (创建警报)”向导的 Define Alarm (定义警报) 页面上，通过分别在 Name (名称) 和 Description (描述) 框中为您的警报提供名称和说明来标识警报。
   b. 定义警报阈值。
   c. 选择继续。
5. 针对该警报配置电子邮件操作：
   a. 在“创建警报”向导的配置操作页面上，为警报状态选择警报。
   b. 为主题选择选择或创建电子邮件。

      创建电子邮件主题意味着设置 Amazon SNS 主题。有关亚马逊 SNS 的更多信息，请参阅亚马逊用户指南中的设置亚马逊 SNS。 CloudWatch
   c. 对于 Topic (主题)，请为主题输入一个描述性名称。
   d. 选择 Add Action。

e. 选择继续。

6. 检查警报设置，然后创建警报：

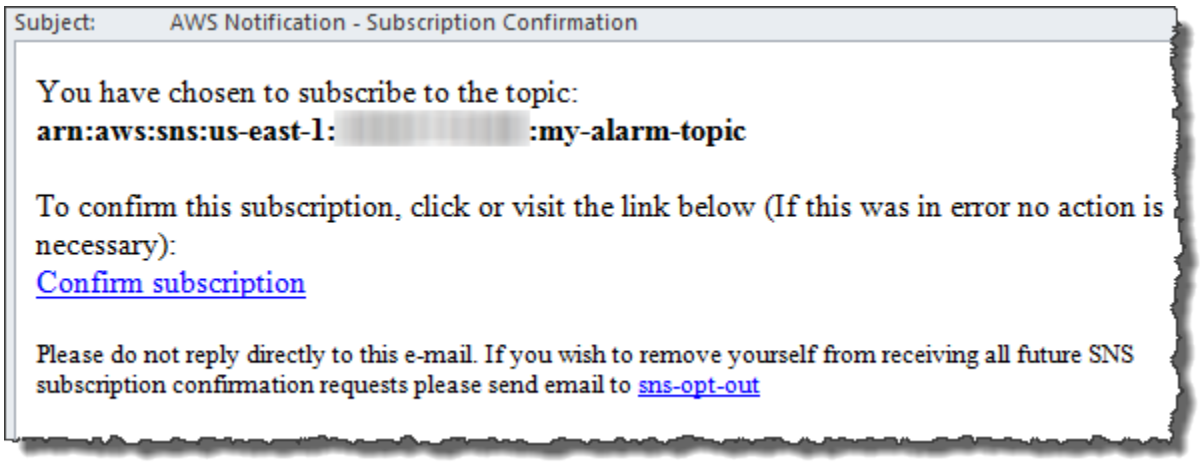
   a. 在“Create Alarm (创建警报)”向导的 Review (查看) 页面上，查看警报定义、指标和要执行的相关操作（例如，发送电子邮件通知）。

   b. 检查警报摘要后，选择 Save Alarm。

7. 确认您对警报主题的订阅：

   a. 打开已发送到您在创建主题时指定的电子邮件地址的 Amazon SNS 电子邮件。

      下图显示了典型电子邮件通知。



   b. 单击电子邮件中的链接，确认您的订阅。

      将显示订阅确认。

监控缓存存储

您可以在下面找到有关如何监控网关的缓存存储以及如何创建警报以便您在缓存参数超过指定阈值时收到通知的信息。通过使用此警报，您可以了解何时向网关添加缓存存储。

您只能监控缓存卷架构中的缓存存储。有关更多信息，请参阅卷网关的工作原理（架构）。

关注项	如何测量
缓存总使用率	将 `CachePercentUsed` 和 `TotalCacheSize` 指标结合 `Average` 统计数据使用。例如，将 `CachePercentUsed` 与 `Average` 统计数据结合使用，以分析一段时间内的缓存使用率。

关注项	如何测量
	`TotalCacheSize` 指标仅在您向网关添加缓存时变化。
从缓存中提供的读取请求的百分比	将 `CacheHitPercent` 指标与 `Average` 统计数据结合使用。 通常，您希望 `CacheHitPercent` 保持较高。
缓存中肮脏的百分比，也就是说，它包含尚未上传到的内容 AWS	将 `CachePercentDirty` 指标与 `Average` 统计数据结合使用。 一般而言，您希望 `CachePercentDirty` 保持较低。

测量网关及其所有卷的缓存废数据百分比

1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 选择 StorageGateway：网关指标维度，然后找到要使用的网关。
3. 选择 `CachePercentDirty` 指标。
4. 对于 Time Range，请选择一个值。
5. 选择 `Average` 统计数据。
6. 对于 Period，请选择值 5 分钟以匹配默认报告时间。

得出的按时间排序的数据点集包含 5 分钟以上的时间内的缓存废数据率。

测量卷的缓存废数据百分比

1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 选择 StorageGateway：交易量指标维度，然后找到您要使用的交易量。
3. 选择 `CachePercentDirty` 指标。
4. 对于 Time Range，请选择一个值。
5. 选择 `Average` 统计数据。
6. 对于 Period，请选择值 5 分钟以匹配默认报告时间。

得出的按时间排序的数据点集包含 5 分钟以上的时间内的缓存废数据率。

了解 CloudWatch 警报

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

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

对于每个激活的网关，我们建议您创建以下 CloudWatch 警报：

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

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

对于已激活 HA 模式的 VMware 主机平台上的网关，我们还建议使用此额外 CloudWatch 警报：

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

下表描述了警报的状态。

省/自治区/直辖市	描述
确定	指标或表达式在定义的阈值范围内。

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

为您的网关创建推荐的 CloudWatch 警报

使用 Storage Gateway 控制台创建新网关时，可以选择在初始设置过程中自动创建所有推荐的 CloudWatch 警报。有关更多信息，请参阅配置卷网关。如果要为现有网关添加或更新推荐的 CloudWatch 警报，请按以下步骤操作。

为现有网关添加或更新推荐的 CloudWatch 警报

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

1. 打开 Storage Gateway 控制台，网址为 https://console.aws.amazon.com/storagegateway/home/。
2. 在导航窗格中，选择 Gateways，然后选择要为其创建推荐 CloudWatch 警报的网关。
3. 在网关详细信息页面上，选择监控选项卡。

4. 在警报下，选择创建推荐警报。自动创建推荐的警报。

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

为您的网关创建自定义 CloudWatch 警报

CloudWatch 使用亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 在警报状态发生变化时发送警报通知。警报会监控您指定的一段时间内的一个指标，并根据相对于给定阈值的指标值每隔若干个时间段执行一项或多项操作。操作是向 Amazon SNS 主题发送的通知。您可以在创建警报时创建 Amazon SNS 主题。 CloudWatch 有关 Amazon SNS 的更多信息，请参阅《Amazon Simple Notification Service 开发人员指南》中的什么是 Amazon SNS？

在 Storage Gateway 控制台中创建 CloudWatch 警报

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

   - 静态阈值警报：基于所选指标的设定阈值的警报。在指标超过阈值的时间达到指定数量的评估期时，警报将变为“警报”状态。

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

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

要创建指标数学表达式警报，请参阅 Amazon CloudWatch 用户指南中的基于指标数学表达式创建 CloudWatch 警报。

- 复合警报：通过监控其他警报的警报状态来确定其警报状态的警报。复合警报可以帮助您降低警报噪音。

  要创建复合警报，请参阅 Amazon CloudWatch 用户指南中的创建复合警报。

6. 在 CloudWatch 控制台中创建警报后，返回到 Storage Gateway 控制台。您可以通过执行以下操作之一查看警报：

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

     警报部分列出了特定网关的所有 CloudWatch 警报。在这里，您可以选择和删除一个或多个警报、打开或关闭警报操作以及创建新的警报。
   - 在导航窗格中，选择网关，然后选择要查看其警报的网关的警报状态。

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

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

监控卷网关

本节说明了如何在缓存卷或存储卷环境中监控网关，包括监控与网关关联的卷以及监控上传缓冲区。您可以使用 AWS Management Console 来查看网关的指标。例如，您可以查看读写操作中使用的字节数、读写操作耗费的时间以及从 Amazon Web Services 云检索数据耗费的时间。借助指标，您可以跟踪网关的运行状况并设置警报，以便在一个或多个指标超出定义的阈值时通知您。

Storage Gateway 免费提供 CloudWatch 指标。记录为期两周的 Storage Gateway 指标。通过使用这些指标，您可以访问历史信息并更好地了解您的网关和卷的表现。有关详细信息 CloudWatch，请参阅 Amazon CloudWatch 用户指南。

主题

- 使用 Amazon 日志获取卷网关健康 CloudWatch 日志
- 使用亚马逊 CloudWatch 指标
- 衡量您的应用程序和网关间的性能。
- 衡量网关与 AWS间的性能
- 了解卷指标

使用 Amazon 日志获取卷网关健康 CloudWatch 日志

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

例如，假设您的网关已部署到激活了 VMware High Availability (HA) 的集群中，并且您需要了解任何错误情况。您可以配置 CloudWatch 日志组来监控您的网关，并在网关遇到错误时收到通知。您可以在激活网关时或在激活网关并运行后配置组。有关如何在激活网关时配置 CloudWatch 日志组的信息，请参阅配置卷网关。有关 CloudWatch 日志组的一般信息，请参阅 Amazon CloudWatch 用户指南中的使用日志组和日志流。

有关如何排查和修复此类错误的信息，请参阅排查卷问题。

以下过程说明如何在激活网关后配置 CloudWatch 日志组。

配置 CloudWatch 日志组以使用您的网关

1. 登录 AWS Management Console 并打开 Storage Gateway 控制台，网址为 https://console.aws.amazon.com/storagegateway/home。
2. 在左侧导航窗格中，选择 Gateways，然后选择要为其配置 CloudWatch 日志组的网关。
3. 在 “操作” 中，选择 “编辑网关信息”，或者在 “详细信息” 选项卡上，在 “He alth log s” 和 “未启用” 下，选择 “配置日志组” 以打开 *CustomerGatewayName*“编辑” 对话框。
4. 对于网关运行状况日志组，请选择以下选项之一：
   - 如果您不想使用@@ 日志组监控网关，请禁用 CloudWatch 日志记录。
   - 创建新的日志组以创建新的 CloudWatch 日志组。
   - 使用现有日志组使用已存在的 CloudWatch 日志组。从现有日志组列表中选择一个日志组。
5. 选择 保存更改。
6. 要查看网关的运行状况日志，请执行以下操作：

1. 在左侧导航窗格中，选择 Gateways，然后选择您为其配置 CloudWatch 日志组的网关。
2. 选择详细信息选项卡，然后在 Healt h Logs 下选择CloudWatch 日志。日志组详情页面将在 Amazon CloudWatch 控制台中打开。

使用亚马逊 CloudWatch 指标

您可以使用 AWS Management Console 或 CloudWatch API 获取网关的监控数据。控制台根据来自 CloudWatch API 的原始数据显示一系列图表。您也可以通过AWS 软件开发套件 (SDK) 或亚马逊 CloudWatch API 工具使用 API。 CloudWatch 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。

无论选择何种方法使用指标，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 的维度为 `GatewayId`、`GatewayName` 和 `VolumeId`。在 CloudWatch 控制台中，您可以使用`Gateway Metrics`和`Volume Metrics`视图轻松选择特定于网关的维度和特定于卷的维度。有关尺寸的更多信息，请参阅 Amazon CloudWatch 用户指南中的尺寸。
- 指标名称，如 `ReadBytes`。

下表总结了您可使用的 Storage Gateway 指标数据的类型。

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` 维度标识要使用的网关。 网关的吞吐量和延迟数据基于网关中的所有卷。 数据在 5 分钟期间内自动可用，无需收费。
	`VolumeId`	该维度筛选卷专属指标数据。通过卷的 `VolumeId` 维度标识要使用的卷。 数据在 5 分钟期间内自动可用，无需收费。

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

- 查看可用指标
- 获取指标的数据
- 创建 CloudWatch 警报

衡量您的应用程序和网关间的性能。

数据吞吐量、数据延迟和每秒操作数是您可用来了解使用网关的应用程序存储性能状况的三个度量指标。当使用正确的聚合统计数据时，您可使用 Storage Gateway 指标来度量这些值。

统计数据 是某指标在指定时间内的集合。在中查看指标值时 CloudWatch，使用统计数据表示数据延迟（毫秒），使用Average统计数据表示数据吞吐量（每秒字节数），使用Sum统计数据表示每秒输入/输出操作数 (IOPS)。Samples有关更多信息，请参阅 Amazon CloudWatch 用户指南中的统计数据。

下表总结了可用来衡量应用程序和网关之间的吞吐量、延迟和 IOPS 的指标和相应统计数据。

关注项	如何测量
吞吐量	将 `ReadBytes` 和 `WriteBytes` 指标结合 Sum CloudWatch 统计数据使用。例如，5 分钟采样周期内的 Sum 指标的 `ReadBytes` 值除以 300 秒可以得出每秒字节数速率的吞吐量。
延迟	将 `ReadTime` 和 `WriteTime` 指标结合 `Average` CloudWatch 统计数据使用。例如，`Average` 指标的 `ReadTime` 值为您提供采样周期内的每个操作的延迟时间。
IOPS	将 `ReadBytes` 和 `WriteBytes` 指标结合 `Samples` CloudWatch 统计数据使用。例如，5 分钟采样周期内的 `Samples` 指标的 `ReadBytes` 值除以 300 秒可以得出 IOPS。

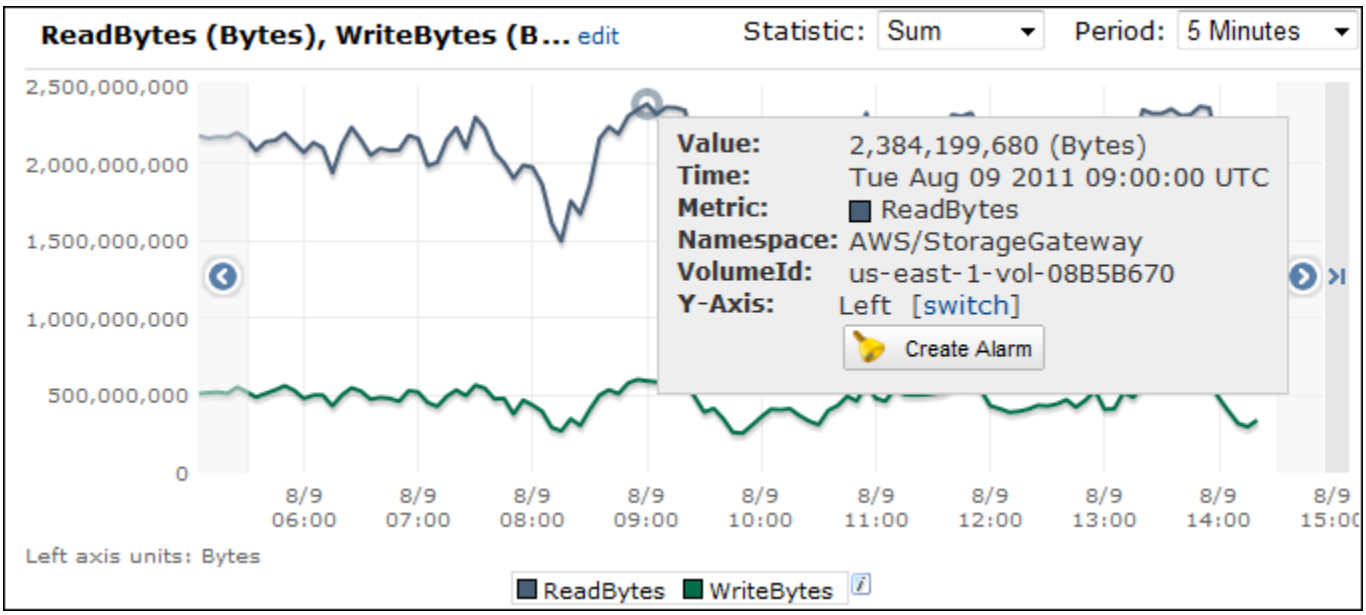
对于平均延迟图表和平均大小图表，平均值通过该期间内完成的操作（读取或写入，以适用于图表者为准）总数计算得出。

度量应用程序到卷的数据吞吐量

1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。

2. 选择 Metrics，再选择 All metrics 选项卡，然后选择 Storage Gateway。
3. 选择 Volume metrics 维度，然后找到要使用的卷。
4. 选择 `ReadBytes` 和 `WriteBytes` 指标。
5. 对于 Time Range，请选择一个值。
6. 选择 Sum 统计数据。
7. 对于 Period，请选择值 5 分钟或更长的时间。
8. 在得出的按时间排序的数据点集中，(其中一个用于 `ReadBytes`，另一个用于 `WriteBytes`)，将各个数据点除以周期 (以秒为单位) 得出采样点当时的吞吐量。总吞吐量是各个点吞吐量的和。

下图使用 `ReadBytes` 统计数据显示了卷的 `WriteBytes` 和 Sum 指标。在图中，将光标悬浮在数据点上就会显示该数据点信息，包括其值和字节数。将字节值除以 Period 值 (5 分钟) 得出采样点当时的数据吞吐量。对于高亮点，读取吞吐量是 2384199680 字节除以 300 秒，即 7.6MB/s。

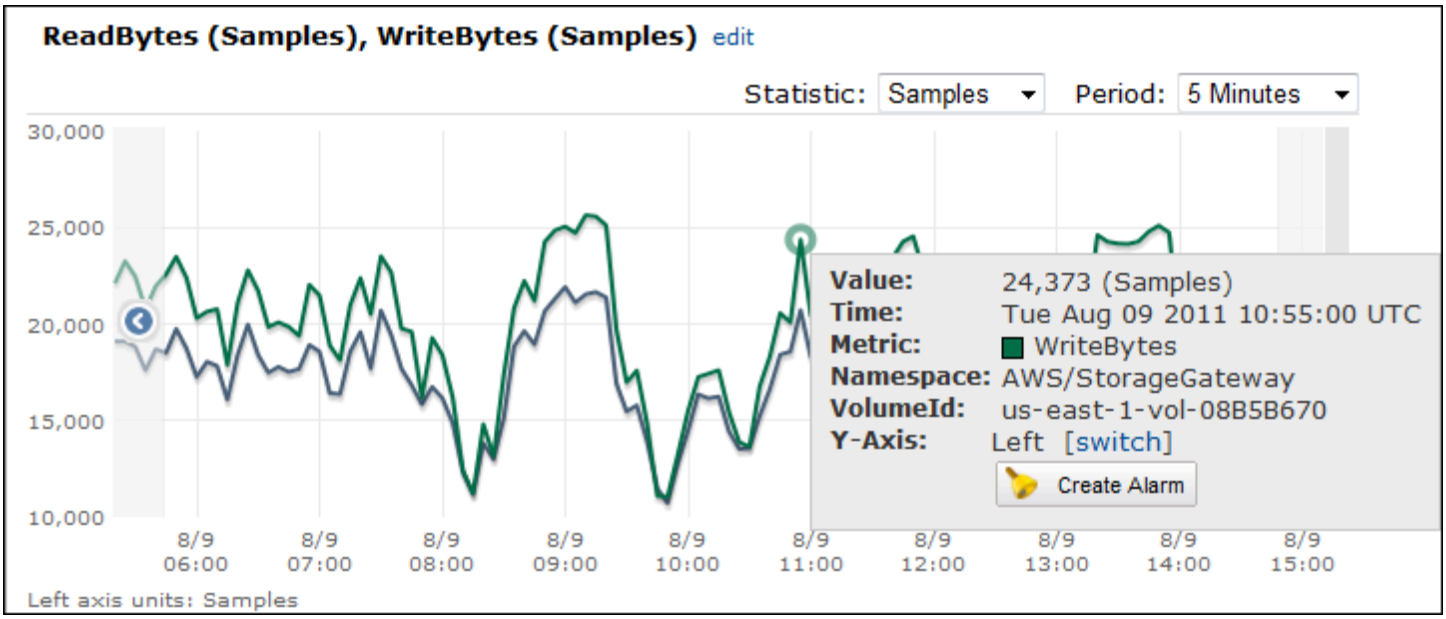


测量从应用程序到卷的每秒输入/输出操作数

1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 选择 Metrics，再选择 All metrics 选项卡，然后选择 Storage Gateway。
3. 选择 Volume metrics 维度，然后找到要使用的卷。
4. 选择 `ReadBytes` 和 `WriteBytes` 指标。
5. 对于 Time Range，请选择一个值。
6. 选择 `Samples` 统计数据。

7. 对于 Period，请选择值 5 分钟或更长的时间。
8. 在得出的按时间排序的数据点集中 (其中一个用于 ReadBytes，另一个用于 WriteBytes)，将各个数据点除以周期 (以秒为单位) 得出 IOPS。

下图使用 ReadBytes 统计数据显示了存储卷的 WriteBytes 和 Samples 指标。在图中，将光标悬浮在数据点上就会显示该数据点信息，包括其值和样本数。将采样值除以 Period 值 (5 分钟) 得出采样点当时的每秒操作数。对于高亮点，写入操作数是 24373 字节除以 300 秒，即每秒 81 次写入操作。



衡量网关与 AWS间的性能

数据吞吐量、数据延迟和每秒操作是您可用来理解使用 Storage Gateway 的应用程序存储性能状况的三个衡量指标。这三个值均可使用 Storage Gateway 指标来衡量，这些指标在您使用正确的集合统计数据时为您提供。下表总结了用来衡量网关和 AWS间的吞吐量、延迟和每秒输入/输出操作次数 (IOPS) 的指标和相应统计数据。

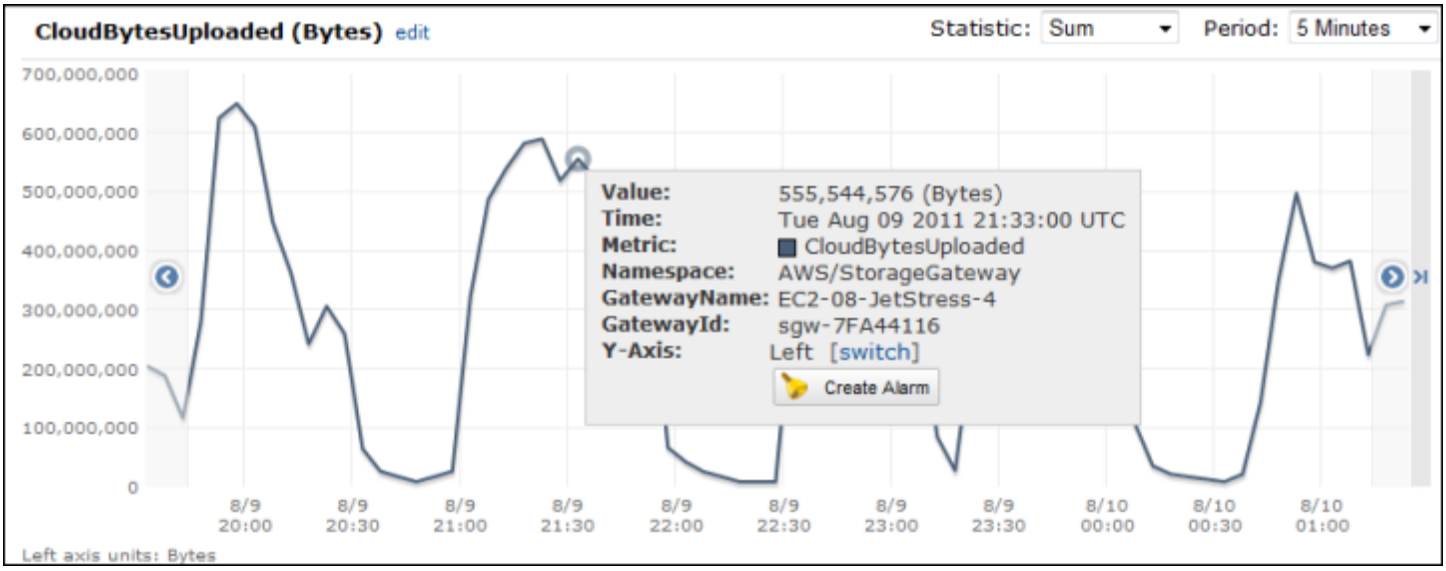
关注项	如何测量
吞吐量	将 ReadBytes 和 WriteBytes 指标结合 Sum CloudWatch 统计数据使用。例如，5 分钟采样周期内的 Sum 指标的 ReadBytes 值除以 300 秒可以得出每秒字节数速率的吞吐量。

关注项	如何测量
延迟	将 ReadTime 和 WriteTime 指标结合 Average CloudWatch 统计数据使用。例如，Average 指标的 ReadTime 值为您提供采样周期内的每个操作的延迟时间。
IOPS	将 ReadBytes 和 WriteBytes 指标结合 Samples CloudWatch 统计数据使用。例如，5 分钟采样周期内的 Samples 指标的 ReadBytes 值除以 300 秒可以得出 IOPS。
吞吐量到 AWS	在Sum CloudWatch 统计数据中使用CloudBytesDownloaded 和CloudBytesUploaded 指标。例如，5 分钟采样周期内的CloudBytesDownloaded 指标Sum值除以 300 秒得出从 AWS 网关到网关的吞吐量，单位为每秒字节数。
数据延迟到 AWS	将 CloudDownloadLatency 指标与 Average 统计数据结合使用。例如，Average 指标的 CloudDownloadLatency 统计数据为您提供每操作延迟。

测量从网关到的上传数据吞吐量 AWS

1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 选择 Metrics，再选择 All metrics 选项卡，然后选择 Storage Gateway。
3. 选择 Gateway metrics 维度并找到您希望使用的卷。
4. 选择 CloudBytesUploaded 指标。
5. 对于 Time Range，请选择一个值。
6. 选择 Sum 统计数据。
7. 对于 Period，请选择值 5 分钟或更长的时间。
8. 在得出的按时间排序的数据点集中，将各个数据点除以周期 (以秒为单位) 获得该样本周期当时的吞吐量。

下图使用 CloudBytesUploaded 统计数据显示了网关卷的 Sum 指标。在图中，将光标悬浮在数据点上就会显示该数据点信息，包括其值和上传的字节数。将该值除以 Period 值 (5 分钟) 得出采样点当时的吞吐量。为了突出显示的一点，从网关到的吞吐量 AWS 为 555,544,576 字节除以 300 秒，即每秒 1.7 兆字节。



如需衡量网关的每操作延迟

1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 选择 Metrics，再选择 All metrics 选项卡，然后选择 Storage Gateway。
3. 选择 Gateway metrics 维度并找到您希望使用的卷。
4. 选择 `ReadTime` 和 `WriteTime` 指标。
5. 对于 Time Range，请选择一个值。
6. 选择 `Average` 统计数据。
7. 对于 Period，请选择值 5 分钟以匹配默认报告时间。
8. 在得出的按时间排序的点集中 (其中一个用于 `ReadTime`，另一个用于 `WriteTime`)，在相同的时间样本添加数据点，以得出以毫秒为单位的总延迟。

测量从网关到的数据延迟 AWS

1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 选择 Metrics，再选择 All metrics 选项卡，然后选择 Storage Gateway。
3. 选择 Gateway metrics 维度并找到您希望使用的卷。
4. 选择 `CloudDownloadLatency` 指标。
5. 对于 Time Range，请选择一个值。
6. 选择 `Average` 统计数据。
7. 对于 Period，请选择值 5 分钟以匹配默认报告时间。

得出的按时间排序的数据点集包含以秒为单位的延迟。

要将网关吞吐量的上限阈值警报设置为 AWS

1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 选择 Alarms。
3. 选择 Create Alarm (创建警报) 可启动“Create Alarm (创建警报)”向导。
4. 选择 Storage Gateway 维度并找到要使用的网关。
5. 选择 `CloudBytesUploaded` 指标。
6. 要定义警报，请在 `CloudBytesUploaded` 指标大于或等于指定时间段的指定值时定义警报状态。例如，您可以定义 `CloudBytesUploaded` 指标在 60 分钟内 大于 10 MB 时的状态。
7. 针对该警报状态配置要采取的行动。例如，可获得向您发送的电子邮件通知。
8. 选择创建警报。

为读取数据设置上限阈值警报 AWS

1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 选择 Create Alarm (创建警报) 可启动“Create Alarm (创建警报)”向导。
3. 选择 StorageGateway：网关指标维度，然后找到要使用的网关。
4. 选择 `CloudDownloadLatency` 指标。
5. 通过定义 `CloudDownloadLatency` 指标在指定时间段大于或等于指定值时的警报状态，定义警报。例如，您可以定义 `CloudDownloadLatency` 在 2 小时内大于 60000 毫秒时的警报状态。
6. 针对该警报状态配置要采取的行动。例如，可获得向您发送的电子邮件通知。
7. 选择创建警报。

了解卷指标

您可以在下面找到有关包含网关的卷的 Storage Gateway 指标的信息。网关的每个卷均有与其关联的一组指标。

一些卷特定的指标具有和某些网关特定的指标相同的名称。这些指标代表同类度量，但其范围限于卷，而非网关。在开始工作之前，请指定要使用网关指标还是卷指标。具体而言，在使用卷指标时，请为要查看其指标的存储卷指定卷 ID。有关更多信息，请参阅使用亚马逊 CloudWatch 指标。

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

下表描述了可用来获取有关存储卷的信息的 Storage Gateway 指标。

指标	描述	缓存卷	存储卷
`AvailabilityNotification`	由卷发送的可用性通知的数量。 单位：计数	支持	支持
`CacheHitPercent`	应用程序从卷中读取的百分率，由缓存传送。样本在报告周期结束时采用。 在没有应用程序从卷读取时，该指标报告 100%。 单位：百分比	支持	不支持
`CachePercentDirty`	卷在未传送到 AWS的网关缓存的总体比例中的占比。样本在报告周期结束时采用。 使用网关的 `CachePercentDirty` 指标来查看未传送到 AWS的网关缓存总体比例。有关更多信息，请参阅了解网关指标。 单位：百分比	支持	支持

指标	描述	缓存卷	存储卷
CachePercentUsed	卷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。有关更多信息，请参阅了解网关指标。 单位：百分比	支持	不支持
CloudBytesDownloaded	从云下载到卷的字节数。 单位：字节	支持	支持
CloudBytesUploaded	从卷上传到云的字节数。 单位：字节	支持	支持
HealthNotification	由卷发送的运行状况通知的数量。 单位：计数	支持	支持
IoWaitPercent	该卷当前使用的 IoWaitPercent 单位百分比。 单位：百分比	支持	支持

指标	描述	缓存卷	存储卷
MemTotalBytes	卷当前所用的总内存的百分比。 单位：百分比	支持	不支持
MemoryUsage	卷当前所用的内存的百分比。 单位：百分比	支持	不支持
ReadBytes	报告周期内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	支持	支持
ReadTime	报告周期内从本地应用程序进行读取操作所耗费的总毫秒数。 将该指标与 Average 统计数据结合使用可测量延迟。 单位：毫秒	支持	支持
UserCpuPercent	卷当前所使用的已分配 CPU 计算单位的百分比。 单位：百分比	支持	支持

指标	描述	缓存卷	存储卷
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	支持	支持
WriteTime	报告周期内从本地应用程序进行写入操作所耗费的总毫秒数。 将该指标与 Average 统计数据结合使用可测量延迟。 单位：毫秒	支持	支持
QueuedWrites	等待写入的字节数 AWS，在报告周期结束时采样。 单位：字节	支持	支持

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。如果您尚未创建网关，请参阅创建网关。

主题

- 关闭网关虚拟机
- 管理 Storage Gateway 的本地磁盘
- 管理的带宽
- 使用 AWS Storage Gateway 控制台管理网关更新
- 在本地控制台上执行维护任务
- 使用 AWS Storage Gateway 控制台删除网关并清除相关资源

关闭网关虚拟机

您可能需要关闭或重新启动虚拟机进行维护，例如在向虚拟机管理程序应用补丁时。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。尽管本节的内容重点说明了使用 Storage Gateway 管理控制台启动和停止网关，但您也可以使用 VM 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。

Important

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

Note

如果您在将备份软件写入磁带或从磁带中读取备份软件时停止网关，则写入或读取任务可能不会成功。在停止网关之前，您应为正在进行的任何任务检查备份软件和备份计划。

- 网关 VM 本地控制台 - 请参阅使用默认凭证登录本地控制台。

- Storage Gateway API — 参见 ShutdownGateway

对于文件网关，您可以直接关闭虚拟机，而不需要关闭网关。

启动和停止卷网关

停止卷网关

1. 打开 Storage Gateway 控制台，网址为 https://console.aws.amazon.com/storagegateway/home。
2. 在导航窗格中，选择 Gateways，然后选择要停止的网关。网关处于 Running 状态。
3. 对于 Actions (操作)，选择 Stop gateway (停止网关) 并验证对话框中的网关 ID，然后选择 Stop gateway (停止网关)。

   在网关停止时，您可能会看到指示网关状态的消息。当网关关闭时，详细信息选项卡中会显示一条消息和启动网关按钮。

当您停止网关时，无法访问存储资源，直至您启动存储。如果在停止网关时网关正在上传数据，当启动网关时，上传操作将会恢复。

启动卷网关

1. 打开 Storage Gateway 控制台，网址为 https://console.aws.amazon.com/storagegateway/home。
2. 在导航窗格中，选择 Gateways，然后选择要启动的网关。网关处于 Shutdown 状态。
3. 选择 Details (详细信息)，然后选择 Start gateway (启动网关)。

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

- 确定本地磁盘存储量
- 确定要分配的上传缓冲区的大小
- 确定要分配的缓存存储的大小

- 配置额外的上传缓冲区和缓存存储

确定本地磁盘存储量

要为网关分配的磁盘的数量和大小由您自己决定。根据您部署的存储解决方案 (请参阅 规划 Storage Gateway 部署)，网关需要以下附加存储：

- 卷网关：
  - 存储网关至少需要一个磁盘用作上传缓冲区。
  - 缓存网关至少需要两个磁盘。一个用作缓存，另一个用作上传缓冲区。

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
上传缓冲区	上传缓冲区在网关将数据上传到 Amazon S3 之前为数据提供了一个暂存区域。您的网关通过加密的安全套接字层 (SSL) 连接将此缓冲区数据上传到 AWS。
缓存存储空间	缓存存储空间用作等待从上传缓冲区上传到 Amazon S3 的数据的本地持久存储。当应用程序对卷或磁带执行 I/O 时，网关会将数据保存到缓存存储以实现低延迟访问。当您的应用程序请求卷或磁带中的数据时，网关在从 AWS下载数据前会先检查缓存存储中的数据。

> **Note**
>
> 预置磁盘时，强烈建议您不要将本地磁盘预置为使用相同物理存储资源（同一磁盘）的上传缓冲区和缓存存储空间。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，用作缓存存储空间或上传缓冲

区) 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，为上传缓冲区选择另一个数据存储。仅由一个底层物理磁盘支持的数据存储在用于同时支持缓存存储空间和上传缓冲区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。

最初配置并部署网关后，您可以通过添加或删除用于上传缓冲区的磁盘来调整本地存储。还可以添加用于缓存存储空间的磁盘。

确定要分配的上传缓冲区的大小

您可以利用上传缓冲区公式来确定要分配的上传缓冲区的大小。我们强烈建议您至少分配 150 GiB 的上传缓冲区。如果公式返回小于 150 GiB 的值，请将 150 GiB 用作您分配给上传缓冲区的空间量。您可以为每个网关配置高达 2TiB 的上传缓冲区容量。

Note

对于卷网关，当上传缓冲区达到其容量后，您的卷将进入“传递”状态。在此状态下，您的应用程序写入的新数据会保存在本地，但不会 AWS 立即上传到。因此，您不能拍摄新快照。当上传缓冲区容量释放时，该卷将进入“BOOTSTRAPPING”(引导) 状态。在此状态下，任何保留在本地的新数据都将上传到。 AWS最后，该卷恢复为“活动”状态。然后，Storage Gateway 会恢复本地存储的数据与存储在中的副本的正常同步 AWS，然后您就可以开始拍摄新快照了。有关卷状态的更多信息，请参阅 了解卷状态和转换。

若要估算要分配的上传缓冲区的容量，您可以确定所需的传入和传出数据速率，并将它们插入到以下公式。

传入数据的速率

此速率指应用程序吞吐量，亦即您的本地应用程序在某段时间内将数据写入网关的速率。

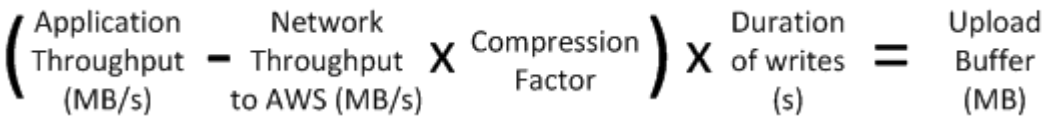
传出数据的速率

此速率指网络吞吐量，亦即您的网关将数据上传到 AWS时可达到的速率。此速率取决于您的网络速度、使用率以及您是否激活了带宽限制。该速率应该针对压缩率进行调整。将数据上传到时 AWS，网关会尽可能应用数据压缩。例如，如果您的应用程序数据为纯文本，您可以获得约 2:1 的

有效压缩率。不过，如果您正在写入视频，网关可能无法实现任何数据压缩，并且可能需要更多的网关上传缓冲区。

如果满足以下任一条件，我们强烈建议您至少分配 150 GiB 的上传缓冲区空间：

- 您的传入费率高于传出费率。
- 公式返回一个小于 150 GiB 的值。



例如，假定您的业务应用程序每天 12 个小时以每秒 40 MB 的速率向网关写入文本数据并且您的网络吞吐量为每秒 12 MB。假定文本数据的压缩系数为 2:1，您将需要为上传缓冲区分配约 690 GiB 的空间。

Example

```
((40 MB/sec) - (12 MB/sec * 2)) * (12 hours * 3600 seconds/hour) = 691200 megabytes
```

您可以将此近似值用来初步确定您希望分配给网关作为上传缓冲区空间的磁盘大小。使用 Storage Gateway 控制台按需添加更多的上传缓冲区空间。此外，您还可以使用 Amazon CloudWatch 运营指标来监控上传缓冲区的使用情况并确定额外的存储需求。有关指标及设置警报的更多信息，请参阅 监控上传缓冲区。

确定要分配的缓存存储的大小

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从上传缓冲区上传到 Amazon S3 的数据的本地持久存储。一般而言，将缓存存储空间的大小配置为上传缓冲区大小的 1.1 倍。有关如何估算缓存存储大小的更多信息，请参阅 确定要分配的上传缓冲区的大小。

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，您可以使用 Amazon CloudWatch 运营指标监控缓存存储空间使用情况，并使用控制台根据需要配置更多存储空间。有关使用指标和设置警报的信息，请参阅 监控缓存存储。

配置额外的上传缓冲区和缓存存储

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

> **Important**
>
> 向现有网关添加缓存或上传缓冲区时，必须在网关主机虚拟机管理程序或 Amazon EC2 实例上创建新磁盘。请勿删除或更改已分配为缓存或上传缓冲区的现有磁盘的大小。

为网关配置额外的上传缓冲区或缓存存储

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

   > **Note**
   >
   > 上传缓冲区是在存储卷网关上分配磁盘的唯一可用选项。

7. 选择保存更改来保存您的配置设置。

管理的带宽

您可以限制（或限制）从网关到网关的上传吞吐量 AWS 或从网关下载到 AWS 网关的吞吐量。使用带宽限制可以帮助您控制网关所用的网络带宽量。默认情况下，已激活的网关不对上传或下载进行速率限制。

您可以使用指定速率限制 AWS Management Console，也可以使用 Storage Gateway API（参见 UpdateBandwidthRateLimit）或 AWS 软件开发套件 (SDK) 以编程方式指定速率限制。通过以编程方式限制带宽，您可以自动更改一天中的限制（例如，通过调度任务来更改带宽）。

您也可以为网关定义基于计划的带宽限制。您可以通过定义一个或多个 bandwidth-rate-limit 间隔来安排带宽限制。有关更多信息，请参阅使用 Storage Gateway 控制台实施基于计划的带宽限制。

配置带宽限制的单一设置在功能上等同于定义一个时间 bandwidth-rate-limit 间隔为 “每天” 的时间表，开始时间为`00:00`，结束时间为。`23:59`

> **Note**
>
> 本节中的信息特定于磁带网关和卷网关。要管理 Amazon S3 文件网关的带宽，请参阅管理 Amazon S3 文件网关的带宽。Amazon FSx 文件网关目前不支持带宽速率限制。

主题

- 使用 Storage Gateway 控制台更改带宽限制
- 使用 Storage Gateway 控制台实施基于计划的带宽限制
- 使用更新网关带宽速率限制 AWS SDK for Java
- 使用更新网关带宽速率限制 AWS SDK for .NET
- 使用更新网关带宽速率限制 AWS Tools for Windows PowerShell

使用 Storage Gateway 控制台更改带宽限制

以下过程介绍如何从 Storage Gateway 控制台更改网关的带宽限制。

如需使用控制台更改网关的带宽限制

1. 打开 Storage Gateway 控制台，网址为 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. 对于操作，选择编辑带宽速率限制。
4. 在编辑速率限制对话框中，输入新的限制值，然后选择保存。您的更改将显示在网关的 Details 选项卡中。

使用 Storage Gateway 控制台实施基于计划的带宽限制

以下过程介绍如何使用 Storage Gateway 控制台来计划对网关带宽限制的更改。

添加或修改网关带宽限制计划

1. 打开 Storage Gateway 控制台，网址为 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. 对于操作，选择编辑带宽速率限制计划。

   网关的 bandwidth-rate-limit 计划显示在编辑带宽速率限制计划对话框中。默认情况下，新的网关 bandwidth-rate-limit 计划为空。
4. 在 “编辑带宽速率限制计划” 对话框中，选择 “添加新项目” 以添加新的间 bandwidth-rate-limit隔。为每个 bandwidth-rate-limit间隔输入以下信息：

   - 一@@ 周中的几天-您可以为工作日（星期一至星期五）、周末（星期六和星期日）、一周中的每一天或一周中的一个或多个特定日期创建 bandwidth-rate-limit 间隔。
   - 开始时间 - 使用 HH:MM 格式输入网关本地时区带宽间隔的开始时间。

     > **Note**
     >
     > 您的 bandwidth-rate-limit 间隔从您在此处指定的分钟开始处开始。

   - 结束时间-使用 HH: MM 格式，以网关的本地时区输入 bandwidth-rate-limit 间隔的结束时间。

     > **Important**
     >
     > 间 bandwidth-rate-limit 隔在此处指定的分钟结束时结束。要计划在小时结束时结束的间隔，请输入 **59**。
     > 要计划不间断的连续备份间隔，在小时开始时转换，并且在各个间隔之间没有中断，请对第一个间隔的结束分钟输入 **59**。对后续间隔的开始分钟输入 **00**。

   - 下载速率 - 输入下载速率限制，以千位/秒 (Kbps) 为单位，或者选择无限制来停用下载的带宽限制。下载速率的最小值为 100 Kbps。
   - 上传速率 - 输入上传速率限制（以 Kbps 为单位），或选择无限制来停用上传的带宽限制。上传速率的最小值为 50 Kbps。

要修改 bandwidth-rate-limit 间隔，可以为间隔参数输入修改后的值。

要删除 bandwidth-rate-limit 间隔，可以选择要删除的间隔右侧的 “删除”。

完成更改后，选择保存。

5. 继续添加 bandwidth-rate-limit 间隔，方法是选择 “添加新项目”，然后输入日期、开始和结束时间以及下载和上传速率限制。

> **Important**
>
> B andwidth-rate-limit 间隔不能重叠。间隔的开始时间必须出现在前一个间隔的结束时间之后和下一个间隔的开始时间之前。

6. 输入所有 bandwidth-rate-limit 间隔后，选择保存更改以保存您的 bandwidth-rate-limit 日程安排。

成功更新 bandwidth-rate-limit 计划后，您可以在网关的详细信息面板中看到当前的下载和上传速率限制。

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 AWS SDK for Java更新网关的带宽速率限制。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《AWS SDK for Java 开发人员指南》中的入门。

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，您必须提供服务端点、网关的 Amazon 资源名称 (ARN) 以及上传和下载限制。有关可以与 Storage Gateway 配合使用的 AWS 服务终端节点列表，请参阅中的AWS Storage Gateway 终端节点和配额AWS 一般参考。

```
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.UpdateBandwidthRateLimitRequest;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitResult;
```

```
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 = 51200;  // Bits per second, minimum 51200
    static long downloadRate = 102400;   // Bits per second, minimum 102400

    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, downloadRate);

    }

    private static void UpdateBandwidth(String gatewayARN2, long uploadRate2,
            long downloadRate2) {
        try
        {
            UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
                new UpdateBandwidthRateLimitRequest()
                .withGatewayARN(gatewayARN)
                .withAverageDownloadRateLimitInBitsPerSec(downloadRate)
                .withAverageUploadRateLimitInBitsPerSec(uploadRate);

            UpdateBandwidthRateLimitResult updateBandwidthRateLimitResult =
 sgClient.updateBandwidthRateLimit(updateBandwidthRateLimitRequest);
            String returnGatewayARN = updateBandwidthRateLimitResult.getGatewayARN();
            System.out.println("Updated the bandwidth rate limits of " +
 returnGatewayARN);
            System.out.println("Upload bandwidth limit = " + uploadRate + " bits per
 second");
```

```
            System.out.println("Download bandwidth limit = " + downloadRate + " 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 AWS SDK for .NET更新网关的带宽速率限制。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《AWS SDK for .NET 开发人员指南》中的入门。

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，您必须提供服务端点、网关的 Amazon 资源名称 (ARN) 以及上传和下载限制。有关可以与 Storage Gateway 配合使用的 AWS 服务终端节点列表，请参阅中的AWS Storage Gateway 终端节点和配额AWS 一般参考。

```
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 = 51200;  // Bits per second, minimum 51200
        static long downloadRate = 102400;   // Bits per second, minimum 102400

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

            UpdateBandwidth(gatewayARN, uploadRate, downloadRate);

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

        public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
downloadRate)
        {
            try
            {
                UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
                    new UpdateBandwidthRateLimitRequest()
                    .WithGatewayARN(gatewayARN)
                    .WithAverageDownloadRateLimitInBitsPerSec(downloadRate)
                    .WithAverageUploadRateLimitInBitsPerSec(uploadRate);

                UpdateBandwidthRateLimitResponse updateBandwidthRateLimitResponse =
sgClient.UpdateBandwidthRateLimit(updateBandwidthRateLimitRequest);
                String returnGatewayARN =
updateBandwidthRateLimitResponse.UpdateBandwidthRateLimitResult.GatewayARN;
                Console.WriteLine("Updated the bandwidth rate limits of " +
returnGatewayARN);
                Console.WriteLine("Upload bandwidth limit = " + uploadRate + " bits per
second");
                Console.WriteLine("Download bandwidth limit = " + downloadRate + " 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 AWS Tools for Windows PowerShell更新网关的带宽速率限制。要使用示例代码，您应该熟悉如何运行 PowerShell脚本。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 脚本示例更新了网关的带宽速率限制。要使用此示例脚本，您必须提供网关的 Amazon 资源名称 (ARN) 以及上传和下载限制。

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

.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 = 51200
$DownloadBandwidthRate = 102400
$gatewayARN = "*** provide gateway ARN ***"

#Update Bandwidth Rate Limits
Update-SGBandwidthRateLimit -GatewayARN $gatewayARN `
                            -AverageUploadRateLimitInBitsPerSec $UploadBandwidthRate `
                            -AverageDownloadRateLimitInBitsPerSec
 $DownloadBandwidthRate
```

```
$limits =  Get-SGBandwidthRateLimit -GatewayARN $gatewayARN

Write-Output("`nGateway: " + $gatewayARN);
Write-Output("`nNew Upload Rate: " + $limits.AverageUploadRateLimitInBitsPerSec)
Write-Output("`nNew Download Rate: " + $limits.AverageDownloadRateLimitInBitsPerSec)
```

使用 AWS Storage Gateway 控制台管理网关更新

Storage Gateway 由托管云服务组件和网关设备组件组成，您可以部署在本地或 AWS 云中的 Amazon EC2 实例上。 AWS 根据需要更新云服务组件，而不会对已部署的网关造成中断。

您部署的网关设备也需要定期更新。更新可能包括操作系统和软件升级、针对稳定性、性能和安全性的修复以及对新功能的访问。所有更新均为累积更新，应用后将网关升级到当前版本。

Gateway 设备会定期接收更新，应用这些更新可能会导致服务短暂中断。网关的虚拟机主机在更新期间无需重新启动，但是在软件设备更新和重新启动期间，网关将在短时间内不可用。

> **Important**
>
> 您应将 Storage Gateway 设备视为托管虚拟机，并且不应尝试以任何方式访问或修改其安装。尝试使用正常网关更新机制以外的方法（例如 SSM 或虚拟机管理程序工具）安装或更新任何软件包可能会导致网关出现故障。

您可以将网关配置为在计划维护时段内自动应用维护更新，也可以等到手动启动维护更新。部署和激活网关时，会设置默认的每周维护时段计划。您可以随时修改维护时段计划。有更新时，网关详细信息选项卡会显示一条维护消息。您还可以在详细信息选项卡上查看上次成功应用更新的日期和时间。

> **Note**
>
> 某些重要的更新有时会根据维护时段计划进行应用，即使定期维护更新已关闭。

在将任何更新应用于您的网关之前， AWS 会在 Storage Gateway 控制台和您的 AWS Health Dashboard。有关更多信息，请参阅 AWS Health Dashboard。要修改发送软件更新通知的电子邮件地址，请转到管理 AWS 账户页面并更新 “操作” 的备用联系人。

以下各节中的过程介绍如何使用 Storage Gateway 控制台管理网关更新。要使用 API 以编程方式管理这些设置，请参阅 Storage Gateway API 参考UpdateMaintenanceStartTime中的。

打开或关闭维护更新

开启维护更新后，您的网关会根据配置的维护时段计划自动应用这些更新。有关更多信息，请参阅修改网关维护时段计划。

如果关闭维护更新，网关将不会自动应用这些更新，但您仍然可以使用 Storage Gateway 控制台、API 或 CLI 手动应用这些更新。无论此设置如何，有时会在您配置的维护时段内应用某些重要更新。

要打开或关闭特定网关的维护更新，请执行以下操作：

1. 打开 Storage Gateway 控制台，网址为 https://console.aws.amazon.com/storagegateway/home。
2. 在导航窗格上，选择 Gateways，然后选择要为其配置维护更新的网关。
3. 选择 “操作”，然后选择 “编辑维护设置”。
4. 要获取维护更新，请选择开启或关闭。
5. 完成后选择 “保存更改”。

您可以在 Storage Gateway 控制台的详细信息选项卡上验证所选网关的更新设置。

修改网关维护时段计划

如果打开了维护更新，您的网关将根据维护时段计划自动应用新的软件更新。无论维护更新设置如何，有时会在您配置的维护时段内应用某些重要更新。

要修改特定网关的维护时段计划，请执行以下操作：

1. 打开 Storage Gateway 控制台，网址为 https://console.aws.amazon.com/storagegateway/home。
2. 在导航窗格上，选择 Gateways，然后选择要为其配置维护更新的网关。
3. 选择 “操作”，然后选择 “编辑维护设置”。
4. 在 “维护窗口开始时间” 下，执行以下操作：

    a. 在 “计划” 中，选择 “每周” 或 “每月” 以设置维护时段节奏。

    b. 如果选择 “每周”，请修改星期和时间的值，以设置每周维护时段开始的具体时间。

    如果选择 “每月”，请修改月中某天和时间的值，以设置每个月中维护时段开始的具体时刻。

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

5. 完成后选择 “保存更改”。

您可以在 Storage Gateway 控制台的详细信息选项卡上验证所选网关的更新设置。

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。可以在 VM 主机或 Amazon EC2 实例上执行本地控制台任务。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。

在 虚拟机本地控制台上执行任务

对于本地部署的网关，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、Hyper-V 和基于 Linux 内核的虚拟机 (KVM) 主机所共有的。

主题

- 使用默认凭证登录本地控制台
- 从 Storage Gateway 控制台设置本地控制台密码
- 通过代理路由本地网关
- 配置网关网络
- 测试网关到 Internet 的连接
- 同步您的网关 VM 时间
- 在本地控制台上运行 Storage Gateway 命令
- 查看您的网关系统资源状态
- 为网关配置网络适配器

使用默认凭证登录本地控制台

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，请使用默认登录凭证来登录。您可以使用这些默认登录凭证来访问一些菜单，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。Storage Gateway 允许您从 AWS Storage Gateway 控制台设置自己的密码，而不必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 从 Storage Gateway 控制台设置本地控制台密码。

登录网关的本地控制台

1. 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**
   >
   > 我们建议更改默认密码，方法是在 AWS 设备激活 - 配置主菜单中为网关控制台输入相应的数字，然后运行 `passwd` 命令。有关如何运行该命令的信息，请参阅在本地控制台上运行 Storage Gateway 命令。您也可以通过 AWS Storage Gateway 控制台设置自己的密码。有关更多信息，请参阅 从 Storage Gateway 控制台设置本地控制台密码。

   > **Important**
   >
   > 对于较旧版本的卷网关或磁带网关，用户名为 `sguser`，密码为 `sgpassword`。如果您重置了密码，并且您的网关更新到更新的版本，则您的用户名将变为 admin，而密码保持不变。

2. 登录后，您将看到 AWS Storage Gateway 配置主菜单，您可以通过这个菜单执行各种任务。

了解此任务	请参阅此主题
为您的网关配置 SOCKS 代理	通过代理路由本地网关.
配置网络	配置网关网络.
测试网关连接性	测试网关到 Internet 的连接.

了解此任务	请参阅此主题
管理虚拟机时间	同步您的网关 VM 时间.
运行 Storage Gateway 控制台命令	在本地控制台上运行 Storage Gateway 命令.
查看系统资源检查	查看您的网关系统资源状态.

要关闭网关，请输入 **0**。

要退出配置会话，请输入 **X**。

从 Storage Gateway 控制台设置本地控制台密码

当您首次登录本地控制台时，使用默认凭证（用户名为 `admin`，密码为 `password`）登录 VM。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. 打开 Storage Gateway 控制台，网址为 https://console.aws.amazon.com/storagegateway/home。
2. 在导航栏中，选择 Gateways，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 对话框中，键入新密码，确认该密码，然后选择 Save。您的新密码会替换默认密码。Storage Gateway 不会保存密码，而是将其安全地传输到 VM。

> **Note**
>
> 密码可以由键盘上的任何字符组成，长度可以为 1 至 512 个字符。

通过代理路由本地网关

卷网关和磁带网关支持在本地网关和 AWS之间配置 Socket Secure 版本 5 (SOCKS5) 代理。

> **Note**
>
> 唯一支持的代理配置是 SOCKS5。

如果网关必须使用代理服务器与 Internet 进行通信，则需要为网关配置 SOCKS 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 通过您的代理服务器路由所有流量。有关网关的网络要求的信息，请参阅网络和防火墙要求。

以下过程显示如何为卷网关和磁带网关配置 SOCKS 代理。

为卷网关和磁带网关配置 SOCKS5 代理

1. 登录到网关的本地控制台。
   - 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。
   - KVM – 有关更多信息，请参阅使用 Linux KVM 访问网关本地控制台。
2. 在 AWS Storage Gateway - 配置主菜单中，输入相应的数字来选择 SOCKS 代理配置。
3. 在 AWS Storage Gateway SOCKS 代理配置菜单中，输入相应的数字来执行以下任务之一：

执行此任务	请执行此操作
配置 SOCKS 代理	输入相应的数字来选择配置 SOCKS 代理。 您需要提供主机名称和端口来完成配置。
查看当前的 SOCKS 代理配置	输入相应的数字来选择查看当前 SOCKS 代理配置。 如果未配置 SOCKS 代理，则会显示消息 `SOCKS Proxy not configured` 。如果 SOCKS 代理已配置，代理的主机名称和端口就会显示。
移除 SOCKS 代理配置	输入相应的数字来选择删除 SOCKS 代理配置。

执行此任务	请执行此操作
	消息 SOCKS Proxy Configuration Removed 将会显示。

4. 重新启动 VM 来应用 HTTP 配置。

配置网关网络

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

如需将您的网关配置为使用静态 IP 地址。

1. 登录到网关的本地控制台。
   - 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。
   - KVM – 有关更多信息，请参阅使用 Linux KVM 访问网关本地控制台。
2. 在 AWS Storage Gateway - 配置主菜单中，输入相应的数字来选择网络配置。
3. 在 AWS Storage Gateway 网络配置菜单中，执行以下任务之一：

执行此任务	请执行此操作
描述网络适配器	输入相应的数字来选择描述适配器。 此时会显示适配器名称的列表，并且系统会提示您输入适配器名称，例如 **eth0**。如果您指定的适配器正在使用中，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

执行此任务	请执行此操作
	• 网关 IP 地址 • DHCP 激活状态 配置静态 IP 地址或设置网关的默认适配器时，使用此处列出的适配器名称。
配置 DHCP	输入相应的数字来选择配置 DHCP。 系统将提示您将网络接口配置为使用 DHCP。

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

执行此任务	请执行此操作
	如果两个接口最初都设置为使用静态 IP 地址且您之后将网关设置为使用 DHCP，那么两个接口都将使用 DHCP。
为网关配置主机名	输入相应的数字来选择配置主机名。 系统会提示您选择网关是使用您指定的静态主机名，还是通过 DHCP 或 rDNS 自动获取主机名。 如果您选择 “静态”，则系统会提示您提供静态主机名，例如`testgateway.example.com` 。输入`y`以应用配置。 **Note** 如果您为网关配置静态主机名，请确保提供的主机名位于网关加入的域中。您还必须在 DNS 系统中创建 A 记录，将网关的 IP 地址指向其静态主机名。
将网关的所有网络配置重置为 DHCP	输入相应的数字来选择全部重置为 DHCP。 所有网络接口均设置为使用 DHCP。 **Important** 如果网关已激活，则必须从 Storage Gateway 控制台关停并重启网关，这样设置才会生效。有关更多信息，请参阅关闭网关虚拟机。

执行此任务	请执行此操作
设置网关的默认路由适配器	输入相应的数字来选择设置默认适配器。 此时会显示可供网关使用的适配器，并且系统会提示您选择其中一个适配器（例如 **eth0**）。
查看网关的 DNS 配置	输入相应的数字来选择查看 DNS 配置。 此时会显示主 DNS 和备用 DNS 名称服务器的 IP 地址。
查看路由表	输入相应的数字来选择查看路由。 网关的默认路由将会显示。

测试网关到 Internet 的连接

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

测试网关到 Internet 的连接

1. 登录到网关的本地控制台。
   - 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。
   - KVM – 有关更多信息，请参阅使用 Linux KVM 访问网关本地控制台。
2. 在 AWS Storage Gateway - 配置主菜单中，输入相应的数字来选择测试网络连接。

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

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

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

同步您的网关 VM 时间

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，如果网络中断时间较长，并且管理程序主机和网关没有更新时间，则网关 VM 的时间将与实际时间不同。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，您应定期检查 VM 的时间。有关更多信息，请参阅 同步您的网关 VM 时间。

在本地控制台上运行 Storage Gateway 命令

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

运行配置或诊断命令

1. 登录到网关的本地控制台：
   - 有关登录到 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 - 配置主菜单中，输入相应的数字来选择网关控制台。
3. 在网关控制台命令提示符处输入 **h**。

   控制台会显示可用命令菜单，其中列出了可用的命令：

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

命令	函数
save-routing-table	保存新添加的路由表条目。
tcptraceroute	收集有关流向目的地的 TCP 流量的 traceroute 输出。

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

要了解命令，请在命令提示符处输入 **man** + *####*。

查看您的网关系统资源状态

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

查看系统资源检查的状态

1. 登录到网关的本地控制台：
   - 有关登录到 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 - 配置主菜单中，输入相应的数字来选择查看系统资源检查。

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

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，但网关可以继续正常工作。Storage Gateway 显示一条消息，描述资源检查的结果。

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

控制台还会在资源检查菜单选项旁边显示错误和警告的数量。

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。还可以将 Storage Gateway 配置为能够通过多个 IP 地址来访问。为此，您可以将网关配置为使用多个网络适配器。

主题

- 将网关配置为使用 VMXNET3 网络适配器
- 将网关配置为使用多个 NIC

将网关配置为使用 VMXNET3 网络适配器

Storage Gateway 支持在 VMware ESXi 和 Microsoft Hyper-V 管理程序主机中使用 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) 适配器类型。有关这些适配器的更多信息，请参阅 Broadcom (VMware) 网站上的为虚拟机选择网络适配器。

> **Important**
>
> 要选择 VMXNET3，您的来宾操作系统类型必须是其他 Linux64。

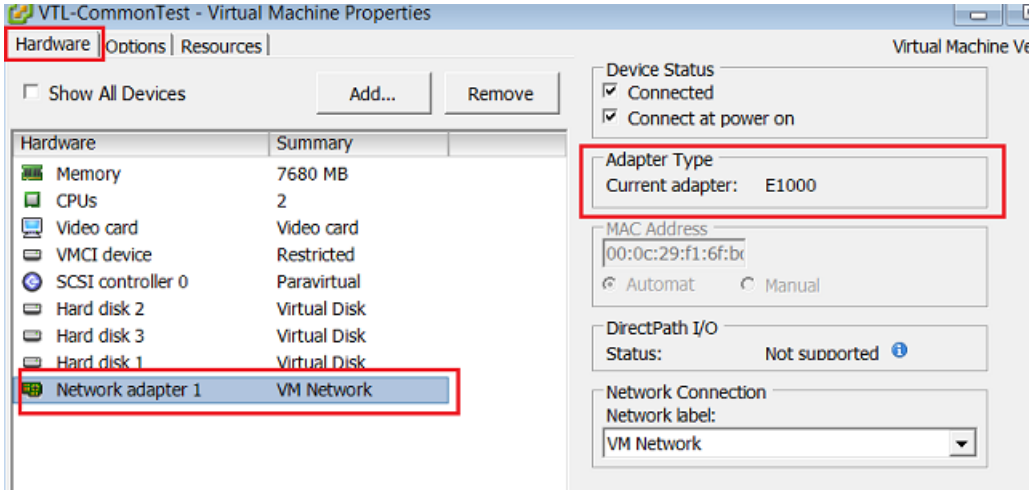
您可执行以下步骤将网关配置为使用 VMXNET3 适配器：

1. 移除默认的 E1000 适配器。
2. 添加 VMXNET3 适配器。
3. 重新启动您的网关。
4. 为网络配置适配器。

下面是有关如何执行每个步骤的详细信息。

移除默认 E1000 适配器并将网关配置为使用 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，选择硬件选项卡。
3. 对于 Hardware，选择 Network adapter。请注意，在适配器类型部分，当前适配器为 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。在本示例中，E1000 网络适配器是网络适配器 1。

> **Note**
>
> 尽管您可以在网关中同时运行 E1000 和 VMXNET3 网络适配器，但我们不建议这样做，因为这样会导致出现网络问题。

5. 选择添加来打开“添加硬件”向导。
6. 选择 Ethernet Adapter，然后选择 Next。
7. 在“网络类型”向导中，为适配器类型选择 **VMXNET3**，然后选择下一步。
8. 在“虚拟机属性”向导中，验证适配器类型部分中的当前适配器是否设置为 VMXNET3，然后选择确定。
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，请参阅使用默认凭证登录本地控制台。
2. 在提示符处输入相应的数字来选择网络配置。
3. 在提示符处，输入相应的数字来选择全部重置为 DHCP，然后在命令提示符处输入 **y**（表示“是”）以将所有适配器设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，则必须从 Storage Gateway 管理控制台将其关闭并重新启动。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，请参阅测试网关与 Internet 的连接。

将网关配置为使用多个 NIC

如果您将网关配置为使用多个网络适配器 (NIC)，就可以通过多个 IP 地址来访问网关。您可能希望在以下情况下执行此操作：

- 最大程度地增加吞吐量 - 当网络适配器成为瓶颈时，您可能希望最大程度地增加网关的吞吐量。
- 应用程序区分 - 您可能需要区分应用程序写入到网关的卷的方式。例如，您可以选择让关键存储应用程序独占使用为网关定义的一个特定适配器。
- 网络限制 - 您的应用程序环境可能需要将 iSCSI 目标及连接到这些目标的启动程序保留在一个独立网络中，该网络不同于网关与 AWS进行通信的网络。

在典型的多适配器用例中，将一个适配器配置为网关与之通信的路由 AWS（即默认网关）。除了这个适配器之外，启动程序必须与包含所连接 iSCSI 目标的适配器位于同一个子网中。否则，可能无法与预定目标通信。如果目标配置在用于与之通信的同一适配器上 AWS，则该目标的 iSCSI 流量和 AWS 流量将流经同一个适配器。

当配置一个适配器连接到 Storage Gateway 控制台，然后添加第二个适配器时，Storage Gateway 会自动将路由表配置为使用第二个适配器作为首选路由。有关如何配置多适配器的说明，请参阅以下各节。

- 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 Amazon EC2 本地控制台上执行任务

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

主题

- 登录到 Amazon EC2 网关本地控制台
- 通过 HTTP 代理路由在 EC2 上部署的网关
- 测试网关的网络连接
- 查看您的网关系统资源状态
- 在本地控制台上运行 Storage Gateway 命令

登录到 Amazon EC2 网关本地控制台

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

登录网关本地控制台

1. 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，您将看到 AWS Storage Gateway - 配置主菜单，您可以通过这个菜单执行各种任务。

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

要关闭网关，请输入 **0**。

要退出配置会话，请输入 **X**。

通过 HTTP 代理路由在 EC2 上部署的网关

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

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

通过本地代理服务器路由网关 Internet 流量

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

测试网关的网络连接

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

测试网关的连接

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

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

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

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

查看您的网关系统资源状态

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

查看系统资源检查的状态

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

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

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

   控制台还会在资源检查菜单选项旁边显示错误和警告的数量。

在本地控制台上运行 Storage Gateway 命令

AWS Storage Gateway 控制台有助于为配置和诊断网关问题提供安全的环境。使用控制台命令，您可以执行维护任务，例如保存路由表或连接到 AWS 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 Amazon EC2 网关本地控制台。
2. 在 AWS 设备激活 - 配置主菜单中，输入相应的数字来选择网关控制台。
3. 在网关控制台命令提示符处输入 h。

   控制台会显示可用命令菜单，其中列出了可用的命令：

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

命令	函数
open-support-channel	Connect to S AWS upport。
save-iptables	保留 IP 表。
save-routing-table	保存新添加的路由表条目。
sslcheck	检查 SSL 有效性以排除网络故障。
tcptraceroute	收集有关流向目的地的 TCP 流量的 traceroute 输出。

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

要了解相关命令，请输入命令名称，然后输入 -h 选项，例如：`sslcheck -h`。

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。

```
[[root@localhost vms]# virsh list
 Id    Name                           State
----------------------------------------------------
 7     SGW_KVM                        running

[root@localhost vms]# virsh console 7
```

2. 使用以下命令访问本地控制台。

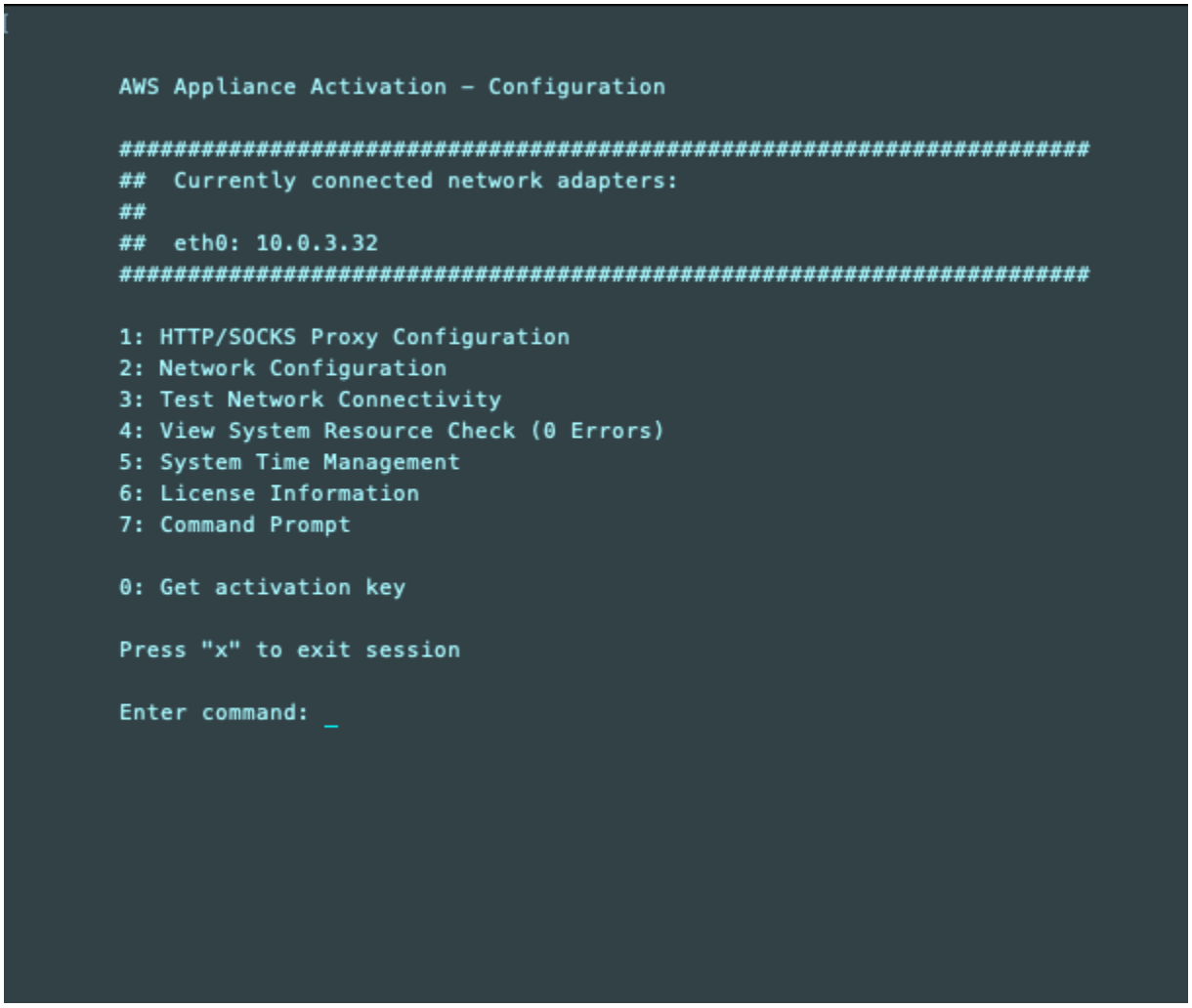
```
# virsh console VM_Id
```

```
[[root@localhost vms]# virsh console 7
Connected to domain SGW_KVM
Escape character is ^]

AWS Appliance

Login to change your network configuration and other settings.
localhost login: _
```

3. 要获取用于登录本地控制台的默认凭证，请参阅使用默认凭证登录本地控制台。
4. 登录后，您可以激活和配置网关。

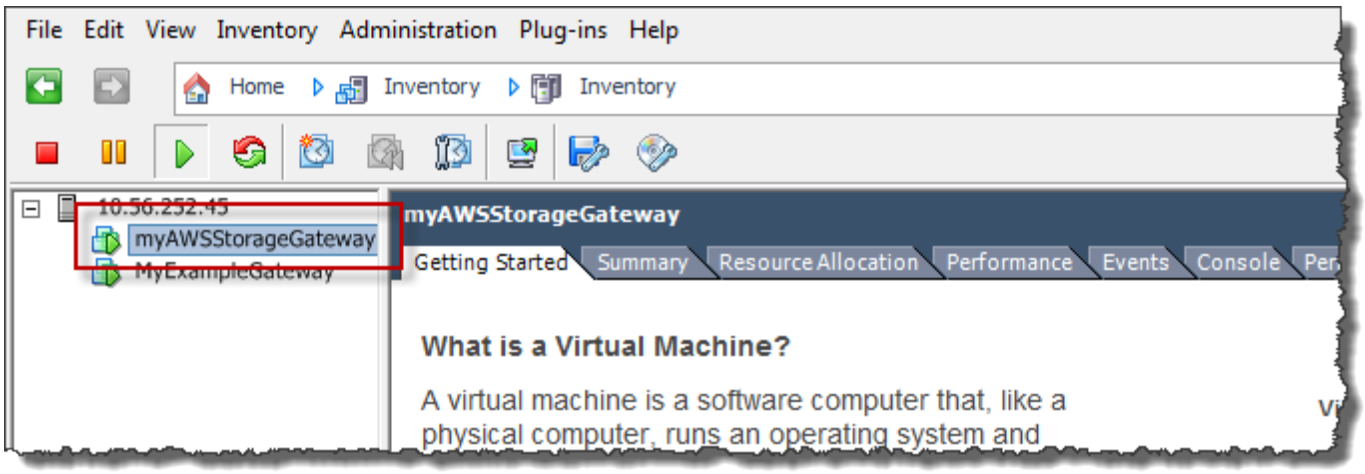


使用 VMware ESXi 访问网关本地控制台

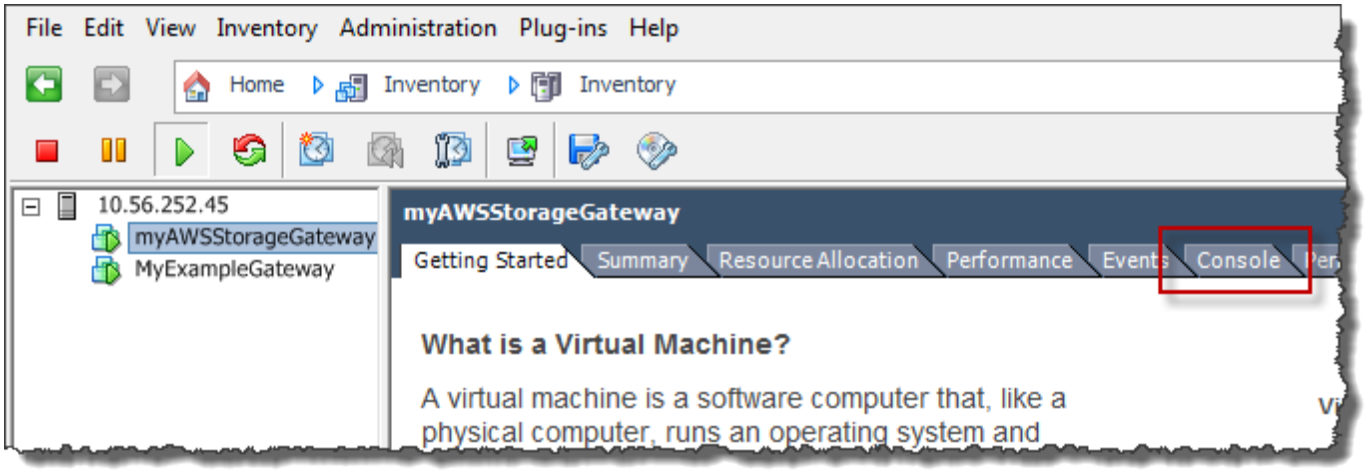
使用 VMware ESXi 访问网关的本地控制台

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。如果网关 VM 未开启，则可以通过选择工具栏菜单上的绿色开机图标将其打开。

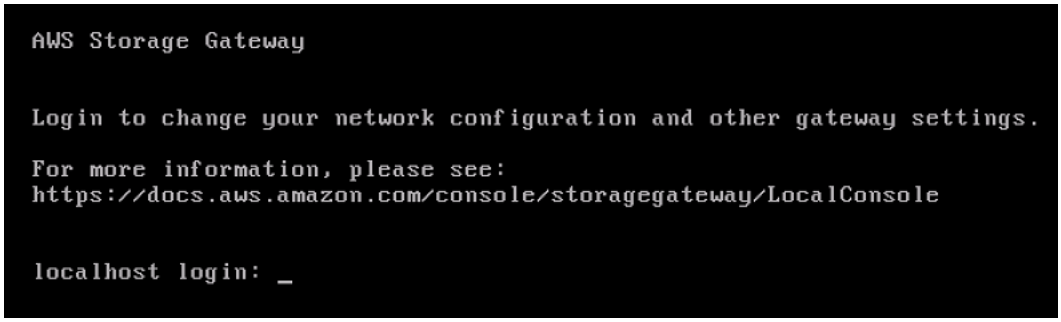


3. 选择 Console (控制台) 选项卡。



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。



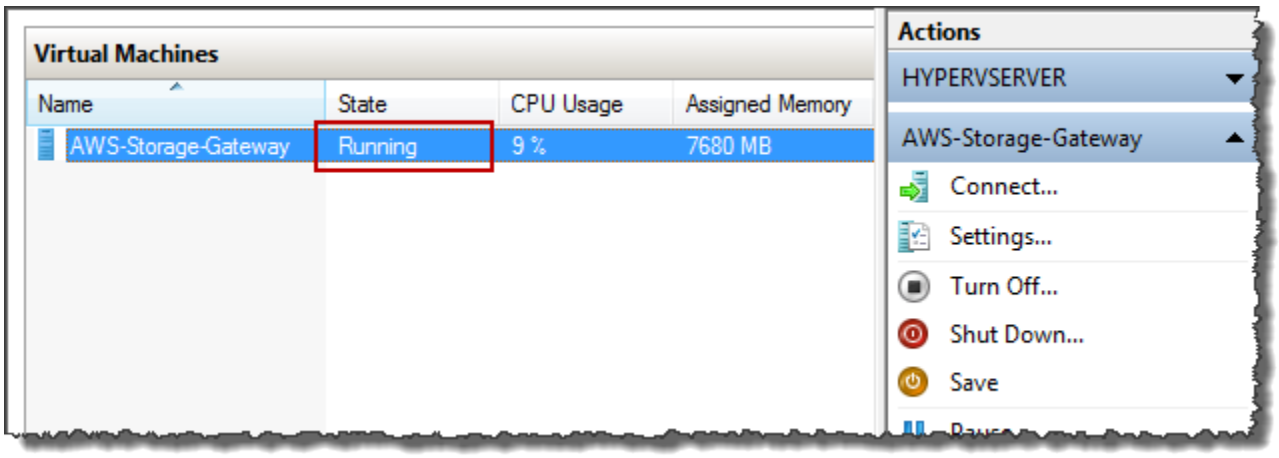
4. 要使用默认凭证登录，请继续执行过程使用默认凭证登录本地控制台。

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)

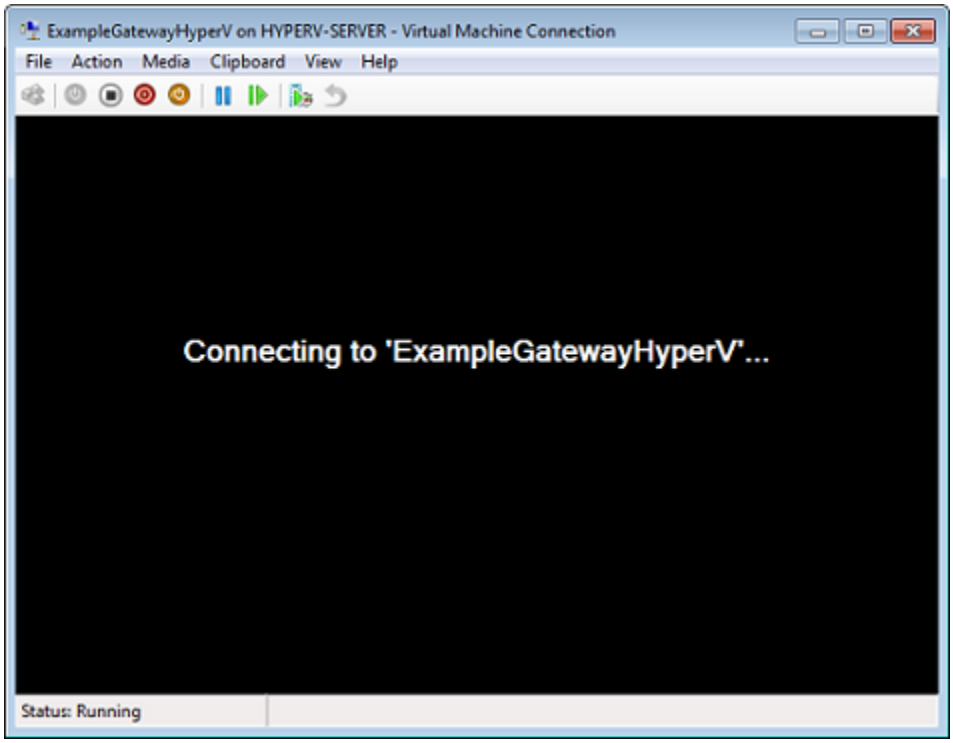
1. 在 Microsoft Hyper-V Manager 的 Virtual Machines (虚拟机) 列表中，选择您的网关 VM。
2. 确保网关已开启。

> **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。如果网关 VM 未开启，则可以通过在操作窗格中选择启动将其打开。



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登录凭证。



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，请继续执行过程使用默认凭证登录本地控制台。

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

以下程序假定您的网关 VM 已定义了一个网络适配器，并说明了如何在 VMware ESXi 上添加适配器。

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. 在虚拟机属性对话框的硬件选项卡上，选择添加来添加设备。
5. 按 Add Hardware (添加硬件) 向导添加网络适配器。

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

   b. 在网络类型窗格中，确保为类型选择开机时连接，然后选择下一步。

      我们建议您将 VMXNET3 网络适配器与 Storage Gateway 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 VM 的摘要选项卡，然后选择 IP 地址 框旁边的查看全部。虚拟机 IP 地址窗口显示您可以用来访问网关的全部 IP 地址。确认第二个 IP 地址已针对该网关列出。

   > **Note**
   >
   > 适配器更改生效和 VM 摘要信息刷新可能需要少许时间。

7. 在 Storage Gateway 控制台中，打开网关。
8. 在 Storage Gateway 控制台的导航窗格中，选择网关，然后选择要在其中添加适配器的网关。确认 Details (详细信息) 选项卡中列出了第二个 IP 地址。

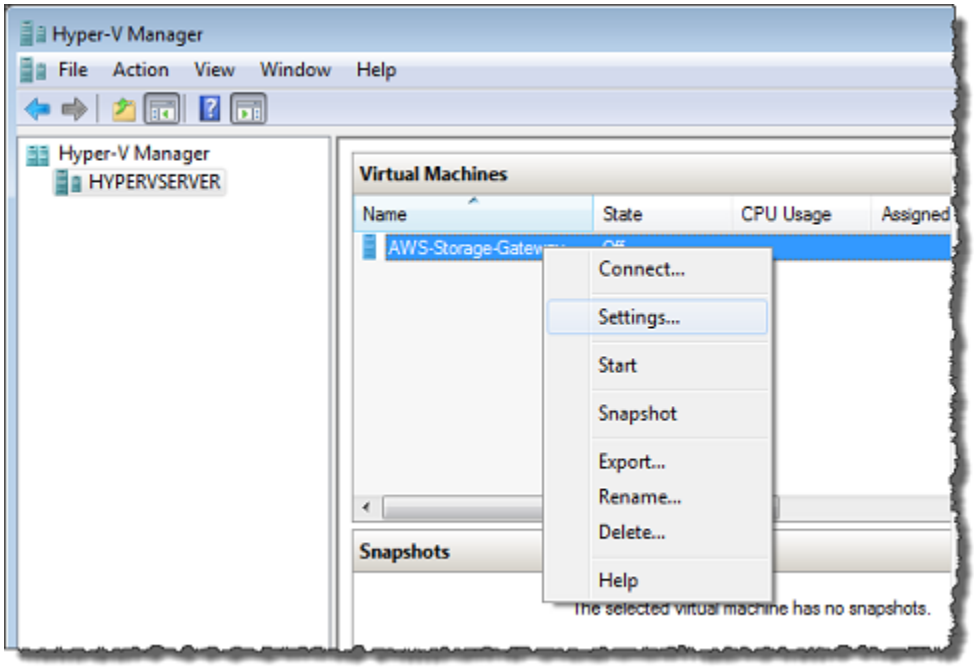
有关 VMware、Hyper-V 和 KVM 主机的常见本地控制台任务的信息，请参阅在 虚拟机本地控制台上执行任务

在 Microsoft Hyper-V 主机中为多个 NIC 配置您的网关

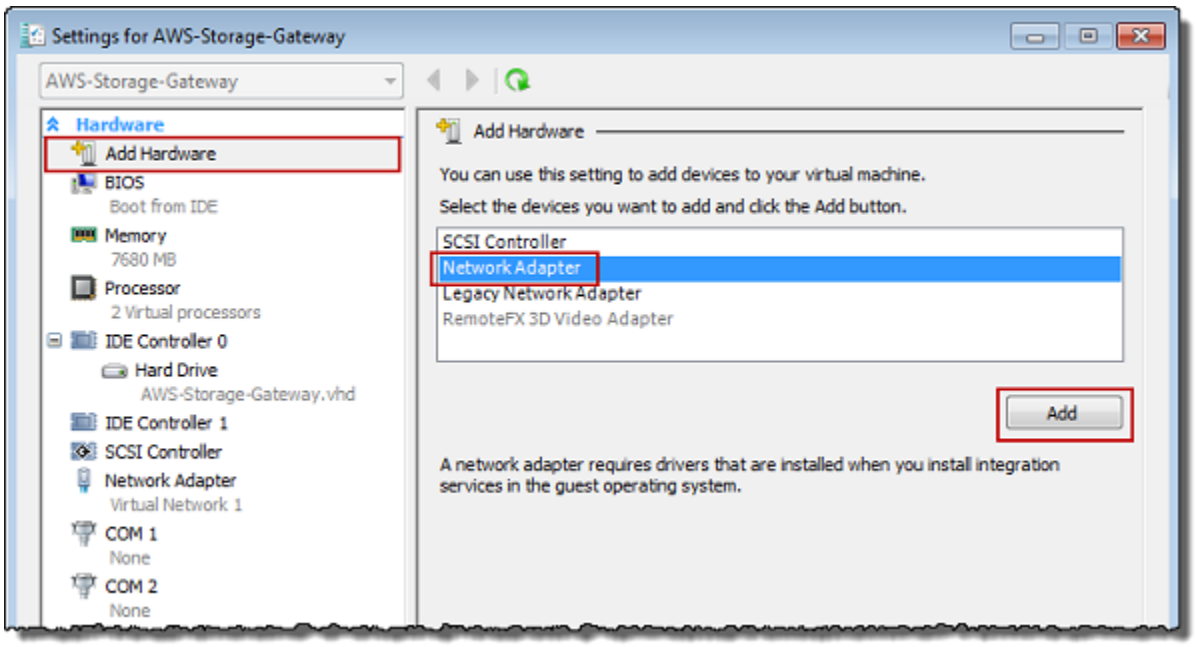
下列步骤假定您的网关 VM 已定义了一个网络适配器，并且您将添加第二个适配器。此过程演示如何为 Microsoft Hyper-V 主机添加适配器。

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 控制台中，关闭网关。有关说明，请参阅停止卷网关。
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)。

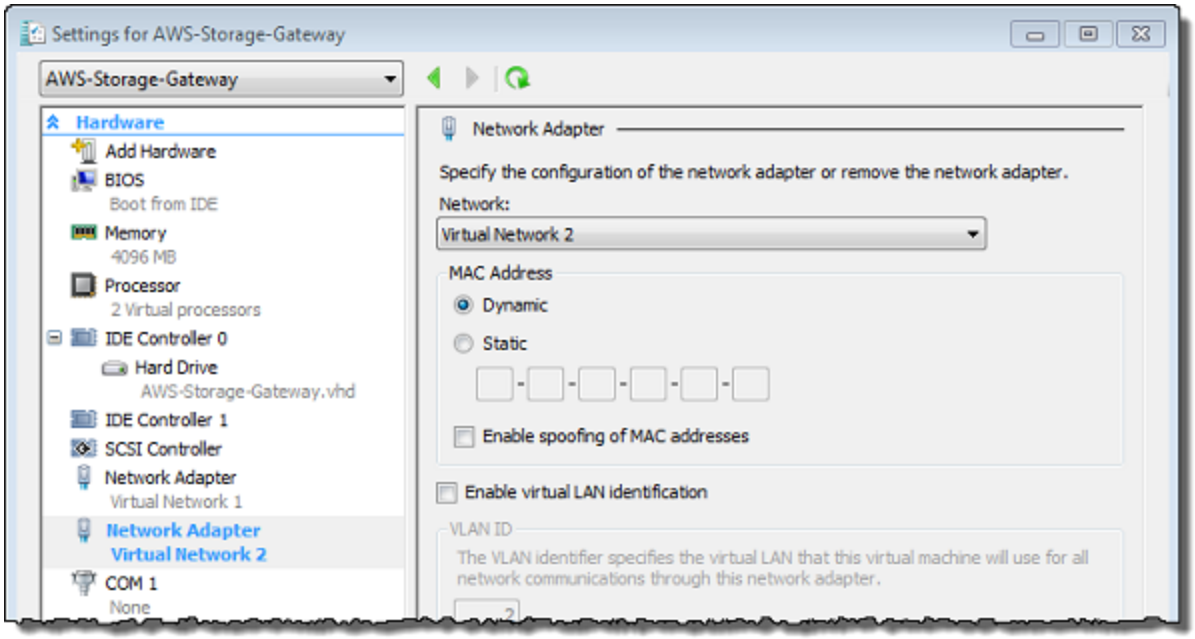


5. 在 VM 的 Settings (设置) 对话框中，对于 Hardware (硬件)，选择 Add Hardware (添加硬件)。
6. 在 Add Hardware (添加硬件) 窗格中，选择 Network Adapter (网络适配器)，然后选择 Add (添加) 以添加设备。



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 控制台中，打开网关。有关说明，请参阅启动卷网关。

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。

> **Note**
>
> Storage Gateway 控制台中的文件共享信息页面上提供的挂载命令会始终包括最近添加到文件共享的关联网关的网络适配器 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 虚拟机本地控制台上执行任务

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。

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

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

主题

- 使用 Storage Gateway 控制台删除网关
- 从本地部署的网关中删除资源
- 从部署在 Amazon EC2 实例上的网关中移除资源

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

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

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

> **Important**
>
> 删除网关后，您就不用再为软件付费，但虚拟磁带、Amazon 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。有关说明，请参阅使用 Storage Gateway 控制台删除网关。
- 删除不需要的所有 Amazon EBS 快照。有关说明，请参阅 Amazon EC2 用户指南中的删除亚马逊 EBS 快照。

从部署在 Amazon EC2 实例上的网关中移除资源

如果您想删除在 Amazon EC2 实例上部署的网关，我们建议您清理用于该网关的 AWS 资源，特别是 Amazon EC2 实例、所有 Amazon EBS 卷以及磁带（如果您部署了磁带网关）。完成此操作有助于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，按使用 Storage Gateway 控制台删除网关中所示删除网关。
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，移除附加到该实例的所有 Amazon EBS 卷（如果您不打算再次使用这些卷）。有关更多信息，请参阅 Amazon EC2 用户指南中的清理您的实例和卷。

Performance

本节介绍了 Storage Gateway 性能。

主题

- 优化网关性能
- 将 VMware vSphere High Availability 与 Storage Gateway 结合使用

优化网关性能

推荐的网关服务器配置

为了使您的网关发挥最佳性能，Storage Gateway 建议您的网关主机服务器采用以下网关配置：

- 至少 24 个专用的物理 CPU 核心
- 对于卷网关，您的硬件应使用以下数量的 RAM：
  - 对于缓存大小不超过 16 TiB 的网关，至少预留 16 GiB 的 RAM
  - 对于缓存大小为 16 TiB 至 32 TiB 的网关，至少预留 32 GiB 的 RAM
  - 对于缓存大小为 32 TiB 至 64 TiB 的网关，至少预留 48 GiB 的 RAM
- 磁盘 1，用作网关缓存，如下所示：
  - 使用 NVMe 控制器的 SSD。
- 磁盘 2，用作网关上传缓冲区，如下所示：
  - 使用 NVMe 控制器的 SSD。
- 磁盘 3，用作网关上传缓冲区，如下所示：
  - 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。

在网关中添加资源

以下瓶颈可能会使的性能降至理论最大持续吞吐量（通往 AWS 云的带宽）以下：

- CPU 核心数
- 缓存/上传缓冲区磁盘吞吐量
- RAM 总量
- 网络带宽至 AWS
- 从启动程序到网关的网络带宽

本节介绍为优化网关性能而可以采取的步骤。向网关或应用程序服务器添加资源是这些指导的基础。

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

缓存和上传缓冲区磁盘吞吐量会限制网关的上传和下载性能。如果您的网关表现出的性能明显低于预期，请考虑通过以下方式提高缓存和上传缓冲区磁盘吞吐量：

- 使用条带化 RAID（例如 RAID 10）来提高磁盘吞吐量，最好使用硬件 RAID 控制器。

  > **Note**
  >
  > RAID（独立磁盘冗余阵列）或专门的磁盘条带化 RAID 配置（如 RAID 10）是将数据主体划分为块并将数据块分布到多个存储设备的过程。您使用的 RAID 级别会影响您可以达到的确切速度和容错能力。通过将 IO 工作负载划分到多个磁盘上，RAID 设备的总体吞吐量远高于任何单个成员磁盘的吞吐量。

- 使用直接连接的高性能磁盘

  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。

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

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

添加更多上传缓冲区磁盘

要实现更高的写入吞吐量，请添加至少两个上传缓冲区磁盘。当数据写入网关时，系统会将其写入并本地存储在上传缓冲区磁盘上。之后，将从待处理和上传到 AWS的磁盘中异步读取存储的本地数据。添加更多上传缓冲区磁盘可以减少对每个磁盘执行的并发 I/O 操作量。这可以增加网关的写入吞吐量。

使用独立物理磁盘支持网关虚拟磁盘

在预配置网关磁盘时，我们强烈建议您不要为使用相同底层物理存储磁盘的上传缓冲区和缓存存储预配置本地磁盘。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，采用性能不太高的 RAID 配置（如 RAID 1 或 RAID 6）的数据存储可能会导致性能下降。

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 的每个虚拟处理器均采用一个专用的 CPU 内核。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该数据上传到 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。

增加网关和 AWS 云之间的带宽

增加进出带宽 AWS 将提高进入网关和输出到 AWS 云端的最大数据速率。如果网速是网关配置中的限制因素，而不是磁盘速度慢或网关启动程序连接带宽不足等其他因素，那么这样可以提高网关性能。

> **Note**
>
> 由于还存在此处列出的其他限制因素（例如缓存/上传缓冲区磁盘吞吐量、CPU 内核数、RAM 总量或启动程序和网关之间的带宽），您观察到的网关性能很可能会低于您的网络带宽。此外，网关的正常运行涉及为保护数据而执行的许多操作，这可能会导致观察到的性能低于您的网络带宽。

更改卷配置

对于卷网关，如果您发现向网关添加更多的存储卷会降低到网关的吞吐量，则应考虑将卷添加到单独的网关。具体而言，如果卷用于高吞吐量应用程序，则应考虑为高吞吐量应用程序另行创建网关。但一般而言，您不应该将一个网关用于所有的高吞吐量应用程序，另一个网关用于所有的低吞吐量应用程序。要测量卷吞吐量，请使用 `ReadBytes` 和 `WriteBytes` 指标。

有关这些指标的更多信息，请参阅 衡量您的应用程序和网关间的性能。 。

优化 iSCSI 设置

您可以优化 iSCSI 启动程序上的 iSCSI 设置，以实现更高的 I/O 性能。我们建议为 `MaxReceiveDataSegmentLength` 和 `FirstBurstLength` 选择 256 KiB，为 `MaxBurstLength` 选择 1 MiB。有关配置 iSCSI 设置的更多信息，请参阅自定义 iSCSI 设置。

> **Note**
>
> 这些建议的设置有助于实现更出色的整体性能。但是，优化性能所需的具体 iSCSI 设置因您使用的备份软件而异。有关详细信息，请参阅备份软件文档。

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

iSCSI 启动程序和网关之间的连接可能会限制您的上传和下载性能。如果您的网关的性能明显低于预期，并且您已经提高了 CPU 核心数量和磁盘吞吐量，请考虑：

- 升级网络电缆，使启动程序和网关之间具有更高的带宽。

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

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

向应用程序环境添加 CPU 资源

如果您的应用程序可以使用额外的 CPU 资源，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 High Availability 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。

vSphere HA 的工作原理是将虚拟机及其所在的主机集中到集群中以实现冗余。集群中的主机将受到监控，如果出现故障，故障主机上的虚拟机将在备用主机上重新启动。通常，恢复速度很快，不会丢失数据。有关 vSphere HA 的更多信息，请参阅 VMware 文档中的 vSphere HA 的工作原理。

> **Note**
>
> 重新启动出现故障的虚拟机并在新主机上重新建立 iSCSI 连接所需的时间取决于许多因素，例如主机操作系统和资源负载、磁盘速度、网络连接以及 SAN/存储基础架构。

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
- 从 Storage Gateway 控制台下载 .ova 映像
- 部署网关
- （可选）为集群上的其他 VM 添加覆盖选项
- 激活网关
- 测试您的 VMware High Availability 配置

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。

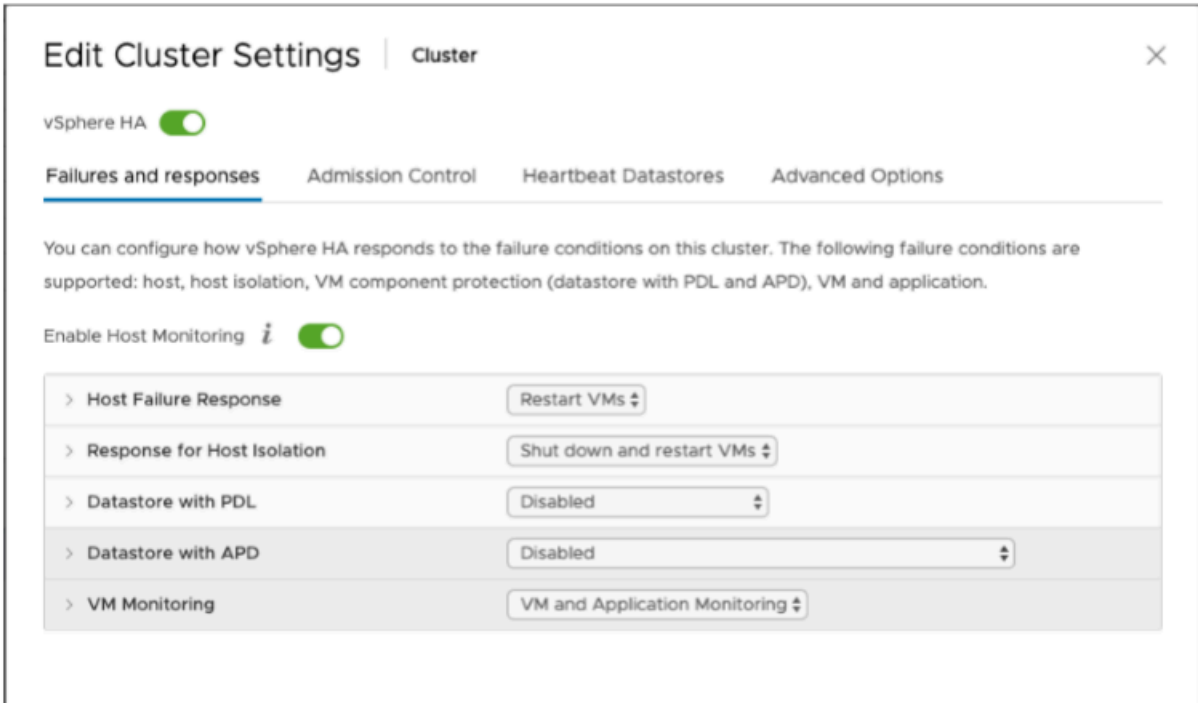
接下来，配置要与 Storage Gateway 结合使用的 VMware 集群。

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：

   - Host Failure Response (主机故障响应)：Restart VMs (重新启动 VM)
   - Response for Host Isolation (主机隔离的响应)：Shut down and restart VMs (关闭并重新启动 VM)
   - Datastore with PDL (具有 PDL 的数据存储)：Disabled (已禁用)
   - Datastore with APD (具有 APD 的数据存储)：Disabled (已禁用)
   - VM Monitoring (VM 监控)：VM and Application Monitoring (VM 和应用程序监控)

   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。
- 最短正常运行时间 - 在 VM 开始监控 VM 工具的检测信号之后，集群等待的时间。
- 每个 VM 的最大重置次数 - 集群在最大重置时段内重启 VM 的最大次数。
- 最大重置次数的时段 - 计算每个 VM 的最大重置次数的时段。

如果您不确定要设置的值，请使用以下示例设置：

- Failure interval (故障间隔)：**30** 秒
- Minimum uptime (最短正常运行时间)：**120** 秒
- Maximum per-VM resets (每个 VM 的最大重置次数)：**3**
- Maximum resets time window (最长重置时段)：**1** 小时

如果您在集群上运行了其他 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。

从 Storage Gateway 控制台下载 .ova 映像

下载适用于您的网关的 .ova 映像

- 在 Storage Gateway 控制台的设置网关页面上，选择您的网关类型和主机平台，然后使用控制台中提供的链接来下载 .ova，如设置卷网关中所述。

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。在 VMware 或本地环境中部署 Storage Gateway .ova 文件时，这些磁盘描述为半虚拟化 SCSI 磁盘。半虚拟化 是一种模式，在此模式下，网关 VM 使用主机操作系统来让控制台标识您添加到 VM 的虚拟磁盘。

   如需将 VM 配置为使用半虚拟化的控制器

1. 在 VMware 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。
2. 在 Virtual Machine Properties 对话框中，选择 Hardware 选项卡，再选择 SCSI controller 0，然后选择 Change Type。
3. 在 Change SCSI Controller Type 对话框中，选择 VMware Paravirtual SCSI 控制器类型，然后选择 OK。

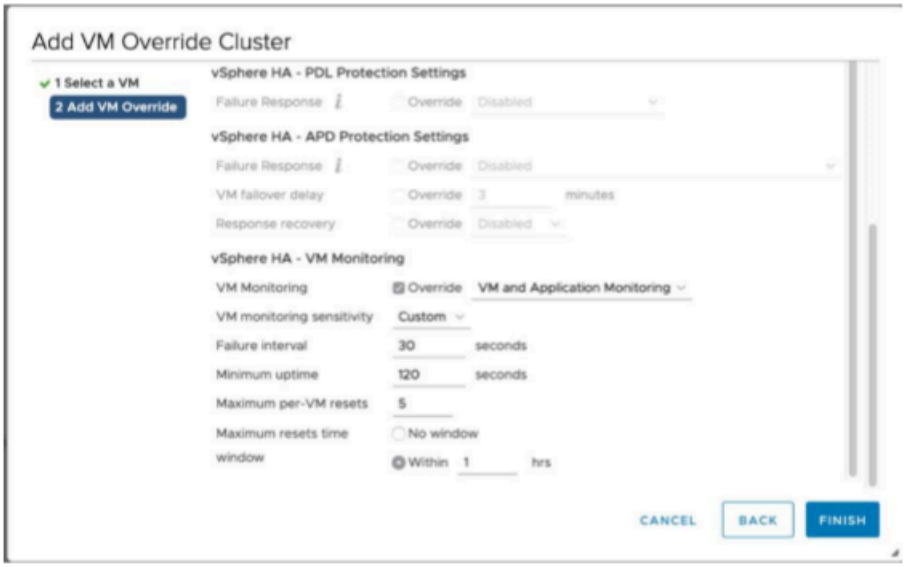
（可选）为集群上的其他 VM 添加覆盖选项

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 覆盖选项来更改每个值。

   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

- 请按照以下主题概述的步骤操作：

  a. 将您的卷网关连接到 AWS
  b. 检查设置并激活卷网关
  c. 配置卷网关

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. 打开 Storage Gateway 控制台，网址为 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. 请选择 Exit（退出）。

您可以在 Amazon CloudWatch 日志组中找到有关 VMware HA 事件的信息。有关更多信息，请参阅获取卷网关运行状况日志。

AWS Storage Gateway 中的安全

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

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

- 云安全 — AWS 负责保护在 Amazon Web Services 云中运行 AWS 服务的基础设施。 AWS 还为您提供可以安全使用的服务。作为AWS 合规计划合规计划合规计划合的一部分，第三方审计师定期测试和验证我们安全的有效性。要了解适用于 AWS Storage Gateway 的合规计划，请参阅按合规计划提供的范围内的AWSAWS 服务按合规计划服务。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

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

主题

- AWS Storage Gateway 中的数据保护
- AWS Storage Gateway 的身份和访问管理
- 登录和监控 AWS Storage Gateway
- AWS Storage Gateway 的合规性验证
- AWS Storage Gateway 中的弹性
- AWS Storage Gateway 中的基础设施安全
- AWS 安全最佳实践

AWS Storage Gateway 中的数据保护

AWS 分担责任模型分担责任模型适用于 AWS Storage Gateway 中的数据保护。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础设施上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题解答。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 IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证 (MFA)。
- 使用 SSL/TLS 与资源通信。 AWS 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-2 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（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括你使用控制台、API 或软件开发工具包 AWS 服务 使用 Storage Gateway 或其他 AWS 软件开发工具包的情况。 AWS CLI在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

使用数据加密 AWS KMS

Storage Gateway 使用 SSL/TLS（安全套接层/传输层安全）来加密在网关设备和存储设备之间传输的数据。 AWS 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 将网关配置为使用服务器端加密和 AWS Key Management Service (SSE-KMS) 密钥对存储在云中的数据进行加密。

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

加密文件共享

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

加密卷

对于缓存和存储的卷，您可以使用 Storage Gateway API 将网关配置为使用 AWS KMS托管密钥加密存储在云中的卷数据。您可以将其中一个托管密钥指定为 KMS 密钥。创建卷后，即无法更改用于加密卷的密钥。有关使用 Storage Gateway API 加密写入缓存或存储卷的数据的信息，请参阅 API 参考中的 CreateCachedisciVol ume 或 CreateStorediscivol ume。AWS Storage Gateway

加密磁带

对于虚拟磁带，您可以使用 Storage Gateway API 将网关配置为使用 AWS KMS托管密钥加密存储在云中的磁带数据。您可以将其中一个托管密钥指定为 KMS 密钥。创建磁带后，即无法更改用于加密磁带数据的密钥。有关使用 Storage Gateway API 加密写入虚拟磁带的数据的信息，请参阅 AWS Storage Gateway API 参考CreateTapes中的。

使用 AWS KMS 加密数据时，请记住以下几点：

- 您的数据在云中进行静态加密。也就是说，在 Amazon S3 中对数据进行加密。
- IAM 用户必须具有调用 AWS KMS API 操作所需的权限。有关更多信息，请参阅《AWS Key Management Service 开发人员指南》中的将 IAM 策略与 AWS KMS结合使用。
- 如果您删除或停用 AWS AWS KMS 密钥或撤消授权令牌，则无法访问卷或磁带上的数据。有关更多信息，请参阅《AWS Key Management Service 开发人员指南》中的删除 KMS 密钥。
- 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。

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

为您的卷配置 CHAP 身份验证

在 Storage Gateway 中，您的 iSCSI 启动程序作为 iSCSI 目标连接到您的卷。Storage Gateway 使用质询握手身份验证协议 (CHAP) 对 iSCSI 和启动程序连接进行身份验证。CHAP 通过要求进行身份验

证才能访问存储卷目标来预防反演攻击。对于每个卷目标，您可以定义一个或多个 CHAP 凭证。对于不同的启动程序，您可以在“Configure CHAP credentials”对话框中查看和编辑这些凭证。

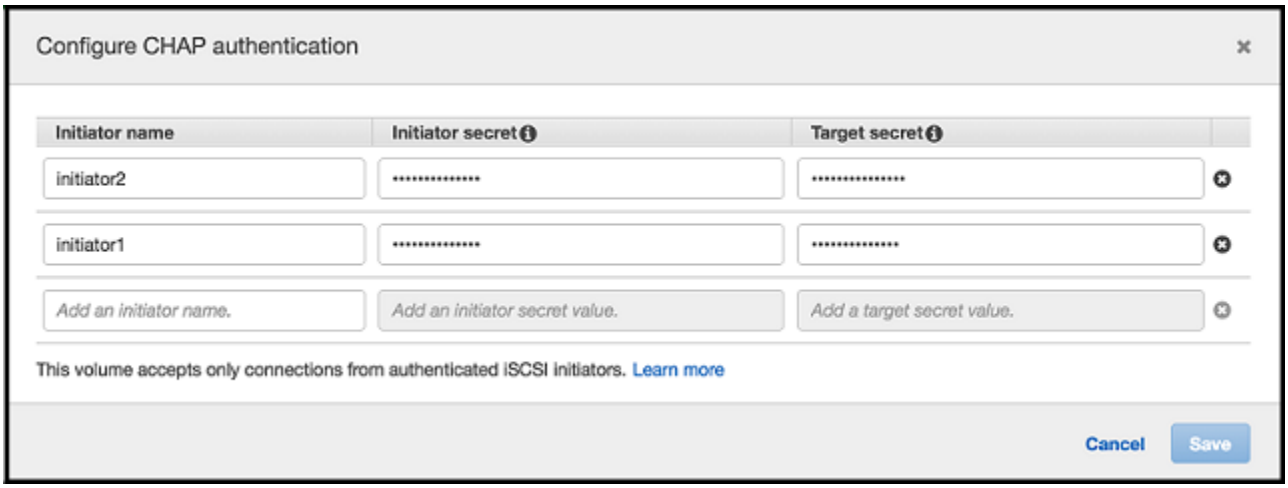
配置 CHAP 凭证

1. 在 Storage Gateway 控制台中，选择卷，然后选择要为其配置 CHAP 凭证的卷。
2. 对于 Actions (操作)，选择 Configure CHAP authentication (配置 CHAP 身份验证)。
3. 对于启动程序名称，键入启动程序的名称。该名称的长度必须至少为 1 个字符，最多 255 个字符。
4. 对于启动程序密钥，提供要用于验证 iSCSI 启动程序的密码。启动程序密码必须最少为 12 个字符，最多为 16 个字符。
5. 对于目标密钥，提供要用于验证双向 CHAP 的目标的密码。目标密码必须最少为 12 个字符，最多为 16 个字符。
6. 选择保存来保存您的输入。

要查看或更新 CHAP 凭证，您必须拥有允许执行该操作的必要 IAM 角色权限。

查看和编辑 CHAP 凭证

您可以为每个用户添加、删除或更新 CHAP 凭证。您必须拥有查看或编辑 CHAP 凭证的必要 IAM 角色权限，且启动程序目标必须附加到运行正常的网关。



添加 CHAP 凭证

1. 在 Storage Gateway 控制台中，选择卷，然后选择要为其添加 CHAP 凭证的卷。
2. 对于 Actions (操作)，选择 Configure CHAP authentication (配置 CHAP 身份验证)。

3. 在“配置 CHAPS”页面上，在各自的框中提供启动程序名称、启动程序密钥和目标密钥，然后选择保存。

删除 CHAP 凭证

1. 在 Storage Gateway 控制台中，选择卷，然后选择要为其删除 CHAP 凭证的卷。
2. 对于 Actions (操作)，选择 Configure CHAP authentication (配置 CHAP 身份验证)。
3. 单击要删除的凭证旁边的 X，然后选择保存。

更新 CHAP 凭证

1. 在 Storage Gateway 控制台中，选择卷，然后选择要为其更新 CHAP 的卷。
2. 对于 Actions (操作)，选择 Configure CHAP authentication (配置 CHAP 身份验证)。
3. 在“Configure CHAP credentials”页面上，更改要更新的凭证的条目。
4. 选择保存。

AWS Storage Gateway 的身份和访问管理

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以进行身份验证（登录）和授权（有权限）使用 AWS SGW 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- Stor AWS age Gateway 如何与 IAM 协作
- 适用于 AWS Storage Gateway 的基于身份的策略示例
- AWS Storage Gateway 身份和访问疑难解答

受众

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

服务用户-如果您使用 AWS SGW 服务完成工作，则您的管理员会为您提供所需的凭证和权限。当你使用更多的 AWS SGW 功能来完成工作时，你可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 AWS SGW 中的功能，请参阅AWS Storage Gateway 身份和访问疑难解答。

服务管理员 — 如果您负责公司的 AWS SGW 资源，则可能拥有对 AWS SGW 的完全访问权限。您的工作是确定您的服务用户应访问哪些 AWS SGW 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要详细了解贵公司如何在 AWS SGW 中使用 IAM，请参阅Stor AWS age Gateway 如何与 IAM 协作。

IAM 管理员 — 如果您是 IAM 管理员，则可能需要详细了解如何编写策略来管理 AWS SGW 的访问权限。要查看您可以在 IAM 中使用的 AWS SGW 基于身份的策略示例，请参阅。适用于 AWS Storage Gateway 的基于身份的策略示例

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （ IAM Identity Center ）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

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

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

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如， AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center 用户指南》中的多重身份验证和《IAM 用户指南》中的在 AWS中使用多重身份验证（MFA）。

AWS 账户 root 用户

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

联合身份

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

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

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

IAM 用户和群组

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的 对于需要长期凭证的使用场景定期轮换访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

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

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。您可以 AWS Management Console 通过切换角色在中临时担任 IAM 角色。您可以通过调用 AWS CLI 或

AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问 – 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的 权限集。
- 临时 IAM 用户权限 – IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Simple Storage Service (Amazon S3) 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
  - 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。
  - 服务相关角色-服务相关角色是一种链接到的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 A@@ mazon EC2 上运行的应用程序 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这优先于在 EC2 实例中存储访问密钥。要向 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建附加到该实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅IAM 用户指南中的何时创建 IAM 角色（而不是用户）。

使用策略管理访问

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

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

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

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

基于身份的策略

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

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

基于资源的策略

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

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

访问控制列表 (ACL)

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

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

其他策略类型

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

- 权限边界：权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅《IAM 用户指南》中的 IAM 实体的权限边界。
- 服务控制策略 (SCP)-SCP 是 JSON 策略，用于指定组织或组织单位 (OU) 的最大权限。 AWS Organizations AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果在组织内启用了所有功能，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organizations 和 SCP 的更多信息，请参阅《AWS Organizations 用户指南》中的 SCP 的工作原理。
- 会话策略 – 会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅《IAM 用户指南》中的会话策略。

多个策略类型

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

Stor AWS age Gateway 如何与 IAM 协作

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

你可以在 AWS Storage Gateway 中使用的 IAM 功能

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

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

SGW 基于身份的策略 AWS

支持基于身份的策略	是

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

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

SGW 基于身份的策略示例 AWS

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

SGW 内部 AWS 基于资源的政策

支持基于资源的策略	否

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

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

AWS SGW 的政策行动

支持策略操作	是

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

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

在策略中包含操作以授予执行关联操作的权限。

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

AWS SGW 中的策略操作在操作前使用以下前缀：

```
sgw
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

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

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

AWS SGW 的政策资源

支持策略资源	是

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

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 Amazon 资源名称 (ARN) 指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

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

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

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

AWS SGW 的策略条件密钥

支持特定于服务的策略条件键	是

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

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM 策略元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件键。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

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

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

SGW 中的 AWS ACL

支持 ACL	否

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

带有 SGW 的 ABA AWS C

支持 ABAC（策略中的标签）	部分

基于属性的访问权限控制（ABAC）是一种授权策略，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以向 IAM 实体（用户或角色）和许多 AWS 资源附加标签。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

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

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

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

在 AWS SGW 中使用临时证书

支持临时凭证	是

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IA M 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的切换到角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

转发 AWS SGW 的访问会话

支持转发访问会话 (FAS)	是

当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

AWS SGW 的服务角色

支持服务角色	是

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

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

SGW 的 AWS 服务相关角色

支持服务相关角色	是

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

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

适用于 AWS Storage Gateway 的基于身份的策略示例

默认情况下，用户和角色无权创建或修改 AWS SGW 资源。他们也无法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM policy。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

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

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

主题

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

策略最佳实践

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

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略或工作职能的AWS 托管式策略。
- 应用最低权限 – 在使用 IAM policy 设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM policy 中的条件进一步限制访问权限 – 您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 AWS CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证 IAM policy，确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，确保策略符合 IAM policy 语言（JSON）和 IAM 最佳实践。IAM Access

Analyzer 提供 100 多项策略检查和可操作的建议，有助于制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM Access Analyzer 策略验证。

- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。要在调用 API 操作时需要 MFA，请将 MFA 条件添加到策略中。有关更多信息，请参阅《IAM 用户指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html中的配置受 MFA 保护的 API 访问。

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

使用 AWS SGW 控制台

要访问 AWS Storage Gateway 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您 AWS 账户的 AWS SGW 资源的详细信息。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色仍然可以使用 AWS SGW 控制台，还要将 AWS SGW *ConsoleAccess* 或*ReadOnly* AWS 托管策略附加到实体。有关更多信息，请参阅《IAM 用户指南》中的为用户添加权限。

允许用户查看他们自己的权限

该示例说明了如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
```

```
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Storage Gateway 身份和访问疑难解答

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

主题

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

我无权在 AWS SGW 中执行任何操作

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

当 `mateojackson` IAM 用户尝试使用控制台查看有关虚构 *`my-example-widget`* 资源的详细信息，但不拥有虚构 `sgw:`*`GetWidget`* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 sgw:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 sgw:*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam：PassRole

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

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 marymajor 的 IAM 用户尝试使用控制台在 AWS SGW 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人 AWS 账户 访问我的 AWS SGW 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以担任角色。对于支持基于资源的策略或访问控制列表（ACL）的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

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

登录和监控 AWS Storage Gateway

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

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

Storage Gateway 信息位于 CloudTrail

CloudTrail 在您创建账户时，将在您的亚马逊 Web Services 账户上激活。当 Storage Gateway 中发生活动时，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在 Amazon Web Services 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录 Amazon Web Services 账户中的事件（包括 Storage Gateway 的事件），请创建跟踪记录。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。默认情况下，当您在控制台中创建跟踪时，该跟踪将应用于所有 AWS 区域。跟踪记录 AWS 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

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

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

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

- 请求是使用根证书还是 AWS Identity and Access Management (IAM) 用户凭证发出。

- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

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

了解 Storage Gateway 日志文件条目

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

以下示例显示了演示该操作的 CloudTrail 日志条目。

```
{ "Records": [{
                "eventVersion": "1.02",
                "userIdentity": {
                "type": "IAMUser",
                "principalId": "AIDAII5AUEPBH2M7JTNVC",
                "arn": "arn:aws:iam::111122223333:user/StorageGateway-team/JohnDoe",
                "accountId": "111122223333",
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                 "userName": "JohnDoe"
               },
                  "eventTime": "2014-12-04T16:19:00Z",
                  "eventSource": "storagegateway.amazonaws.com",
                  "eventName": "ActivateGateway",
                  "awsRegion": "us-east-2",
                  "sourceIPAddress": "192.0.2.0",
                  "userAgent": "aws-cli/1.6.2 Python/2.7.6 Linux/2.6.18-164.el5",
                   "requestParameters": {
                                          "gatewayTimezone": "GMT-5:00",
                                          "gatewayName": "cloudtrailgatewayvtl",
                                          "gatewayRegion": "us-east-2",
                                          "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
                                          "gatewayType": "VTL"
                                               },
                                               "responseElements": {
                                                                      "gatewayARN":
 "arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayvtl"
                                               },
```

```
                                                    "requestID":
 "54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
                                                    "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
                                                    "eventType": "AwsApiCall",
                                                    "apiVersion": "20130630",
                                                    "recipientAccountId": "444455556666"
             }]
}
```

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

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

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

AWS Storage Gateway 的合规性验证

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

有关特定合规计划范围内的 AWS 服务列表，请参阅按合规计划划分的范围内的AWSAWS 服务按合规计划。有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 Storage Gateway 时的合规性责任由您的数据的敏感性、您公司的合规性目标以及适用的法律法规决定。 AWS 提供以下资源来帮助满足合规性要求：

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了在上部署以安全性和合规性为重点的基准环境的步骤。 AWS
- HIPAA 安全与合规架构白皮书 — 本白皮书描述了公司如何使用来 AWS 创建符合 HIPAA 标准的应用程序。
- AWS 合规资源AWS — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 此 AWS 服务可全面了解您的安全状态 AWS ，帮助您检查是否符合安全行业标准和最佳实践。

AWS Storage Gateway 中的弹性

AWS 全球基础设施是围绕 AWS 区域和可用区构建的。 AWS 区域提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络相连。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失效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 全球基础架构外，Storage Gateway 还提供多项功能来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 High Availability 与 Storage Gateway 结合使用。
- AWS Backup 用于备份您的音量。有关更多信息，请参阅备份您的卷。
- 从恢复点克隆您的卷。有关更多信息，请参阅克隆卷。

AWS Storage Gateway 中的基础设施安全

作为一项托管服务， AWS Storage Gateway 受亚马逊网络服务：安全流程概述白皮书中描述的 AWS 全球网络安全程序的保护。

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

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

AWS 安全最佳实践

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

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。文件共享的故障排除信息适用于文件网关类型。卷的故障排除信息适用于卷网关类型。磁带的故障排除信息适用于磁带网关类型。网关问题的疑难解答信息适用于使用 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

- 故障排除： AWS Storage Gateway 控制台中网关状态显示为离线
- 故障排除：在 Storage Gateway 激活期间收到内部错误
- 排查本地网关问题
- 排查 Microsoft Hyper-V 设置
- 排查 Amazon EC2 网关问题
- 排查硬件设备问题
- 排查卷问题
- 排查高可用性问题
- 恢复数据的最佳实践

故障排除： AWS Storage Gateway 控制台中网关状态显示为离线

使用以下故障排除信息来确定如果 AWS Storage Gateway 控制台显示您的网关处于离线状态，该怎么做。

由于以下一个或多个原因，您的网关可能显示为离线：

- 网关无法到达 Storage Gateway 服务端点。
- 网关意外关闭。
- 与网关关联的缓存磁盘已断开连接或修改，或者出现故障。

要使网关恢复联机，请确定并解决导致网关离线的问题。

检查关联的防火墙或代理

如果您将网关配置为使用代理，或者将网关置在防火墙后面，请查看代理或防火墙的访问规则。代理或防火墙必须允许进出 Storage Gateway 所需的网络端口和服务端点的流量。有关更多信息，请参阅网络和防火墙要求。

检查是否正在对网关流量进行 SSL 检查或深度数据包检查

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

检查虚拟机管理程序主机上是否出现停电或硬件故障

网关的虚拟机管理程序主机出现停电或硬件故障可能会导致网关意外关闭并无法访问。恢复电源和网络连接后，您的网关将再次可访问。

网关重新联机后，请务必采取措施恢复数据。有关更多信息，请参阅实践恢复数据的最佳实践。

检查关联的缓存磁盘是否有问题

如果至少有一个与您的网关关联的缓存磁盘被移除、更改或调整了大小，或者该缓存磁盘已损坏，则网关可能会脱机。

如果从虚拟机管理程序主机上移除了正常工作的缓存磁盘：

1. 关闭网关。
2. 重新添加磁盘。

> **Note**
>
> 确保将磁盘添加到同一个磁盘节点。

3. 重新启动网关。

如果缓存磁盘损坏、被更换或调整了大小：

1. 关闭网关。
2. 重置缓存磁盘。
3. 为缓存存储空间重新配置磁盘。

4. 重新启动网关。

故障排除：在 Storage Gateway 激活期间收到内部错误

Storage Gateway 激活请求会通过两条网络路径传输。客户端发送的传入激活请求通过端口 80 连接到网关的虚拟机 (VM) 或亚马逊弹性计算云 (Amazon EC2) 实例。如果网关成功收到激活请求，则网关将与 Storage Gateway 端点通信以接收激活密钥。如果网关无法到达 Storage Gateway 终端节点，则网关会向客户端发送一条内部错误消息。

使用以下疑难解答信息来确定在尝试激活时收到内部错误消息时该怎么做 AWS Storage Gateway。

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

解决使用公共终端节点激活网关时出现的错误

要解决使用公共终端节点激活网关时的激活错误，请执行以下检查和配置。

检查所需的端口

对于本地部署的网关，请检查本地防火墙上的端口是否已打开。对于部署在 Amazon EC2 实例上的网关，请检查实例安全组上的端口是否已打开。要确认端口已打开，请从服务器在公共端点上运行 telnet 命令。此服务器必须与网关位于同一个子网中。例如，以下 telnet 命令测试与端口 443 的连接：

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

要确认网关本身是否可以到达终端节点，请访问网关的本地虚拟机控制台（适用于本地部署的网关）。或者，您可以通过 SSH 连接到网关的实例（适用于部署在 Amazon EC2 上的网关）。然后，运行网络连接测试。确认测试已返回[PASSED]。有关更多信息，请参阅 net 的连接。

> **Note**
>
> 网关控制台的默认登录用户名为admin，默认密码为password。

确保防火墙安全不会修改从网关发送到公共端点的数据包

SSL 检查、深度数据包检查或其他形式的防火墙安全措施可能会干扰从网关发送的数据包。如果 SSL 证书的修改与激活端点的预期不同，SSL 握手就会失败。要确认没有正在进行的 SSL 检查，请在端口 443 的主激活端点 (anon-cp.storagegateway.region.amazonaws.com) 上运行 OpenSSL 命令。您必须从与网关位于同一子网的计算机上运行以下命令：

```
$ openssl s_client -connect  anon-cp.storagegateway.region.amazonaws.com:443 -
servername anon-cp.storagegateway.region.amazonaws.com
```

> **Note**
>
> 将##替换为你的 AWS 区域。

如果没有正在进行的 SSL 检查，则该命令将返回类似于以下内容的响应：

```
$ openssl s_client -connect anon-cp.storagegateway.us-east-2.amazonaws.com:443 -
servername anon-cp.storagegateway.us-east-2.amazonaws.com
CONNECTED(00000003)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-2.amazonaws.com
verify return:1
---
Certificate chain
 0 s:/CN=anon-cp.storagegateway.us-east-2.amazonaws.com
   i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
 1 s:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
   i:/C=US/O=Amazon/CN=Amazon Root CA 1
 2 s:/C=US/O=Amazon/CN=Amazon Root CA 1
   i:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
```

```
 3 s:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
   i:/C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority
---
```

如果正在进行 SSL 检查，则响应会显示证书链已更改，如下所示：

```
$ openssl s_client -connect  anon-cp.storagegateway.ap-southeast-1.amazonaws.com:443 -
servername anon-cp.storagegateway.ap-southeast-1.amazonaws.com
CONNECTED(00000003)
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.ap-southeast-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

激活端点仅在识别 SSL 证书时才接受 SSL 握手。这意味着网关到终端节点的出站流量必须免受网络中防火墙的检查。这些检查可能是 SSL 检查或深度数据包检查。

检查网关时间同步

时间偏差过大可能会导致 SSL 握手错误。对于本地网关，您可以使用网关的本地虚拟机控制台来检查网关的时间同步。时间偏差不应大于 60 秒。有关更多信息，请参阅。

系统时间管理选项在 Amazon EC2 实例上托管的网关上不可用。要确保 Amazon EC2 网关能够正确同步时间，请确认 Amazon EC2 实例可以通过端口 UDP 和 TCP 123 连接到以下 NTP 服务器池列表：

- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org
- 2.amazon.pool.ntp.org
- 3.amazon.pool.ntp.org

解决使用 Amazon VPC 终端节点激活网关时出现的错误

要解决使用亚马逊虚拟私有云（Amazon VPC）终端节点激活网关时出现的激活错误，请执行以下检查和配置。

检查所需的端口

确保本地防火墙（对于本地部署的网关）或安全组（对于部署在 Amazon EC2 中的网关）中的所需端口已打开。将网关连接到 Storage Gateway VPC 终端节点所需的端口与将网关连接到公共终端节点时所需的端口不同。连接到 Storage Gateway VPC 终端节点需要以下端口：

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

有关更多信息，请参阅为 Storage Gatew ay 创建 VPC 终端节点。

此外，请检查连接到您的 Storage Gateway VPC 终端节点的安全组。连接到终端节点的默认安全组可能不允许所需的端口。创建一个新的安全组，允许来自网关 IP 地址范围的流量通过所需端口。然后，将该安全组附加到 VPC 终端节点。

> **Note**
>
> 使用 Amazon VPC 控制台验证连接到 VPC 终端节点的安全组。从控制台查看您的 Storage Gateway VPC 终端节点，然后选择安全组选项卡。

要确认所需端口已打开，您可以在 Storage Gateway VPC 终端节点上运行 telnet 命令。您必须从与网关位于同一子网的服务器上运行这些命令。您可以对第一个未指定可用区域的 DNS 名称进行测试。例如，以下 telnet 命令使用 DNS 名称 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 测试所需的端口连接：

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 443
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1026
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1027
```

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1028
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1031
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 2222
```

确保防火墙安全不会修改从网关发送到您的 Storage Gateway Amazon VPC 终端节点的数据包

SSL 检查、深度数据包检查或其他形式的防火墙安全措施可能会干扰从网关发送的数据包。如果 SSL 证书的修改与激活端点的预期不同，SSL 握手就会失败。要确认没有正在进行的 SSL 检查，请在您的 Storage Gateway VPC 终端节点上运行 OpenSSL 命令。您必须从与网关位于同一子网的计算机上运行此命令。为每个必需的端口运行命令：

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:443 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1026 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1028 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1031 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:2222 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

如果没有正在进行的 SSL 检查，则该命令将返回类似于以下内容的响应：

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
```

```
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-1.amazonaws.com
verify return:1
---
Certificate chain
 0 s:CN = anon-cp.storagegateway.us-east-1.amazonaws.com
   i:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
 1 s:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
   i:C = US, O = Amazon, CN = Amazon Root CA 1
 2 s:C = US, O = Amazon, CN = Amazon Root CA 1
   i:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
 3 s:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
   i:C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification
 Authority
---
```

如果正在进行 SSL 检查，则响应会显示证书链已更改，如下所示：

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.us-
east-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.us-east-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

激活端点仅在识别 SSL 证书时才接受 SSL 握手。这意味着，网关通过所需端口到您的 VPC 终端节点的出站流量不受网络防火墙的检查。这些检查可能是 SSL 检查或深度数据包检查。

检查网关时间同步

时间偏差过大可能会导致 SSL 握手错误。对于本地网关，您可以使用网关的本地虚拟机控制台来检查网关的时间同步。时间偏差不应大于 60 秒。有关更多信息，请参阅。

系统时间管理选项在 Amazon EC2 实例上托管的网关上不可用。要确保 Amazon EC2 网关能够正确同步时间，请确认 Amazon EC2 实例可以通过端口 UDP 和 TCP 123 连接到以下 NTP 服务器池列表：

- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org
- 2.amazon.pool.ntp.org
- 3.amazon.pool.ntp.org

检查 HTTP 代理并确认相关的安全组设置

在激活之前，请检查您是否在本地网关虚拟机上将 Amazon EC2 上的 HTTP 代理配置为端口 3128 上的 Squid 代理。在这种情况下，请确认以下内容：

- 附加到 Amazon EC2 上的 HTTP 代理的安全组必须具有入站规则。此入站规则必须允许来自网关 VM 的 IP 地址的 Squid 代理流量通过端口 3128。
- 连接到 Amazon EC2 VPC 终端节点的安全组必须具有入站规则。这些入站规则必须允许来自亚马逊 EC2 上 HTTP 代理 IP 地址的端口 1026-1028、1031、2222 和 443 上的流量。

解决使用公有终端节点激活网关且同一 VPC 中有 Storage Gateway VPC 终端节点时出现的错误

要解决在同一 VPC 中有 Amazon Virtual Private Cloud (Amazon VPC) 终端节点时使用公共终端节点激活网关时出现的错误，请执行以下检查和配置。

确认您的 Storage Gateway VPC 终端节点上未启用 “启用私有 DNS 名称” 设置

如果启用了启用私有 DNS 名称，则无法激活从该 VPC 到公有终端节点的任何网关。

要禁用私有 DNS 名称选项，请执行以下操作：

1. 打开 Amazon VPC 控制台。
2. 在导航窗格中，选择端点。

3. 选择您的 Storage Gateway VPC 终端节点。
4. 选择操作。
5. 选择 “管理私有 DNS 名称”。
6. 在 “启用私有 DNS 名称” 中，清除 “为此端点启用”。
7. 选择修改私有 DNS 名称以保存设置。

排查本地网关问题

您可以在下面找到有关在使用本地网关时可能遇到的典型问题以及如何激活 AWS Support 以帮助排除网关故障的信息。

下表列出了您在使用场内网关时可能遇到的典型问题。

问题	要采取的操作
您找不到网关的 IP 地址。	请使用管理程序客户端连接主机，以便查找网关 IP 地址。 • 对于 VMware ESXi，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。 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。 • 不应激活 SSL 证书验证/检查。Storage Gateway 使用双向 TLS 身份验证，如果任何第三方应用程序尝试拦截/签署任一证书，则该身份验证将失败。 • 如果使用防火墙或路由器来筛选或限制网络流量，则必须配置防火墙和路由器以允许这些服务端点与 AWS进行出站通信。有关网络和防火墙要求的更多信息，请参阅网络和防火墙要求。

问题	要采取的操作
当您单击 Storage Gateway 管理控制台中的继续激活按钮时，网关的激活过程会失败。	• 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 通过代理路由本地网关。 • 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 同步您的网关 VM 时间。 • 执行这些步骤后，您可以使用 Storage Gateway 控制台和设置并激活网关向导重新尝试网关部署。 • 不应激活 SSL 证书验证/检查。Storage Gateway 使用双向 TLS 身份验证，如果任何第三方应用程序尝试拦截/签署任一证书，则该身份验证将失败。 • 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。	有关移除分配为上传缓冲区的磁盘的说明，请参阅从网关中移除磁盘
您需要提高网关和 AWS之间的带宽。	您可以将互联网连接设置为 AWS 与连接应用程序和网关 VM 的网卡 (NIC) 分开的网络适配器 (NIC)，从而 AWS 改善从网关到的带宽。如果您有高带宽连接， AWS 并且想要避免带宽争用，尤其是在快照还原期间，则采用这种方法很有用。对于高吞吐量工作负载需求，您可以使用 AWS Direct Connect 在本地网关和 AWS间建立专用网络连接。要测量从您的网关到的连接带宽 AWS，请使用网关的`CloudBytesDownloaded` 和`CloudBytesUploaded` 指标。有关本主题的更多信息，请参阅 衡量网关与 AWS间的性能。提高 Internet 连接性能有助于确保您的上传缓冲区不被填满。

问题	要采取的操作

往返您网关的吞吐量将为零。	• 在 Storage Gateway 控制台的网关选项卡上，确认网关 VM 的 IP 地址与使用管理程序客户端软件（即 VMware vSphere 客户端或 Microsoft Hyper-V Manager）看到的 IP 地址相同。如果发现 IP 地址不一致，请从 Storage Gateway 控制台重启网关，如关闭网关虚拟机中所述。重启后，Storage Gateway 控制台的网关选项卡中 IP 地址列表中的地址应与您从管理程序客户端确定的网关 IP 地址相匹配。
	  • 对于 VMware ESXi，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。
	• 检查您的网关与的连接， AWS 如中所述测试网关到 Internet 的连接。
	• 检查网关的网络适配器配置，确保要激活的所有网关接口均已激活。若要查看网关的网络适配器配置，请遵循 配置网关网络 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 控制台查看进出网关的吞吐量。有关测量进出网关的吞吐量的更多信息 AWS，请参阅衡量网关与 AWS间的性能。

在 Microsoft Hyper-V 中导入（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。
您收到一条消息，指出“已写入网关卷中的数据未安全存储在 AWS中”。	如果您的网关虚拟机是从另一个网关虚拟机的克隆或快照创建的，则您会收到此消息。如果不是这种情况，请联系 AWS Support。

允许帮助 AWS Support 对本地托管的网关进行故障排除

Storage Gateway 提供了一个本地控制台，您可以使用它来执行多项维护任务，包括激活 AWS Support 以访问网关以帮助您解决网关问题。默认情况下，对您的网关的 AWS Support 访问处于停用

状态。您可通过主机的本地控制台来实现此访问。要 AWS Support 访问您的网关，请先登录主机的本地控制台，导航到 Storage Gateway 的控制台，然后连接到支持服务器。

允许 AWS Support访问您的网关

1. 登录到主机的本地控制台。

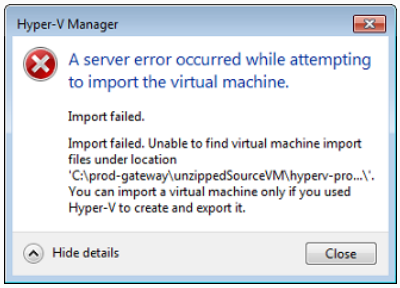
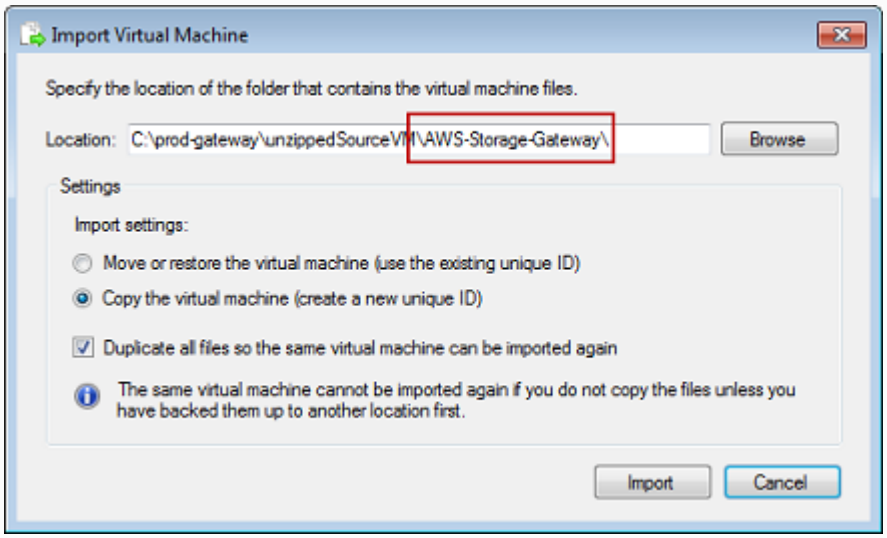
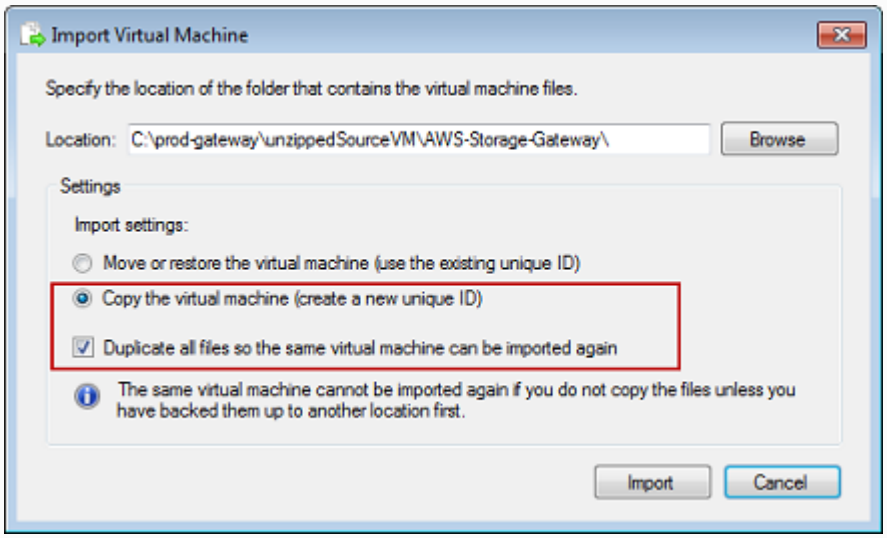
   - VMware ESXi - 有关更多信息，请参阅使用 VMware ESXi 访问网关本地控制台。
   - Microsoft Hyper-V - 有关更多信息，请参阅使用 Microsoft Hyper-V 访问网关本地控制台。
2. 在提示符处输入相应的数字来选择网关控制台。
3. 输入 **h** 打开可用命令的列表。
4. 请执行以下操作之一：

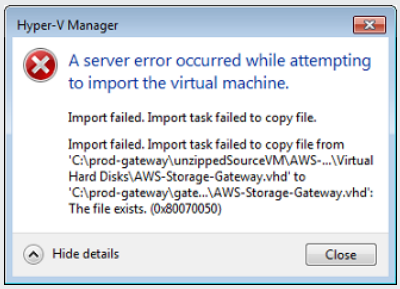
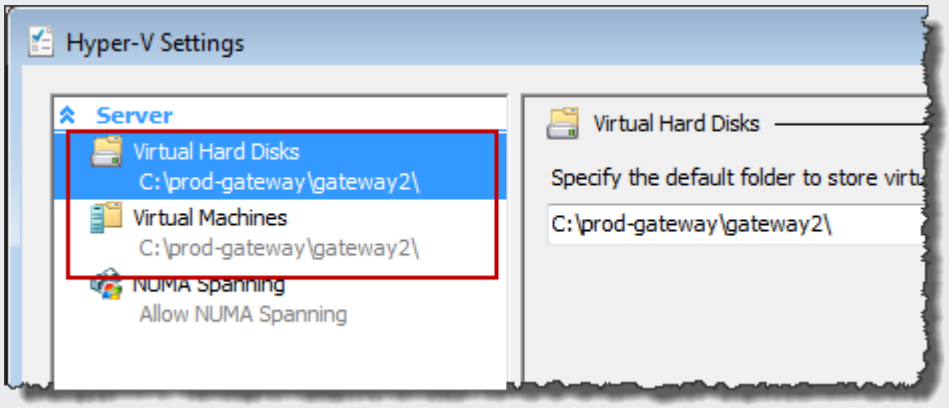
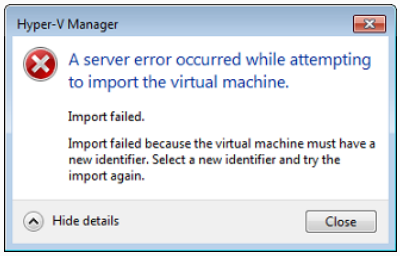
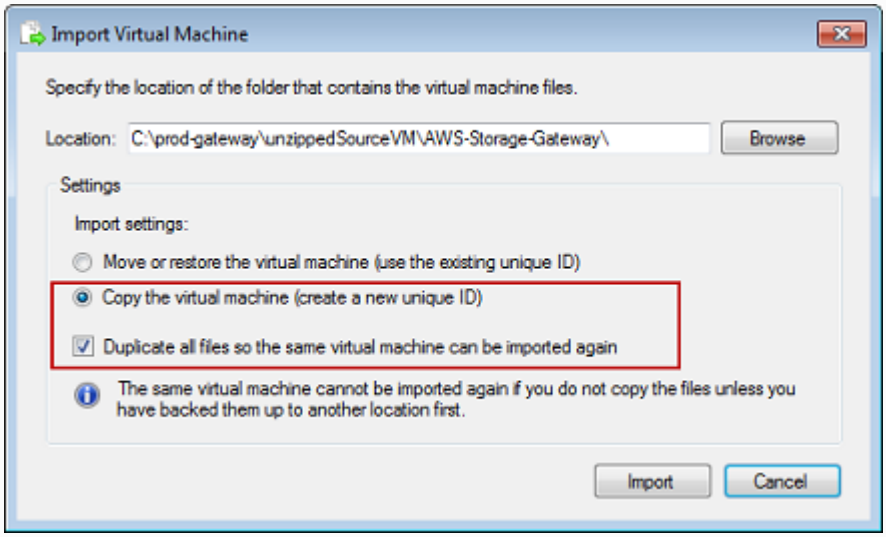
   - 如果网关使用的是公有端点，请在可用命令窗口中，输入 **`open-support-channel`** 来连接到 Storage Gateway 的客户支持。允许 TCP 端口 22，以便您可以打开 AWS的支持通道。在连接到客户支持时，Storage Gateway 将为您分配支持编号。请记下您的支持编号。
   - 如果网关使用的是 VPC 端点，请在 AVAILABLE COMMANDS 窗口中，输入 **`open-support-channel`**。如果未激活网关，请提供要连接到 Storage Gateway 客户支持的 VPC 端点或 IP 地址。允许 TCP 端口 22，以便您可以打开 AWS的支持通道。在连接到客户支持时，Storage Gateway 将为您分配支持编号。请记下您的支持编号。

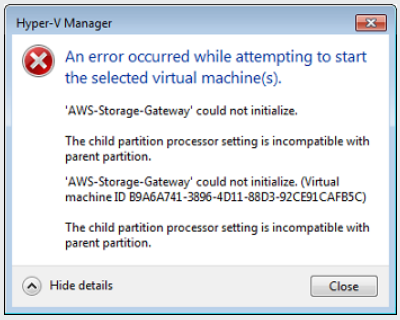
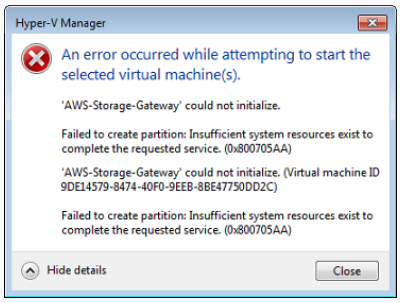
   > **Note**
   >
   > 渠道号不是传输控制协议/用户数据报协议 (TCP/UDP) 端口号。相反，网关会与 Storage Gateway 服务器建立 Secure Shell (SSH) (TCP 22) 连接，并提供用于连接的支持通道。
5. 建立支持渠道后，请向提供您的支持服务号码， AWS Support AWS Support 以便提供故障排除帮助。
6. 在支持会话完成后，输入 **q** 以将其结束。在 Amazon Web Services Support 通知您支持会话完成之前，请勿关闭该会话。
7. 输入 **`exit`** 注销该网关控制台。
8. 按照提示操作退出本地控制台。

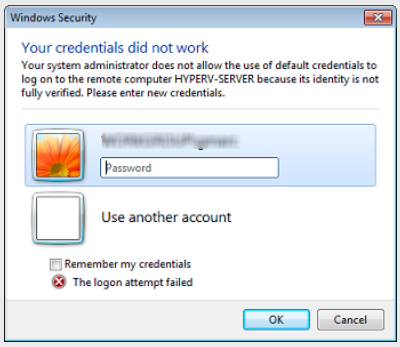
排查 Microsoft Hyper-V 设置

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	要采取的操作
您在尝试导入网关时会收到错误消息“Import failed。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，但没有在导入虚拟机对话框中选择复制虚拟机选项和复制所有文件选项，则在解压缩的网关文件所在位置创建 VM，并且您无法再从这个位置导入。为了修复此问题，请获取最新的解压缩网关源文件副本，并将其复制到新的位置。将新的位置用作导入源目录。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	要采取的操作
您在尝试导入网关时会收到错误消息“Import failed。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“Import failed。Import failed because the virtual machine must have a new identifier。Select a new identifier and try the import again.” 	导入网关时，请确保在导入虚拟机对话框中选择复制虚拟机选项并选中复制所有文件选项，为 VM 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	要采取的操作
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 Storage Gateway 要求的更多信息，请参阅要求。
您尝试启动网关 VM，但收到下列一种错误消息“Failed to create partition: Insufficient resources exist to complete the requested service.” 	此错误很可能是该网关所需的 RAM 和主机上可用的 RAM 之间的差异导致的。 有关 Storage Gateway 要求的更多信息，请参阅要求。
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，请参阅同步您的网关 VM 时间。
您需要将解压缩的 Microsoft Hyper-V Storage Gateway 文件放入主机文件系统中。	按照访问典型 Microsoft Windows 服务器的方式访问主机。例如，如果虚拟机监控程序主机名为 `hyperv-server` ，则可使用以下 UNC 路径 `\\hyperv-server\c$` ，其中假定可解析名称 `hyperv-server` ，或在本地 hosts 文件中定义了该名称。

问题	要采取的操作
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。
如果您在使用 Broadcom 网络适配器的 Hyper-V 主机上激活虚拟机队列 (VMQ)，您可能会注意到网络性能不佳。	有关解决方法的信息，请参阅 Microsoft 文档，请参阅如果启用了 VMQ，则 Windows Server 2012 Hyper-V 主机上虚拟机上的网络性能不佳。

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。若要详细了解本地网关和 Amazon EC2 中部署的网关之间的区别，请参阅 部署 Amazon EC2 实例来托管卷网关。

主题

- 过了一会儿您的网关并未激活
- 您在实例列表中找不到 EC2 网关实例
- 您创建了一个 Amazon EBS 卷，但无法将其附加到 EC2 网关实例
- 您不能将启动程序挂载到 EC2 网关的卷目标
- 您在尝试添加存储卷时收到一条消息称“无可用磁盘”
- 您希望删除一个分配为上传缓冲区空间的磁盘来减少上传缓冲区空间
- 进出 EC2 网关的吞吐量降为零
- 您 AWS Support 想帮忙排除 EC2 网关故障
- 您需要使用 Amazon EC2 Serial Console 连接到您的网关实例

过了一会儿您的网关并未激活

在 Amazon EC2 控制台中检查以下项：

- 已在与实例关联的安全组中激活端口 80。有关添加安全组规则的更多信息，请参阅 Amazon EC2 用户指南中的添加安全组规则。
- 网关实例会标记为“running”。在 Amazon EC2 控制台中，实例的状态应该是“正在运行”。
- 确保您的 Amazon EC2 实例类型满足最低要求，如存储需求中所述。

纠正该问题后，请尝试重新激活网关。为此，请打开 Storage Gateway 控制台，选择在 Amazon EC2 上部署新网关，然后重新输入实例的 IP 地址。

您在实例列表中找不到 EC2 网关实例

如果您没有为您的实例赋予资源标签，并且有很多实例在运行，则很难分辨哪个实例是您启动的。在这种情况下，可执行以下操作来查找网关实例：

- 检查实例说明选项卡上的 Amazon 系统映像 (AMI) 名称。基于 Storage Gateway AMI 的实例应以 **`aws-storage-gateway-ami`** 文本开头。
- 如果您有几个实例基于 Storage Gateway AMI，请查看实例启动时间来找到正确的实例。

您创建了一个 Amazon EBS 卷，但无法将其附加到 EC2 网关实例

检查讨论中的 Amazon EBS 卷是否与网关实例在同一可用区中。如果在不同的可用区，请在您的实例所在的可用区中创建一个新的 Amazon EBS 卷。

您不能将启动程序挂载到 EC2 网关的卷目标

检查您启动实例时所使用的安全组是否包含允许您用于 iSCSI 访问的端口的规则。该端口通常设置为 3260。有关连接到卷的更多信息，请参阅将卷连接到 Windows 客户端。

您在尝试添加存储卷时收到一条消息称“无可用磁盘”

没有为新激活的网关定义卷存储。在定义卷存储之前，必须将本地磁盘分配给网关，以便用作上传缓冲区和缓冲存储空间。对于部署到 Amazon EC2 的网关，本地磁盘是附加到实例的 Amazon EBS 卷。出现这个错误消息很可能是因为没有为实例定义 Amazon EBS 卷。

查看为运行网关的实例所定义的块储存设备。如果只存在两个数据块储存设备 (AMI 附带的默认设备)，那么应该增加存储。有关执行此操作的更多信息，请参阅 部署 Amazon EC2 实例来托管卷网关。在附加两个或两个以上的 Amazon EBS 卷后，尝试在网关上创建卷存储。

您希望删除一个分配为上传缓冲区空间的磁盘来减少上传缓冲区空间

按照 确定要分配的上传缓冲区的大小 中的步骤操作。

进出 EC2 网关的吞吐量降为零

验证网关实例是否在运行。例如，如果实例因系统重启而处于启动过程中，请等待该实例完成重启。

另外，验证网关 IP 是否改变。如果实例已停止，然后重新启动，那么实例的 IP 地址可能会发生更改。在这种情况下，您必须激活新的网关。

您可以从 Amazon CloudWatch 控制台查看进出网关的吞吐量。有关测量进出网关的吞吐量的更多信息 AWS，请参阅衡量网关与 AWS间的性能。

您 AWS Support 想帮忙排除 EC2 网关故障

Storage Gateway 提供了一个本地控制台，您可以使用它来执行多项维护任务，包括激活 AWS Support 以访问网关以帮助您解决网关问题。默认情况下，对您的网关的 AWS Support 访问处于停用状态。通过 Amazon EC2 本地控制台来提供此访问。通过 Secure Shell (SSH) 登录到 Amazon EC2 本地控制台。要通过 SSH 成功登录，您的实例的安全组必须具有开放 TCP 端口 22 的规则。

> **Note**
>
> 如果将新规则添加到现有安全组，则新规则适用于使用该安全组的所有实例。有关安全组以及如何添加安全组规则的更多信息，请参阅《Amazon EC2 用户指南》中的 Amazon EC2 安全组。

要 AWS Support 连接您的网关，您需要先登录 Amazon EC2 实例的本地控制台，导航到存储网关的控制台，然后提供访问权限。

激活对部署在 Amazon EC2 实例上的网关的 AWS Support 访问权限

1. 登录到 Amazon EC2 实例的本地控制台。有关说明，请转到《Amazon EC2 用户指南》中的连接到您的实例。

您可使用以下命令登录到 EC2 实例的本地控制台。

```
ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
```

> **Note**
>
> *PRIVATE-KEY* 是 .pem 文件，其中包含用来启动 Amazon EC2 实例的 EC2 密钥对的私有证书。有关更多信息，请参阅《Amazon EC2 用户指南》中的检索密钥对的公有密钥。*INSTANCE-PUBLIC-DNS-NAME* 是运行网关的 Amazon EC2 实例的公有域名系统 (DNS) 名称。可通过在 EC2 控制台中选择 Amazon EC2 实例并单击说明选项卡来获取此公有 DNS 名称。

2. 在提示符处，输入 **6 - Command Prompt** 来打开 AWS Support 通道控制台。
3. 输入 **h** 以打开 AVAILABLE COMMANDS 窗口。
4. 请执行以下操作之一：

   - 如果网关使用的是公有端点，请在可用命令窗口中，输入 **open-support-channel** 来连接到 Storage Gateway 的客户支持。允许 TCP 端口 22，以便您可以打开 AWS的支持通道。在连接到客户支持时，Storage Gateway 将为您分配支持编号。请记下您的支持编号。
   - 如果网关使用的是 VPC 端点，请在 AVAILABLE COMMANDS 窗口中，输入 **open-support-channel**。如果未激活网关，请提供要连接到 Storage Gateway 客户支持的 VPC 端点或 IP 地址。允许 TCP 端口 22，以便您可以打开 AWS的支持通道。在连接到客户支持时，Storage Gateway 将为您分配支持编号。请记下您的支持编号。

   > **Note**
   >
   > 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 Secure Shell (SSH) (TCP 22) 连接，并提供用于连接的支持通道。

5. 建立支持渠道后，请向提供您的支持服务号码， AWS Support AWS Support 以便提供故障排除帮助。
6. 在支持会话完成后，输入 **q** 以将其结束。在 AWS Support 通知您支持会话已完成之前，请勿关闭会话。
7. 输入 **exit** 来退出 Storage Gateway 控制台。
8. 通过控制台菜单操作来注销 Storage Gateway 实例。

您需要使用 Amazon EC2 Serial Console 连接到您的网关实例

您可以使用 Amazon EC2 Serial Console 来排查引导、网络配置和其他问题。有关说明和故障排除提示，请参阅《Amazon Elastic Compute Cloud 用户指南》中的 Amazon EC2 Serial Console。

排查硬件设备问题

以下主题介绍了您可能遇到的 Storage Gateway 硬件设备问题以及排查这些问题的建议。

您无法确定服务 IP 地址

当尝试连接到您的服务时，请确保您使用的是该服务的 IP 地址，而不是主机的 IP 地址。在服务控制台中配置服务 IP 地址，并在硬件控制台中配置主机 IP 地址。您将在启动硬件设备时看到硬件控制台。要从硬件控制台转到服务控制台，请选择 Open Service Console (打开服务控制台)。

如何执行出厂重置？

如果您需要在设备上执行出厂重置，请联系 Storage Gateway 硬件设备团队来获得支持，如后面的“支持”部分中所述。

如何执行远程重启？

如果您需要远程重启设备，可以使用 Dell iDRAC 管理界面执行此操作。有关更多信息，请参阅 Dell Technologies 网站上的 iDRac9 虚拟电源循环：远程重启 Dell EMC PowerEdge 服务器。 InfoHub

您在何处获得 Dell iDRAC 支持？

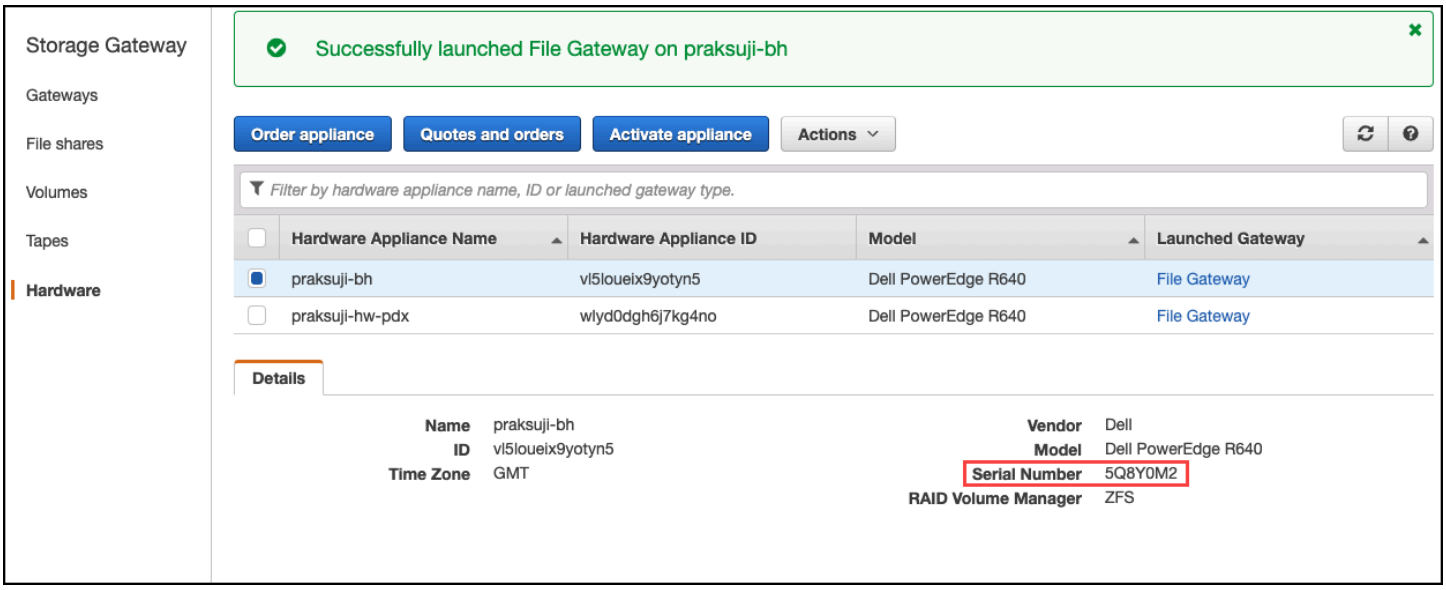
戴尔 PowerEdge R640服务器配有戴尔iDRAC管理接口。我们建议执行下列操作：

- 如果您使用 iDRAC 管理界面，则应更改默认密码。有关iDRAC凭证的更多信息，请参阅 PowerEdge 戴尔——iDRAC的默认登录凭据是什么？ 。
- 确保固件是 up-to-date 为了防止安全漏洞。
- 将 iDRAC 网络接口移动到正常的 (em) 端口可能会导致性能问题或阻止设备正常运行。

您找不到硬件设备序列号

要查找硬件设备的序列号，请转到 Storage Gateway 控制台中的硬件设备概述页面，如下所示。

Storage Gateway 控制台硬件选项卡，其中选定了设备并显示了详细信息。



Storage Gateway 控制台硬件选项卡，其中选定了设备并显示了详细信息。

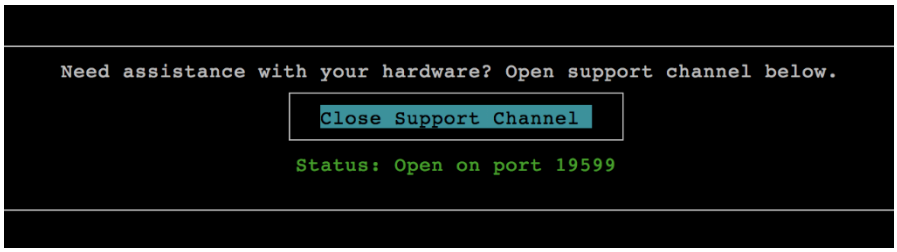
在何处获得硬件设备支持

要联系 Storage Gateway 硬件设备支持人员，请参阅AWS Support。

该 AWS Support 团队可能会要求您激活支持渠道，以远程解决您的网关问题。您无需打开此端口即可实现网关的正常操作，但在进行问题排查时需要打开。您可以从硬件控制台激活支持通道，如下面的过程所示。

要打开支持渠道 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。
   硬件设备控制台，其中显示了支持通道状态。

   硬件设备控制台，其中显示了支持通道状态。

   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. 记下端口号并将其提供给 AWS Support。

排查卷问题

您可以找到有关您使用卷时可能遇到的最典型问题以及为解决这些问题我们建议您采取的措施的信息。

主题

- 控制台显示您的卷未配置
- 控制台显示您的卷无法恢复
- 您的缓存网关无法访问，您希望恢复数据
- 控制台显示您的卷处于 PASS THROUGH 状态
- 您要验证卷的完整性并修复可能的错误
- 您的卷的 iSCSI 目标未在 Windows 磁盘管理控制台中显示
- 您要更改卷的 iSCSI 目标名称
- 您计划的卷快照未创建
- 您需要移除或更换出现故障的磁盘
- 从应用程序到卷的吞吐量降为零
- 您网关中的一个缓存磁盘遇到了故障
- 卷快照处于 PENDING 状态的时间长于预期时间
- 高可用性运行状况通知

控制台显示您的卷未配置

如果 Storage Gateway 控制台显示您的卷处于“未配置上传缓冲区”状态，请为您的网关添加上传缓冲区容量。如果网关的上传缓冲区尚未配置，您就不能用网关存储应用程序数据。有关更多信息，请参阅为网关配置额外的上传缓冲区或缓存存储。

控制台显示您的卷无法恢复

对于存储卷，如果 Storage Gateway 控制台显示您的卷处于“无法恢复”状态，则您无法再使用此卷。您可以尝试在 Storage Gateway 控制台中删除该卷。如果该卷上有数据，您可以在创建新卷时根据最初用来创建该卷的 VM 本地磁盘恢复这些数据。在创建新卷时，请选择 Preserve existing data。移除卷前，请确保删除卷的待创建快照。有关更多信息，请参阅删除快照。如果在 Storage Gateway 控制台中删除该卷不起作用，那么为该卷分配的磁盘可能已错误地从 VM 中移除，并且无法从设备中移除。

对于缓存卷，如果 Storage Gateway 控制台显示您的卷处于“无法恢复”状态，则您无法再使用此卷。如果卷上有数据，您可以创建卷的快照，然后从快照恢复数据，也可以从上一个恢复点克隆卷。您可以在恢复数据后删除卷。有关更多信息，请参阅您的缓存网关无法访问，您希望恢复数据。

对于存储卷，您可以从曾用于创建无法恢复的卷的磁盘创建新卷。有关更多信息，请参阅创建卷。有关卷状态的信息，请参阅了解卷状态和转换。

您的缓存网关无法访问，您希望恢复数据

当您的网关变得无法访问时 (例如，在您关闭网关时)，您可以选择从卷恢复点创建快照并使用该快照，也可以选择从现有卷的上一个恢复点克隆新卷。与创建快照相比，从卷恢复点进行克隆将更快且更经济高效。有关克隆卷的更多信息，请参阅克隆卷。

Storage Gateway 在缓存卷网关架构中提供各个卷的恢复点。卷的恢复点 是一个时间点，该卷在此时间点的所有数据均一致，并且您可以从该点创建快照或克隆卷。

控制台显示您的卷处于 PASS THROUGH 状态

在某些情况下，Storage Gateway 控制台可能会显示您的卷处于“传递”状态。卷可能会因若干原因处于 PASSTHROUGH 状态。对某些原因需要采取措施，而对另一些则不需要。

例如，当网关用完了上传缓冲区空间时，如果您的卷处于 PASS THROUGH 状态，则应该采取措施。要验证过去是否超过了上传缓冲区，您可以在 Amazon CloudWatch 控制台中查看该`UploadBufferPercentUsed`指标；有关更多信息，请参阅监控上传缓冲区。如果您的网关由于上传缓冲区空间用完而处于“传递”状态，则应为网关分配更多的上传缓冲区空间。添加更多缓冲区空间会自动使您的卷从“传递”转换为“正在引导”，然后再转换为“可用”。当卷处于“正在引导”状态时，网关从卷的磁盘中读取数据，将这些数据上传到 Amazon S3，然后根据需要补充数据。当网关补充完数据并将卷数据保存到 Amazon S3 后，卷状态即变为“可用”，并且可再次启动快照。请注意，当卷处于 PASS THROUGH 或 BOOTSTRAPPING 状态时，您可以继续在卷磁盘中读取和写入数据。有关添加更多上传缓冲区空间的更多信息，请参阅 确定要分配的上传缓冲区的大小。

如需在超出上传缓冲区空间前采取行动，您可以对网关的上传缓冲区设置阈值警报。有关更多信息，请参阅如需为网关的上传缓冲区设置上阈值警报。

相反，在卷处于 PASS THROUGH 状态时无需采取措施的一个示例是：该卷因为另一个卷当前正在引导中而排队等待引导。网关在同一时间自举一个卷。

PASS THROUGH 状态偶尔可能表示分配为上传缓冲区的磁盘已失效。在此情况下，您应该移除磁盘。有关更多信息，请参阅卷网关。有关卷状态的信息，请参阅了解卷状态和转换。

您要验证卷的完整性并修复可能的错误

如果您要验证卷的完整性并修复可能的错误，且您的网关使用 Microsoft Windows 启动程序连接到其卷，则可以使用 Windows CHKDSK 实用工具来验证卷的完整性并修复卷上的任何错误。Windows 在检测到卷损坏时会自动运行 CHKDSK 工具，您也可以自行运行。

您的卷的 iSCSI 目标未在 Windows 磁盘管理控制台中显示

如果您的卷的 iSCSI 目标未在 Windows 的磁盘管理控制台中显示，请检查您是否为网关配置了上传缓冲区。有关更多信息，请参阅为网关配置额外的上传缓冲区或缓存存储。

您要更改卷的 iSCSI 目标名称

如果您要更改卷的 iSCSI 目标名称，则必须移除该卷并使用新的目标名称重新添加该卷。如果这样做，您可以将数据保存在卷上。

您计划的卷快照未创建

如果您计划的卷快照未能创建，请检查您的卷是否处于 PASSTHROUGH 状态，或者网关的上传缓冲区是否在计划的快照时间之前被填满。您可以在 Amazon CloudWatch 控制台中查看网关的`UploadBufferPercentUsed`指标，并为该指标创建警报。有关更多信息，请参阅 监控上传缓冲区 和 如需为网关的上传缓冲区设置上阈值警报。

您需要移除或更换出现故障的磁盘

如果您需要更换出现故障的卷磁盘或更换不再需要的卷，则应先使用 Storage Gateway 控制台移除该卷。有关更多信息，请参阅删除卷。然后使用管理程序客户端移除备份存储：

- 对于 VMware ESXi，请按照 删除卷 中的说明移除备份存储。
- 对于 Microsoft Hyper-V，请删除支持存储。

从应用程序到卷的吞吐量降为零

如果从应用程序到卷的吞吐量降为零，请尝试以下操作：

- 如果您正在使用 VMware vSphere 客户端，请检查卷的 Host IP 地址与 Summary 选项卡上 vSphere 客户端中显示的地址之一是否匹配。您可以在 Storage Gateway 控制台中存储卷的详细信息选项卡中找到该卷的主机 IP 地址。举例而言，在您向网关分配新的静态 IP 地址的情况下，可能会发生 IP 地址的不一致情况。如果出现不一致，请从 Storage Gateway 控制台重启您的网关，如关闭网关虚

拟机中所述。重启后，存储卷的 ISCSI 目标信息选项卡中的主机 IP 地址应与网关的摘要选项卡上的 vSphere 客户端中显示的 IP 地址相匹配。

- 如果 Host IP 框中没有该卷的 IP 地址，网关处于联机状态。例如，当您创建的卷与配有两个或两个以上网络适配器的网关中某个网络适配器的 IP 地址关联时，就会出现此情况。当您移除或停用与该卷关联的网络适配器时，主机 IP 框中可能不会显示 IP 地址。要解决这一问题，请在保存现有数据的同时移除卷然后重新创建。
- 检查您的应用程序使用的 iSCSI 启动程序是否正确映射到存储卷的 iSCSI 目标。有关连接到存储卷的更多信息，请参阅 将卷连接到 Windows 客户端。

您可以从 Amazon CloudWatch 控制台查看卷的吞吐量并创建警报。有关测量应用程序到卷的吞吐量的更多信息，请参阅衡量您的应用程序和网关间的性能。。

您网关中的一个缓存磁盘遇到了故障

如果网关中的一个或多个缓存磁盘出现故障，则该网关会阻止对虚拟磁带执行读写操作。要恢复正常功能，请按如下所述重新配置网关：

- 如果缓存磁盘无法访问或不可用，请从网关配置中删除该磁盘。
- 如果缓存磁盘仍然可以访问和使用，请将其重新连接到您的网关。

> **Note**
>
> 如果删除缓存磁盘，则当网关恢复正常功能时，拥有干净数据的磁带或卷（即其缓存磁盘中的数据和 Amazon S3 中的数据已同步）将继续可用。例如，如果您的网关有三个缓存磁盘，而您删除了两个缓存磁盘，则干净的磁带或卷将处于“可用”状态。其他磁带和卷将处于“不可恢复”状态。
>
> 如果您使用临时磁盘作为网关的缓存磁盘或将缓存磁盘装载到临时驱动器，则关闭网关时缓存磁盘将丢失。在缓存磁盘和 Amazon S3 未同步时关闭网关会导致数据丢失。因此，我们不建议使用临时驱动器或磁盘。

卷快照处于 PENDING 状态的时间长于预期时间

如果卷快照保持 PENDING 状态的时间长于预期时间，则网关 VM 可能已意外崩溃，或卷的状态可能已更改为 PASS THROUGH 或 IRRECOVERABLE。如果是以上任一情况，则快照将保持 PENDING 状态且快照不会成功完成。如果出现这些情况，建议您删除快照。有关更多信息，请参阅删除快照。

当卷恢复 AVAILABLE 状态时，请为卷创建新快照。有关卷状态的信息，请参阅了解卷状态和转换。

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

- 运行状况通知
- 指标

运行状况通知

当您在 VMware vSphere HA 上运行网关时，所有网关都会向您配置的 Amazon CloudWatch 日志组生成以下运行状况通知。这些通知将转至名为 `AvailabilityMonitor` 的日志流中。

主题

- 通知：重启
- 通知： HardReboot
- 通知： HealthCheckFailure
- 通知： AvailabilityMonitorTest

通知：重启

在重新启动网关 VM 时，您会收到重启通知。您可以使用 VM 管理程序管理控制台或 Storage Gateway 控制台重新启动网关 VM。您也可以在网关维护周期内使用网关软件来重新启动。

措施

如果重启时间在网关的已配置维护开始时间的 10 分钟内，则此情况可能是正常的，并不指示任何问题。如果重启发生在维护时段之外，请检查是否已手动重新启动网关。

通知： HardReboot

当网关 VM 意外重启时，您会收到 `HardReboot` 通知。此类重启可能是因断电、硬件故障或其他事件导致的。对于 VMware 网关，通过 vSphere High Availability 应用程序监控进行重置会启动此事件。

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。

通知： HealthCheckFailure

对于 VMware vSphere HA 上的网关，当运行状况检查失败并请求重新启动 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。

通知： AvailabilityMonitorTest

对于 VMware vSphere HA 上的网关，当您在 VMware 中对可用性和应用程序监控系统运行测试时，您会收到 `AvailabilityMonitorTest` 通知。

指标

`AvailabilityNotifications` 指标适用于所有网关。此指标是网关生成的与可用性相关的运行状况通知数。使用 `Sum` 统计数据可观察网关是否遇到了任何与可用性相关的事件。有关事件的详细信息，请咨询您配置的 CloudWatch 日志组。

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 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

- 从虚拟机意外关闭中恢复
- 从故障网关或 VM 恢复您的数据
- 从不可恢复卷恢复您的数据
- 从出现故障的缓存磁盘恢复您的数据
- 从受损文件系统恢复您的数据
- 从不可访问的数据中心恢复您的数据

从虚拟机意外关闭中恢复

如果您的 VM 意外关闭，例如在停电期间，您的网关会变得不可访问。当电力和网络连接恢复后，您的网关会变得能够访问并开始正常运行。下面是此时您能够采取的有助于恢复数据的一些步骤：

- 如果断电导致网络连接问题，您可以进行对此问题进行排查。有关如何测试网络连接的信息，请参阅测试网关到 Internet 的连接。
- 对于缓存卷设置，当您的网关可供访问时，您的卷会进入“正在引导”状态。此功能可确保您本地存储的数据继续与同步 AWS。有关此状态的更多信息，请参阅了解卷状态和转换。
- 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。

从故障网关或 VM 恢复您的数据

如果您的网关或虚拟机出现故障，则可以恢复已上传到 AWS 并存储在 Amazon S3 中的卷上的数据。对于缓存卷网关，您可以从恢复快照恢复数据。对于存储卷网关，您可以从卷的最近一个 Amazon EBS 快照恢复数据。对于磁带网关，您可以将一个或多个磁带从恢复点恢复到新的磁带网关。

如果您的缓存卷网关变得不可访问，您可以采用以下步骤从恢复快照恢复您的数据：

1. 在中 AWS Management Console，选择出现故障的网关，选择要恢复的卷，然后从中创建恢复快照。
2. 部署并激活新的卷网关。或者，如果有运行正常的现有卷网关，您可以使用该网关来恢复您的卷数据。
3. 查找您创建的快照，将其还原到运行正常的网关上的新卷。
4. 将此新卷作为 iSCSI 设备安装到您的本地应用程序服务器上。

有关如何从恢复快照恢复缓存卷数据的详细信息，请参阅您的缓存网关无法访问，您希望恢复数据。

从不可恢复卷恢复您的数据

如果您卷的状态是 IRRECOVERABLE，您不再能够使用此卷。

对于存储卷，您可以使用以下步骤将数据从无法恢复的卷恢复到新卷：

1. 从您曾用于创建此不可恢复卷的磁盘创建一个新卷。
2. 当您创建新卷时，保留现有数据。
3. 删除此不可恢复卷的所有挂起快照任务。
4. 将此不可恢复卷从网关删除。

对于缓存卷，我们建议使用上一个恢复点来克隆新卷。

有关如何从无法恢复的卷将数据恢复到新卷的详细信息，请参阅控制台显示您的卷无法恢复。

从出现故障的缓存磁盘恢复您的数据

如果缓存磁盘出现故障，我们建议您根据具体情况采用以下步骤恢复数据：

- 如果故障是因将缓存磁盘从您的主机中移除导致的，则关闭网关，重新添加该磁盘，然后重新启动网关。
- 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。

从受损文件系统恢复您的数据

如果文件系统受损，您可以使用 **fsck** 命令检查文件系统是否出现错误并对其进行修复。如果可以修复文件系统，则可以从该文件系统上的卷恢复数据，如下所述：

1. 关闭您的虚拟机，然后使用 Storage Gateway 管理控制台来创建恢复快照。此快照表示存储在中的最新数据 AWS。

   > **Note**
   >
   > 如果文件系统不能修复或者快照创建过程无法成功完成，您可以将此快照作为后备。

   有关如何创建恢复快照的信息，请参阅您的缓存网关无法访问，您希望恢复数据。
2. 使用 **fsck** 命令检查文件系统是否出现错误并尝试修复。
3. 重新启动您的网关 VM。
4. 当您的管理程序主机开始启动时，按住 Shift 键进入 GRUB 启动菜单。
5. 从菜单中按 **e** 进行编辑。
6. 选择内核行（第二行），然后按 **e** 进行编辑。
7. 将以下选项附加到内核命令行：**init=/bin/bash**。使用空格分隔上一个选项与您刚附加的选项。
8. 删除两个 `console=` 行，确保删除 = 符号后面的所有值，包括用逗号分隔的值。
9. 按 **Return** 保存更改。
10. 按 **b**，使用修改的内核选项启动您的计算机。您的计算机将启动到 `bash#` 提示符。
11. 输入 **/sbin/fsck -f *dev/sda1***，从提示符处手动运行此命令，以便检查和修复您的文件系统。如果该命令与 `/dev/sda1` 路径不匹配，则可以使用 **lsblk** 来确定 / 的根文件系统设备并改用该路径。
12. 当文件系统检查和修复完成后，重新启动该实例。grub 设置将恢复为原始值，网关通常将正常启动。
13. 等待为原始网关完成拍摄快照，然后验证快照数据。

您可以继续按原样使用原始卷，也可以使用基于恢复快照或已完成的快照的新卷创建一个新网关。或者，您可以根据该卷的任何已完成快照创建一个新卷。

从不可访问的数据中心恢复您的数据

如果您的网关或数据中心出于某种原因变得无法访问，您可将数据恢复到位于不同数据中心的另一个网关或在 Amazon EC2 实例上托管的网关。如果您无权访问另一个数据中心，则建议在 Amazon EC2 实例上创建网关。您要执行的步骤取决于您要从中恢复数据的网关类型。

从不可访问的数据中心内的卷网关恢复数据

1. 在 Amazon EC2 主机上创建并激活新的卷网关。有关更多信息，请参阅部署 Amazon EC2 实例来托管卷网关。

   > **Note**
   >
   > 无法在 Amazon EC2 实例上托管网关存储卷。

2. 创建新卷并选择 EC2 网关作为目标网关。有关更多信息，请参阅创建卷。

   基于 Amazon EBS 快照创建新卷或从您要恢复的卷的上一个恢复点克隆。

   如果卷基于快照，请提供快照 ID。

   如果选择从恢复点克隆卷，请选择源卷。

其他 Storage Gateway 资源

本节介绍 AWS 可帮助您设置或管理网关的第三方软件、工具和资源，以及 Storage Gateway 配额。

主题

- 主机设置
- 卷网关
- 获取网关的激活密钥
- 连接 iSCSI 启动程序
- AWS Direct Connect 与 Storage Gateway 一起使用
- 端口要求
- 连接到网关
- 了解 Storage Gateway 资源和资源 ID
- 标记 Storage Gateway 资源
- 使用 AWS Storage Gateway的开源组件
- AWS Storage Gateway 配额

主机设置

主题

- 为 Storage Gateway 配置 VMware
- 同步您的网关 VM 时间
- 部署 Amazon EC2 实例来托管卷网关
- 使用默认设置部署 Amazon EC2
- 修改 Amazon EC2 实例元数据选项

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 VM 时间与主机时间同步
- 将 AWS Storage Gateway VM 配置为使用半虚拟化磁盘控制器
- 将 Storage Gateway 与 VMware High Availability 结合使用

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。

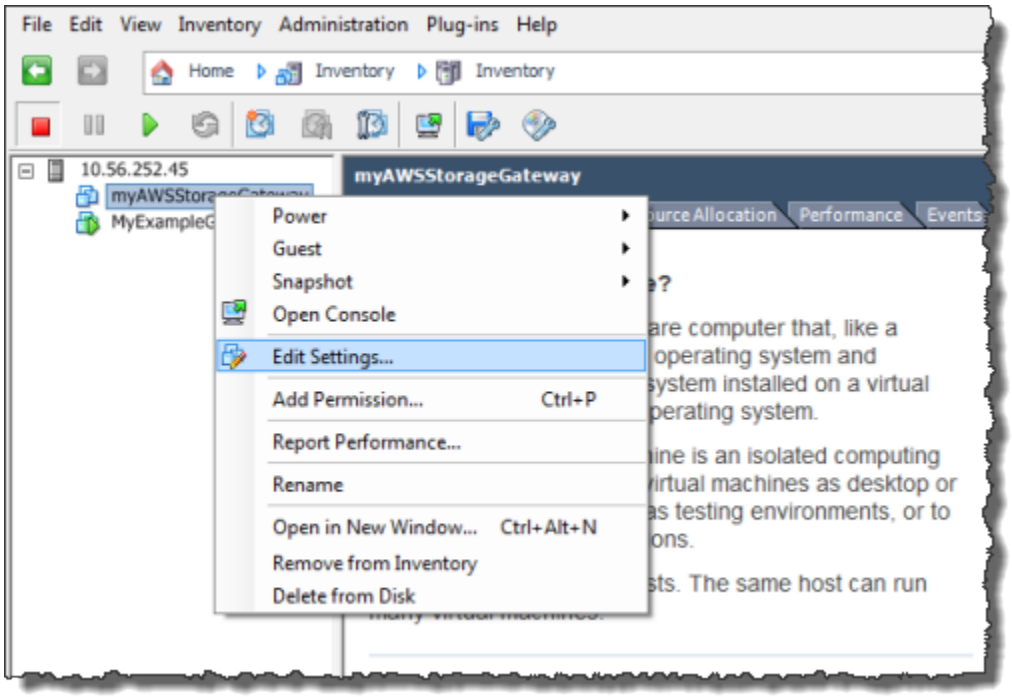
> **Important**
>
> 要成功激活网关，就需要同步 VM 时间和主机时间。

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。

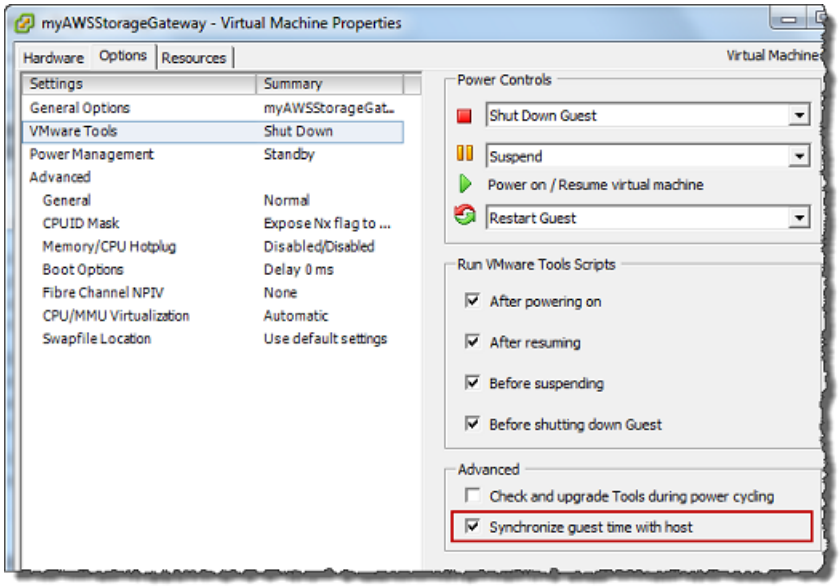
   “Virtual Machine Properties”对话框打开。



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。



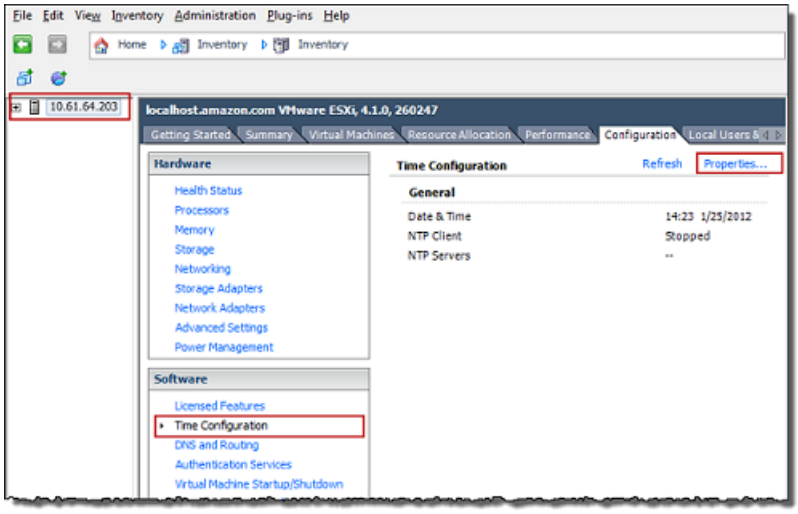
2. 配置主机时间。

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。

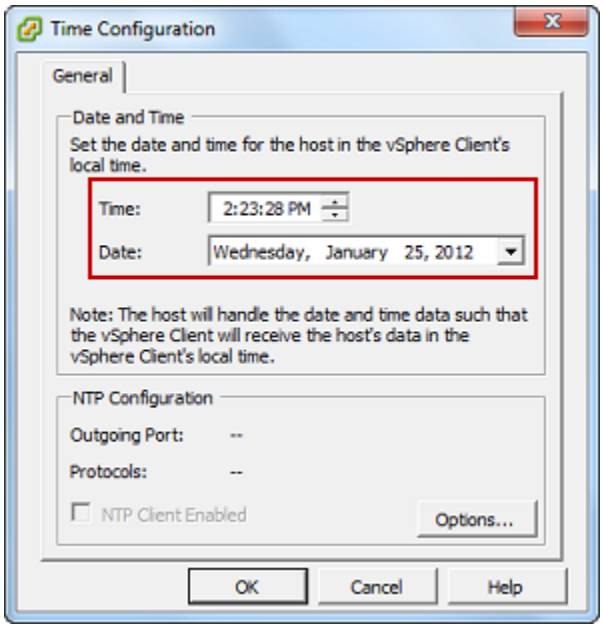
a. 在 VMware vSphere 客户端中，选择左侧窗格中的 vSphere 主机节点，然后选择 Configuration 选项卡。

b. 在软件面板中选择时间配置，然后选择属性链接。

“Time Configuration”对话框显示。

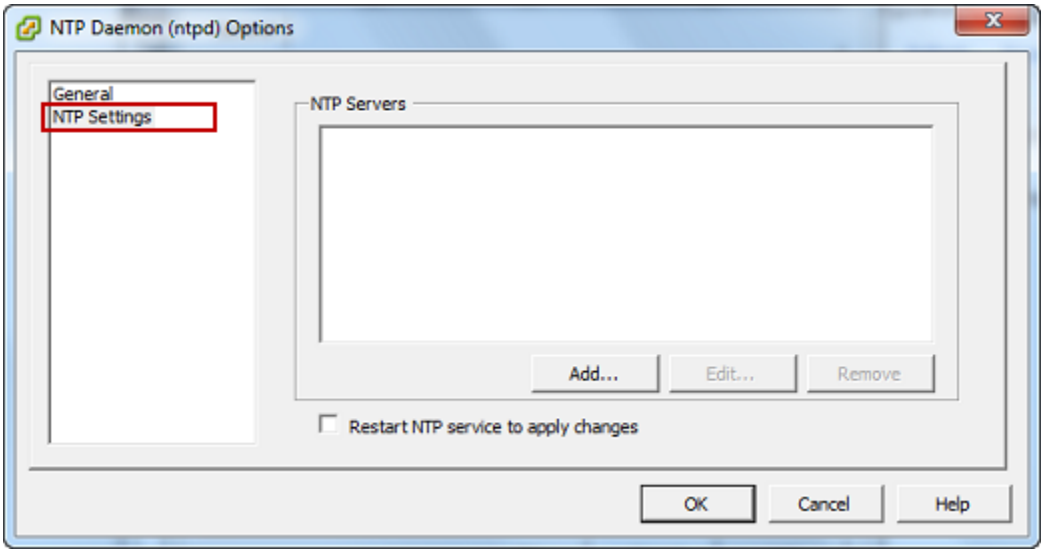


c. 在 Date and Time (日期和时间) 面板中，设置日期和时间。



d. 将主机配置为自动将其时间与 NTP 服务器同步。

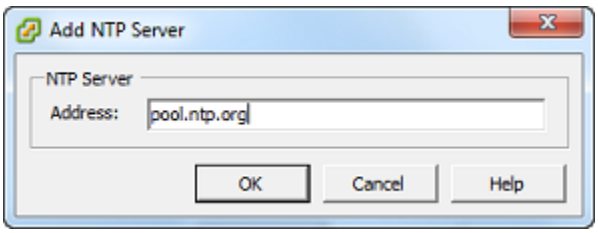
i. 在时间配置对话框中，选择选项，然后在 NTP 守护程序 (ntpd) 选项对话框中，选择左侧窗格中的 NTP 设置。



ii. 选择 Add 以添加新 NTP 服务器。

iii. 在 Add NTP Server 对话框中，键入 NTP 服务器的 IP 地址或完全限定域名，然后选择 OK。

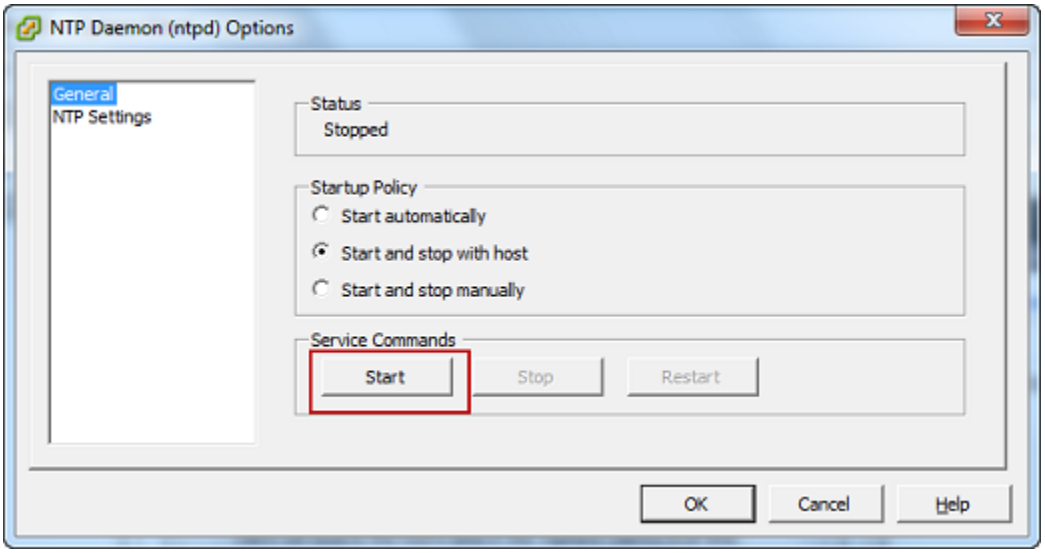
您可使用 `pool.ntp.org`，如以下示例所示。



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。

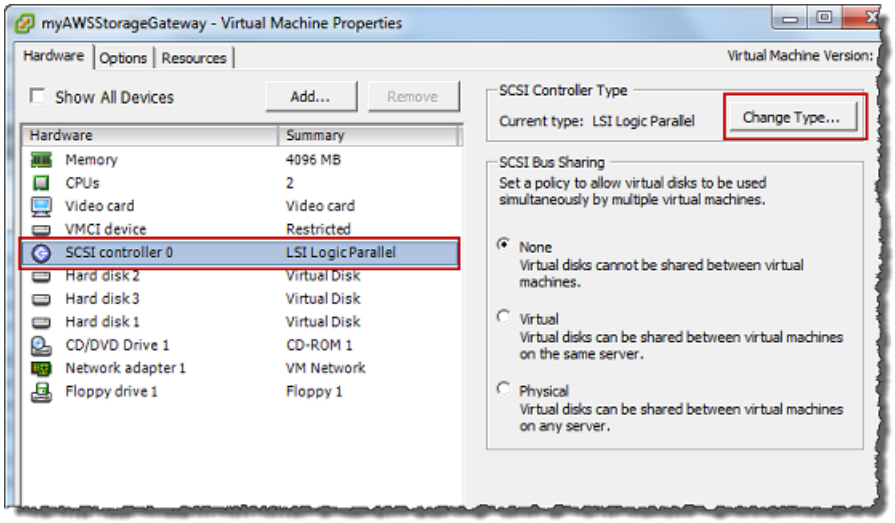
将 AWS Storage Gateway VM 配置为使用半虚拟化磁盘控制器

在此任务中，您将设置 iSCSI 控制器以便让 VM 使用半虚拟化。半虚拟化 是一种模式，在此模式下，网关 VM 使用主机操作系统来让控制台标识您添加到 VM 的虚拟磁盘。

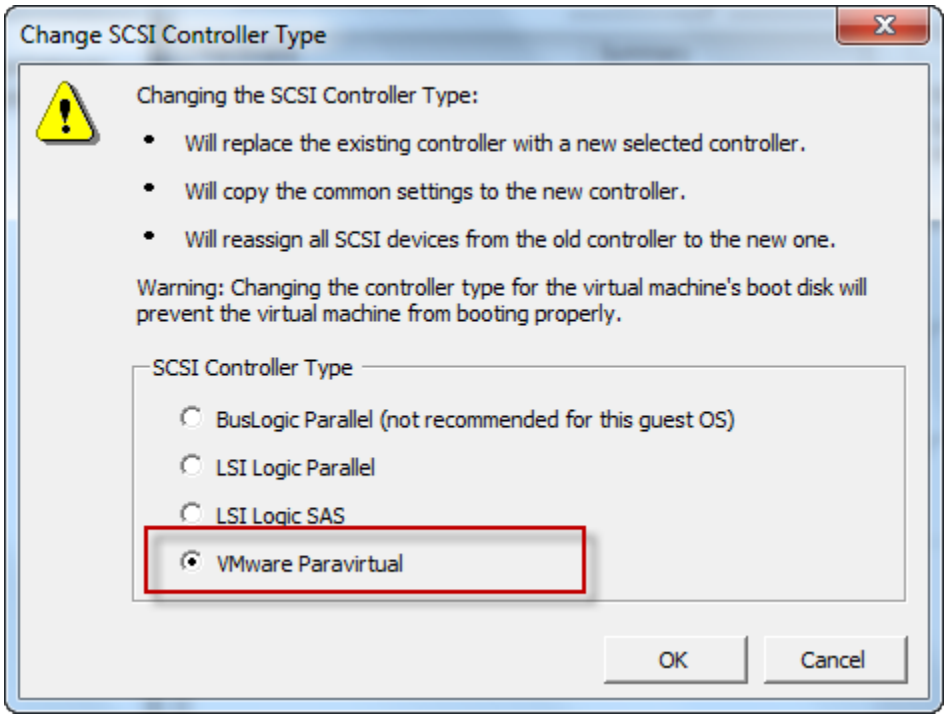
> **Note**
>
> 您必须完成此步骤才能避免在网关控制台中配置这些磁盘时出现磁盘标识问题。

如需将 VM 配置为使用半虚拟化的控制器

1. 在 VMware 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。
2. 在 Virtual Machine Properties 对话框中，选择 Hardware 选项卡，再选择 SCSI controller 0，然后选择 Change Type。



3. 在 Change SCSI Controller Type 对话框中，选择 VMware Paravirtual SCSI 控制器类型，然后选择 OK。



将 Storage Gateway 与 VMware High Availability 结合使用

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 网站上的 VMware HA：概念和最佳实践。

若要将 Storage Gateway 与 VMware HA 一起使用，建议执行下列操作：

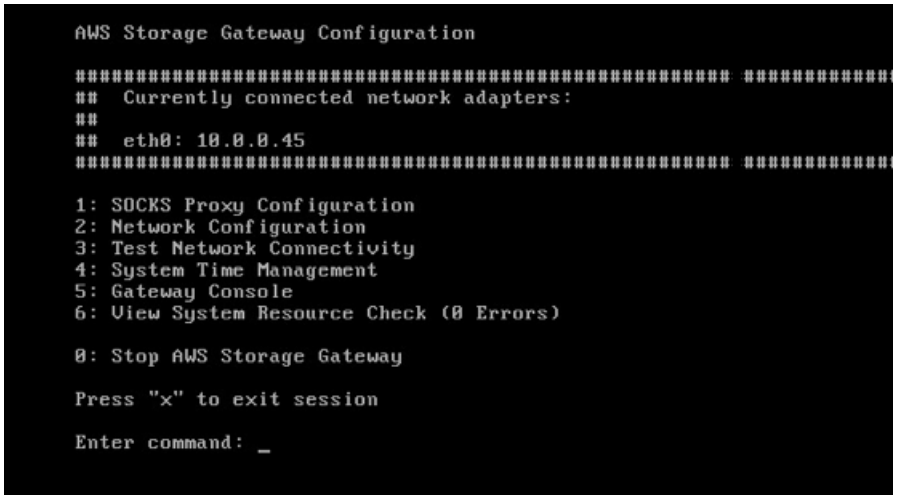
- 仅在集群中的一台主机上部署包含 Storage Gateway VM 的 VMware ESX `.ova` 可下载程序包。
- 在部署 `.ova` 程序包时，选择一个不在主机本地的数据存储。而是使用一个可供群集的所有主机访问的数据存储。如果您选择的是主机本地数据存储，而主机发生了故障，则群集中的其他主机可能无法访问该数据源，并且可能无法成功地故障转移到另一台主机。
- 要防止启动程序在故障转移期间与存储卷目标断开连接，请遵循针对您的操作系统建议的 iSCSI 设置。在故障转移事件中，网关 VM 在故障转移群集中的新主机中启动时，需要花费几秒钟到几分钟的时间。Windows 和 Linux 客户端的建议 iSCSI 超时超过了完成故障转移通常所需的时间。有关自定义 Windows 客户端的超时设置的更多信息，请参阅 自定义您的 Windows iSCSI 设置。有关自定义 Linux 客户端的超时设置的更多信息，请参阅 自定义您的 Linux iSCSI 设置。
- 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

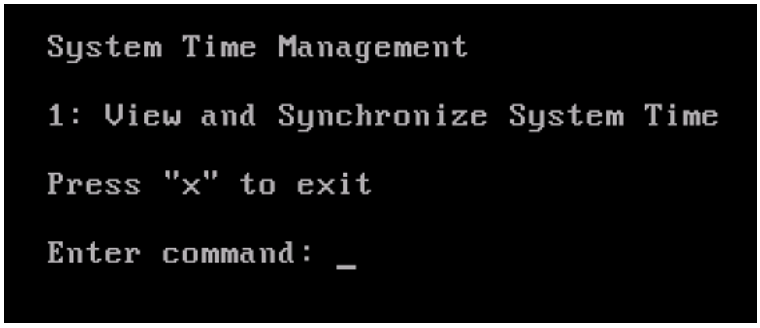
对于 VMware ESXi 上部署的网关，设置管理程序主机时间并将 VM 时间与主机同步，就足以避免时间偏差。有关更多信息，请参阅将 VM 时间与主机时间同步。对于 Microsoft Hyper-V 上部署的网关，您应该定期使用下面介绍的步骤查看 VM 的时间。

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 Storage Gateway 配置主菜单上，为系统时间管理输入 **4**。



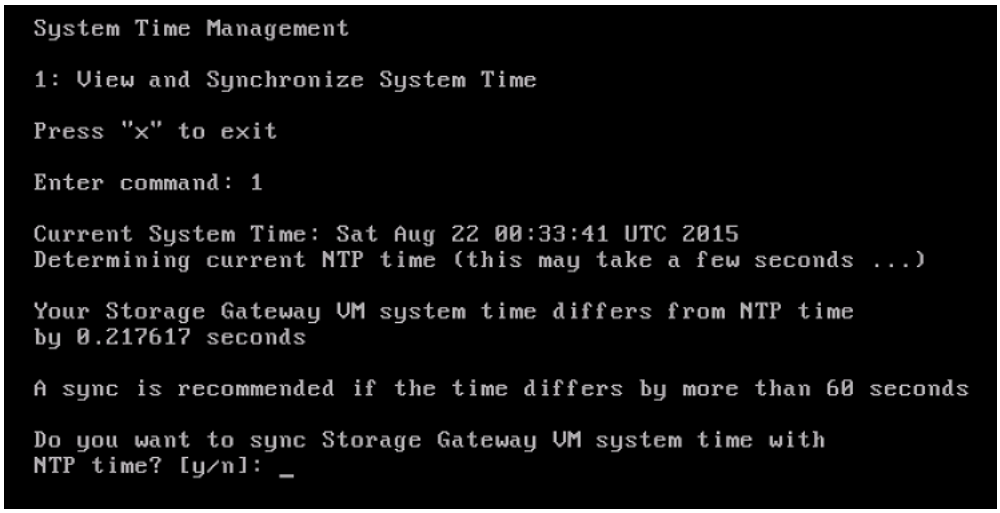
3. 在系统时间管理菜单上，为查看和同步系统时间输入 **1**。



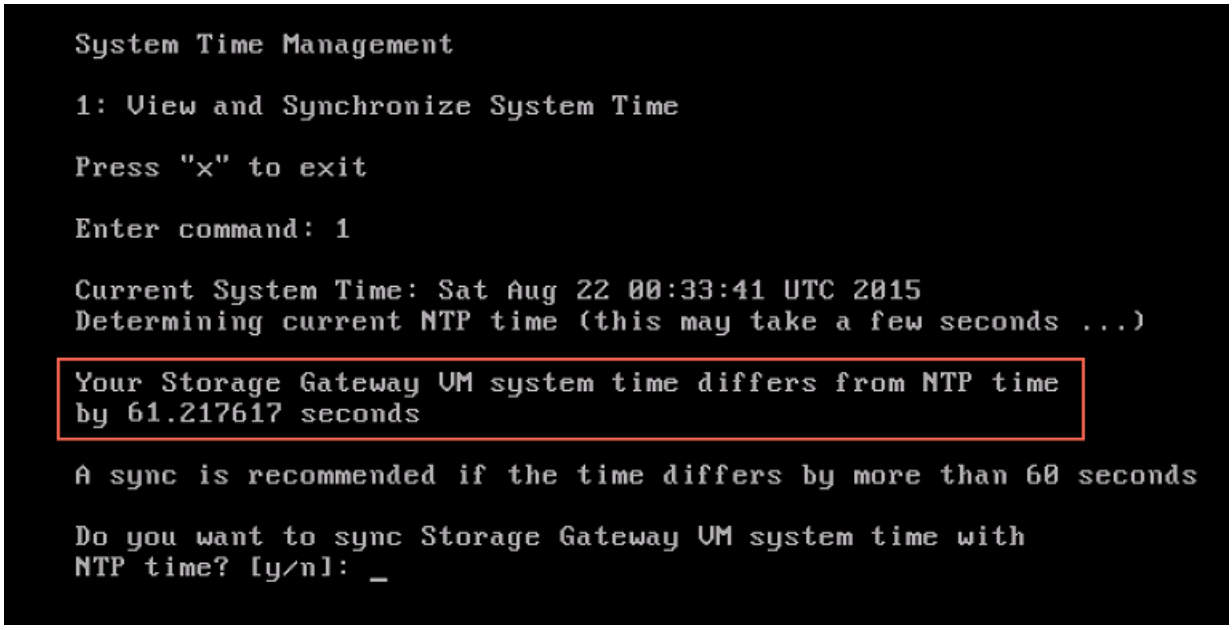
4. 如果结果指示您应该将 VM 的时间与 NTP 时间同步，请输入 **y**。否则，请输入 **n**。

   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。



部署 Amazon EC2 实例来托管卷网关

您可以在 Amazon Elastic Compute Cloud (Amazon EC2) 实例上部署和激活卷网关。 AWS Storage Gateway Amazon 系统映像 (AMI) 以社区 AMI 形式提供。

> **Note**
>
> AWS已发布并完全支持 Storage Gateway 社区 AMI。你可以看到发布者是一个 AWS经过验证的提供商。
> 卷网关 AMI 使用以下命名约定。AMI 名称中附加的版本号会随着每个版本的发布而变化。
> `aws-storage-gateway-CLASSIC-2.9.0`

部署 Amazon EC2 实例来托管卷网关

1. 开始使用 Storage Gateway 控制台来设置新的网关。有关说明，请参阅设置卷网关。当您进入平台选项部分时，选择 Amazon EC2 作为主机平台，然后按照以下步骤启动将托管您的卷网关的 Amazon EC2 实例。

> **Note**
>
> Amazon EC2 主机平台仅支持缓存卷。存储卷网关不能部署在 EC2 实例上。

2. 选择启动实例，在 Amazon EC2 控制台中打开 AWS Storage Gateway AMI 模板，您可以在其中配置其他设置。

   使用 Quicklaunch 来启动具有默认设置的 Amazon EC2 实例。有关 Amazon EC2 Quicklaunch 默认规格的更多信息，请参阅 。Amazon EC2 的 Quicklaunch 配置规范。

3. 在名称中，为 Amazon EC2 实例输入一个名称。实例部署完成后，您可以搜索此名称，在 Amazon EC2 控制台的列表页面上找到您的实例。

4. 在实例类型部分的实例类型列表中，为您的实例选择硬件配置。硬件配置必须满足某些最低要求才能支持您的网关。我们建议您首先使用 m5.xlarge 实例类型，它满足网关正常运行所需的最低硬件要求。有关更多信息，请参阅 对 Amazon EC2 实例类型的要求。

   如果需要，您可以在启动后调整实例的大小。有关更多信息，请参阅 Amazon EC2 用户指南中的调整实例大小。

   > **Note**
   >
   > 某些实例类型，尤其是 i3 EC2，使用的是 NVMe SSD 磁盘。这可能会在您启动或停止卷网关时导致出现问题；例如，您可能会丢失缓存中的数据。监控 `CachePercentDirty` Amazon CloudWatch 指标，只有在该参数为时才启动或停止系统`0`。要了解有关网关监控指标的更多信息，请参阅 CloudWatch 文档中的 Storage Gateway 指标和维度。

5. 在密钥对(登录) 部分的密钥对名称 -必需中，选择要用于安全连接到实例的密钥对。如有必要，您可以创建新的密钥对。有关更多信息，请参阅《适用于 Linux 实例的 Amazon Elastic Compute Cloud 用户指南》中的创建密钥对。

6. 在网络设置部分，检查预配置的设置并选择编辑来更改以下字段：

   a. 对于 VPC - 必需，请选择要在其中启动 Amazon EC2 实例的 VPC。有关 Amazon VPC 的更多信息，请参阅《Amazon Virtual Private Cloud 用户指南》中的 Amazon VPC 的工作原理。

   b. （可选）对于子网，请选择要在其中启动 Amazon EC2 实例的子网。

   c. 对于自动分配公有 IP，选择启用。

7. 在防火墙（安全组）子部分中，查看预配置的设置。如果您愿意，可以更改要为您的 Amazon EC2 实例创建的新安全组的默认名称和描述，也可以选择应用现有安全组中的防火墙规则。

8. 在入站安全组规则子部分中，添加防火墙规则来打开客户端用于连接实例的端口。有关卷网关所需端口的更多信息，请参阅端口要求。有关添加防火墙规则的更多信息，请参阅《适用于 Linux 实例的 Amazon Elastic Compute Cloud 用户指南》中的安全组规则。

   > **Note**
   >
   > 卷网关要求在网关激活期间为入站流量和一次性 HTTP 访问打开 TCP 端口 80。激活后，您可以关闭此端口。
   > 此外，您必须打开 TCP 端口 3260 才能访问 iSCSI。

9. 在高级网络配置子部分中，检查预配置的设置，必要时进行更改。
10. 在配置存储部分，选择添加新卷，将存储添加到网关实例。

    > **Important**
    >
    > 除了预配置的根卷外，您还必须至少添加一个容量至少为 165 GiB 的 Amazon EBS 卷作为缓存存储，并至少添加一个容量至少为 150 GiB 的 Amazon EBS 卷作为上传缓冲区。为了提高性能，我们建议分配多个 EBS 卷作为缓存存储，每个卷至少为 150 GiB。

11. 在高级详细信息部分，检查预配置的设置，必要时进行更改。
12. 选择启动实例，使用已配置的设置启动您的新 Amazon EC2 网关实例。
13. 要确认您的新实例可成功启动，请导航至 Amazon EC2 控制台中的实例页面，然后按名称搜索您的新实例。确保实例状态显示为正在运行且带有绿色复选标记，并确保状态检查已完成且显示绿色复选标记。
14. 从详细信息页面中选择您的实例。从实例摘要部分复制公有 IPv4 地址，然后返回 Storage Gateway 控制台中的设置网关页面，继续设置您的卷网关。

您可以使用 Storage Gateway 控制台或查询 AWS Systems Manager 参数存储来确定用于启动卷网关的 AMI ID。

要确定 AMI ID，请执行以下任一操作：

- 开始使用 Storage Gateway 控制台来设置新的网关。有关说明，请参阅设置卷网关。当您进入平台选项部分时，选择 Amazon EC2 作为主机平台，然后选择启动实例以在 Amazon EC2 控制台中打开 AWS Storage Gateway AMI 模板。

  您将被重定向到 EC2 社区 AMI 页面，您可以在网址中看到您所在 AWS 地区的 AMI ID。

- 查询 Systems Manager 参数存储。您可以使用 AWS CLI 或 Storage Gateway API 查询缓存卷网关或存储卷网关命名空间`/aws/service/storagegateway/ami/CACHED/latest`下的 Systems Manager 公共参数。`/aws/service/storagegateway/ami/STORED/latest`例如，使用以下 CLI 命令返回 AWS 区域 您指定的当前 AMI 的 ID。

```
aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/
STORED/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/
STORED/latest",
        "Name": "/aws/service/storagegateway/ami/STORED/latest",
        "Value": "ami-123c45dd67d891000"
    }
}
```

使用默认设置部署 Amazon EC2

本主题列出了使用默认规格部署 Amazon EC2 主机的步骤。

您可以在 Amazon Elastic Compute Cloud (Amazon EC2) 实例上部署和激活卷网关。 AWS Storage Gateway Amazon 系统映像 (AMI) 以社区 AMI 形式提供。

> **Note**
>
> AWS已发布并完全支持 Storage Gateway 社区 AMI。你可以看到发布者是一个 AWS经过验证的提供商。

1. 要设置 Amazon EC2 实例，请在工作流的平台选项部分中选择 Amazon EC2 作为主机平台。有关配置 Amazon EC2 实例的说明，请参阅部署 Amazon EC2 实例来托管卷网关。
2. 选择 “启动实例”，在 Amazon EC2 控制台中打开 AWS Storage Gateway AMI 模板并自定义其他设置，例如实例类型、网络设置和配置存储。

3. 或者，您可以在 Storage Gateway 控制台中选择使用默认设置，使用默认配置来部署 Amazon EC2 实例。

   使用默认设置创建的 Amazon EC2 实例具有以下默认规格：

   - 实例类型 - m5.xlarge
   - 网络设置
     - 对于 VPC，选择要在其中运行 EC2 实例的 VPC。
     - 对于子网，指定要在其中启动 EC2 实例的子网。

     > **Note**
     >
     > 只有在 VPC 管理控制台中为 VPC 子网激活了自动分配公有 IPv4 地址设置后，VPC 子网才会出现在下拉列表中。

     - 自动分配公有 IP – 已激活

   已创建 EC2 安全组并与 EC2 实例关联。安全组具有以下入站端口规则：

   > **Note**
   >
   > 在网关激活期间，您需要打开端口 80。在激活后立即关闭该端口。此后，只能通过选定 VPC 中的其他端口来访问您的 EC2 实例。
   > 只能通过与网关位于同一 VPC 中的主机来访问网关上的 iSCSI 目标。如果需要从 VPC 之外的主机访问 iSCSI 目标，则应更新相应的安全组规则。
   > 您可以随时编辑安全组，方法是导航到 Amazon EC2 实例详细信息页面，选择安全，导航到安全组详细信息并选择安全组 ID。

端口	协议	文件系统协议				
80	TCP	用于激活的 HTTP 访问权限				
3260	TCP	iSCSI				

- 配置存储

默认设置	AMI 根卷	卷 2 缓存	卷 3 缓存			
设备名称		'/dev/sdb'	'/dev/sdc'			
大小	80 GiB	165 GiB	150 GiB			
卷类型	gp3	gp3	gp3			
IOPS	3000	3000	3000			
终止时删除	支持	是	支持			
已加密	不支持	否	不支持			
吞吐量	125	125	125			

修改 Amazon EC2 实例元数据选项

实例元数据服务 (IMDS) 是一个实例组件，可提供对 Amazon EC2 实例元数据的安全访问。可以将实例配置为接受使用 IMDS 版本 1 (imdsv1) 或要求所有元数据请求都使用 IMDS 版本 2 (imdsv2) 的传入元数据请求。IMDSv2 使用面向会话的请求，并防范了多种类型的漏洞，这些漏洞可用于尝试访问 IMDS。有关 imdsv2 的信息，请参阅亚马逊弹性计算云用户指南中的实例元数据服务版本 2 的工作原理。

我们建议托管 Storage Gateway 的所有亚马逊 EC2 实例都需要 imdsv2。默认情况下，所有新启动的网关实例都需要 IMDSv2。如果您的现有实例仍配置为接受 imdsv1 元数据请求，请参阅亚马逊弹性计算云用户指南中的要求使用 imdsv2，了解修改实例元数据选项以要求使用 imdsv2 的说明。应用此更改不需要重启实例。

卷网关

主题

- 从网关中移除磁盘
- 为在 Amazon EC2 上托管的网关添加和删除 Amazon EBS 卷

从网关中移除磁盘

尽管我们不建议您从网关中移除底层磁盘，但您可能希望从网关中移除磁盘，例如，当您有发生故障的磁盘时。

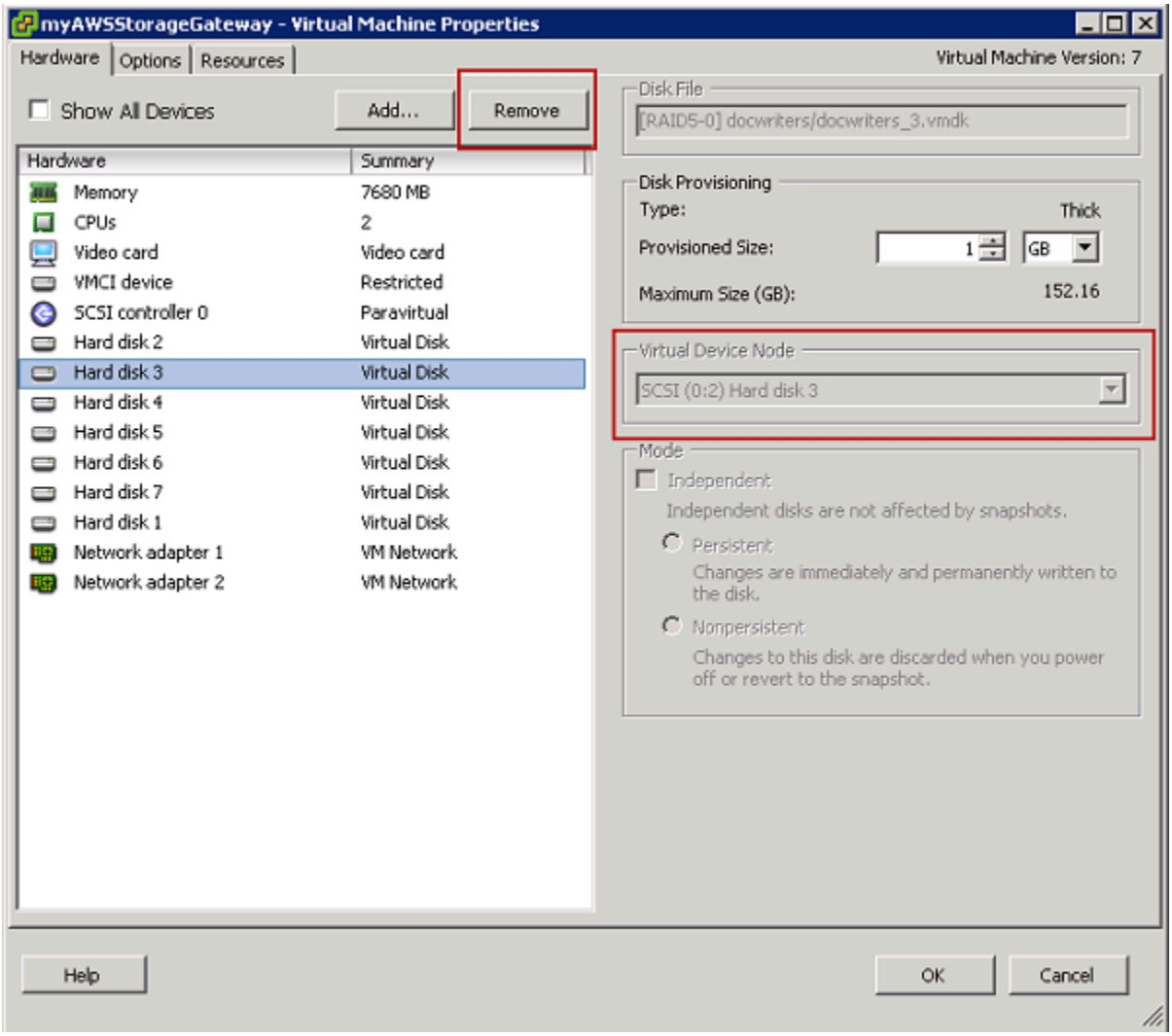
从托管于 VMware ESXi 上的网关中移除磁盘

您可以使用以下过程从托管于 VMware 管理程序上的网关中移除磁盘。

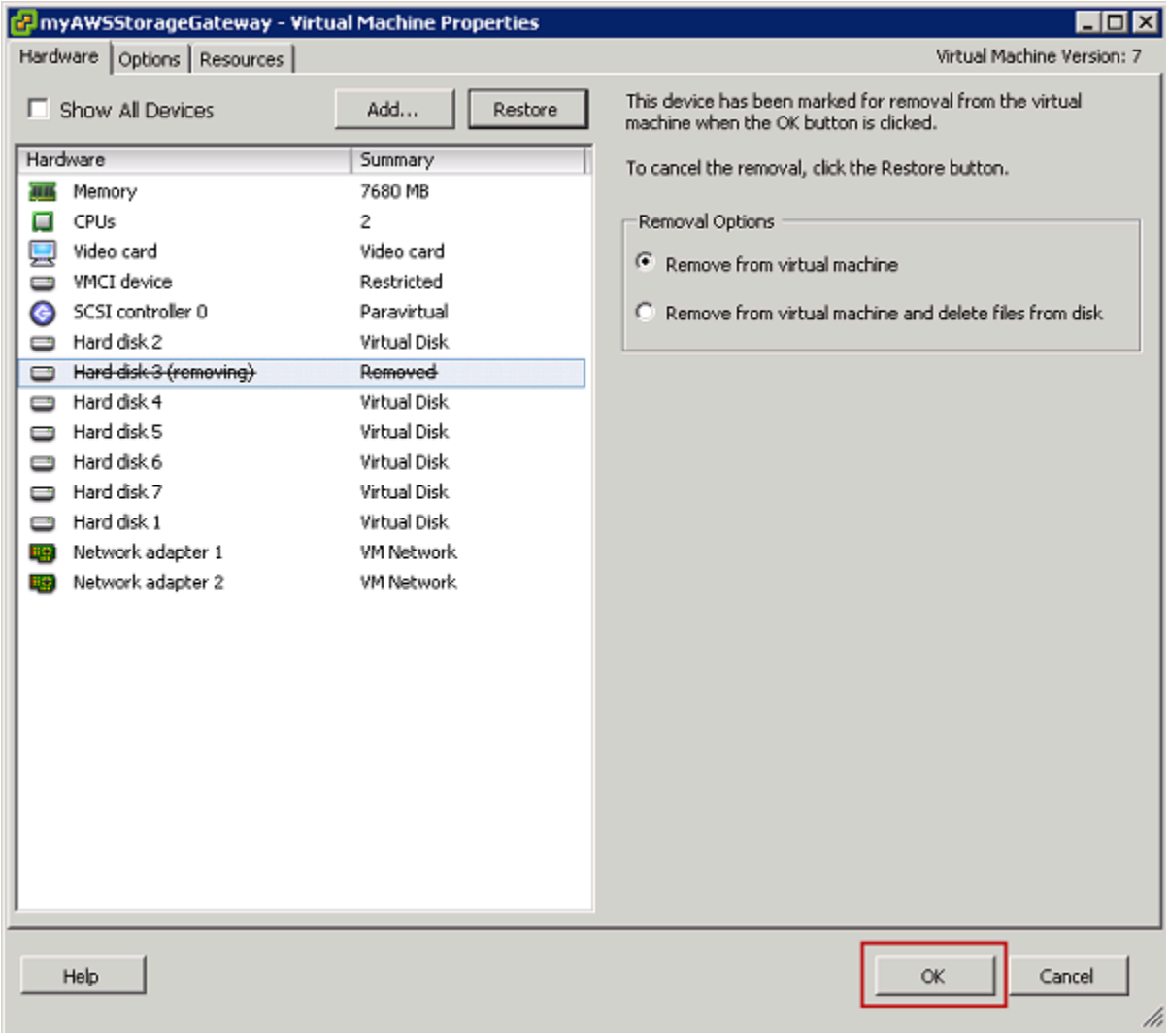
移除为上传缓冲区分配的磁盘 (VMware ESXi)

1. 在 vSphere 客户端中，打开上下文 (右键单击) 菜单，选择网关 VM 的名称，然后选择 Edit Settings。
2. 在虚拟机属性对话框的硬件选项卡上，选择分配为上传缓冲区空间的磁盘，然后选择移除。

   确认虚拟机属性对话框中的虚拟设备节点值与之前记下的值相同。这样做可帮助确保移除正确的磁盘。



3. 在 Removal Options 面板中选择一个选项，然后选择 OK 以完成移除磁盘的过程。



从托管于 Microsoft Hyper-V 上的网关中移除磁盘

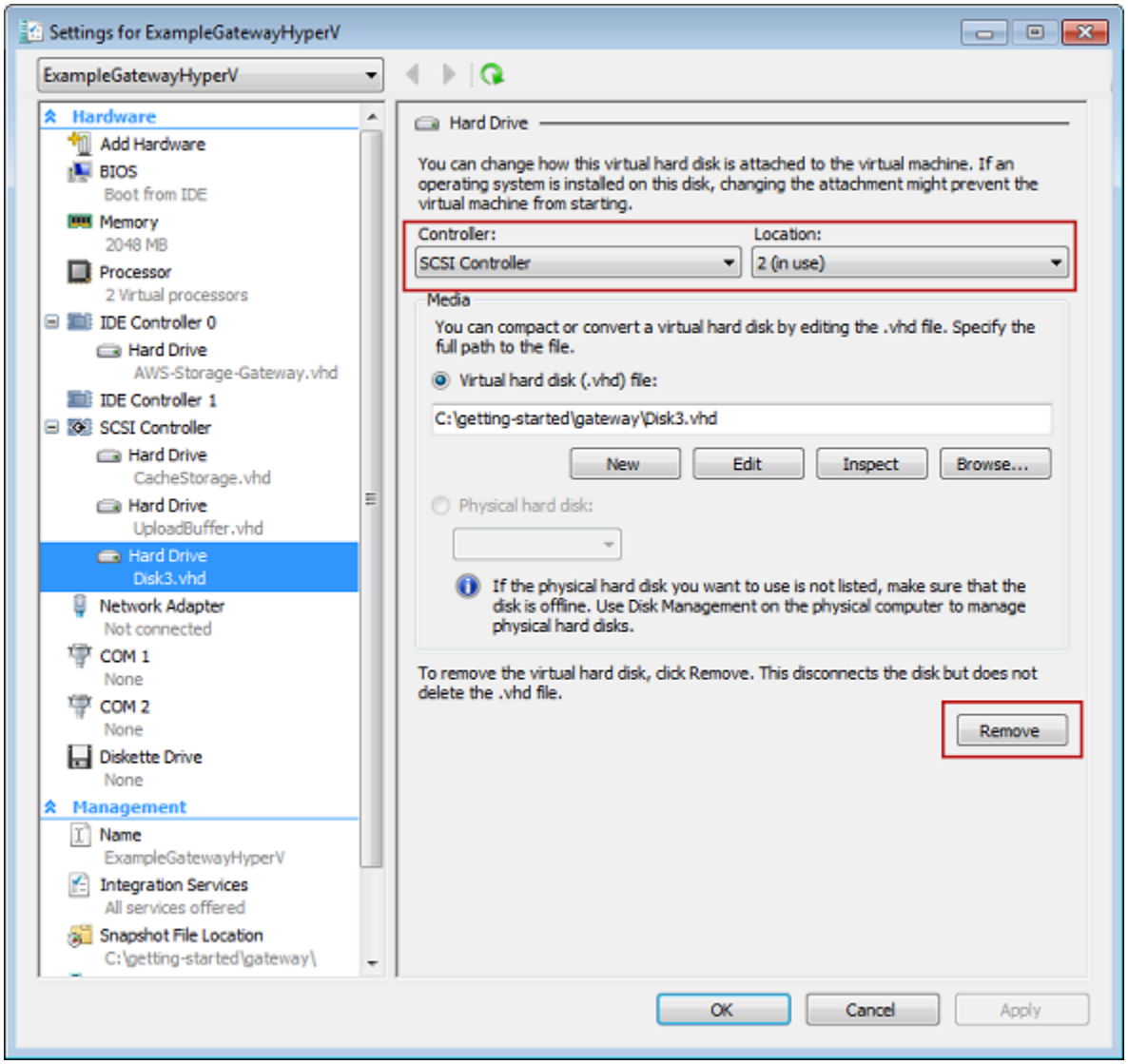
利用以下过程，您可以从托管于 Microsoft Hyper-V 管理程序上的网关中移除磁盘。

移除为上传缓冲区分配的底层磁盘 (Microsoft Hyper-V)

1. 在 Microsoft Hyper-V Manager 中，打开上下文 (右键单击) 菜单，选择网关 VM 的名称，然后选择 Settings。
2. 在设置对话框的硬件列表中，选择要移除的磁盘，然后选择移除。

   添加到网关的磁盘显示在硬件列表的 SCSI 控制器条目下面。确认 Controller (控制器) 和 Location (位置) 值与之前记录的值相同。这样做可帮助确保移除正确的磁盘。

   在 Microsoft Hyper-V Manager 中显示的第一个 SCSI Controller 是控制器 0。



3. 选择 OK 以应用更改。

从托管于 Linux KVM 上的网关中移除磁盘

要将磁盘从基于 Linux 内核的虚拟机 (KVM) 管理程序上托管的网关分离，可以使用类似于以下命令的 `virsh` 命令。

```
$ virsh detach-disk domain_name /device/path
```

有关管理 KVM 磁盘的更多详细信息，请参阅 Linux 发行版的文档。

为在 Amazon EC2 上托管的网关添加和删除 Amazon EBS 卷

在最初将网关配置为以 Amazon EC2 实例形式运行时，您分配了 Amazon EBS 卷来用作上传缓冲区和缓存存储。由于应用程序需求会随着时间发生变化，因此可分配额外的 Amazon EBS 卷来达到此目的。还可通过删除以前分配的 Amazon EBS 卷来减少已分配的存储。有关亚马逊 EBS 的更多信息，请参阅亚马逊 EC2 用户指南中的亚马逊 Elastic Block Store (Amazon EBS)。

在向网关添加更多存储之前，应检查如何根据网关的应用程序需求调整上传缓冲区和缓存存储的大小。为此，请参阅确定要分配的上传缓冲区的大小和确定要分配的缓存存储的大小。

可分配为上传缓冲区和缓存存储的最大存储存在配额。可向实例附加所需数量的 Amazon EBS 卷，但是，将这些卷配置为上传缓冲区和缓存存储空间时必须遵守这些存储配额。有关更多信息，请参阅 AWS Storage Gateway 配额。

添加 Amazon EBS 卷并为网关配置该卷

1. 创建 Amazon EBS 卷。有关说明，请参阅 Amazon EC2 用户指南中的创建或恢复 Amazon EBS 卷。
2. 将 Amazon EBS 卷挂载到您的 Amazon EC2 实例。有关说明，请参阅 Amazon EC2 用户指南中的将 Amazon EBS 卷附加到实例。
3. 将添加的 Amazon EBS 卷配置为上传缓冲区或缓存存储。有关说明，请参阅管理 Storage Gateway 的本地磁盘。

有时，可能会发现为上传缓冲区分配的存储量大于需要的存储量。

删除 Amazon EBS 卷

> **Warning**
>
> 这些步骤仅适用于分配为上传缓冲区空间的 Amazon EBS 卷，不适用于分配为缓存的卷。

1. 通过按照关闭网关虚拟机一节中介绍的方法操作，关闭网关。
2. 将 Amazon EBS 卷与 Amazon EC2 实例分离。有关说明，请参阅 Amazon EC2 用户指南中的将 Amazon EBS 卷与实例分离。
3. 删除 Amazon EBS 卷。有关说明，请参阅亚马逊 EC2 用户指南中的删除 Amazon EBS 卷。
4. 通过按照关闭网关虚拟机一节中介绍的方法操作，启动网关。

获取网关的激活密钥

要接收网关的激活密钥，请向网关虚拟机 (VM) 发出 Web 请求。VM 返回包含激活密钥的重定向，激活密钥作为 `ActivateGateway` API 操作的参数之一传递，用于指定网关的配置。有关更多信息，请参阅 Storage Gateway API 参考ActivateGateway中的。

> **Note**
>
> 如果未使用，网关激活密钥将在 30 分钟后过期。

您向网关 VM 发出的请求包括激活发生的 AWS 区域。响应中重定向返回的 URL 包含称为 `activationkey` 的查询字符串参数。此查询字符串参数是您的激活密钥。此查询字符串的格式如下所示：`http://`*`gateway_ip_address`*`/?activationRegion=`*`activation_region`*。此查询的输出会返回激活区域和密钥。

URL 还包括 `vpcEndpoint`，即使用 VPC 端点类型连接的网关的 VPC 端点 ID。

> **Note**
>
> Storage Gateway 硬件设备、VM 映像模板和 Amazon EC2 Amazon 系统映像 (AMI) 已预先配置了接收和响应本页所述 Web 请求所需的 HTTP 服务。不要求也不建议在网关上安装任何其他服务。

主题

- Linux (curl)
- Linux (bash/zsh)
- 微软 Windows PowerShell
- 使用本地控制台

Linux (curl)

以下示例向您显示如何使用 Linux (curl) 获取激活密钥。

> **Note**
>
> 将突出显示的变量替换为您的网关的实际值。可接受的值如下所示：

- *gateway_ip_address* - 您的网关的 IPv4 地址，例如 172.31.29.201
- *gateway_t* ype-要激活的网关类型，例如、STORED、CACHEDVTL、FILE_S3或。FILE_FSX_SMB
- *region_code* - 要在其中激活网关的区域。请参阅《AWS 一般参考指南》中的区域端点。如果未指定此参数，或者提供的值拼写错误或与有效区域不匹配，则该命令将默认为该区域。us-east-1
- *vpc_endpoint* - 您的网关的 VPC 端点名称，例如 vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com。

要获取公有端点的激活密钥，请执行以下操作：

```
curl "http://gateway_ip_address/?activationRegion=region_code&no_redirect"
```

要获取 VPC 端点的激活密钥，请执行以下操作：

```
curl "http://gateway_ip_address/?
activationRegion=region_code&vpcEndpoint=vpc_endpoint&no_redirect"
```

Linux (bash/zsh)

以下示例显示如何使用 Linux (bash/zsh) 获取 HTTP 响应、分析 HTTP 标头以及获取激活密钥。

```
function get-activation-key() {
  local ip_address=$1
  local activation_region=$2
  if [[ -z "$ip_address" || -z "$activation_region" || -z "$gateway_type" ]]; then
    echo "Usage: get-activation-key ip_address activation_region gateway_type"
    return 1
  fi

  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region&gatewayType=$gateway_type"); then
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
    echo "$activation_key_param" | cut -f2 -d=
  else
```

```
    return 1
  fi
}
```

微软 Windows PowerShell

以下示例向您展示了如何使用 Microsoft Windows PowerShell 获取 HTTP 响应、解析 HTTP 标头和获取激活密钥。

```
function Get-ActivationKey {
  [CmdletBinding()]
  Param(
    [parameter(Mandatory=$true)][string]$IpAddress,
    [parameter(Mandatory=$true)][string]$ActivationRegion,
    [parameter(Mandatory=$true)][string]$GatewayType
  )
  PROCESS {
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion&gatewayType=$GatewayType" -MaximumRedirection 0 -
ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

使用本地控制台

以下示例显示了如何使用本地控制台来生成和显示激活密钥。

从本地控制台获取网关的激活密钥

1. 登录到本地控制台。如果要从 Windows 计算机连接到 Amazon EC2 实例，请以 admin 身份登录。
2. 登录并查看 AWS 设备激活 - 配置主菜单后，选择 0 来选择获取激活密钥。
3. 选择 Storage Gateway 作为网关系列选项。
4. 出现提示时，输入要激活网关的 AWS 区域。
5. 对于公有端点，输入 1，或对于 VPC 端点，输入 2 作为网络类型。

6. 对于标准端点，输入 1，或对于美国联邦信息处理标准 (FIPS) 端点，输入 2 作为端点类型。

连接 iSCSI 启动程序

在管理网关时，您将使用作为 Internet 小型计算机系统接口 (iSCSI) 目标公开的卷或虚拟磁带库 (VTL) 设备。对于卷网关，iSCSI 目标是卷。对于磁带网关，目标为 VTL 设备。作为此工作的一部分，您将执行以下任务：连接到这些目标、自定义 iSCSI 设置、从 Red Hat Linux 客户端进行连接以及配置质询握手身份验证协议 (CHAP)。

主题

- 将卷连接到 Windows 客户端
- 将卷或 VTL 设备连接到 Linux 客户端
- 自定义 iSCSI 设置
- 为 iSCSI 目标配置 CHAP 身份验证

iSCSI 标准是一种基于互联网协议 (IP) 的存储网络标准，该标准用于启动和管理基于 IP 的存储设备与客户端之间的连接。以下列表定义了用来描述 iSCSI 连接和相关组件的一些术语。

iSCSI 启动程序

iSCSI 网络的客户端组件。启动程序向 iSCSI 目标发送请求。可以在软件或硬件中实施启动程序。Storage Gateway 仅支持软件启动程序。

iSCSI 目标

iSCSI 网络的服务器组件，接收并响应来自启动程序的请求。每个卷均作为一个 iSCSI 目标公开。仅对每个 iSCSI 目标连接一个 iSCSI 启动程序。

Microsoft iSCSI 启动程序

Microsoft Windows 计算机上的软件程序，让您可以将客户端计算机（即运行您希望将其数据写入网关的应用程序的计算机）连接到基于 iSCSI 的外部阵列（即网关）。使用主机的以太网网络适配卡建立此连接。Microsoft iSCSI 启动程序在 Windows 8.1、Windows 10、Windows Server 2012 R2、Windows Server 2016 和 Windows Server 2019 上已经通过验证，可以与 Storage Gateway 一起使用。启动程序内置在这些操作系统中。

Red Hat iSCSI 启动程序

`iscsi-initiator-utils` 资源包管理器 (RPM) 程序包为您提供了在适用于 Red Hat Linux 的软件中实施的 iSCSI 启动程序。该包含有用于 iSCSI 协议的服务器守护进程。

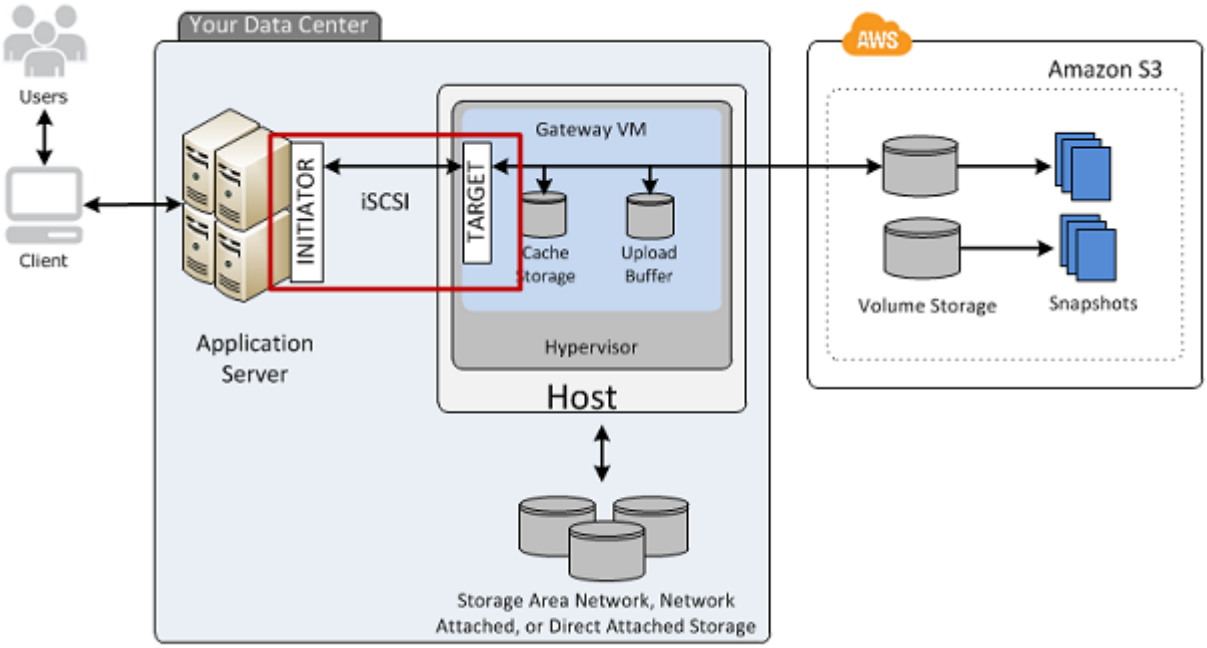
每种类型的网关都可以连接到 iSCSI 设备，而您可以自定义这些连接，如下所述。

将卷连接到 Windows 客户端

卷网关将您为网关创建的卷作为 iSCSI 目标公开。有关更多信息，请参阅将卷连接到客户端。

> **Note**
>
> 要连接到卷目标，您的网关必须已配置了上传缓冲区。如果没有为网关配置上传缓冲区，那么您的卷的状态就会显示为 UPLOAD BUFFER NOT CONFIGURED。要在存储卷设置中为网关配置上传缓冲区，请参阅为网关配置额外的上传缓冲区或缓存存储。要在缓存卷设置中为网关配置上传缓冲区，请参阅为网关配置额外的上传缓冲区或缓存存储。

下图在 Storage Gateway 架构的大图中突出显示了 iSCSI 目标。有关更多信息，请参阅卷网关的工作原理（架构）。



您可以从 Windows 或 Red Hat Linux 客户端连接到卷。您可以为任一客户端类型配置 CHAP。

您的网关使用您指定的名称将您的卷作为 iSCSI 目标公开，名称前加 `iqn.1997-05.com.amazon:`。例如，如果您指定 `myvolume` 的目标名称，那么您用来连接到卷的 iSCSI 目标就是 `iqn.1997-05.com.amazon:myvolume`。有关如何配置您的应用程序以便在 iSCSI 上安装卷的更多信息，请参阅 将卷连接到 Windows 客户端。

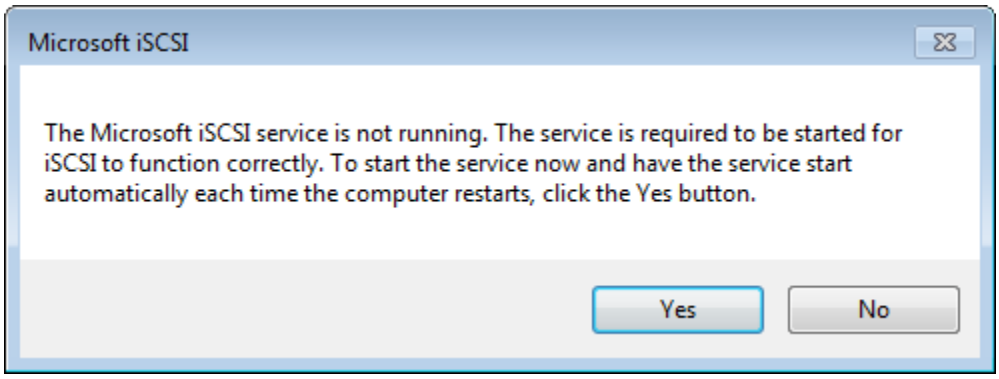
目的	参见
从 Windows 连接到您的卷。	连接到 Microsoft Windows 客户端
从 Red Hat Linux 连接到您的卷。	连接到 Red Hat Enterprise Linux 客户端
为 Windows 和 Red Hat Linux 配置 CHAP 身份验证。	为 iSCSI 目标配置 CHAP 身份验证

将 Windows 客户端连接到存储卷

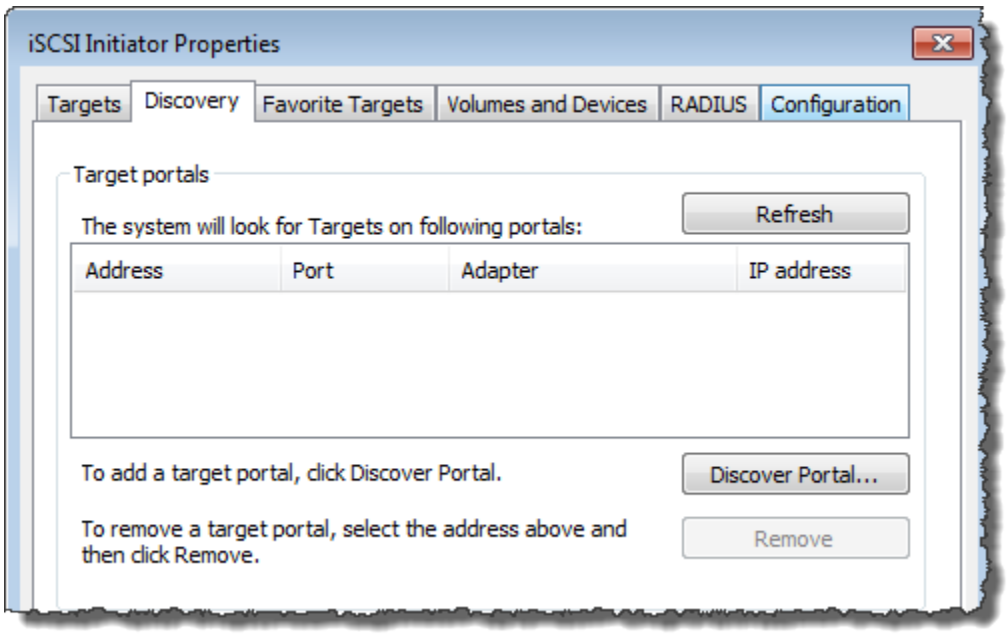
1. 在 Windows 客户端计算机的开始菜单上，在搜索程序和文件框中输入 **`iscsicpl.exe`**，找到 iSCSI 启动程序，然后运行它。

   > **Note**
   >
   > 必须具有客户端计算机上的管理员权限才能运行 iSCSI 启动程序。

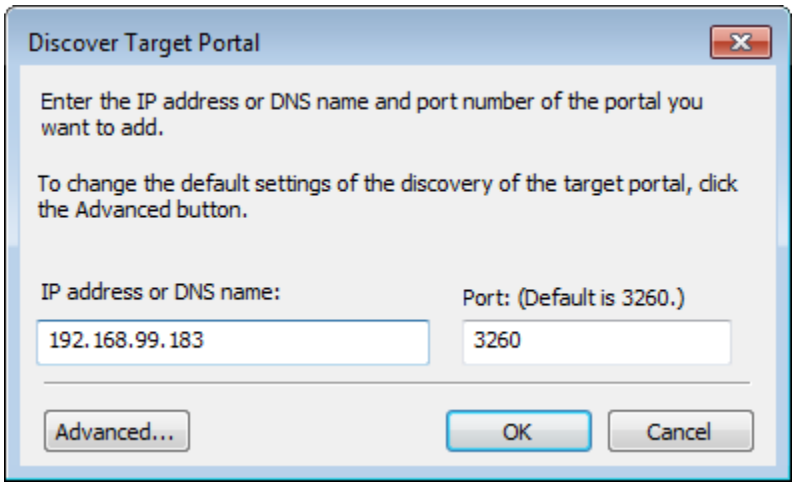
2. 如果出现提示，则单击 Yes 以启动 Microsoft iSCSI 启动程序服务。



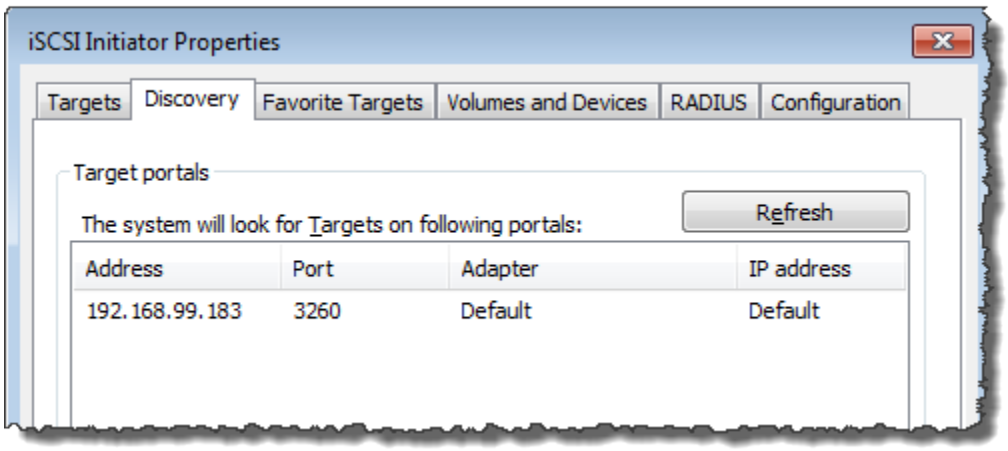
3. 在 iSCSI Initiator Properties (iSCSI 发起程序属性) 对话框中，选择 Discovery (发现) 选项卡，然后选择 Discover Portal (发现门户)。



4. 在发现目标门户对话框中，在 IP 地址或 DNS 名称中输入 iSCSI 目标的 IP 地址，然后选择确定。要获取网关的 IP 地址，请查看 Storage Gateway 控制台上的网关选项卡。如果您在 Amazon EC2 实例上部署了网关，则可以在 Amazon EC2 控制台的描述选项卡中找到公有 IP 或 DNS 地址。



现在，发现选项卡上的目标门户列表中会显示 IP 地址。



> **Warning**
>
> 对于部署于 Amazon EC2 实例上的网关，不支持通过公有 Internet 连接来访问该网关。无法使用 Amazon EC2 实例的弹性 IP 地址作为目标地址。

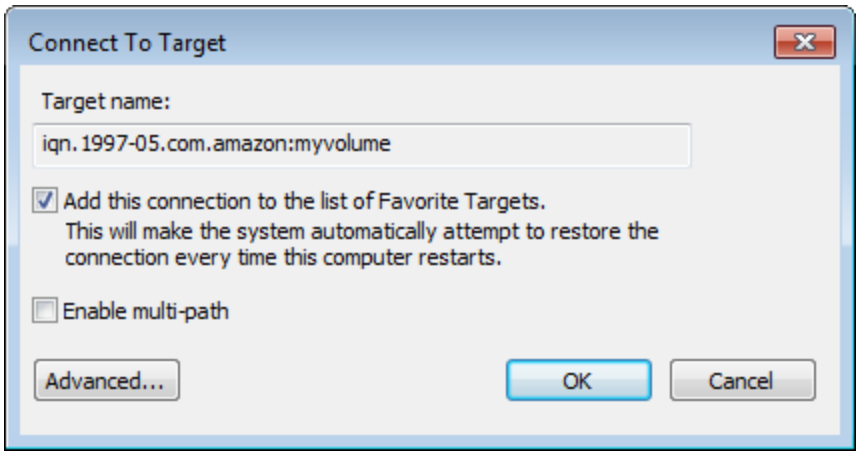
5. 将新的目标门户连接到网关上的存储卷目标：

   a. 选择目标选项卡。

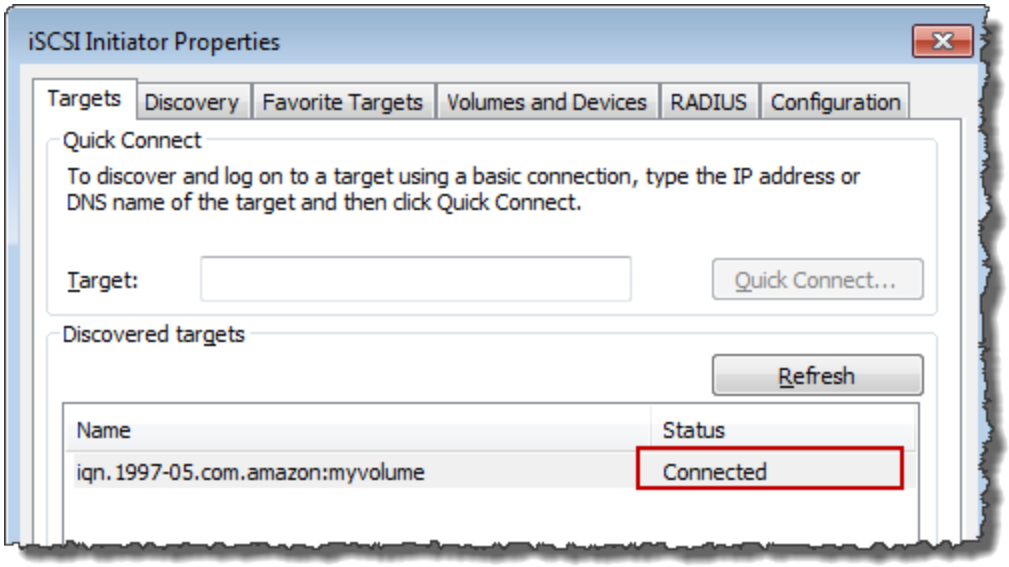
      新目标门户显示未激活状态。显示的目标名称应该与您在步骤 1 中为存储卷指定的名称相同。

   b. 选择该目标，然后选择 Connect。

如果尚未填入目标名称，请按照步骤 1 中所示输入目标名称。在连接到目标对话框中，选择将此连接添加到常用目标列表，然后选择确定。



c. 在目标选项卡中，确保目标状态的值为已连接（表示已连接目标），然后单击确定。



您现在可以为 Windows 初始化并格式化该存储卷，以便开始在卷中保存数据。您可以使用 Windows 磁盘管理工具执行此操作。

> **Note**
>
> 尽管对于本练习并非必需，但我们仍强烈建议您在真实使用某应用程序时自定义 iSCSI 设置，如自定义您的 Windows iSCSI 设置中所述。

将卷或 VTL 设备连接到 Linux 客户端

使用 Red Hat Enterprise Linux (RHEL) 时，应使用 `iscsi-initiator-utils` RPM 程序包连接到网关 iSCSI 目标（卷或 VTL 设备）。

将 Linux 客户端连接到 iSCSI 目标

1. 如果尚未在您的客户端上安装 `iscsi-initiator-utils` RPM 程序包，请安装程序包。

   您可以使用下面的命令来安装该包。

   ```
   sudo yum install iscsi-initiator-utils
   ```

2. 确保 iSCSI 守护进程正在运行。

   a. 使用下以下命令之一验证 iSCSI 守护进程是否正在运行。

      对于 RHEL 5 或 RHEL 6，请使用以下命令。

      ```
      sudo /etc/init.d/iscsi status
      ```

      对于 RHEL 7，请使用以下命令。

      ```
      sudo service iscsid status
      ```

   b. 如果 status 命令未返回 running 状态，则使用以下命令之一启动守护程序。

      对于 RHEL 5 或 RHEL 6，请使用以下命令。

      ```
      sudo /etc/init.d/iscsi start
      ```

      对于 RHEL 7，请使用以下命令。对于 RHEL 7，您通常不需要显式启动 `iscsid` 服务。

      ```
      sudo service iscsid start
      ```

3. 要发现为网关定义的卷目标或 VTL 设备目标，请使用以下发现命令。

   ```
   sudo /sbin/iscsiadm --mode discovery --type sendtargets --portal [GATEWAY_IP]:3260
   ```

用您网关的 IP 替代上一命令中的 *[GATEWAY_IP]* 变量。您可以在 Storage Gateway 控制台上某个卷的 iSCSI 目标信息属性中找到网关 IP。

发现命令的输出内容类似如下示例输出内容。

对于卷网关：*[GATEWAY_IP]*:3260, 1 iqn.1997-05.com.amazon:myvolume

对于磁带网关：iqn.1997-05.com.amazon:*[GATEWAY_IP]*-tapedrive-01

您的 iSCSI 限定名称 (IQN) 与以上所示不同，因为每个组织的 IQN 值不同。目标名称是您创建卷时指定的名称。在 Storage Gateway 控制台上选择某个卷时，也可以在 iSCSI 目标信息属性窗格中找到此目标名称。

4. 要连接到目标，请使用以下命令。

请注意，您需要在连接命令中指定正确的 *[GATEWAY_IP]* 和 IQN。

> **Warning**
>
> 对于部署于 Amazon EC2 实例上的网关，不支持通过公有 Internet 连接来访问该网关。无法使用 Amazon EC2 实例的弹性 IP 地址作为目标地址。

```
sudo /sbin/iscsiadm --mode node --targetname
 iqn.1997-05.com.amazon:[ISCSI_TARGET_NAME] --portal [GATEWAY_IP]:3260,1 --login
```

5. 要确认卷已附加到客户端 (启动程序)，请使用以下命令。

```
ls -l /dev/disk/by-path
```

命令的输出如下面的示例输出所示。

```
lrwxrwxrwx. 1 root root 9 Apr 16 19:31 ip-[GATEWAY_IP]:3260-iscsi-
iqn.1997-05.com.amazon:myvolume-lun-0 -> ../../sda
```

设置启动程序后，我们强烈建议您按自定义您的 Linux iSCSI 设置中介绍的方式自定义 iSCSI 设置。

自定义 iSCSI 设置

我们强烈建议您在设置启动程序后，自定义 iSCSI 设置以防止启动程序从目标断开。

通过增大下列步骤中所示的 iSCSI 超时值，您可以提高应用程序对需要较长时间的写入操作以及网络中断等其他瞬态问题的处理能力。

> **Note**
>
> 修改注册表前，您应该制作一份该注册表的备份副本。有关制作备份副本的信息以及使用注册表时应遵循的其他最佳做法，请参阅 Microsoft TechNet 库中的注册表最佳做法。

主题

- 自定义您的 Windows iSCSI 设置
- 自定义您的 Linux iSCSI 设置
- 为卷网关自定义 Linux 磁盘超时设置

自定义您的 Windows iSCSI 设置

使用 Windows 客户端时，用 Microsoft iSCSI 启动程序连接到您的网关卷。有关如何连接到卷的说明，请参阅将卷连接到客户端。

1. 将您的磁带网关设备连接到 Windows 客户端。
2. 如果要使用备份应用程序，则将该应用程序配置为使用这些设备。

如需自定义您的 Windows iSCSI 设置

1. 提高请求排队的最长时间。

   a. 启动注册表编辑器 (`Regedit.exe`)。

   b. 导航到设备类别的全局唯一标识符 (GUID) 密钥，其中包含 iSCSI 控制器设置，如下所示。

> **Warning**
>
> 确保您使用的是CurrentControlSet子键而不是其他控件集，例如 00 ControlSet1 或 ControlSet00 2。

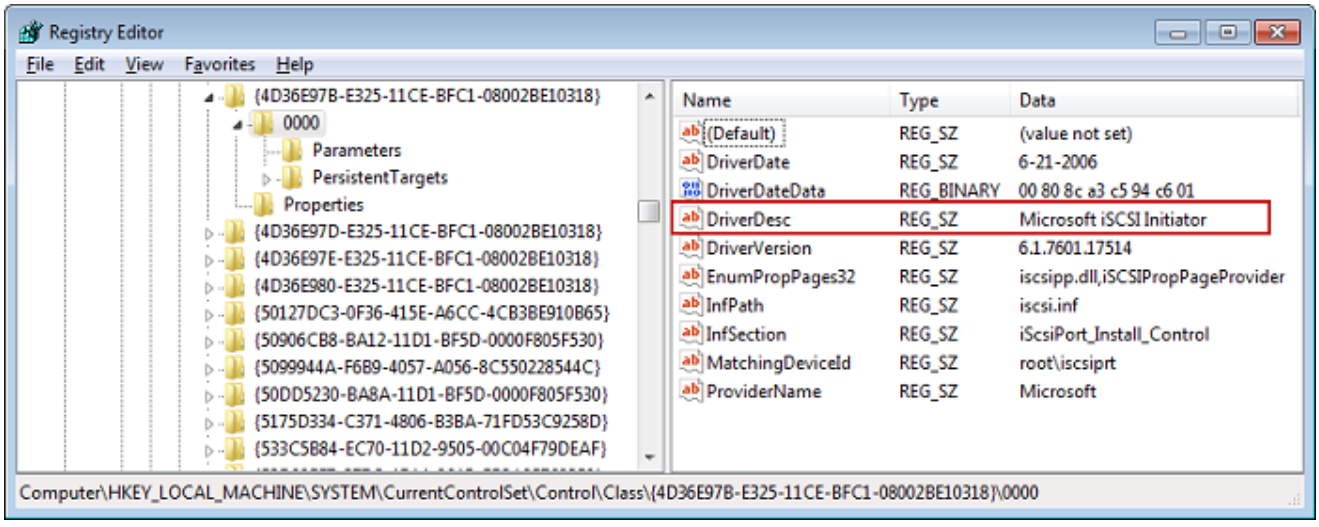
```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}
```

c. 查找 Microsoft iSCSI 启动程序的子项，在下面显示为 *[<####]*。

该项由四位数字表示，如 `0000`。

```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\[<Instance Number]
```

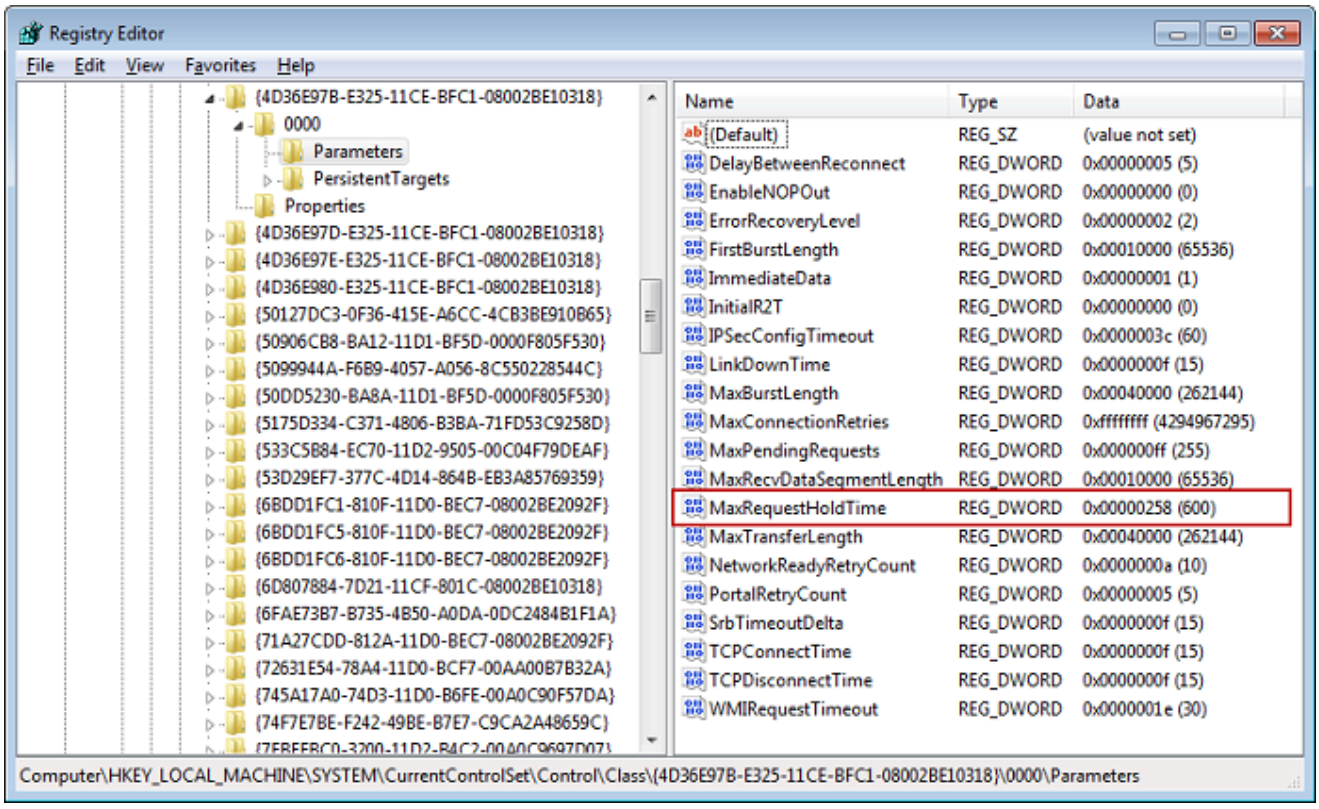
根据计算机上安装的内容，Microsoft iSCSI 启动程序可能不是子项 `0000`。可通过验证字符串 `DriverDesc` 是否具有以下示例所示的 `Microsoft iSCSI Initiator` 值来确保选择了纠正的子项。



d. 要显示 iSCSI 设置，请选择 Parameters (参数) 子项。

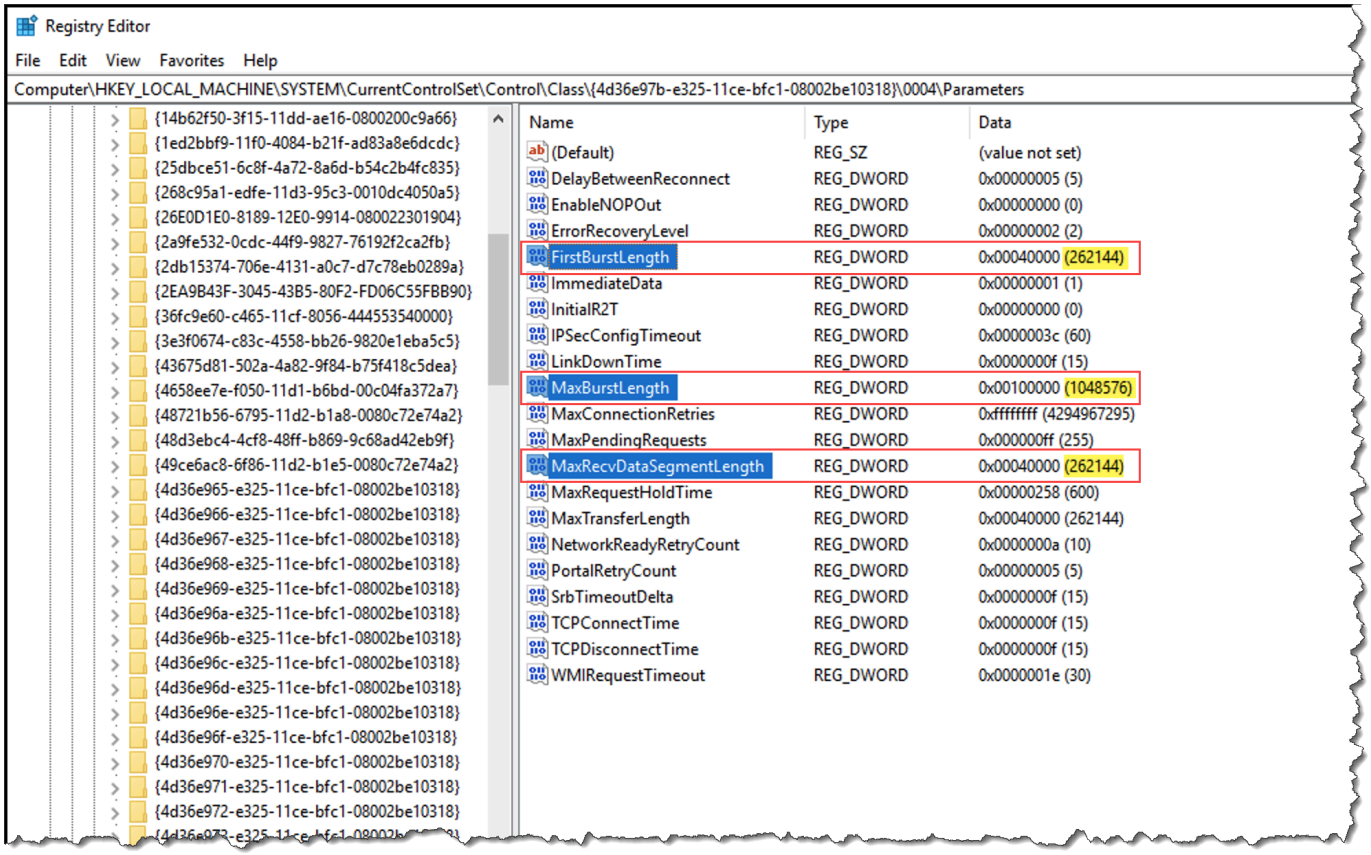
e. 打开 MaxRequestHoldTimeDWORD（32 位）值的上下文（右键单击）菜单，选择 “修改”，然后将该值更改为。**`600`**

MaxRequestHoldTime指定在通知上层事件之前，Microsoft iSCSI 启动器应保留多长时间并重试未完成的命令。`Device Removal`此值表示 600 秒的保持时间，如以下示例所示。



2. 通过修改以下参数，可以提高可在 iSCSI 数据包中发送的最大数据量：

   - FirstBurstLength控制在未经请求的写入请求中可以传输的最大数据量。将此值设置为 **262144** 或 Windows 操作系统的默认值，以较高者为准。
   - MaxBurstLength类似于 FirstBurstLength，但它设置了在请求的写入序列中可以传输的最大数据量。将此值设置为 **1048576** 或 Windows 操作系统的默认值，以较高者为准。
   - MaxRecvDataSegmentLength控制与单个协议数据单元 (PDU) 关联的最大数据段大小。将此值设置为 **262144** 或 Windows 操作系统的默认值，以较高者为准。



> **Note**
>
> 不同的备份软件可使用不同的 iSCSI 设置进行优化来达到最佳效果。要确认如何设置这些参数的值才能提供最佳性能，请参阅备份软件的文档。

3. 增大磁盘超时值，如下所示：

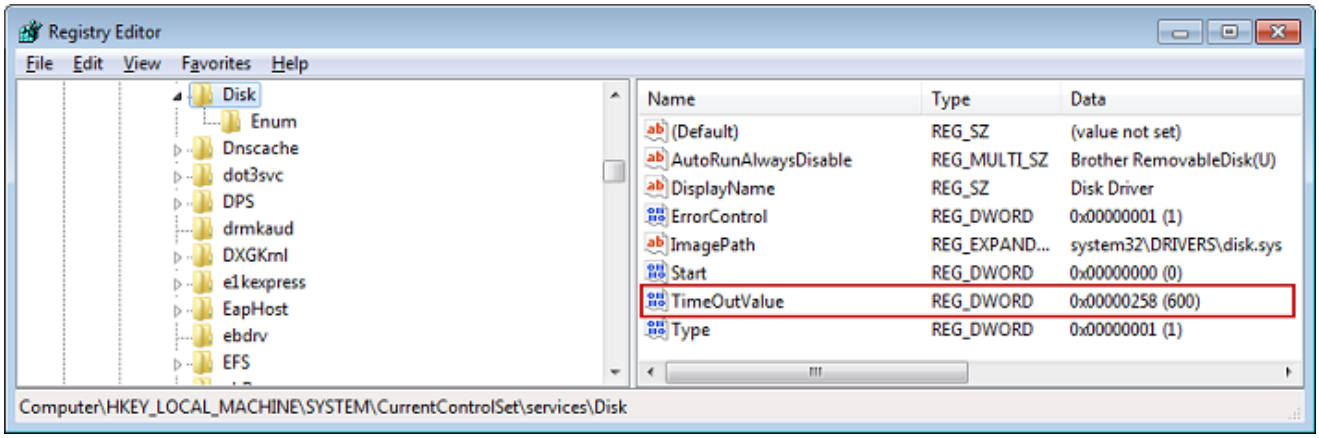
   a. 如果您尚未启动注册表编辑器 (Regedit.exe)，请将其启动。

   b. 导航到 “服务” 子项中的 “磁盘” 子项 CurrentControlSet，如下所示。

   ```
   HKEY_Local_Machine\SYSTEM\CurrentControlSet\Services\Disk
   ```

   c. 打开 TimeOutValueDWORD（32 位）值的上下文（右键单击）菜单，选择 “修改”，然后将该值更改为。**600**

   TimeOutValue指定 iSCSI 启动器在尝试通过断开并重新建立连接来恢复会话之前，将等待目标的响应多少秒。此值表示 600 秒的超时时间，如以下示例所示。



4. 要确保新配置的值生效，请重新启动系统。

   重新启动之前，必须确保刷新了对卷进行的所有写入操作的结果。要这样做，请在重启前将任何映射的存储卷磁盘脱机。

自定义您的 Linux iSCSI 设置

为网关设置启动程序后，我们强烈建议您自定义 iSCSI 设置以防止启动程序从目标断开。通过增大下面所示的 iSCSI 超时值，您可以提高应用程序对需要较长时间的写入操作以及网络中断等其他瞬态问题的处理能力。

> **Note**
>
> 命令可能与 Linux 的其他命令类型略有不同。以下示例基于 Red Hat Linux。

如需自定义您的 Linux iSCSI 设置

1. 提高请求排队的最长时间。

   a. 打开 `/etc/iscsi/iscsid.conf` 文件，然后找到以下各行。

   ```
   node.session.timeo.replacement_timeout = [replacement_timeout_value]
   node.conn[0].timeo.noop_out_interval = [noop_out_interval_value]
   node.conn[0].timeo.noop_out_timeout = [noop_out_timeout_value]
   ```

   b. 将 *[replacement_timeout_value]* 值设为 **600**。

      将 *[noop_out_interval_value]* 值设为 **60**。

将 *[noop_out_timeout_value]* 值设为 **600**。

这三种值的单位均为秒。

> **Note**
>
> 必须在发现网关之前进行 iscsid.conf 设置。如果已发现网关和/或已登录到目标，则可使用以下命令从发现数据库中删除该项。然后可以重新发现或登录，从而使新设置生效。
>
> ```
> iscsiadm -m discoverydb -t sendtargets -p [GATEWAY_IP]:3260 -o delete
> ```

2. 提高可在每个响应中传输的最大数据量。

   a. 打开 /etc/iscsi/iscsid.conf 文件，然后找到以下各行。

   ```
   node.session.iscsi.FirstBurstLength = [replacement_first_burst_length_value]
   node.session.iscsi.MaxBurstLength = [replacement_max_burst_length_value]
   node.conn[0].iscsi.MaxRecvDataSegmentLength
    = [replacement_segment_length_value]
   ```

   b. 我们建议使用以下值，以实现更佳性能。您的备份软件可以使用不同的值进行优化，因此请参阅备份软件文档了解最佳效果。

   将 *[replacement_first_burst_length_value]* 值设置为 **262144** 或 Linux 操作系统默认值，以较高者为准。

   将 *[replacement_max_burst_length_value]* 值设置为 **1048576** 或 Linux 操作系统默认值，以较高者为准。

   将 *[replacement_segment_length_value]* 值设置为 **262144** 或 Linux 操作系统默认值，以较高者为准。

   > **Note**
   >
   > 不同的备份软件可使用不同的 iSCSI 设置进行优化来达到最佳效果。要确认如何设置这些参数的值才能提供最佳性能，请参阅备份软件的文档。

3. 重启系统以确保新配置的值生效。

   重新启动之前，确保刷新了对卷进行的所有写入操作的结果。为此，请在重新启动之前卸载磁带。

为卷网关自定义 Linux 磁盘超时设置

如果您使用的是卷网关，则除了上一节中描述的 iSCSI 设置外，还可以自定义以下 Linux 磁盘超时设置。

自定义 Linux 磁盘超时设置

1. 在规则文件中增大磁盘超时值。

   a. 如果您使用了 RHEL 5 启动程序，请打开 `/etc/udev/rules.d/50-udev.rules` 文件并查找以下行。

   ```
   ACTION=="add", SUBSYSTEM=="scsi" , SYSFS{type}=="0|7|14", \
   RUN+="/bin/sh -c 'echo [timeout] > /sys$$DEVPATH/timeout'"
   ```

   此规则文件在 RHEL 6 或 RHEL 7 启动程序中不存在，因此您必须使用以下规则创建它。

   ```
   ACTION=="add", SUBSYSTEMS=="scsi" , ATTRS{model}=="Storage Gateway",
   RUN+="/bin/sh -c 'echo [timeout] > /sys$$DEVPATH/timeout'"
   ```

   要在 RHEL 6 中修改超时值，请使用以下命令，然后添加上面所示的代码行。

   ```
   sudo vim /etc/udev/rules.d/50-udev.rules
   ```

   要在 RHEL 7 中修改超时值，请使用以下命令，然后添加上面所示的代码行。

   ```
   sudo su -c "echo 600 > /sys/block/[device name]/device/timeout"
   ```

   b. 将 *[timeout]* 值设为 **600**。

   该值表示 600 秒的超时值。

2. 重启系统以确保新配置的值生效。

   重新启动之前，确保刷新了对卷进行的所有写入操作的结果。要这样做，请在重启前卸载存储卷。

3. 您可以使用以下命令测试配置。

```
udevadm test [PATH_TO_ISCSI_DEVICE]
```

此命令显示了应用到 iSCSI 设备的 udev 规则。

为 iSCSI 目标配置 CHAP 身份验证

Storage Gateway 支持使用质询握手身份验证协议 (CHAP) 在网关和 iSCSI 启动程序之间进行身份验证。CHAP 通过定期验证 iSCSI 启动程序的身份是否具有访问卷目标和 VTL 设备目标的权限来预防反演攻击。

> **Note**
>
> CHAP 配置是可选的，但强烈推荐进行此配置。

要设置 CHAP，必须在 Storage Gateway 控制台和用于连接目标的 iSCSI 启动程序软件中对其进行配置。Storage Gateway 使用双方 CHAP，即启动程序对目标进行身份验证，目标对启动程序进行身份验证。

为目标设置双向 CHAP

1. 在 Storage Gateway 控制台上配置 CHAP，如 为 Storage Gateway 控制台上的卷目标配置 CHAP 中所述。
2. 在客户端启动程序软件中，完成 CHAP 配置：
   - 要在 Windows 客户端上配置双向 CHAP，请参阅 在 Windows 客户端上配置双向 CHAP。。
   - 要在 Red Hat Linux 客户端上配置双向 CHAP，请参阅 如需在 Red Hat Linux 客户端上配置双向 CHAP。

为 Storage Gateway 控制台上的卷目标配置 CHAP

在本步骤中，您指定两个用来对卷进行读取和写入操作的私有密钥。这两个密钥也用来在本步骤中配置客户端启动程序。

1. 在 Storage Gateway 控制台的“导航”窗格中，选择卷。
2. 对于 Actions (操作)，选择 Configure CHAP Authentication (配置 CHAP 身份验证)。

3. 在配置 CHAP 身份验证对话框中提供要求的信息。

   a. 对于启动程序名称，请输入 iSCSI 启动程序的名称。此名称是 Amazon iSCSI 限定名称 (IQN)，前面加上 `iqn.1997-05.com.amazon:`，后跟目标名称。以下是示例。

      `iqn.1997-05.com.amazon:`*`your-volume-name`*

      您可以使用 iSCSI 启动程序软件找到启动程序名称。例如，对于 Windows 客户端，该名称为 iSCSI 启动程序的 Configuration (配置) 选项卡上的值。有关更多信息，请参阅在 Windows 客户端上配置双向 CHAP。。

      > **Note**
      >
      > 如需更改启动程序名称，您必须先停用 CHAP，在 iSCSI 启动程序软件中更改启动程序名称，然后使用新名称激活 CHAP。

   b. 对于用于对启动程序进行身份验证的密钥，输入要求的密钥。

      此私有密钥的长度最少为 12 个字符，最多为 16 个字符。此值是私有密钥，启动程序 (即 Windows 客户端) 必须知道该私有密钥才能参与到与目标的 CHAP 中。

   c. 对于用于对目标进行身份验证的密钥（双向 CHAP），输入要求的密钥。

      此私有密钥的长度最少为 12 个字符，最多为 16 个字符。目标必须知道此值才能参与到与启动程序的 CHAP 中。

      > **Note**
      >
      > 用来验证目标身份的私有密钥必须不同于用来验证启动程序的私有密钥。

   d. 选择保存。

4. 选择 Details 选项卡并确认 iSCSI CHAP authentication 设置为 true。

在 Windows 客户端上配置双向 CHAP。

在此过程中，您使用在控制台中为卷配置 CHAP 所用的同一密钥在 Microsoft iSCSI 启动程序中配置 CHAP。

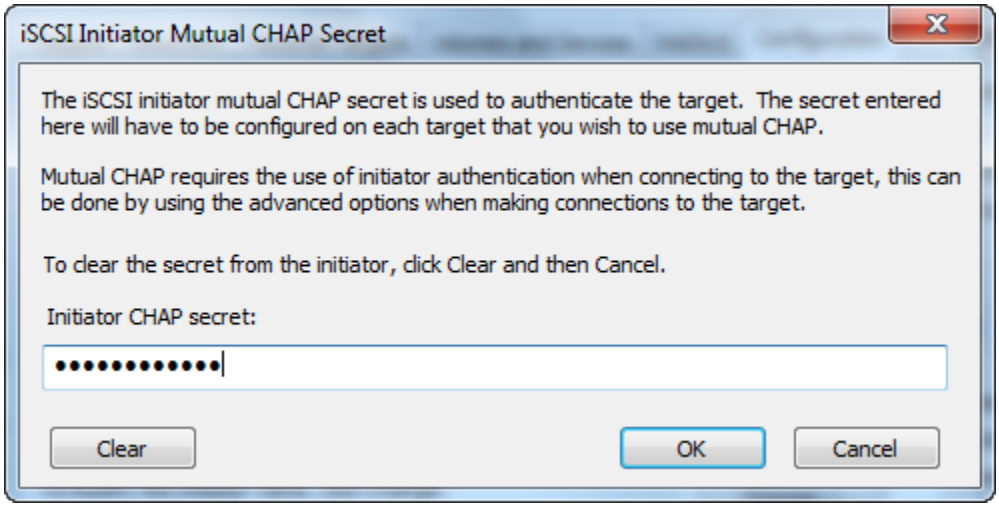
1. 如果 iSCSI 启动程序尚未启动，请在 Windows 客户端计算机的开始菜单上，选择运行，输入 **`iscsicpl.exe`**，然后选择确定来运行该程序。
2. 为启动程序 (即 Windows 客户端) 配置双向 CHAP 配置：

   a. 选择配置选项卡。

   > **Note**
   >
   > Initiator Name 值对于您的启动程序和公司是唯一的。前面显示的名称是您在 Storage Gateway 控制台的配置 CHAP 身份验证对话框中使用的值。
   > 示例图像中所示名称仅作示范用途。

   b. 选择 CHAP。

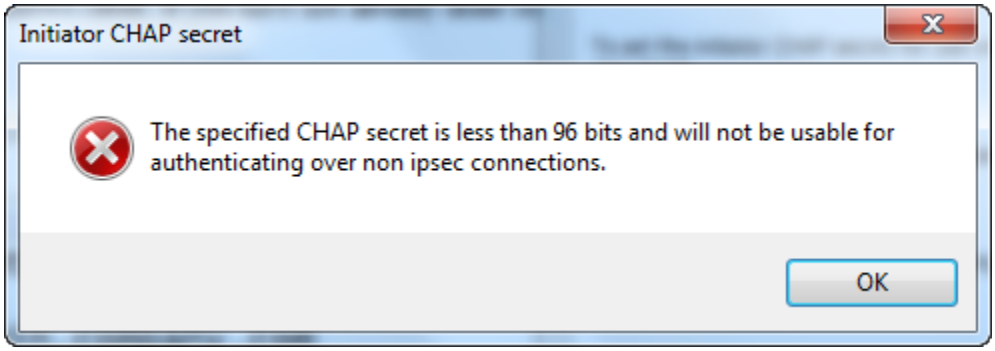
   c. 在 iSCSI 启动程序双向 CHAP 密钥对话框中，输入双向 CHAP 密钥值。



   在此对话框中，输入启动程序 (Windows 客户端) 用来对目标 (存储卷) 进行身份验证的私有密钥。该私有密钥允许目标读取并写入启动程序。此密钥与在配置 CHAP 身份验证对话框的用于对目标进行身份验证的密钥（双向 CHAP）框中输入的密钥相同。有关更多信息，请参阅为 iSCSI 目标配置 CHAP 身份验证。

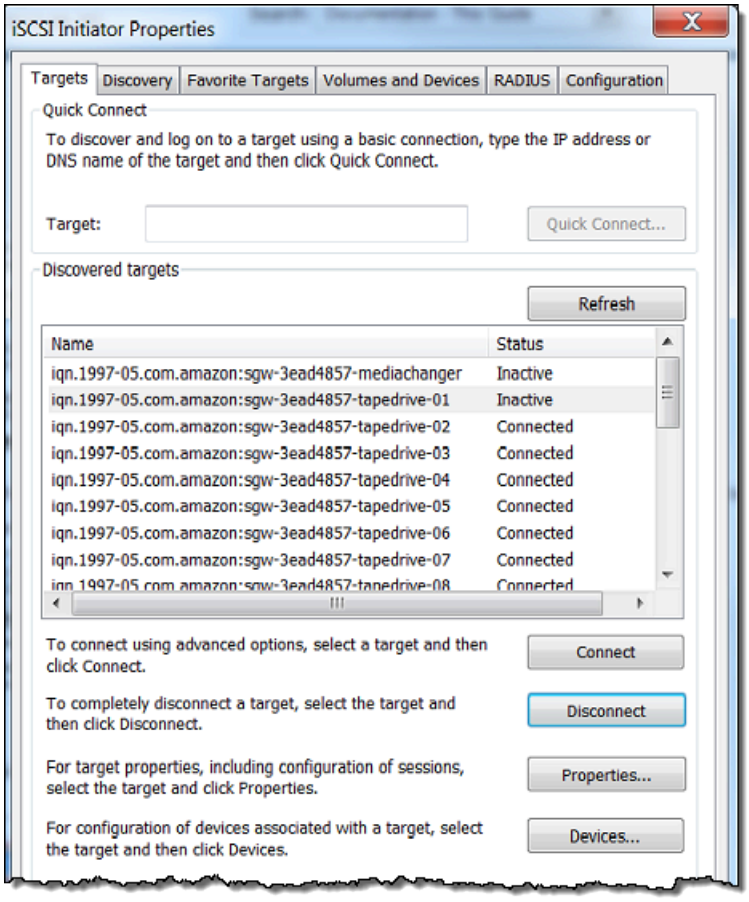
   d. 如果您输入的密钥少于 12 个字符或多于 16 个字符，则会显示启动程序 CHAP 密钥错误对话框。

选择确定，然后重新输入密钥。



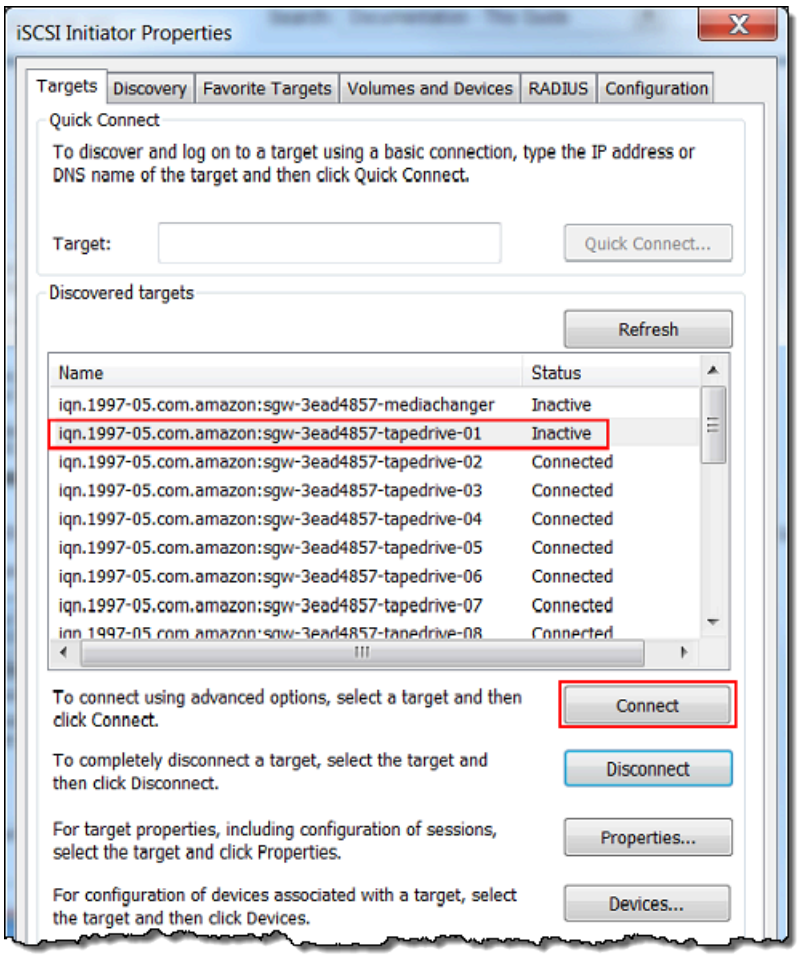
3. 使用启动程序的密钥进行配置，完成双向 CHAP 配置。

   a. 选择目标选项卡。

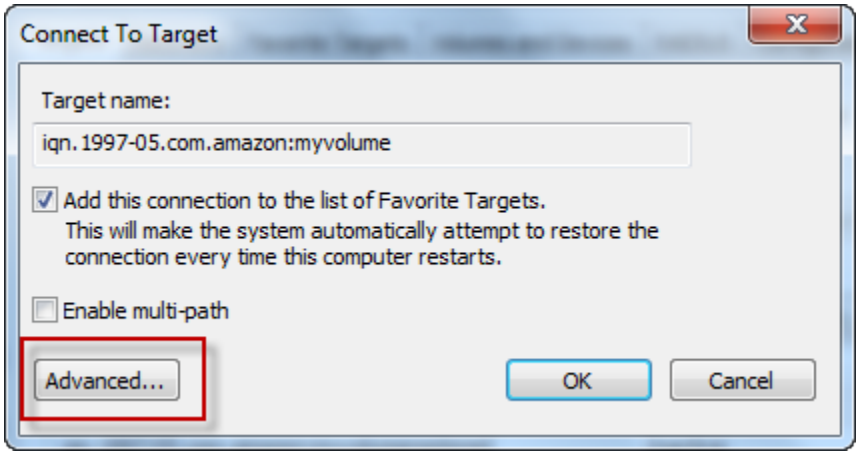


   b. 如果当前连接了要为 CHAP 配置的目标，则通过选择该目标并选择 Disconnect 来断开该目标。

   c. 选择要为 CHAP 配置的目标，然后选择 Connect。



d. 在 Connect to Target 对话框中，选择 Advanced。



e. 在“Advanced Settings”对话框中，配置 CHAP。

i. 选择激活 CHAP 登录。

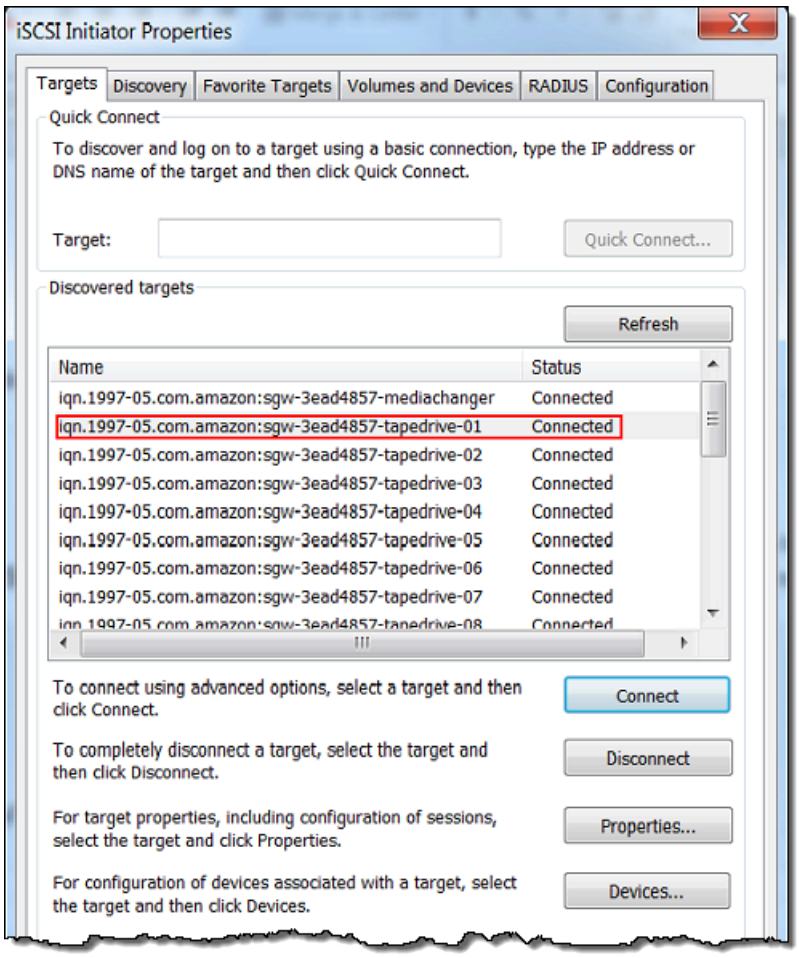
ii. 输入验证启动程序所需的密钥。此密钥与在配置 CHAP 身份验证对话框的用于对启动程序进行身份验证的密钥框中输入的密钥相同。有关更多信息，请参阅为 iSCSI 目标配置 CHAP 身份验证。

iii. 选择“Perform mutual authentication”。

iv. 要应用更改，请选择 OK。

f. 在 Connect to Target 对话框中，选择 OK。

4. 如果提供的私有密钥正确无误，则目标将显示 Connected (已连接) 状态。



如需在 Red Hat Linux 客户端上配置双向 CHAP

在此过程中，您使用在 Storage Gateway 控制台中为卷配置 CHAP 所用的同一密钥在 Linux iSCSI 启动程序中配置 CHAP。

1. 确保 iSCSI 守护进程正在运行并且您已连接到目标。如果您尚未完成这两项任务，请参阅连接到 Red Hat Enterprise Linux 客户端。

2. 断开并移除您即将为其配置 CHAP 的目标的任何现有配置。

   a. 要查找目标名称并确保其为定义的配置，请使用以下命令列出保存的配置。

   ```
   sudo /sbin/iscsiadm --mode node
   ```

   b. 从目标断开。

   以下命令从 Amazon iSCSI 限定名称 (IQN) 中定义的名为 **myvolume** 的目标断开连接。按您的需求情况更改目标名称和 IQN。

   ```
   sudo /sbin/iscsiadm --mode node --logout GATEWAY_IP:3260,1
    iqn.1997-05.com.amazon:myvolume
   ```

   c. 移除目标的配置。

   下面的命令移除 **myvolume** 目标的配置。

   ```
   sudo /sbin/iscsiadm --mode node --op delete --targetname
    iqn.1997-05.com.amazon:myvolume
   ```

3. 编辑 iSCSI 配置文件来激活 CHAP。

   a. 获取启动程序 (即您正在使用的客户端) 的名称。

   以下命令从文件 /etc/iscsi/initiatorname.iscsi 获取发起程序名称。

   ```
   sudo cat /etc/iscsi/initiatorname.iscsi
   ```

   该命令的输出内容类似于以下内容：

   ```
   InitiatorName=iqn.1994-05.com.redhat:8e89b27b5b8
   ```

   b. 打开 /etc/iscsi/iscsid.conf文件。

   c. 取消文件中下列各行的注释，并为 *username*、*password*、*username_in* 和 *password_in* 指定正确的值。

   ```
   node.session.auth.authmethod = CHAP
   node.session.auth.username = username
   node.session.auth.password = password
   node.session.auth.username_in = username_in
   ```

```
node.session.auth.password_in = password_in
```

有关要指定的值的指南，请参阅下表。

配置设置	值
username	您在此过程中的上一步中找到的启动程序名称。该值以 iqn 开头。例如，**iqn.1994-05.com.redhat:8e89b27b5b8** 是有效的 *username* 值。
##	用于在启动程序 (您正在使用的客户端) 与卷通信时对启动程序进行身份验证的私有密钥。
username_in	目标卷的 IQN。该值以 iqn 开头，以目标名称结尾。例如，**iqn.1997-05.com.amazon:myvolume** 是有效的 *username_in* 值。
password_in	用于在目标 (卷) 与启动程序通信时对目标进行身份验证的私有密钥。

d. 保存配置文件中的更改，然后关闭该文件。

4. 发现并登录到目标。为此，请按照连接到 Red Hat Enterprise Linux 客户端中的步骤进行操作。

AWS Direct Connect 与 Storage Gateway 一起使用

AWS Direct Connect 将您的内部网络链接到亚马逊 Web Services 云。通过 AWS Direct Connect 与 Storage Gateway 配合使用，您可以创建满足高吞吐量工作负载需求的连接，从而在本地网关和 AWS 之间提供专用的网络连接。

Storage Gateway 使用公有端点。 AWS Direct Connect 建立连接后，您可以创建一个公共虚拟接口，以允许将流量路由到 Storage Gateway 端点。该公共虚拟接口将绕过您的网络路径中的 Internet 服务提供商。Storage Gateway 服务的公共终端节点可以与该 AWS Direct Connect 位置位于同一个 AWS 区域，也可以位于不同的 AWS 区域。

下图显示了如何 AWS Direct Connect 使用 Storage Gateway 的示例。
网络架构显示 Storage Gateway 使用 AWS 直接连接连接到云端。

以下过程假定您已创建正常运行的网关。

AWS Direct Connect 与 Storage Gateway 配合使用

1. 在您的本地数据中心和 Storage Gateway 终端节点之间创建并建立 AWS Direct Connect 连接。有关如何创建连接的更多信息，请参阅《AWS Direct Connect 用户指南》中的 AWS Direct Connect 入门。
2. 将您的本地 Storage Gateway 设备连接到 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。即使使用 Direct Connect，也必须使用 HAProxy 创建 VPC 端点。有关更多信息，请参阅《AWS Direct Connect 用户指南》中的创建虚拟接口。

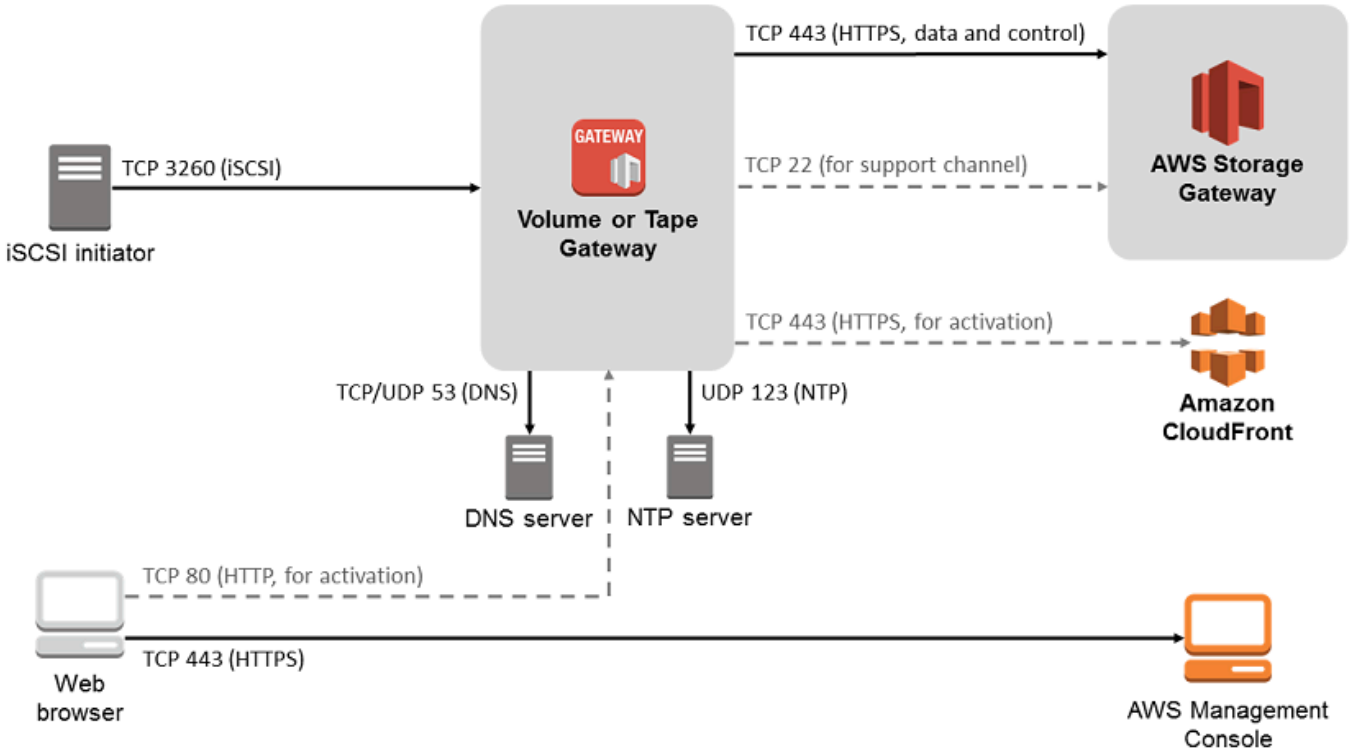
有关的详细信息 AWS Direct Connect，请参阅什么是 AWS Direct Connect？ 在《AWS Direct Connect 用户指南》中。

端口要求

Storage Gateway 需要以下端口才能正常运行。有些端口是所有网关类型的通用端口，也是所有网关类型所必需的端口。其他端口则是特定网关类型所需要的。在本节中，您可以找到卷网关必需端口的插图和列表。

卷网关

下图显示要为卷网关操作开放的所有端口。



下列端口是所有网关类型的通用端口，也是所有网关类型必需的端口。

From	目的	协议	端口	如何使用	
Storage Gateway VM	AWS	传输控制协议 (TCP)	443（HTTPS）	用于从 Storage Gateway 出站虚拟机与 AWS 服务端点进行通信。有关服务端点的信息，请参阅允许通过防火墙和路由器进行 AWS Storage Gateway 访问。	

From	目的	协议	端口	如何使用	
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。仅在激活 Storage Gateway 设备期间使用端口 80。 Storage Gateway VM 不要求可公开访问端口 80。端口 80 所需的访问级别取决于网络配置。如果您从 Storage Gateway 管理控制台激活了网关，则您连接到控制台所用的主机必须对网关端口 80 具有访问权限。	
Storage Gateway VM	域名服务 (DNS) 服务器	用户数据报协议 (UDP)/UDP	53 (DNS)	用于 Storage Gateway VM 和 DNS 服务器之间的通信。	

From	目的	协议	端口	如何使用	
Storage Gateway VM	AWS	TCP	22 (支持渠道)	AWS Support 允许访问您的网关以帮助您解决网关问题。您无需打开此端口即可实现网关的正常操作，但在进行问题排查时需要如此。	
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	

From	目的	协议	端口	如何使用	
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。	

除了通用端口之外，卷网关还需要下列端口。

From	目的	协议	端口	如何使用	
iSCSI 启动程序	Storage Gateway VM	TCP	3260 (iSCSI)	由本地系统用于连接由网关公开的 iSCSI 目标。	

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，您也可以从 Amazon EC2 管理控制台获取 Amazon EC2 实例的 IP 地址。要了解如何获取网关的 IP 地址，请参阅以下内容之一：

- VMware 主机：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。然后返回到 Storage Gateway 控制台并在控制台中键入该 IP 地址。

从 Amazon EC2 主机获取 IP 地址

要获取用于部署网关的 Amazon EC2 实例的 IP 地址，请登录到 EC2 实例的本地控制台。然后从控制台页面顶部获取 IP 地址。有关说明，请参阅登录到 Amazon EC2 网关本地控制台。

您也可以从 Amazon EC2 管理控制台获取 IP 地址。我们建议使用公有 IP 地址进行激活。要获取公有 IP 地址，请使用程序 1。如果您选择使用弹性 IP 地址，请参阅程序 2。

程序 1：使用公有 IP 地址连接到网关

1. 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。返回到 Storage Gateway 控制台并键入该 IP 地址。

如果您想使用弹性 IP 地址进行激活，可使用以下程序。

程序 2：使用弹性 IP 地址连接到网关

1. 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。返回到 Storage Gateway 控制台并键入弹性 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，主要资源是网关，而其他资源类型包括：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*
卷 ARN	arn:aws:storagegateway: *region*:*account-id* :gateway/ *gateway-id* /volume/*volume-id*
目标 ARN (iSCSI 目标)	arn:aws:storagegateway: *region*:*account-id* :gateway/ *gateway-id* /target/*iSCSItarget*

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 使用大写字母。不过，当您将这些资源 ID 与 Amazon EC2 API 结合使用时，Amazon EC2 需要采用小写形式的资源 ID。您必须将资源 ID 更改为小写才能将其与 EC2 API 结合使用。例如，在 Storage Gateway 中，卷的 ID 可能为 `vol-1122AABB`。当您将此 ID 与 EC2 API 结合使用时，您必须将其更改为 `vol-1122aabb`。否则，EC2 API 的行为方式可能不符合预期。

标记 Storage Gateway 资源

在 Storage Gateway 中，您可以使用标签来管理资源。利用标签，您可以向资源添加元数据和对资源分类，以便更轻松地管理它们。每个标签都包含您定义的一个键-值对。您可以向网关、卷和虚拟磁带添加标签。您可以根据添加的标签搜索和筛选这些资源。

例如，您可以使用这些标签标识组织中的每个部门使用的 Storage Gateway 资源。您可能为会计部使用的网关和卷添加类似于下面的标签：(`key=department` 和 `value=accounting`)。然后，您可以使用此标签进行筛选，以便标识会计部使用的所有网关和卷并使用此信息确定成本。有关更多信息，请参阅使用成本分配标签和使用标签编辑器。

如果您存档了一个已标记的虚拟磁带，则该磁带将在存档中保留其标签。同样，如果您将磁带从存档取回到另一网关，则该标记将保留在新网关中。

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。此前缀保留供 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) 处理标签。下面的过程介绍如何在控制台上添加、编辑和删除标签。

添加标签

1. 打开 Storage Gateway 控制台，网址为 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. 打开 Storage Gateway 控制台，网址为 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. 打开 Storage Gateway 控制台，网址为 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。

使用 AWS Storage Gateway的开源组件

本节介绍我们在提供 Storage Gateway 功能时所依赖的第三方工具和许可证。

可在以下网址下载 AWS Storage Gateway 软件附带的某些开源软件组件的源代码：

- 对于在 VMware ESXi 上部署的网关，请下载 sources.tar
- 对在 Microsoft Hyper-V 上部署的网关，请下载 sources_hyperv.tar
- 对在基于 Linux 内核的虚拟机 (KVM) 上部署的网关，请下载 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。

AWS Storage Gateway 配额

在本主题中，您可找到有关 Storage Gateway 的卷和磁带配额、配置和性能限制的信息。

主题

- 卷的配额
- 为网关建议的本地磁盘大小

卷的配额

下表列出了卷的配额。

描述	缓存卷	存储卷
卷的最大大小 **Note** 如果从缓存卷创建了大小超过 16 TiB 的快照，您可以将其还原到 Storage Gateway 卷，但不能还原到 Amazon Elastic Block Store (Amazon EBS) 卷。	32 TiB	16 TiB
每个网关的最大卷数	32	32
网关中所有卷的总大小	1,024 TiB	512 TiB

为网关建议的本地磁盘大小

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）	上传缓冲区（最小值）	上传缓冲区（最大值）	其他必需的本地磁盘
缓存卷网关	150 GiB	64 TiB	150 GiB	2 TiB	—
存储卷网关	—	—	150 GiB	2 TiB	一个或多个，用于存储卷

> **Note**
>
> 您可以为缓存和上传缓冲区配置一个或多个不超过最大容量的本地驱动器。
> 在向现有网关添加缓存或上传缓冲区时，在主机（管理程序或 Amazon EC2 实例）中创建新磁盘，这很重要。如果之前已将磁盘分配为缓存或上传缓冲区，请勿更改现有磁盘的大小。

Storage Gateway 的 API 参考

除了使用控制台外，您还可以使用 AWS Storage Gateway API 以编程方式配置和管理您的网关。本节介绍 AWS Storage Gateway 操作、身份验证请求签名和错误处理。有关 Storage Gateway 可用的区域和端点的信息，请参阅《AWS 一般参考》中的 AWS Storage Gateway 端点和配额。

> **Note**
>
> 在使用开发应用程序时，您也可以使用软件开发 AWS 工具包。 AWS Storage Gateway适用于 Java、.NET 和 PHP 的 AWS 软件开发工具包封装了底层 AWS Storage Gateway API，从而简化了您的编程任务。有关下载开发工具包库的信息，请参阅示例代码库。

主题

- Storage Gateway 必需的请求标头
- 对请求进行签名
- 错误响应
- 操作

Storage Gateway 必需的请求标头

本部分描述您每次向 Storage Gateway 发送 POST 请求时必须使用的标头。您将 HTTP 标头包含在内以识别有关请求的密钥信息，包括您希望调用的操作、请求的日期以及表示您拥有请求发送者授权的信息。标头区分大小写，其次序不重要。

以下示例显示了ActivateGateway操作中使用的标头。

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120425/us-east-2/
storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target,
 Signature=9cd5a3584d1d67d57e61f120f35102d6b3649066abdd4bf4bbcf05bd9f2f8fe2
x-amz-date: 20120912T120000Z
```

```
x-amz-target: StorageGateway_20120630.ActivateGateway
```

以下是必须包含在向 Storage Gateway 发送的 POST 请求中的标头。下面显示的以 “x-amz” 开头的标题是 AWS特定标题。列出的其他所有标头均为 HTTP 事务中使用的普通标头。

标题	描述
`Authorization`	授权标头包含有关请求的数种信息，这些信息可以让 Storage Gateway 确定请求是否为请求者的有效操作。该标头的格式如下所示 (为便于阅读，添加了换行符)： `Authorization: AWS4-HMAC_SHA456 Credentials= YourAccessKey /yyymmdd/region/storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature= CalculatedSignature` 在前面的语法中，您可以指定YourAccessKey年、月和日 (yyyymmdd)、区域和。CalculatedSignature授权标头的格式由 AWS V4 签名过程的要求决定。签名的详细信息在主题 对请求进行签名 中进行讨论。
`Content-Type`	将 `application/x-amz-json-1.1` 用作所有发往 Storage Gateway 的请求的内容类型。 `Content-Type: application/x-amz-json-1.1`
`Host`	使用主机标头指定向其发送请求的 Storage Gateway 网关端点。例如，`storagegateway.us-east-2.amazonaws.com` 是美国东部（俄亥俄州）区域的端点。有关 Storage Gateway 可用的端点的更多信息，请参阅《AWS 一般参考》中的 AWS Storage Gateway 端点和配额。 `Host: storagegateway. region.amazonaws.com`
`x-amz-date`	您必须在 HTTP `Date` 标头或标头中 AWS `x-amz-date` 提供时间戳。(部分 HTTP 客户端库文件不允许您设置`Date`标头。) 当存在 `x-amz-`

标题	描述
	`date` 标头时，Storage Gateway 会在请求验证期间忽略任何 Date 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` 操作名称值（例如 ActivateGateway “”）可以从 API 列表中找到。Storage Gateway 的 API 参考

对请求进行签名

Storage Gateway 要求通过对请求进行签名，验证所发送的每个请求的身份。您使用加密哈希函数计算数字签名，从而对请求签名。加密哈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。

在收到您的请求后，Storage Gateway 将使用您用于对该请求进行签名的同一哈希函数和输入重新计算签名。如果所得签名与该请求中的签名相匹配，则 Storage Gateway 处理该请求。否则，请求将被拒绝。

Storage Gateway 支持使用 AWS 签名版本 4 进行身份验证。计算签名的过程可分为三个任务：

- 任务 1：创建规范请求

  将您的 HTTP 请求重新排列为规范格式。必须使用规范格式，因为 Storage Gateway 在重新计算签名以与您发送的签名进行比较时使用同一规范格式。
- 任务 2：创建待签字符串

创建一个字符串，将该字符串用作您的加密哈希函数输入值中的一项。该字符串称为待签字符串，是哈希算法名称、请求日期、凭证范围字符串以及来自上一任务的规范化请求的结合。凭证范围字符串本身是日期、区域和服务信息的结合。

- 任务 3：创建签名

  使用加密哈希函数为您的请求创建签名，该函数接受两种输入字符串：待签字符串和派生密钥。派生密钥的计算方法是，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

以下示例引导您了解为 ListGateways 创建签名的详细信息。该示例可用作核查您的签名计算方法的参考。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。
- 端点是美国东部（俄亥俄州）区域。

通用请求语法 (包括 JSON 正文) 为：

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
x-amz-Date: 20120910T000000Z
Authorization: SignatureToBeCalculated
Content-type: application/x-amz-json-1.1
x-amz-target: StorageGateway_20120630.ListGateways
{}
```

为任务 1：创建规范请求计算的请求规范格式为：

```
POST
/

content-type:application/x-amz-json-1.1
host:storagegateway.us-east-2.amazonaws.com
x-amz-date:20120910T000000Z
x-amz-target:StorageGateway_20120630.ListGateways
```

```
content-type;host;x-amz-date;x-amz-target
44136fa355b3678a1146ad16f7e8649e94fb4fc21fe77e8310c060f61caaff8a
```

规范请求的最后一行是请求正文的哈希值。另外，请注意规范请求的第三行是空的。这是因为此 API（或任何 Storage Gateway API）没有查询参数。

任务 2：创建待签字符串 的待签字符串是：

```
AWS4-HMAC-SHA256
20120910T000000Z
20120910/us-east-2/storagegateway/aws4_request
92c0effa6f9224ac752ca179a04cecbede3038b0959666a8160ab452c9e51b3e
```

用来签名的请求的第一行是算法，第二行是时间戳，第三行是证书范围，最后一行是任务 1 中规范请求的哈希值。

对于 任务 3：创建签名，派生密钥可表示为：

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey,"20120910"),"us-
east-2"),"storagegateway"),"aws4_request")
```

如果使用私有访问密钥 wjalrxutnfemi/k7mdeng/ CYEXAMPLEK bPxRfi EY，则计算出的签名为：

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

最终步骤是构造 Authorization 标头。对于演示访问密钥 AKIAIOSFODNN7EXAMPLE，标头（为了便于阅读，添加了换行符）是：

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120910/us-east-2/
storagegateway/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

错误响应

主题

- 异常
- 操作错误代码
- 错误响应

本节提供有关 AWS Storage Gateway 错误的参考信息。这些错误以错误例外和操作错误代码表示。例如，如果请求签名存在问题，那么会由任何 API 响应返回错误例外 `InvalidSignatureException`。但是，`ActivationKeyInvalid`仅返回 ActivateGatewayAPI 的操作错误代码。

根据错误类型的情况，Storage Gateway 可能只返回例外，或者可能同时返回例外和操作错误代码。错误响应 中显示了误差响应示例。

异常

下表列出了 AWS Storage Gateway API 异常。当 AWS Storage Gateway 操作返回错误响应时，响应正文包含其中一个异常。`InternalServerError` 和 `InvalidGatewayRequestException` 返回操作错误代码 (提供特定的操作错误代码的 操作错误代码 消息代码) 之一。

例外	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`	请求的操作无效。	400 错误请求
`InvalidClientTokenId`	我们的记录中不存在提供的 X.509 证书或 AWS 访问密钥 ID。	403 禁止访问
`InvalidGatewayRequestException`	操作错误代码 中的操作错误代码消息之一。	400 错误请求

例外	消息	HTTP 状态代码
InvalidSignatureException	我们计算出的请求签名与您提供的签名不匹配。检查您的 AWS 访问密钥和签名方法。	400 错误请求
MissingAction	请求中遗漏了一个操作或运行参数。	400 错误请求
MissingAuthenticationToken	请求必须包含有效（已注册的）AWS 访问密钥 ID 或 X.509 证书。	403 禁止访问
RequestExpired	请求超过有效期或请求时间 (或用 15 分钟填补)，或将来发送请求的时间超过 15 分钟。	400 错误请求
SerializationException	序列化期间出现错误。查看您的 JSON 负载结构是否良好。	400 错误请求
ServiceUnavailable	由于服务器发生临时故障而导致请求失败。	503 服务不可用
SubscriptionRequiredException	AWS 访问密钥 ID 需要订阅该服务。	400 错误请求
ThrottlingException	费率已超。	400 错误请求
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

下表显示了 AWS Storage Gateway 操作错误代码和可以返回错误代码的 API 之间的映射关系。返回所有操作错误代码，包含异常中所述的两个一般异常（InternalServerError 和 InvalidGatewayRequestException）之一。

操作错误代码	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。	CreateCachediscsiVolu CreateStorediscsiVolu
InitiatorNotFound	找不到指定的启动程序。	DeleteChapCredentials
DiskAlreadyAllocated	指定的磁盘已分配。	AddCache AddUploadBuffer AddWorkingStorage CreateStorediscsiVolu
DiskDoesNotExist	指定的磁盘不存在。	AddCache AddUploadBuffer AddWorkingStorage CreateStorediscsiVolu
DiskSizeNotGigAligned	指定的磁盘没有以 GB 为整单位。	CreateStorediscsiVolu
DiskSizeGreaterThanVolumeMaxSize	指定的磁盘大小超过最高卷大小。	CreateStorediscsiVolu

操作错误代码	消息	返回此错误代码的操作
DiskSizeLessThanVolumeSize	指定的磁盘大小低于最高卷大小。	CreateStorediscsiVolu
DuplicateCertificateInfo	指定的证书信息是副本。	ActivateGateway

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 CreateCachediscsiVolu CreateSnapshot CreateStorediscsiVolu CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachedisciVolum DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediscsiVolum 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 CreateCachediscsiVolu CreateSnapshot CreateStorediscsiVolu CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachedisciVolum DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediscsiVolum 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 CreateCachediscsiVolu CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediscsiVolu DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachedisciVolum DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediscsiVolum 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 CreateCachediscsiVolu CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediscsiVolu DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediscsiVolum DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediscsiVolum 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 CreateCachediscsiVolu CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediscsiVolu DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachedisciVolum DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediscivolum

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	指定的请求中包含错误参数。	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediscsiVolu CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediscsiVolu DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachedisciVolum DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediscivolum

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 错误。	CreateStorediscsiVolu
MaximumVolumeCountExceeded	已超过最大卷计数。	CreateCachediscsiVolu CreateStorediscsiVolu DescribeCachedisciVolum DescribeStoredisciVolum

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。	CreateCachediscsiVolu CreateStorediscsiVolu

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 CreateCachediscsiVolu CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediscsiVolu DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachedisciVolum DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediscivolum

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
SnapshotInProgressException	指定的快照在进行中。	DeleteVolume
SnapshotIdInvalid	指定的快照无效。	CreateCachediscsiVolu CreateStorediscsiVolu
StagingAreaFull	暂存区域已满。	CreateCachediscsiVolu CreateStorediscsiVolu

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。	CreateCachediscsiVolu CreateStorediscsiVolu
TargetInvalid	指定的目标无效。	CreateCachediscsiVolu CreateStorediscsiVolu DeleteChapCredentials DescribeChapCredentials UpdateChapCredentials
TargetNotFound	找不到指定的目标。	CreateCachediscsiVolu CreateStorediscsiVolu 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 CreateCachediscsiVolu CreateSnapshotFromVolumeRecoveryPoint CreateStorediscsiVolu DeleteSnapshotSchedule DescribeCache DescribeCachediscsiVolum DescribeStorediscsiVolum DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
VolumeAlreadyExists	已存在指定的卷。	CreateCachediscsiVolu CreateStorediscsiVolu
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 DescribeCachedisciVolum DescribeSnapshotSchedule DescribeStorediscVolum UpdateSnapshotSchedule
VolumeNotReady	指定的卷没有准备好。	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

错误响应

当存在错误时，响应头信息会包含：

- 内容类型：应用程序/ -1.1 x-amz-json
- 适当的 4xx 或 5xx HTTP 状态码

错误响应的正文会包含有关错误出现的信息。下列错误响应示例显示的是所有错误响应中常见的响应元素的输出语法。

```
{
    "__type": "String",
    "message": "String",
    "error":
        { "errorCode": "String",
          "errorDetails": "String"
        }
```

```
}
```

下表介绍了前一语法中显示的 JSON 错误响应字段。

__type

异常 中的例外之一。

类型：字符串

error

包含特定于 API 的错误详细信息。在常规的 (即不特定于任何 API 的) 错误中，不显示这个误差信息。

类型：集合

errorCode

其中一个操作错误代码。

类型：字符串

errorDetails

此字段不在 API 的当前版本中使用。

类型：字符串

message

一个操作错误代码消息。

类型：字符串

错误响应示例

如果您使用 sciVolum DescribeStoredi es API 并指定了不存在的网关 ARN 请求输入，则会返回以下 JSON 正文。

```
{
  "__type": "InvalidGatewayRequestException",
  "message": "The specified volume was not found.",
  "error": {
```

```
    "errorCode": "VolumeNotFound"
  }
}
```

如果 Storage Gateway 计算的签名不符合通过请求发送的签名，那么会返回如下 JSON 正文。

```
{
  "__type": "InvalidSignatureException",
  "message": "The request signature we calculated does not match the signature you
 provided."
}
```

Storage Gateway 中的操作

有关 Storage Gateway 操作的列表，请参阅《AWS Storage Gateway API 参考》中的操作。

《卷网关用户指南》的文档历史记录

- API 版本：2013-06-30
- 文档最近更新时间：2020 年 11 月 24 日

下表描述了在 2018 年 4 月后每次发布《AWS Storage Gateway 用户指南》时进行的重要更改。要获得本文档的更新通知，您可以订阅 RSS 源。

变更	说明	日期
添加了打开或关闭维护更新的选项	Storage Gateway 会定期收到维护更新，其中可能包括操作系统和软件升级、用于解决稳定性、性能和安全性的修复以及对新功能的访问。现在，您可以配置一项设置，为部署中的每个网关开启或关闭这些更新。有关更多信息，请参阅使用控制台管理网关更新。 AWS Storage Gateway	2024 年 6 月 6 日
Snowball Edge 上已弃用对磁带网关的支持	无法再在 Snowball Edge 设备上托管磁带网关。	2024 年 3 月 14 日
更新了使用第三方应用程序测试网关设置的说明	现在，使用第三方应用程序测试网关设置的说明描述了在执行备份任务期间网关重新启动时的预期行为。有关更多信息，请参阅。	2023 年 10 月 24 日
更新了推荐的 CloudWatch 警报	该 CloudWatch `HealthNotifications` 警报现在适用于所有网关类型和主机平台，并建议该警报适用于所有网关类型和主机平台。`HealthNotifications` 和	2023 年 10 月 2 日

	AvailabilityNotifications 的建议配置设置也已更新。有关更多信息，请参阅了解 CloudWatch 警报。	
单独的磁带网关和卷网关用户指南	《Storage Gateway 用户指南》以前包含有关磁带网关和卷网关类型的信息，现已分为《磁带网关用户指南》和《卷网关用户指南》，每份指南仅包含有关一种网关类型的信息。有关更多信息，请参阅磁带网关用户指南和卷网关用户指南。	2022 年 3 月 23 日
更新了网关创建程序	使用 Storage Gateway 控制台创建所有网关类型的过程均已更新。有关更多信息，请参阅创建网关。	2022 年 1 月 18 日
新的磁带接口	AWS Storage Gateway 控制台中的磁带概述页面已更新，增加了新的搜索和筛选功能。为了描述新功能，本指南中的所有相关程序均已更新。有关更多信息，请参阅管理您的磁带网关。	2021 年 9 月 23 日
支持适用于磁带网关的 Quest NetVault Backup 13	磁带网关现在支持在微软 Windows Server 2012 R2 或微软 Windows Server 2016 上运行的 Quest B NetVault ackup 13。有关更多信息，请参阅 “使用 Quest NetVault Backup 测试您的设置”。	2021 年 8 月 22 日

S3 文件网关主题已从磁带网关和卷网关指南中删除	为了使设置各自网关类型的客户更容易遵循磁带网关和卷网关的用户指南，删除了一些不必要的主题。	2021 年 7 月 21 日
为磁带网关支持 Windows 和 Linux 上的 IBM Spectrum Protect 8.1.10	磁带网关现在支持在 Microsoft Windows Server 和 Linux 上运行的 IBM Spectrum Protect 8.1.10。有关更多信息，请参阅使用 IBM Spectrum Protect 测试您的设置。	2020 年 11 月 24 日
FedRAMP 合规性	Storage Gateway 现已符合 FedRAMP 标准。有关更多信息，请参阅 Storage Gateway 的合规性验证。	2020 年 11 月 24 日
基于计划的带宽限制	Storage Gateway 现在支持对磁带网关和卷网关进行基于计划的带宽限制。有关更多信息，请参阅使用 Storage Gateway 控制台调度带宽限制。	2020 年 11 月 9 日
缓存卷和磁带网关本地缓存存储增加 4 倍	Storage Gateway 现在为缓存卷和磁带网关支持高达 64 TB 的本地缓存，通过提供对更大工作数据集的低延迟访问来提高本地应用程序的性能。有关更多信息，请参阅为网关推荐的本地磁盘大小。	2020 年 11 月 9 日
网关迁移	Storage Gateway 现在支持将缓存的卷网关迁移到新的虚拟机。有关更多信息，请参阅将缓存卷移至新的缓存卷网关虚拟机。	2020 年 9 月 10 日

支持磁带保留锁和 write-once-read-many (WORM) 磁带保护	Storage Gateway 支持虚拟磁带上的磁带保留锁定和一次写入多次读取 (WORM)。磁带保留锁定让您可以指定已存档虚拟磁带的保留模式和期限，从而在长达 100 年的固定时间段内防止删除这些磁带。这包括权限控制，用于控制谁可以删除磁带或修改保留设置。有关更多信息，请参阅使用磁带保留锁定。已激活 WORM 的虚拟磁带有助于确保无法覆盖或擦除虚拟磁带库中活动磁带上的数据。有关更多信息，请参阅一次写入多次读取 (WORM) 磁带保护。	2020 年 8 月 19 日
通过控制台订购硬件设备	现在，您可以通过 AWS Storage Gateway 控制台订购硬件设备。有关更多信息，请参阅使用 Storage Gateway 硬件设备。	2020 年 8 月 12 日
在新的 AWS 区域支持美国联邦信息处理标准 (FIPS) 端点	现在您可以在美国东部（俄亥俄州）、美国东部（弗吉尼亚州北部）、美国西部（北加利福尼亚）、美国西部（俄勒冈州）和加拿大（中部）区域通过 FIPS 端点激活网关。有关更多信息，请参阅《AWS 一般参考》中的 AWS Storage Gateway 端点和配额。	2020 年 7 月 31 日
网关迁移	Storage Gateway 现在支持将磁带和存储的卷网关迁移到新的虚拟机。有关更多信息，请参阅将数据移到新网关。	2020 年 7 月 31 日

在 Storage Gateway 控制台中查看亚马逊 CloudWatch 警报	现在，您可以在 Storage Gateway 控制台中查看 CloudWatch 警报。有关更多信息，请参阅了解 CloudWatch 警报。	2020 年 5 月 29 日
支持美国联邦信息处理标准 (FIPS) 端点	现在，您可以在 AWS GovCloud (US) 区域中通过 FIPS 终端节点激活网关。要为卷网关选择 FIPS 端点，请参阅选择服务端点。要为磁带网关选择 FIPS 端点，请参阅将磁带网关连接到 AWS。	2020 年 5 月 22 日
新 AWS 区域	Storage Gateway 现已在非洲（开普敦）和欧洲（米兰）区域推出。有关更多信息，请参阅《AWS 一般参考》中的 AWS Storage Gateway 端点和配额。	2020 年 5 月 7 日
支持 S3 Intelligent-Tiering 存储类	Storage Gateway 现在支持 S3 Intelligent-Tiering 存储类。S3 智能分层存储类可以通过自动将数据移至最具成本效益的存储访问层来优化存储成本，而不会影响性能或产生运营开销。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的可自动优化经常访问和不常访问对象的存储类。	2020 年 4 月 30 日

磁带网关的读写性能提升了两倍	Storage Gateway 将读写磁带网关上的虚拟磁带的性能提高了两倍，从而使您能够比之前更快地执行备份和还原。有关更多信息，请参阅《Storage Gateway 用户指南》中的磁带网关性能指导。	2020 年 4 月 23 日
支持自动磁带创建	Storage Gateway 现在可以自动创建新的虚拟磁带。磁带网关可以自动创建新的虚拟磁带，从而维持您配置的最小可用磁带数，然后将这些新磁带设为可由备份应用程序导入，从而使备份任务能够不间断地运行。有关更多信息，请参阅《Storage Gateway 用户指南》中的自动创建磁带。	2020 年 4 月 23 日
新 AWS 区域	Storage Gateway 现已在 AWS GovCloud（美国东部）地区推出。有关更多信息，请参阅《AWS 一般参考》中的 AWS Storage Gateway 端点和配额。	2020 年 3 月 12 日
支持基于 Linux 内核的虚拟机 (KVM) 管理程序	Storage Gateway 现在可将本地网关部署在 KVM 虚拟化平台上。KVM 上部署的网关与现有本地网关具有相同的功能和功能。有关更多信息，请参阅《Storage Gateway 用户指南》中的支持的虚拟机管理程序和主机要求。	2020 年 2 月 4 日

支持 VMware vSphere High Availability	Storage Gateway 现在支持 VMware 高可用性，从而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。有关更多信息，请参阅《Storage Gateway 用户指南》中的将 VMware vSphere High Availability 与 Storage Gateway 一起使用。此版本还包含性能改进。有关更多信息，请参阅《Storage Gateway 用户指南》中的性能。	2019 年 11 月 20 日
磁带网关的新 AWS 区域	磁带网关现已在南美洲（圣保罗）区域推出。有关更多信息，请参阅《AWS 一般参考》中的 AWS Storage Gateway 端点和配额。	2019 年 9 月 24 日
在 Linux 上支持 IBM Spectrum Protect 7.1.9，对于磁带网关，最大磁带大小增加到 5 TiB	除了在 Microsoft Windows 上运行之外，磁带网关现在还支持在 Linux 上运行的 IBM Spectrum Protect (Tivoli Storage Manager) 7.1.9。有关更多信息，请参阅《Storage Gateway 用户指南》中的使用 IBM Spectrum Protect 测试您的设置。此外，对于磁带网关，虚拟磁带的最大大小现在从 2.5 TiB 增加到 5 TiB。有关更多信息，请参阅《Storage Gateway 用户指南》中的磁带配额。	2019 年 9 月 10 日

支持 Amazon CloudWatch 日志	现在，您可以使用 Amazon CloudWatch 日志组配置文件网关，以获得有关错误以及网关及其资源的运行状况的通知。有关更多信息，请参阅 Storage Gateway 用户指南中的获取有关网关运行状况和亚马逊 CloudWatch 日志组错误的通知。	2019 年 9 月 4 日
新 AWS 区域	Storage Gateway 现已在亚太地区（香港）区域推出。有关更多信息，请参阅《AWS 一般参考》中的 AWS Storage Gateway 端点和配额。	2019 年 8 月 14 日
新 AWS 区域	Storage Gateway 现已在中东（巴林）区域推出。有关更多信息，请参阅《AWS 一般参考》中的 AWS Storage Gateway 端点和配额。	2019 年 7 月 29 日
支持在 Virtual Private Cloud (VPC) 中激活网关	现在，您可以在 VPC 中激活网关。您可以在本地软件设备和基于云的存储基础设施之间创建私有连接。有关更多信息，请参阅在 Virtual Private Cloud 中激活网关。	2019 年 6 月 20 日

支持将虚拟磁带从 S3 Glacier Flexible Retrieval 移动到 S3 Glacier Deep Archive	您现在可以将在 S3 Glacier Flexible Retrieval 存储类中存档的虚拟磁带转移到 S3 Glacier Deep Archive 存储类，从而实现经济高效且长期的数据留存。有关更多信息，请参阅将磁带从 S3 Glacier Flexible Retrieval 转移到 S3 Glacier Deep Archive。	2019 年 5 月 28 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) 来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
与 S3 Glacier Deep Archive 集成	磁带网关与 S3 Glacier Deep Archive 集成在一起。现在，您可以在 S3 Glacier Deep Archive 中存档虚拟磁带来实现长期数据留存。有关更多信息，请参阅存档虚拟磁带。	2019 年 3 月 27 日
Storage Gateway 硬件设备在欧洲推出	Storage Gateway 硬件设备现已在欧洲推出。有关更多信息，请参阅《AWS 一般参考》中的 AWS Storage Gateway 硬件设备区域。此外，您现在还可以将 Storage Gateway 硬件设备上的可用存储从 5 TB 增加到 12 TB，并将安装的铜质网卡更换为 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

与集成 AWS Backup	Storage Gateway 与集成 AWS Backup。现在，您可以使用备份使用 AWS Backup Storage Gateway 卷进行云支持的存储的本地业务应用程序。有关更多信息，请参阅备份您的卷。	2019 年 1 月 16 日
支持 Bacula Enterprise 和 IBM Spectrum Protect	磁带网关现在支持 Bacula Enterprise 和 IBM Spectrum Protect。Storage Gateway 现在还支持更新版本的 Veritas NetBackup、Veritas Backup Exec 和 Quest 备份。NetVault 现在，您可以使用这些备份应用程序将数据备份到 Amazon S3 并直接存档到脱机存储（S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）中。有关更多信息，请参阅使用备份软件来测试您的网关设置。	2018 年 11 月 13 日
支持 Storage Gateway 硬件设备	Storage Gateway 硬件设备包括在第三方服务器上预安装的 Storage Gateway 软件。您可以从 AWS Management Console管理设备。该设备可以承载文件、磁带和卷网关。有关更多信息，请参阅使用 Storage Gateway 硬件设备。	2018 年 9 月 18 日

与 Microsoft System Center 2016 Data Protection Manager (DPM) 的兼容性	磁带网关现在与 Microsoft System Center 2016 Data Protection Manager (DPM) 兼容。现在，您可以使用 Microsoft DPM 将数据备份到 Amazon S3 并直接存档到脱机存储（S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）中。有关更多信息，请参阅使用 Microsoft System Center Data Protection Manager 测试您的设置。	2018 年 7 月 18 日
支持服务器消息块 (SMB) 协议	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
支持文件共享、缓存卷和虚拟磁带加密	现在，您可以使用 AWS Key Management Service (AWS KMS) 对写入文件共享、缓存卷或虚拟磁带的数据进行加密。目前，您可以使用 AWS Storage Gateway API 执行此操作。有关更多信息，请参阅使用 AWS KMS进行数据加密。	2018 年 6 月 12 日

对 NovaStor DataCenter / Network 的支持	磁带网关现在支持 NovaStor DataCenter /Network。现在，你可以使用 NovaStor DataCenter /Network 版本 6.4 或 7.1 将数据备份到 Amazon S3，然后直接存档到离线存储（S3 Glacier 灵活检索或 S3 Glacier Deep Archive Deep Archive）。有关更多信息，请参阅使用 NovaStor DataCenter /Network 测试您的设置。	2018 年 5 月 24 日

早期更新

下表描述了 2018 年 5 月之前的每个 AWS Storage Gateway 用户指南发行版中的重要更改。

更改	描述	更改日期
支持 S3 One Zone_IA 存储类别	对于文件网关，您现在可以选择 S3 One Zone_IA 作为文件共享的默认存储类。使用此存储类，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
新的 区域	磁带网关现已在亚太地区（新加坡）区域推出。有关详细信息，请参阅AWS 区域。	2018 年 4 月 3 日
支持刷新缓存通知、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 Storage Gateway API 参考中的 RefreshCache.html。 借助文件网关，申请方或读取者（而不是存储桶拥有者）现在能够支付访问费用。 借助文件网关，您现在能够向映射到 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

更改	描述	更改日期
支持 Dell EMC NetWorker v9.x	磁带网关现在支持 Dell EMC NetWorker v9.x。现在，您可以使用 Dell EMC NetWorker v9.x 将数据备份到 Amazon S3，然后直接存档到离线存储（S3 Glacier 灵活检索或 S3 Glacier Deep Archive）。有关更多信息，请参阅使用 Dell EMC 测试您的设置 NetWorker。	2018 年 2 月 27 日
新的 区域	Storage Gateway 现已在欧洲（巴黎）区域推出。有关详细信息，请参阅AWS 区域。	2017 年 12 月 18 日
支持文件上传通知和 MIME 类型猜测	现在，写入 NFS 文件共享的所有文件均已上传至 Amazon S3 后，文件网关会向您发送通知。有关更多信息，请参阅 Storage Gateway API 参考NotifyWhenUploaded中的。 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	AWS Storage Gateway 现在支持 VMware ESXi 虚拟机管理程序版本 6.5。这是对版本 4.1、5.0、5.1、5.5 和 6.0 支持提供的补充。有关更多信息，请参阅 受支持的管理程序和主机要求。	2017 年 9 月 13 日
与 Commvault 11 兼容	磁带网关现在与 Commvault 11 兼容。现在，您可以使用 Commvault 将数据备份到 Amazon S3 并直接存档到脱机存储（S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）中。有关更多信息，请参阅使用 Commvault 测试您的设置。	2017 年 9 月 12 日
文件网关支持 Microsoft Hyper-V 管理程序	现在您可以在 Microsoft Hyper-V 管理程序上部署文件网关。有关信息，请参阅 受支持的管理程序和主机要求。	2017 年 6 月 22 日
支持在三至五个小时内从存档中检索磁带	对于磁带网关，您现在可以在三至五个小时内从存档中取回磁带。您还可以确定从备份应用程序或虚拟磁带库 (VTL) 写入到磁带中的数据量。有关更多信息，请参阅查看磁带使用情况。	2017 年 5 月 23 日

更改	描述	更改日期
新的 区域	Storage Gateway 现已在亚太地区（孟买）区域推出。有关详细信息，请参阅AWS 区域。	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RefreshCache中的。	2017 年 3 月 28 日
对克隆卷的支持	对于缓存卷网关， AWS Storage Gateway 现在支持从现有卷克隆卷的功能。有关克隆卷的更多信息，请参阅克隆卷。	2017 年 3 月 16 日
支持 Amazon EC2 上的文件网关	AWS Storage Gateway 现在提供了在 Amazon EC2 中部署文件网关的功能。您可以使用现在以社区 AMI 形式存在的 Storage Gateway Amazon 系统映像 (AMI) 在 Amazon EC2 中启动文件网关。有关如何创建文件网关并将其部署到 EC2 实例上的信息，请参阅创建和激活 Amazon S3 文件网关或创建和激活 Amazon FSx 文件网关。有关如何启动文件网关 AMI 的信息，请参阅在 Amazon EC2 主机上部署 S3 文件网关或在 Amazon EC2 主机上部署 FSx 文件网关。	2017 年 2 月 8 日
与 Arcserve 17 的兼容性	磁带网关现在与 Arcserve 17 兼容。您现在可使用 Arcserve 将数据备份到 Amazon S3 并直接存档到 S3 Glacier Flexible Retrieval。有关更多信息，请参阅使用 Arcserve Backup r17.0 测试您的设置。	2017 年 1 月 17 日
新的 区域	Storage Gateway 现已在欧洲（伦敦）区域推出。有关详细信息，请参阅AWS 区域。	2016 年 12 月 13 日
新的 区域	Storage Gateway 现已在加拿大（中部）区域推出。有关详细信息，请参阅AWS 区域。	2016 年 12 月 8 日

更改	描述	更改日期
支持文件网关	除了卷网关和磁带网关外，Storage Gateway 现在还提供文件网关。文件网关将服务和虚拟软件设备组合在一起，使您能够使用行业标准文件协议（例如，网络文件系统 (NFS)）在 Amazon S3 中存储和检索对象。利用网关，可以将 Amazon S3 中的对象作为 NFS 装载点上的文件进行访问。	2016 年 11 月 29 日
Backup Exec 16	磁带网关现与 Backup Exec 16 兼容。现在，您可以使用 Backup Exec 16 将数据备份到 Amazon S3 并直接存档到脱机存储（S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）中。有关更多信息，请参阅使用 Veritas Backup Exec 测试您的设置。	2016 年 11 月 7 日
与 Micro Focus (HPE) Data Protector 9.x 兼容	磁带网关现在与 Micro Focus (HPE) Data Protector 9.x 兼容。您现在可以使用 HPE Data Protector 将数据备份到 Amazon S3 并直接存档到 S3 Glacier Flexible Retrieva。有关更多信息，请参阅使用 Micro Focus (HPE) Data Protector 测试您的设置。	2016 年 11 月 2 日
新的 区域	Storage Gateway 现已在美国东部（俄亥俄州）区域推出。有关详细信息，请参阅AWS 区域。	2016 年 10 月 17 日
Storage Gateway 控制台重新设计	Storage Gateway 管理控制台经过了重新设计，您可以更加轻松地配置、管理和监控您的网关、卷和虚拟磁带。用户界面现在提供可筛选的视图，并提供指向集成 AWS 服务（例如 CloudWatch 和 Amazon EBS）的直接链接。有关更多信息，请参阅 报名参加 AWS Storage Gateway。	2016 年 8 月 30 日
与 Veeam Backup & Replication V9 Update 2 或更高版本的兼容性	磁带网关现在与 Veeam Backup & Replication V9 Update 2 或更高版本（即 9.0.0.1715 或更高版本）兼容。现在，您可以使用 Veeam Backup Replication V9 Update 2 或更高版本将数据备份到 Amazon S3 并直接存档到脱机存储（S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）中。有关更多信息，请参阅使用 Veeam Backup & Replication 测试您的设置。	2016 年 8 月 15 日

更改	描述	更改日期
加长格式的卷和快照 ID	Storage Gateway 引入了加长格式的卷和快照 ID。您可以为卷、快照和其他支持的 AWS 资源激活加长 ID 格式。有关更多信息，请参阅 了解 Storage Gateway 资源和资源 ID。	2016 年 4 月 25 日
新的 区域 支持存储最大 512 TiB 的存储卷 对 Storage Gateway 本地控制台的其他网关更新和增强	磁带网关现已在亚太（首尔）区域推出。有关更多信息，请参阅 AWS 区域。 对于存储卷，您现在最多可以创建 32 个存储卷，每个存储卷最大为 16 TiB，最大存储量为 512 TiB。有关更多信息，请参阅存储卷架构和AWS Storage Gateway 配额。 一个虚拟磁带库中所有磁带的总大小增加到 1 PiB。有关更多信息，请参阅 AWS Storage Gateway 配额。 您现在可以在 Storage Gateway 控制台上设置您的 VM 本地控制台的密码。有关信息，请参阅 从 Storage Gateway 控制台设置本地控制台密码。	2016 年 3 月 21 日
与 Dell EMC NetWorker 8.x 的兼容性	磁带网关现在与 Dell EMC NetWorker 8.x 兼容。现在，您可以使用 Dell EMC NetWorker 将数据备份到 Amazon S3，然后直接存档到离线存储（S3 Glacier 灵活检索或 S3 Glacier Deep Archive Deep Archive）。有关更多信息，请参阅使用 Dell EMC 测试您的设置 NetWorker。	2016 年 2 月 29 日

更改	描述	更改日期
对 VMware ESXi 管理程序 6.0 版和 Red Hat Enterprise Linux 7 iSCSI 启动程序的支持	AWS Storage Gateway 现在支持 VMware ESXi Hypervisor 版本 6.0 和红帽企业 Linux 7 iSCSI 启动器。有关更多信息，请参阅 受支持的管理程序和主机要求 和 受支持的 iSCSI 启动程序。	2015 年 10 月 20 日
调整内容	此版本包含以下改进：该文档现在包含结合了所有网关解决方案的常见管理任务的“管理已激活的网关”部分。在下文中，您可以找到有关如何在部署并激活网关后管理网关的说明。有关更多信息，请参阅 管理您的网关。	
支持存储最大 1024 TiB 的缓存卷 支持 VMware ESXi 管理程序中的 VMXNET3 (10 GbE) 网络适配器类型 性能增强 对 Storage Gateway 本地控制台的多项改进和更新	对于缓存卷，您现在最多可以创建 32 个存储卷，每个存储卷最大为 32 TiB，最大总存储为 1024 TiB。有关更多信息，请参阅缓存卷架构和AWS Storage Gateway 配额。 如果您的网关在 VMware ESXi 管理程序上托管，则可将该网关重新配置为使用 VMXNET3 适配器类型。有关更多信息，请参阅 为网关配置网络适配器。 Storage Gateway 的最高上传速率提高到了每秒 120 MB，最高下载速率提高到了每秒 20 MB。 Storage Gateway 本地控制台已更新并通过额外功能进行增强，从而有助于执行维护任务。有关更多信息，请参阅 配置网关网络。	2015 年 9 月 16 日
对标签的支持	Storage Gateway 现在支持资源标记。现在，您可以为网关、卷和虚拟磁带添加标签，以便更轻松地管理它们。有关更多信息，请参阅 标记 Storage Gateway 资源。	2015 年 9 月 2 日

更改	描述	更改日期
与 Quest（前身为戴尔）NetVault Backup 10.0 的兼容性	磁带网关现在与 Quest NetVault Backup 10.0 兼容。现在，你可以使用 Quest NetVault Backup 10.0 将数据备份到 Amazon S3，然后直接存档到离线存储（S3 Glacier 灵活检索或 S3 Glacier Deep Archive）。有关更多信息，请参阅使用 Quest NetVault Backup 测试您的设置。	2015 年 6 月 22 日
支持将 16 TiB 存储卷用于存储卷网关设置	Storage Gateway 现在支持将 16 TiB 存储卷用于存储卷网关设置。您现在最多可以创建 12 个 16 TiB 存储卷，最大存储空间为 192 TiB。有关更多信息，请参阅存储卷架构。	2015 年 6 月 3 日
支持 Storage Gateway 本地控制台上的系统资源检查	现在，您可以确定系统资源（虚拟 CPU 核心、根卷大小和 RAM）是否足够让网关正常运行。有关更多信息，请参阅查看您的网关系统资源状态或查看您的网关系统资源状态。	
支持 Red Hat Enterprise Linux 6 iSCSI 启动程序	Storage Gateway 现在支持 Red Hat Enterprise Linux 6 iSCSI 启动程序。有关更多信息，请参阅 要求。 此版本包括以下 Storage Gateway 改进和更新： • 在 Storage Gateway 控制台中，您现在可以查看上次成功将软件更新应用到网关的日期和时间。有关更多信息，请参阅 使用 AWS Storage Gateway 控制台管理网关更新。 • Storage Gateway 现在提供了 API，您可以使用该 API 来列出连接到存储卷的 iSCSI 启动程序。有关更多信息，请参阅 API 参考ListVolumeInitiators中的。	

更改	描述	更改日期
支持 Microsoft Hyper-V 管理程序版本 2012 和 2012 R2	Storage Gateway 现在支持 Microsoft Hyper-V 管理程序版本 2012 和 2012 R2。这是对 Microsoft Hyper-V 管理程序版本 2008 R2 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。	2015 年 4 月 30 日
与 Symantec Backup Exec 15 的兼容性	磁带网关现在与 Symantec Backup Exec 15 兼容。现在，您可以使用 Symantec Backup Exec 15 将数据备份到 Amazon S3 并直接存档到脱机存储（S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）中。有关更多信息，请参阅使用 Veritas Backup Exec 测试您的设置。	2015 年 4 月 6 日
存储卷的 CHAP 身份验证支持	Storage Gateway 现在支持为存储卷配置 CHAP 身份验证。有关更多信息，请参阅为卷配置 CHAP 身份验证。	2015 年 4 月 2 日
支持 VMware ESXi Hypervisor 版本 5.1 和 5.5	Storage Gateway 现在支持 VMware ESXi Hypervisor 5.1 和 5.5。这是对 VMware ESXi 管理程序版本 4.1 和 5.0 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。	2015 年 3 月 30 日
支持 Windows CHKDSK 实用工具	Storage Gateway 现在支持 Windows CHKDSK 实用工具。您可以使用此实用工具来验证卷的完整性并修复卷上的错误。有关更多信息，请参阅排查卷问题。	2015 年 3 月 04 日

更改	描述	更改日期
与集成 AWS CloudTrail 以捕获 API 调用	Storage Gateway 现已与集成 AWS CloudTrail。 AWS CloudTrail 捕获您的 Amazon Web Services 账户中由 Storage Gateway 或代表 Storage Gateway 发出的 API 调用，并将日志文件传输到您指定的亚马逊 S3 存储桶。有关更多信息，请参阅 登录和监控 AWS Storage Gateway。 此版本包括以下 Storage Gateway 改进和更新： • 现在，当网关缓存的驱动器发生更改时，将恢复在缓存存储中包含废数据（即包含尚未上传到 AWS的内容）的虚拟磁带。有关更多信息，请参阅从无法恢复的网关恢复虚拟磁带。	2014 年 12 月 16 日

更改	描述	更改日期
与更多备份软件和介质更换器的兼容性	磁带网关现在与以下备份软件兼容： • Symantec Backup Exec 2014 • Microsoft System Center 2012 R2 Data Protection Manager • Veeam Backup & Replication V7 • Veeam Backup & Replication V8 现在，您可以使用这四种备份软件产品和 Storage Gateway 虚拟磁带库 (VTL) 将数据备份到 Amazon S3 并直接存档到脱机存储（S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）中。有关更多信息，请参阅使用备份软件来测试您的网关设置。 Storage Gateway 现在提供了另一种可用于新备份软件的介质更换器。 此版本包括其他 AWS Storage Gateway 改进和更新。	2014 年 11 月 3 日
欧洲地区（法兰克福）区域	Storage Gateway 现已在欧洲（法兰克福）区域推出。有关详细信息，请参阅AWS 区域。	2014 年 10 月 23 日
调整内容	已创建对所有网关解决方案通用的“入门”章节。在下文中，您可以找到有关下载、部署和激活网关的说明。在部署和激活网关后，您可以继续参考特定于存储卷、缓存卷和磁带网关设置的进一步说明。有关更多信息，请参阅创建磁带网关。	2014 年 5 月 19 日

更改	描述	更改日期
与 Symantec Backup Exec 2012 兼容	磁带网关现在与 Symantec Backup Exec 2012 兼容。现在，您可以使用 Symantec Backup Exec 2012 将数据备份到 Amazon S3 并直接存档到脱机存储（S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）中。有关更多信息，请参阅使用 Veritas Backup Exec 测试您的设置。	2014 年 4 月 28 日
对 Windows Server 故障转移集群的支持 对 VMware ESX 启动程序的支持 支持在 Storage Gateway 本地控制台上执行配置任务	• 如果主机使用 Windows Server 失效转移集群 (WSFC) 协调访问，Storage Gateway 现在支持将多个主机与同一个卷关联。但是，若未使用 WSFC，则不能将多个主机与同一个卷关联。 • Storage Gateway 现在使您可以直接通过 ESX 主机管理存储连接。这提供了使用您的 VM 的来宾 OS 中驻留的启动程序的替代方法。 • Storage Gateway 现在支持在 Storage Gateway 本地控制台中执行配置任务。有关在本地部署的网关上执行配置任务的信息，请参阅 在 虚拟机本地控制台上执行任务 或 在 虚拟机本地控制台上执行任务。有关在 EC2 实例上部署的网关上执行配置任务的信息，请参阅 在 Amazon EC2 本地控制台上执行任务 或 在 Amazon EC2 本地控制台上执行任务。	2014 年 1 月 31 日

更改	描述	更改日期
支持虚拟磁带库 (VTL) 并引入 API 版本 2013-06-30	Storage Gateway 将本地软件设备与基于云的存储连接起来，将您的本地 IT 环境与 AWS 存储基础架构集成。除了卷网关（缓存卷和存储卷）外，Storage Gateway 现在还支持网关虚拟磁带库 (VTL)。对于每个网关，最多可为磁带网关配置 10 个虚拟磁带驱动器。每个虚拟磁带驱动器均可响应 SCSI 命令集，因此现有的本地备份应用程序无需修改即可工作。有关更多信息，请参阅《AWS Storage Gateway 用户指南》中的以下主题。 • 有关架构概述，请参阅磁带网关的工作原理（架构）。 • 要开始使用磁带网关，请参阅创建磁带网关。	2013 年 11 月 5 日
支持 Microsoft Hyper-V	Storage Gateway 现在可将本地网关部署在 Microsoft Hyper-V 虚拟化平台上。在 Microsoft Hyper-V 上部署的网关拥有的功能与现有的本地 Storage Gateway 完全相同。要开始用 Microsoft Hyper-V 部署网关，请参阅受支持的管理程序和主机要求。	2013 年 4 月 10 日
支持在 Amazon EC2 上部署网关	Storage Gateway 现在可以在 Amazon Elastic Compute Cloud (Amazon EC2) 中部署网关。您可以使用 AWS Marketplace 中提供的 Storage Gateway AMI 在 Amazon EC2 中启动网关实例。要开始使用 Storage Gateway AMI 部署网关，请参阅 部署 Amazon EC2 实例来托管卷网关。	2013 年 1 月 15 日

更改	描述	更改日期
支持缓存卷并推出了 API 版本 2012-06-30	在此版本中，Storage Gateway 引入了对缓存卷的支持。缓存卷可尽量避免扩展本地存储基础设施，还能为您的应用程序提供对其活动数据的低延迟访问。您可以创建容量高达 32 TiB 的存储卷，并从本地应用程序服务器将其安装为 iSCSI 设备。向缓存卷写入的数据将存储在 Amazon Simple Storage Service (Amazon S3) 中，而只有近期写入和读取的数据的缓存才会存储在本地存储硬件中。借助缓存卷，您可以对接受较高检索延迟的数据（例如不常访问的早期数据）使用 Amazon S3，同时为要求低延迟访问的数据在本地保留存储。 在此版本中，Storage Gateway 还引入了一个新的 API 版本，该版本除了支持当前的操作之外，还提供新操作来支持缓存卷。 有关两种 Storage Gateway 解决方案的更多信息，请参阅 卷网关的工作原理（架构）。 您也可以尝试测试设置。有关说明，请参阅创建磁带网关。	2012 年 10 月 29 日

更改	描述	更改日期
API 和 IAM 支持	在此版本中，Storage Gateway 引入了 API 支持以及对 AWS Identity and Access Management(IAM) 的支持。 • API 支持 - 您现在可以以编程方式配置和管理 Storage Gateway 资源。有关 API 的更多信息，请参阅《AWS Storage Gateway 用户指南》中的 Storage Gateway 的 API 参考。 • IAM 支持 - 利用 AWS Identity and Access Management (IAM)，您可以创建用户并通过 IAM 策略来管理用户对您的 Storage Gateway 资源的访问权限。有关 IAM 策略的示例，请参阅 AWS Storage Gateway 的身份和访问管理。有关 IAM 的更多信息，请参阅 AWS Identity and Access Management (IAM) 详情页面。	2012 年 5 月 9 日
支持静态 IP	您现在可以为本地网关指定静态 IP。有关更多信息，请参阅 配置网关网络。	2012 年 3 月 5 日
新指南	这是 AWS Storage Gateway 用户指南的首个版本。	2012 年 1 月 24 日

卷网关设备软件的发行说明

这些发行说明描述了每个版本的 T ay 设备中包含的新增和更新的功能、改进和修复。每个软件版本都由其发布日期和唯一版本号标识。

您可以通过在 Storage Gateway 控制台中查看网关的详细信息页面来确定网关的软件版本号，或者使用类似于以下内容的 AWS CLI 命令调用 DescribeGatewayInformationAPI 操作：

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

版本号将在 API 响应的`SoftwareVersion`字段中返回。

> **Note**
>
> 在以下情况下，网关不会报告软件版本信息：
>
> - 网关处于离线状态。
> - 网关正在运行不支持版本报告的旧软件。
> - 网关类型为 FSx 文件网关。

有关 T ateway V olume G ateway 更新的更多信息，包括如何修改网关的默认自动维护和更新计划，请参阅使用 Storage Gateway e Gateway 控制台管理网关更新。 AWS

发行日期	软件版本	发布说明
2024-05-28	2.9.0	• 缩短了软件更新期间的网关重启时间 • 减少了用于估算网络带宽的数据传输量
2024-05-08	2.8.3	• 解决了使用 SOCKS5 代理服务器时的云连接问题
2024-04-10	2.8.1	• 解决了 2.8.0 中引入的内存使用问题

发行日期	软件版本	发布说明
		• 安全补丁更新 • 改进了软件更新流程 • 修复了新网关缺少的网络时间协议 (NTP) 组件的问题
2024-03-06	2.8.0	• 新网关的操作系统更新 • 安全补丁更新
2023-12-19	2.7.0	• 新网关的操作系统更新
2023-12-14	2.6.6	• 维护版本