

---

# AWS Storage Gateway

用户指南

API Version 2013-06-30



## AWS Storage Gateway: 用户指南

Copyright © 2013 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

The following are trademarks or registered trademarks of Amazon: Amazon, Amazon.com, Amazon.com Design, Amazon DevPay, Amazon EC2, Amazon Web Services Design, AWS, CloudFront, EC2, Elastic Compute Cloud, Kindle, and Mechanical Turk. In addition, Amazon.com graphics, logos, page headers, button icons, scripts, and service names are trademarks, or trade dress of Amazon in the U.S. and/or other countries. Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon.

All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

---

什么是 AWS Storage Gateway ? .....	1
规划您的 AWS Storage Gateway 部署 .....	2
AWS Storage Gateway 运行原理 .....	3
卷网关 ( 网关缓存和网关存储 ) 架构 .....	3
网关缓存卷架构 .....	3
网关存储卷架构 .....	4
网关 VTL 架构 .....	5
要求 .....	7
可用的 AWS 区域 .....	8
定价 .....	9
访问 AWS Storage Gateway .....	9
卷网关 .....	10
入门 ( 卷网关 ) .....	10
注册 .....	11
尝试示例设置 ( 卷网关 ) .....	11
步骤 1 : 设置并激活网关 .....	12
选择网关配置 .....	12
VMware 主机 .....	13
预配置主机 .....	13
下载并部署 VM .....	13
预配置本地磁盘存储 ( 网关缓存 ) .....	21
预配置本地磁盘存储 ( 网关存储 ) .....	26
配置 VM 以使用半虚拟化的磁盘控制器 .....	31
激活网关 .....	32
Hyper-V 主机 .....	35
预配置主机 .....	35
下载并部署 VM .....	35
预配置本地磁盘存储 .....	45
激活网关 .....	56
步骤 2 : 创建卷 .....	62
网关缓存 .....	62
网关存储 .....	67
步骤 3 : 访问您的卷 .....	72
步骤 4 : 测试设置 .....	80
网关缓存 .....	80
网关存储 .....	83
我从这里可以继续进行哪些内容 ? .....	87
设置卷网关 ( 网关缓存和网关存储 ) .....	89
本地部署和激活网关 .....	89
VMware ESXi 主机 .....	90
下载和部署 VM .....	90
预配置本地磁盘存储 .....	90
网关缓存 .....	92
网关存储 .....	100
将 VM 配置为使用半虚拟化 .....	108
激活网关 .....	109
Hyper-V 主机 .....	113
下载和部署 VM .....	113
预配置本地磁盘存储 .....	113
网关缓存 .....	115
网关存储 .....	122
激活网关 .....	128
在 Amazon EC2 上部署并激活网关 .....	133
启动并激活 Amazon EC2 网关 AMI .....	134
管理您的 Amazon EC2 网关 .....	139
从实例中添加和删除 Amazon EBS 卷 .....	139
启用和禁用 AWS Support 的访问 .....	141
配置安全组 .....	142

在删除网关后清理资源 .....	142
配置上传缓冲区和缓存存储空间 .....	142
配置上传缓冲区 ( 网关缓存 ) .....	143
配置缓存存储空间 ( 网关缓存 ) .....	145
配置上传缓冲区 ( 网关存储 ) .....	146
创建存储卷 .....	149
网关缓存 .....	149
网关存储 .....	151
配置应用程序对存储卷的访问 .....	153
从 Windows 客户端连接到您的存储卷 .....	154
从 Red Hat 连接到您的存储卷 .....	156
为存储卷配置 CHAP 验证 .....	159
管理已激活的卷网关 .....	166
管理存储卷 .....	167
网关缓存 .....	171
网关存储 .....	173
管理上传缓冲区和缓存存储空间 ( 网关缓存 ) .....	177
添加并移除上传缓冲区容量 .....	179
添加缓存存储空间 .....	182
配置上传缓冲区 ( 网关存储 ) .....	182
添加并移除上传缓冲区容量 .....	184
使用快照 .....	187
查找快照 .....	188
使用适用于 Java 的 AWS 软件开发工具包查找快照 .....	190
使用适用于 .NET 的 AWS 软件开发工具包查找快照 .....	192
使用适用于 Windows PowerShell 的 AWS 工具查找快照 .....	194
编辑快照计划 .....	195
创建临时快照 .....	196
删除快照 .....	197
使用适用于 Java 的 AWS 软件开发工具包删除快照 .....	198
使用适用于 .NET 的 AWS 软件开发工具包删除快照 .....	201
使用适用于 Windows PowerShell 的 AWS 工具删除快照 .....	204
还原快照 .....	205
还原快照 .....	206
将快照还原为 Amazon EBS 卷 .....	208
执行维护任务 .....	208
关停并启动网关 .....	210
管理网关更新 .....	212
更新网关速率限制 .....	213
使用适用于 Java 的 AWS 软件开发工具包更新网关速率限制 .....	213
使用适用于 .NET 的 AWS 软件开发工具包更新网关速率限制 .....	215
使用适用于 Windows PowerShell 的 AWS 工具更新网关速率限制 .....	217
删除网关 .....	217
登录到网关本地控制台 .....	218
将网关路由选为通过代理 .....	222
允许通过防火墙和路由器进行网关访问 .....	223
将您的网关配置为使用静态 IP 地址 .....	224
测试网关到 Internet 的连接性 .....	226
同步您的网关 VM 时间 .....	227
针对多个网络适配器 (NIC) 配置网关 .....	229
使用多个网络适配器在网关中创建存储卷 .....	235
故障排除 .....	236
优化网关性能 .....	242
监控 AWS Storage Gateway .....	243
使用 Amazon CloudWatch 控制台 .....	244
衡量您的应用程序和网关间的性能。 .....	245
衡量网关和 AWS 间的性能 .....	246
监控上传缓冲区 .....	249

监控缓存卷 .....	252
理解 AWS Storage Gateway 指标 .....	253
网关 VTL .....	257
入门 ( 网关 VTL ) .....	257
注册 .....	258
尝试示例虚拟磁带库 (VTL) 设置 .....	258
步骤 1 : 部署 VM 并激活网关 VTL .....	259
选择网关 VTL 配置 .....	260
VMware 主机 .....	260
配置 VMware 主机 .....	260
下载并部署 VM .....	261
为 VM 配置本地存储 .....	269
激活网关 VTL .....	275
Hyper-V 主机 .....	278
配置 Hyper-V 主机 .....	278
下载并部署 VM .....	278
为 VM 配置本地存储 .....	288
激活网关 VTL .....	294
步骤 2 : 配置本地存储和警报 .....	300
步骤 3 : 创建虚拟磁带 .....	301
步骤 4 : 将 VTL 设备连接到 Windows 客户端 .....	302
步骤 5 : 测试设置 .....	304
配置 NetBackup 存储设备 .....	305
将数据备份到磁带 .....	306
将磁带存档 .....	310
从 VTS 检索存档的磁带 .....	310
从磁带还原数据 .....	311
步骤 6 : 在示例练习后进行清除 .....	312
我从这里可以继续哪些内容 ? .....	312
设置网关 VTL .....	313
本地部署和激活网关 .....	313
VMware ESXi 主机 .....	313
下载和部署 VM .....	314
预配置本地磁盘存储 .....	314
将 VM 配置为使用半虚拟化 .....	322
激活网关 VTL .....	323
Hyper-V 主机 .....	328
下载和部署 VM .....	328
预配置本地磁盘存储 .....	328
激活网关 VTL .....	334
在 Amazon EC2 上部署并激活网关 .....	341
配置上传缓冲区和缓存存储空间 .....	346
创建虚拟磁带 .....	347
连接到 VTL 设备 .....	348
从 Windows 客户端进行连接 .....	349
从 Red Hat 客户端连接到 VTL 设备 .....	351
配置 CHAP 身份验证 .....	353
管理已激活的网关 VTL .....	361
监控网关 VTL .....	362
使用 Amazon CloudWatch 控制台 .....	362
衡量网关 VTL 和 AWS 间的性能 .....	363
监控上传缓冲区 .....	365
监控缓存卷 .....	368
理解 AWS Storage Gateway 指标 .....	369
管理磁带 .....	371
在 VTL 中管理磁带 .....	371
创建磁带 .....	373
删除磁带 .....	373

将虚拟磁带存档 .....	374
取消磁带检索 .....	374
取消磁带存档 .....	375
恢复磁带 .....	375
管理 VTS 上的磁带 .....	376
检索磁带 .....	377
删除磁带 .....	378
执行网关 VTL 维护 .....	378
常见网关 VTL 维护任务 .....	378
管理上传缓冲区和缓存存储 .....	379
添加并移除上传缓冲区容量 .....	380
关停并启动网关 VTL .....	383
管理网关 VTL 更新 .....	384
更新带宽速率限制 .....	384
使用 AWS SDK for Java .....	385
使用 AWS SDK for .NET .....	387
使用 AWS Tools for Windows PowerShell .....	389
禁用网关 VTL .....	389
删除网关 VTL .....	390
网关 VTL 在本地运行时的维护任务 .....	390
登录到您的网关 VTL 本地控制台 .....	391
通过代理路由网关 VTL .....	394
允许网关 VTL 通过防火墙和路由器进行访问 .....	396
将您的网关 VTL 配置为使用静态 IP 地址 .....	396
测试您的网关 VTL 与 Internet 的连接 .....	399
同步 VM 时间 .....	399
配置您的网关 VTL 以使用多个网络适配器 (NIC) .....	401
优化网关 VTL 性能 .....	407
以 EC2 实例的形式运行时网关 VTL 的维护任务 .....	408
从网关 VTL 实例中添加和删除 Amazon EBS 卷 .....	408
允许和禁止 AWS Support 访问在 Amazon EC2 实例上运行的网关 .....	409
配置安全组 .....	410
在 EC2 网关 VTL 练习后进行清除 .....	410
故障排除 .....	411
访问控制 .....	415
API 参考 .....	418
必需的请求标头 .....	418
签名请求 .....	420
错误响应 .....	421
操作 .....	438
文档历史记录 .....	439
附录 .....	441
附录 A : vSphere 环境中的组件 .....	441
附录 B : 配置 VMware ESXi 主机 .....	442
附录 C : Hyper-V 环境中的组件 .....	446
附录 D : 配置 Hyper-V 主机 .....	447
附录 E : AWS Storage Gateway 资源 .....	456
附录 F : AWS Storage Gateway 限制 .....	457

# 什么是 AWS Storage Gateway ?

---

## Topics

- [您是 AWS Storage Gateway 的新用户吗？ \(p. 2\)](#)
- [规划您的 AWS Storage Gateway 部署 \(p. 2\)](#)
- [AWS Storage Gateway 的运行原理 \(架构\) \(p. 3\)](#)
- [要求 \(p. 7\)](#)
- [可用的 AWS 区域 \(p. 8\)](#)
- [AWS Storage Gateway 定价 \(p. 9\)](#)
- [访问 AWS Storage Gateway \(p. 9\)](#)

欢迎使用 *AWS Storage Gateway User Guide*。AWS Storage Gateway 将本地软件设施与基于云的存储设施相连接，从而提供本地 IT 环境和 Amazon Web Services (AWS) 存储基础设施间的无缝安全整合。您可以使用该服务安全地将数据存储在 AWS 云中以获得可扩展且经济实用的存储。AWS Storage Gateway 提供了基于卷的存储解决方案和基于磁带的存储解决方案：

- **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中作为 iSCSI 设备安装。该网关支持以下卷配置：
  - **网关缓存卷** – 在此情况下，将数据存储在 Amazon Simple Storage Service (Amazon S3) 中，并本地保留经常访问的数据子集的副本。网关缓存卷不仅能帮助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。
  - **网关存储卷** – 当需要对整个数据集进行低延迟访问时，您可以将本地网关配置为本地存储所有数据，然后以异步方式将此数据的时间点快照备份到 Amazon S3。此配置提供了耐久且价格低廉的场外备份，例如，当您出于灾难恢复目的需要替代容量时，可以在本地或从 Amazon EC2 恢复这些备份。
- **网关 - 虚拟磁带库 (VTL)** – 您可以经济高效且持久的方式在 Amazon Glacier 中存储存档并对数据进行长期备份。网关 VTL 提供了磁带基础设施，该基础设施可根据您的业务需求以无缝方式扩展，并可消除配置、扩展和维护物理磁带基础设施的操作负担。

您可以选择在本地将 AWS Storage Gateway 作为虚拟机 (VM) 设备运行，或在 AWS 中将其作为 EC2 实例运行。

有关架构概述，请参见 [AWS Storage Gateway 的运行原理 \(架构\) \(p. 3\)](#)。

AWS Storage Gateway 支持各种使用案例。有关更多信息，请转到 [AWS Storage Gateway 产品详细信息页](#)。

## 您是 AWS Storage Gateway 的新用户吗？

前一部分概述了 AWS Storage Gateway 提供的存储服务。有关这些服务的详细架构概览，请参见 [AWS Storage Gateway 的运行原理 \(架构\)](#) (p. 3)。

本文档根据网关类型分为两个主要部分：卷网关（网关缓存和网关存储）和网关 VTL。每一部分介绍了如何开始使用、设置和管理您的网关。“入门”为新用户提供了有关设置和使用完全运行的网关的说明。

- [卷网关 \(网关缓存和网关存储\)](#) (p. 10) (网关缓存和网关存储)
  - [卷网关入门 \(网关缓存卷和网关存储卷\)](#) (p. 10)
  - [设置卷网关 \(网关缓存和网关存储\)](#) (p. 89)
  - [管理已激活的卷网关 \(网关缓存和网关存储\)](#) (p. 166)
- [网关 - 虚拟磁带库 \(网关 VTL\)](#) (p. 257)
  - [入门 \(网关 VTL\)](#) (p. 257)
  - [设置网关 VTL](#) (p. 313)
  - [管理已激活的网关 VTL](#) (p. 361)

以上部分主要介绍了使用 AWS Management Console 进行的网关操作。若要以编程方式执行这些操作，请参见 [AWS Storage Gateway API Reference](#) 以了解有关支持的操作的信息。

## 规划您的 AWS Storage Gateway 部署

利用 AWS Storage Gateway 软件设备，您可以将现有本地应用程序基础设施与可扩展的、安全且经济实用的 AWS 云存储结合使用。

若要部署 AWS Storage Gateway 解决方案，您首先需要确定以下两项：

1. 存储解决方案 – 根据您的需求，您可以选择以下存储解决方案之一：

- [网关 VTL](#) – 如果您正在寻找经济实用且耐用的长期场外数据存档替代方法，则可以部署网关 VTL 解决方案。利用该解决方案提供的虚拟磁带库 (VTL) 接口，您可以通过现有的基于磁带的备份应用程序基础设施来将数据存储到您在网关上创建的虚拟磁带盒上。您可以轻松地在虚拟磁带架 (VTS) 中创建虚拟磁带、计划备份和存档磁带，而无需担心本地管理磁带以安排场外磁带发运。有关架构概述，请参见 [网关 - 虚拟磁带库 \(网关 VTL\) 架构](#) (p. 5)。
- [卷网关 \(网关缓存或网关存储\)](#) – 利用卷网关，您可以在 AWS 云中创建存储卷，可在该云中将本地应用程序作为 iSCSI 目标进行访问。提供了两个选项 — 网关缓存或网关存储。

利用网关缓存卷，可以将卷数据存储存储在 AWS 中，并将一小部分最近访问的数据存储在本地缓存中。这将允许对经常访问的数据集进行低延迟访问，并提供对存储在 AWS 中的整个数据集的无缝访问。这允许您扩展存储资源，而无需配置其他硬件。

利用网关存储卷，您可以本地存储整个卷数据，并将定期时间点备份（快照）存储在 AWS 中。在此模式中，您的本地存储是主存储，并且将提供对整个数据集的低延迟访问，而 AWS 存储是当数据中心发生灾难时可还原的备份。

有关卷网关的架构概述，请参见 [卷网关 \(网关缓存和网关存储\) 架构](#) (p. 3)。

2. 托管选项 – 您可以选择在本地将 AWS Storage Gateway 作为虚拟机 (VM) 设备运行，或在 AWS 中将其作为 Amazon EC2 实例运行。有关更多信息，请参见 [要求](#) (p. 7)。

EC2 实例上承载的网关对于灾难恢复很有用。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。AWS Storage Gateway 提供了包含网关 VM 映像的亚马逊系统映像 (AMI)。

此外，在配置主机以部署网关软件设备时，您将需要为网关 VM 分配足够的存储空间。如果您在防火墙后部署网关，则需要使网关 VM 能够访问某些端口。有关上述要求和其他要求的更多信息，请参见 [要求 \(p. 7\)](#)。

在规划过程中，建议您尝试示例设置。以下入门主题提供了设置网关的说明。

有关卷网关设置的信息，请参见 [卷网关入门 \( 网关缓存卷和网关存储卷 \) \(p. 10\)](#)。

有关网关 VTL 设置的信息，请参见 [入门 \( 网关 VTL \) \(p. 257\)](#)。

## AWS Storage Gateway 的运行原理 ( 架构 )

本部分提供了可用的 AWS Storage Gateway 解决方案的架构概述。

### Topics

- [卷网关 \( 网关缓存和网关存储 \) 架构 \(p. 3\)](#)
- [网关 - 虚拟磁带库 \( 网关 VTL \) 架构 \(p. 5\)](#)

## 卷网关 ( 网关缓存和网关存储 ) 架构

AWS Storage Gateway 提供了两种卷网关配置。在这两种配置下，所有数据都将安全存储到 AWS 中。主要差异在于本地存储的数据量。

### Topics

- [网关缓存卷架构 \(p. 3\)](#)
- [网关存储卷架构 \(p. 4\)](#)

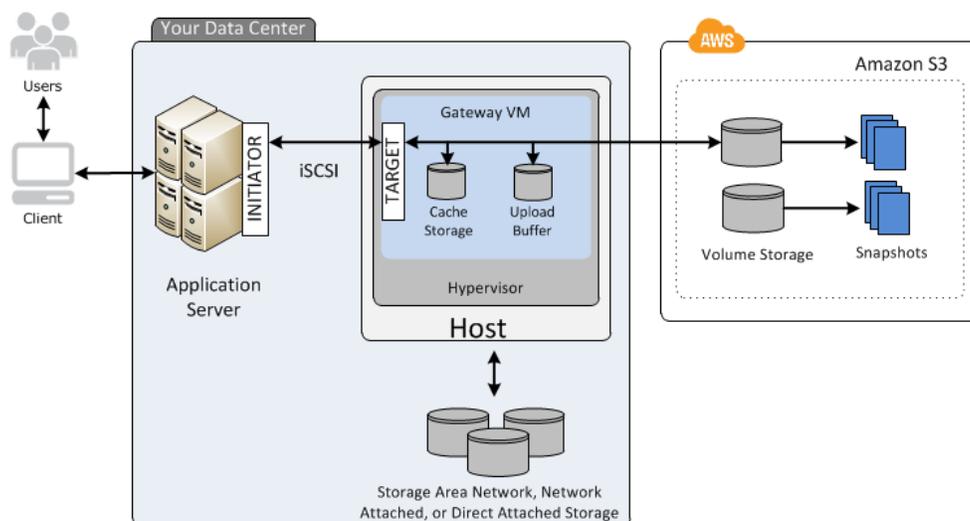
## 网关缓存卷架构

网关缓存卷可让您以主要数据存储的方式使用 Amazon S3，同时将经常访问的数据本地保留在存储网关中。网关缓存的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经常访问数据的低延迟访问。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。网关将这些卷中写入的数据存储在 Amazon S3 中，并将最近读取的数据保留在本地存储网关的缓存和上传缓冲区存储中。

网关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。为网关缓存卷配置的每个网关可以支持最多 20 个卷和总共 150 TiB 的卷存储。

在网关缓存卷解决方案中，AWS Storage Gateway 将您的所有本地应用程序数据保存在 Amazon S3 的存储卷中。

下图提供了 AWS Storage Gateway 缓存卷部署的概览。



在数据中心的主机上安装并激活 AWS Storage Gateway 的软件设施（虚拟机 (VM)）后，您可以使用 AWS Management Console 配置 Amazon S3 支持的存储卷。您还可以使用 AWS Storage Gateway API 或 AWS 软件开发工具包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：

- 由网关用作缓存存储空间的磁盘 – 由于您的应用程序会将数据写入 AWS 中的存储卷，因此网关会在将这些数据上传到 Amazon S3 之前，最初会将其存储到称作缓存存储空间的本地磁盘中。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。

缓存存储空间还让您的网关能够场内存储您的应用程序的最近访问数据，获得低延迟访问。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空间中的数据。

提供了一些准则，您可以使用这些准则确定您可以为缓存存储空间分配的磁盘空间量。一般而言，您至少应该分配 20% 的现有文件存储大小；不过，缓存存储空间应该大于上传缓冲区。这样可以确保缓存存储空间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。

- 由网关用作上传缓冲区的磁盘 – 为了准备对 Amazon S3 进行上传操作，网关还将传入数据存储称作上传缓冲区的中转区中。您的网关将这些缓冲区数据通过加密 SSL 连接上传到 AWS，然后以加密形式存储在 Amazon S3 中。

您可以对 Amazon S3 中的存储卷拍摄增量备份，亦即“快照”。这些时间点快照也以 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。您可以按预定或临时方式启动快照的拍摄。删除快照时，只会移除其他任何快照不需要的数据。

您可以在需要还原数据备份的情况下，将 Amazon EBS 快照还原为网关存储卷。我们计划在近期添加对 Amazon EC2 可部署网关的支持，以便您能够将快照还原为 Amazon EC2 网关存储卷。另外，对于大小约为 1 TiB 的快照，您可以将快照用作新的 Amazon EBS 卷的起点，随后将该卷连接到 Amazon EC2 实例。

所有的网关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) 进行安全加密。不过，您不能使用 Amazon S3 API 或借助 Amazon S3 控制台等其他工具访问这些数据。

## 网关存储卷架构

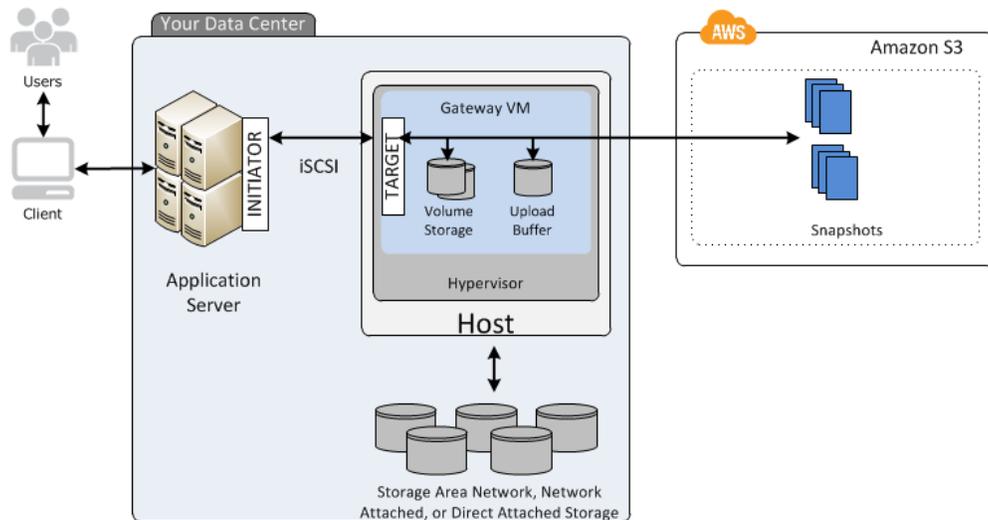
网关存储卷可让您在本地存储主要数据，同时将这些数据异步备份到 AWS。网关存储卷为您的场内应用程序提供对整个数据集的低延迟访问，同时提供持久的异地备份。您可以创建容量高达 1 TiB 的存储卷，

并从本地应用程序服务器将其安装为 iSCSI 设备。写入到您的网关存储卷的数据保存在场内存储硬件中，并且以 Amazon EBS 快照的形式异步备份到 Amazon S3。

网关存储卷的大小范围可以是 1 GiB 到 1 TiB，并且必须四舍五入到最接近的 GiB 值。为网关存储卷配置的每个网关可以支持最多 12 个卷和总共 12 TiB 的卷存储

在网关存储卷解决方案中，您在数据中心场内维护卷存储空间。亦即，您将所有的应用程序场内保存在存储硬件中。网关然后将数据上传到 AWS 云，进行具有成本效益的备份和快速灾难恢复。如果您希望将数据本地保存在场内，这就是个理想的解决方案，因为您需要对所有数据的低延迟访问并在 AWS 中维护备份。

以下示意图提供了 AWS Storage Gateway 存储卷部署的概览



在数据中心的主机上安装并激活 AWS Storage Gateway 的软件设施（虚拟机 (VM)）后，您可以创建网关存储卷并将其映射到本地直接连接的存储空间 (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。您然后将将这些存储卷作为 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。

为了准备将数据上传到 Amazon S3，网关还将传入数据存储称为上传缓冲区的中转区中。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 SSL 连接将数据从上传缓冲区上传到运行于 AWS 云中的 AWS Storage Gateway 服务中。随后，该服务将数据加密存储在 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。您可以按预定或临时方式启动快照的拍摄。删除快照时，只会删除其他快照都不需要的数据。

您可以在需要还原数据备份的情况下，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，并随后将卷连接到 Amazon EC2 实例。

## 网关 - 虚拟磁带库（网关 VTL）架构

网关 VTL 提供了一种耐用且经济使用的数据存档解决方案以便在 AWS 云中对数据进行存档。利用该解决方案提供的 VTL 接口，您可以通过现有的基于磁带的备份应用程序基础设施来将数据存储到您在网关 VTL 上创建的虚拟磁带盒上。使用媒体转换器和磁带驱动器预配置每个网关 VTL，可将这些媒体转换器和磁带驱动器作为 iSCSI 设备用于现有客户端备份应用程序。根据需要添加磁带盒以存档数据。

下图提供了网关 VTL 部署的概览



该图标识了下列网关 VTL 组件：

- 虚拟磁带 – 虚拟磁带类似于物理磁带盒；但是，虚拟磁带数据将存储在 AWS 云中。与物理磁带一样，虚拟磁带可以为空，也可以将数据写入到其中。您可以通过使用 AWS Storage Gateway 控制台创建虚拟磁带，也可以借助 AWS Storage Gateway API 以编程方式创建虚拟磁带。每个网关一次性可包含最多 1500 个磁带或最多 150 TiB 磁带数据。每个虚拟磁带的大小（可在创建磁带时进行配置）介于 100 GiB 和 2.5 TiB 之间。
- 虚拟磁带库 (VTL) – VTL 类似于带机械臂和磁带驱动器的本地可用的物理磁带库，以及存储了虚拟磁带的集合。每个网关 VTL 均附带了一个 VTL。

您创建的虚拟磁带将显示在网关的 VTL 中。VTL 中的磁带由 Amazon S3 进行备份：当备份软件将数据写入网关时，该网关会本地存储数据，然后以异步方式将数据上传到 VTL 中的虚拟磁带（即 Amazon Simple Storage Service (Amazon S3)）中。

- 磁带驱动器 – VTL 磁带驱动器类似于可对此单执行 I/O 和搜索操作的物理磁带驱动器。每个 VTL 均附带一组磁带驱动器（供 10 个），这些驱动器可作为 iSCSI 设备用于您的备份应用程序。
- 媒体转换器 – VTL 媒体转换器类似于将磁带在物理磁带库的存储槽和磁带驱动器之间移动的机器人。每个 VTL 均附带一个媒体转换器，该转换器可作为 iSCSI 设备用于您的备份应用程序。
- 虚拟磁带架 (VTS) – VTS 类似于场外磁带支撑设备。您可以将网关 VTL 中的磁带存档到 VTS，如果需要，还可将 VTS 中的磁带检索回网关的 VTL。
- 存档磁带 – 在备份软件弹出磁带时，网关会将磁带移至您在激活网关时指定的 AWS 区域中的 VTS 以便长期存储。VTS 中的磁带将存储在 Amazon Glacier 中，后者是一项用于数据存档和备份的成本极低的存储服务。
- 检索磁带 – 无法直接读取存档到 VTS 的磁带。若要读取存档的磁带，您必须先通过使用 AWS Storage Gateway 控制台或使用 AWS Storage Gateway API 将其检索到网关 VTL。检索到的磁带在约 24 小时后将可在 VTL 中可用。

对于每个 AWS 区域，您在账户中都有一个 VTS。例如，如果您在同一个 AWS 区域中创建多个网关，则一个 VTS 将会为所有网关保留弹出的磁带。如果您在不同的 AWS 区域中创建网关，则每个 AWS 区域将有一个 VTS。

在部署并激活网关 VTL 后，您在本地应用程序服务器上将虚拟磁带驱动器和媒体转换器作为 iSCSI 设备安装。根据需要创建虚拟磁带，然后使用现有备份软件应用程序将数据写入虚拟磁带中。媒体转换器在虚拟磁带驱动器中加载和卸载虚拟磁带以进行读取和写入操作。

## 为网关 VM 分配本地磁盘

网关 VM 需要为以下目的分配的本地磁盘：

- 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 的数据的持久存储器。  
如果您的应用程序读取虚拟磁带中的数据，则网关会将数据保存到缓存存储空间。网关将最近访问的数据存储在缓存存储中以实现低延迟访问。如果您的应用程序请求磁带数据，则网关在从 AWS 下载数据前会先检查缓存存储空间中的数据。
- 上传缓冲区 – 上传缓冲区在数据上传到虚拟磁带前为网关提供一个暂存区域。上传缓冲区对于创建可用来从意外故障中恢复磁带的还原点也非常重要。有关更多信息，请参见 [发生故障的网关恢复虚拟磁带 \(p. 375\)](#)。

当备份应用程序将数据写入网关时，网关会先将数据复制到缓存存储空间和上传缓冲区，然后再确认已完成对备份应用程序的写入操作。

提供了用于确定您应为缓存存储空间和上传缓冲区分配的磁盘空间量的相关指南。有关更多信息，请参见 [在 VMware ESXi 主机上为 AWS Storage Gateway VTL VM 配置本地磁盘存储 \(p. 314\)](#)。

## 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。

### 托管选项

您可以选择在本地将 AWS Storage Gateway 作为虚拟机 (VM) 设备运行，或在 AWS 中将其作为 EC2 实例运行。对于本地托管，AWS Storage Gateway 支持 VMware ESXi 管理程序和 Microsoft Hyper-V 2008 R2 管理程序。有关更多信息，请参见 [要求 \(p. 7\)](#)。

EC2 实例上承载的网关对于灾难恢复很有用。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。AWS Storage Gateway 提供了包含网关 VM 映像的亚马逊系统映像 (AMI)。

本指南中的以下入门练习将本地部署网关：

- 有关卷网关 (网关缓存、网关存储) 的信息，请参见 [卷网关入门 \(网关缓存卷和网关存储卷\) \(p. 10\)](#)
- 有关网关 VTL 的信息，请参见 [入门 \(网关 VTL\) \(p. 257\)](#)

以下主题提供了有关将网关作为 EC2 实例运行的信息：

- 有关卷网关 (网关缓存) 的信息，请参见 [在 Amazon EC2 上部署并激活 AWS Storage Gateway \(p. 133\)](#)
- 有关网关 VTL 的信息，请参见 [启动并激活 Amazon EC2 网关 AMI \(p. 134\)](#)

### 托管要求

您可以选择在本地将 AWS Storage Gateway 作为虚拟机设备运行，或在 AWS 中将其作为 EC2 实例运行。

AWS Storage Gateway 支持通过以下主机进行本地部署：

- VMware ESXi 管理程序 (版本 4.1 或 5.0)。免费 VMware 版本可从 [VMware 网站](#) 获取。您还需要 VMware vSphere 客户端才能连接到主机。
- Microsoft Hyper-V 2008 R2。[Microsoft 下载中心](#) 免费提供单独的 Hyper-V 版本下载。您将需要 Windows 客户端计算机上的 Microsoft Hyper-V Manager 才能连接到主机。

您必须确保在其上部署网关 VM 的基础硬件能够用于以下资源：

- 分配给 VM 的四个虚拟处理器
- 分配给 VM 的 7.5 GB RAM
- 75GB 磁盘空间，适用于安装虚拟机映像和系统数据。

如果将网关作为 EC2 实例运行，则实例类型必须是 AWS Storage Gateway 的 AWS Marketplace 页面上描述的类型之一，否则实例将不会启动。例如，AWS Storage Gateway 支持 EC2 实例类型 Standard XL (m1.xlarge) 和更高版本。

### 存储要求

除了 VM 的 75 GB 磁盘空间外，您还需要网关的其他磁盘。

- 对于网关缓存卷配置，您需要用于本地缓存的存储空间和上传缓冲区。有关更多信息，请参见 [预配置本地磁盘 \(网关缓存\) \(p. 92\)](#)。

- 对于网关存储卷配置，您将需要用于整个数据集的存储空间和上传缓冲区。有关上传缓冲区大小的信息，请参见 [配置上传缓冲区的大小 \(网关存储\)](#) (p. 104)。
- 对于网关 VTL 配置，您将需要本地缓存存储空间和上传缓冲区。有关更多信息，请参见 [在 VMware ESXi 主机上为 AWS Storage Gateway VTL VM 配置本地磁盘存储](#) (p. 314)。

## 支持的 iSCSI 启动程序

当部署卷网关（网关缓存或网关存储）时，可以在网关上创建 iSCSI 存储卷。当部署网关 VTL 时，使用一个媒体转换器和十个磁带驱动器预配置网关。这些磁带驱动器和媒体转换器可作为 iSCSI 设备用于您的现有客户端备份应用程序。为了连接到这些 iSCSI 设备，AWS Storage Gateway 支持以下 iSCSI 启动程序：

- Windows Server 2008 和 Windows 7
- Red Hat Enterprise Linux 5

## 网络要求

网关使用特定端口来执行其操作。如果在防火墙后部署网关，请确保这些端口是可访问的：

- vSphere 客户端和 Hyper-V 管理器使用网关上的端口 80 和 443 来与主机进行通信。如果客户端无法连接到主机，则将无法在主机上部署网关。
- 在从 AWS Storage Gateway 控制台激活网关时，使用端口 80。
- 端口 3260 是应用程序服务器用来连接到 iSCSI 目标的默认端口。

## 备份软件 (仅网关 VTL)

通常，您将使用备份应用程序通过网关 VTL 对磁带进行读取、写入和管理操作。本文档中的示例使用 Symantec NetBackup 7.5 版备份软件。有关 Symantec NetBackup 的信息，请转到 [Symantec 网站](#)。



### Note

虽然 AWS 仅利用网关 VTL 测试 NetBackup 软件，但其他备份软件也可以运行。

## 可用的 AWS 区域

AWS Storage Gateway 将卷、快照和磁带数据存储在于激活的 AWS 区域中。下表列出了激活网关时可选择的 AWS 区域：

地区名称	地区字符串	网关缓存	网关存储	网关 VTL
美国东部 (弗吉尼亚北部) 地区	us-east-1	X	X	X
US West (Northern California) Region	us-west-1	X	X	X
US West (Oregon) Region	us-west-2	X	X	X
EU (Ireland) Region	eu-west-1	X	X	X

地区名称	地区字符串	网关缓存	网关存储	网关 VTL
Asia Pacific (Singapore) Region	ap-southeast-1	X	X	
Asia Pacific (Sydney) Region	ap-southeast-2	X	X	X
Asia Pacific (Tokyo) Region	ap-northeast-1	X	X	X
南美洲 ( 圣保罗 )	sa-east-1	X	X	

## AWS Storage Gateway 定价

有关定价的当前信息，请转到 [AWS Storage Gateway 详细信息页](#)。

## 访问 AWS Storage Gateway

可以使用 AWS Storage Gateway 控制台执行各种网关配置和管理任务。本指南的“入门”和其他部分使用控制台来阐释网关功能。

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，请参见 [AWS Storage Gateway 的 API 参考 \(p. 418\)](#)。

您还可以使用 AWS 软件开发工具包开发与 AWS 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 AWS Storage Gateway API 以简化您的编程任务。有关开发工具包库文件的信息，请参阅 [示例代码库](#)。

## 卷网关 ( 网关缓存和网关存储 )

---

### Topics

- [卷网关入门 \( 网关缓存卷和网关存储卷 \) \(p. 10\)](#)
- [设置卷网关 \( 网关缓存和网关存储 \) \(p. 89\)](#)
- [管理已激活的卷网关 \( 网关缓存和网关存储 \) \(p. 166\)](#)

本部分介绍如何部署、设置和管理网关缓存卷或网关存储卷。

利用网关缓存解决方案，您可以创建存储卷，并将其作为 iSCSI 设备从本地应用程序服务器进行安装。网关将您写入网关缓存卷的数据存储在 Amazon Simple Storage Service (Amazon S3) 中，并且仅将经常访问数据的缓存存储在本地存储硬件中。

利用网关存储解决方案，您可以将所有数据本地存储在本地存储硬件的存储卷中。网关定期拍摄快照作为增量备份，并将其存储在 Amazon S3 中。

## 卷网关入门 ( 网关缓存卷和网关存储卷 )

### Topics

- [AWS Storage Gateway 的入门要求 \(p. 11\)](#)
- [AWS Storage Gateway 的入门视频 \(p. 11\)](#)
- [注册 AWS Storage Gateway \(p. 11\)](#)
- [尝试示例设置 \( 卷网关 \) \(p. 11\)](#)
- [我从这里可以继续哪些内容？ \(p. 87\)](#)

“入门”一节说明如何设置 AWS Storage Gateway 虚拟机 (VM)、激活它和配置它，以使网关正常工作。您通过将示例数据经由 iSCSI 连接本地保存到您的存储卷并且拍摄时间点备份快照来测试设置。网关将快照上传到 AWS。要完成练习，需要将快照还原到新卷，并了解 AWS Storage Gateway 如何使您可还原数据。

在练习结束时，网关将正常工作，并具有以下示例配置：

- 一个 AWS Storage Gateway VM，部署在 VMware ESXi 虚拟机监控程序主机或 Microsoft Hyper-V 主机上
- 一个为缓存的卷或存储的卷而激活的网关

- 您的 Windows 客户端经由 iSCSI 连接到您的本地存储卷中的一个。



#### Note

在按本入门部分中的步骤进行操作时，将使用 AWS Storage Gateway 控制台中的设置并激活网关向导。在向导的几个步骤中，您将在控制台外执行任务，然后返回控制台。如果会话超时或浏览器关闭，您可以返回到控制台，从上一步骤继续执行。

## AWS Storage Gateway 的入门要求

要按此处所述部署、配置和测试 AWS Storage Gateway 设置，需要一个主机以部署 AWS Storage Gateway VM。您还需要客户端来将网关 VM 部署在主机上并测试设置。有关更多信息，请参阅 [要求 \(p. 7\)](#)。

本练习假定使用动态主机配置协议 (DHCP) 自动配置网关 IP 地址。如果部署 AWS Storage Gateway 的环境要求为网关指定静态 IP 地址，则可照做。有关配置网关以使用静态 IP 地址的详细信息，请参阅 [将您的 AWS Storage Gateway 配置为使用静态 IP 地址 \(p. 224\)](#)。

## AWS Storage Gateway 的入门视频

在开始本教程之前，可观看这段入门视频，了解端到端设置体验：[AWS Storage Gateway 入门](#)

## 注册 AWS Storage Gateway

注册 AWS Storage Gateway 账户即创建了 Amazon Web Service (AWS) 账户，您可以使用该账户访问所有的 Amazon Web Services、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。如果您已有账户，可跳过本步骤。

如需注册 AWS Storage Gateway

1. 请转至 <http://aws.amazon.com>，然后单击“注册”。
2. 按照屏幕上的说明进行操作。

在注册过程中，您会接到一个电话，需要您使用电话按键输入 PIN 码。

## 尝试示例设置（卷网关）

在本练习中，您要做出两个决策，其中决定要遵照的途径。您必须确定：

- 将用于托管 Storage Gateway 的本地虚拟化平台。
- 将配置的 Storage Gateway 的类型，即缓存网关或存储网关。有关这些网关设置的详细信息，请参阅 [AWS Storage Gateway 的运行原理（架构）\(p. 3\)](#)。

本部分提供了有关两种受到支持的虚拟平台（VMware ESXi 和 Microsoft Hyper-V）以及两种类型网关配置（缓存或者存储网关）的说明。

#### Topics

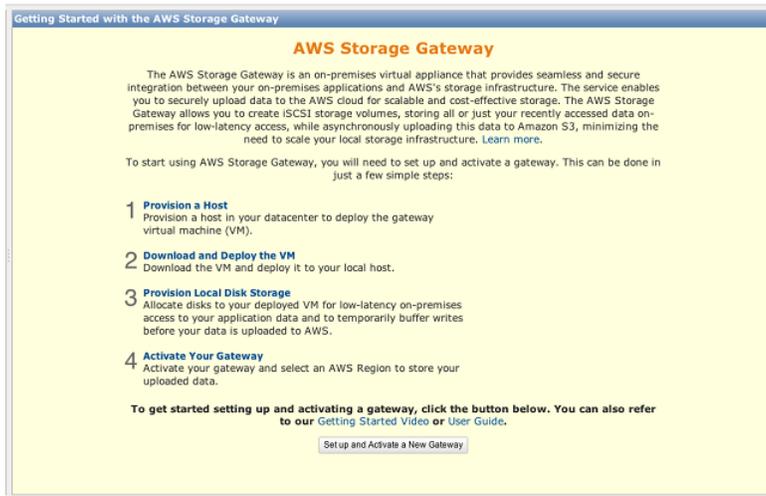
- [步骤 1：设置并激活 AWS Storage Gateway \(p. 12\)](#)
- [步骤 2：使用 AWS Storage Gateway 控制台创建卷 \(p. 62\)](#)
- [步骤 3：访问您的 AWS Storage Gateway 卷 \(p. 72\)](#)
- [步骤 4：测试设置 \(p. 80\)](#)

## 步骤 1 : 设置并激活 AWS Storage Gateway

### Topics

- [选择网关配置 \(p. 12\)](#)
- [设置和激活 \( VMware 主机 \) \(p. 13\)](#)
- [设置和激活 \( Hyper-V 主机 \) \(p. 35\)](#)

本练习要求您使用 AWS Storage Gateway 控制台下载最新的网关 VM 并激活您的网关。转到 <http://console.aws.amazon.com/storagegateway> 上的控制台。如果您注册了服务但尚未激活网关，控制台将在您着手部署网关的情况下显示以下页面。



如果已激活网关，则不会看到上一页。而是可通过在导航窗格中单击部署新网关，部署并激活新网关。



### 选择网关配置

#### 选择网关配置

1. 在设置并激活网关向导中的配置主机步骤中，选择网关缓存卷或网关存储卷，然后单击继续。



选择网关配置后，接下来决定要在其上部署网关的虚拟化平台。VMware ESXi [设置和激活 \( VMware 主机 \) \(p. 13\)](#)和 Microsoft Hyper-V 虚拟化 [设置和激活 \( Hyper-V 主机 \) \(p. 35\)](#)上同时支持网关缓存卷和网关存储卷。

2. 在下一页上，单击下一步以配置主机。

如需...	单击此处。
设置并激活 VMWare 主机	<a href="#">设置和激活 ( VMware 主机 ) (p. 13)</a>
设置并激活 Hyper-V 主机	<a href="#">设置和激活 ( Hyper-V 主机 ) (p. 35)</a>

## 设置和激活 (VMware 主机)

在本部分中，您将预配置场内 VMware 主机、向主机下载和部署网关 VM、配置网关 VM 并进行激活。

### 配置 VMware 主机以部署 AWS Storage Gateway VM

在本步骤中，您在数据中心创建 VMware 主机，用来部署网关虚拟机 (VM)。

如需预配置主机

1. 核查最低主机要求。有关更多信息，请参见 [要求 \(p. 7\)](#)。
2. 使用 VMware ESXi 管理程序在数据中心设置主机。

本指南中的附录提供安装管理程序操作系统的最低限度指导。有关更多信息，请参见 [附录 B：为 AWS Storage Gateway 配置 VMware ESXi 主机 \(p. 442\)](#)。



#### Note

如果计划部署使用 VMware High Availability (HA) 进行故障转移保护的 AWS Storage Gateway，请参阅 [AWS Storage Gateway 和 VMware High Availability 一起使用 \(p. 90\)](#)。在本教程中，您将 AWS Storage Gateway VM 部署在未配置集群或故障转移的单个主机上。

### 下载 AWS Storage Gateway VM 并将其部署到您的主机上

以 VMware ESX .ova 软件包形式提供 AWS Storage Gateway 虚拟机。本部分介绍如何下载 .ova 文件到本地、将其部署到主机以及同步 VM 时间和主机时间。



#### Important

要成功激活网关，就需要同步 VM 时间和主机时间。

### 下载 AWS Storage Gateway VM

如需下载该 VM

1. 在 [AWS Storage Gateway](#) 控制台的设置并激活网关向导中，导航到下载并部署 VM 页。
2. 选择我要在 VMware ESXi 上运行 AWS Storage Gateway，然后单击继续。

The screenshot shows a web-based wizard titled "Setup and Activate Gateway". At the top, there is a progress bar with four steps: "PROVISION HOST", "DOWNLOAD AND DEPLOY VM" (which is currently active and highlighted), "PROVISION LOCAL DISK STORAGE", and "ACTIVATE GATEWAY". Below the progress bar, the text reads "Select a virtualization platform to run the AWS Storage Gateway Virtual Machine (VM)". There are two radio button options: "I want to run the AWS Storage Gateway on VMWare ESXi" (which is selected) and "I want to run the AWS Storage Gateway on Microsoft Hyper-V". At the bottom left, there is a "Back" button, and at the bottom right, there is a "Continue" button.

3. 单击下载以下载一个 .zip 文件，其中包含 .ova 文件。将 .zip 保存到您的计算机上的某个位置。



#### Note

该 .zip 文件大小超过 500 MB，根据网速的不同，下载该文件可能需要一些时间。



## 将 AWS Storage Gateway VM 部署到您的主机

1. 连接到您的管理程序主机：



### Note

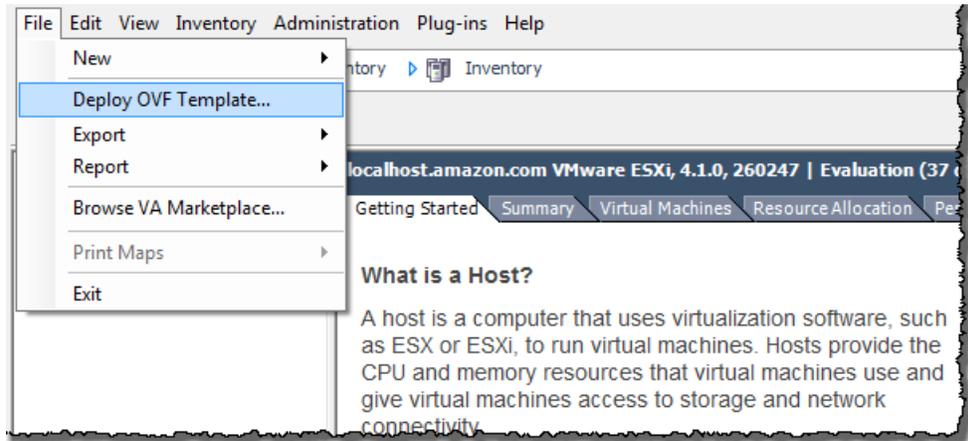
根据所用虚拟机监控程序版本的不同，这些过程中显示的图形用户界面 (GUI) 可能略有不同。

- a. 在您的 Windows 客户端上启动 VMware vSphere client。
- b. 在登录对话框中输入主机 IP 地址并在相应字段中输入登录证书。
- c. 单击登录。

您的 vSphere 客户端现已连接到您的主计算机。

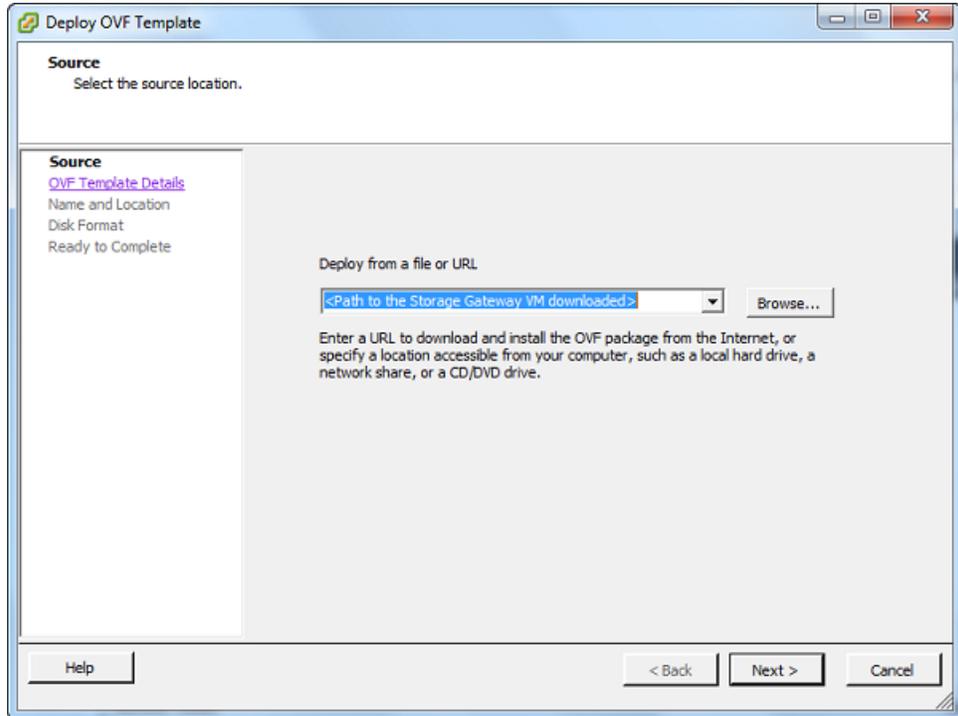
2. 将 AWS Storage Gateway VM 部署到主机上：

- a. 从 vSphere 客户端的文件菜单中，单击部署 OVF 模板。



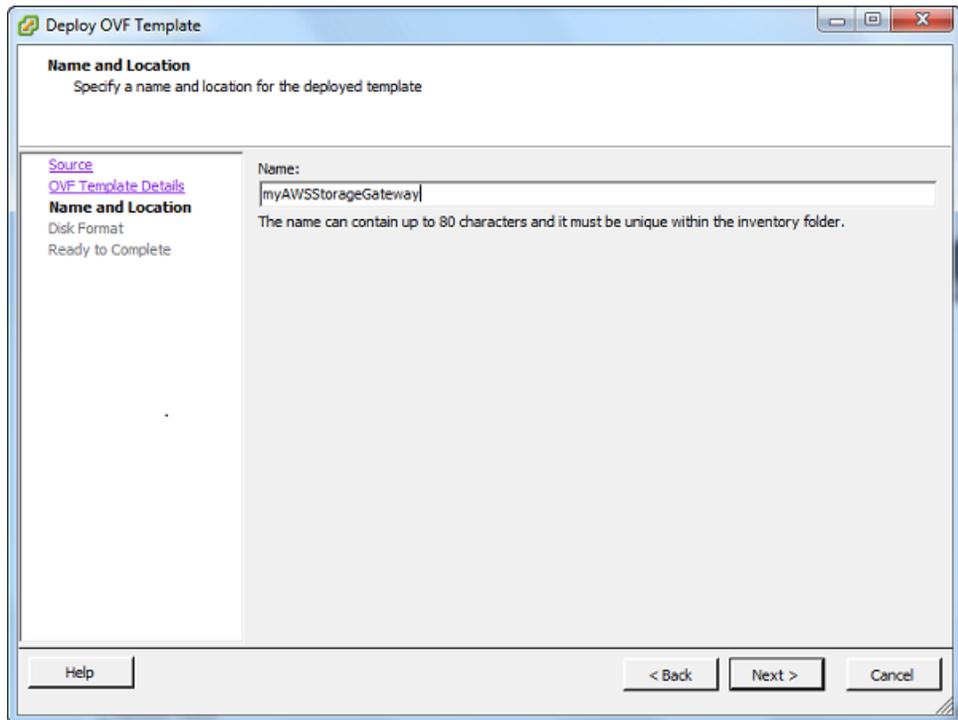
此操作将打开部署 OVF 模板向导。向导是让您提供部署 VM 所需信息的一系列步骤。

- b. 在源窗格中，提供 AWS Storage Gateway .ova 软件包的文件路径，然后单击下一步。



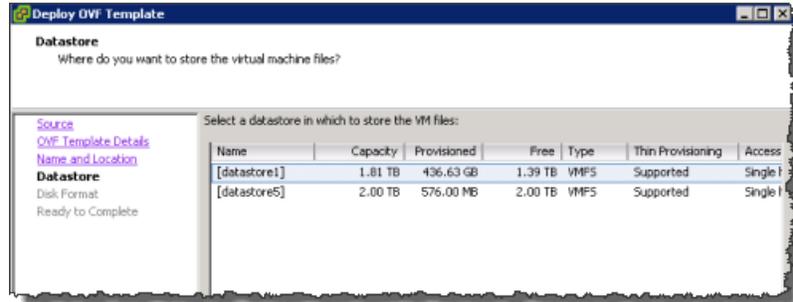
- c. 在 OVF 模板详细信息窗格中，单击下一步。
- d. 在名称和位置窗格中的名称字段中，输入 VM 名称，然后单击下一步。

该 VM 名称显示在 vSphere 客户端中。但是，AWS Storage Gateway 在任何位置均不使用此名称。



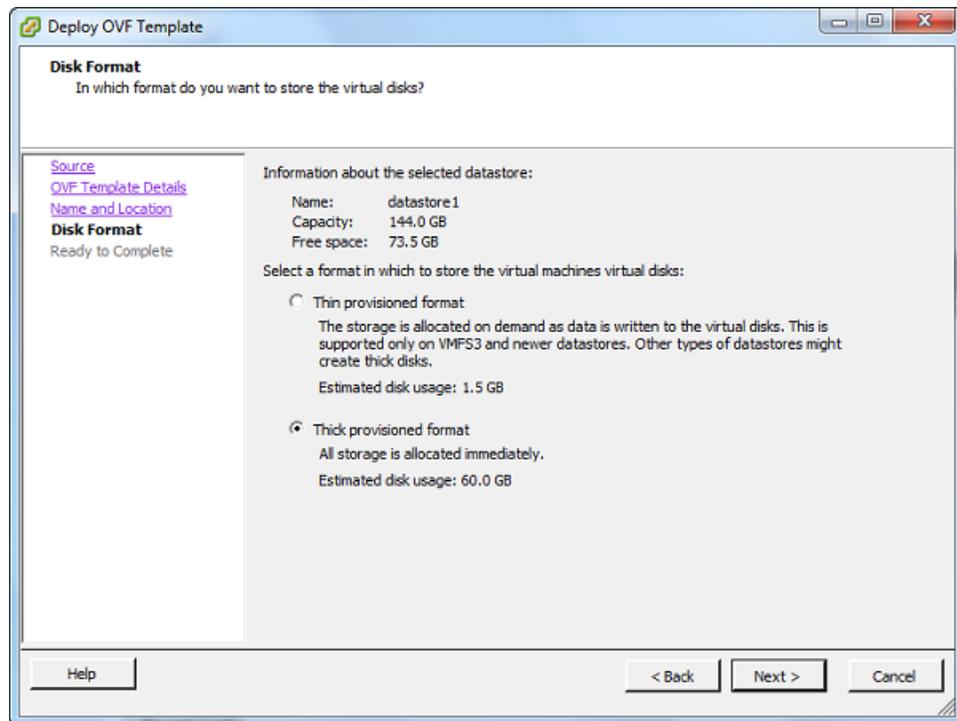
- e. 仅在主机具有多个数据存储时，才会显示以下数据存储窗格。在此窗格中，选择要从中部署 VM 的数据存储，然后单击下一步。如果您的主机仅有一个数据存储，请跳到下一步。

数据存储是底层物理存储资源的虚拟表示形式。下例展示一个主机，它具有两个数据存储：datastore1 和 datastore2。



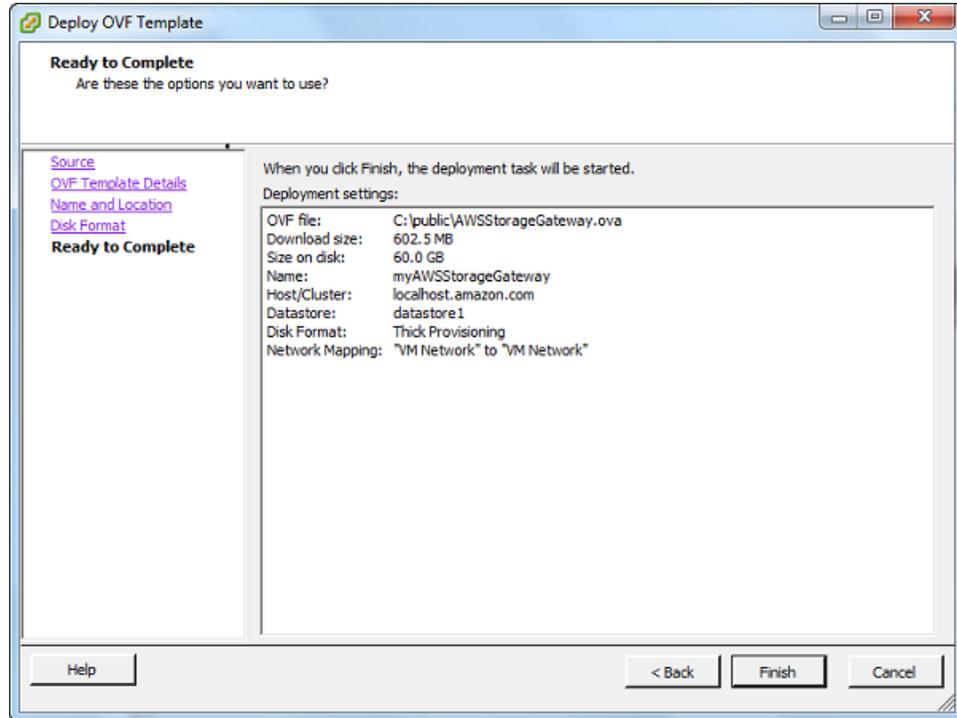
- f. 在磁盘格式化窗格中，选择完全配置格式，然后单击下一步。

选择存储自动配置时，磁盘空间立即分配，从而取得更好的性能。反之，自动精简配置按需分配存储空间。按需分配可能会影响 AWS Storage Gateway 的正常运行。因此，为使 AWS Storage Gateway 正常运行，必须以完全配置格式存储虚拟机磁盘。

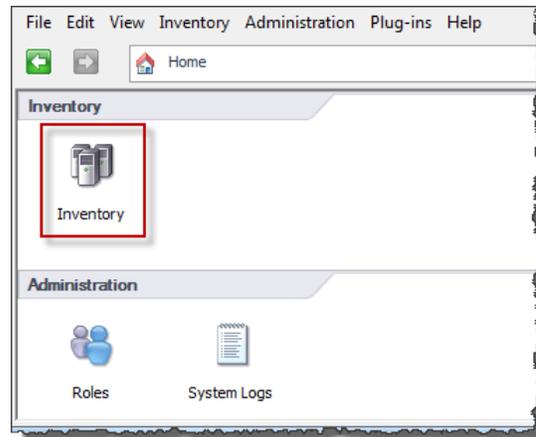


- g. 在已准备好完成窗格中，单击完成。

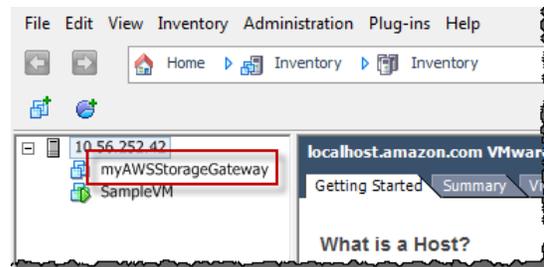
随后开始向您的主机部署 AWS Storage Gateway VM。



- h. 查看新 VM 的详细信息。
- i. 根据 vSphere 客户端状态的不同，可能需要先单击清点图标才能查看包含新 VM 的主机数据元。



- ii. 扩展主机数据元，查看新 VM 的详细信息。



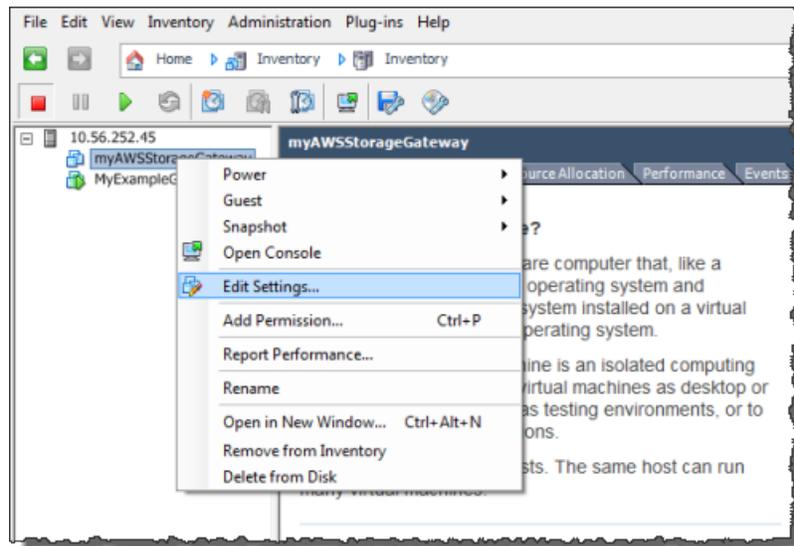
## 将 VM 时间与主机时间同步

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。成功激活网关需要同步 VM 和主机时间。在本步骤中，您首先将 VM 时间与主机时间同步。然后检查主机时间。如果需要，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。

如需将 VM 时间与主机时间同步

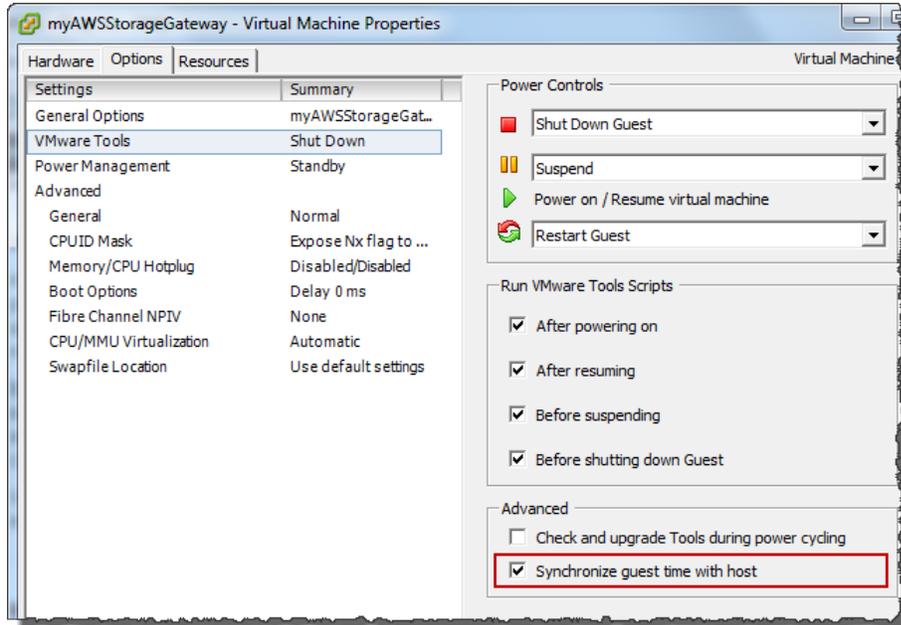
1. 配置您的 VM 时间。
  - a. 在 vSphere 客户端中，右键单击网关 VM 的名称，然后选择编辑设置。

随后将打开虚拟机属性对话框。



- b. 在选项选项卡中，从选项列表中选择 VMware 工具。
- c. 选中将来宾时间与主机同步选项，然后单击确定。

VM 时间与主机进行同步。

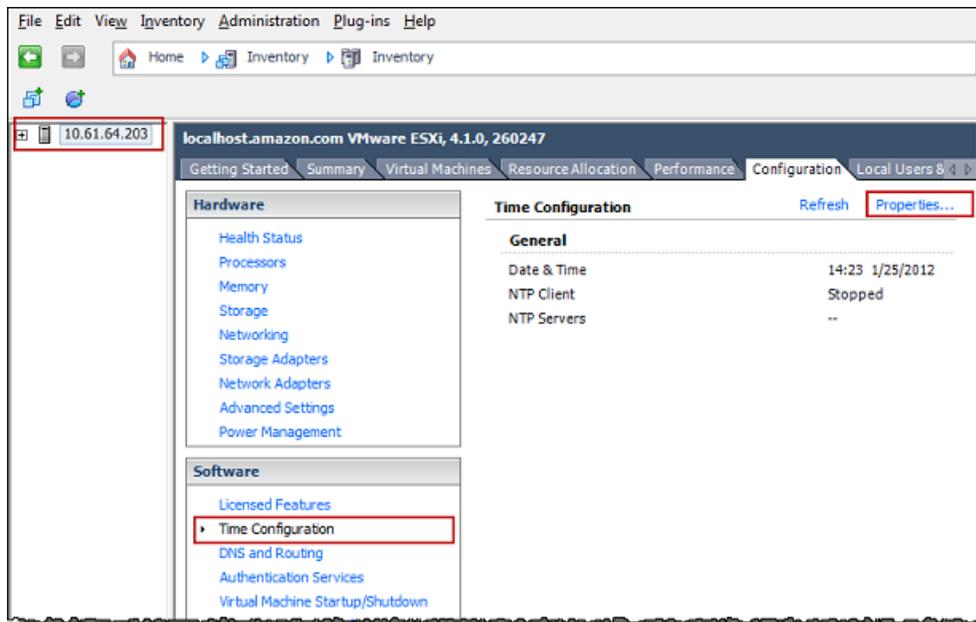


## 2. 配置主机时间。

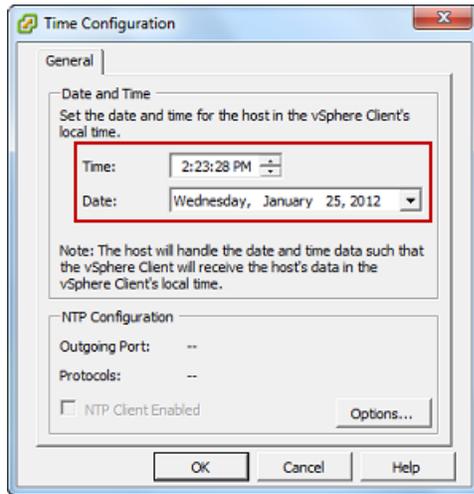
请注意，确保您设置了正确的主机时间。如果您尚未配置主机时间，请使用下面的步骤进行设置并将其与 NTP 服务器同步。

- 在 VMware vSphere 客户端中，在左侧窗格中选择 vSphere 主机节点，然后选择配置选项卡。
- 在软件面板中选择时间配置。
- 单击属性链接。

随后将显示时间配置对话框。

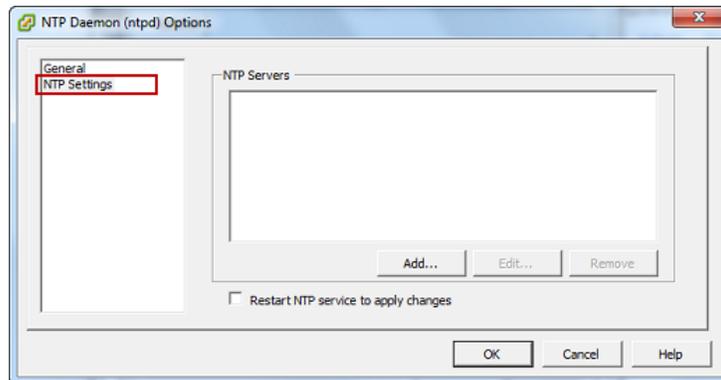


- d. 在日期和时间窗格中设置日期和时间。



- e. 将主机配置为自动与网络时间协议 (NTP) 服务器同步：

- i. 在时间配置对话框中单击选项。
- ii. 在 NTP 守护程序(ntpd)选项对话框中的左侧窗格中选择 NTP 设置。



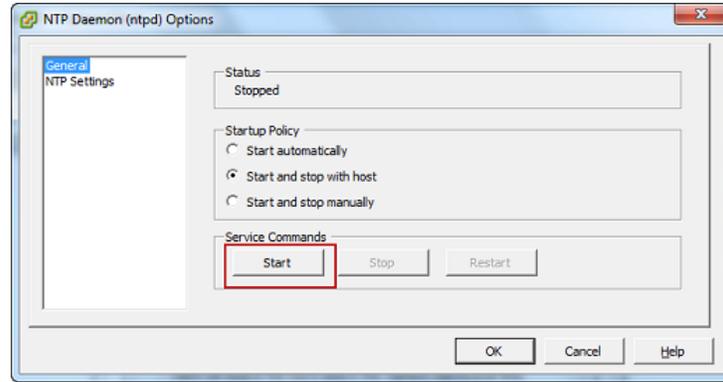
- iii. 单击添加以添加新 NTP 服务器。
- iv. 在添加 NTP 服务器对话框中，输入某个 NTP 服务器的 IP 地址或完全限定域名，然后单击确定。

可使用 `pool.ntp.org`，如本例所示。



- v. 在 NTP 守护程序(ntpd)选项对话框中的左侧窗格中单击常规。
- vi. 在服务命令窗格中，单击启动以启动服务。

请注意如果您稍后更改或添加另一 NTP 服务器参考，就需要重启服务才能使用新服务器。



- f. 单击确定以关闭 NTP 守护程序(ntpd)选项对话框。
- g. 单击确定以关闭时间配置对话框。

如需...	单击此处。
为网关缓存配置本地磁盘存储	<a href="#">预配置本地磁盘存储 (网关缓存架构) (p. 21)</a>
为网关存储配置本地磁盘存储	<a href="#">预配置本地磁盘存储 (网关存储架构) (p. 26)</a>

### 预配置本地磁盘存储 (网关缓存架构)

在下面的步骤中，您将给部署的网关 VM 分配本地磁盘。完成这些步骤后，您便成功添加了两个虚拟磁盘。

在本练习中，您向专供网关使用的 VM 分配 20 GiB 作为缓存存储，10 GiB 作为上传缓冲区。



#### Important

在本教程中，您给 VM 分配用作缓存存储空间和上传缓冲区的虚拟磁盘大小不适合实际工作负载。我们强烈建议您至少分配 150 GiB 的上传缓冲区。缓存存储空间的大小应根据上传缓冲区的大小而定。在本教程后面的步骤 ([针对实际工作负载配置网关存储的大小 \(p. 87\)](#)) 中，您将了解如何针对真实工作负载适当地调整缓存存储和上传缓冲区的大小。

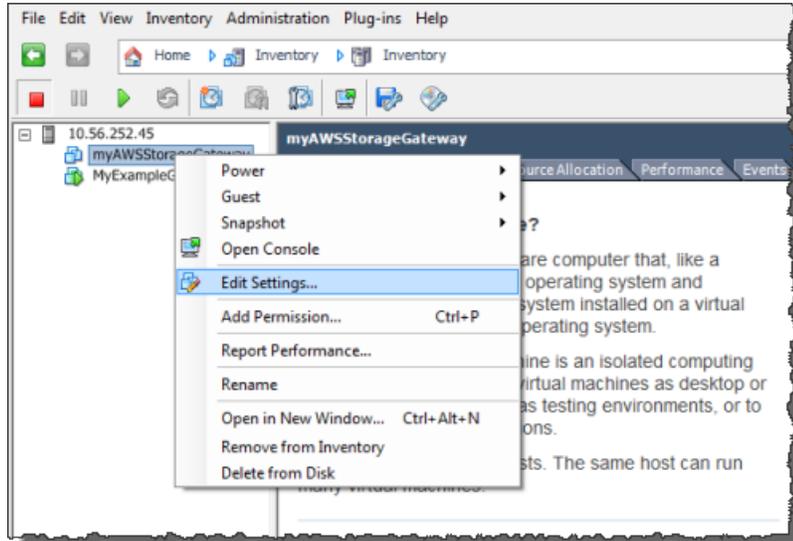
### 为缓冲存储区分配本地磁盘

您经常访问的应用程序数据在本地维护。您必须在 VM 上分配一个磁盘，作为存储这些数据的缓存。本节说明如何从直接连接存储 (DAS) 磁盘添加虚拟磁盘。使用下面的指导预配置一个磁盘，以便存储您的应用程序数据。有关从现有的存储区域网络 (SAN) 连接 iSCSI 卷，以使您可在这一步使用这些卷的说明，请参阅 [如需添加新的 iSCSI 目标 \(p. 443\)](#)。

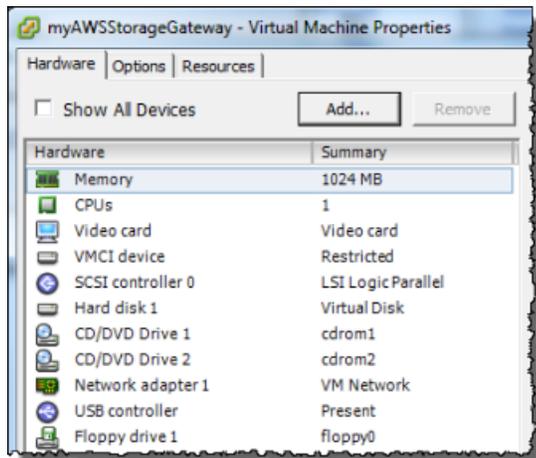
在本练习中，您向 VM 分配一个 20 GiB 的虚拟磁盘。

#### 如需将本地磁盘分配为缓存

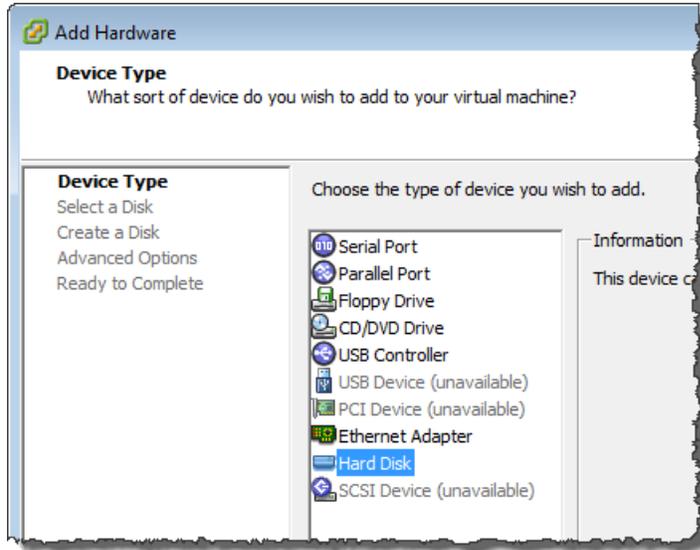
1. 启动 VMware vSphere 客户端并连接到您的主机。
2. 在客户端中，右键单击网关 VM 的名称，然后单击编辑设置。



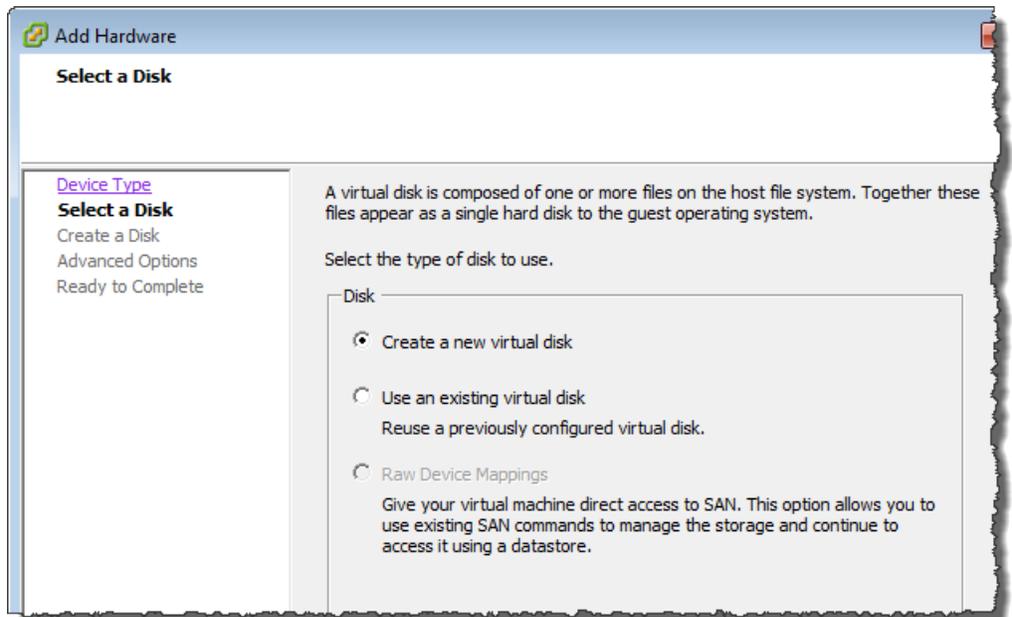
3. 在虚拟机属性对话框的硬件选项卡中，单击添加以添加一个设备。



4. 根据添加硬件向导添加磁盘：
  - a. 在设备类型窗格中，单击硬盘以添加一个磁盘，然后单击下一步。



- b. 在选择磁盘窗格中，选择新建虚拟磁盘，然后单击下一步。



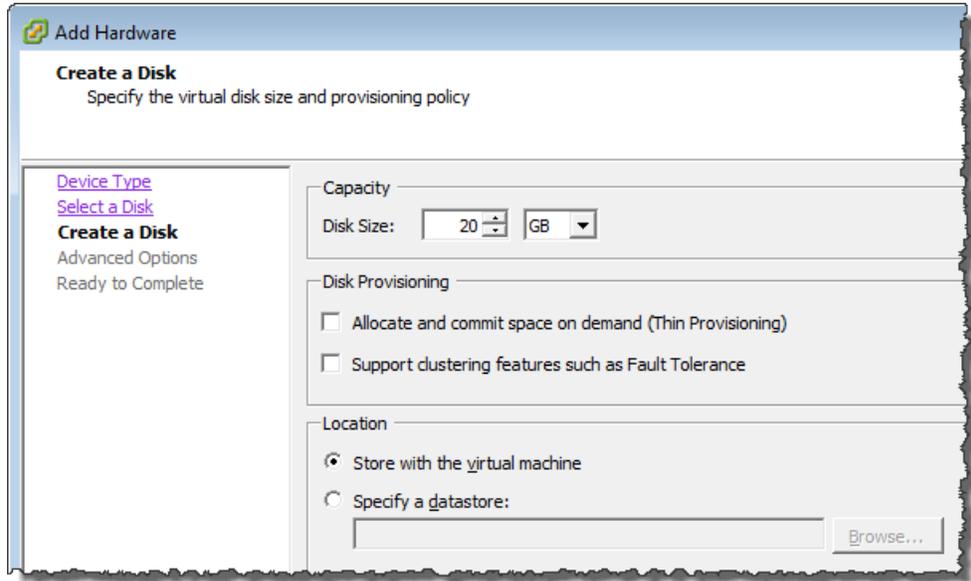
- c. 在创建磁盘窗格中，将磁盘的大小指定为 20 GiB，然后单击下一步。

选择存储自动配置时，磁盘空间立即分配，从而取得更好的性能。反之，自动精简配置按需分配存储空间。按需分配可能会影响 AWS Storage Gateway 的正常运行。因此，为使 AWS Storage Gateway 正常运行，必须以完全配置格式存储虚拟机磁盘。

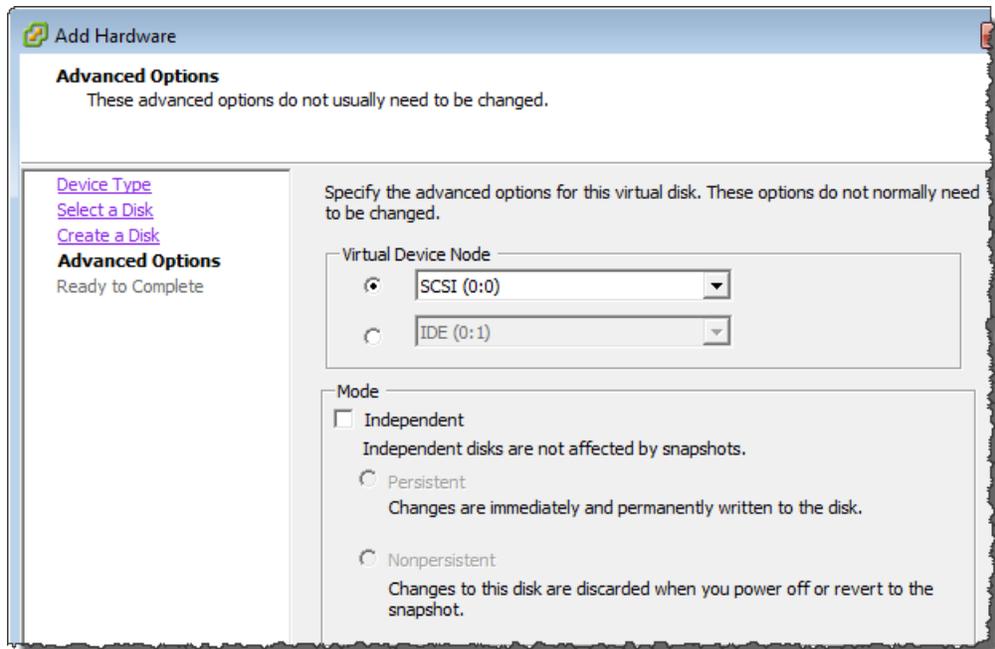


#### Note

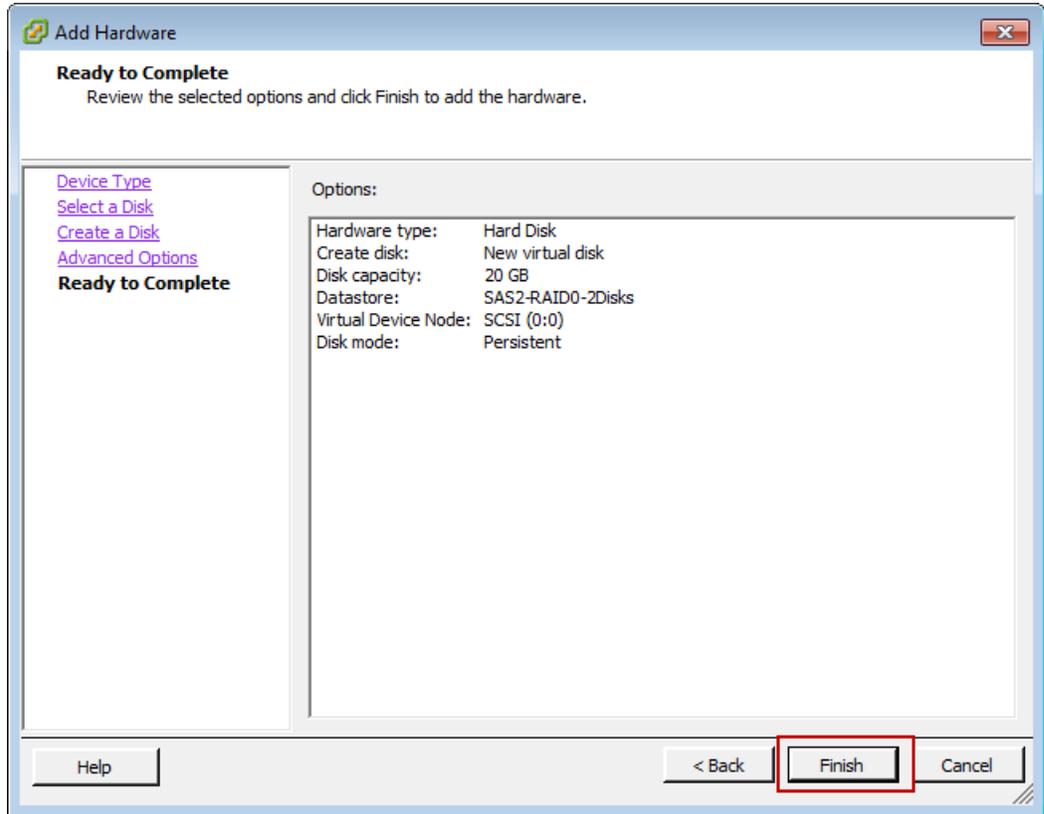
在本例设置中，将磁盘的位置与虚拟机存储在一起。对于实际工作负载，我们强烈建议您不要使用相同的底层物理存储磁盘预配置本地磁盘。根据托管环境的不同，为您在本步骤中预配置的磁盘选择不同的数据存储设备可能更好。有关更多信息，请参阅 [预配置本地磁盘 \( 网关缓存 \)](#) (p. 92)。



- d. 在高级选项窗格中，接受默认值，然后单击下一步。



- e. 在已准备好完成窗格中，接受默认值，然后单击完成。



- f. 在虚拟机属性对话框中，单击确定以完成添加磁盘。

### 为上传缓冲区分配本地磁盘

网关在上传快照到 AWS 时，需要缓存空间以临时存储数据。这一空间称为上传缓冲区。您必须给 VM 添加虚拟磁盘，专供 VM 使用。网关需要的上传缓冲区大小取决于您指定的经常访问数据的缓存。有关相关准则，请参阅[配置上传缓冲区的大小 \(网关缓存\)](#) (p. 97)。

在本练习中，您向专供网关使用的 VM 分配一个 10 GiB 的虚拟磁盘。在向导的创建磁盘窗格中，输入 10 GiB 作为磁盘大小。

如需将本地磁盘分配为上传缓冲区

- 重复前一节 ([如需将本地磁盘分配为缓存](#) (p. 21)) 中的步骤以向网关添加另一个虚拟磁盘。

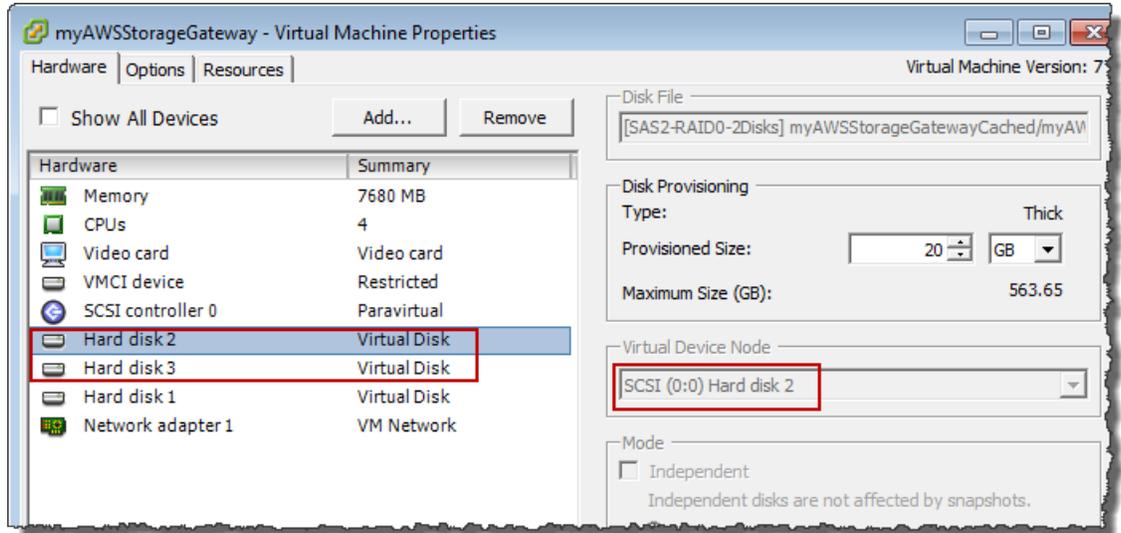
### 验证网关 VM 有两个磁盘

本练习的其余部分要求您已向网关 VM 分配两个磁盘。您可以使用下面的可选步骤验证已给网关 VM 分配好两个磁盘。如果需要分配其他磁盘，则重复[如需将本地磁盘分配为缓存](#) (p. 21) 过程中的步骤。

如需验证 VM 有两个磁盘

1. 在客户端中，右键单击网关 VM 的名称，然后单击编辑设置。
2. 在虚拟机属性对话框的硬件选项卡中，确认硬件列表中显示硬盘 2 和硬盘 3。

这两个磁盘随后将在 AWS Storage Gateway 控制台使用，并在下拉列表中显示为 SCSI (0:0) 和 SCSI (0:1)。



### 预配置本地磁盘存储 ( 网关存储架构 )

在下面的步骤中，您将给部署的网关 VM 分配本地磁盘。完成这些步骤后，您便成功添加了两个虚拟磁盘。

### 为存储卷分配本地磁盘 ( 用于您的应用程序数据 )

您所有的应用程序数据均在本地维护。您必须给 VM 分配磁盘，以便存储应用程序数据。本节说明如何从直接连接存储 (DAS) 磁盘添加虚拟磁盘。使用下面的指导预配置一个磁盘，以便存储您的应用程序数据。有关从现有的存储区域网络 (SAN) 连接 iSCSI 卷，以使您可在这一步使用这些卷的说明，请参阅[如需添加新的 iSCSI 目标 \(p. 443\)](#)。

在本练习中，您向 VM 分配一个 2 GiB 的虚拟磁盘用于存储应用程序数据，向 VM 分配一个 10 GiB 的上传缓冲区专供网关使用。

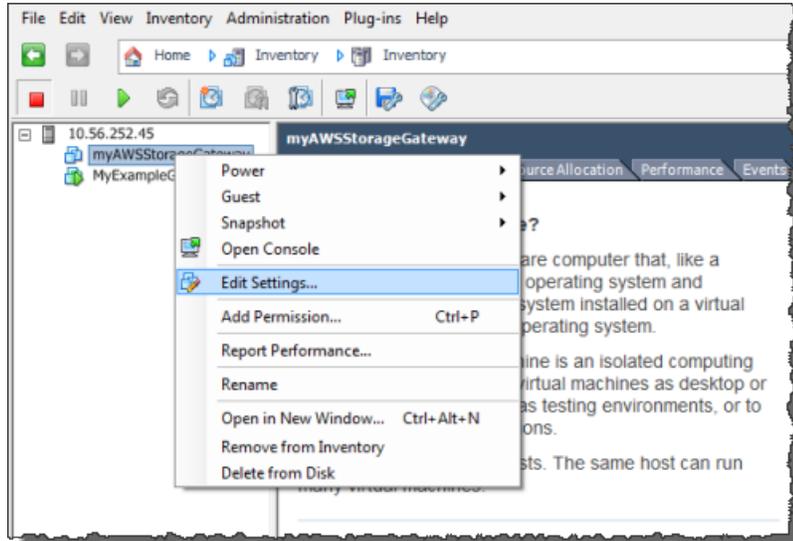


#### Important

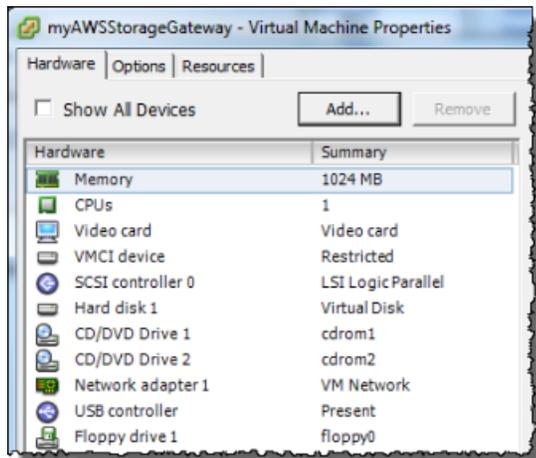
您给 VM 分配用作上传缓冲区的 10 GiB 磁盘不适合实际工作负载。强烈建议您至少分配 150 GiB 的上传缓冲区。在本教程后面的步骤 ([针对实际工作负载配置网关存储的大小 \(p. 87\)](#)) 中，您将了解如何针对真实工作负载适当地调整上传缓冲区的大小。

### 如需分配磁盘以存储您的应用程序数据

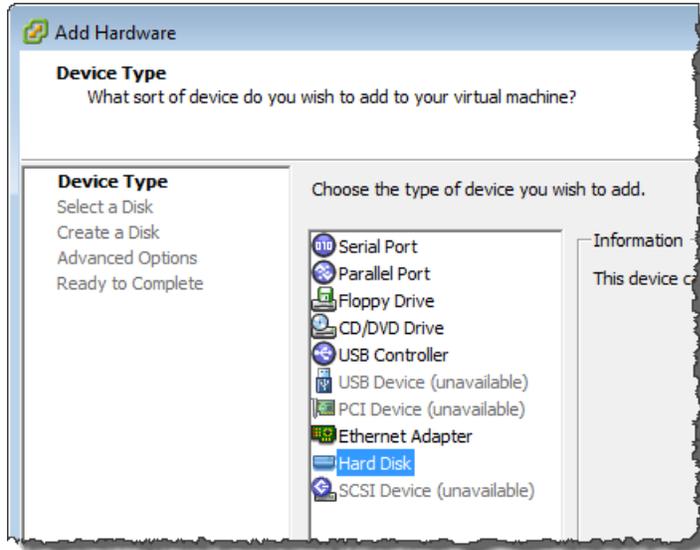
1. 启动 VMware vSphere 客户端并连接到您的主机。
2. 在客户端中，右键单击网关 VM 的名称，然后单击编辑设置。



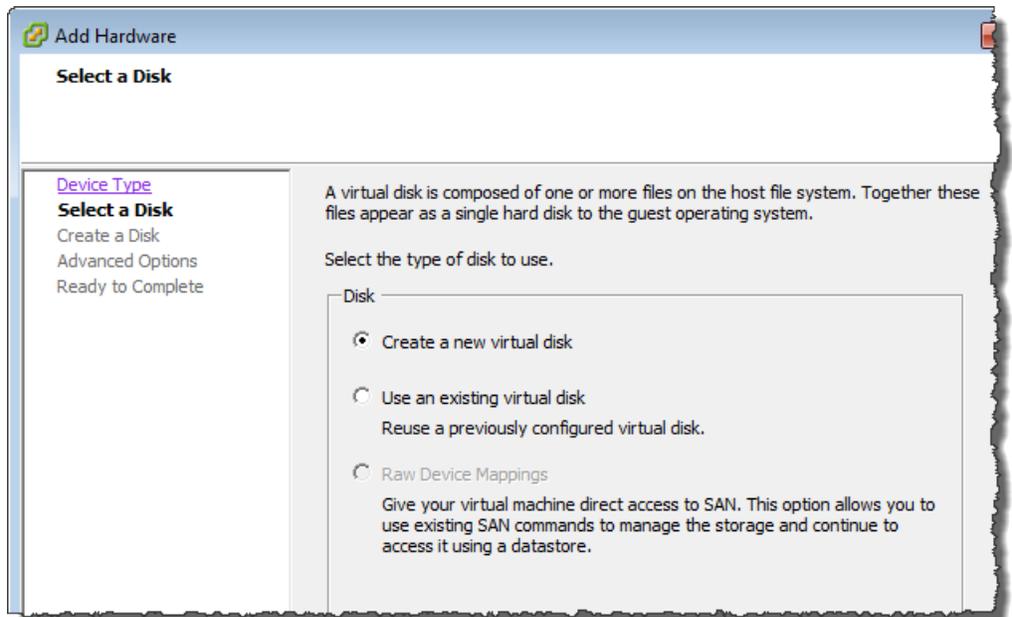
3. 在虚拟机属性对话框的硬件选项卡中，单击添加以添加一个设备。



4. 根据添加硬件向导添加磁盘：
  - a. 在设备类型窗格中，单击硬盘以添加一个磁盘，然后单击下一步。



- b. 在选择磁盘窗格中，选择新建虚拟磁盘，然后单击下一步。



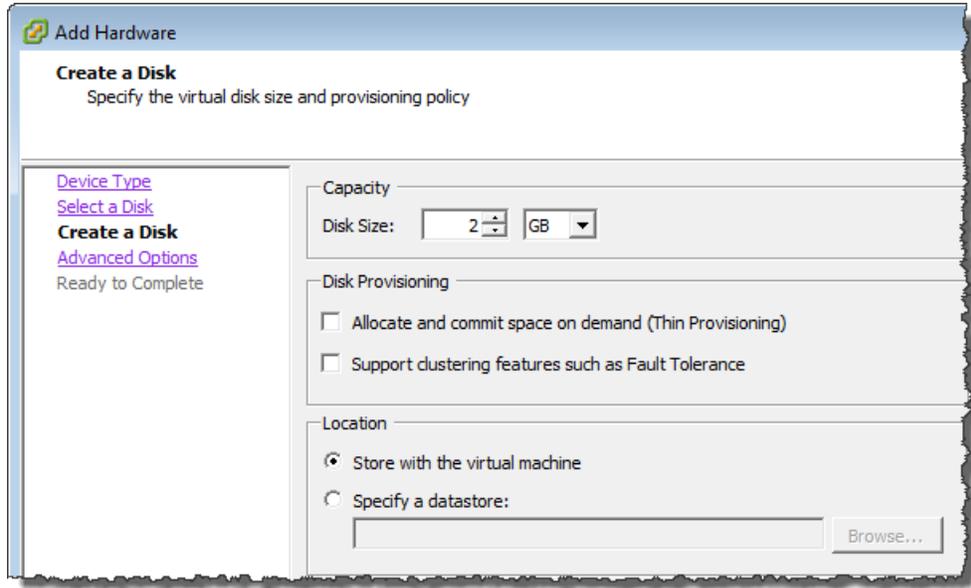
- c. 在创建磁盘窗格中，将磁盘的大小指定为 2 GiB，然后单击下一步。

选择存储自动配置时，磁盘空间立即分配，从而取得更好的性能。反之，自动精简配置按需分配存储空间。按需分配可能会影响 AWS Storage Gateway 的正常运行。因此，为使 AWS Storage Gateway 正常运行，必须以完全配置格式存储虚拟机磁盘。

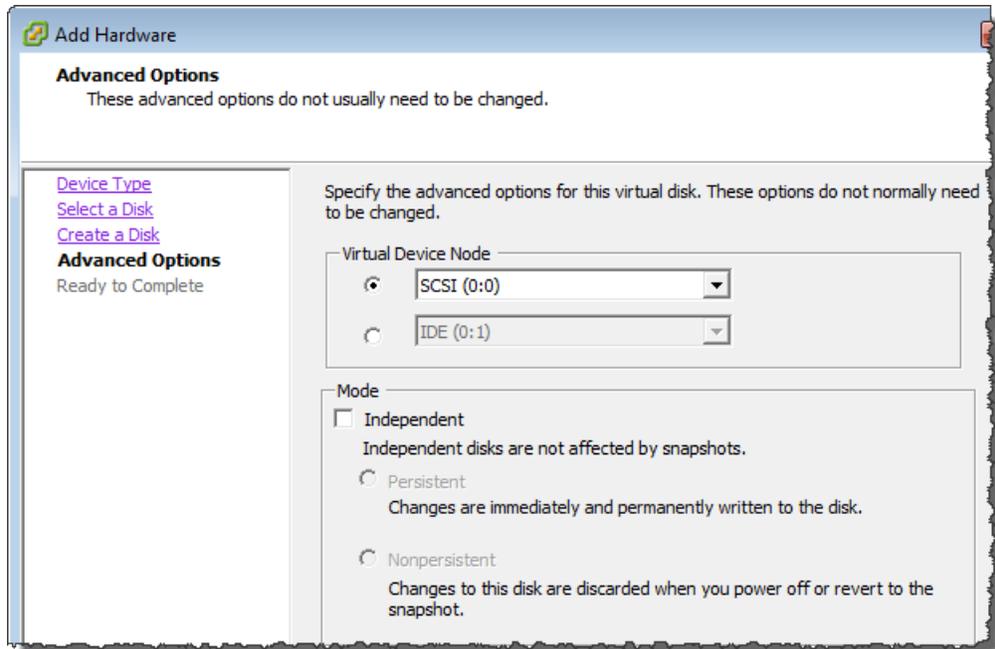


#### Note

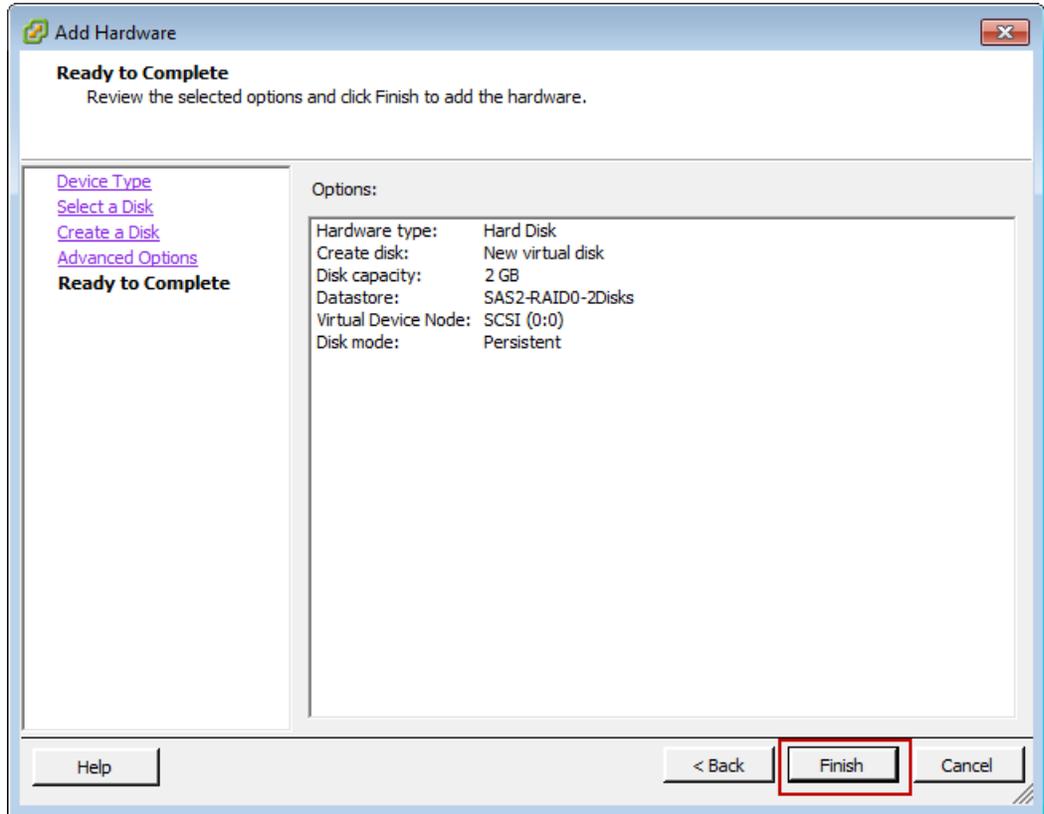
在本例设置中，将磁盘的位置与虚拟机存储在一起。对于实际工作负载，我们强烈建议您不要使用相同的底层物理存储磁盘预配置本地磁盘。根据托管环境的不同，为您在本步骤中预配置的磁盘选择不同的数据存储设备可能更好。有关更多信息，请参阅 [预配置本地磁盘 \( 网关存储 \)](#) (p. 100)。



- d. 在高级选项窗格中，接受默认值，然后单击下一步。



- e. 在已准备好完成窗格中，接受默认值，然后单击完成。



- f. 在虚拟机属性对话框中，单击确定以完成添加磁盘。

### 为上传缓冲区分配本地磁盘

网关在上传快照到 AWS 时，需要缓存空间以临时存储数据。这一空间称为上传缓冲区。您必须给 VM 添加虚拟磁盘，专供 VM 使用。网关所需上传缓冲区的大小取决于您为存储数据而分配的磁盘大小。有关相关准则，请参阅[配置上传缓冲区的大小 \(网关存储\)](#) (p. 104)。

对于本教程，您给 VM 分配 10 GiB 的虚拟磁盘，专供网关使用。在向导的创建磁盘窗格中，输入 10 GiB 作为磁盘大小。

### 如需为上传缓冲区分配本地磁盘

- 重复[如需分配磁盘以存储您的应用程序数据](#) (p. 26) 过程中的步骤以向网关添加另一个虚拟磁盘。

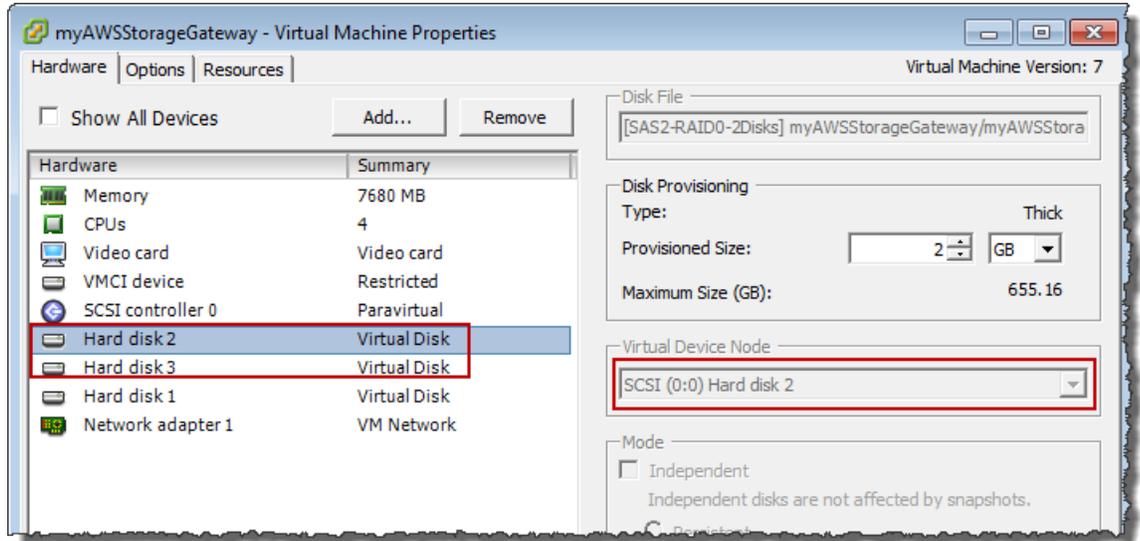
### 验证网关 VM 有两个磁盘

此教程的其余部分要求您已向网关 VM 分配好两个磁盘；请使用下面的可选步骤来验证这一点。如果需要分配其他磁盘，则重复[如需分配磁盘以存储您的应用程序数据](#) (p. 26) 过程中的步骤。

### 如需验证 VM 有两个磁盘

1. 在客户端中，右键单击网关 VM 的名称，然后单击编辑设置。
2. 在虚拟机属性对话框的硬件选项卡中，确认硬件列表中显示硬盘 2 和硬盘 3。

这两个磁盘随后将用于 AWS Storage Gateway 控制台中，并在下拉列表中显示为 SCSI (0:0) 和 SCSI (0:1)。



### 配置 AWS Storage Gateway VM 以使用半虚拟化的磁盘控制器

在本任务中，iSCSI 控制器设置为 VM 采用半虚拟化的模式，在该模式中网关 VM 与主机 OS 协同工作，以便控制台能够正确识别您给 VM 添加的虚拟磁盘。

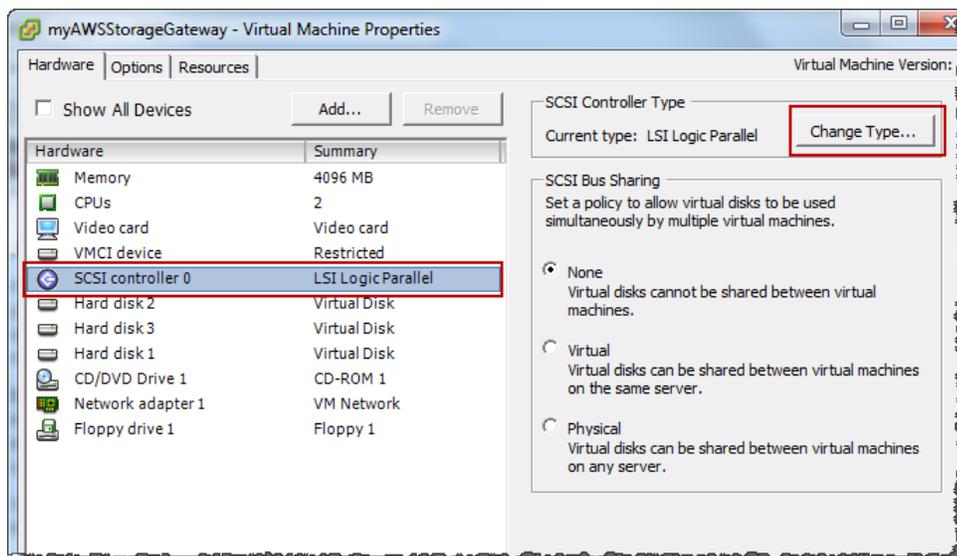


#### Note

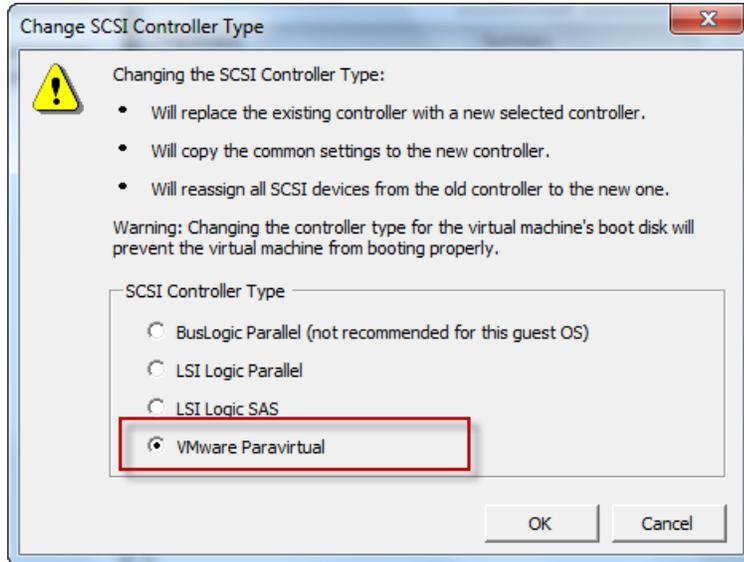
您必须完成本步骤以避免随后在识别这些磁盘时发生问题。

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，右键单击您的网关 VM 名称。
2. 选择编辑设置。
3. 在虚拟机属性对话框中，单击硬件选项卡，选择 SCSI 控制器 0，然后单击更改类型。



4. 在更改 SCSI 控制器类型对话框中，选择 VMware 半虚拟化 SCSI 控制器类型，然后单击确定。

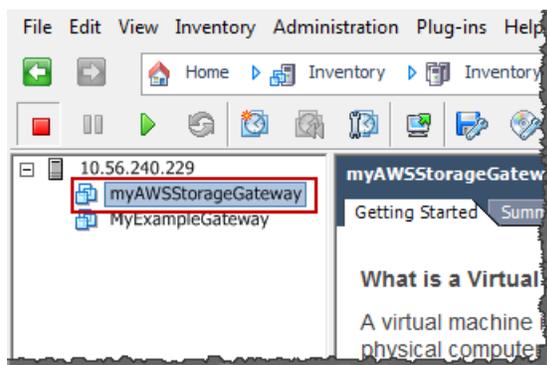


## 激活网关

现在，您已可随时激活网关。激活过程将您的网关与 AWS 账户关联。您必须在激活网关前启动网关 VM。

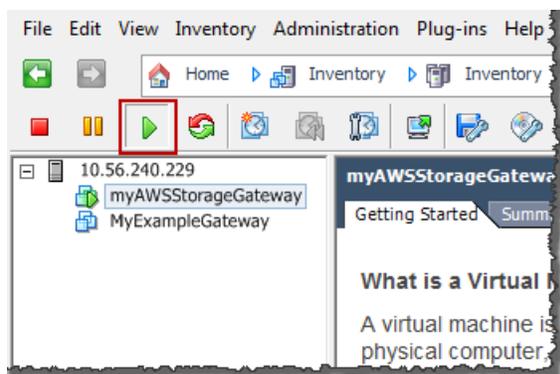
如需激活网关

1. 启动 VM。
  - a. 在 vSphere 客户端中，选择网关 VM。



- b. 在工具栏菜单中，单击开机图标。

您的网关 VM 图标现在包含一个绿色箭头图标，表示您已启动 VM。



## 2. 激活网关。

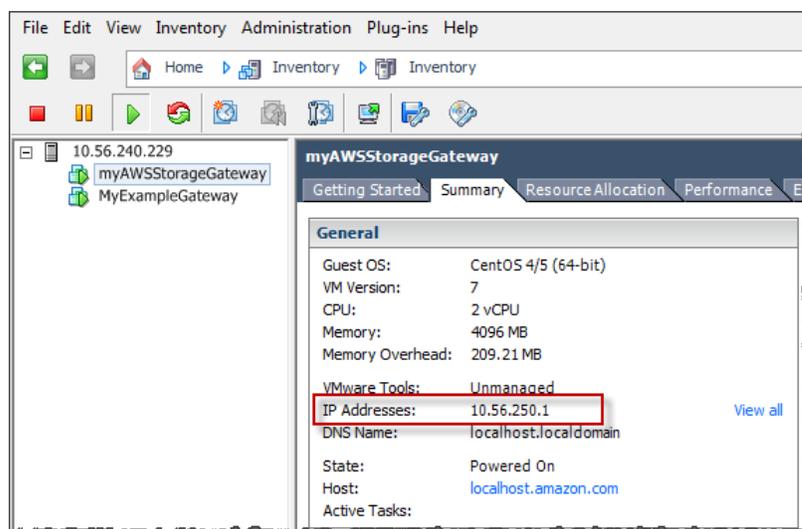
### a. 取得您的网关的 IP 地址。

- i. 在 vSphere 客户端中，选择部署的网关 VM。
- ii. 单击摘要选项卡以获得该 IP 地址。



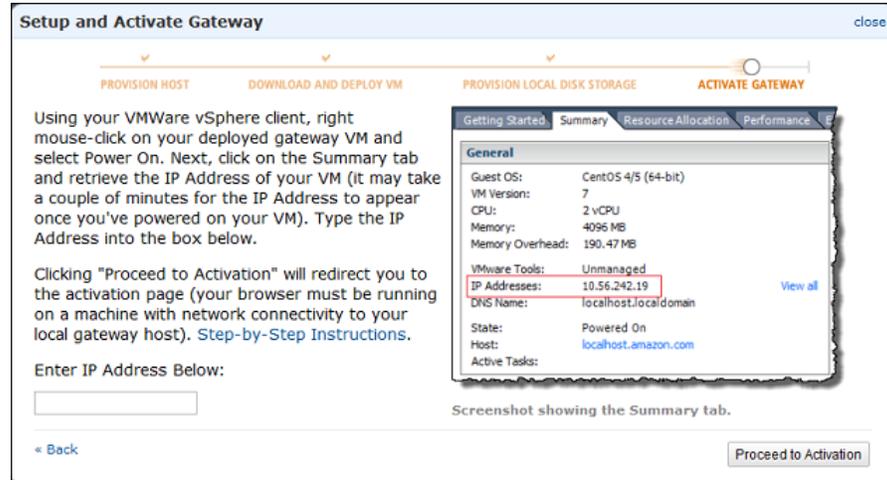
#### Note

网关的 IP 地址显示为摘要的一部分。启动 VM 后，IP 地址可能需要几分钟的时间才能显示。



### b. 将您的网关关联到 AWS 账户。

- i. 在 AWS Storage Gateway 控制台的设置并激活网关向导中，导航到以下激活网关页。
  - A. 如果尚未启动该向导，则单击设置并激活新网关按钮。
  - B. 在向导的每个步骤中单击继续，直到抵达激活网关页。
- ii. 输入您的网关的 IP 地址，然后单击继续激活。



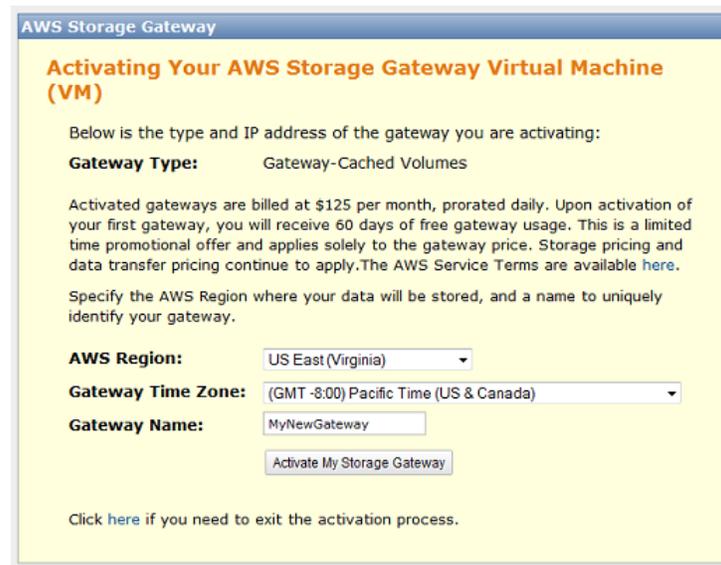
### Note

激活期间，您的浏览器连接到网关。如果激活失败，请检查您输入的 IP 地址是否正确。如果 IP 地址正确，请确认您的网络配置为可允许浏览器访问网关 VM。

- iii. 在激活页面填写完成激活所需的信息。

AWS 地区决定 AWS 存储快照的位置。如果您选择将快照还原为 Amazon EBS 卷，Amazon EBS 卷就必须和快照在同一地区。您不能在网关激活后更改地区。

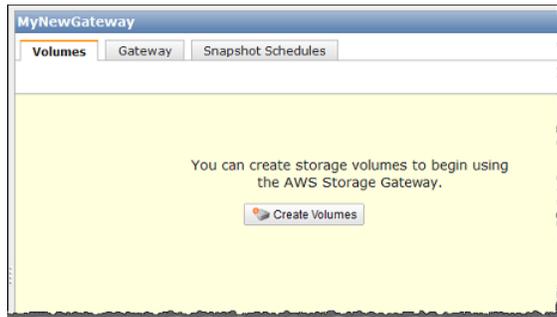
网关名称在控制台中标识您的网关。您使用该名称在控制台中管理网关，可在激活后更改名称。该名称必须是您账户的唯一名称。



- iv. 单击激活我的 Storage Gateway。

成功激活后，AWS 存储网关 控制台在导航窗格的网关部分下显示一个链接，指向已激活的网关。单击您刚刚添加的网关。

随后将显示创建卷按钮。



## 设置和激活 (Hyper-V 主机)

在本部分中，您将预配置场内 Microsoft Hyper-V 主机、向主机下载和部署网关 VM、配置网关 VM 并进行激活。

### 配置 Hyper-V 主机以部署 AWS Storage Gateway VM

在本步骤中，您在数据中心创建 Hyper-V 主机，用来部署网关虚拟机 (VM)。

如需预配置主机

1. 核查最低主机要求。有关更多信息，请参见 [要求 \(p. 7\)](#)。
2. 使用 Microsoft Hyper-V 主机在数据中心设置主机。

本指南中的附录提供安装管理程序操作系统的最低限度指导。有关更多信息，请参阅 [附录 D：为 AWS Storage Gateway 配置 Microsoft Hyper-V 主机 \(p. 447\)](#)。

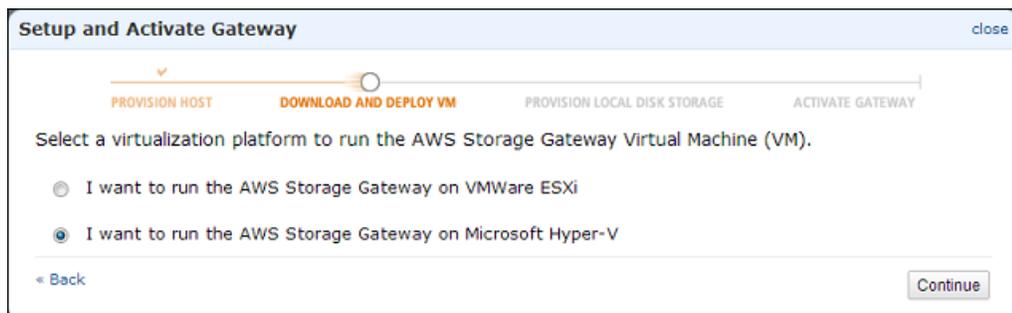
### 下载 AWS Storage Gateway VM 并将其部署在您的主机上

以 Hyper-V 可下载的 .zip 文件形式提供 AWS Storage Gateway 虚拟机。本部分介绍如何将该文件下载到本地，并导入到您的主机。

### 下载 AWS Storage Gateway VM

如需下载该 VM

1. 在 [AWS Storage Gateway](#) 控制台的设置并激活网关向导中，导航到下载并部署 VM 页。
2. 选择我要在 Microsoft Hyper-V 上运行 AWS Storage Gateway，然后单击继续。



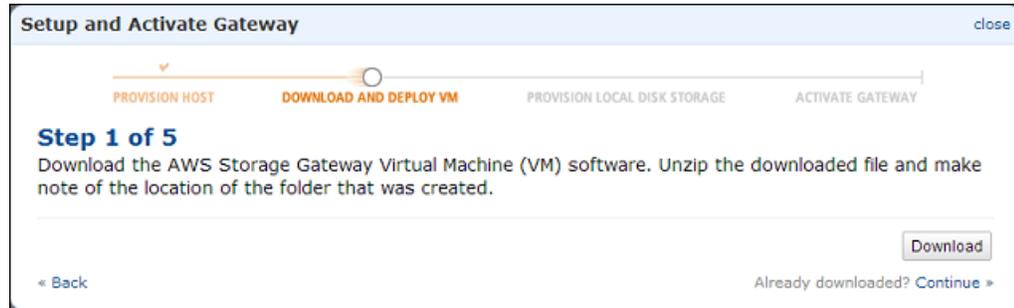
3. 单击下载以下载包含该 VM 的 .zip 文件。

将 .zip 保存到您的计算机上的某个位置。解压缩已下载的文件，并记下已创建的文件夹的位置。



#### Note

该 .zip 文件大小超过 500 MB，根据网速的不同，下载该文件可能需要一些时间。

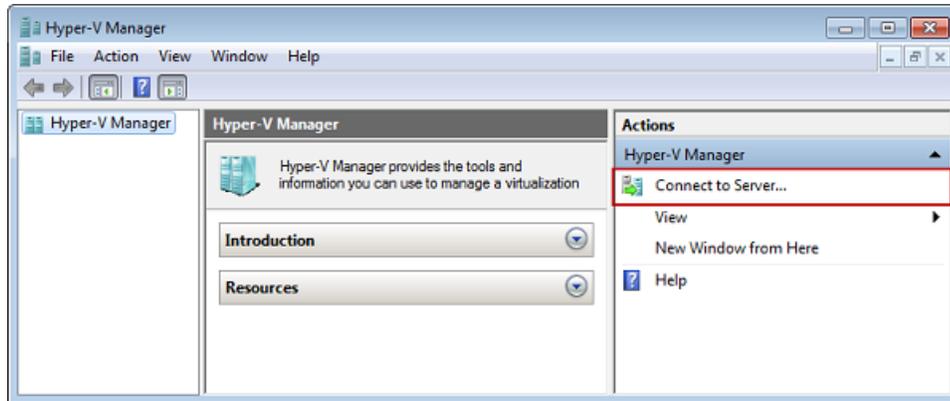


### 将 AWS Storage Gateway VM 部署到您的主机

要与管理程序主机一起运行，您必须连接到该主机。在连接后，您应指定 VM 的存储位置、导入 VM 和配置 VM 的网络。

如需连接到管理程序主机

1. 在您的 Windows 客户端上启动 Microsoft Hyper-V Manager。
2. 在操作窗格中，单击连接到服务器...

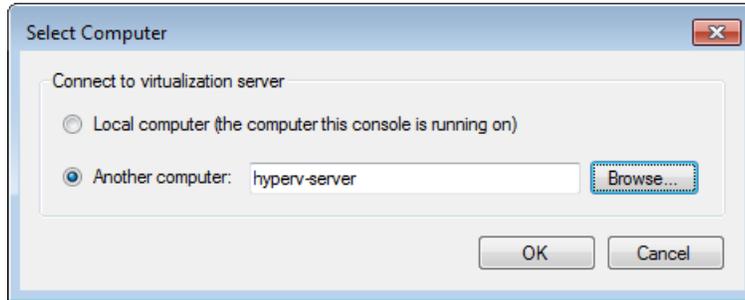


3. 在选择计算机对话框中，选择另一台计算机，输入 IP 地址或主机名，然后单击确定。



#### Note

在本练习中，我们使用 `hyperv-server` 作为主机。您的主机名会与此不同。如果在使用选择计算机对话框时找不到您的主机名，则可能需要在 `hosts` 文件中输入一个条目，以使 Hyper-V 管理器可解析服务器名称。



您的 Microsoft Hyper-V Manager 现已连接到您的主计算机。

既然您已连接到主机，下一个步骤就是在该主机上创建文件夹，以便存储已下载的源 VM、已导入的正在运行 VM 以及该 VM 所关联的虚拟硬盘。

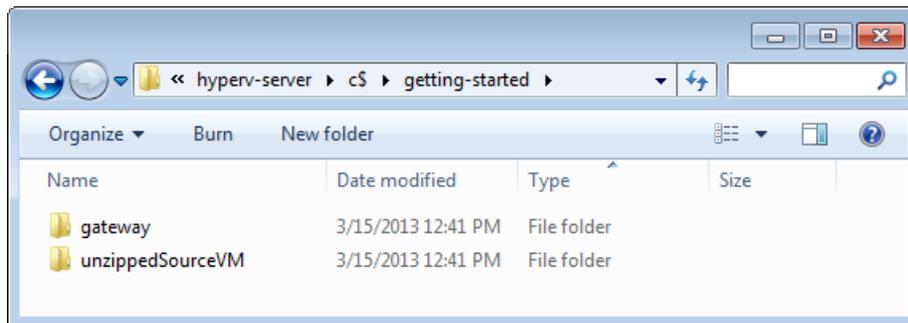
### 指定虚拟硬盘和 VM 的位置

1. 在管理程序主机上为网关虚拟硬盘和 VM 创建位置。

- a. 导航到管理程序所在的驱动器。

例如，使用本练习中主机的名称，并假定 C 驱动器对于您的主机有效，则可在“开始”菜单中键入 \\hyperv-server\c\$。

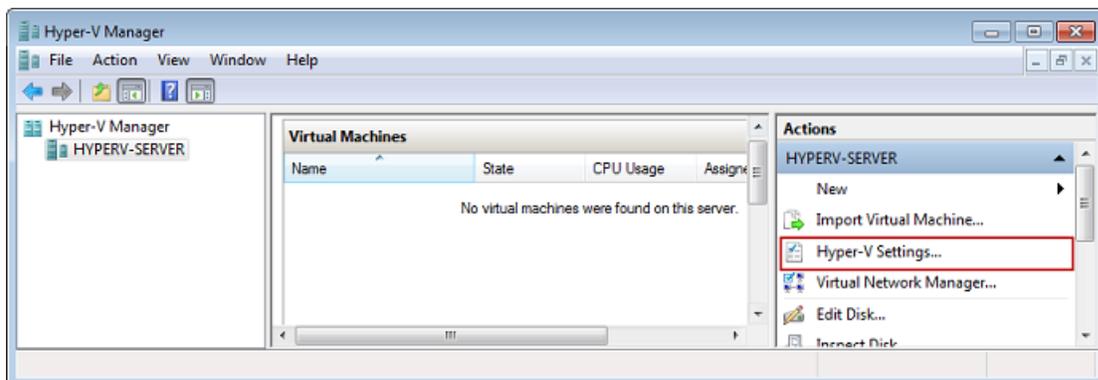
- b. 创建一个名为 getting-started 的文件夹，其中含有两个子文件夹 unzippedSourceVM 和 gateway。



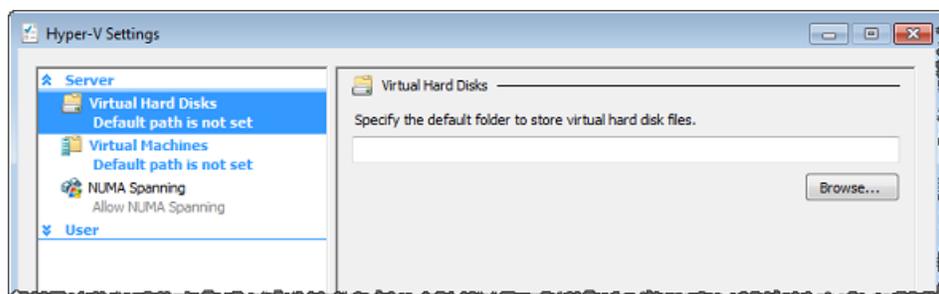
2. 配置 Hyper-V 管理器，使其指向您创建的 gateway 文件夹。

这也是正在运行的 VM 将用于存储其配置的文件夹。

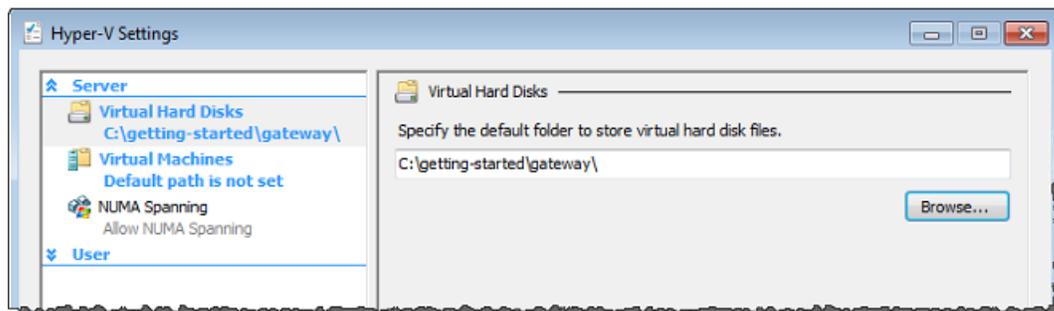
- a. 在操作菜单中，单击 Hyper-V 设置...



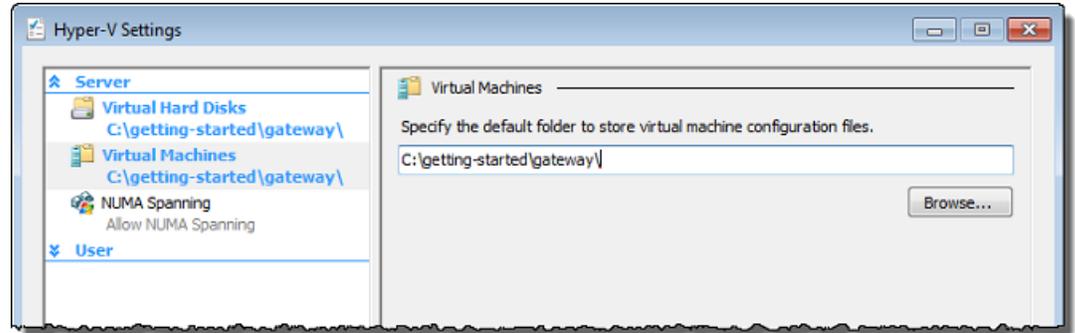
- b. 在 Hyper-V 设置对话框中，配置虚拟硬盘和虚拟机的位置。
  - i. 在左侧窗格中的服务器下，选择虚拟硬盘设置。



- ii. 通过浏览，查找以前创建的 gateway 文件夹。  
您在管理程序 ( 主机 ) 服务器上浏览。

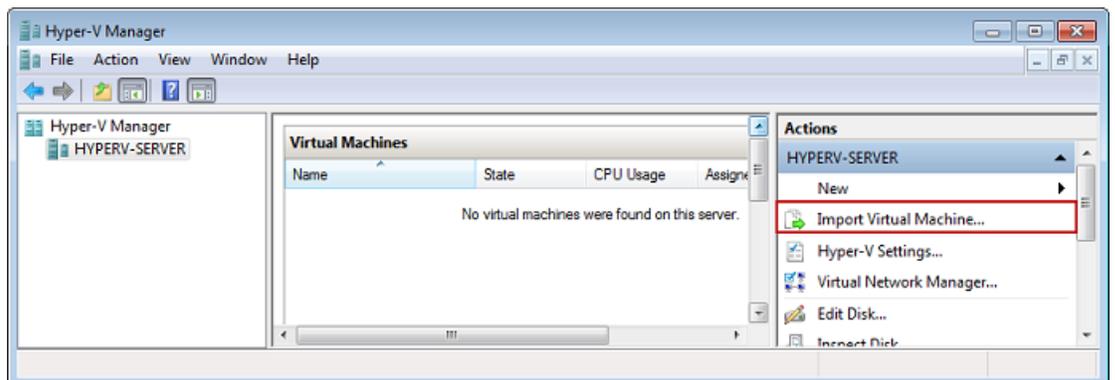


- iii. 在左侧窗格中的服务器下，选择虚拟机设置。
      - iv. 通过浏览，将该位置设为相同的 gateway 文件夹。



### 导入该 VM

1. 将解压缩的源 VM 文件复制到您在主机计算机上创建的文件夹。在本练习中，该路径为  
\\hyperv-server\c\$\getting-started\unzippedSourceVM\AWS-Storage-Gateway。
2. 将 AWS Storage Gateway VM 导入到主机。
  - a. 在 Hyper-V 管理器的左侧控制台树窗格中，选择主机 hyperv-server。
  - b. 在操作菜单中，单击导入虚拟机...



- c. 在导入虚拟机对话框中：
  - i. 在位置框中，找到以前创建的位置  
\\hyperv-server\c\$\getting-started\unzippedSourceVM\AWS-Storage-Gateway。



### Caution

您必须指向正确的文件夹，导入才会成功。要选择正确文件夹 (AWS-Storage-Gateway) 将包含其他三个文件夹 ( Snapshots、Virtual Hard Disks、Virtual Machines ) 和一个文件 (config.xml)。根据网关源文件的解压缩方式，您最后可能会得到一个额外的文件夹级别。要帮助排除导入方面的故障，请参阅[故障诊断 Microsoft Hyper-V 设置 \(p. 453\)](#)。

- ii. 选择复制虚拟机(新建唯一 ID)。
- iii. 选中复制所有文件以便可以再次导入同一虚拟机。
- iv. 单击导入。



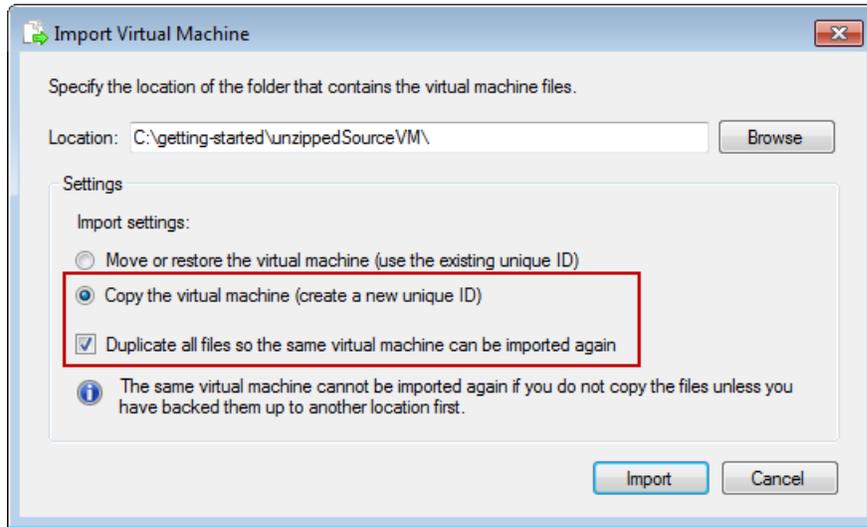
### Caution

选择复制虚拟机(新建唯一 ID)和复制所有文件以便可以再次导入同一虚拟机选项很重要，尤其是要重用解压缩的网关源文件时。



### Important

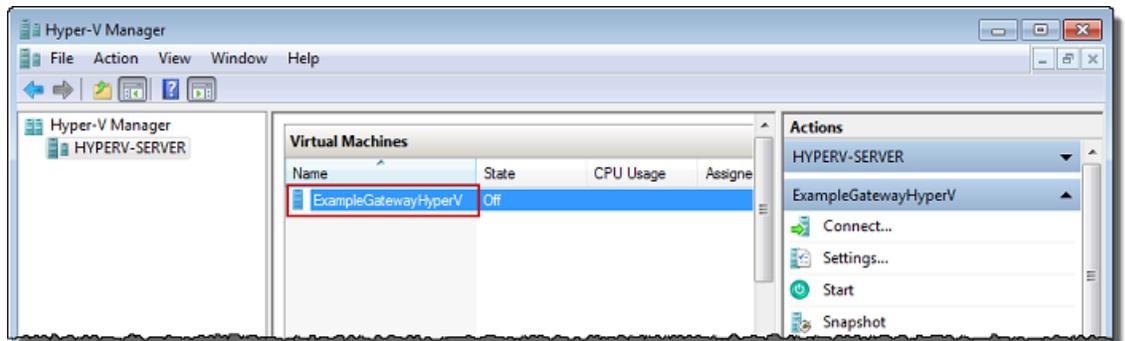
您必须具有 75 GiB 的磁盘空间，以便安装 VM 映像和系统数据。



在导入完成后，会创建名为 AWS-Storage-Gateway 的虚拟机。

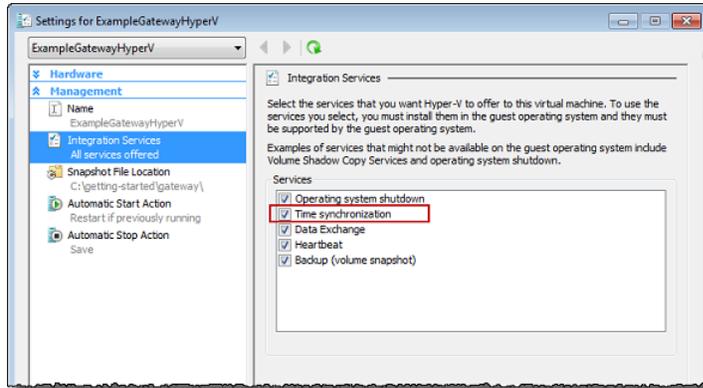
3. 重命名虚拟机，避免与您在该主机上导入的其他虚拟机混淆。
  - a. 选择该虚拟机，单击右键并选择重命名。
  - b. 为虚拟机提供新的名称。

在本练习中，我们将使用 ExampleGatewayHyperV。



4. 确认在集成服务中为该 VM 选择了时间同步。

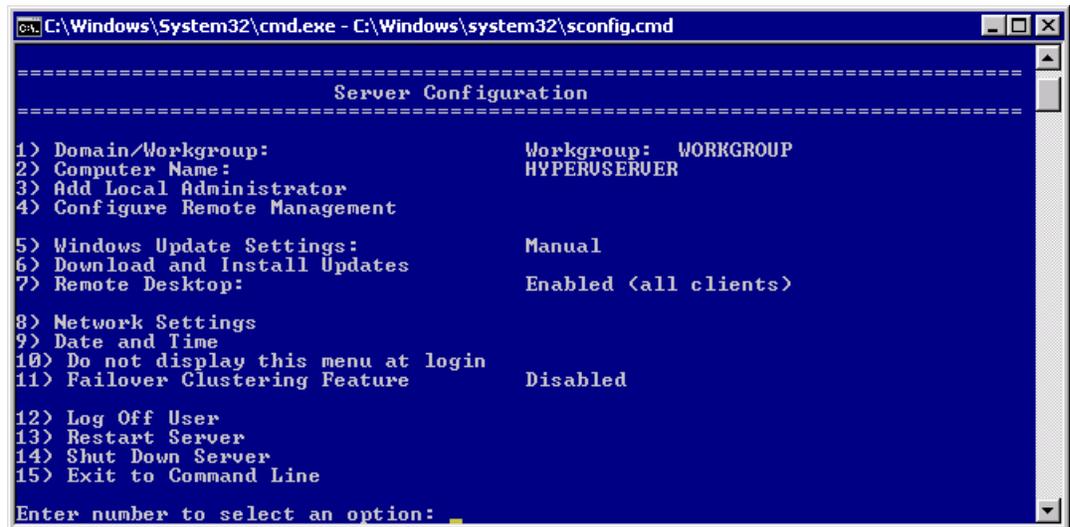
- a. 在虚拟机列表窗格中，选择虚拟机 ExampleGatewayHyperV。
- b. 在操作菜单中，单击设置...。
- c. 在设置对话框中的管理下，选择集成服务，然后确认选中了时间同步。



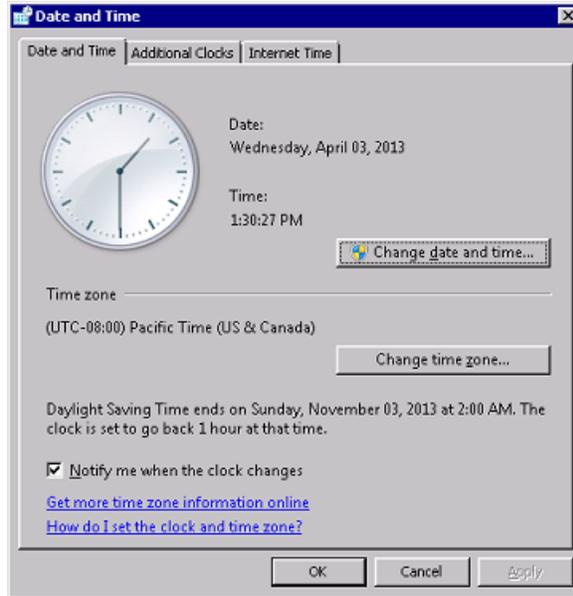
5. 如果您尚未执行这些操作，请配置主机时间。

请注意，确保您设置了正确的主机时间。以下步骤介绍如何使用"Server Configuration Tool"(Sconfig.cmd) 设置该时间。有关 Sconfig.cmd 的详细信息，请转到[使用 Sconfig.cmd 配置服务器核心服务器](#)。（根据正在运行的 Microsoft Hyper-V 版本，您可以使用其他方式设置该时间。）

- a. 您可以通过访问管理程序主机控制台或者远程登录，访问 Sconfig.cmd 工具。



- b. 输入选项 9 日期和时间。  
随后将显示日期和时间控制面板。
- c. 配置时间，然后单击确定。



## 配置虚拟网络并在 VM 上使用

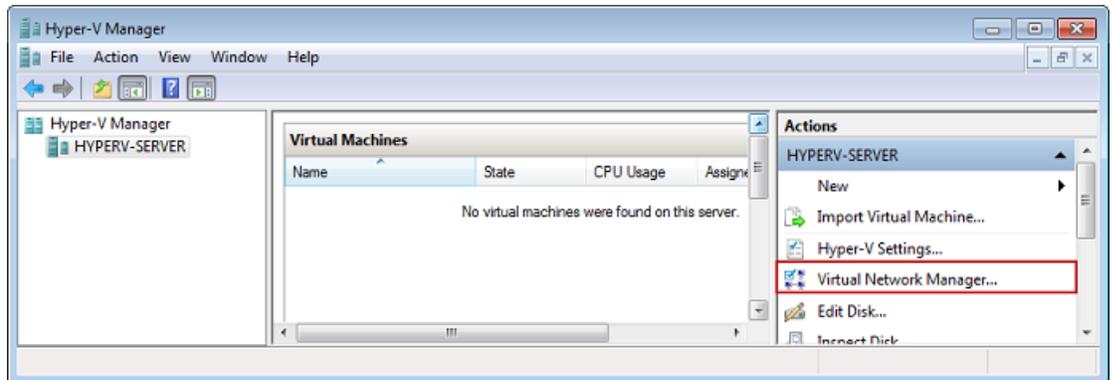
1. 配置 Hyper-V 主机的虚拟网络设置。



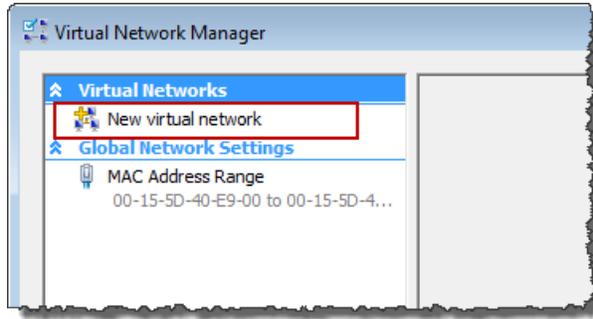
### Note

在本练习中，我们假定该主机尚未配置虚拟网络设置。如果您已经配置了虚拟网络，请转到步骤 2。

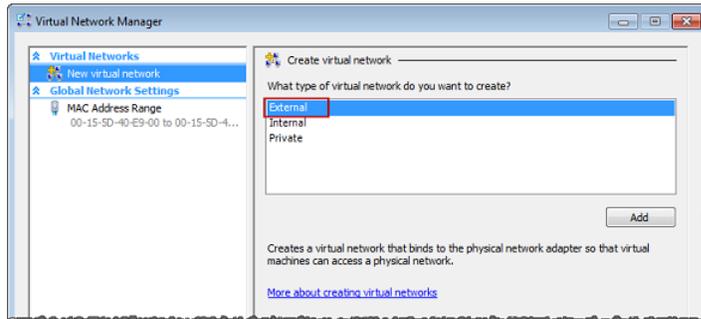
- a. 在操作菜单中的虚拟机监控程序主机名 (例如, hyperv-server) 下, 单击虚拟网络管理器...



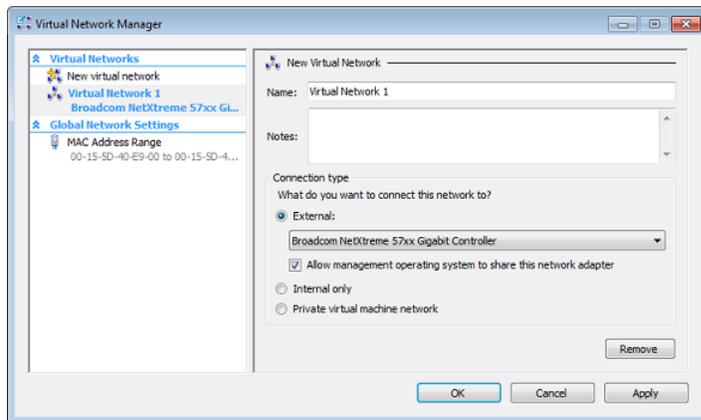
- b. 在虚拟网络管理器对话框中，选择新建虚拟网络。



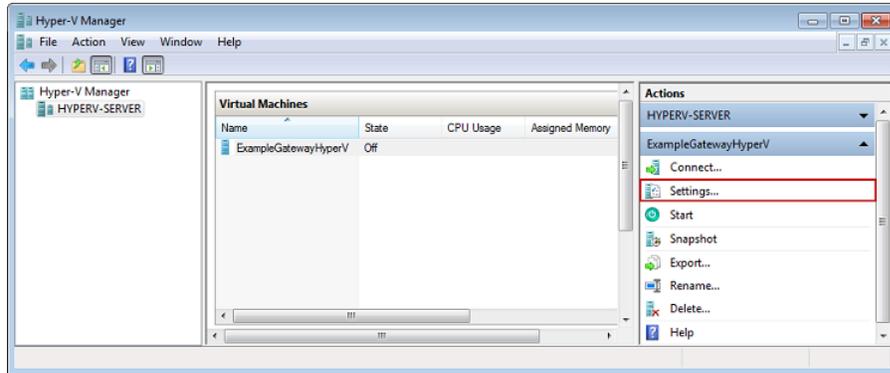
- c. 选择外部作为虚拟网络类型，然后单击添加。



- d. 为该网络提供一个名称，然后单击确定。

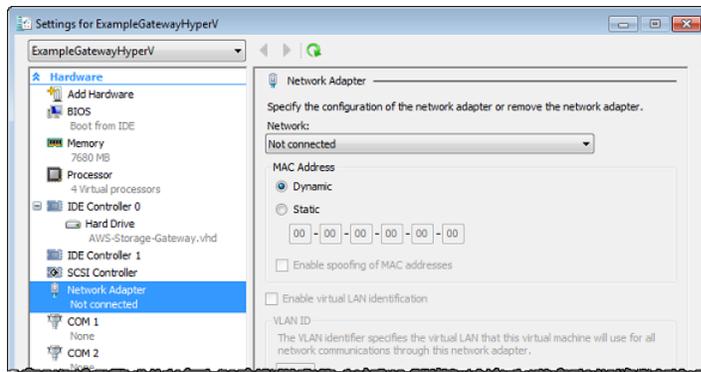


2. 配置虚拟机，以使用虚拟网络。
- a. 在虚拟机列表窗格中，选择虚拟机 ExampleGatewayHyperV。
  - b. 在操作窗格中，选择设置...。



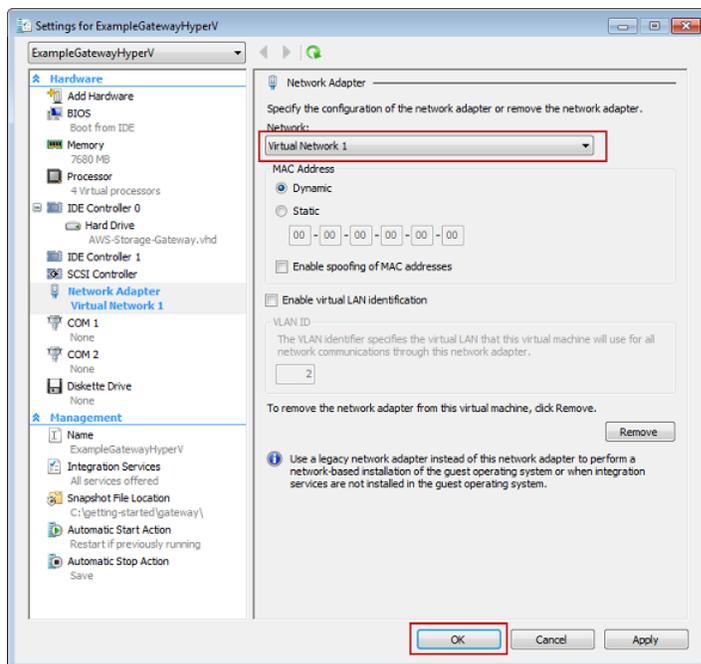
c. 在设置窗口中，选择网络适配器。

网络适配器的状态应为未连接。



d. 在网络框中的右窗格中，选择一个网络。

在下例中，选择了虚拟网络 1。



- e. 单击确定。

### 为您的 AWS Storage Gateway VM 配置本地磁盘存储

在 AWS Storage Gateway 控制台的设置并激活网关向导中，导航到配置本地磁盘存储步骤。

根据您的计划测试的网关架构 ( 网关缓存或网关存储 ) 的差异，单击下列链接之一，获得下一步指导。

如需...	请执行此操作...
为网关缓存卷预配置本地磁盘	按 <a href="#">预配置本地磁盘存储 ( 网关缓存 ) (p. 45)</a> 中的步骤进行操作。
为网关存储卷预配置本地磁盘。	按 <a href="#">预配置本地磁盘存储 ( 网关存储 ) (p. 51)</a> 中的步骤进行操作。

### 预配置本地磁盘存储 ( 网关缓存 )

在下面的步骤中，您将给部署的网关 VM 分配本地磁盘。完成这些步骤后，您便成功添加了两个虚拟磁盘。

在本练习中，您向专供网关使用的 VM 分配 20 GiB 作为缓存存储，10 GiB 作为上传缓冲区。



#### Important

在本教程中，您给 VM 分配用作缓存存储空间和上传缓冲区的虚拟磁盘大小不适合实际工作负载。我们强烈建议您至少分配 150 GiB 的上传缓冲区。缓存存储空间的大小应根据上传缓冲区的大小而定。在本教程后面的步骤 ( [针对实际工作负载配置网关存储的大小 \(p. 87\)](#) ) 中，您将了解如何针对真实工作负载适当地调整缓存存储和上传缓冲区的大小。

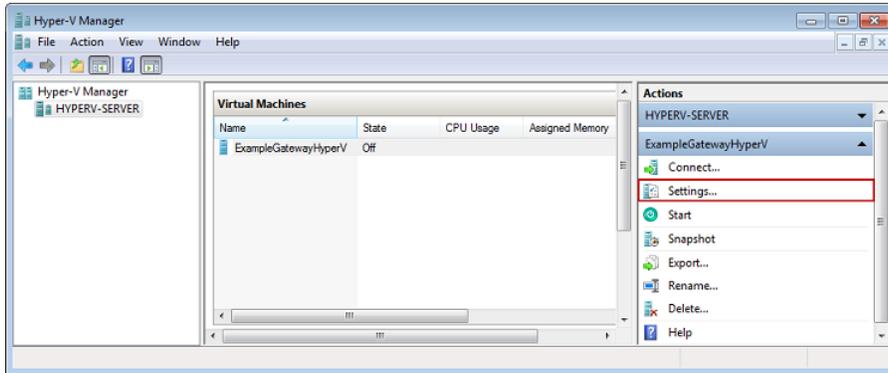
### 为缓冲存储区分配本地磁盘

您经常访问的应用程序数据在本地维护。您必须在 VM 上分配一个磁盘，作为存储这些数据的缓存。本部分说明如何在主机的物理磁盘上添加虚拟硬盘。在真实应用程序中，您应该考虑将独立的物理磁盘用作后备存储空间。有关使用一个单独的物理磁盘为虚拟硬盘充当后备的说明，请参阅[添加通过硬盘支持的虚拟磁盘 \(p. 452\)](#)。

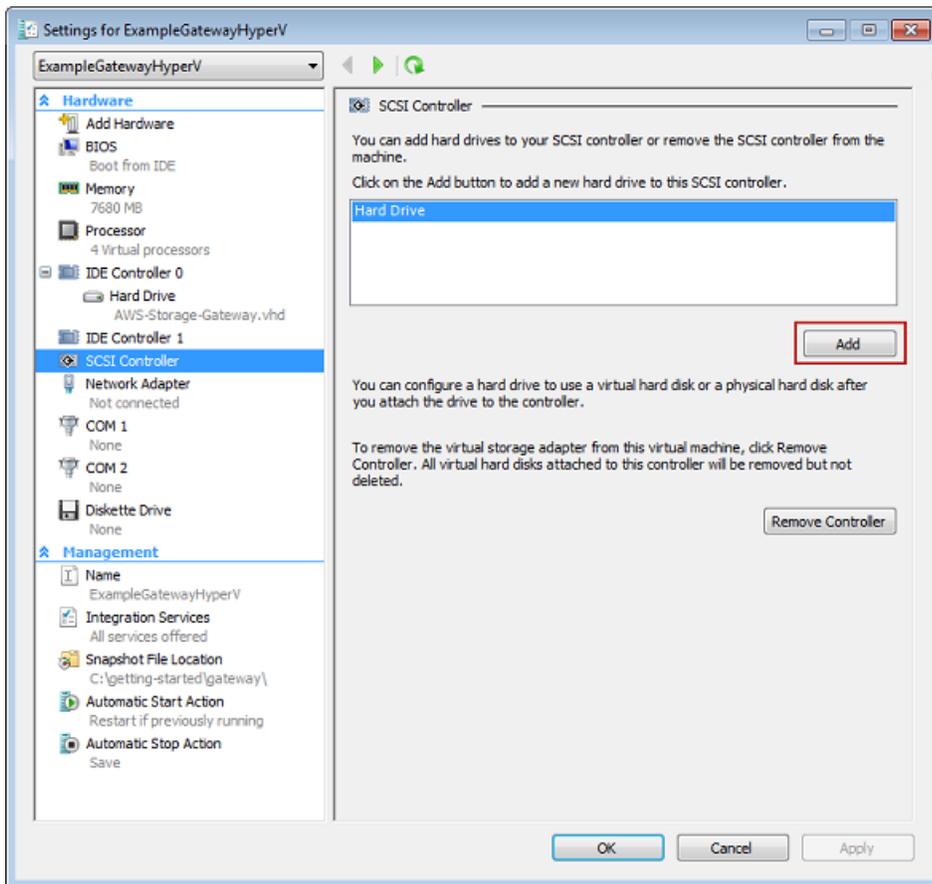
在本练习中，您向 VM 分配一个 20 GiB 的虚拟磁盘。

如需将本地磁盘分配为缓存

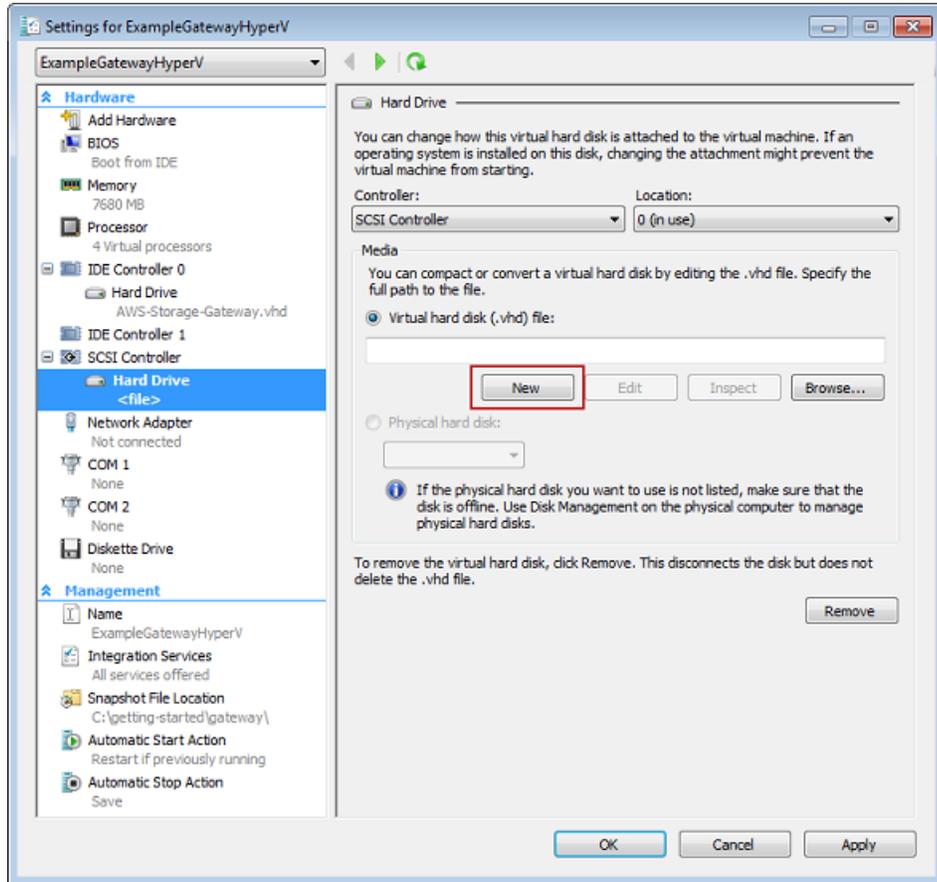
1. 启动 Microsoft Hyper-V Manager，然后连接到虚拟机监控程序。
2. 在虚拟机列表窗格中，选择虚拟机 ExampleGatewayHyperV。
3. 在操作窗格中，选择设置...



4. 在设置窗口中，选择 SCSI 控制器，然后单击添加。

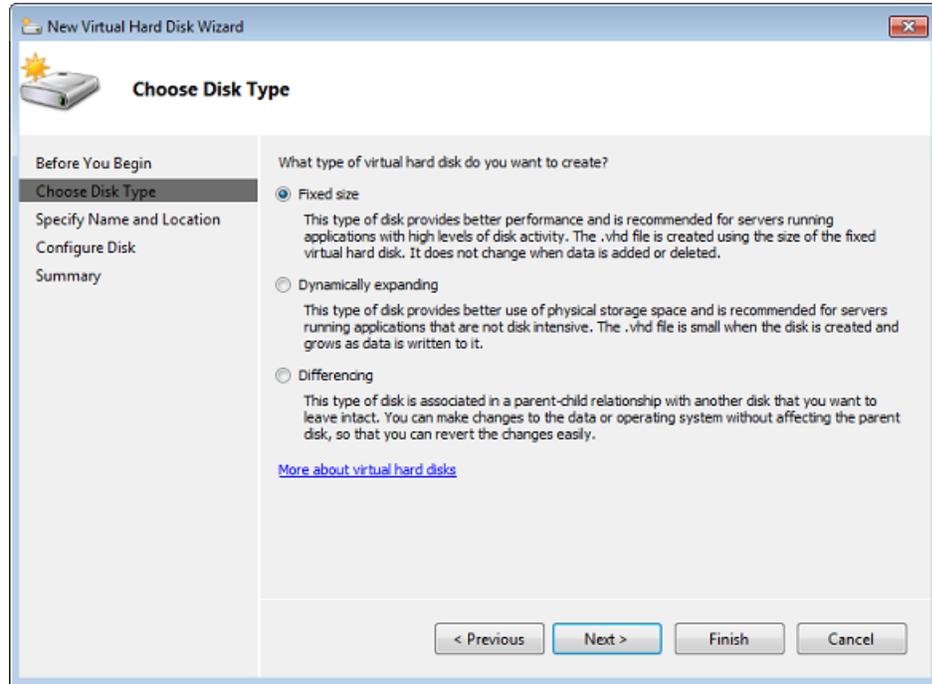


5. 在硬盘驱动器窗格中的介质下，单击新建。



6. 在新建虚拟硬盘向导中，新建一个虚拟硬盘。
  - a. 在开始之前页上，单击下一步。
  - b. 在选择磁盘类型页上，选择固定大小，然后单击下一步。

使用固定大小配置时，将立即分配磁盘存储，这样性能更好。如果不使用固定大小配置，则按需分配存储，这样可能会影响 AWS Storage Gateway 的正常运行。因此，为使 AWS Storage Gateway 正常运行，必须以固定大小配置的格式存储虚拟机磁盘。



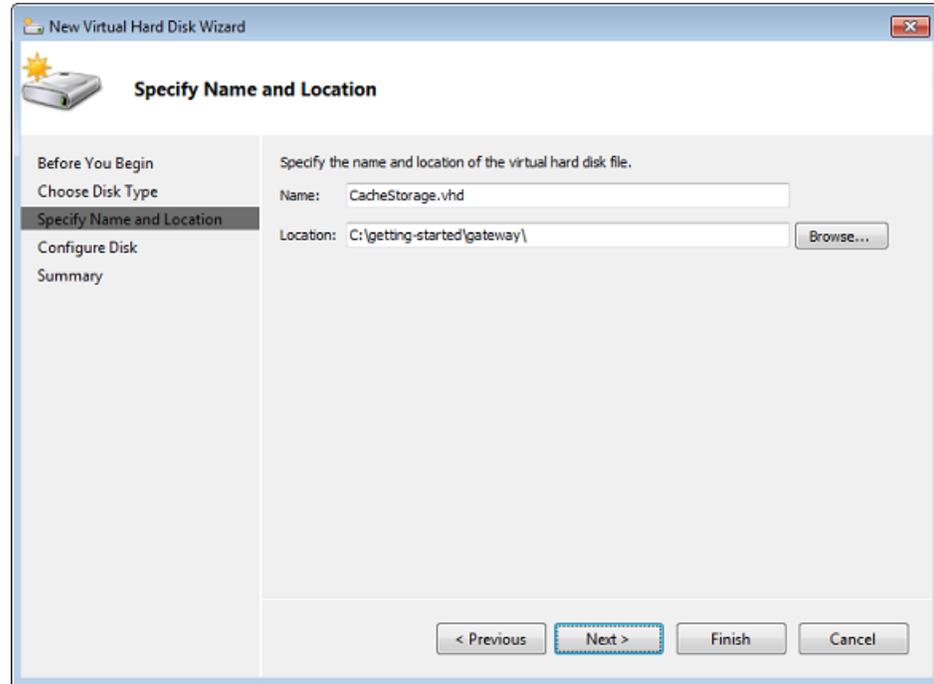
- c. 在指定名称和位置页上，指定该虚拟硬盘的名称和位置。
  - i. 指定 CacheStorage.vhd 作为名称。
  - ii. 将位置指定为 c\$\getting-started\gateway。



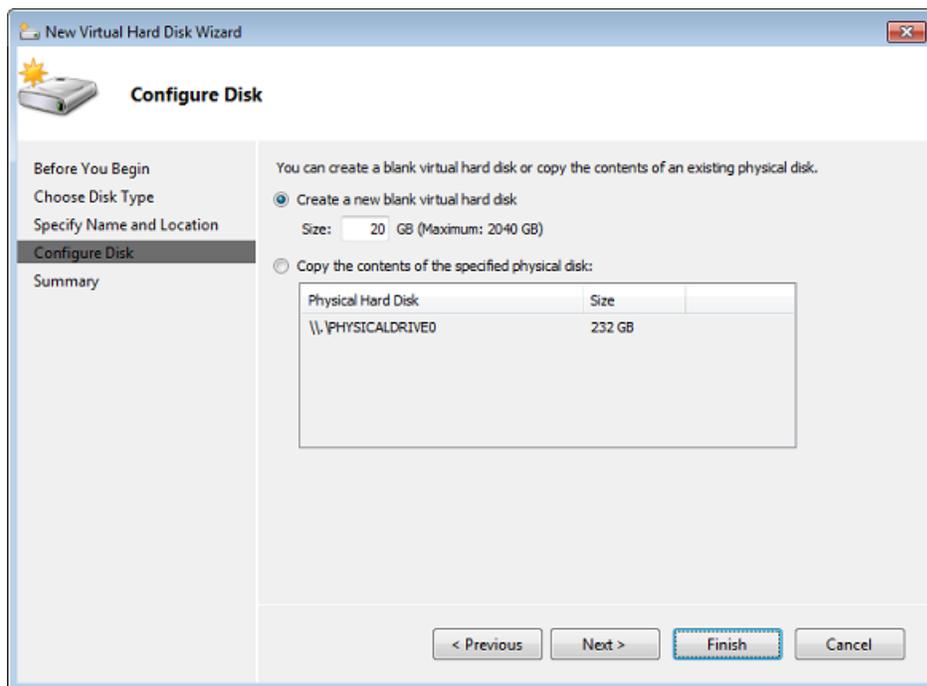
#### Note

在本示例设置中，您使用虚拟机存储虚拟磁盘。对于真实的工作负载，我们强烈建议您不要使用同一底层物理存储磁盘配置本地磁盘。根据主机托管环境、性能和便携性要求，最好在这个步骤选择一个不同的物理磁盘。有关更多信息，请参阅 [预配置本地磁盘 \( 网关缓存 \)](#) (p. 92)。

- iii. 单击下一步。



- d. 在配置磁盘页中，将磁盘的大小指定为 20 GiB，然后单击完成。

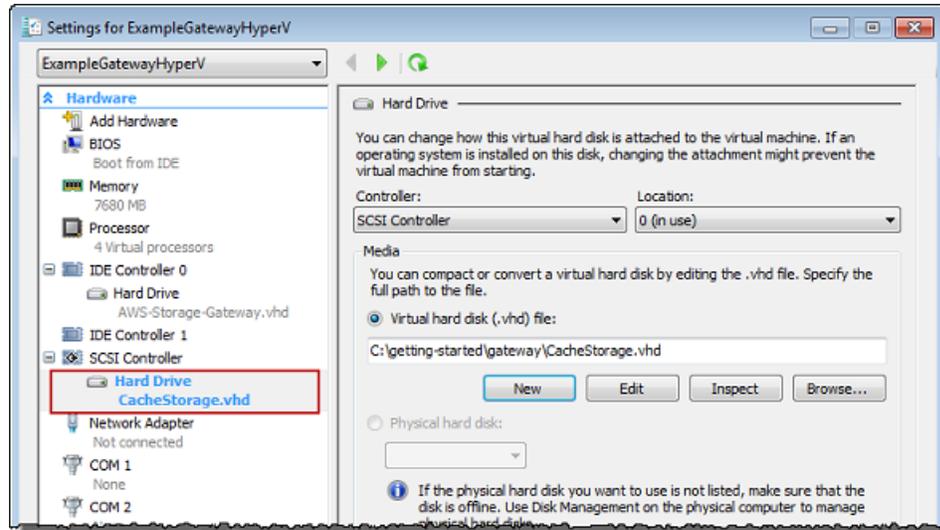


- e. 在创建虚拟磁盘后，确认在 SCSI 控制器下显示硬盘驱动器。  
f. 单击 SCSI 控制器以准备添加另一个硬盘驱动器。



### Warning

在添加另一个硬盘驱动器时，需要先单击 SCSI 控制器，然后再按此过程中的步骤进行操作。在查看现有硬盘驱动器的详细信息时单击新建将替换该现有驱动器。



7. 单击确定。

### 为上传缓冲区分配本地磁盘

网关在上传快照到 AWS 时，需要缓存空间以临时存储数据。这一空间称为上传缓冲区。您必须给 VM 添加虚拟磁盘，专供 VM 使用。网关需要的上传缓冲区大小取决于您指定的经常访问数据的缓存。有关相关准则，请参阅[配置上传缓冲区的大小 \(网关缓存\)](#) (p. 97)。

在本练习中，您向专供网关使用的 VM 分配一个 10 GiB 的虚拟磁盘。在向导的创建磁盘窗格中，输入 10 GiB 作为磁盘大小。

如需将本地磁盘分配为上传缓冲区

- 重复前一节 ([如需将本地磁盘分配为缓存](#) (p. 45)) 中的步骤以向网关添加另一个虚拟磁盘。除了使用名称 `UploadBuffer.vhd` 作为磁盘名称，并使用 10 GiB 作为磁盘大小之外，请严格按这些步骤进行操作。

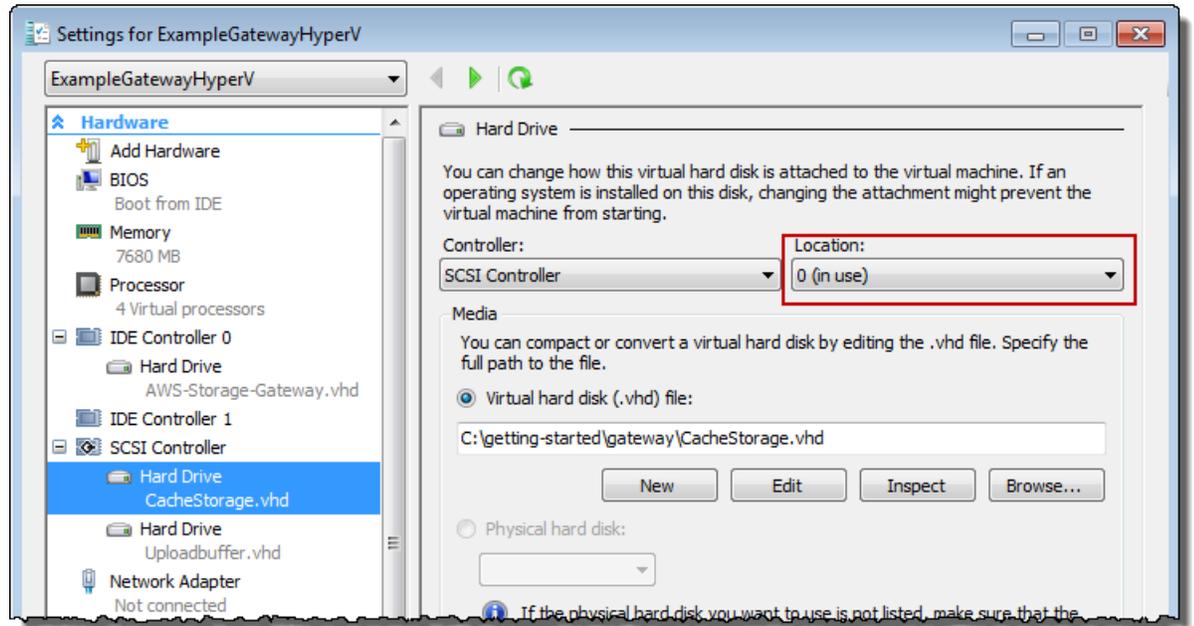
### 验证网关 VM 有两个磁盘

本练习的其余部分要求您已向网关 VM 分配两个磁盘。您可以使用下面的可选步骤验证已给网关 VM 分配好两个磁盘。如果需要分配其他磁盘，则重复[如需将本地磁盘分配为缓存](#) (p. 45) 过程中的步骤。

如需验证 VM 有两个磁盘

1. 启动 Microsoft Hyper-V Manager，然后连接到虚拟机监控程序。
2. 在虚拟机列表窗格中，选择虚拟机 ExampleGatewayHyperV。
3. 在操作窗格中，选择设置...
4. 在设置窗口中，选择 SCSI 控制器，然后确认有两个磁盘。

您创建的这两个磁盘随后将在 AWS Storage Gateway 控制台中使用，并在下拉列表中显示为 SCSI (0:0) 和 SCSI (0:1)。在下例中，选择 CacheStorage.vhd 磁盘，并且它为 SCSI (0:0)。



### 预配置本地磁盘存储 ( 网关存储 )

在下面的步骤中，您将给部署的网关 VM 分配本地磁盘。完成这些步骤后，您便成功添加了两个虚拟磁盘。

### 为存储卷分配本地磁盘 ( 用于您的应用程序数据 )

您所有的应用程序数据均在本地维护。您必须给 VM 分配磁盘，以便存储应用程序数据。本部分说明如何在主机的物理磁盘上添加虚拟硬盘。在真实应用程序中，您应该考虑将独立的物理磁盘用作后备存储空间。有关使用一个单独的物理磁盘为虚拟硬盘充当后备的说明，请参阅[添加通过硬盘支持的虚拟磁盘 \(p. 452\)](#)。

在本练习中，您向 VM 分配一个 2 GiB 的虚拟磁盘用于存储应用程序数据，向 VM 分配一个 10 GiB 的上传缓冲区专供网关使用。

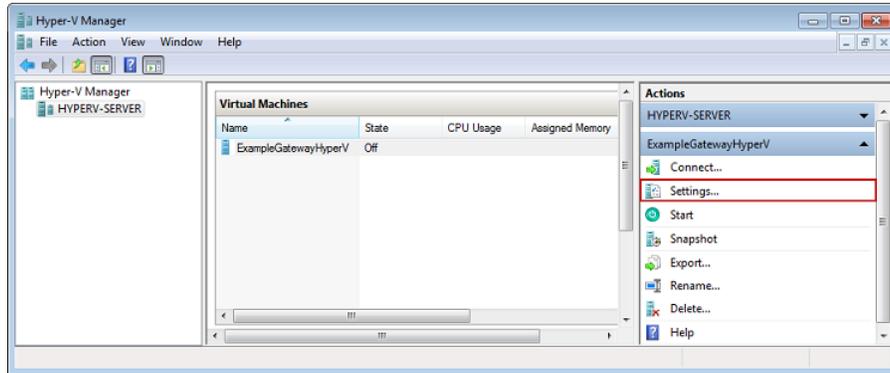


#### Important

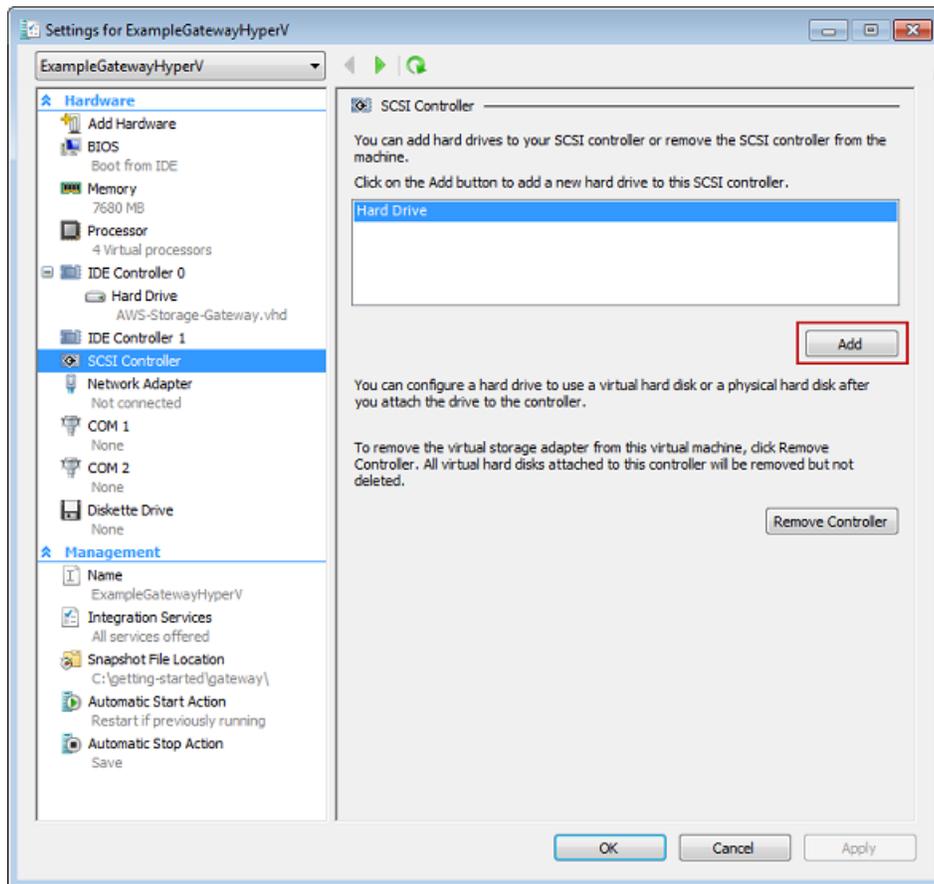
您给 VM 分配用作上传缓冲区的 10 GiB 磁盘不适合实际工作负载。强烈建议您至少分配 150 GiB 的上传缓冲区。在本教程后面的步骤 ([针对实际工作负载配置网关存储的大小 \(p. 87\)](#)) 中，您将了解如何针对真实工作负载适当地调整上传缓冲区的大小。

### 如需分配磁盘以存储您的应用程序数据

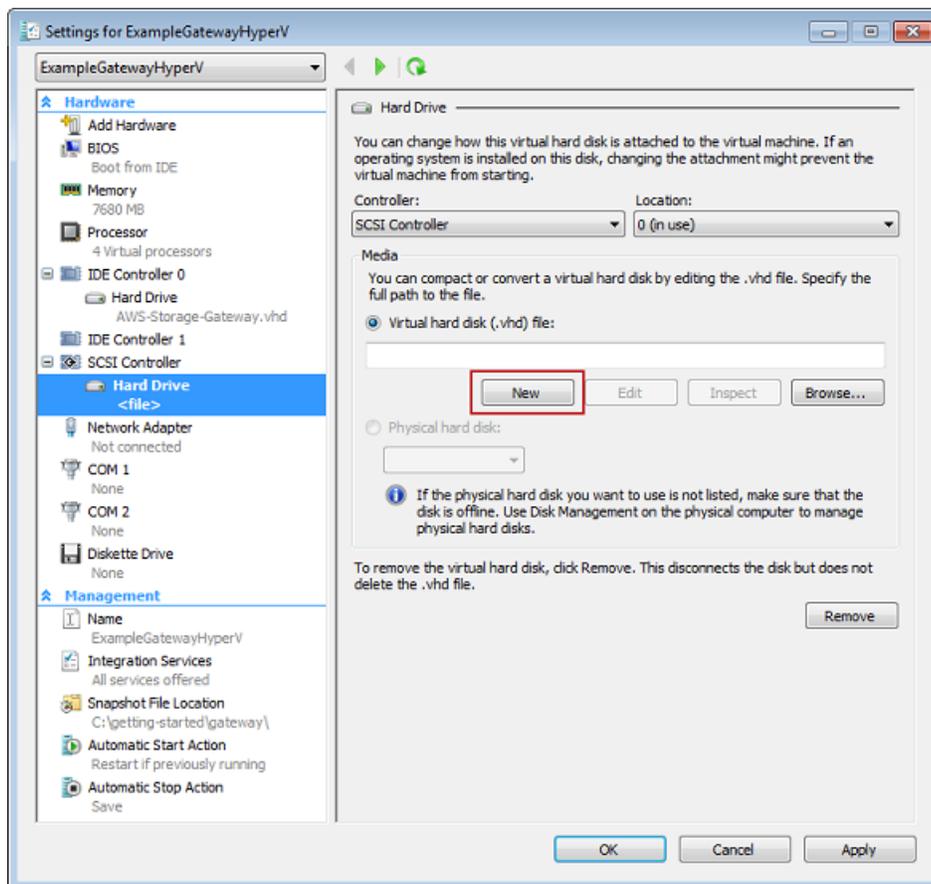
1. 启动 Microsoft Hyper-V Manager，然后连接到虚拟机监控程序。
2. 在虚拟机列表窗格中，选择虚拟机 ExampleGatewayHyperV。
3. 在操作窗格中，选择设置...



4. 在设置窗口中，选择 SCSI 控制器，然后单击添加。

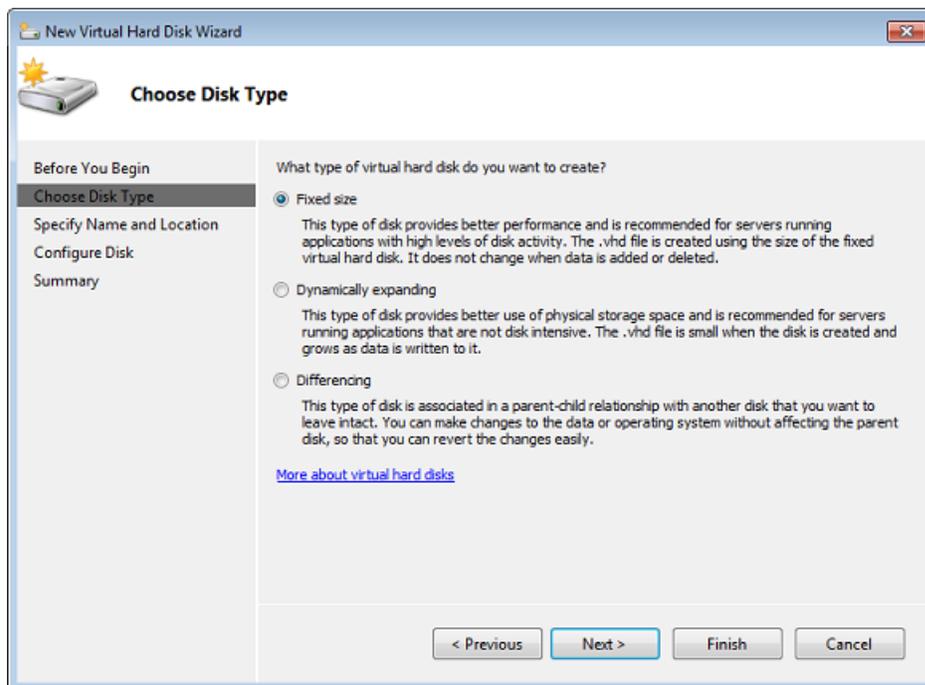


5. 在硬盘驱动器窗格中的介质下，单击新建。



6. 在新建虚拟硬盘向导中，新建一个虚拟硬盘。
  - a. 在开始之前页上，单击下一步。
  - b. 在选择磁盘类型页上，选择固定大小，然后单击下一步。

使用固定大小配置时，将立即分配磁盘存储，这样性能更好。如果不使用固定大小配置，则按需分配存储，这样可能会影响 AWS Storage Gateway 的正常运行。因此，为使 AWS Storage Gateway 正常运行，必须以固定大小配置的格式存储虚拟机磁盘。



c. 在指定名称和位置页上，指定该虚拟硬盘的名称和位置。

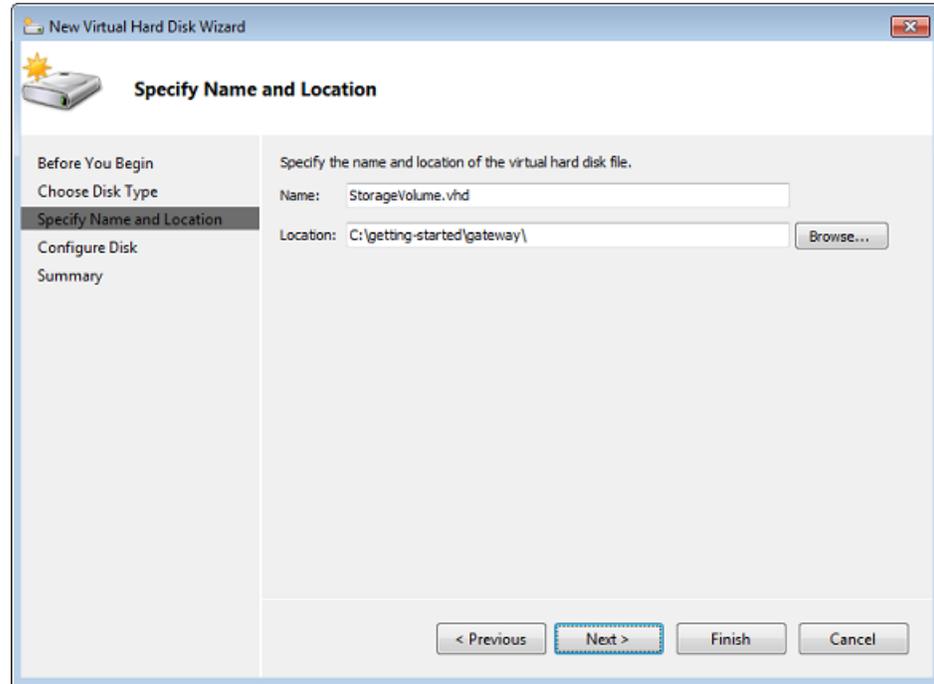
- i. 指定 StorageVolume.vhd 作为名称。
- ii. 将位置指定为 c\$\getting-started\gateway。



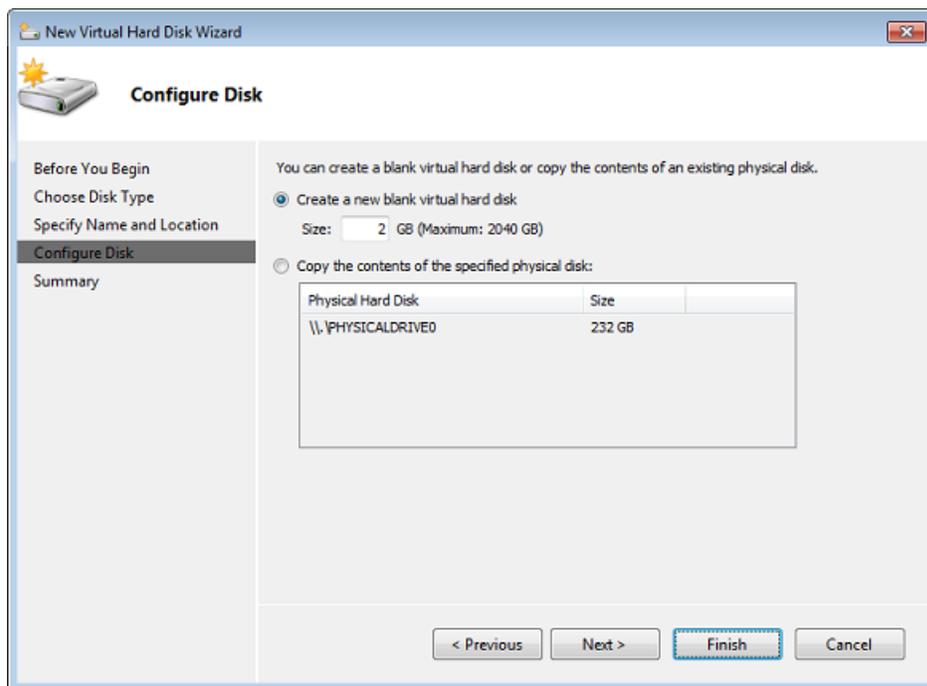
#### Note

在本示例设置中，您使用虚拟机存储虚拟磁盘。对于真实的工作负载，我们强烈建议您不要使用同一底层物理存储磁盘配置本地磁盘。根据主机托管环境、性能和便携性要求，最好在这个步骤选择一个不同的物理磁盘。有关更多信息，请参阅 [预配置本地磁盘 \( 网关存储 \)](#) (p. 100)。

iii. 单击下一步。



- d. 在配置磁盘页中，将磁盘的大小指定为 2 GiB，然后单击完成。



- e. 在创建虚拟磁盘后，确认在 SCSI 控制器下显示硬盘驱动器。  
f. 单击 SCSI 控制器以准备添加另一个硬盘驱动器。

## 为上传缓冲区分配本地磁盘

网关在上传快照到 AWS 时，需要缓存空间以临时存储数据。这一空间称为上传缓冲区。您必须给 VM 添加虚拟磁盘，专供 VM 使用。网关所需上传缓冲区的大小取决于您为存储数据而分配的磁盘大小。有关相关准则，请参阅[配置上传缓冲区的大小 \( 网关存储 \)](#) (p. 104)。

对于本教程，您给 VM 分配 10 GiB 的虚拟磁盘，专供网关使用。在向导的创建磁盘窗格中，输入 10 GiB 作为磁盘大小。

### 如需为上传缓冲区分配本地磁盘

- 重复[如需分配磁盘以存储您的应用程序数据](#) (p. 51) 过程中的步骤以向网关添加另一个虚拟磁盘。除了使用名称 UploadBuffer.vhd 作为磁盘名称，并使用 10 GiB 作为磁盘大小之外，请严格按这些步骤进行操作。

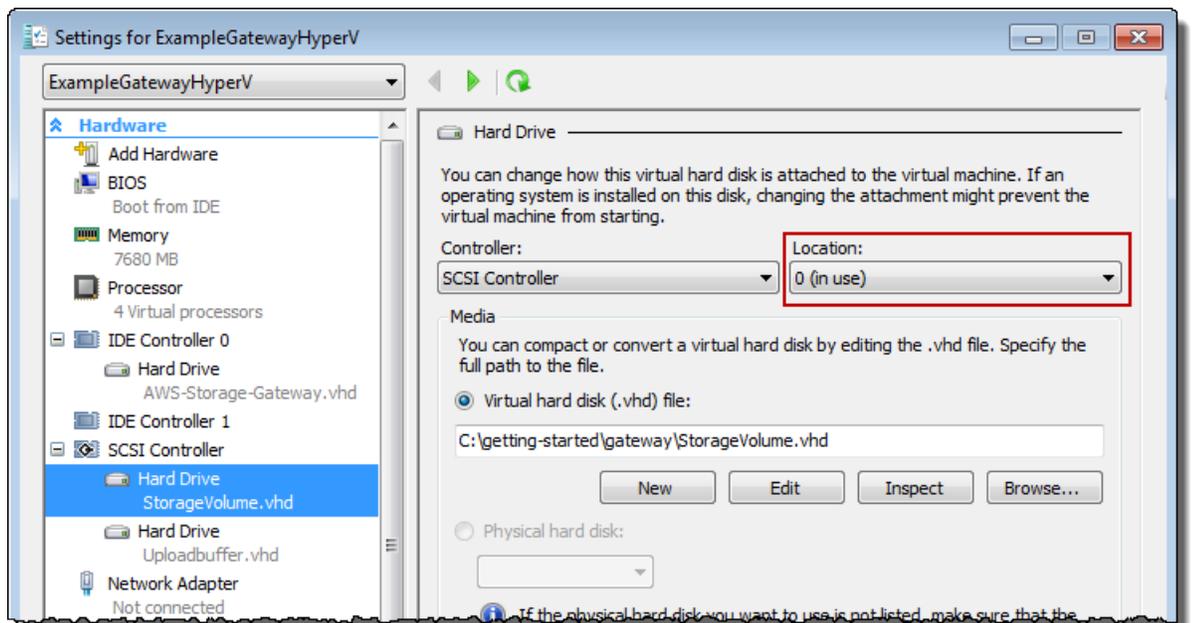
## 验证网关 VM 有两个磁盘

此教程的其余部分要求您已向网关 VM 分配好两个磁盘；请使用下面的可选步骤来验证这一点。如果需要分配其他磁盘，则重复[如需分配磁盘以存储您的应用程序数据](#) (p. 51) 过程中的步骤。

### 如需验证 VM 有两个磁盘

1. 启动 Microsoft Hyper-V Manager，然后连接到虚拟机监控程序。
2. 在虚拟机列表窗格中，选择虚拟机 ExampleGatewayHyperV。
3. 在操作窗格中，选择设置...。
4. 在设置窗口中，选择 SCSI 控制器，然后确认有两个磁盘。

您创建的这两个磁盘随后将在 AWS Storage Gateway 控制台使用，并在下拉列表中显示为 SCSI (0:0) 和 SCSI (0:1)。在下例中，选择 StorageVolume.vhd 磁盘，并且它为 SCSI (0:0)。



## 激活网关

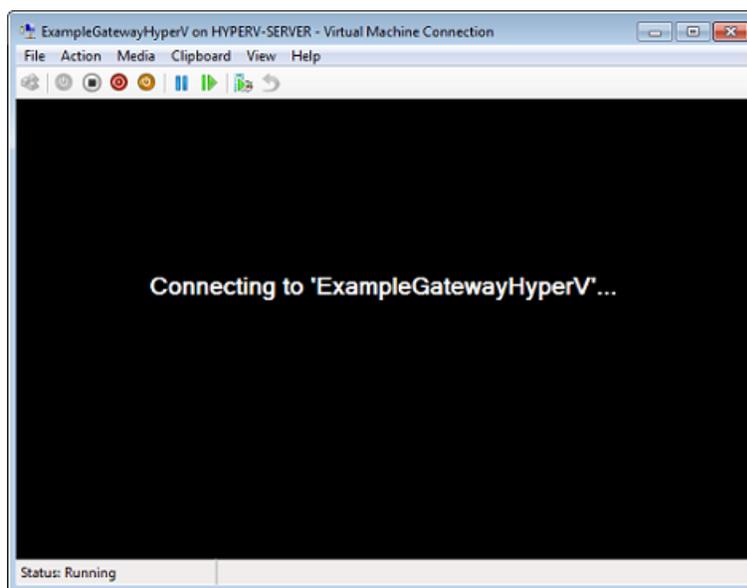
现在，您已可随时激活网关。激活过程将您的网关与 AWS 账户关联。您必须在激活网关前启动网关 VM。

如需激活网关

1. 启动 VM。

- a. 启动 Microsoft Hyper-V Manager，然后连接到虚拟机监控程序。
- b. 在虚拟机列表窗格中，选择虚拟机 ExampleGatewayHyperV。
- c. 在操作窗格中，选择启动。

随后将显示虚拟机连接窗口。

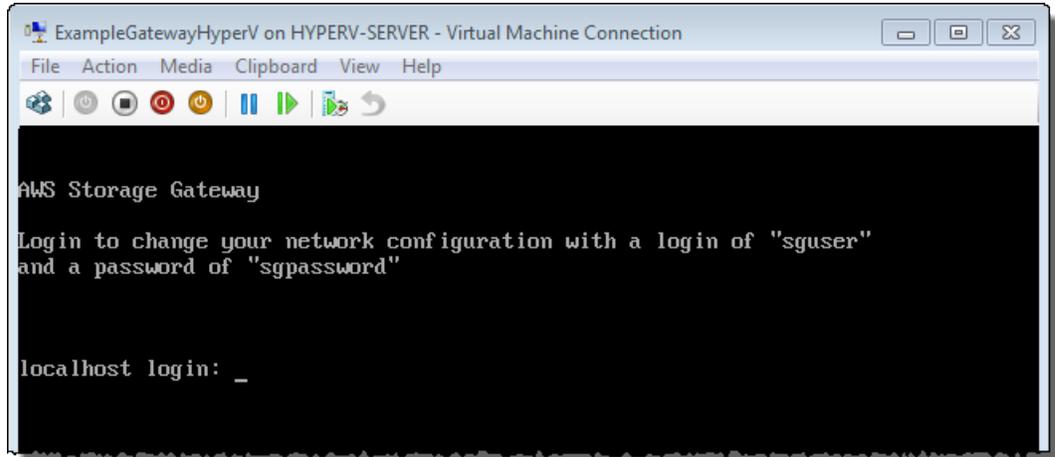


- d. 如果显示身份验证窗口，请输入管理程序管理员向您提供的用户名称和密码。



- e. 在过几分钟时间后，虚拟机就会准备就绪，供您登录了。

下面的示例介绍了您在 VM 准备就绪时会看到的登录提示。



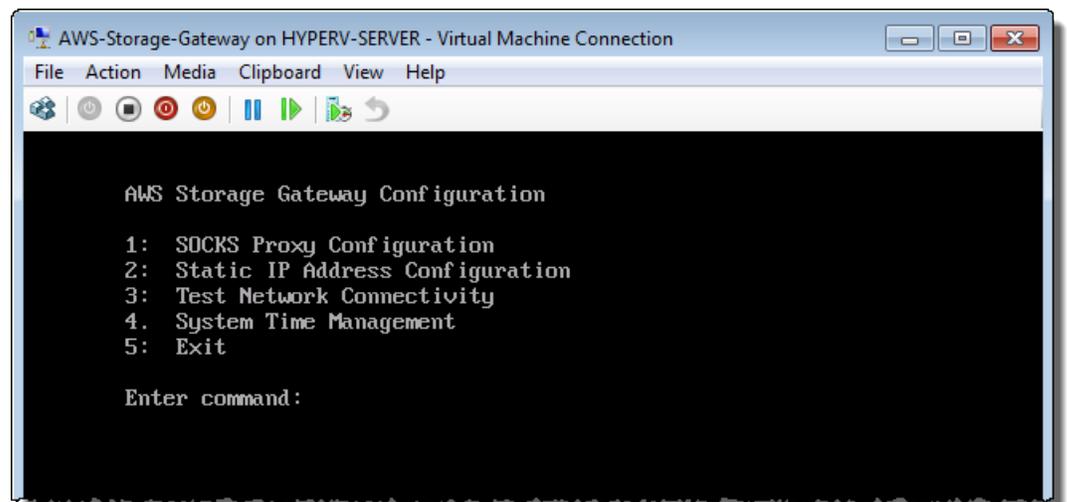
2. 激活网关。

a. 取得您的网关的 IP 地址。

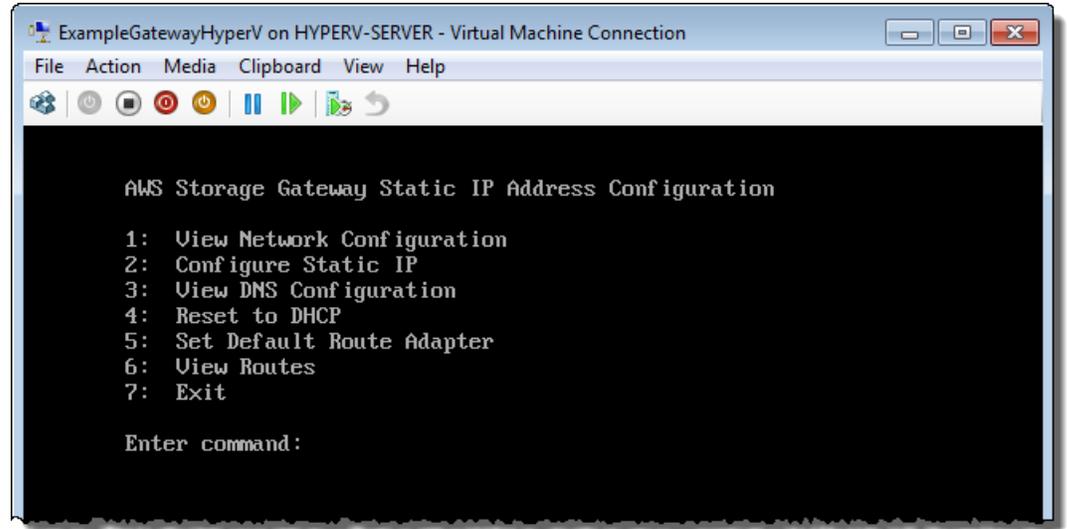
- i. 在 Microsoft Hyper-V Manager 中，选择部署的网关 VM。
- ii. 在虚拟机列表窗格中，选择虚拟机 ExampleGatewayHyperV。
- iii. 在操作窗格中，选择连接...

随后将显示虚拟机连接窗口。

- iv. 在出现登录提示时，输入用户名 `sguser` 和密码 `sgpassword`。
- v. 在 AWS Storage Gateway 配置菜单中，选择选项 2 静态 IP 地址配置。

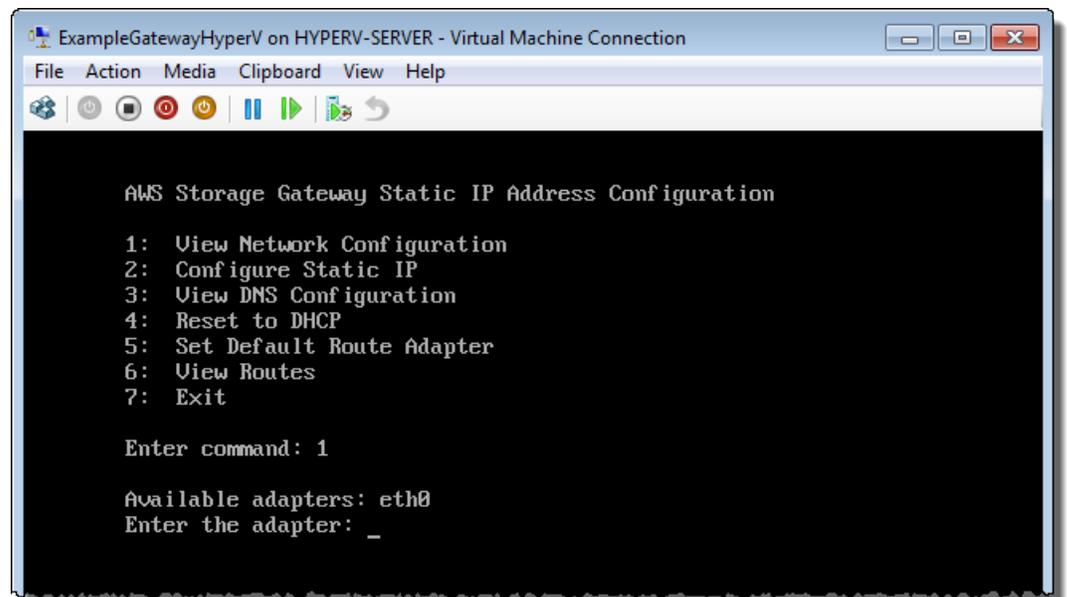


- vi. 在 AWS Storage Gateway 静态 IP 地址配置菜单中，选择选项 1 查看网络配置。



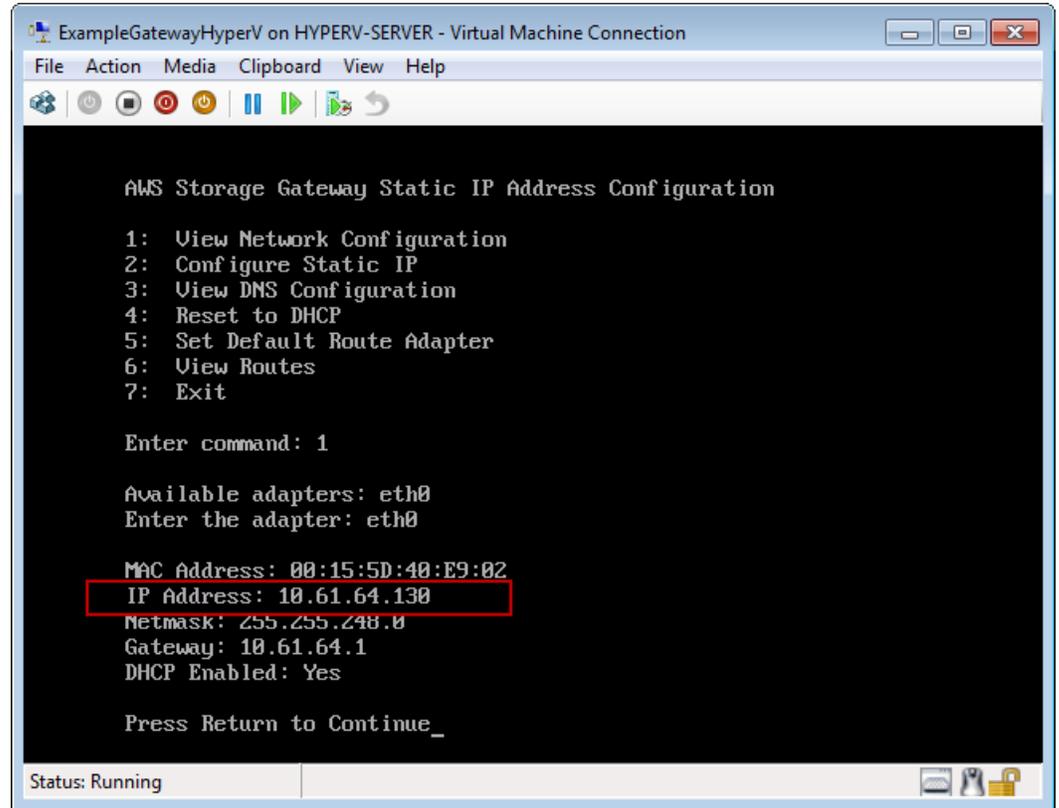
vii. 键入适配器的标识符。

在大多数设置中，eth0 将是适配器标识符。

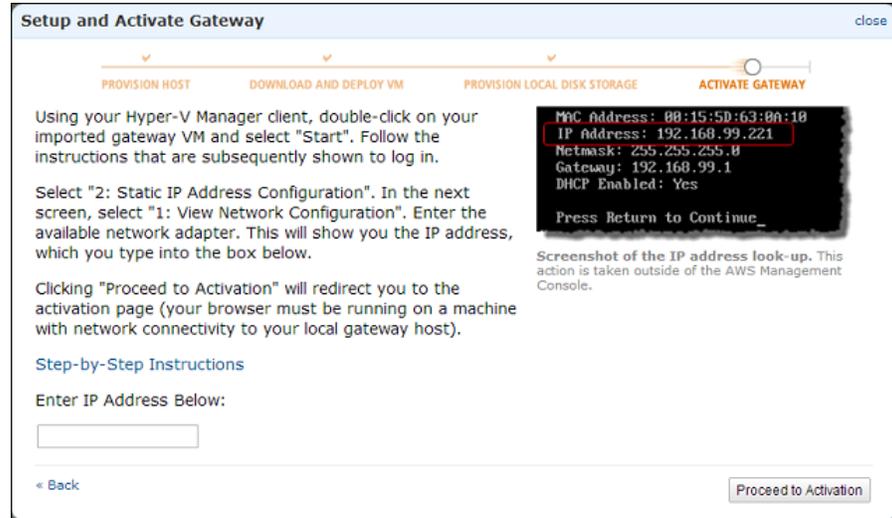


viii. 从适配器信息中获取 IP 地址。

在下例中，IP 地址为 10.61.64.130。您的网关的 IP 地址将会不同。



- ix. 按 Return，然后按提示退出配置菜单。
- b. 将您的网关关联到 AWS 账户。
  - i. 在 AWS Storage Gateway 控制台的设置并激活网关向导中，导航到以下激活网关页。
    - A. 如果尚未启动该向导，则单击设置并激活新网关按钮。
    - B. 在向导的每个步骤中单击继续，直到抵达激活网关页。
  - ii. 输入您的网关的 IP 地址，然后单击继续激活。



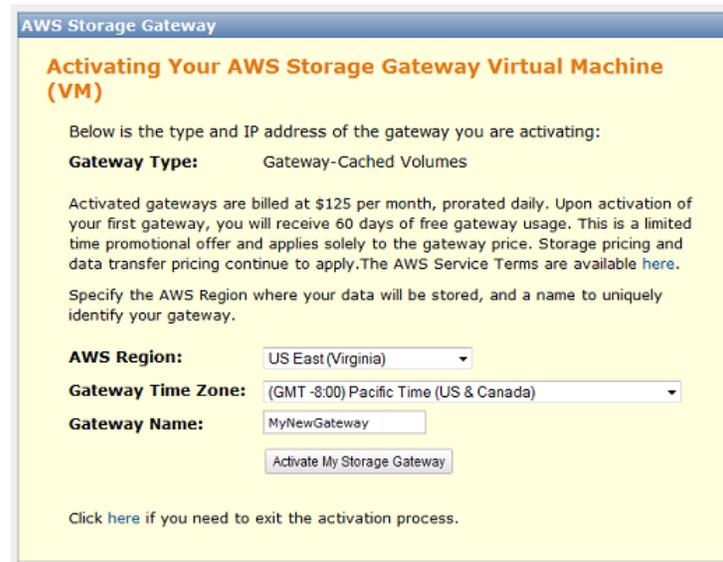
### Note

激活期间，您的浏览器连接到网关。如果激活失败，请检查您输入的 IP 地址是否正确。如果 IP 地址正确，请确认您的网络配置为可允许浏览器访问网关 VM。

- iii. 在激活页面填写完成激活所需的信息。

AWS 地区决定 AWS 存储快照的位置。如果决定将快照还原到某个 Amazon EBS 卷，则该 Amazon EBS 卷必须与快照在同一地区。您不能在网关激活后更改地区。

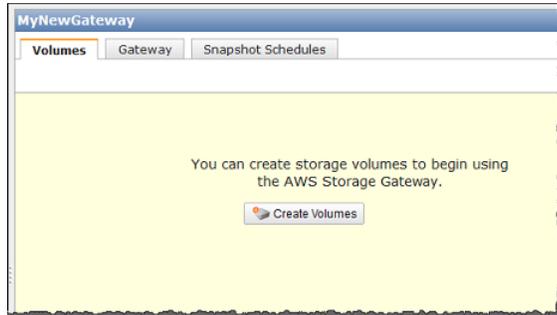
网关名称在控制台中标识您的网关。您使用该名称在控制台中管理网关，可在激活后更改名称。该名称必须是您账户的唯一名称。



- iv. 单击激活我的 Storage Gateway。

成功激活后，AWS 存储网关 控制台在导航窗格的网关部分下显示一个链接，指向已激活的网关。单击您刚刚添加的网关。

随后将显示创建卷按钮。



## 步骤 2：使用 AWS Storage Gateway 控制台创建卷

至此，您已部署了网关 VM、分配了磁盘并且激活了网关。现在您可以随时创建 iSCSI 存储卷。对于这一设置，您使用控制台创建这些卷。

- 如果在测试网关缓存架构的设置 ( 请参阅 [AWS Storage Gateway 的运行原理 \( 架构 \) \(p. 3\)](#) )，则分配以前添加到该 VM 的两个磁盘，其中一个磁盘用于缓存存储，另一个用于上传缓冲区。然后在 Amazon S3 中创建一个 iSCSI 存储卷。本地应用程序中的数据写入此卷，而此卷存储在 Amazon S3 中。网关在缓存存储空间中维护卷最近访问的数据。
- 如果在测试网关存储架构的设置，请创建一个 iSCSI 存储卷，该卷映射到先前添加到 VM 的两个磁盘中的一个。您将剩余磁盘分配到网关的上传缓冲区。数据从您的场内应用程序写入该卷，存储在本地。网关定期拍摄快照 ( 增量备份 ) 并将快照上传到 Amazon S3。

点击下面的链接并按指示创建卷。

如需...	请执行此操作...
创建卷 ( 网关缓存架构 )	按 <a href="#">创建卷 ( 网关缓存 ) (p. 62)</a> 中的步骤进行操作。
创建卷 ( 网关存储架构 )	按 <a href="#">创建卷 ( 网关存储 ) (p. 67)</a> 中的步骤进行操作。

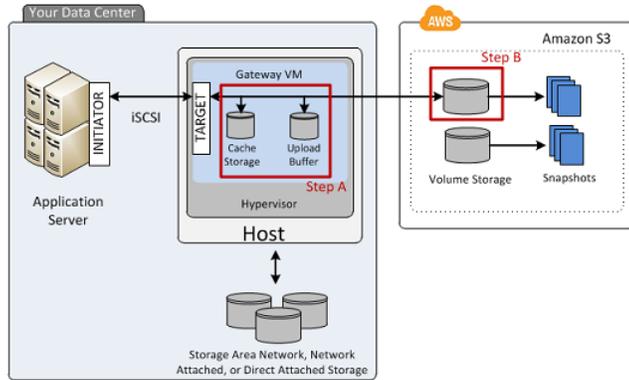
### 创建卷 ( 网关缓存 )

#### Topics

- [在本地磁盘上创建缓存存储和上传缓冲区并配置可选警报 \(p. 63\)](#)
- [在 Amazon S3 中创建卷 \(p. 65\)](#)

在网关缓存设置中 ( 请参阅 [AWS Storage Gateway 的运行原理 \( 架构 \) \(p. 3\)](#) )，分配以前添加到该 VM 的两个磁盘，分别用于缓存存储和上传缓冲区。然后在 Amazon S3 中创建一个 iSCSI 存储卷。本地应用程序中写入此卷的数据存储在 Amazon S3 中。网关在缓存存储空间中维护卷最近访问的数据。

下面的架构示意图显示您在创建网关缓存设置的哪个部分。



### 在本地磁盘上创建缓存存储和上传缓冲区并配置可选警报

在本步骤中，您在本地磁盘上创建缓存存储空间和上传缓冲区并配置警报。

如需创建本地卷（缓存存储空间和上传缓冲区）

1. 在控制台的导航窗格中，选择您的网关，单击卷选项卡，然后单击创建卷。



2. 在配置已激活的网关向导中，配置本地的工作存储，它由上传缓冲区和缓存存储组成。



- a. 在您预配置的两个磁盘中选择一个作为上传缓冲区，选择另一个作为缓存存储区，如下示例所示。

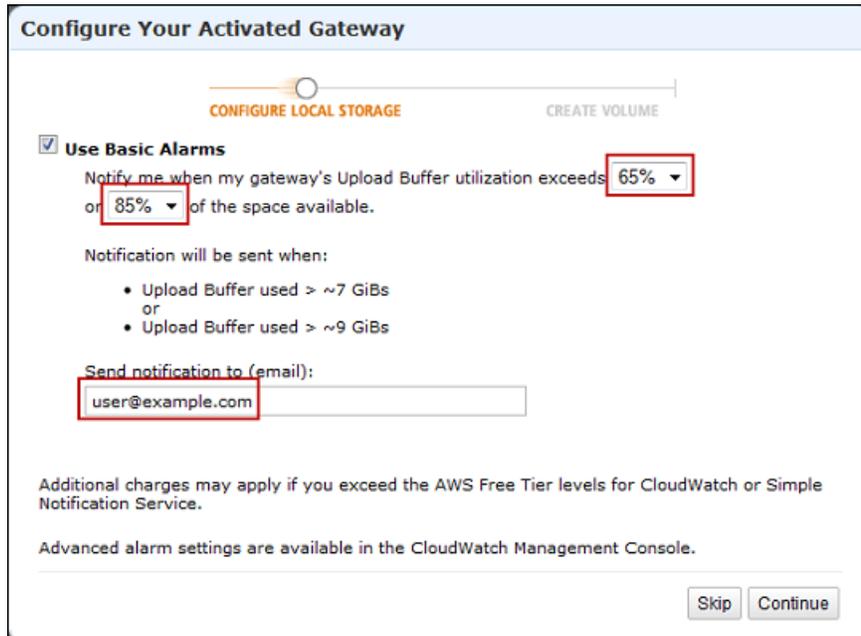


- b. 单击下一步。

现在您可以创建可选警报以监控您所创建的两个卷的存储空间使用率。

#### 如需配置可选警报

1. 在上传缓冲区警报对话框中，配置上传缓冲区使用率警报。



- a. 使用两个下拉框，选择用来创建两个上传缓冲区警报的使用率。

例如，您可以选择阈值，从而让第一个阈值（较低百分率值）代表您希望在其被超过的情况下收到相关警报的上传缓冲区使用率。可以选择第二个阈值来代表这样一个上传缓冲区使用率，即在其超过的情况下成为添加更多上传缓冲区空间等操作的触发原因。

完成此步骤后，可随时转到 Amazon CloudWatch 控制台并更改警报阈值。

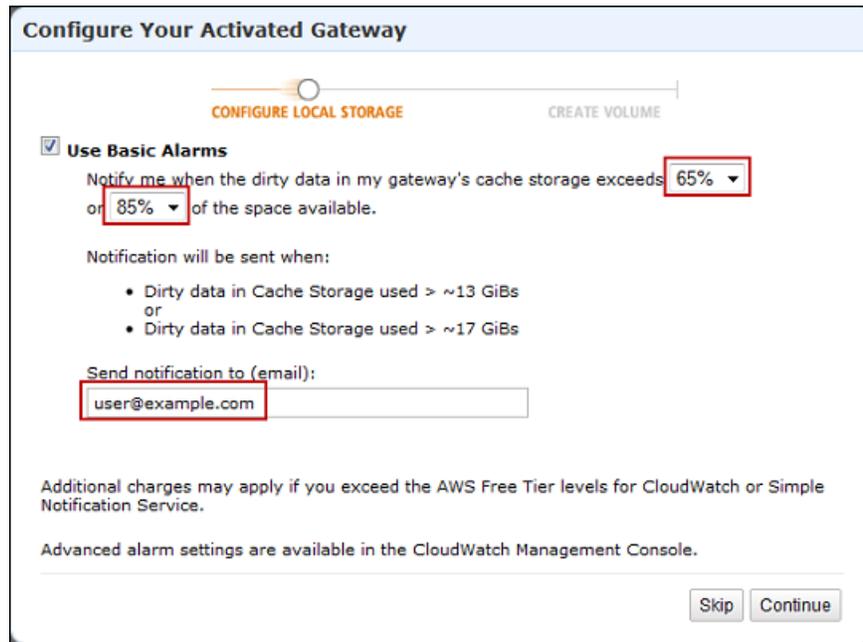
- b. 输入电子邮箱地址。

- c. 单击继续。

创建了两个警报。例如，使用网关名称 *MyNewGatewayCached*，则创建的警报为 *MyNewGatewayCached-UploadBufferUtilization-Alarm1* 和 *MyNewGatewayCached-UploadBufferUtilization-Alarm2*。

- d. 检查是否向指示的电子邮件地址发送了订阅确认电子邮件，然后按这封电子邮件中的说明确认您对 Amazon Simple Notification Service (Amazon SNS) 主题的订阅。确认订阅后，无论超过了您指定的哪一阈值，都会收到电子邮件。

2. 单击继续以创建警报。
3. 在缓存存储空间警报对话框中，配置缓存存储空间警报。



**Configure Your Activated Gateway**

CONFIGURE LOCAL STORAGE CREATE VOLUME

**Use Basic Alarms**

Notify me when the dirty data in my gateway's cache storage exceeds 65% or 85% of the space available.

Notification will be sent when:

- Dirty data in Cache Storage used > ~13 GiBs
- or
- Dirty data in Cache Storage used > ~17 GiBs

Send notification to (email):

user@example.com

Additional charges may apply if you exceed the AWS Free Tier levels for CloudWatch or Simple Notification Service.

Advanced alarm settings are available in the CloudWatch Management Console.

Skip Continue

按上一步骤中的指示配置配置该警报。

例如，使用网关名称 *MyNewGatewayCached*，则创建的警报为 *MyNewGatewayCached-CacheUtilization-Alarm1* 和 *MyNewGatewayCached-CacheUtilization-Alarm2*。

4. 单击继续以创建警报。

在下一节中，继续在 Amazon S3 中创建卷存储。

## 在 Amazon S3 中创建卷

在上一部分中，您在场内硬件上创建了卷（缓存存储空间和上传缓冲区）。现在，您在 Amazon S3 中创建卷存储。这是您存放应用程序数据的地方。

### 在 Amazon S3 中创建缓存卷

1. 在配置已激活的网关对话框中，在 Amazon S3 中创建一个 iSCSI 存储卷。

**Configure Your Activated Gateway** close

CONFIGURE LOCAL STORAGE CREATE VOLUME

Create an iSCSI storage volume up to 32 TBs in size. This volume will be stored in Amazon S3, with only a cache of recently accessed data kept locally. Your client applications will connect to this volume over an iSCSI interface. [Learn More](#).

**Capacity:** 50 TBs (Max: 32 TBs)

**iSCSI Target Name:** iqn.1997-05.com.amazon:myvolume

**Based on Snapshot ID:**

**Host IP:** 192.168.99.227

**Port:** 3260

Cancel Create Volume

- a. 对于容量，指定 50 GiB。

您可以指定的最大上限为 32 TiB。

- b. 在 iSCSI 目标名称字段中输入一个名称。

目标名称可包含小写字母、数字句点 (.) 和连词符 (-)。经过发现后，在 iSCSI Microsoft 发起程序用户界面的目标选项卡中，此目标名称显示为 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 SAN 网络内具有全局唯一性。

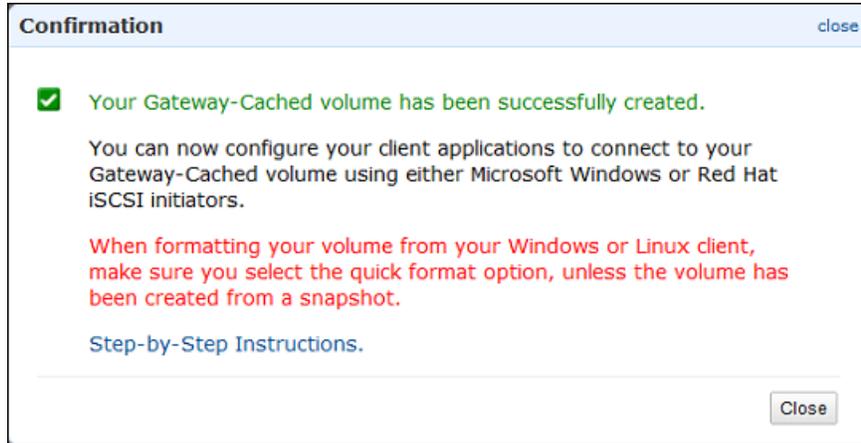
在本教程中，使用 `myvolume`。

- c. 将基于快照 ID 字段留空。

如果您希望将现有的 Amazon EBS 快照或网关快照继续还原为正在创建的存储卷，则必须指定快照 ID。网关将您现有的快照数据下载到存储卷。

- d. 确认主机 IP 字段为您的网关的 IP 地址，然后单击创建缓存卷。

2. 在配置 iSCSI 发起程序对话框中，单击关闭。



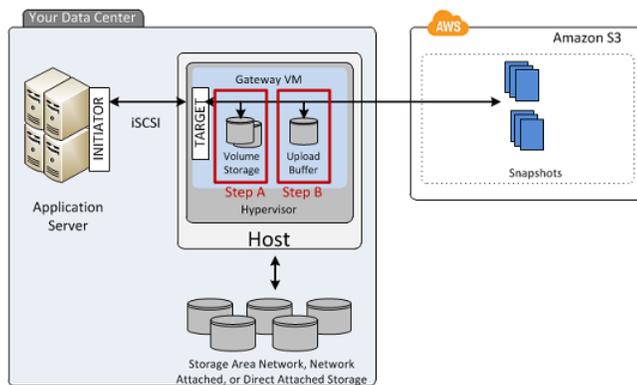
## 创建卷 (网关存储)

### Topics

- [创建存储卷 \(p. 67\)](#)
- [创建上传缓冲区 \(p. 69\)](#)

在网关存储设置中 (请参阅 [AWS Storage Gateway 的运行原理 \(架构\) \(p. 3\)](#))，创建一个 iSCSI 存储卷，它映射到以前添加到该 VM 的两个磁盘之一。您将剩余磁盘分配到网关的上传缓冲区。您的场内应用程序写入该卷的数据存储在本地。网关定期拍摄快照 (增量备份) 并将快照上传到 Amazon S3。

下面的架构概览示意图显示您正在创建的网关存储设置部分。



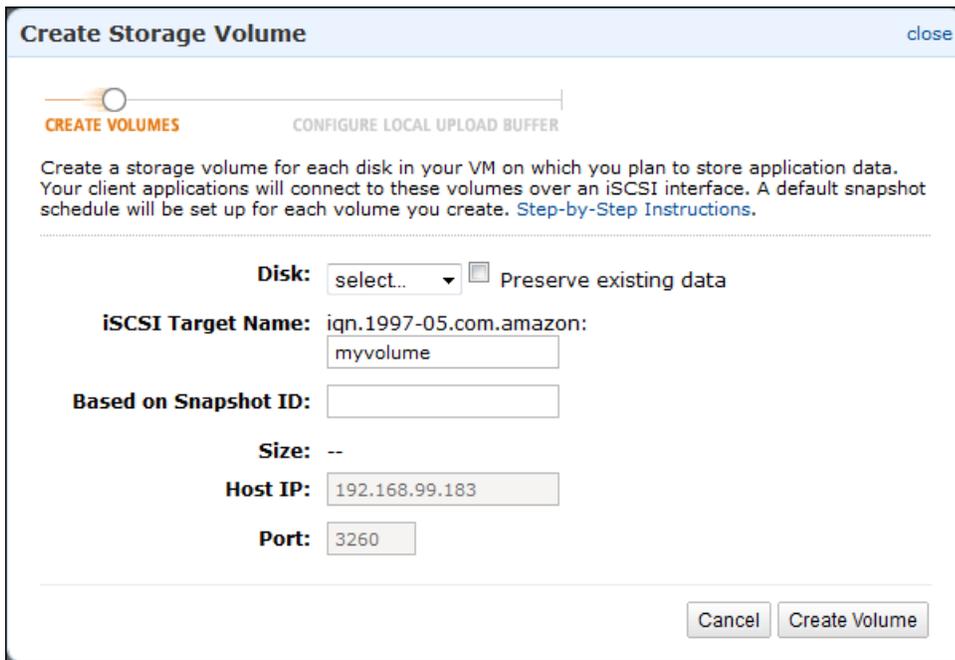
## 创建存储卷

### 如需创建存储卷

1. 在控制台的导航窗格中，选择您的网关，单击卷选项卡，然后单击创建卷。



2. 在创建存储卷向导中，提供存储卷信息。



- a. 在磁盘字段的下拉列表中，选择您的 VM 上的 2 GiB 虚拟磁盘。  
该下拉列表显示您添加到网关 VM 的虚拟磁盘。选择您计划用来存储数据的磁盘。
- b. 使保留现有数据复选框保持取消选中。



**Caution**

确保您在虚拟磁盘上没有任何数据。该磁盘上的任何现有数据都会丢失。

- c. 在 iSCSI 目标名称字段中输入一个名称。  
目标名称可包含小写字母、数字句点 (.) 和连字符 (-)。经过发现后，在 iSCSI Microsoft 发起程序用户界面的目标选项卡中，此目标名称显示为 iSCSI 目标节点名称。例如，名称 target1 将显示为 iqn.1007-05.com.amazon:target1。确保目标名称在您的 SAN 内具有全局唯一性。
- d. 将基于快照 ID 字段留空。  
如果您希望将现有的 Amazon EBS 快照或网关快照继续还原为正在创建的存储卷，则必须指定快照 ID。网关将您现有的快照数据下载到存储卷。

- e. 确认主机 IP 设置是您的网关的 IP 地址，然后单击创建卷。

**Create Storage Volume** close

**CREATE VOLUMES** CONFIGURE LOCAL UPLOAD BUFFER

Create a storage volume for each disk in your VM on which you plan to store application data. Your client applications will connect to these volumes over an iSCSI interface. A default snapshot schedule will be set up for each volume you create. [Step-by-Step Instructions](#).

**Disk:** SCSI (0:0)  Preserve existing data

**iSCSI Target Name:** iqn.1997-05.com.amazon:  
myvolume

**Based on Snapshot ID:**

**Size:** 2 GiB

**Host IP:** 192.168.99.183

**Port:** 3260

Cancel Create Volume

### 创建上传缓冲区

AWS Storage Gateway 需要存储空间以缓冲您的传入应用程序数据，然后再将其上传到 AWS。在本步骤中，您将一个磁盘配置为上传缓冲区。



#### Note

将磁盘配置为上传缓冲区时，您会丢失磁盘上的任何现有数据，因此请注意保留您的数据。

为您的 AWS Storage Gateway VM 分配上传缓冲区

1. 在创建存储卷对话框中，单击配置本地上传缓冲区。

**Create Storage Volume** close

CREATE VOLUMES CONFIGURE LOCAL UPLOAD BUFFER

Create a storage volume for each disk in your VM on which you plan to store application data. Your client applications will connect to these volumes over an iSCSI interface. A default snapshot schedule will be set up for each volume you create. [Step-by-Step Instructions](#).

Disk:   Preserve existing data

iSCSI Target Name:

Based on Snapshot ID:

Size: 2 GiB

Host IP:

Port:

1 Volume Created

To start using the volumes you have created, proceed to the next step of allocating local Upload Buffer for your gateway.

2. 选择剩余磁盘旁的复选框以分配该磁盘作为上传缓冲区，然后单击下一步。

该对话框列出您的 VM 上所有可用的磁盘。您此前向 VM 添加了两个虚拟磁盘，并且将其中一个配置为存储卷。因此，对话框应显示一个可用磁盘。选择该磁盘，将其分配为上传缓冲区。您随后可以扩展上传缓冲区，而不打断 iSCSI I/O。

**Configure Local Upload Buffer** close

CREATE VOLUMES CONFIGURE LOCAL UPLOAD BUFFER

Please select which disks the VM can use for Upload Buffer. Please see our documentation for recommendations on how much space to provide given your workload and network connection. [Step-by-Step Instructions](#)

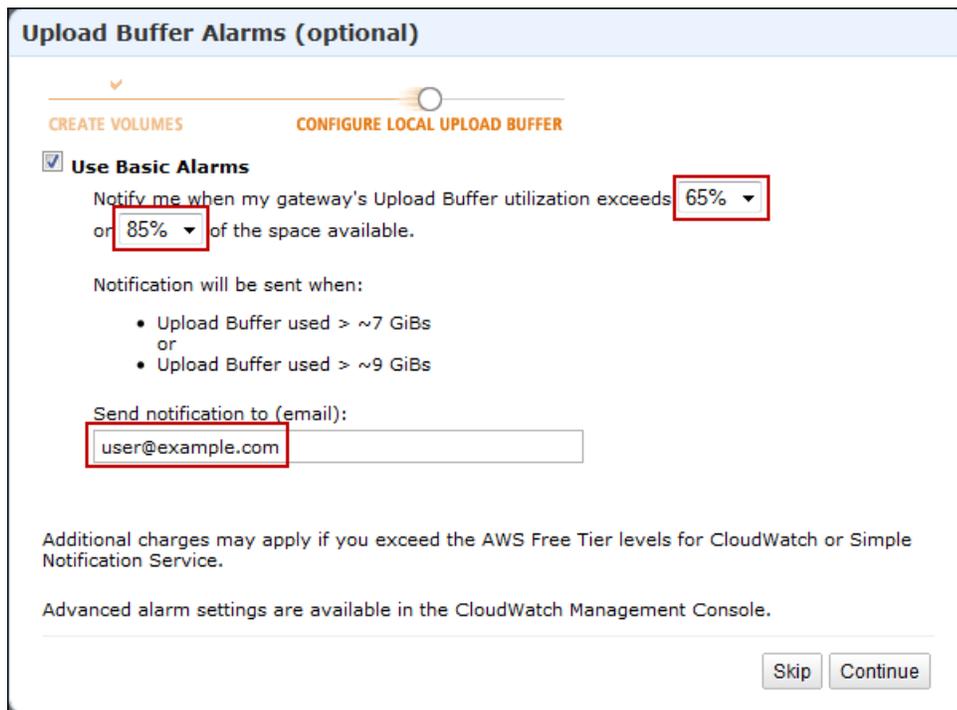
**Local Disks**

SCSI (0:0)	2.00 GiB	<input type="checkbox"/>	In Use for Storage Volume
SCSI (0:1)	10.00 GiB	<input checked="" type="checkbox"/>	Use for Upload Buffer Space

3. 在确认对话框中，选中复选框，然后单击确认。



4. 在上传缓冲区警报对话框中，为您的上传缓冲区配置警报。



- a. 使用两个下拉框，选择用来创建两个上传缓冲区警报的使用率。

例如，您可以选择阈值，从而让第一个阈值（较低百分率值）代表您希望在其被超过的情况下收到相关警报的上传缓冲区使用率。可以选择第二个阈值来代表这样一个上传缓冲区使用率，即在其超过的情况下成为添加更多上传缓冲空间等操作的触发原因。

完成此步骤后，可随时转到 Amazon CloudWatch 控制台并更改警报阈值。

- b. 输入电子邮箱地址。  
c. 单击继续。

创建了两个警报。以本教程中的网关名称为例，警报的名称将为 *MyNewGateway-UploadBufferUtilization-Alarm1* 和 *MyNewGateway-UploadBufferUtilization-Alarm2*。

- d. 检查是否向指示的电子邮件地址发送了订阅确认电子邮件，然后按这封电子邮件中的说明确认您对 Amazon Simple Notification Service (Amazon SNS) 主题的订阅。确认订阅后，无论超过了您指定的哪一阈值，都会收到电子邮件。

有关创建上传缓冲区警报的更多详细信息，请参阅[监控上传缓冲区 \(p. 249\)](#)。

5. 在配置 iSCSI 发起程序对话框中，单击关闭。



### 步骤 3 : 访问您的 AWS Storage Gateway 卷

现在，您可以随时将 Windows 客户端连接到 iSCSI 存储卷。在本练习中，您在您的客户端上使用 Microsoft iSCSI 发起程序进行此项连接。有关从 Linux 中访问 iSCSI 存储卷的说明，请参阅[从 Red Hat 连接到您的存储卷 \(p. 156\)](#)。



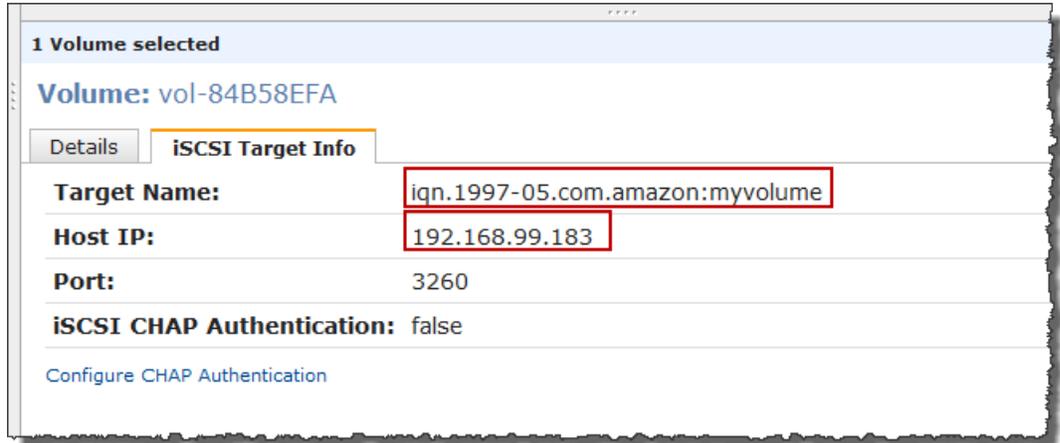
#### Note

运行 iSCSI 启动程序您需要有管理员权限。

如需将您的 Windows 客户端连接到存储卷

1. 您需要即将连接的存储卷的主机 IP 和目标名称信息。可在 AWS Storage Gateway 控制台中找到此信息。
  - a. 在控制台的导航窗格中，选择您的网关。
  - b. 在卷选项卡中，单击要连接到的卷。

iSCSI 目标信息选项卡显示将您的客户端连接到此卷所需的信息。



您将使用目标名称和主机 IP，如上图中所突出显示。以下步骤需要主机 IP，而目标名称用于确认选择的 iSCSI 目标正确无误。



#### Warning

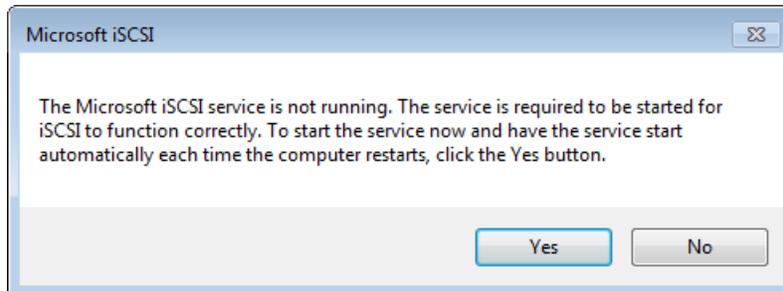
对于部署在 Amazon EC2 实例上的 Amazon Storage Gateway，不支持通过公共 Internet 访问网关。无法使用 EC2 实例的弹性 IP 地址作为目标地址。

## 2. 启动 iSCSI 启动程序。

- a. 在 Windows 客户端计算机的开始菜单中，输入 `iscsicpl.exe` 并运行该程序。

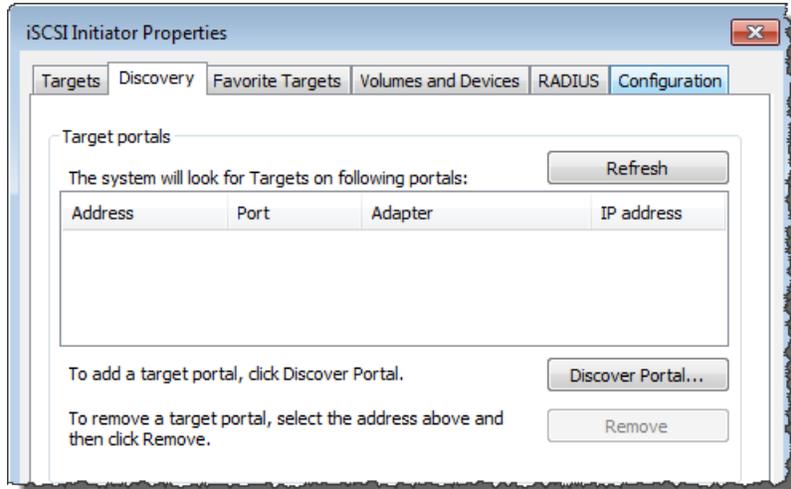
如果正在运行 iSCSI 发起程序服务，则显示 iSCSI 发起程序属性对话框。

- b. 如果 Microsoft iSCSI 启动程序服务不在运行，系统就会提示您启动服务并让服务在计算机每次开机时自动运行。在 Microsoft iSCSI 对话框中单击是以启动该服务。

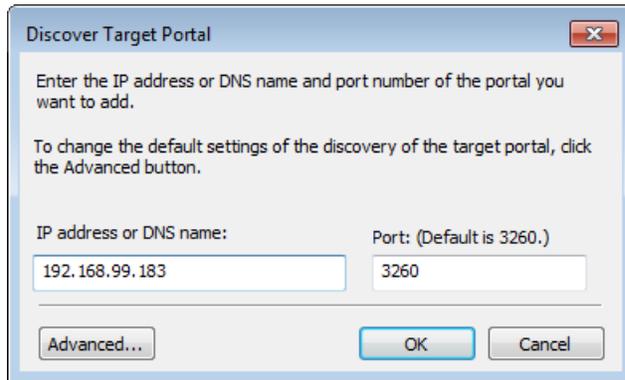


## 3. 发现网关：

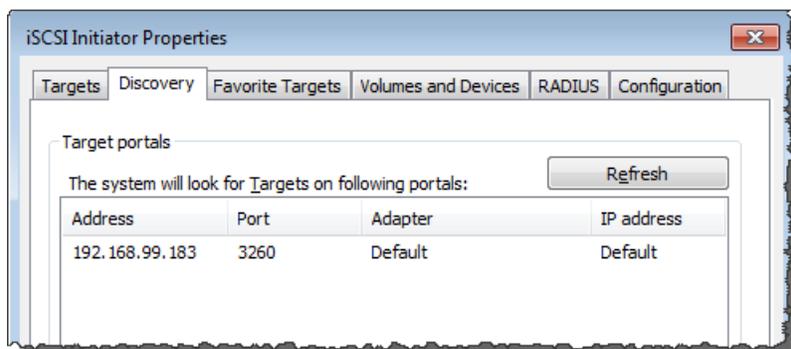
- a. 在 iSCSI 发起程序属性对话框中，单击发现选项卡，然后单击发现门户按钮。



- b. 在发现目标门户对话框的 IP 地址或 DNS 名称字段中，输入 iSCSI 目标的 IP 地址，然后单击确定。



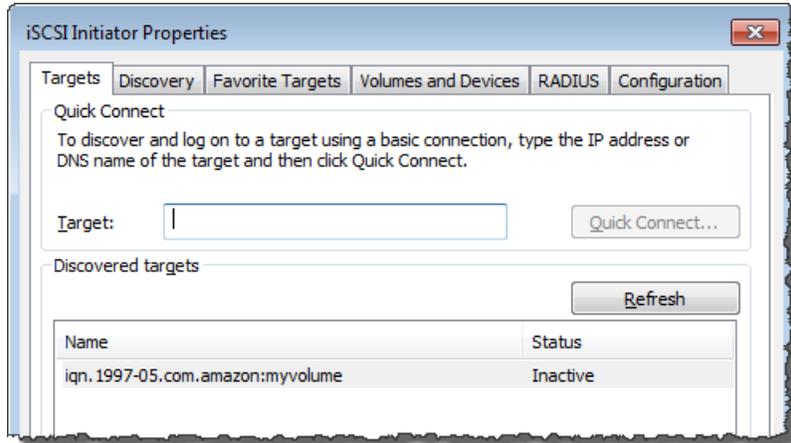
- c. 现在，发现选项卡中的目标门户列表中显示该 IP 地址。



4. 连接到网关上的存储卷目标：

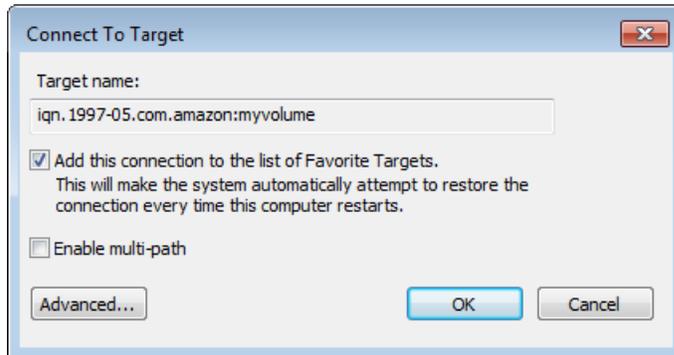
- a. 单击目标选项卡。

您刚刚发现的目标以未激活状态显示。请注意显示的目标名称应该与您在步骤 1 中记下的存储卷名称相同。

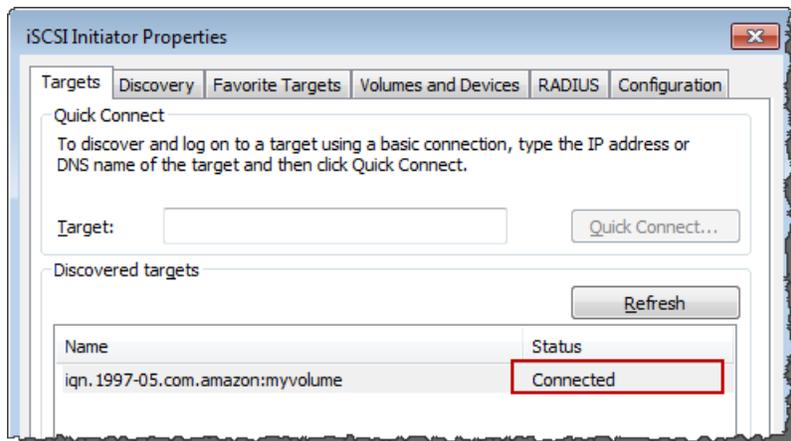


- b. 选择该目标，然后单击连接。

在连接到目标对话框中，如果尚未预先填充目标名称，则按第 1 步所示，输入目标的名称，选中将此连接添加到收藏的目标列表旁的复选框，然后单击确定。



- 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。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。您可以通过 Windows 磁盘管理工具进行此项操作。



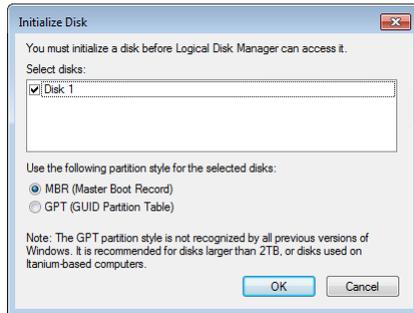
### Note

尽管对于本练习并非必需，但我们仍强烈建议您为真实应用程序自定义您的 iSCSI 设置，如同[自定义您的 Windows iSCSI 设置 \(p. 154\)](#)主题中讨论的那样。

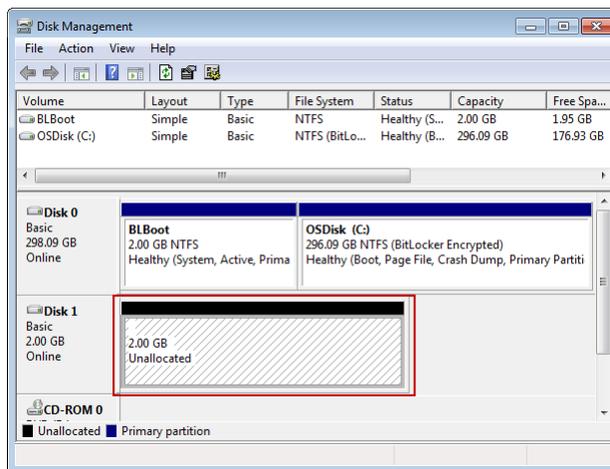
如需初始化并格式化您刚刚映射的存储卷

1. 在开始菜单中，输入 `diskmgmt.msc` 以打开磁盘管理控制台。
2. 在初始化磁盘对话框中，选择 MBR (主启动记录) 作为分区类型，然后单击确定。选择分区类型时，应考虑所连接到的卷的类型 ( 缓存卷或存储卷 )，如下表所示。

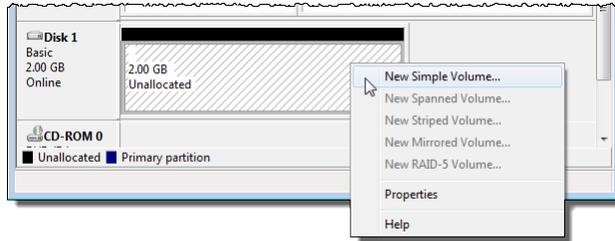
分区形式	用于以下情况
MBR ( 主启动记录 )	适用于所有存储卷 ( 大小上限为 1 TiB )，或者少于 2 TiB 的缓存卷。
GPT ( GUID 分区表 )	所有存储卷和缓存卷。对于超过 2 TiB 的缓存卷，您必须使用 GPT。



3. 创建简单卷：
  - a. 如果磁盘为脱机状态，您必须在初始化前将其联机。磁盘初始化后，可随时格式化为简单卷。所有可用的卷均显示在磁盘管理控制台中。在下例中，磁盘 1 为存储卷。请注意选择新卷后，卷将会显示剖面线，表示已选定。

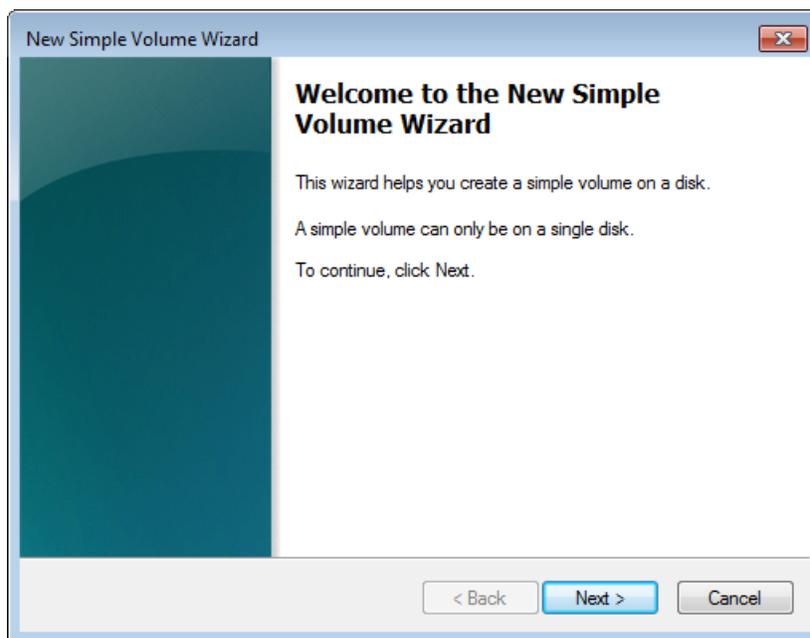


- b. 右键单击该磁盘，然后选择新建简单卷。

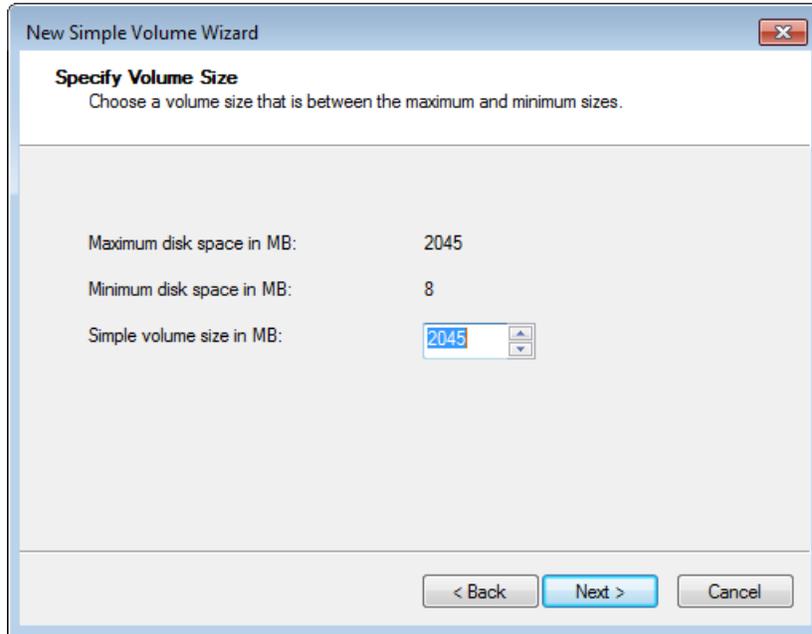


### Important

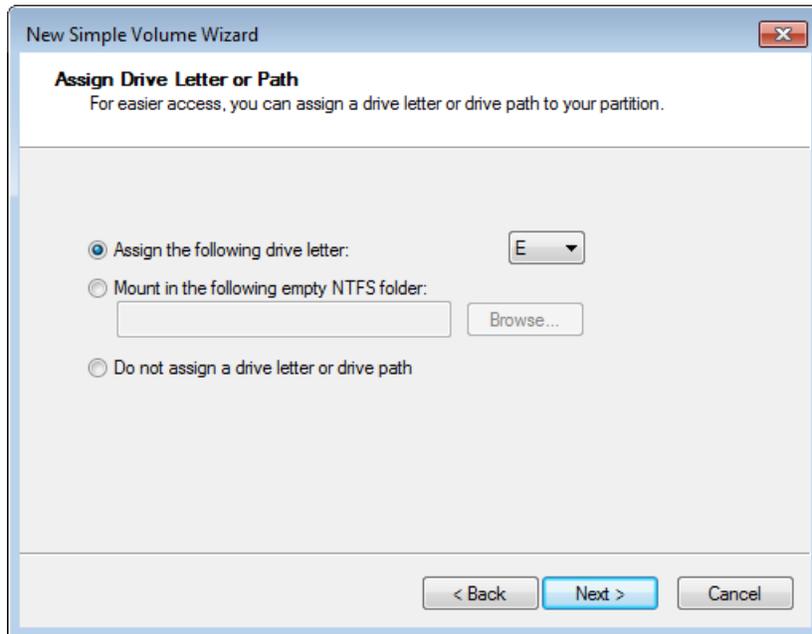
请谨慎处理，避免错误地将其他磁盘格式化。检查以确保所格式化的磁盘与分配给网关 VM 的本地磁盘的大小相匹配，并且其状态为未分配。



- c. 在新建简单卷向导中，单击下一步。
- d. 在指定卷大小对话框中，保留默认值，然后单击下一步。



- e. 在分配驱动器号或路径对话框中，保留默认值，然后单击下一步。

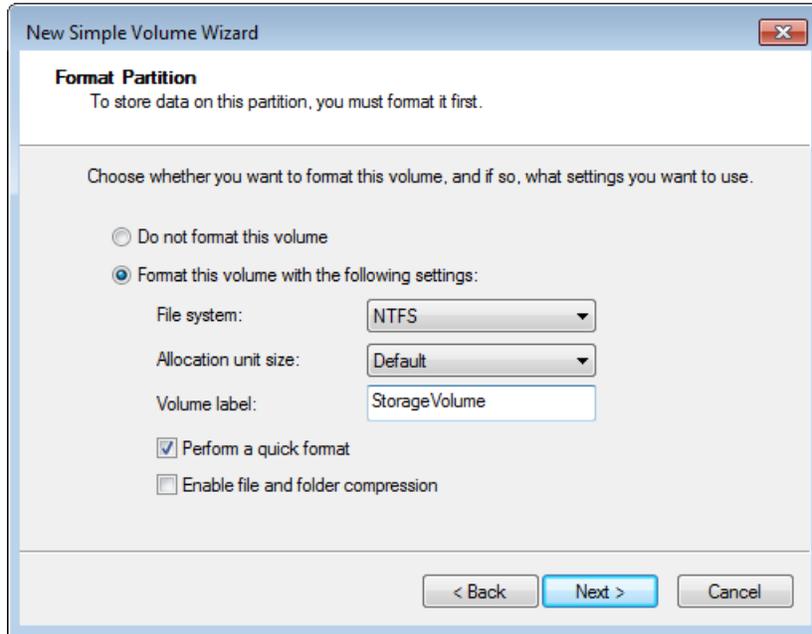


- f. 在格式化分区对话框中，指定某个卷标字段，然后确保选择了执行快速格式化。单击下一步。



#### Caution

强烈建议对于缓存卷选择执行快速格式化，因为这样可减少初始化 I/O、减小初始快照大小、使卷最快地可用，并可避免仅因完全格式化过程而非任何与应用程序数据相关的活动而使用缓存卷。

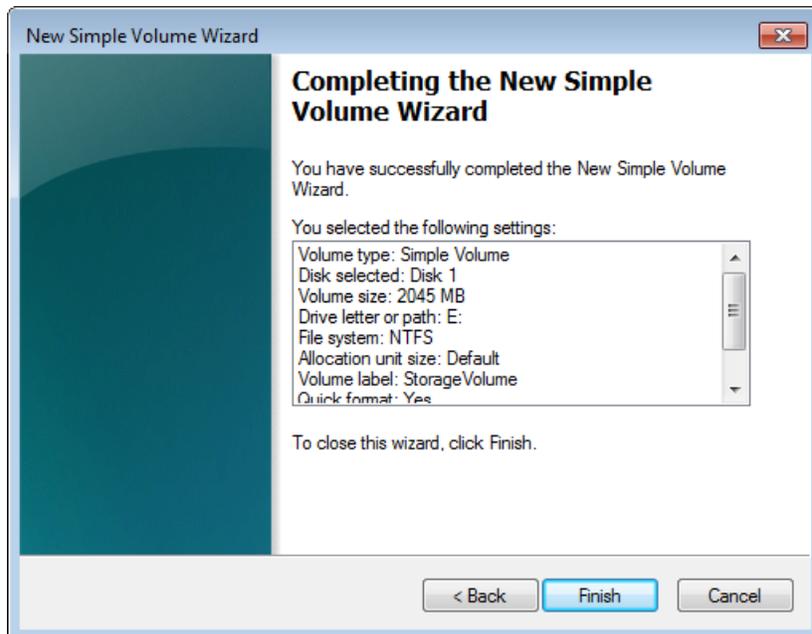


- g. 单击完成以关闭向导。



**Note**

格式化卷所需的时间取决于卷的大小，可能需要几分钟。



## 步骤 4 : 测试设置

此时，您就拥有了具有一个 iSCSI 存储卷的激活网关。现在，您可随时通过将数据写入卷、拍摄快照以及将快照还原到另一个卷来测试您的设置。

单击下列任一链接，然后按指示测试链接。

如需...	请执行此操作...
测试设置 (网关缓存架构)	按 <a href="#">测试设置 (网关缓存)</a> (p. 80)中的步骤进行操作。
测试设置 (网关存储架构)	按 <a href="#">测试设置 (网关存储)</a> (p. 83)中的步骤进行操作。

### 测试设置 (网关缓存)

本部分中，您通过拍摄网关缓存卷的快照备份来验证设置。然后将其还原到另一个卷。

此项操作需要您首先创建卷的快照。然后从该快照创建另一个卷。您的网关从 AWS 中的指定快照复制数据到新卷。

如需创建存储卷快照

1. 在 Windows 计算机上，将一些数据复制到您的映射存储卷上。

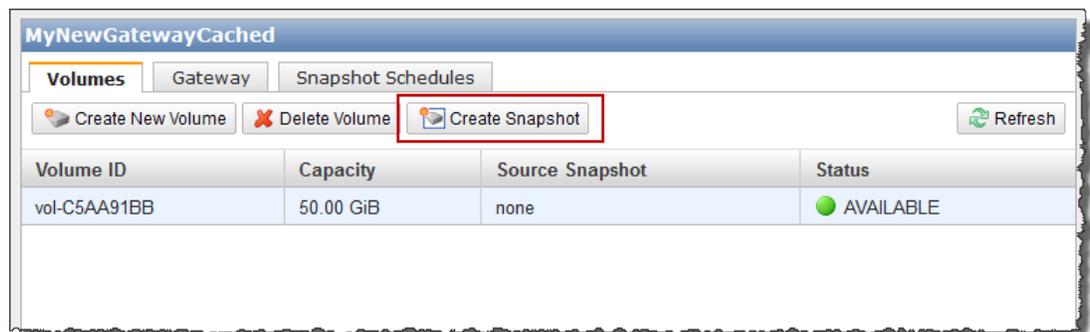
复制的数据量对于本示范无关紧要。一个小文件即足够用来展示还原过程。

2. 在 AWS Storage Gateway 控制台的导航窗格中，选择该网关。
3. 在卷选项卡中，选择为该网关创建的存储卷。

该网关应仅有一个存储卷。选择卷时，会显示它的属性。

4. 单击创建快照按钮以创建该卷的快照。

根据磁盘上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。记录您为其创建快照的卷的 ID。该 ID 用来查找快照。



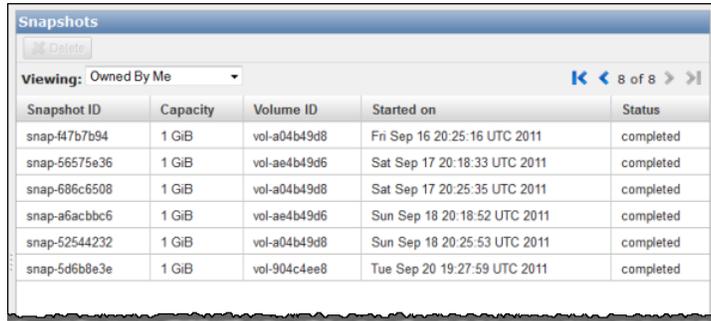
5. 在拍摄了快照确认窗口中，单击关闭。



6. 在导航窗格中，单击快照，然后查找刚刚创建的快照。

可使用始于列值和以前记下的卷 ID 确认快照的来源。注意，始于时间为 UTC 时间。

快照的状态可能是待处理。在此情况下，必须等待快照的状态变为已完成，然后再还原快照。

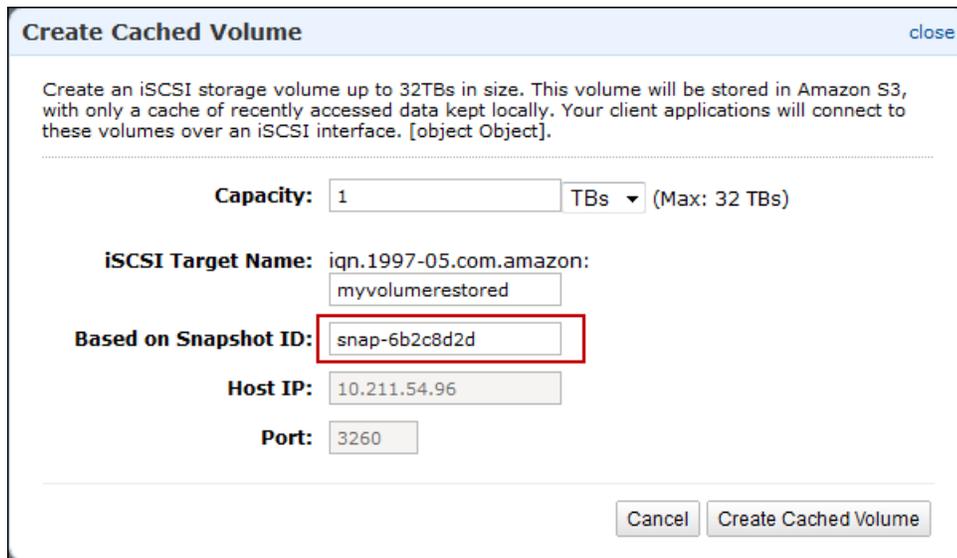


Snapshot ID	Capacity	Volume ID	Started on	Status
snap-47b7b94	1 GiB	vol-a04b49d8	Fri Sep 16 20:25:16 UTC 2011	completed
snap-56575e36	1 GiB	vol-ae4b49d6	Sat Sep 17 20:18:33 UTC 2011	completed
snap-686c6508	1 GiB	vol-a04b49d8	Sat Sep 17 20:25:35 UTC 2011	completed
snap-a6acbbc6	1 GiB	vol-ae4b49d6	Sun Sep 18 20:18:52 UTC 2011	completed
snap-52544232	1 GiB	vol-a04b49d8	Sun Sep 18 20:25:53 UTC 2011	completed
snap-5d6b8e3e	1 GiB	vol-904c4ee8	Tue Sep 20 19:27:59 UTC 2011	completed

7. 复制快照 ID，以便您可在后续步骤中根据快照创建存储卷时输入它。

#### 如需还原快照

1. 在 AWS Storage Gateway 控制台的导航窗格中单击该网关的名称。
2. 单击卷选项卡，然后单击创建新卷。
3. 在创建存储卷对话框中，输入以下信息。



**Create Cached Volume** close

Create an iSCSI storage volume up to 32TBs in size. This volume will be stored in Amazon S3, with only a cache of recently accessed data kept locally. Your client applications will connect to these volumes over an iSCSI interface. [object Object].

**Capacity:**  TBs (Max: 32 TBs)

**iSCSI Target Name:**

**Based on Snapshot ID:**

**Host IP:**

**Port:**

- a. 在容量文本框中，输入与拍摄快照的原始卷相同的容量。
- b. 在 iSCSI 目标名称框中，输入 iSCSI 目标的名称，例如 `myvolumerestored`。

目标名称可包含小写字母、数字句点 (.) 和连字符 (-)。经过发现后，在 iSCSI Microsoft 发起程序用户界面的目标选项卡中，此目标名称显示为 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 SAN 网络内具有全局唯一性。

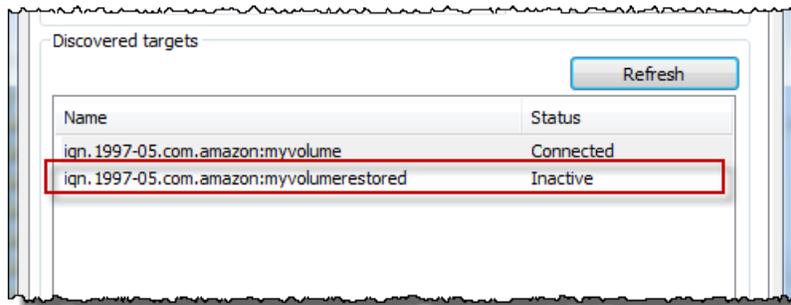
- c. 在基于快照 ID 字段中，输入快照 ID。
- d. 单击创建缓存卷。

此项操作根据您的快照创建存储卷。随后在 AWS Storage Gateway 控制台中显示该卷的详细信息。

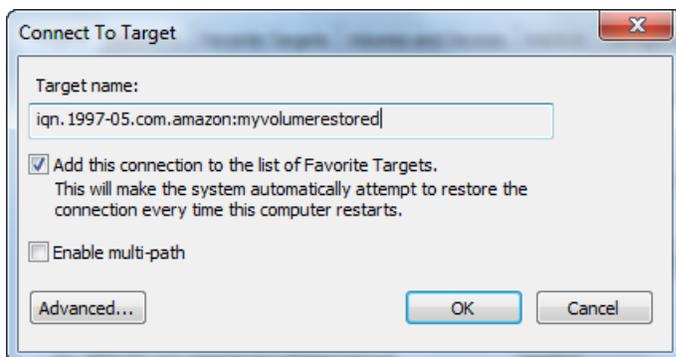
4. 连接到新卷目标。

- a. 在 Windows 客户端计算机的开始菜单中，输入 `iscsicpl.exe` 并运行该程序。
- b. 在 iSCSI 发起程序属性对话框中，单击目标选项卡。如果发现的目标窗格中未显示新目标，则单击刷新。

您应该可以看到原目标和新目标。新目标的状态将为不活动。

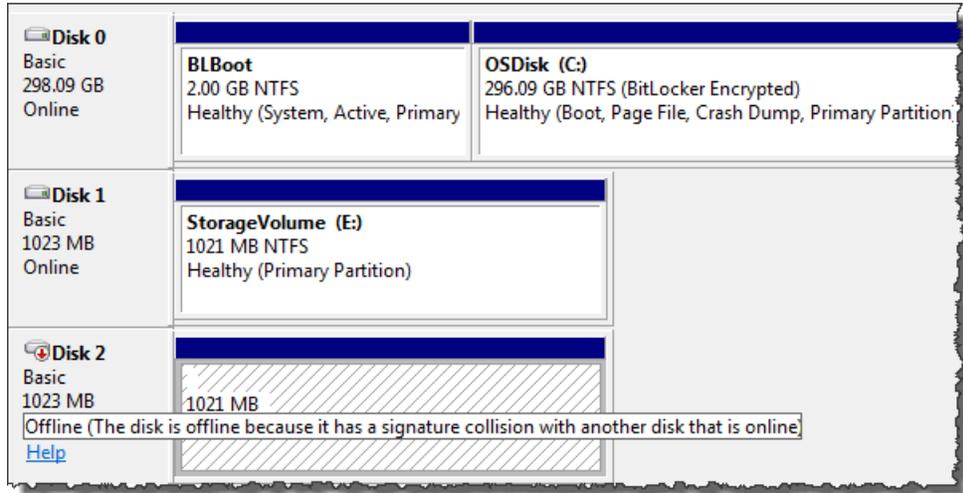


- c. 选择新目标，然后单击连接。
- d. 在连接到目标对话框中，单击确定。

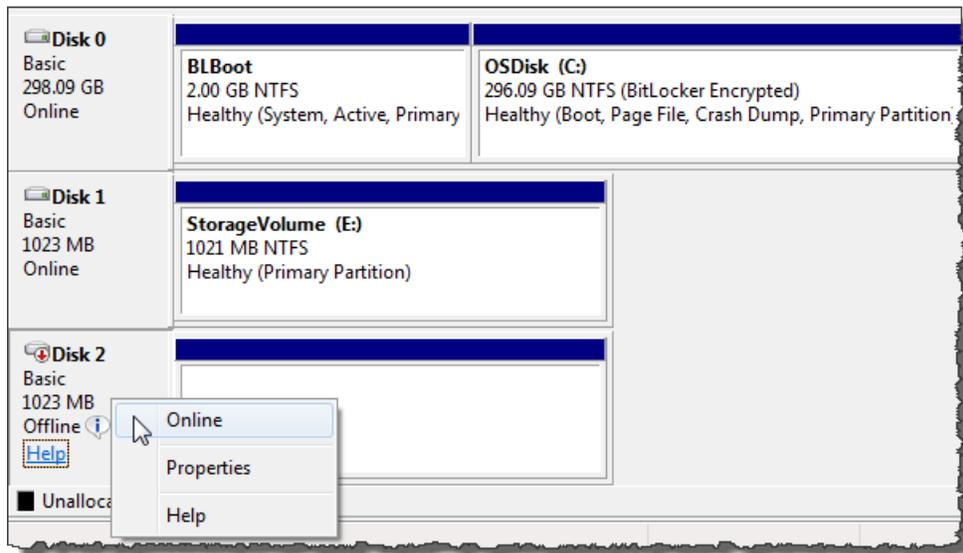


5. 将存储卷联机。

- a. 如果尚未打开磁盘管理控制台，则在开始菜单中，键入 `diskmgmt.msc`。  
还原的存储卷显示在控制台中，并带有警告。



- b. 右键单击还原的卷，然后选择联机。这项操作将卷联机，然后给其分配不同的驱动器号。



- 6. 打开还原的卷，并验证您之前保存的数据存在。

### 测试设置 ( 网关存储 )

本步骤中，您通过拍摄存储卷快照备份验证设置。然后将其还原到另一存储卷。

这项操作需要您先创建存储卷的快照。您然后添加另一本地磁盘到 VM 作为新存储卷，并且从该快照创建新存储卷。您的网关将数据从 AWS 中的指定快照下载到存储卷的本地磁盘。

如需创建存储卷快照

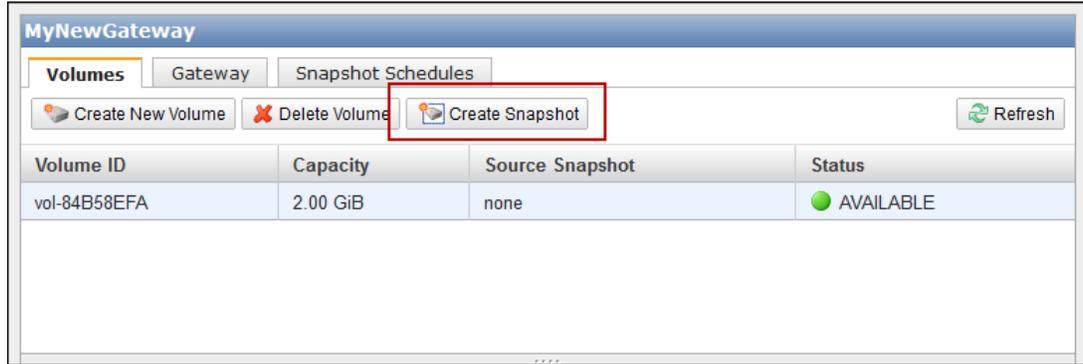
1. 在 Windows 计算机上，将一些数据复制到您的映射存储卷上。  
复制的数据量对于本示范无关紧要。一个小文件即足够用来展示还原过程。
2. 在 AWS Storage Gateway 控制台的导航窗格中选择该网关。

3. 在卷选项卡中，选择为该网关创建的存储卷。

该网关应仅有一个存储卷。选择卷时，会显示它的属性。

4. 单击创建快照按钮以创建该卷的快照。

根据磁盘上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。记录您为其创建快照的卷的 ID。该 ID 用来查找快照。



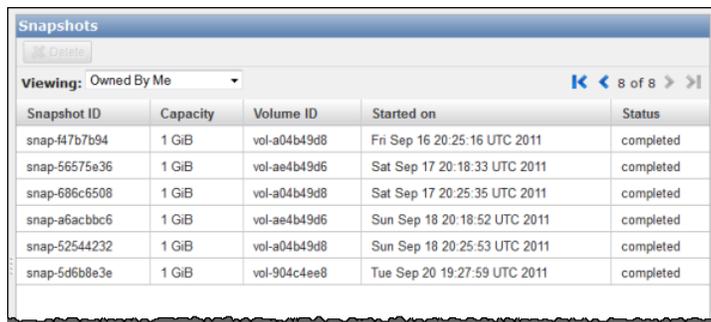
5. 在拍摄了快照确认窗口中，单击关闭。



6. 在导航窗格中，单击快照，然后查找刚刚创建的快照。

可使用始于列值和以前记下的卷 ID 确认快照的来源。注意，始于时间为 UTC 时间。

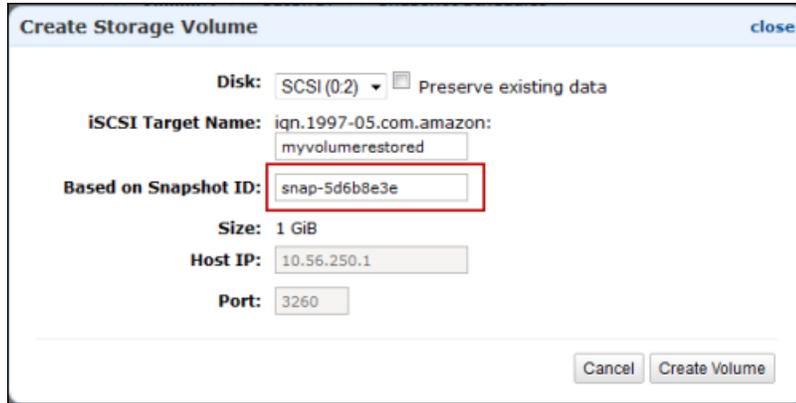
快照的状态可能是待处理。在此情况下，必须等待快照的状态变为已完成，然后再还原快照。



7. 复制快照 ID，以便您可在后续步骤中根据快照创建存储卷时输入它。

### 如需还原快照

1. 向您的 VM 添加另一虚拟磁盘，该磁盘将成为您用来存储快照的新存储卷。因为此存储卷的大小是 2 GiB，所以，创建一个具有相同大小的新虚拟磁盘。有关说明，请参阅[如需分配磁盘以存储您的应用程序数据 \(p. 26\)](#)。
2. 在 AWS Storage Gateway 控制台的导航窗格中单击该网关的名称。
3. 单击卷选项卡，然后单击创建新卷。
4. 在创建存储卷对话框中，输入以下信息。



- a. 在磁盘下拉列表中，选择在前面的步骤中添加的虚拟磁盘。
- b. 在 iSCSI 目标名称框中，输入 iSCSI 目标的名称，例如 `myvolumerestored`。

目标名称可包含小写字母、数字句点 (.) 和连词符 (-)。经过发现后，在 iSCSI Microsoft 发起程序用户界面的目标选项卡中，此目标名称显示为 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 SAN 网络内具有全局唯一性。

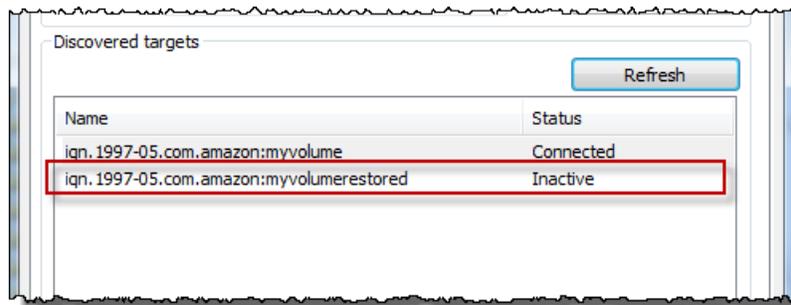
- c. 在基于快照 ID 框中，输入快照 ID。
- d. 单击创建卷。

此项操作根据您的快照创建存储卷。随后在 AWS Storage Gateway 控制台中显示存储卷详细信息。

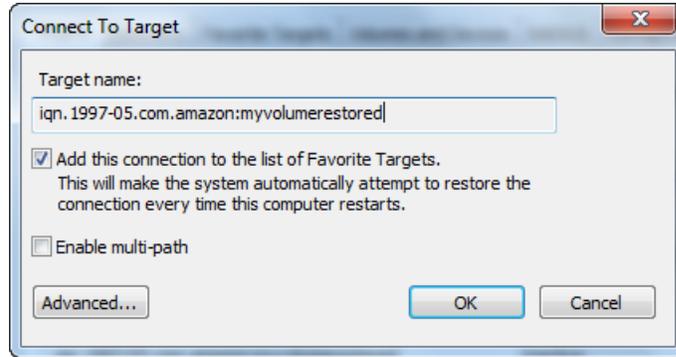
5. 连接到新卷目标。

- a. 在 Windows 客户端计算机的开始菜单中，输入 `iscsicpl.exe` 并运行该程序。
- b. 在 iSCSI 发起程序属性对话框中，单击目标选项卡。如果发现的目标窗格中未显示新目标，则单击刷新。

您应该可以看到原目标和新目标。新目标的状态将为不活动。

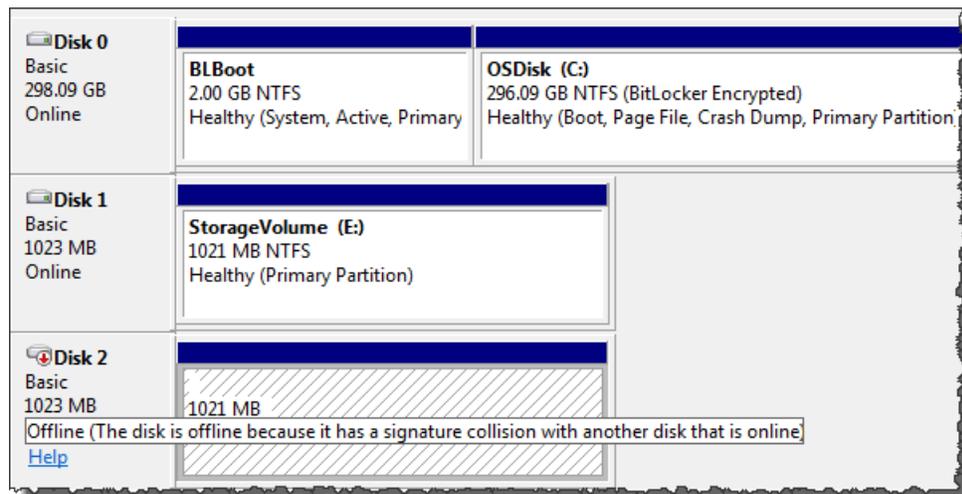


- c. 选择新目标，然后单击连接。
- d. 在连接到目标对话框中，单击确定。

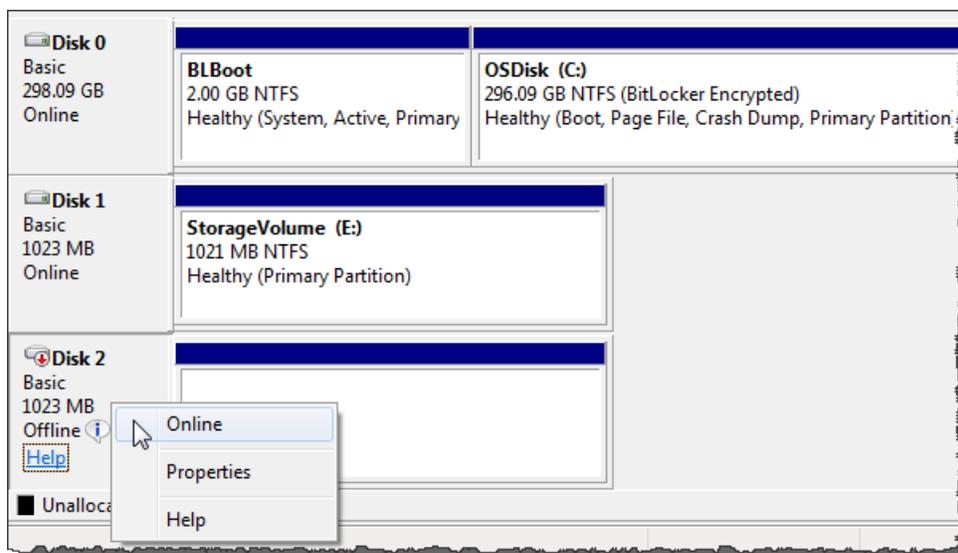


6. 将存储卷联机。

- a. 如果尚未打开磁盘管理控制台，则在开始菜单中，键入 `diskmgmt.msc`。  
还原的存储卷显示在控制台中，并带有警告。



- b. 右键单击还原的卷，然后选择联机。这项操作将卷联机，然后为其分配不同的驱动器号。



7. 打开还原的卷，并验证您之前保存的数据存在。

## 我从这里可以继续进行哪些内容？

AWS Storage Gateway 服务提供一种简单的方式，供您用 AWS 云的存储基础设施支持您的应用程序存储。在[卷网关入门（网关缓存卷和网关存储卷）](#) (p. 10)中，您创建并配置了一个网关，然后将您的 Windows 主机连接到该网关的存储卷。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。

结束本练习后：

- 如果您计划继续使用网关，您就应该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[针对实际工作负载配置网关存储的大小](#) (p. 87)。
- 如果您没有计划继续使用网关，请考虑删除网关，避免产生任何费用。有关更多信息，请参阅[使用 AWS Storage Gateway 控制台删除网关](#) (p. 217)。

本指南的其他部分包括如何进行下列各项的相关信息：

- 详细了解存储卷以及如何创建这些卷（请参阅[管理 AWS Storage Gateway 中的存储卷](#) (p. 167)）。
- 解决网关问题（请参阅[卷网关（网关缓存或网关存储）问题排查](#) (p. 236)）。
- 优化网关（请参阅[优化 AWS Storage Gateway 性能](#) (p. 242)）。
- 了解 Storage Gateway 指标以及可怎样监控网关运行情况（请参阅[监控 AWS Storage Gateway](#) (p. 243)）。
- 连接到网关的 iSCSI 目标以存储数据（请参阅[配置应用程序对存储卷的访问](#) (p. 153)）。

## 针对实际工作负载配置网关存储的大小

此时，您就有了一个可以运行的简单网关。但是，由于用于创建此网关的假设不适合真实工作负载，因此需要做两件事：如果尚未适当调整上传缓冲区的大小并设置对上传缓冲区的监控，则请照做。本步骤介绍了如何执行这两个任务。如果已激活了缓存卷的网关，您还需要针对实际工作负载配置缓存存储空间大小。

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[配置上传缓冲区的大小（网关缓存）](#) (p. 97)中所显示的公式调整上传缓冲区大小，并使用[配置缓存存储空间的大小（网关缓存）](#) (p. 93)中的公式调整缓存存储大小。我们强烈建议您至少分配 150 GiB 的上传缓冲区。因此，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。

上传缓冲区算入您的应用程序到网关的吞吐量以及您的网关到 AWS 的吞吐量之间的差，然后乘以您希望写入数据的时长。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。

如需为网关存储设置配置上传缓冲区的大小

- 使用[配置上传缓冲区的大小（网关存储）](#) (p. 104)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。因此，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。

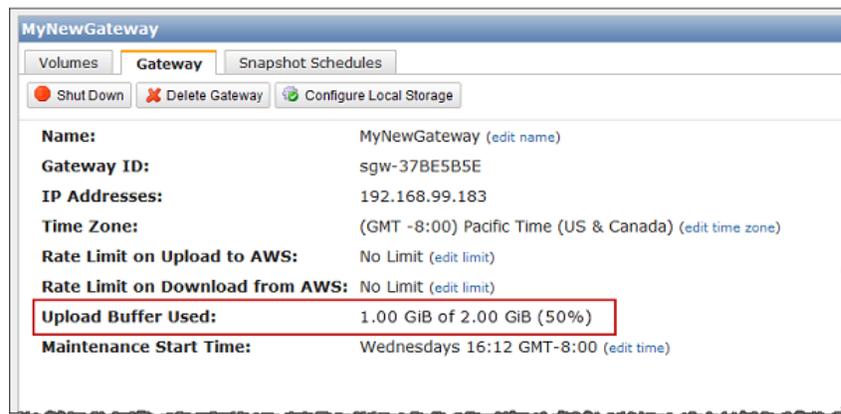
上传缓冲区算入您的应用程序到网关的吞吐量以及您的网关到 AWS 的吞吐量之间的差，然后乘以您希望写入数据的时长。例如，假定您的应用程序每天 12 个小时以每秒 40 MB 的速度向网关写入文本数据并且您的网络吞吐量为 12 MB 每秒。假定文本数据压缩系数为 2:1，公式就会指定您大约需要分配 675 GiB 的上传缓冲区空间。

如需监控您的上传缓冲区

1. 查看网关当前的上传缓冲区。

- 在 AWS Storage Gateway 控制台的网关选项卡中，查找上传缓冲区用量字段。

下例显示上传缓冲区的使用率为百分之三。



2. 对上传缓冲区设置警报。

强烈建议在 Amazon CloudWatch 控制台中创建上传缓冲区警报。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](#) (p. 249)。

## 设置卷网关 ( 网关缓存和网关存储 )

### Topics

- [本地部署和激活 AWS Storage Gateway \(p. 89\)](#)
- [在 Amazon EC2 上部署并激活 AWS Storage Gateway \(p. 133\)](#)
- [配置上传缓冲区和缓存存储空间 \(p. 142\)](#)
- [创建存储卷 \(p. 149\)](#)
- [配置应用程序对存储卷的访问 \(p. 153\)](#)

在本部分，我们向您介绍如何在两个不同的主机托管环境中设置 AWS Storage Gateway。

- 本地—使用本地虚拟环境在本地托管您的网关。若要开始使用，请参见 [本地部署和激活 AWS Storage Gateway \(p. 89\)](#)。
- 云—使用 Amazon EC2 实例在云中托管网关，供灾难恢复和按需计算情况使用。若要开始使用，请参见 [在 Amazon EC2 上部署并激活 AWS Storage Gateway \(p. 133\)](#)。

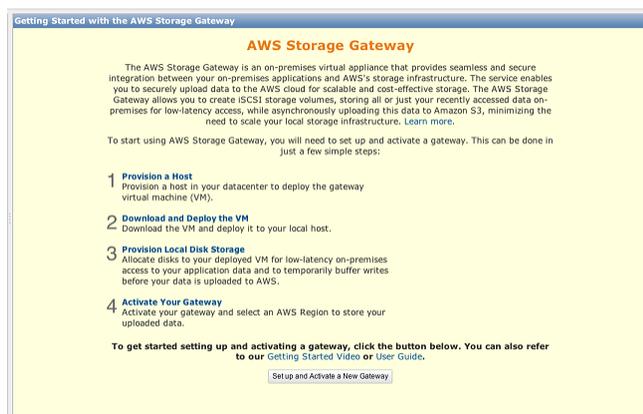
在向主机托管环境部署和激活网关后，无论主机托管环境如何，剩余的网关设置步骤都是相同的，且包括配置上传缓冲区和缓冲存储、创建存储卷以及配置存储卷的访问。

## 本地部署和激活 AWS Storage Gateway

在本部分，我们将介绍如何下载 AWS Storage Gateway 和在虚拟主机上部署网关 VM。我们将介绍如何使用 VMware ESXi 和 Microsoft Hyper-V 虚拟环境托管您的网关。这两种主机类型的网关部署流程在概念上都是十分类似的。在设置和激活网关后，剩下的步骤 ( 创建和访问卷 ) 对于这两种主机类型都是相同的。我们建议您在继续本部分之前查阅入门部分 ( 请参见 [卷网关入门 \( 网关缓存卷和网关存储卷 \) \(p. 10\)](#) )。

### 如需开始设置

1. 请转到 [AWS Storage Gateway](#) 并单击注册。  
下载并部署 AWS Storage Gateway 前，您必须注册该服务。
2. 如果您的 AWS 账户下没有已激活的网关，就需要从下页开始学习使用 AWS Storage Gateway。单击设置并激活新网关按钮以启动设置并激活网关向导。



如果您已激活一个或多个网关，控制台就会显示您的网关列表。在导航窗格中，单击部署新网关以启动设置并激活新网关向导。



## 在 VMware ESXi 主机上部署和激活场内 AWS Storage Gateway

本部分向您介绍如何使用 VMware ESXi 创建场内虚拟机，以托管 AWS Storage Gateway。此处描述的任务假定您已经预配置了 VMware ESXi 主机。如果您尚未完成此操作，请参见此练习中的 [配置 VMware 主机以部署 AWS Storage Gateway VM \(p. 13\)](#)。

### 下载和部署 AWS Storage Gateway VM

配置 VMware ESXi 主机后，设置并激活网关向导中的后续步骤为选择 VMware ESXi 平台，下载用于此平台的 VM 软件，然后部署 VM。



有关说明，请参阅 [下载 AWS Storage Gateway VM 并将其部署在您的主机上 \(p. 13\)](#)。

### AWS Storage Gateway 和 VMware High Availability 一起使用

VMware 高可用性 (HA) 是一种 vSphere 组件，可以在支持网关 VM 的基础结构层提供故障防护。为此，VMware HA 使用配置为集群的多个主机，以使如果一个运行网关 VM 的主机发生故障，则可自动在该集群内的其他主机上重新启动该网关 VM。有关 VMware HA 的详细信息，请转到 [VMware HA：概念和最佳实践](#)。

应该按下列建议做法将 AWS Storage Gateway 与 VMware HA 一起使用。

- 只在群集中的一个主机上部署网关的开放虚拟应用程序 (Open Virtualization Application, OVA)。
- 当部署 OVA 时，选择一个不在主机本地的数据存储器。相反，使用一个可供群集的所有主机访问的数据存储器。如果您选择的是主机本地的数据存储器，而主机发生了故障，那么，群集中的其他主机可能无法访问该数据源，且可能无法进行故障转移。
- 采用建议的 iSCSI 设置，防止启动程序在故障转移期间与存储卷目标断开连接。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需要花费几秒钟到几分钟的时间。Windows 客户端（请参阅 [自定义您的 Windows iSCSI 设置 \(p. 154\)](#)）和 Linux 客户端（请参阅 [自定义您的 Linux iSCSI 设置 \(p. 158\)](#)）的建议 iSCSI 超时大于进行故障转移通常所需的时间。
- 在使用集群的情况下，如果您给集群部署 OVA，系统会要求您选择主机。或者您也可以直接部署到群集中的主机里。

### 为 AWS Storage Gateway VM 配置本地磁盘存储

#### Topics

- [关于网关 VM 用来存储系统数据的磁盘 \(p. 91\)](#)
- [预配置本地磁盘（网关缓存）\(p. 92\)](#)

- [预配置本地磁盘（网关存储）](#) (p. 100)
- [将 AWS Storage Gateway VM 配置为使用半虚拟化](#) (p. 108)

在为部署的网关 VM 预配置本地磁盘存储前，应该确定 AWS Storage Gateway 的配置。您有以下选项：

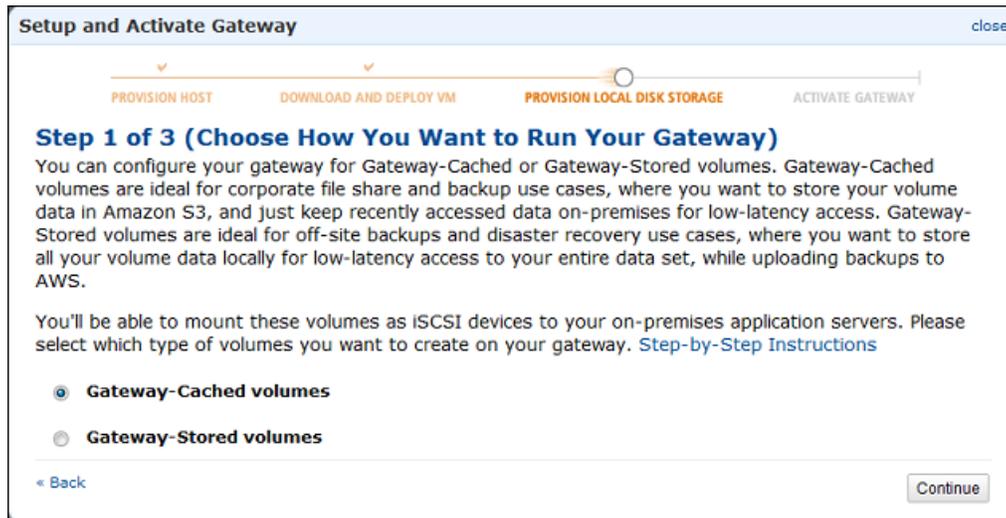
- 使用网关缓存卷—在此配置中，网关将在 Amazon S3 中存储您的卷数据。

网关为最近访问的数据维持缓存存储空间以实现低延迟访问。网关将尚未上传到 Amazon S3 的数据持续承载在缓存存储器中；因此，您必须为缓存存储空间分配场内磁盘。您还必须为上传缓冲区分配磁盘，以便在将数据上传到 AWS 前临时缓冲您的数据。缓存存储空间应该大于上传缓冲区（请参见 [AWS Storage Gateway 的运行原理（架构）](#) (p. 3)）。

- 使用网关存储卷—在此配置中，网关将在本地存储硬件上存储您的卷数据。

您必须分配场内磁盘，以便承载所有数据。网关随后将数据快照安全地上传到 Amazon S3，以便进行具有成本效益的备份和快速灾难恢复。您必须为网关的上传缓冲区分配磁盘（请参见 [AWS Storage Gateway 的运行原理（架构）](#) (p. 3)）。

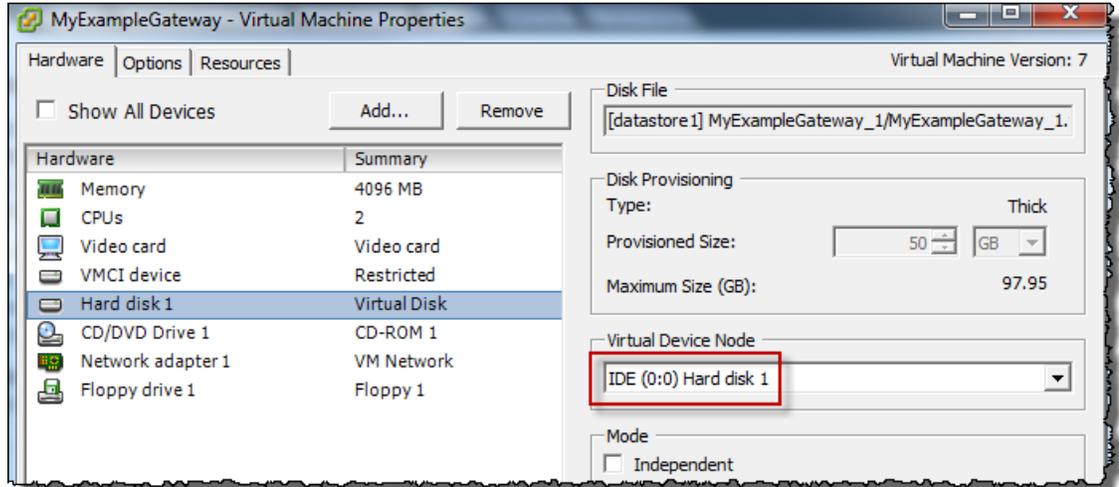
如果您按设置并激活网关控制台向导操作，控制台就会显示以下提示，供您选择卷类型。



选择卷类型后，您必须为在激活网关前支持卷类型所必需的网关 VM 预配置本地磁盘。

### 关于网关 VM 用来存储系统数据的磁盘

部署网关 VM 后，它包括预先配置的处理器和内存和承载 VM 基础设施的 IDE 磁盘。该 IDE 磁盘在 vSphere 客户端的虚拟机属性窗口中显示为“IDE (0:0) Hard disk1”，如以下示例屏幕截图所示。不过，您可以直接访问或使用该磁盘。网关用该磁盘来存储系统数据。



## 预配置本地磁盘（网关缓存）

### Topics

- [为缓存存储空间添加本地磁盘（网关缓存）](#) (p. 92)
- [为上传缓冲区添加本地磁盘（网关缓存）](#) (p. 96)

在网关缓存架构中，网关将您的卷数据存储在 Amazon S3 中。不过，您必须对网关 VM 将磁盘预配置为缓存存储空间或上传缓冲区。有关网关如何工作的更多信息，请参见 [AWS Storage Gateway 的运行原理（架构）](#) (p. 3)。



### Note

预配置磁盘时，强烈建议您不要将本地磁盘预配置为使用相同底层物理存储资源（磁盘）的上传缓冲区和缓存存储空间。底层的物理存储资源在 VMware 中表示为数据存储器。部署网关 VM 时，您选择用来存储 VM 文件的数据存储器。预配置本地磁盘时（例如用作缓存存储空间或上传缓冲区），您可以选择将虚拟磁盘存储在与 VM 相同的数据存储器中，也可以选择存储在不同的存储器中。如果您有一个以上的数据存储器，强烈建议为缓存存储空间选择一个数据存储器，为上传缓冲区选择另一个数据存储器。仅由一个底层物理磁盘支持，或者仅由一个 RAID 1 等低性能 RAID 配置支持的数据存储器可能在用来支持缓存存储空间和上传缓冲区的某些情况下导致性能不佳。

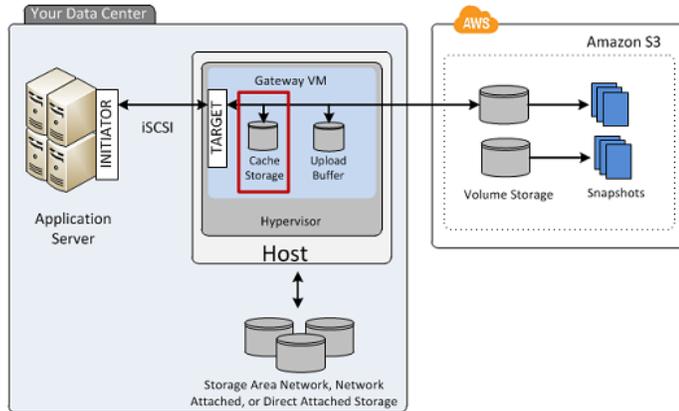
## 为缓存存储空间添加本地磁盘（网关缓存）

### Topics

- [配置缓存存储空间的大小（网关缓存）](#) (p. 93)
- [为缓存存储空间添加虚拟磁盘（网关缓存）](#) (p. 93)

在网关缓存架构中，您的网关为最近访问的数据维持场内缓存存储空间。网关持续将尚未上传到 Amazon S3 的数据存储在缓存存储空间中。您需要为缓存存储空间场内分配磁盘。

下图以更大幅的 AWS Storage Gateway 架构为背景，突出显示了缓存存储空间（请参见 [AWS Storage Gateway 的运行原理（架构）](#) (p. 3)）。



### 配置缓存存储空间的大小 ( 网关缓存 )

网关使用缓存存储空间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 的数据的场内持久存储器。因此缓存存储空间应该大于上传缓冲区。

网关缓存存储总空间可高达 16 TiB。

如需估算网关所需的缓存存储空间量，该公式取决于您的使用案例：

- 备份使用案例—使用上传缓冲区 1.1 倍的缓存存储空间容量。对于备份使用案例，缓存是在上传到 AWS 前的持久存储器，并且必须将其大小配置为大于上传缓冲区，从而确保在 VM 发生故障的情况下不丢失数据。
- 其他使用案例—使用以下两个值中的较大值：现有本地存储的 20% 或上传缓冲区大小的 1.1 倍。

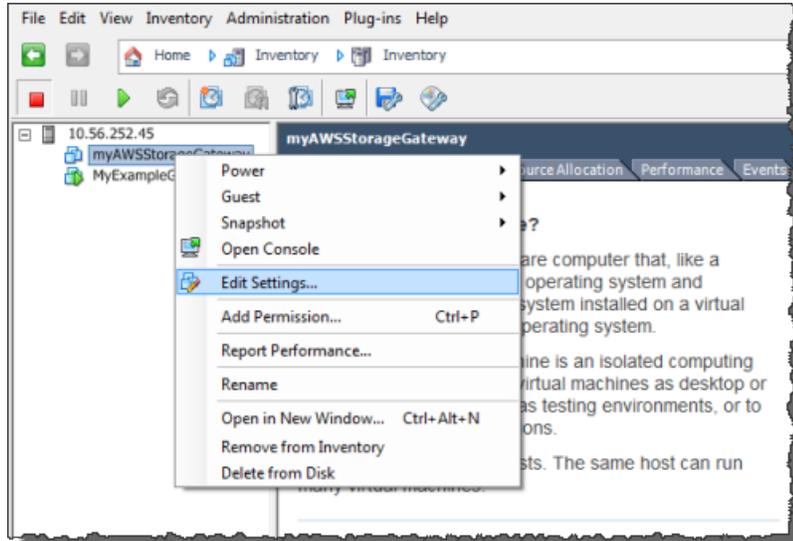
您可以将此近似值用来初步为缓存存储空间预配置磁盘。您然后可以使用 Amazon CloudWatch 运行指标来监控缓存存储空间使用率并使用控制台按需预配置更多的存储空间。有关使用指标和设置警报的信息，请参见 [监控缓存卷 \(p. 252\)](#)。

### 为缓存存储空间添加虚拟磁盘 ( 网关缓存 )

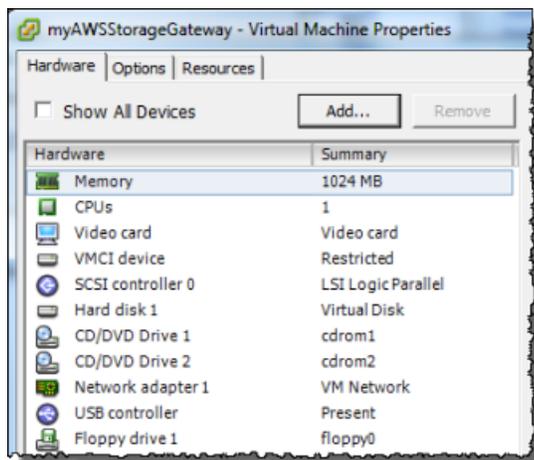
您可以从主机上可用的直接连接存储 (DAS) 磁盘或者存储区域网络 (SAN) 磁盘向 VM 分配虚拟磁盘。下列步骤提供有关从主机上可用的 DAS 磁盘添加虚拟磁盘的指导。

如需向磁盘分配新的虚拟磁盘以用作缓存存储空间

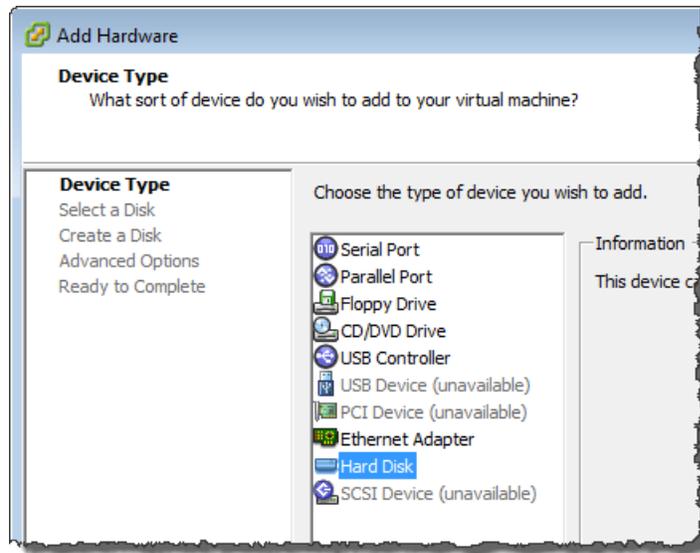
1. Start the VMware vSphere client and connect to your host.
2. In the client, right-click the name of your gateway VM and click Edit Settings....



3. In the Hardware tab of the Virtual Machine Properties dialog box, click Add... to add a device.

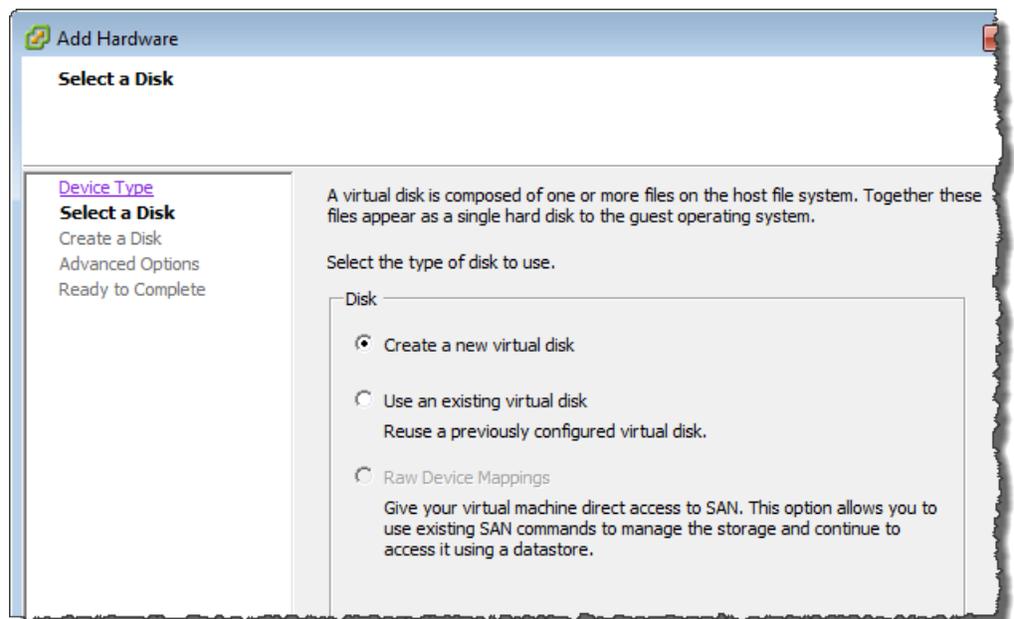


4. Follow the Add Hardware wizard to add a disk:
  - a. In the Device Type pane, click Hard Disk to add a disk, and click Next.



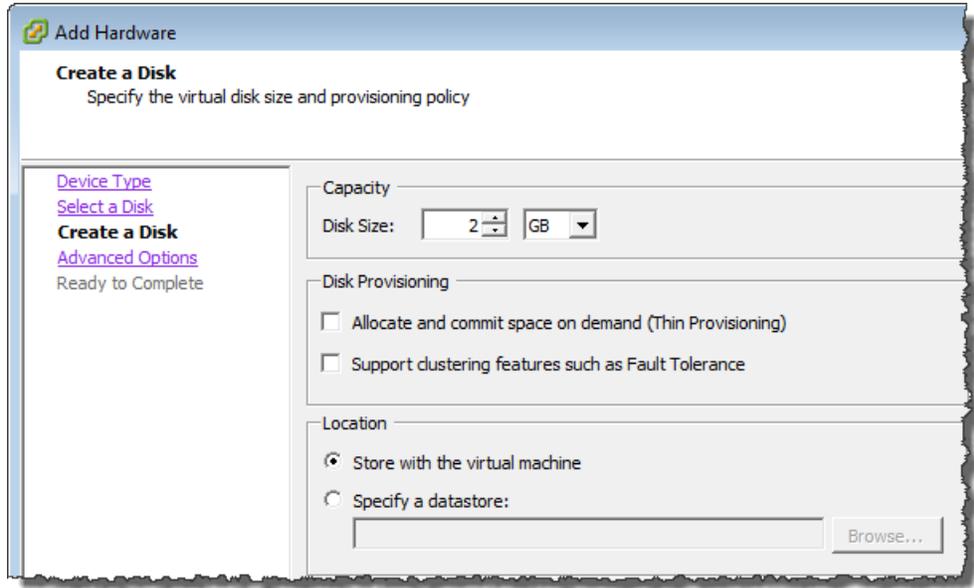
- b. In the Select a Disk pane, select Create a new virtual disk and click Next.

If the disk you are adding for your application storage contains pre-existing data that you want to preserve, select the Use an existing virtual disk option.



- c. In the Create a Disk pane, specify the size of the disk and click Next.

When you use thick provisioning, the disk storage is allocated immediately, resulting in better performance. In contrast, thin provisioning allocates storage on demand. On-demand allocation can affect the normal function of AWS Storage Gateway. Therefore, for AWS Storage Gateway to function properly, the virtual machine disks must be stored in thick-provisioned format.



- d. In the Advanced Options pane, click Next.
  - e. In the Ready to Complete pane, click Finish.
5. If you have not already done so, you must configure your VM to use a paravirtualized controller for your local disks.



#### Important

Configuring your VM for paravirtualization is a critical task. If you do not configure paravirtualization, the AWS Storage Gateway console will not be able to communicate with the disks that you have allocated. For steps on configuring paravirtualization, see [将 AWS Storage Gateway VM 配置为使用半虚拟化 \(p. 108\)](#).

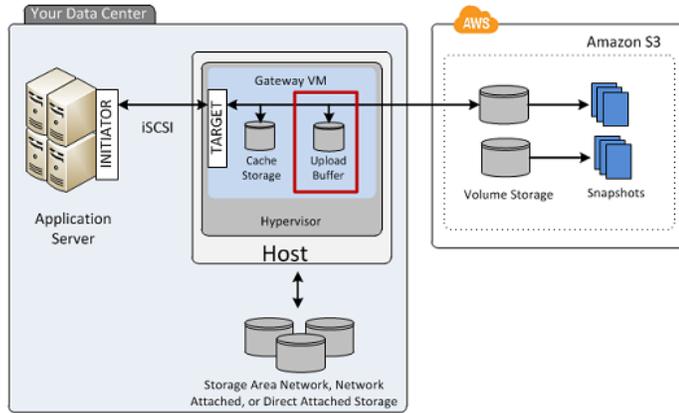
### 为上传缓冲区添加本地磁盘 ( 网关缓存 )

#### Topics

- [配置上传缓冲区的大小 \( 网关缓存 \) \(p. 97\)](#)
- [为上传缓冲区添加虚拟磁盘 \( 网关缓存 \) \(p. 98\)](#)

您必须为网关分配场内磁盘，以便用作上传缓冲区，从而在数据上传到 AWS 前临时缓冲数据。有关分配磁盘存储量的准则，请参见 [配置上传缓冲区的大小 \( 网关缓存 \) \(p. 97\)](#)。

下图以更大幅的 AWS Storage Gateway 架构为背景，突出显示了上传缓冲区 ( 请参见 [AWS Storage Gateway 的运行原理 \( 架构 \) \(p. 3\)](#) )。



### 配置上传缓冲区的大小 (网关缓存)

您可以利用上传缓冲区公式来确定上传缓冲区的大小。我们强烈建议您至少分配 150 GiB 的上传缓冲区。因此，如果公式得出小于 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 2 TiB 的上传缓冲区。

#### Note

上传缓冲区达到其容量后，您的应用程序将持续不断地继续从/向存储卷读写数据；不过，网关不会将任何卷数据写入到其上传缓冲区，也不会将任何此类数据上传到 AWS 中，直到 Storage Gateway 将本地存储在缓存缓冲区的数据与存储在 AWS 中的数据副本进行同步。处于此状态的卷被称为处于 BOOTSTRAPPING 状态的卷。在 BOOTSTRAPPING 状态期间，应用程序写入的数据会持续不断地继续存储在网关缓存缓冲区中。BOOTSTRAPPING 完成后，系统会重新启用上传缓冲区，且该卷会返回已激活状态。有关卷状态的信息，请参见 [管理 AWS Storage Gateway 中的存储卷 \(p. 167\)](#) 和 [排查存储卷问题 \(p. 239\)](#) 中的“排查存储卷问题”部分。

如需更精确地估算上传缓冲区的量，您可以计算数据的传输和传出速率，并且根据这些速率进行估算。

- 数据传入速率—该速率指应用程序吞吐量，亦即您的场内应用程序在某段时间内将数据写入到网关的速率。
- 数据传出速率—该速率指网络吞吐量，亦即您的网关将数据上传到 AWS 时可达到的速率。该速率取决于您的网络速度以及您是否启用了带宽限制。该速率应该针对压缩率进行调整。将数据上传到 AWS 时，网关在可能的情况下实施数据压缩。例如，如果您的应用程序为纯文本，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，因而需要更多的网关上传缓冲区。

如果传入速率高于传出速率，您可以使用以下公式来确定网关所需的大致上传缓冲区大小。

$$\left( \text{Application Throughput (MB/s)} - \text{Network Throughput to AWS (MB/s)} \times \text{Compression Factor} \right) \times \text{Duration of writes (s)} = \text{Upload Buffer (MB)}$$

例如，假定您的商业应用程序每天 12 个小时以每秒 40 兆字节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 兆字节。假定文本数据的压缩系数为 2:1，您就需要为上传缓冲区分配约 690 GB 的空间。

$$((40 \text{ MB/sec}) - (12 \text{ MB/sec} * 2)) * (12 \text{ hours} * 3600 \text{ seconds/hour}) = 691200 \text{ megabytes}$$

请注意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 AWS Storage Gateway 控制台按需添加更多的上传缓冲区空间。另外，您可以使用 Amazon CloudWatch 运行指标来监控上传缓冲区使用率并确定额外的存储空间需求。有关指标和设置警报的信息，请参见 [监控上传缓冲区](#) (p. 249)。

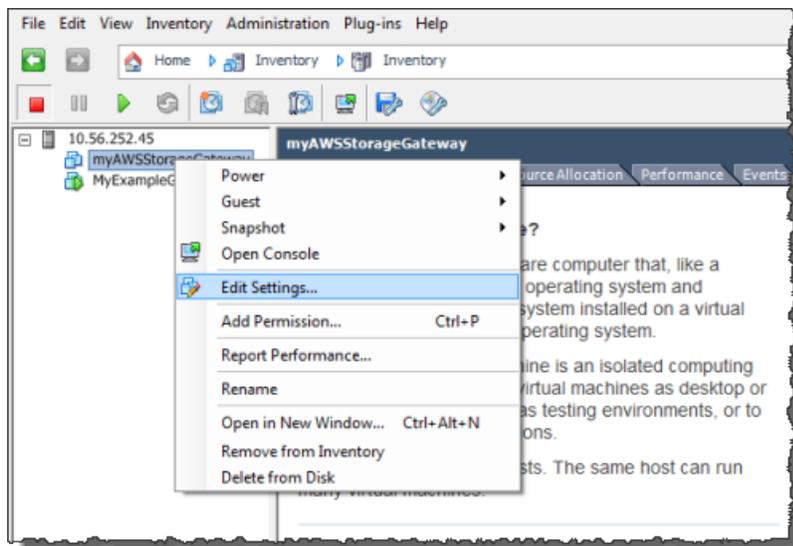
### 为上传缓冲区添加虚拟磁盘 (网关缓存)

在本部分中，您向 VM 分配虚拟磁盘，该磁盘将被用作网关的上传缓冲区。

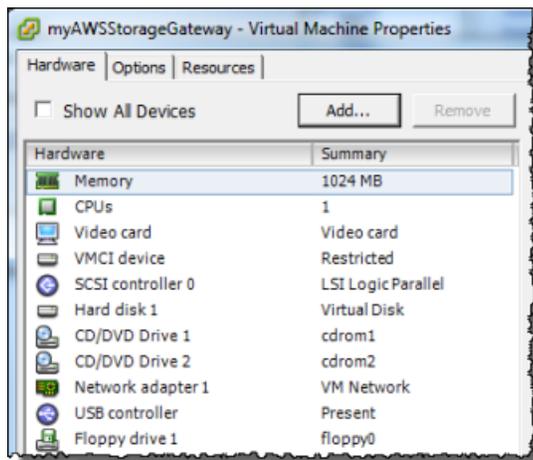
您可以从主机上可用的直接连接存储 (DAS) 磁盘或者存储区域网络 (SAN) 磁盘向 VM 分配虚拟磁盘。以下步骤提供从主机上可用的 DAS 磁盘添加虚拟磁盘的指导。

如需向 VM 分配新的虚拟磁盘用作上传缓冲区

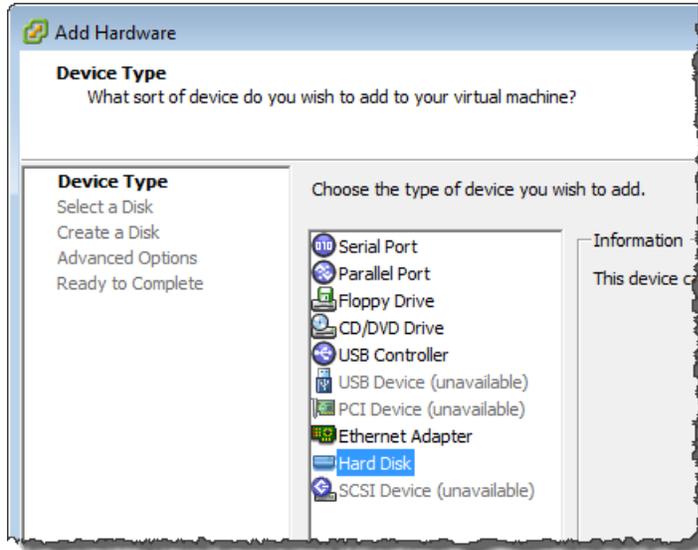
1. Start the VMware vSphere client and connect to your host.
2. In the client, right-click the name of your gateway VM and click Edit Settings....



3. In the Hardware tab of the Virtual Machine Properties dialog box, click Add... to add a device.

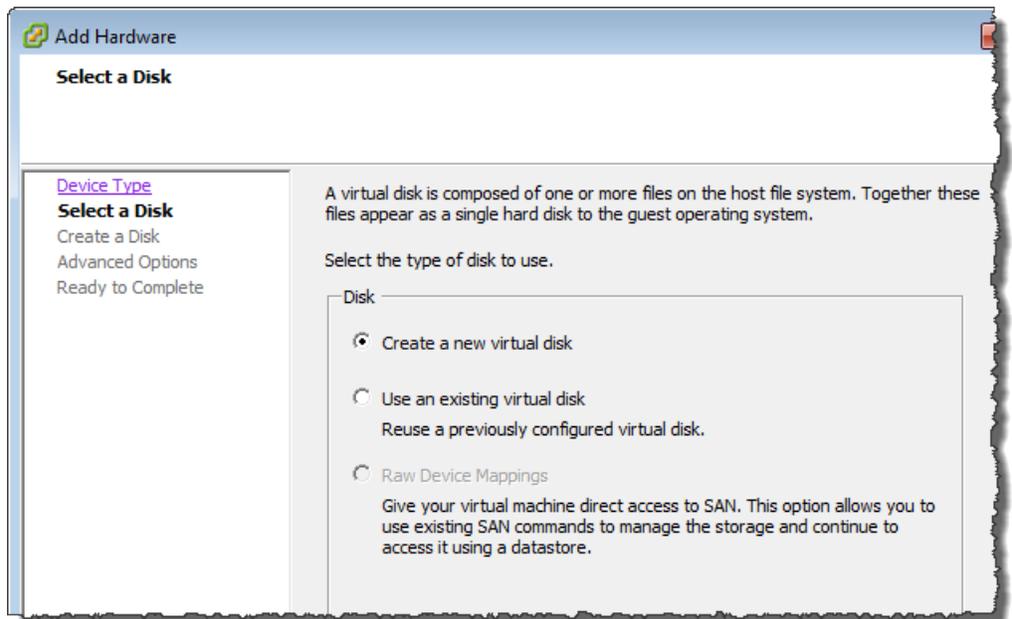


4. Follow the Add Hardware wizard to add a disk:
  - a. In the Device Type pane, click Hard Disk to add a disk, and click Next.



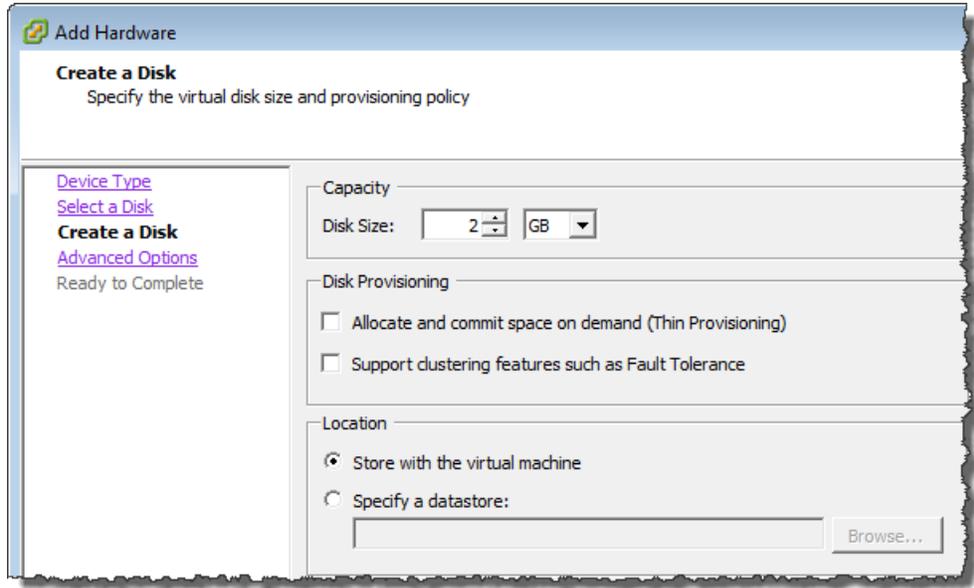
- b. In the Select a Disk pane, select Create a new virtual disk and click Next.

If the disk you are adding for your application storage contains pre-existing data that you want to preserve, select the Use an existing virtual disk option.



- c. In the Create a Disk pane, specify the size of the disk and click Next.

When you use thick provisioning, the disk storage is allocated immediately, resulting in better performance. In contrast, thin provisioning allocates storage on demand. On-demand allocation can affect the normal function of AWS Storage Gateway. Therefore, for AWS Storage Gateway to function properly, the virtual machine disks must be stored in thick-provisioned format.



- d. In the Advanced Options pane, click Next.
  - e. In the Ready to Complete pane, click Finish.
5. If you have not already done so, you must configure your VM to use a paravirtualized controller for your local disks.



#### Important

Configuring your VM for paravirtualization is a critical task. If you do not configure paravirtualization, the AWS Storage Gateway console will not be able to communicate with the disks that you have allocated. For steps on configuring paravirtualization, see [将 AWS Storage Gateway VM 配置为使用半虚拟化 \(p. 108\)](#).

## 预配置本地磁盘 ( 网关存储 )

### Topics

- [为存储卷添加本地磁盘 \( 网关存储 \) \(p. 101\)](#)
- [为上传缓冲区添加本地磁盘 \( 网关存储 \) \(p. 104\)](#)

在本地存储架构中，网关将您的卷数据存储在在场内存硬件中。您的所有应用程序数据均在场内保存。您必须给网关 VM 预配置磁盘，用作卷存储。您还须预配置磁盘，用作网关的上传缓冲区。有关网关工作方式的更多信息，请参见 [AWS Storage Gateway 的运行原理 \( 架构 \) \(p. 3\)](#)。



#### Note

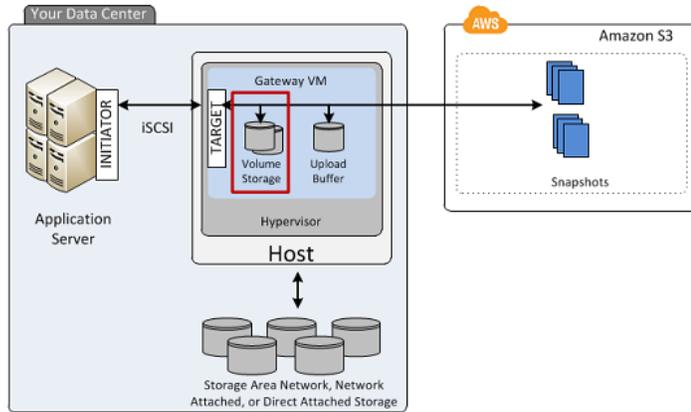
配置磁盘时，强烈建议您不要将本地磁盘配置为使用相同底层物理存储资源 ( 磁盘 ) 的上传缓冲区和本地应用程序存储空间。底层的物理存储资源在 VMware 中表示为数据存储器。部署网关 VM 时，您选择用来存储 VM 文件的数据存储器。预配置本地磁盘时 ( 例如用作本地应用程序存储空间或上传缓冲区 )，您可以选择将虚拟磁盘存储在与 VM 相同的数据存储器中，也可以存储在不同的数据存储器中。如果您有一个以上的数据存储器，强烈建议您为本地应用程序存储空间选择一个数据存储器，为上传缓冲区选择另一个存储器。仅由一个底层物理磁盘支持，或者仅由

一个 RAID 1 等低性能 RAID 配置支持的数据存储器可能在用来支持本地应用存储空间和上传缓冲区的某些情况下导致性能不佳。

### 为存储卷添加本地磁盘 ( 网关存储 )

在网关存储架构中，您的应用程序数据在本地存储。您需要向网关 VM 预配置磁盘，以便存储您的数据。

以下示意图以更大幅的 AWS Storage Gateway 架构为背景，突出显示了存储卷 ( 请参见 [AWS Storage Gateway 的运行原理 \( 架构 \)](#) (p. 3) )。

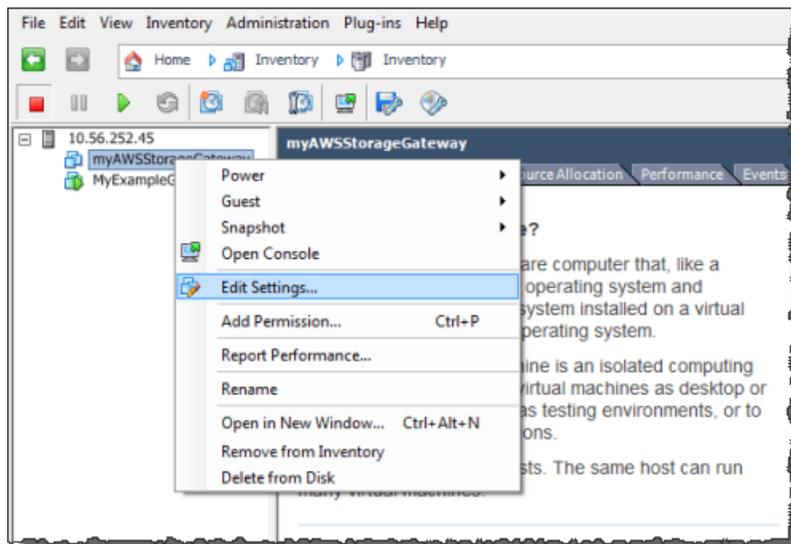


每个磁盘的大小可高达 1 TiB，并且须四舍五入到最接近的整 GiB 值，而 GiB 值使用 Base 2 ( 即  $\text{GiB} = 1024^3$  字节 ) 计算。

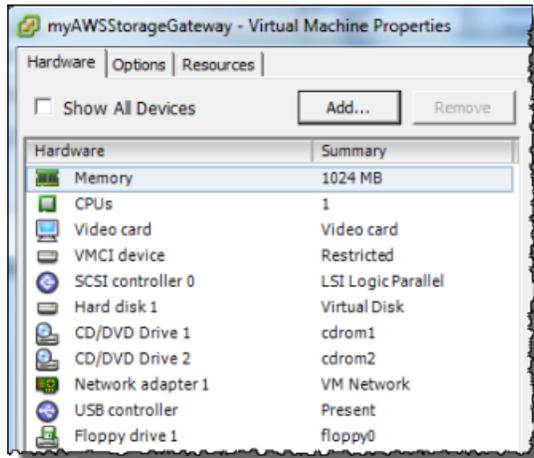
您可以从主机上可用的直接连接存储 (DAS) 磁盘或者存储区域网络 (SAN) 磁盘向 VM 预配置磁盘，以使用作卷存储空间。对于卷存储空间，您分配的磁盘可以有现有数据。我们在创建您的 iSCSI 存储卷时保存这些数据。下列步骤提供从 DAS 磁盘添加虚拟磁盘的指导。

### 为应用程序数据向 VM 添加新的虚拟磁盘

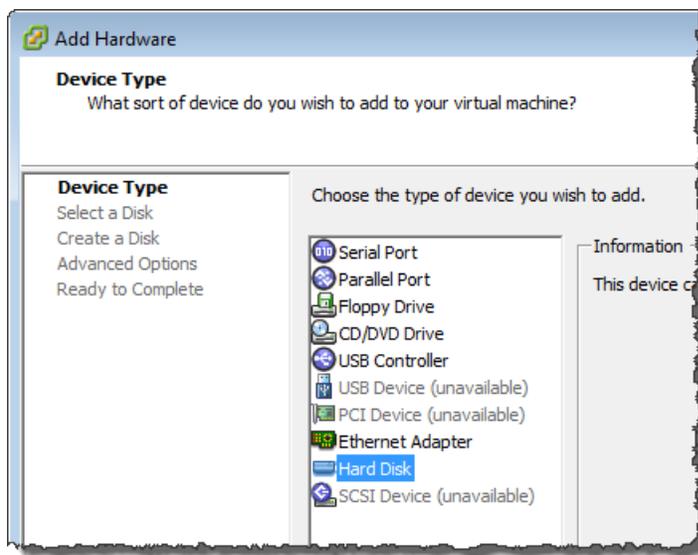
1. Start the VMware vSphere client and connect to your host.
2. In the client, right-click the name of your gateway VM and click Edit Settings....



3. In the Hardware tab of the Virtual Machine Properties dialog box, click Add... to add a device.

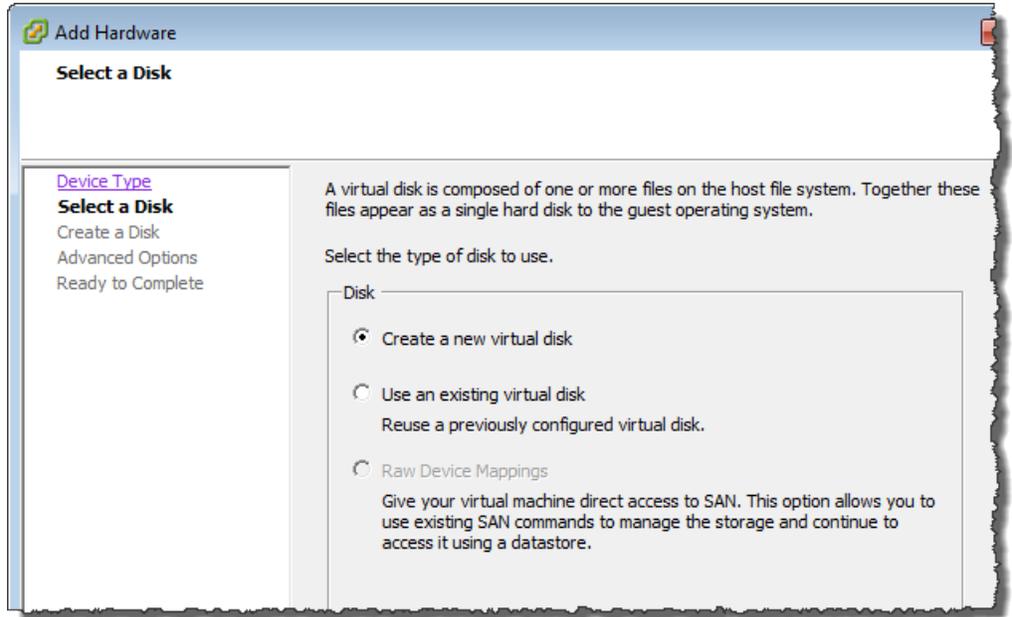


4. Follow the Add Hardware wizard to add a disk:
  - a. In the Device Type pane, click Hard Disk to add a disk, and click Next.



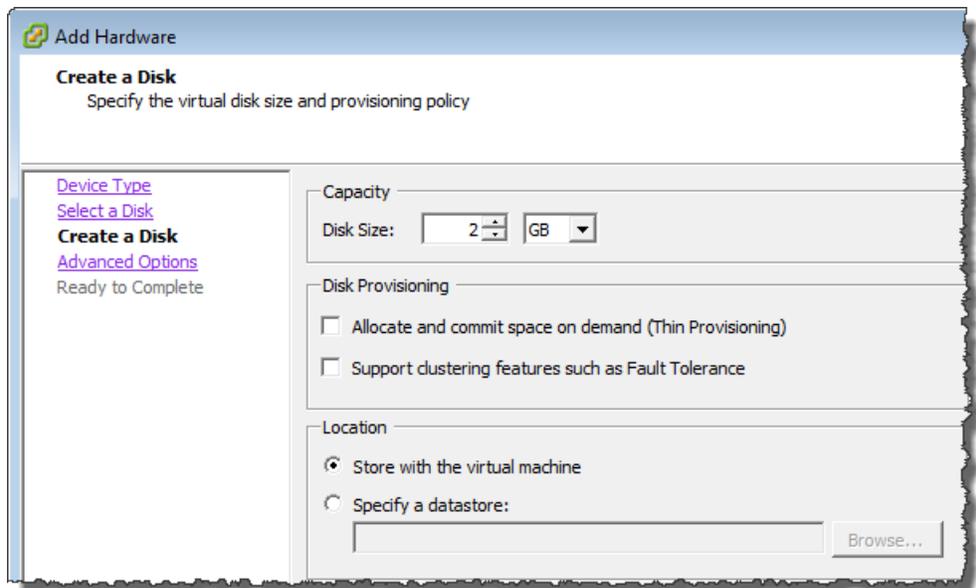
- b. In the Select a Disk pane, select Create a new virtual disk and click Next.

If the disk you are adding for your application storage contains pre-existing data that you want to preserve, select the Use an existing virtual disk option.



- c. In the Create a Disk pane, specify the size of the disk and click Next.

When you use thick provisioning, the disk storage is allocated immediately, resulting in better performance. In contrast, thin provisioning allocates storage on demand. On-demand allocation can affect the normal function of AWS Storage Gateway. Therefore, for AWS Storage Gateway to function properly, the virtual machine disks must be stored in thick-provisioned format.



- d. In the Advanced Options pane, click Next.
  - e. In the Ready to Complete pane, click Finish.
5. If you have not already done so, you must configure your VM to use a paravirtualized controller for your local disks.



### Important

Configuring your VM for paravirtualization is a critical task. If you do not configure paravirtualization, the AWS Storage Gateway console will not be able to communicate with the disks that you have allocated. For steps on configuring paravirtualization, see [将 AWS Storage Gateway VM 配置为使用半虚拟化 \(p. 108\)](#).

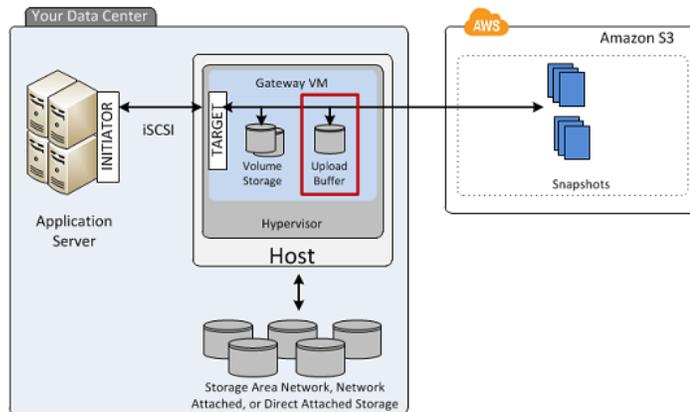
## 为上传缓冲区添加本地磁盘 ( 网关存储 )

### Topics

- [配置上传缓冲区的大小 \( 网关存储 \) \(p. 104\)](#)
- [为上传缓冲区添加虚拟磁盘 \( 网关存储 \) \(p. 105\)](#)

您必须为网关分配场内磁盘，以使用作上传缓冲区，从而在数据上传到 AWS 前临时缓冲数据。

下图以更大幅的 AWS Storage Gateway 架构为背景，突出显示了上传缓冲区 ( 请参见 [AWS Storage Gateway 的运行原理 \( 架构 \) \(p. 3\)](#) )。



## 配置上传缓冲区的大小 ( 网关存储 )

您可以利用上传缓冲区公式来确定上传缓冲区的大小。强烈建议您至少分配 150 GiB 的上传缓冲区空间。因此，如果公式得出小于 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 2 TiB 的上传缓冲区。



### Note

上传缓冲区达到其容量后，您的应用程序将持续不断地继续从/向存储卷读写数据；不过，网关不会将任何卷数据写入到其上传缓冲区，也不会将任何此类数据上传到 AWS 中，直到 Storage Gateway 将本地存储在缓存缓冲区的数据与存储在 AWS 中的数据副本进行同步。处于此状态的卷被称为处于 BOOTSTRAPPING 状态的卷。在 BOOTSTRAPPING 状态期间，应用程序写入的数据会持续不断地继续存储在网关缓存缓冲区中。BOOTSTRAPPING 完成后，系统会重新启用上传缓冲区，且该卷会返回已激活状态。有关卷状态的信息，请参见 [管理 AWS Storage Gateway 中的存储卷 \(p. 167\)](#) 和 [排查存储卷问题 \(p. 239\)](#) 中的“排查存储卷问题”部分。

如需估算上传缓冲区的量，您可以计算数据的传输和传出速率，并且根据这些速率进行估算。

- 数据传入速率—该速率指应用程序吞吐量，亦即您的场内应用程序在某段时间内将数据写入到网关的速率。

- 数据传出速率—该速率指网络吞吐量，亦即您的网关将数据上传到 AWS 时可达到的速率。该速率取决于您的网络速度以及您是否启用了带宽限制。该速率应该针对压缩率进行调整。将数据上传到 AWS 时，网关在可能的情况下实施数据压缩。例如，如果您的应用程序为纯文本，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，因而需要更多的网关上传缓冲区。

如果传入速率高于传出速率，您可以使用以下公式来确定网关所需的大致上传缓冲区大小。

$$\left( \text{Application Throughput (MB/s)} - \text{Network Throughput to AWS (MB/s)} \right) \times \text{Compression Factor} \times \text{Duration of writes (s)} = \text{Upload Buffer (MB)}$$

例如，假定您的商业应用程序每天 12 个小时以每秒 40 兆字节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 兆字节。假定文本数据的压缩系数为 2:1，您就需要为上传缓冲区分配约 690 GB 的空间。

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

请注意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 AWS Storage Gateway 控制台按需添加更多的上传缓冲区空间。另外，您可以使用 Amazon CloudWatch 运行指标来监控上传缓冲区使用率并确定额外的存储空间需求。有关指标和设置警报的信息，请参见 [监控上传缓冲区](#) (p. 249)。

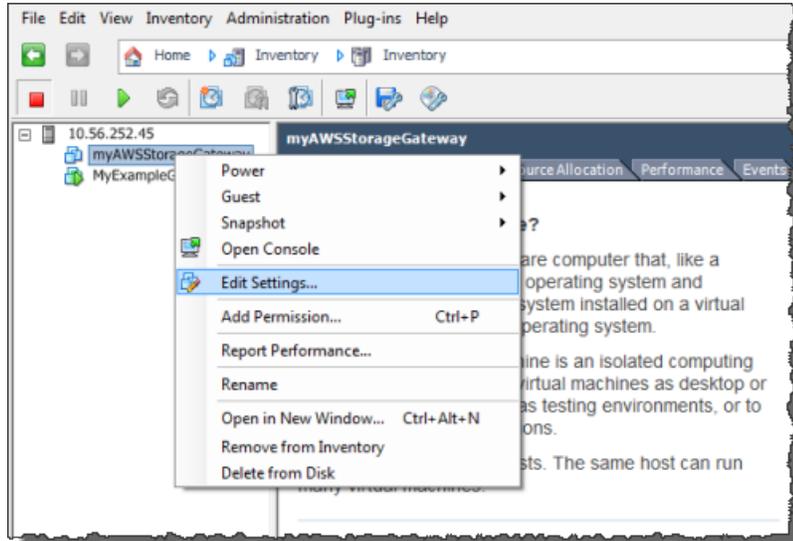
#### 为上传缓冲区添加虚拟磁盘 (网关存储)

在本部分中，您向 VM 分配虚拟磁盘，该磁盘将被用作网关的上传缓冲区。若要估算网关所需的上传缓冲区，请参见 [配置上传缓冲区的大小 \(网关存储\)](#) (p. 104)。

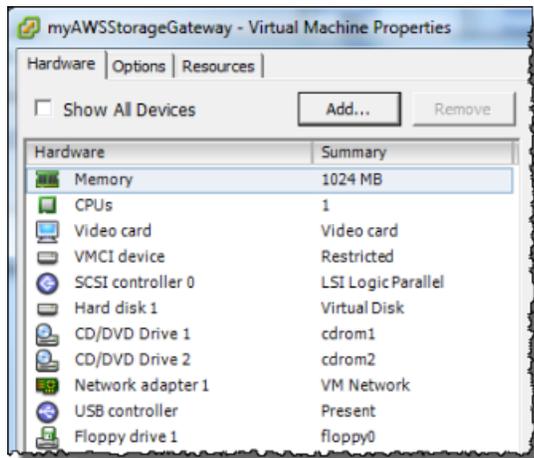
您可以从主机上可用的直接连接存储 (DAS) 磁盘或者存储区域网络 (SAN) 磁盘向 VM 分配虚拟磁盘。以下步骤提供从主机上可用的 DAS 磁盘添加虚拟磁盘的分步指导。

如需向 VM 分配新的虚拟磁盘用作上传缓冲区

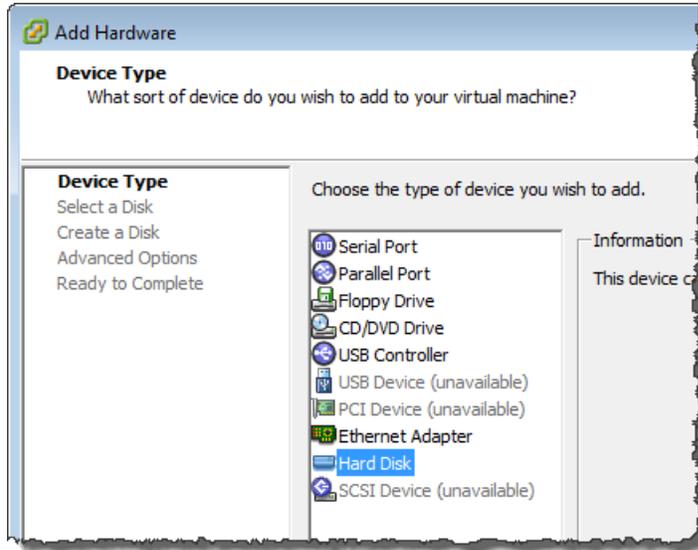
1. Start the VMware vSphere client and connect to your host.
2. In the client, right-click the name of your gateway VM and click Edit Settings....



3. In the Hardware tab of the Virtual Machine Properties dialog box, click Add... to add a device.

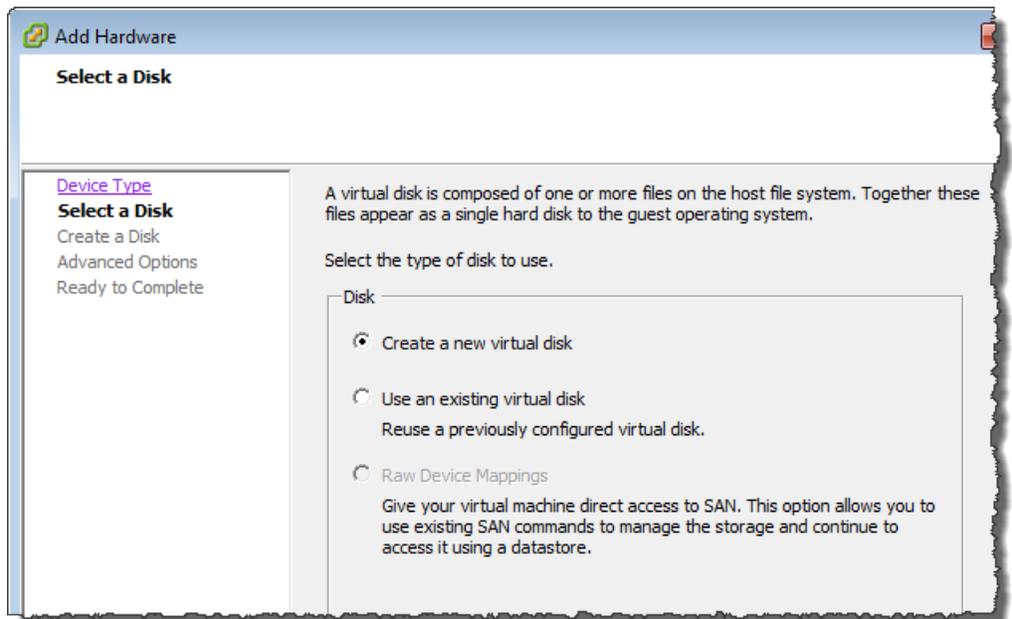


4. Follow the Add Hardware wizard to add a disk:
  - a. In the Device Type pane, click Hard Disk to add a disk, and click Next.



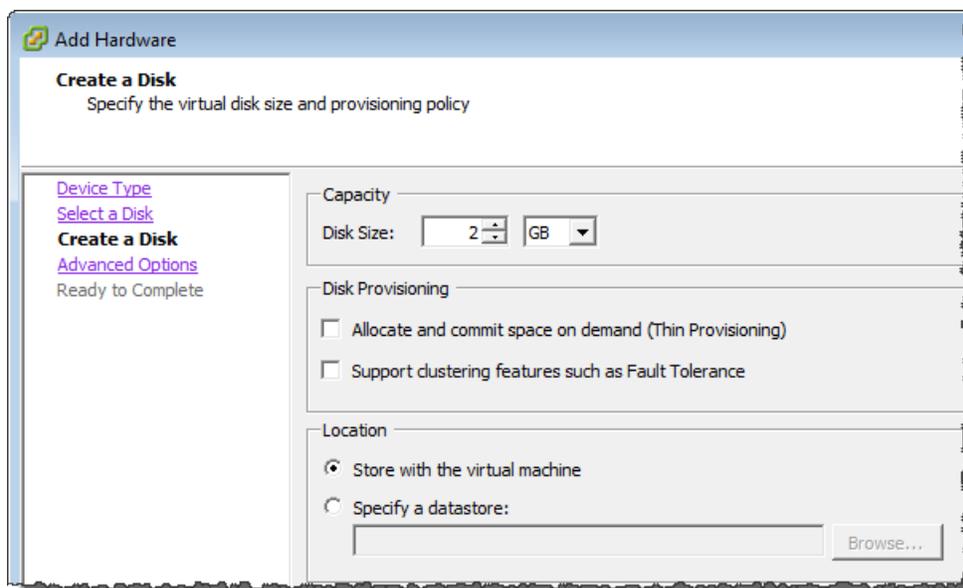
- b. In the Select a Disk pane, select Create a new virtual disk and click Next.

If the disk you are adding for your application storage contains pre-existing data that you want to preserve, select the Use an existing virtual disk option.



- c. In the Create a Disk pane, specify the size of the disk and click Next.

When you use thick provisioning, the disk storage is allocated immediately, resulting in better performance. In contrast, thin provisioning allocates storage on demand. On-demand allocation can affect the normal function of AWS Storage Gateway. Therefore, for AWS Storage Gateway to function properly, the virtual machine disks must be stored in thick-provisioned format.



- d. In the Advanced Options pane, click Next.
  - e. In the Ready to Complete pane, click Finish.
5. If you have not already done so, you must configure your VM to use a paravirtualized controller for your local disks.



#### Important

Configuring your VM for paravirtualization is a critical task. If you do not configure paravirtualization, the AWS Storage Gateway console will not be able to communicate with the disks that you have allocated. For steps on configuring paravirtualization, see [将 AWS Storage Gateway VM 配置为使用半虚拟化 \(p. 108\)](#).

### 将 AWS Storage Gateway VM 配置为使用半虚拟化

为了让 AWS Storage Gateway 控制台正确识别磁盘，您必须配置 VM，以便使用本地磁盘的超虚拟控制器。在实际工作中，您可在网关的初始安装期间设置超虚拟，也就是说，在部署 VM 和添加本地磁盘后但在打开 VM 前。要设置超虚拟，必须关闭 VM。



#### Note

如果您给 VM 至少预配置了一个 SCSI 磁盘，那么，只能设置 iSCSI 控制器的虚拟。有关更多信息，请参见 [为 AWS Storage Gateway VM 配置本地磁盘存储 \(p. 90\)](#)。

#### 如需将 VM 配置为使用半虚拟化的控制器

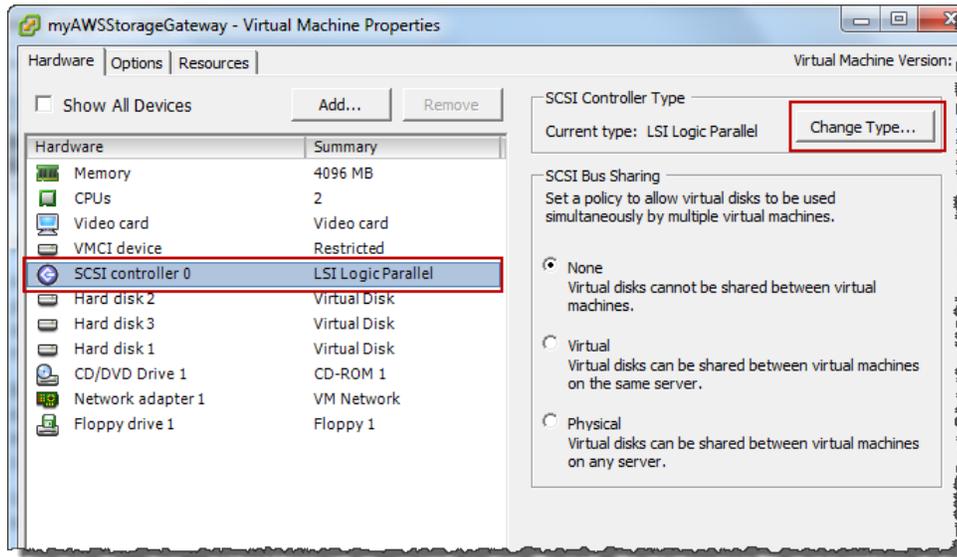
1. 在 VMware vSphere 客户端中，右键单击您的网关虚拟机的名称。

验证是否已关闭 VM。如果没有，请予以关闭。有关更多信息，请参见 [网关激活步骤 \(p. 110\)](#)。在关闭 VM 前，请确保没有使用网关。

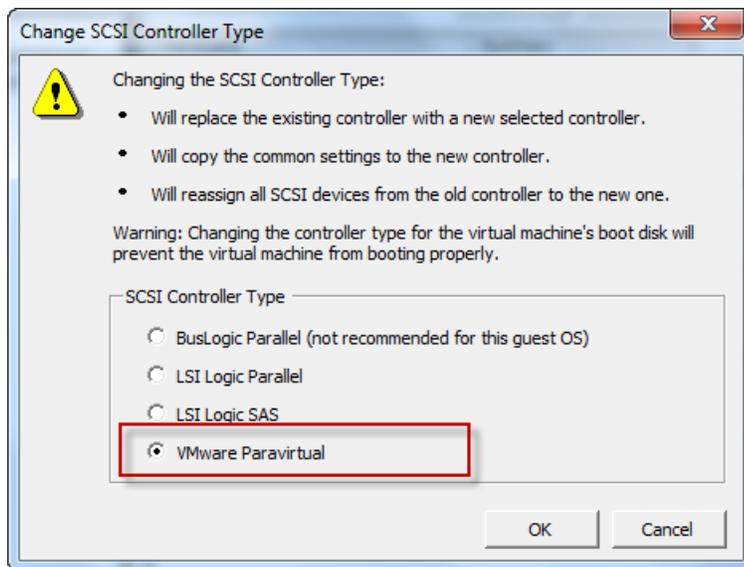
2. 选择编辑设置...

随后将打开虚拟机属性对话框。

3. 在硬件选项卡中，选择硬件列表中的 SCSI 控制器 0 设置，然后单击更改类型...



4. 选择 VMware ParaVirtual SCSI 控制器类型，然后单击确定。



## 激活 AWS Storage Gateway

部署 AWS Storage Gateway VM 后，您必须使用 AWS Storage Gateway 控制台激活该网关。激活过程将您的网关与 AWS 账户关联。建立该连接后，您可以从管理平台管理网关的几乎所有方面。在激活过程中，您指定网关的 IP 地址，命名网关，识别希望存储快照备份的 AWS 地区，并且指定网关时区。激活后，您开始产生费用。有关定价的信息，请参阅 [AWS Storage Gateway](#)。

### 激活前清单

您可以在完成下表总结的步骤后激活网关。控制台向导引导您完成这些步骤。

步骤	说明
下载并部署 VM	在 AWS Storage Gateway 控制台中，下载以 .ova 文件形式分发的最新虚拟机 (VM)，然后将此 VM 部署在您的 VMware 主机上。有关更多信息，请参阅 <a href="#">下载和部署 AWS Storage Gateway VM (p. 90)</a> 。
将本地磁盘预配置到 VM	预配置的 VM 没有磁盘。根据您的网关类型的不同，您必须为下列各项添加本地磁盘： <ul style="list-style-type: none"><li>• 为已激活缓存卷的网关添加缓存存储空间和上传缓冲区。有关更多信息，请参阅 <a href="#">预配置本地磁盘 (网关缓存) (p. 92)</a>。</li><li>• 为存储卷激活的网关的应用程序数据和上传缓冲区。有关更多信息，请参阅 <a href="#">预配置本地磁盘 (网关存储) (p. 100)</a>。</li></ul>
将 VM 配置为使用半虚拟化	将 VM 配置为使用半虚拟化是至关重要的任务。如果您没有配置半虚拟化，AWS Storage Gateway 控制台就不能与您分配的磁盘通信。有关更多信息，请参阅 <a href="#">将 AWS Storage Gateway VM 配置为使用半虚拟化 (p. 108)</a> 。

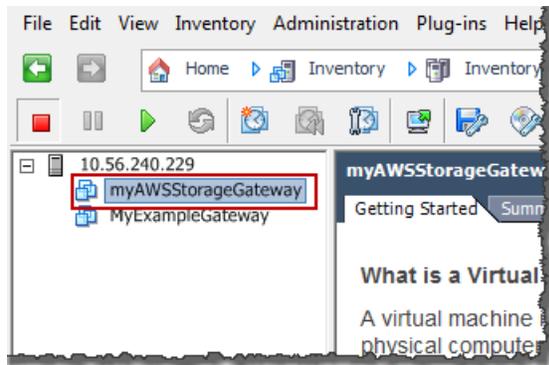
### 网关激活步骤

可使用 AWS Storage Gateway 控制台或 AWS Storage Gateway API ( 请参阅 [API\\_ActivateGateway](#) ) 激活网关。如需激活网关，您需要了解网关 VM 的 IP 地址。开始激活过程前，请确保将用来进行激活的计算机可通过网络访问网关。

以下过程展示如何使用 vSphere 客户端激活网关以获取网关 VM 的 IP 地址，然后如何在控制台的设置并激活网关向导中使用该 IP 地址。

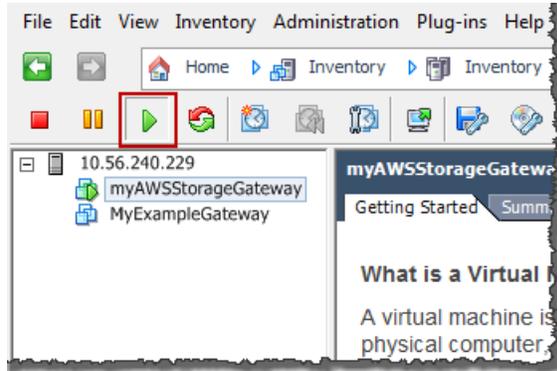
#### 如需使用控制台激活网关

1. 如果 VM 尚未启动，请启动。
  - a. 在 vSphere 客户端中，选择网关 VM。



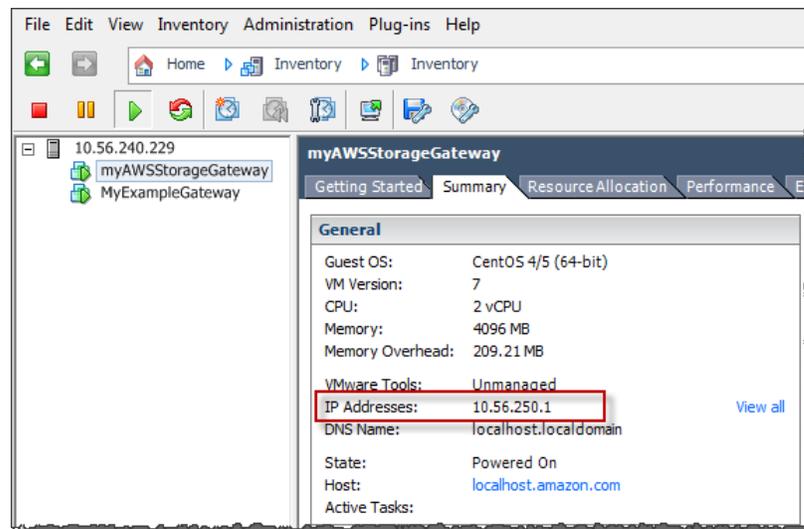
- b. 单击工具栏菜单上的开机图标。

您的网关 VM 图标现在包含一个绿色箭头图标，表示您已启动了 VM。



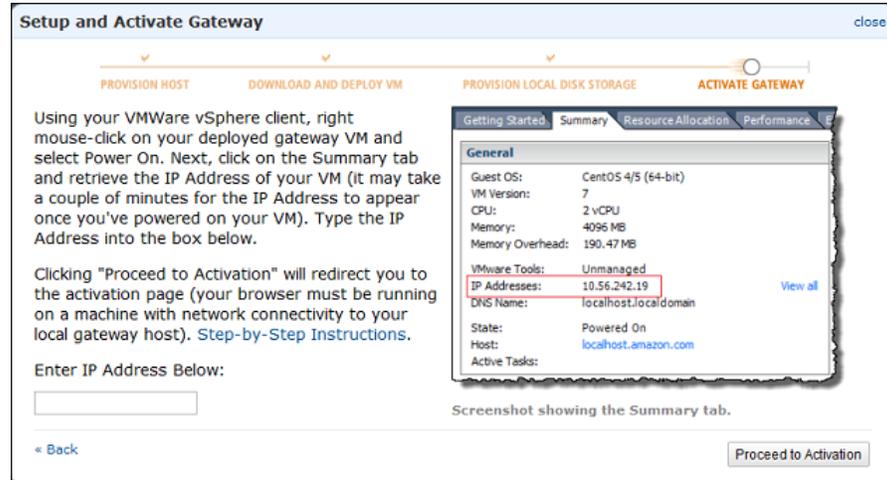
## 2. 激活网关。

- a. 取得您的网关的 IP 地址。请注意，启动 VM 后，IP 地址可能需要一段时间才能显示。
  - i. 使用 vSphere 客户端登录您的主机。
  - ii. 选择部署的网关 VM。
  - iii. 单击摘要选项卡以获得该 IP 地址。



## b. 将您的网关关联到 AWS 账户

- i. 返回控制台，如果尚未打开设置并激活网关向导，则请照做，继续进行激活网关步骤，输入 IP 地址，然后单击继续激活。您的浏览器必须运行在可通过网络连接到本地网关主机的机器上。



### Note

如果激活失败，请检查您输入的 IP 地址是否正确，然后重试激活。如果 IP 地址正确无误，则确认网关可访问 Internet，如有必要，则还要设置代理（请参阅[将 AWS Storage Gateway 的路由选为通过代理](#) (p. 222)）。

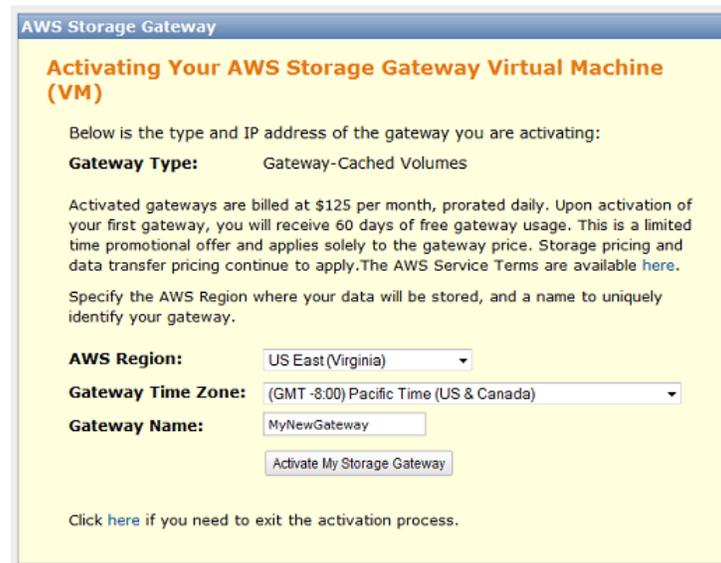
- ii. 在激活页面上，填写请求的信息以完成激活过程。

网关类型指定所激活的网关的类型。您可以激活网关的缓存卷或存储卷。有关更多信息，请参阅[AWS Storage Gateway 的运行原理（架构）](#) (p. 3)。

AWS 地区决定 AWS 存储快照的位置。如果您选择将快照还原为 Amazon EBS 卷，Amazon EBS 卷就必须和快照在同一地区。您不可以在网关激活后更改地区。

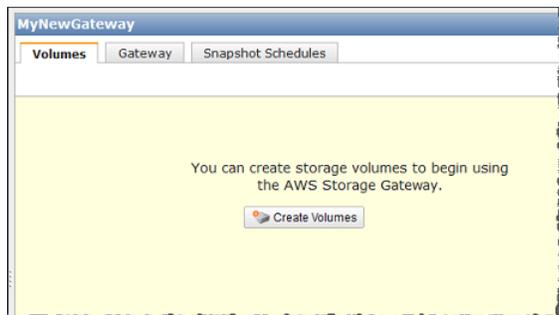
网关时区是显示基于时间的信息（如来自 AWS 的维护消息以及快照调度）时使用的时区。您可以在激活后更改时区。

网关名称在控制台中标识您的网关。您可以使用该名称在控制台中管理网关，然后在激活后更改名称。



- iii. 单击激活我的 Storage Gateway。

成功激活后，AWS 存储网关 控制台即显示激活的 gateway 和一个链接，供您创建卷。



#### 相关部分

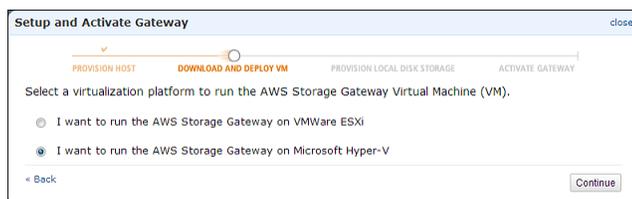
- [AWS Storage Gateway 的 API 参考 \(p. 418\)](#)

## 在 Microsoft Hyper-V 主机上部署和激活场内 AWS Storage Gateway

本部分向您介绍如何使用 Microsoft Hyper-V 创建场内虚拟机，以托管 AWS Storage Gateway。此处描述的任务假定您已经预配置了 Microsoft Hyper-V 主机。如果您尚未完成此操作，请参见此入门练习中的 [配置 Hyper-V 主机以部署 AWS Storage Gateway VM \(p. 35\)](#)。

### 下载和部署 AWS Storage Gateway VM

配置 Microsoft Hyper-V 主机后，设置并激活网关向导中的后续步骤为选择 Microsoft Hyper-V 平台，下载用于此平台的 VM 软件，然后部署 VM。



有关说明，请参阅 [下载 AWS Storage Gateway VM 并将其部署在您的主机上 \(p. 35\)](#)。

### 为 AWS Storage Gateway VM 配置本地磁盘存储

#### Topics

- [系统数据的 IDE 磁盘 \(p. 114\)](#)
- [预配置本地磁盘 \(网关缓存\) \(p. 115\)](#)
- [预配置本地磁盘 \(网关存储\) \(p. 122\)](#)

为部署的网关 VM 配置本地磁盘存储前，您应该确定计划使用的 iSCSI 存储卷类型。您有以下选项：

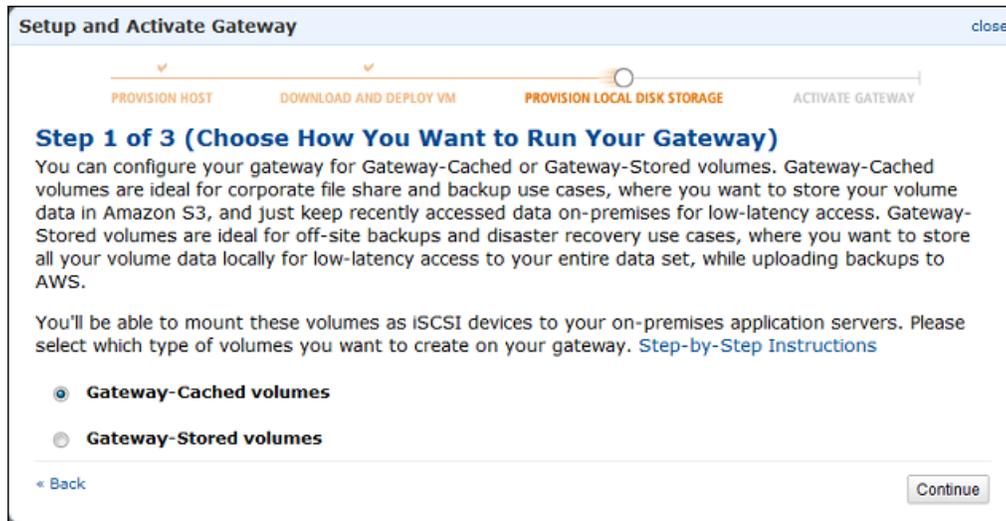
- 使用网关缓存卷 – 在这种情况下，网关将在 Amazon S3 中存储您的卷数据。

在此情况中，网关为最近访问的数据维持缓存存储空间以实现低延迟访问。网关将尚未上传到 Amazon S3 的数据持续承载在缓存存储器中；因此，您必须为缓存存储空间分配场内磁盘。您还必须为上传缓冲区分配磁盘，以便在将数据上传到 AWS 前临时缓冲您的数据。缓存存储空间应该大于上传缓冲区（请参见 [AWS Storage Gateway 的运行原理（架构）](#)（p. 3））。

- 使用网关存储卷 – 在此情况下，网关将在本地存储硬件上存储您的卷数据。

您必须分配场内磁盘，以便承载所有数据。网关随后将数据快照安全地上传到 Amazon S3，以便进行具有成本效益的备份和快速灾难恢复。您必须为网关的上传缓冲区分配磁盘（请参见 [AWS Storage Gateway 的运行原理（架构）](#)（p. 3））。

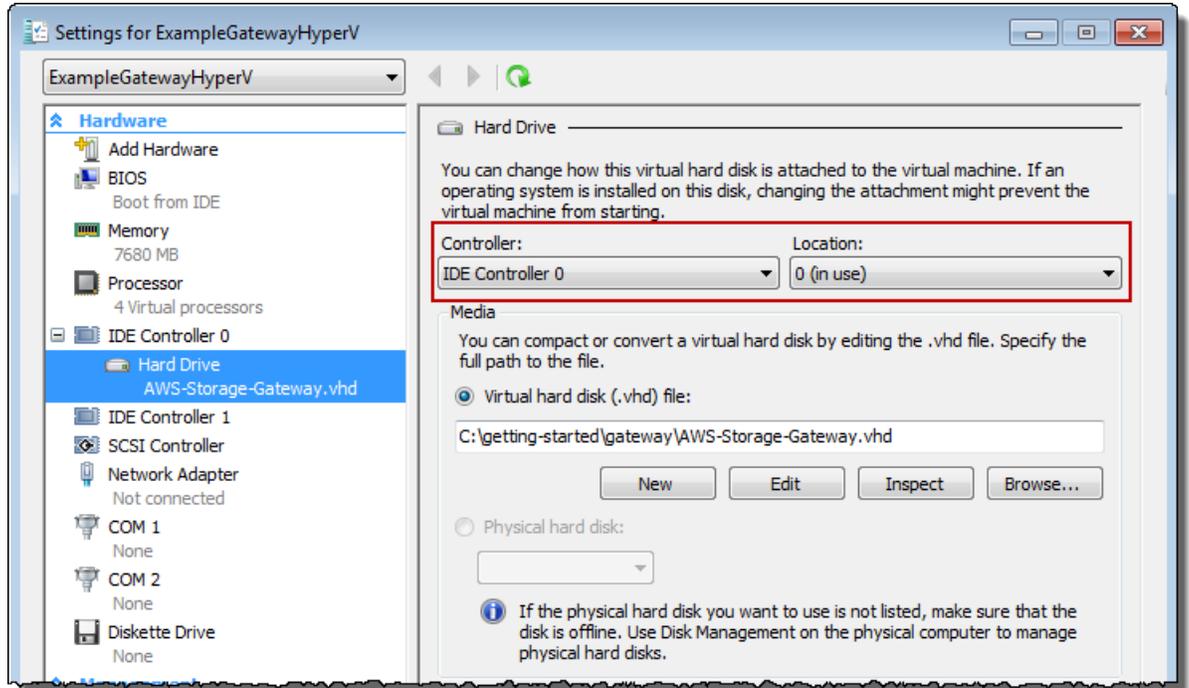
如果您按设置并激活网关控制台向导操作，控制台就会显示以下提示，供您选择卷类型。



选择卷类型后，您必须为在激活网关前支持卷类型所必需的网关 VM 预配置本地磁盘。

### 系统数据的 IDE 磁盘

部署（导入）网关 VM 后，它包括预先配置的处理器、内存和承载 VM 基础设施的 IDE 磁盘。在 Microsoft Hyper-V Manager 的设置窗口中，此 IDE 磁盘会显示为 AWS-Storage-Gateway.vhd 和控制器 IDE (0:0)，如下例屏幕截图所示。不过，您可以直接访问或使用该磁盘。网关用该磁盘来存储系统数据。



## 预配置本地磁盘（网关缓存）

### Topics

- 为缓存存储空间添加本地磁盘（网关缓存）(p. 115)
- 为上传缓冲区添加本地磁盘（网关缓存）(p. 118)

在网关缓存架构中，网关将您的卷数据存储存储在 Amazon S3 中。不过，您必须对网关 VM 将磁盘预配置为缓存存储空间或上传缓冲区。有关网关如何工作的更多信息，请参见 [AWS Storage Gateway 的运行原理（架构）](#) (p. 3)。



### Note

配置磁盘时，强烈建议您不要将本地磁盘配置为使用相同底层物理存储资源（磁盘）的上传缓冲区和缓存存储空间。部署网关 VM 时，您选择用来存储 VM 文件的磁盘位置。预配置本地磁盘时（例如用作缓存存储空间或上传缓冲区），您可以选择将虚拟磁盘存储在与 VM 相同的磁盘位置中，也可以选择存储在不同的位置中。如果您有一个以上的磁盘，强烈建议为缓存存储空间选择一个磁盘位置，为上传缓冲区选择另一个磁盘位置。仅由一个底层物理磁盘支持，或者仅由一个 RAID 1 等低性能 RAID 配置支持的一个磁盘位置可能在用来支持缓存存储空间和上传缓冲区的某些情况下导致性能不佳。

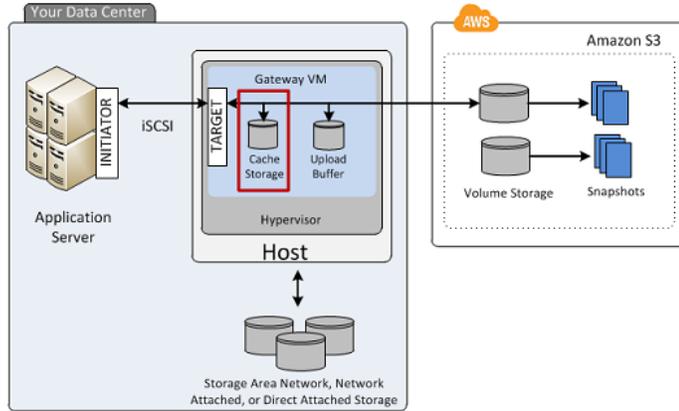
## 为缓存存储空间添加本地磁盘（网关缓存）

### Topics

- 配置缓存存储空间的大小（网关缓存）(p. 116)
- 为缓存存储空间添加虚拟磁盘（网关缓存）(p. 116)

在网关缓存架构中，您的网关为最近访问的数据维持场内缓存存储空间。网关持续将尚未上传到 Amazon S3 的数据存储在缓存存储空间中。您需要为缓存存储空间场内分配磁盘。

下图以更大幅的 AWS Storage Gateway 架构为背景，突出显示了缓存存储空间（请参见 [AWS Storage Gateway 的运行原理（架构）](#)（p. 3））。



### 配置缓存存储空间的大小（网关缓存）

网关使用缓存存储空间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 的数据的场内持久存储器。因此缓存存储空间应该大于上传缓冲区。

网关缓存存储总空间可高达 16 TiB。

如需估算网关所需的缓存存储空间量，该公式取决于您的使用案例：

- 备份使用案例—使用上传缓冲区 1.1 倍的缓存存储空间容量。对于备份使用案例，缓存是在上传到 AWS 前的持久存储器，并且必须将其大小配置为大于上传缓冲区，从而确保在 VM 发生故障的情况下不丢失数据。
- 其他使用案例—使用以下两个值中的较大值：现有本地存储的 20% 或上传缓冲区大小的 1.1 倍。

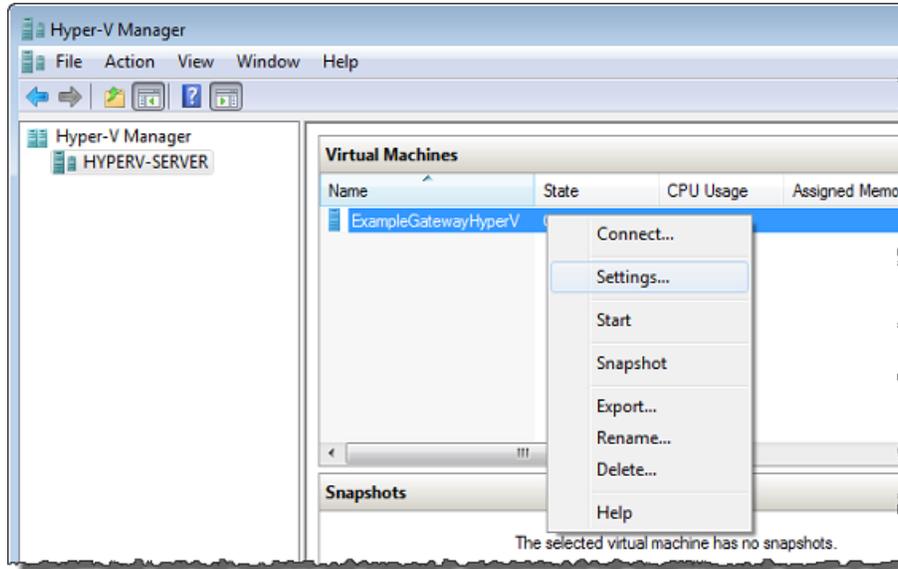
您可以将此近似值用来初步为缓存存储空间预配置磁盘。您然后可以使用 Amazon CloudWatch 运行指标来监控缓存存储空间使用率并使用控制台按需预配置更多的存储空间。有关使用指标和设置警报的信息，请参见 [监控缓存卷](#)（p. 252）。

### 为缓存存储空间添加虚拟磁盘（网关缓存）

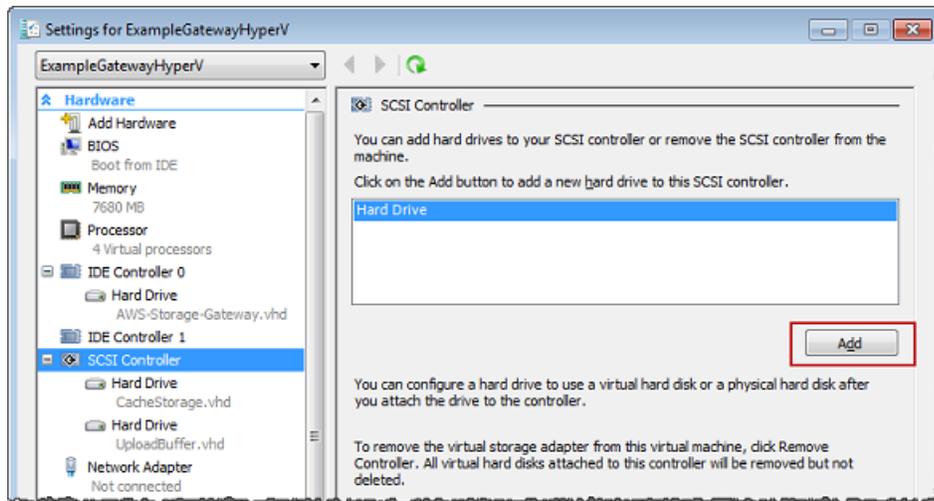
您可以从主机上可用的直接连接存储 (DAS) 磁盘或者存储区域网络 (SAN) 磁盘向 VM 分配虚拟磁盘。下列步骤提供有关从主机上可用的 DAS 磁盘添加虚拟磁盘的指导。

如需向磁盘分配新的虚拟磁盘以用作缓存存储空间

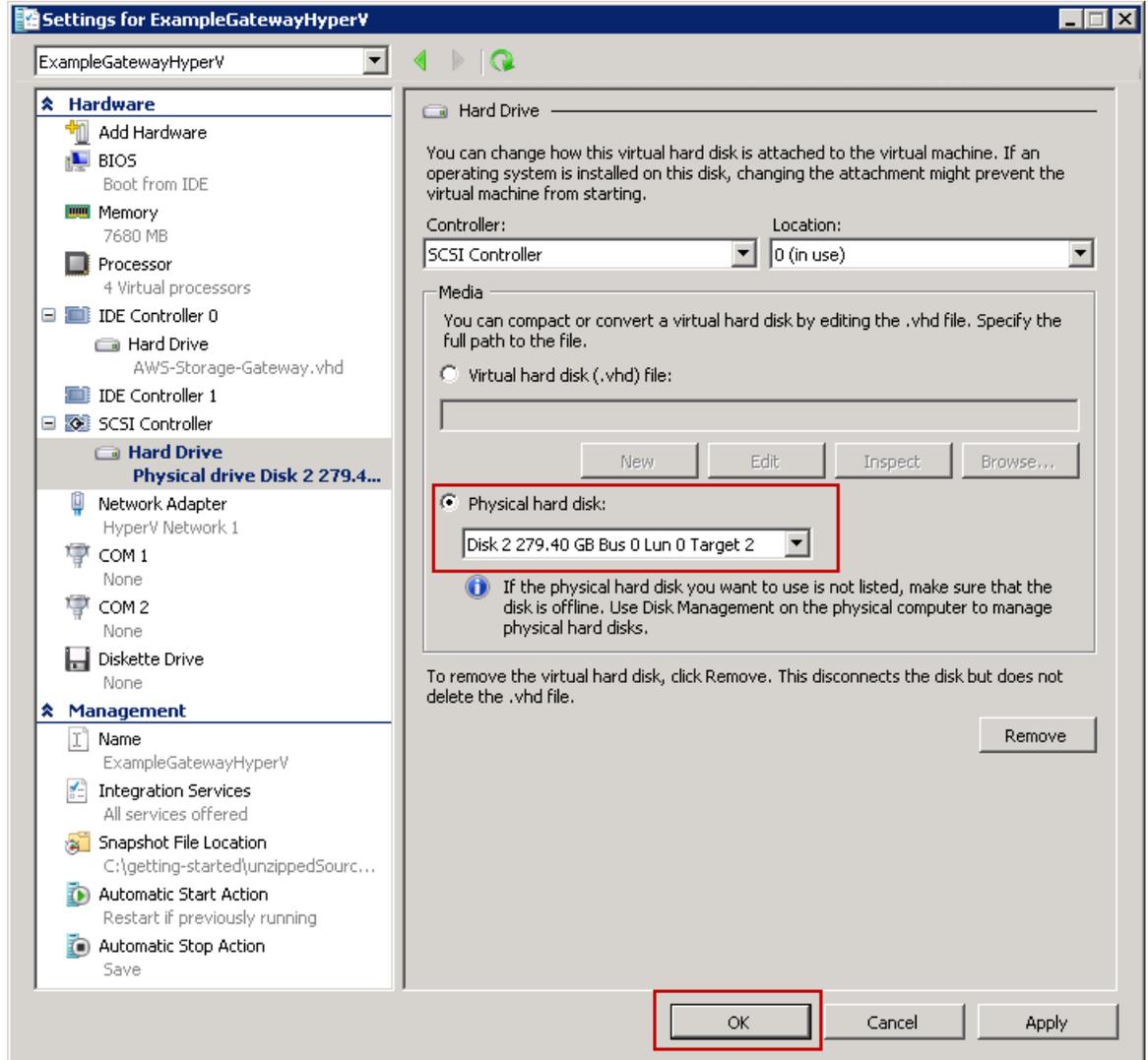
1. Start the Microsoft Hyper-V Manager and connect to your host.
2. In the client, right-click the name of your gateway VM and click Settings....



3. In the Hardware list in the left pane, click SCSI Controller.
4. In the SCSI Controller pane, Click Add.



5. In the Hard Drive pane, in the Media section click Physical hard disk and select a disk from the box.



6. Click OK.

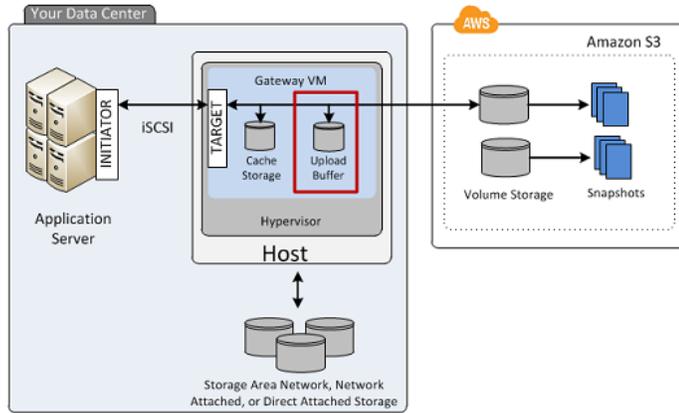
## 为上传缓冲区添加本地磁盘（网关缓存）

### Topics

- [配置上传缓冲区的大小（网关缓存）](#) (p. 119)
- [为上传缓冲区添加虚拟磁盘（网关缓存）](#) (p. 120)

您必须为网关分配场内磁盘，以使用作上传缓冲区，从而在数据上传到 AWS 前临时缓冲数据。有关分配磁盘存储量的准则，请参见 [配置上传缓冲区的大小（网关缓存）](#) (p. 97)。

下图以更大幅的 AWS Storage Gateway 架构为背景，突出显示了上传缓冲区。（请参见 [AWS Storage Gateway 的运行原理（架构）](#) (p. 3)）。



### 配置上传缓冲区的大小 (网关缓存)

您可以利用上传缓冲区公式来确定上传缓冲区的大小。我们强烈建议您至少分配 150 GiB 的上传缓冲区。因此，如果公式得出小于 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 2 TiB 的上传缓冲区。

#### Note

上传缓冲区达到其容量后，您的应用程序将持续不断地继续从/向存储卷读写数据；不过，网关不会将任何卷数据写入到其上传缓冲区，也不会将任何此类数据上传到 AWS 中，直到 Storage Gateway 将本地存储在缓存缓冲区的数据与存储在 AWS 中的数据副本进行同步。处于此状态的卷被称为处于 BOOTSTRAPPING 状态的卷。在 BOOTSTRAPPING 状态期间，应用程序写入的数据会持续不断地继续存储在网关缓存缓冲区中。BOOTSTRAPPING 完成后，系统会重新启用上传缓冲区，且该卷会返回已激活状态。有关卷状态的信息，请参见 [管理 AWS Storage Gateway 中的存储卷 \(p. 167\)](#) 和 [排查存储卷问题 \(p. 239\)](#) 中的“排查存储卷问题”部分。

如需更精确地估算上传缓冲区的量，您可以计算数据的传输和传出速率，并且根据这些速率进行估算。

- 数据传入速率—该速率指应用程序吞吐量，亦即您的场内应用程序在某段时间内将数据写入到网关的速率。
- 数据传出速率—该速率指网络吞吐量，亦即您的网关将数据上传到 AWS 时可达到的速率。该速率取决于您的网络速度以及您是否启用了带宽限制。该速率应该针对压缩率进行调整。将数据上传到 AWS 时，网关在可能的情况下实施数据压缩。例如，如果您的应用程序为纯文本，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，因而需要更多的网关上传缓冲区。

如果传入速率高于传出速率，您可以使用以下公式来确定网关所需的大致上传缓冲区大小。

$$\left( \text{Application Throughput (MB/s)} - \text{Network Throughput to AWS (MB/s)} \times \text{Compression Factor} \right) \times \text{Duration of writes (s)} = \text{Upload Buffer (MB)}$$

例如，假定您的商业应用程序每天 12 个小时以每秒 40 兆字节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 兆字节。假定文本数据的压缩系数为 2:1，您就需要为上传缓冲区分配约 690 GB。

$$((40 \text{ MB/sec}) - (12 \text{ MB/sec} * 2)) * (12 \text{ hours} * 3600 \text{ seconds/hour}) = 691200 \text{ megabytes}$$

请注意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 AWS Storage Gateway 控制台按需添加更多的上传缓冲区空间。另外，您可以使用 Amazon CloudWatch 运行指标来监控上传缓冲区使用率并确定额外的存储空间需求。有关指标和设置警报的信息，请参见 [监控上传缓冲区](#) (p. 249)。

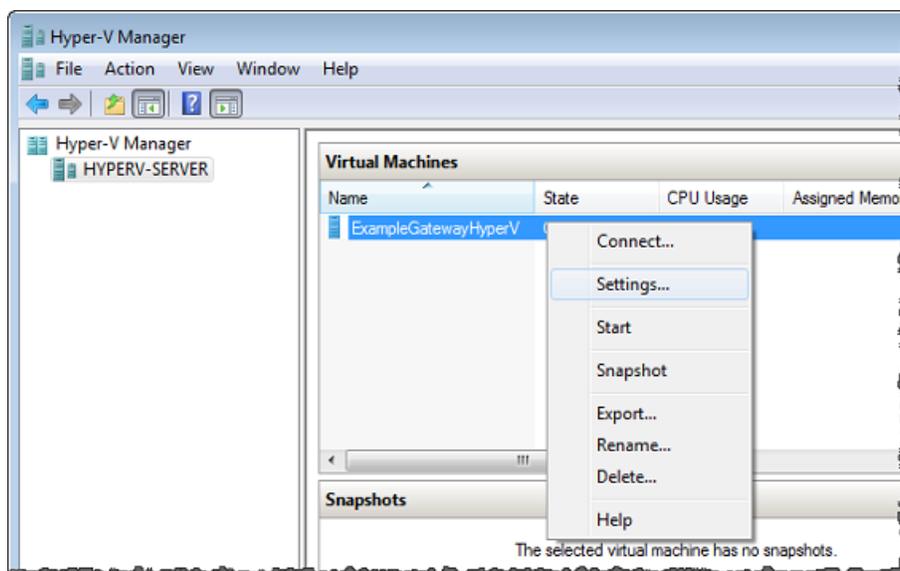
### 为上传缓冲区添加虚拟磁盘 (网关缓存)

在本部分中，您向 VM 分配虚拟磁盘，该磁盘将被用作网关的上传缓冲区。

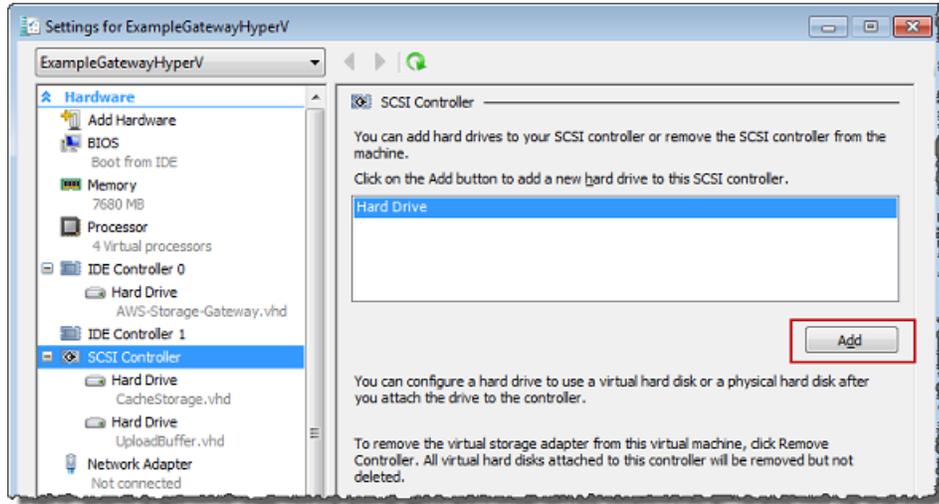
您可以从主机上可用的直接连接存储 (DAS) 磁盘或者存储区域网络 (SAN) 磁盘向 VM 分配虚拟磁盘。以下步骤提供从主机上可用的 DAS 磁盘添加虚拟磁盘的分步指导。

如需向 VM 分配新的虚拟磁盘用作上传缓冲区

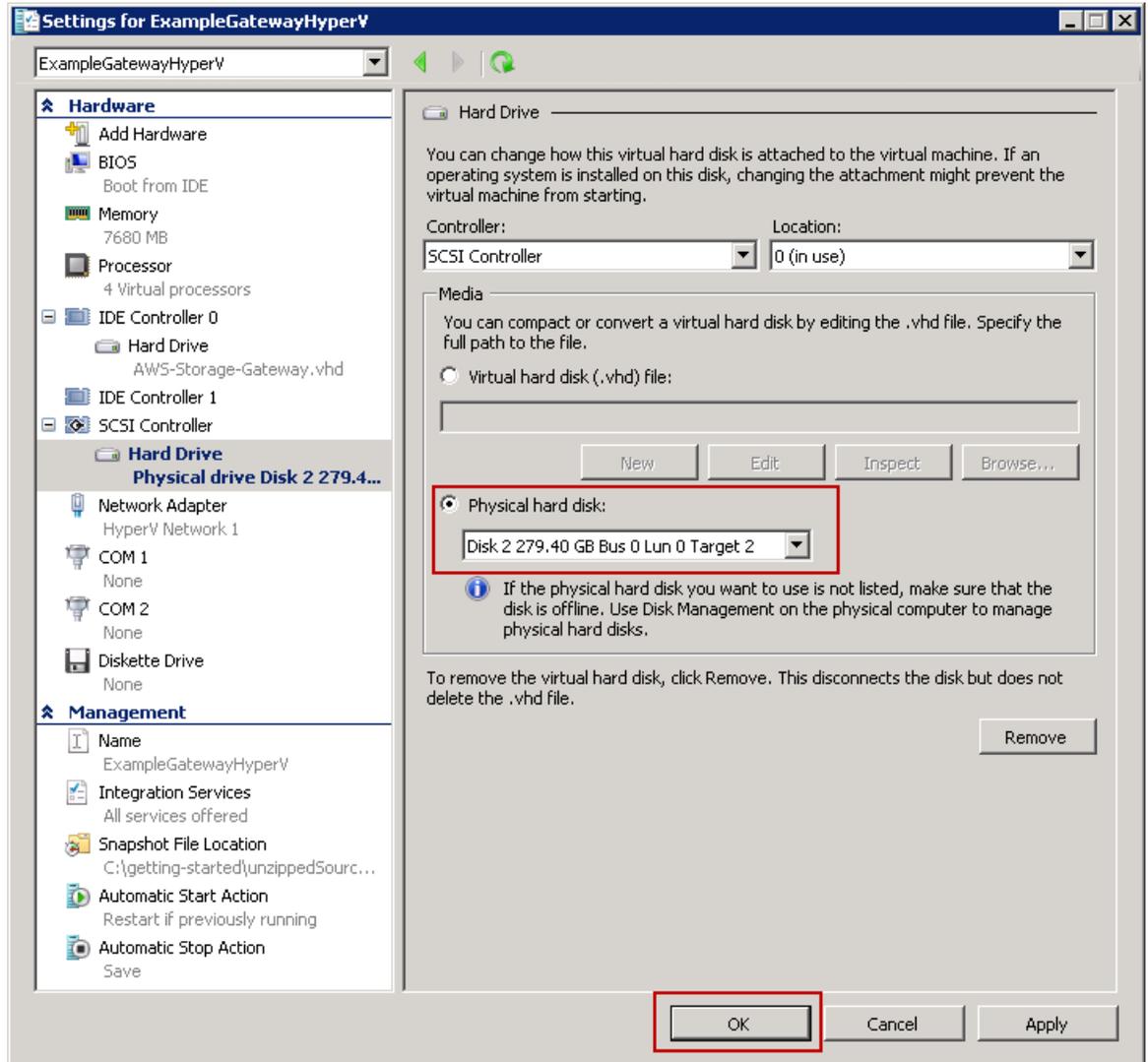
1. Start the Microsoft Hyper-V Manager and connect to your host.
2. In the client, right-click the name of your gateway VM and click Settings....



3. In the Hardware list in the left pane, click SCSI Controller.
4. In the SCSI Controller pane, Click Add.



5. In the Hard Drive pane, in the Media section click Physical hard disk and select a disk from the box.



6. Click OK.

## 预配置本地磁盘 ( 网关存储 )

### Topics

- 为存储卷添加本地磁盘 ( 网关存储 ) (p. 122)
- 为上传缓冲区添加本地磁盘 ( 网关存储 ) (p. 124)

在本地存储架构中，网关将您的卷数据存储在场内存储硬件中。您的所有应用程序数据均在场内保存。您必须给网关 VM 预配置磁盘，用作卷存储。您还须预配置磁盘，用作网关的上传缓冲区。有关网关工作方式的更多信息，请参见 [AWS Storage Gateway 的运行原理 \( 架构 \)](#) (p. 3)。



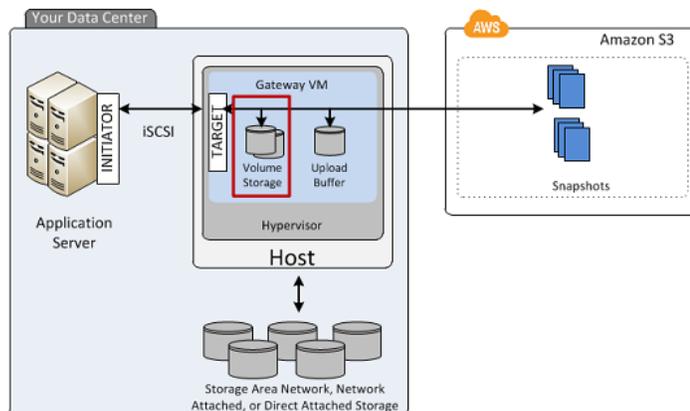
### Note

配置磁盘时，强烈建议您不要将本地磁盘配置为使用相同底层物理存储资源 ( 磁盘 ) 的上传缓冲区和本地应用程序存储空间。在 Microsoft Hyper-V 中，当为网关预配置本地磁盘时 ( 例如，将其用作本地应用程序存储或者上传缓冲区 )，您可以将其创建为虚拟硬盘 (.vhd) 文件，或者从物理硬盘中创建。是选择 .vhd 还是物理磁盘，取决于您的性能和便携性要求。根据物理磁盘预配置本地磁盘的便携性低于使用 .vhd。

## 为存储卷添加本地磁盘 ( 网关存储 )

在网关存储架构中，您的应用程序数据在本地存储。您需要向网关 VM 预配置磁盘，以便存储您的数据。

以下示意图以更大幅的 AWS Storage Gateway 架构为背景，突出显示了存储卷 ( 请参见 [AWS Storage Gateway 的运行原理 \( 架构 \)](#) (p. 3) )。

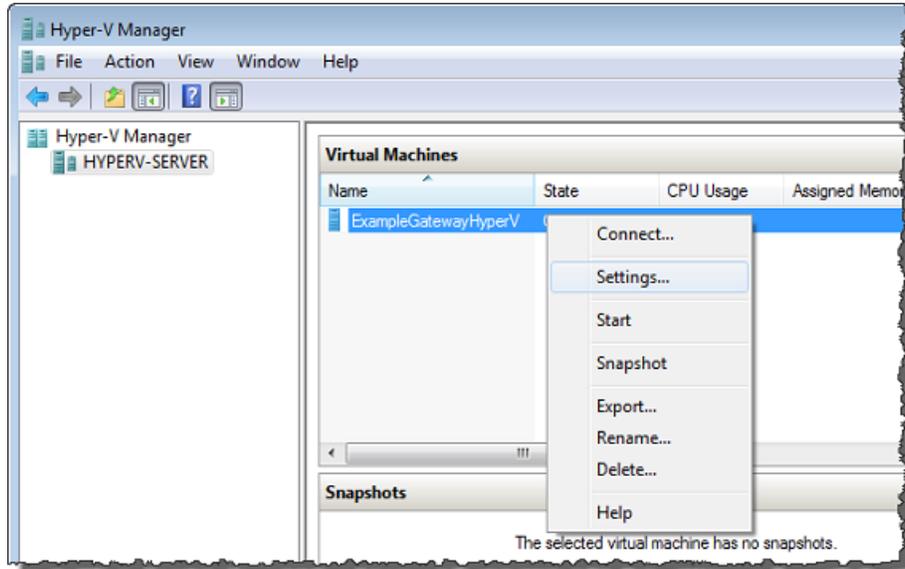


每个磁盘的大小可高达 1 TiB，并且须四舍五入到最接近的整 GiB 值，而 GiB 值使用 Base 2 ( 即  $\text{GiB} = 1024^3$  字节 ) 计算。

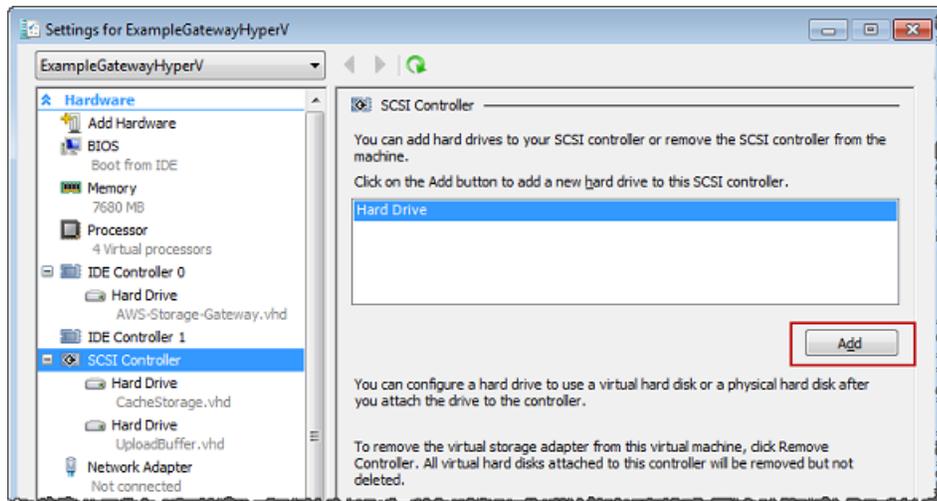
您可以从主机上可用的直接连接存储 (DAS) 磁盘或者存储区域网络 (SAN) 磁盘向 VM 预配置磁盘，以使用作卷存储空间。对于卷存储空间，您分配的磁盘可以有现有数据。我们在创建您的 iSCSI 存储卷时保存这些数据。下列步骤提供从 DAS 磁盘添加虚拟磁盘的指导。

### 为应用程序数据向 VM 添加新的虚拟磁盘

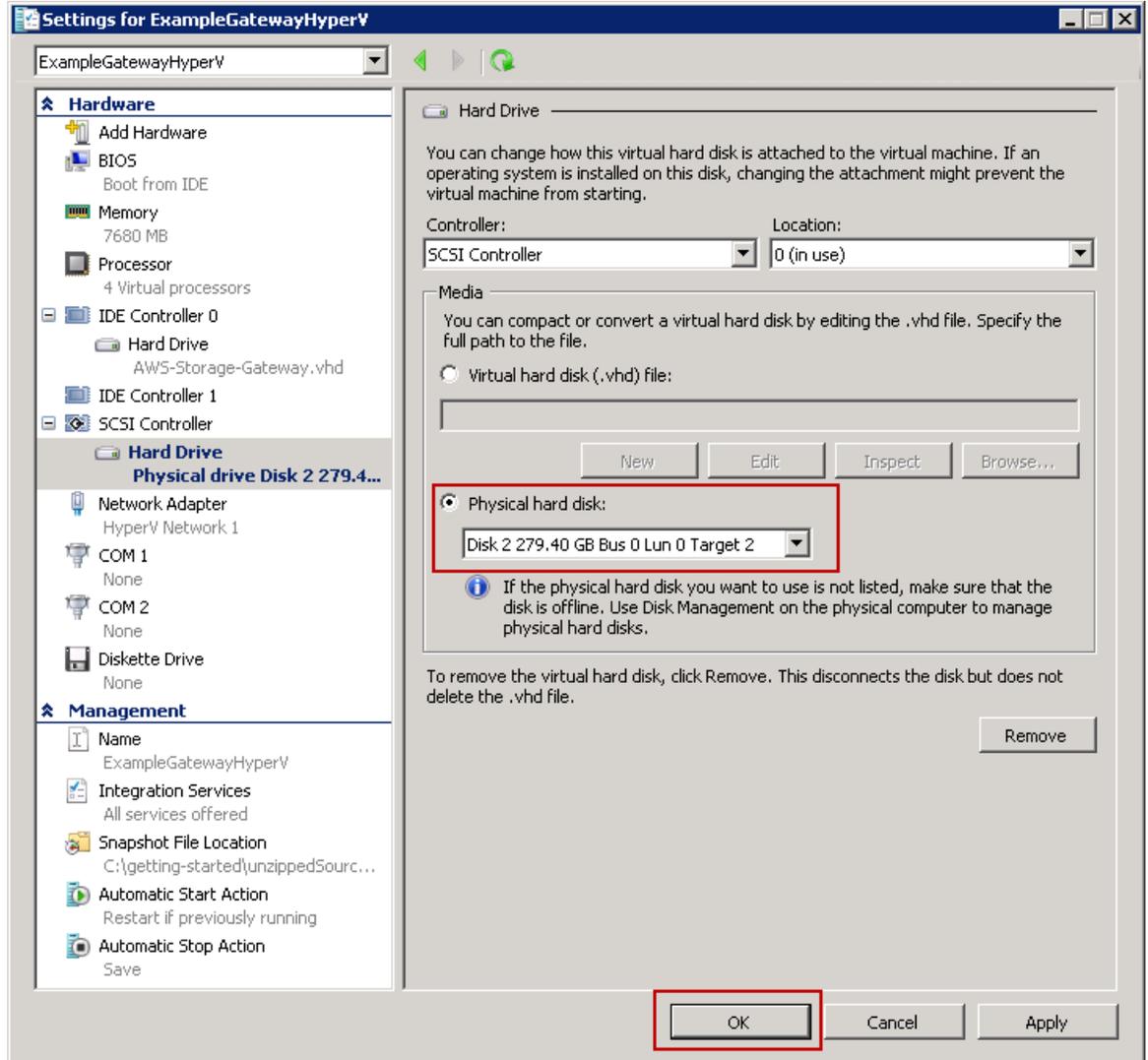
1. Start the Microsoft Hyper-V Manager and connect to your host.
2. In the client, right-click the name of your gateway VM and click Settings....



3. In the Hardware list in the left pane, click SCSI Controller.
4. In the SCSI Controller pane, Click Add.



5. In the Hard Drive pane, in the Media section click Physical hard disk and select a disk from the box.



6. Click OK.

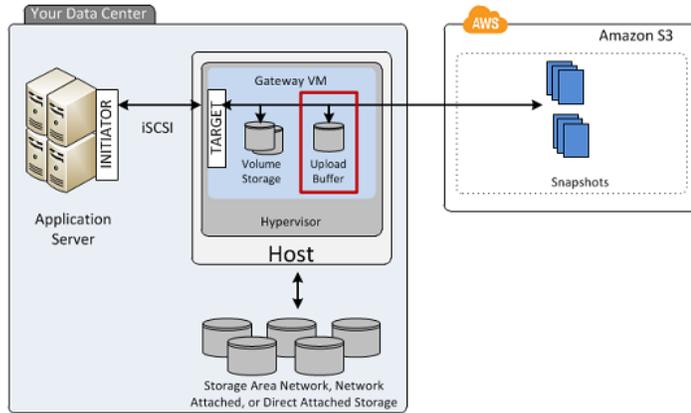
### 为上传缓冲区添加本地磁盘（网关存储）

#### Topics

- [配置上传缓冲区的大小（网关存储）](#) (p. 125)
- [为上传缓冲区添加虚拟磁盘（网关存储）](#) (p. 126)

您必须为网关分配场内磁盘，以使用作上传缓冲区，从而在数据上传到 AWS 前临时缓冲数据。

下图以更大幅的 AWS Storage Gateway 架构为背景，突出显示了上传缓冲区（请参见 [AWS Storage Gateway 的运行原理（架构）](#) (p. 3)）。



### 配置上传缓冲区的大小 ( 网关存储 )

您可以利用上传缓冲区公式来确定上传缓冲区的大小。我们强烈建议您至少分配 150 GiB 的上传缓冲区。因此，如果公式得出小于 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 2 TiB 的上传缓冲区。



#### Note

上传缓冲区达到其容量后，您的应用程序将持续不断地继续从/向存储卷读写数据；不过，网关不会将任何卷数据写入到其上传缓冲区，也不会将任何此类数据上传到 AWS 中，直到 Storage Gateway 将本地存储在缓存缓冲区的数据与存储在 AWS 中的数据副本进行同步。处于此状态的卷被称为处于 BOOTSTRAPPING 状态的卷。在 BOOTSTRAPPING 状态期间，应用程序写入的数据会持续不断地继续存储在网关缓存缓冲区中。BOOTSTRAPPING 完成后，系统会重新启用上传缓冲区，且该卷会返回已激活状态。有关卷状态的信息，请参见 [管理 AWS Storage Gateway 中的存储卷 \(p. 167\)](#) 和 [排查存储卷问题 \(p. 239\)](#) 中的“排查存储卷问题”部分。

如需估算上传缓冲区的量，您可以计算数据的传输和传出速率，并且根据这些速率进行估算。

- 数据传入速率—该速率指应用程序吞吐量，亦即您的场内应用程序在某段时间内将数据写入到网关的速率。
- 数据传出速率—该速率指网络吞吐量，亦即您的网关将数据上传到 AWS 时可达到的速率。该速率取决于您的网络速度以及您是否启用了带宽限制。该速率应该针对压缩率进行调整。将数据上传到 AWS 时，网关在可能的情况下实施数据压缩。例如，如果您的应用程序为纯文本，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，因而需要更多的网关上传缓冲区。

如果传入速率高于传出速率，您可以使用以下公式来确定网关所需的大致上传缓冲区大小。

$$\left( \text{Application Throughput (MB/s)} - \text{Network Throughput to AWS (MB/s)} \times \text{Compression Factor} \right) \times \text{Duration of writes (s)} = \text{Upload Buffer (MB)}$$

例如，假定您的商业应用程序每天 12 个小时以每秒 40 兆字节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 兆字节。假定文本数据的压缩系数为 2:1，您就需要为上传缓冲区分配约 690 GB。

$$((40 \text{ MB/sec}) - (12 \text{ MB/sec} * 2)) * (12 \text{ hours} * 3600 \text{ seconds/hour}) = 691200 \text{ megabytes}$$

请注意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 AWS Storage Gateway 控制台按需添加更多的上传缓冲区空间。另外，您可以使用 Amazon CloudWatch 运行指标来监控上传缓冲区使用率并确定额外的存储空间需求。有关指标和设置警报的信息，请参见 [监控上传缓冲区](#) (p. 249)。

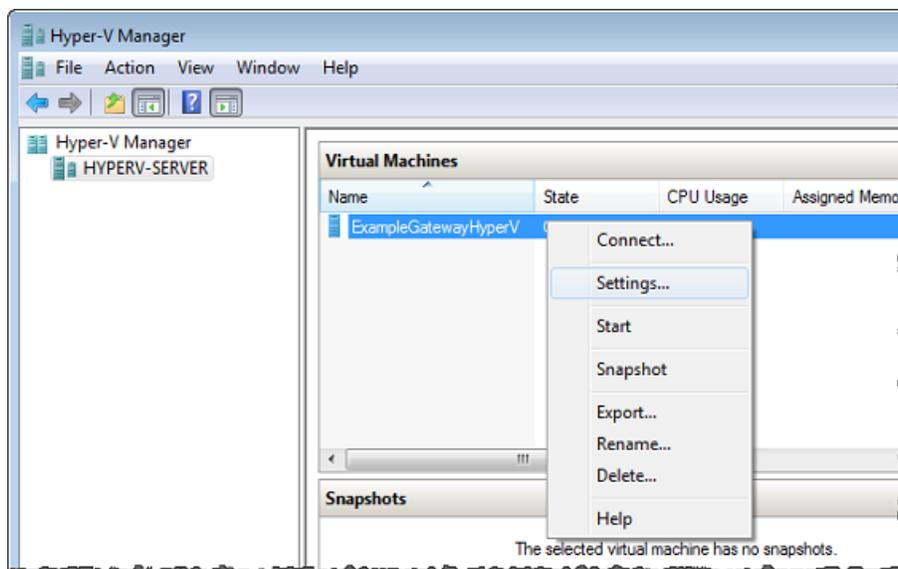
### 为上传缓冲区添加虚拟磁盘 (网关存储)

在本部分中，您向 VM 分配虚拟磁盘，该磁盘将被用作网关的上传缓冲区。若要估算网关所需的上传缓冲区，请参见 [配置上传缓冲区的大小 \(网关存储\)](#) (p. 104)。

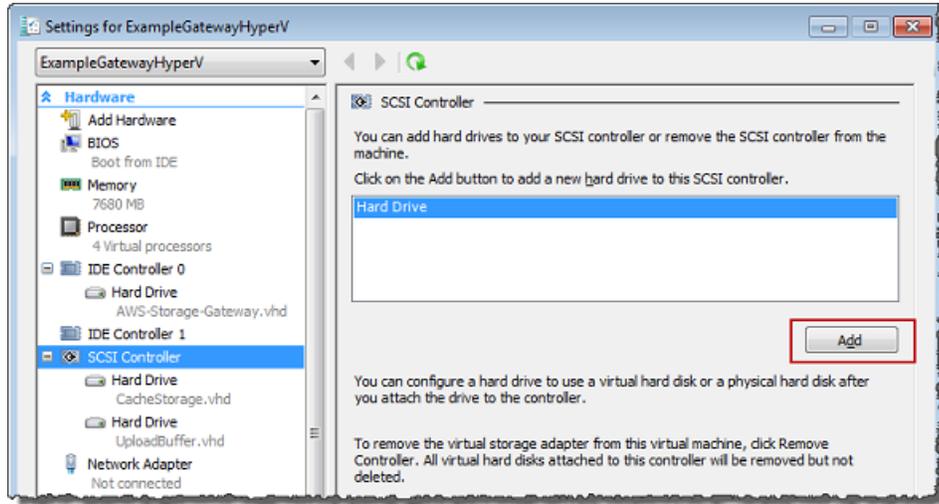
您可以从主机上可用的直接连接存储 (DAS) 磁盘或者存储区域网络 (SAN) 磁盘向 VM 分配虚拟磁盘。以下步骤提供从主机上可用的 DAS 磁盘添加虚拟磁盘的分步指导。

### 如需向 VM 分配新的虚拟磁盘用作上传缓冲区

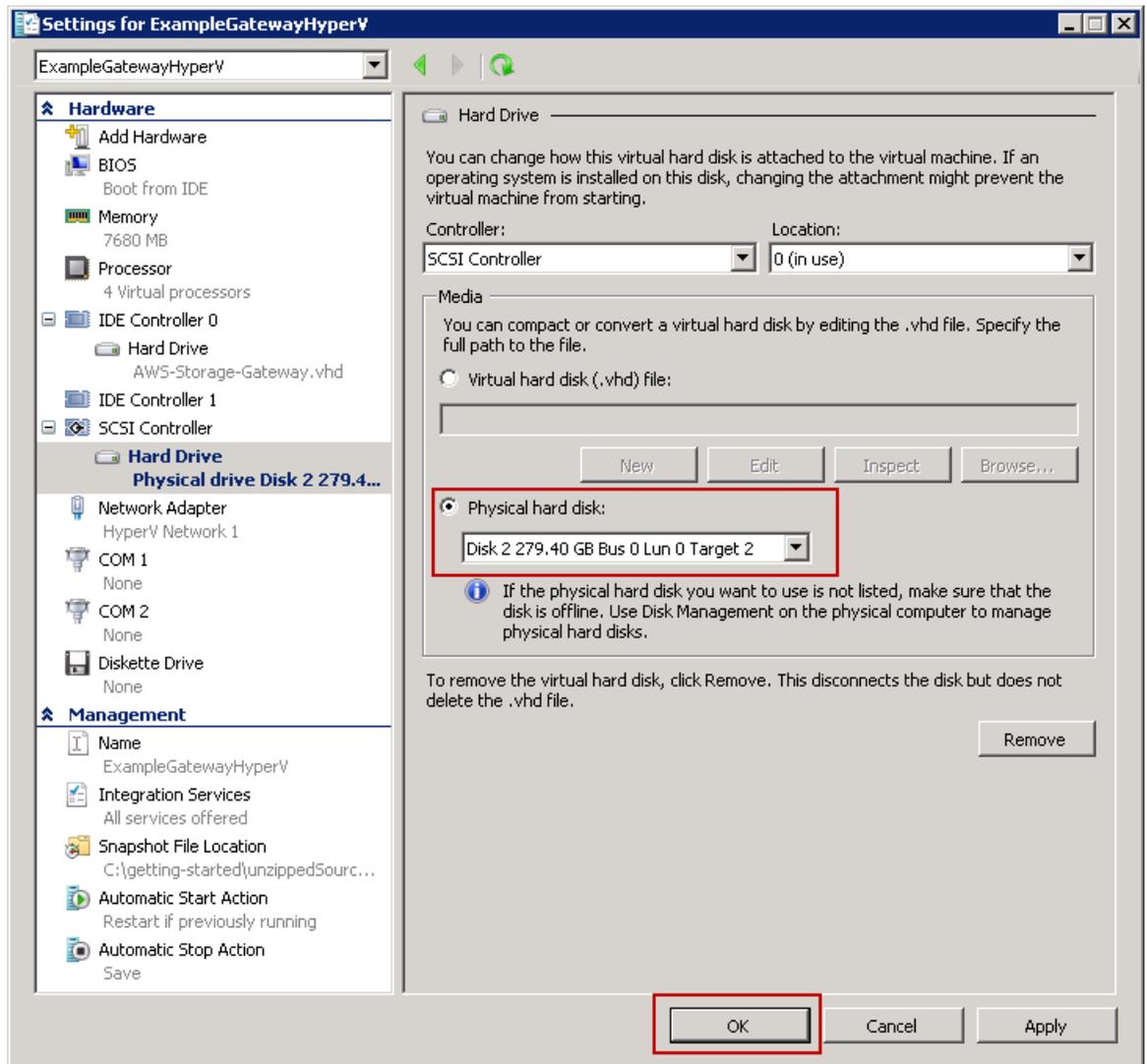
1. Start the Microsoft Hyper-V Manager and connect to your host.
2. In the client, right-click the name of your gateway VM and click Settings....



3. In the Hardware list in the left pane, click SCSI Controller.
4. In the SCSI Controller pane, Click Add.



5. In the Hard Drive pane, in the Media section click Physical hard disk and select a disk from the box.



6. Click OK.

## 激活 AWS Storage Gateway

部署 AWS Storage Gateway VM 后，您必须使用 AWS Storage Gateway 控制台激活该网关。激活过程将您的网关与 AWS 账户关联。建立该连接后，您可以从管理台管理网关的几乎所有方面。在激活过程中，您指定网关的 IP 地址，命名网关，识别希望存储快照备份的 AWS 地区，并且指定网关时区。激活后，您开始产生费用。有关定价的信息，请参阅 [AWS Storage Gateway](#)。

### 激活前清单

您可以在完成下表总结的步骤后激活网关。控制台向导引导您完成这些步骤。

步骤	说明
下载并部署 VM	在 AWS Storage Gateway 控制台中，下载以 .zip 文件形式分发的最新虚拟机 (VM)，然后将此 VM 部署 (导入) 到您的 Microsoft Hyper-V 主机上。有关更多信息，请参阅 <a href="#">下载和部署 AWS Storage Gateway VM (p. 113)</a> 。
将本地磁盘预配置到 VM	预配置的 VM 没有磁盘。根据您激活的网关类型的不同，您必须为下列各项添加本地磁盘： <ul style="list-style-type: none"><li>• 为已激活缓存卷的网关添加缓存存储空间和上传缓冲区。有关更多信息，请参阅 <a href="#">预配置本地磁盘 (网关缓存) (p. 115)</a>。</li><li>• 为存储卷激活的网关的应用程序数据和上传缓冲区。有关更多信息，请参阅 <a href="#">预配置本地磁盘 (网关存储) (p. 122)</a>。</li></ul>

### 网关激活步骤

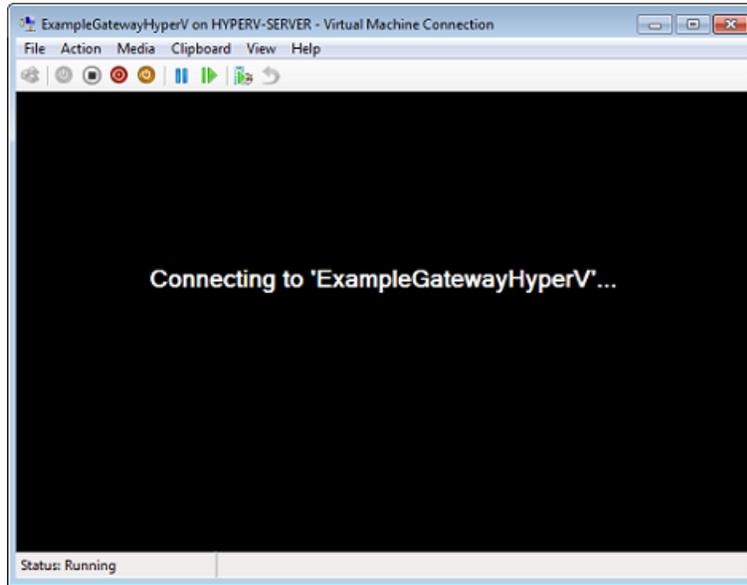
可使用 AWS Storage Gateway 控制台或 AWS Storage Gateway API ( 请参阅 [API\\_ActivateGateway](#) ) 激活网关。如需激活网关，您需要了解网关 VM 的 IP 地址。开始激活过程前，请确保将用来进行激活的计算机可通过网络访问网关。

以下过程展示如何使用 Microsoft Hyper-V 管理器激活网关以获取网关 VM 的 IP 地址，然后如何在控制台的设置并激活网关向导中使用该 IP 地址。

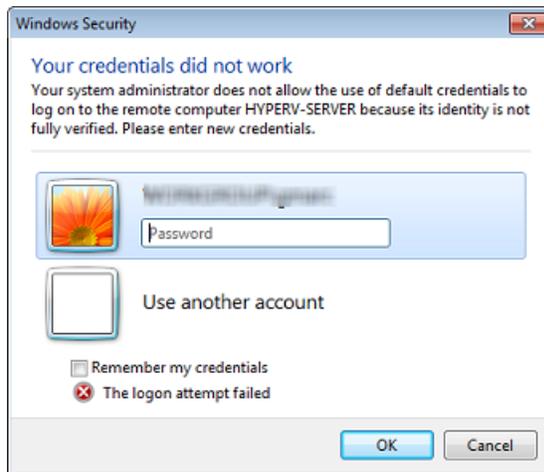
#### 如需使用控制台激活网关

1. 如果 VM 尚未启动，请启动。
  - a. 启动 Microsoft Hyper-V Manager，然后连接到虚拟机监控程序。
  - b. 在虚拟机列表窗格中，选择虚拟机 ExampleGatewayHyperV。
  - c. 在操作窗格中，选择启动。

随后将显示虚拟机连接窗口。



- d. 如果显示身份验证窗口，请输入管理程序管理员向您提供的用户名称和密码。



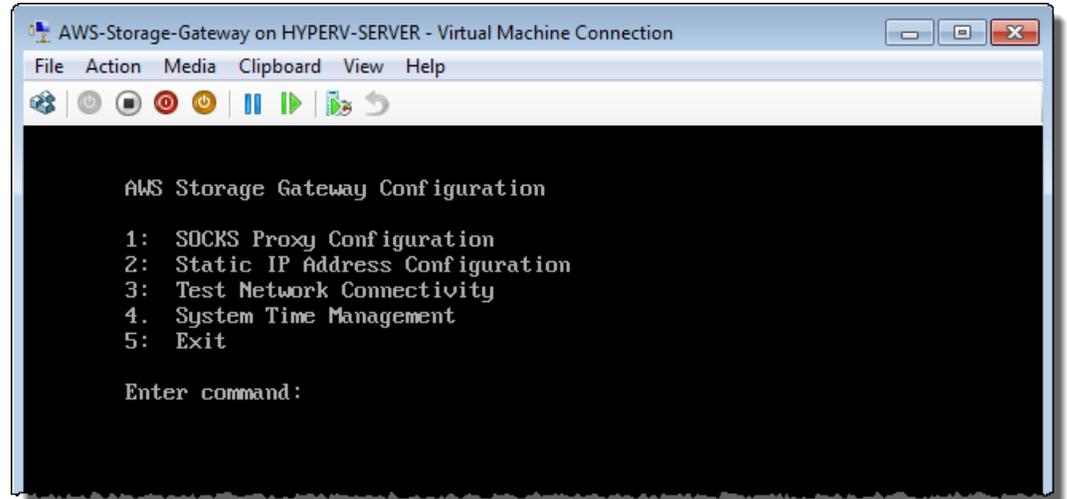
- e. 在过几分钟时间后，虚拟机就会准备就绪，供您登录了。

## 2. 激活网关。

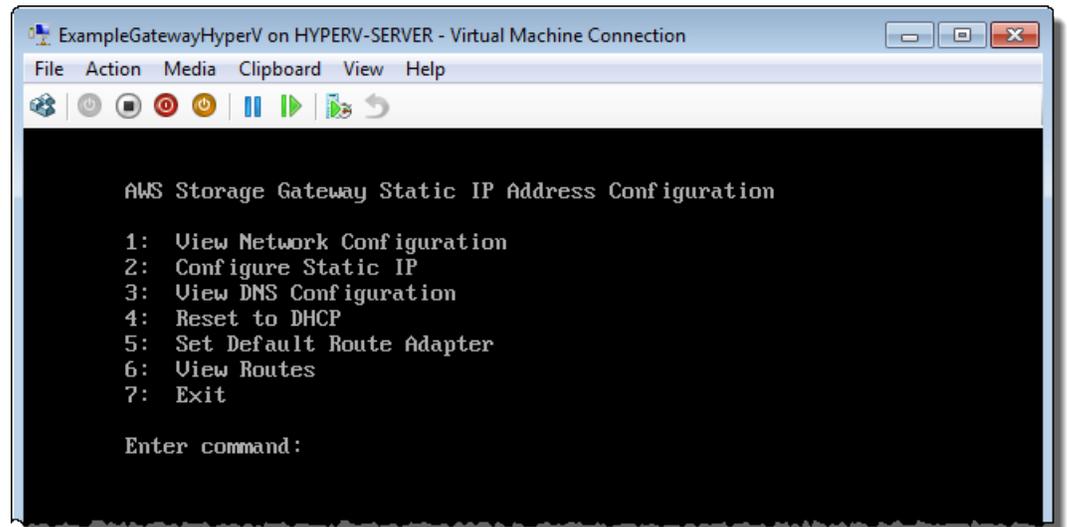
- a. 取得您的网关的 IP 地址。请注意，在打开 VM 后，可能需要一些时间才能让网关准备好，以便您登录和获取 IP 地址。
- 在 Microsoft Hyper-V Manager 中，选择部署的网关 VM。
  - 在虚拟机列表窗格中，选择虚拟机 ExampleGatewayHyperV。
  - 在操作窗格中，选择连接。

随后将显示虚拟机连接窗口。

- 在出现登录提示时，输入用户名 `sguser` 和密码 `sgpassword`。
- 在 AWS Storage Gateway 配置菜单中，选择选项 2 静态 IP 地址配置。

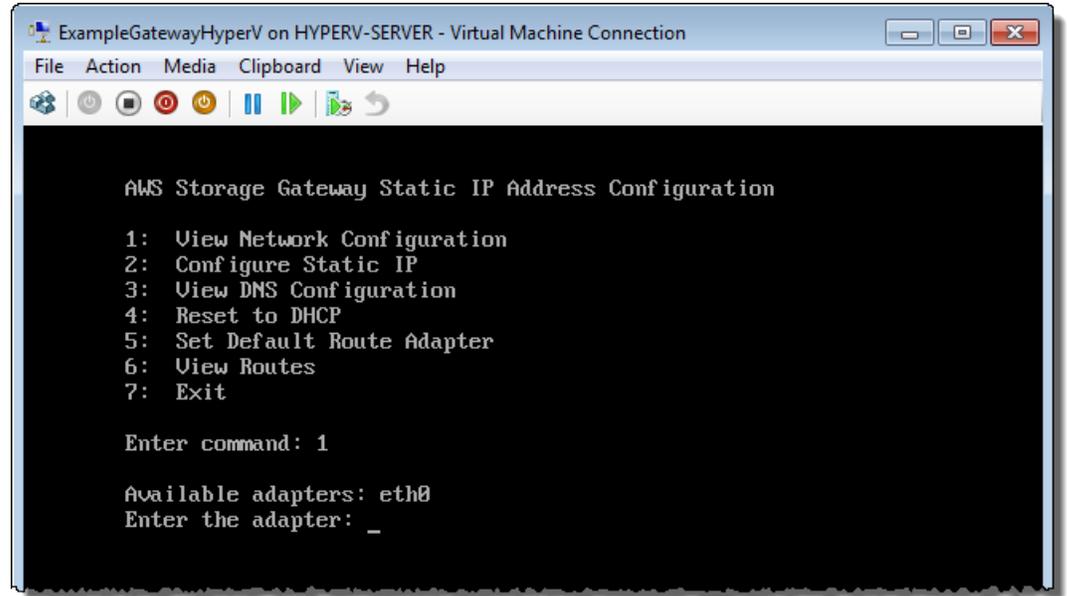


- vi. 在 AWS Storage Gateway 静态 IP 地址配置菜单中，选择选项 1 查看网络配置。



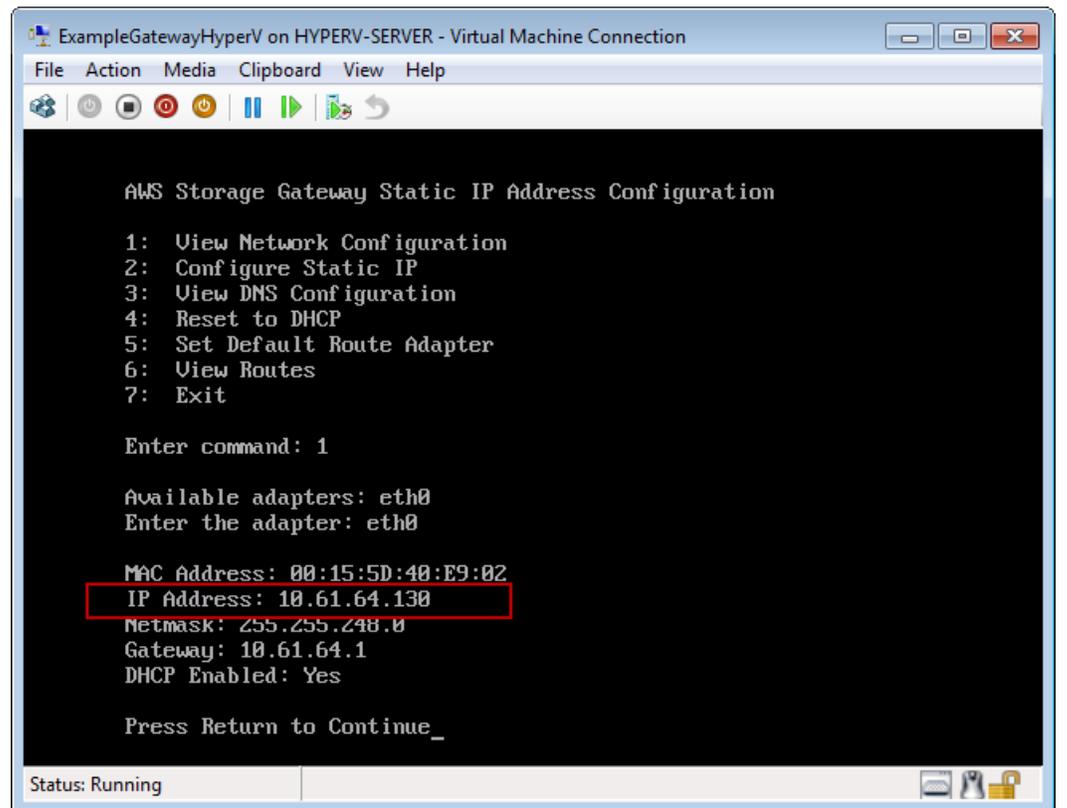
- vii. 键入适配器的标识符。

在大多数情况下，eth0 将为该适配器标识符。



viii. 从适配器信息中获取 IP 地址。

在下例中，IP 地址为 10.61.64.130。您的网关的 IP 地址将会不同。



ix. 按 Return，然后按提示退出配置菜单。

b. 将您的网关关联到 AWS 账户

- i. 返回控制台，如果尚未打开设置并激活网关向导，则请照做，继续进行激活网关步骤，输入 IP 地址，然后单击继续激活。您的浏览器必须运行在可通过网络连接到本地网关主机的机器上。

**Setup and Activate Gateway** close

PROVISION HOST    DOWNLOAD AND DEPLOY VM    PROVISION LOCAL DISK STORAGE    **ACTIVATE GATEWAY**

Using your Hyper-V Manager client, double-click on your imported gateway VM and select "Start". Follow the instructions that are subsequently shown to log in.

Select "2: Static IP Address Configuration". In the next screen, select "1: View Network Configuration". Enter the available network adapter. This will show you the IP address, which you type into the box below.

```
MAC Address: 08:15:5D:63:8A:18
IP Address: 192.168.99.221
Netmask: 255.255.255.0
Gateway: 192.168.99.1
DHCP Enabled: Yes

Press Return to Continue_
```

Screenshot of the IP address look-up. This action is taken outside of the AWS Management Console.

Clicking "Proceed to Activation" will redirect you to the activation page (your browser must be running on a machine with network connectivity to your local gateway host).

**Step-by-Step Instructions**

Enter IP Address Below:

[Back](#) Proceed to Activation



#### Note

如果激活失败，请检查您输入的 IP 地址是否正确，然后重试激活。如果 IP 地址正确无误，则确认网关可访问 Internet，如有必要，则还要设置代理（请参阅[将 AWS Storage Gateway 的路由选为通过代理](#) (p. 222)）。

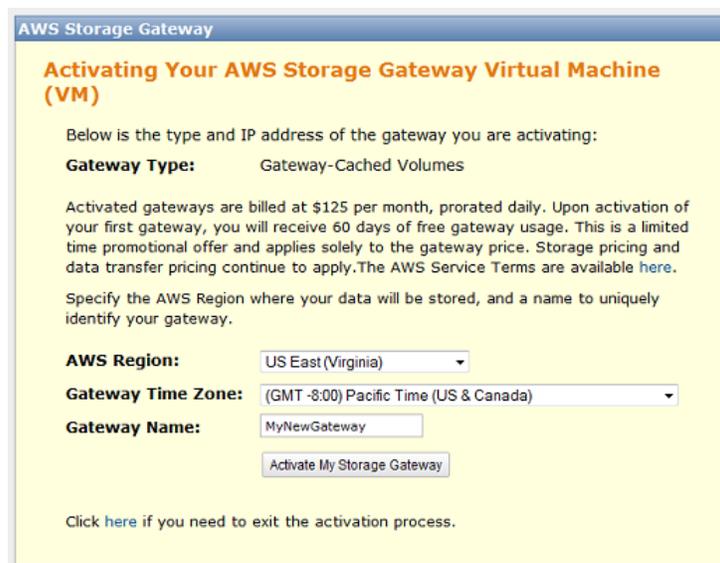
- ii. 在激活页面上，填写请求的信息以完成激活过程。

网关类型指定所激活的网关的类型。您可以激活网关的缓存卷或存储卷。有关更多信息，请参阅[AWS Storage Gateway 的运行原理（架构）](#) (p. 3)。

AWS 地区决定 AWS 存储快照的位置。如果您选择将快照还原为 Amazon EBS 卷，Amazon EBS 卷就必须和快照在同一地区。您不可以在网关激活后更改地区。

网关时区是显示基于时间的信息（如来自 AWS 的维护消息以及快照调度）时使用的时区。您可以在激活后更改时区。

网关名称在控制台中标识您的网关。您可以使用该名称在控制台中管理网关，然后在激活后更改名称。



**AWS Storage Gateway**

### Activating Your AWS Storage Gateway Virtual Machine (VM)

Below is the type and IP address of the gateway you are activating:

**Gateway Type:** Gateway-Cached Volumes

Activated gateways are billed at \$125 per month, prorated daily. Upon activation of your first gateway, you will receive 60 days of free gateway usage. This is a limited time promotional offer and applies solely to the gateway price. Storage pricing and data transfer pricing continue to apply. The AWS Service Terms are available [here](#).

Specify the AWS Region where your data will be stored, and a name to uniquely identify your gateway.

**AWS Region:** US East (Virginia)

**Gateway Time Zone:** (GMT -8:00) Pacific Time (US & Canada)

**Gateway Name:** MyNewGateway

[Click here](#) if you need to exit the activation process.

iii. 单击激活我的 Storage Gateway。

成功激活后，AWS 存储网关 控制台即显示激活的 gateway 和一个链接，供您创建卷。



#### 相关部分

- [AWS Storage Gateway 的 API 参考 \(p. 418\)](#)

## 在 Amazon EC2 上部署并激活 AWS Storage Gateway

#### Topics

- [Amazon EC2 网关与本地网关的比较 \(p. 134\)](#)
- [启动并激活 Amazon EC2 网关 AMI \(p. 134\)](#)
- [管理您的 Amazon EC2 网关 \(p. 139\)](#)

本节讨论如何在 Amazon Elastic Compute Cloud (Amazon EC2) 上部署 AWS Storage Gateway 缓存卷。部署网关并添加本地磁盘存储后，您激活并使用该网关，如同使用本地网关一样。有关网关缓存卷的工作方式的信息，请参阅 [AWS Storage Gateway 的运行原理 \(架构\) \(p. 3\)](#)。

用于 Amazon EC2 的 AWS Storage Gateway 缓存卷是一个亚马逊系统映像 (AMI)，通过它可创建实例。可在 AWS Marketplace 中以 [AWS Storage Gateway](#) 的形式获得该 AMI，也可从 AWS Storage Gateway 控制台中访问它。本节介绍如何使用 AMI 创建 & EC2 托管的网关缓存卷。有关使用 AMI 的详细信息，请转到 *Amazon Elastic Compute Cloud 用户指南* 中的 [亚马逊系统映像 \(AMI\)](#)。

建议网关缓存卷和网关 VTL 架构使用托管在 Amazon EC2 实例中的网关（请参阅 [AWS Storage Gateway 的运行原理（架构）](#) (p. 3)）。部署在 Amazon EC2 上的网关支持创建最大为 32 TiB 的卷。要开始创建 Amazon EC2- 托管的网关缓存卷，请转到 [启动并激活 Amazon EC2 网关 AMI](#) (p. 134)。

## Amazon EC2 网关与本地网关的比较

在云中 Amazon EC2 实例中托管的网关与在本地托管的 VMware ESXi 或 Microsoft Hyper-V 等虚拟化环境中托管的网关有一些区别。下表总结了这些不同之处。

功能	本地网关缓存卷	EC2 网关缓存卷
网关提供方式	以 .ova 文件形式提供本地网关，可从 AWS Storage Gateway 控制台中下载它。有关 .ova 文件的详细信息，请参阅 <a href="#">下载和部署 AWS Storage Gateway VM</a> (p. 90)。	以 AMI 形式提供 Amazon EC2 网关，可通过它创建 EC2 实例。可在 <a href="#">AWS Marketplace</a> 中获得 AMI，也可单击 AWS Storage Gateway 控制台中的部署链接，通过该链接将进入 AWS Marketplace。有关部署 Amazon EC2 AMI 作为网关的详细信息，请参阅 <a href="#">启动并激活 Amazon EC2 网关 AMI</a> (p. 134)。
登录到网关	您可以登录到场内网关执行维护任务，例如将网关路由选定为通过代理，将网关配置为使用静态 IP 地址，测试网关到 Internet 的连接等。有关更多信息，请参阅 <a href="#">登录到 AWS Storage Gateway 本地控制台</a> (p. 218)。	可使用 <code>sguser</code> 用户和您的私钥允许或禁止 AWS Support 访问您的网关。AWS Support 对网关的访问默认不启用。您可以在启动实例后启用 Support 的访问。请务必保存好您在创建实例过程中使用的密钥对，以便稍后连接到该实例。有关更多信息，请参阅 <a href="#">启用和禁用 AWS Support 的访问</a> (p. 141)。
多个网络适配器	您可以为一个场内网关配置多个网络适配器。有关更多信息，请参阅 <a href="#">针对多个网络适配器 (NIC) 配置 AWS Storage Gateway</a> (p. 229)。	您不能为一个 EC2 托管的网关配置多个网络适配器。
维护您的网关	有关维护本地网关的信息，请参阅 <a href="#">针对多个网络适配器 (NIC) 配置 AWS Storage Gateway</a> (p. 229)。	有关维护部署在 Amazon EC2 上的网关的信息，请参阅 <a href="#">管理您的 Amazon EC2 网关</a> (p. 139)。

## 启动并激活 Amazon EC2 网关 AMI

可在云中以 EC2 实例的形式运行网关。AWS Storage Gateway 提供一个亚马逊系统映像 (AMI)，其中包含网关 VM 映像。可在 AWS Marketplace ([AWS Storage Gateway](#)) 上获得 AMI，供您从 Amazon EC2 控制台中或从 AWS Storage Gateway 控制台中启动实例。



### Important

无论采用何种方式访问 AMI，我们都强烈建议您选择 AWS Marketplace 中的与 EC2 控制台一同启动选项用于启动您的实例。下方的过程中记载了执行此操作的步骤。如果决定使用单键启动功能启动实例，则需要启动该实例后，作为一个单独的步骤，将 Amazon EBS 卷添加到您的实例。

本节介绍启动 AWS Storage Gateway AMI 和激活网关缓存的过程。

### 步骤 1：选择某个 AWS Storage Gateway AMI

1. 在 AWS Storage Gateway 控制台中，单击在 Amazon EC2 上部署新网关。



2. 在在 Amazon EC2 上设置并激活网关向导中，选择网关缓存卷作为网关类型，然后完成四个步骤。



3. 在在 Amazon EC2 上设置并激活网关向导的第 1 步中，单击启动网关 AMI。

此操作将在浏览器的新选项卡中打开 AWS Marketplace 页。

4. 在 AMI 的 AWS Marketplace 页上，单击继续。

**AWS Storage Gateway**  
Sold by: [Amazon Web Services](#)

The AWS Storage Gateway is a service connecting a software appliance with cloud-based storage to provide seamless and secure integration between an organization's EC2 instances and AWS's storage infrastructure. The service enables you to securely store data to the AWS cloud for scalable and cost-effective storage. The AWS Storage Gateway supports industry-standard storage protocols that work with your existing applications. It provides low-latency performance by maintaining frequently accessed data locally while securely storing all of your data encrypted in the Amazon Simple Storage Service ... [Read more](#)

**Customer Rating** [Be the first to review this product](#)

**Latest Version** 1.0

**Base Operating System** Linux/Unix, Amazon Linux 2012.09

**Delivery Method** 64-bit Amazon Machine Image (AMI) ([Learn more](#))

**Support** [See details below](#)

**AWS Services Required** Amazon EC2, Amazon EBS

**Highlights**

- Secure: The AWS Storage Gateway securely transfers your data to AWS over SSL and stores data encrypted at rest in Amazon S3 using Advanced Encryption Standard (AES) 256, a secure symmetric-key encryption standard using 256-bit encryption keys.
- Durably backed by Amazon S3: The AWS Storage Gateway durably stores your application data by uploading it to Amazon S3. Amazon S3 stores data in multiple facilities and on multiple devices within each facility.

**Pricing Details**  
Hourly Fees  
Total hourly fees will vary by instance type and EC2 region.

For region **US East (Virginia)**

EC2 Instance Type	Software	EC2	Total*
Standard XL (m1.xlarge)	\$0.00/hr	\$0.52/hr	\$0.52/hr
High-Memory XL (m2.xlarge)	\$0.00/hr	\$0.45/hr	\$0.45/hr
High-Memory 2XL (m2.2xlarge)	\$0.00/hr	\$0.90/hr	\$0.90/hr
High-Memory 4XL (m2.4xlarge)	\$0.00/hr	\$1.80/hr	\$1.80/hr
High-CPU XL (c1.xlarge)	\$0.00/hr	\$0.66/hr	\$0.66/hr

\*EBS fees and data transfer fees not included. Assumes On-Demand EC2 pricing; prices for Reserved and Spot Instances will be lower. [See details](#)

[Learn about instance types](#)

5. 在 AMI 的启动页上，选择与 EC2 控制台一同启动选项卡。

**Launch on EC2:**

**AWS Storage Gateway**

**1-Click Launch**  
Review, modify, and launch

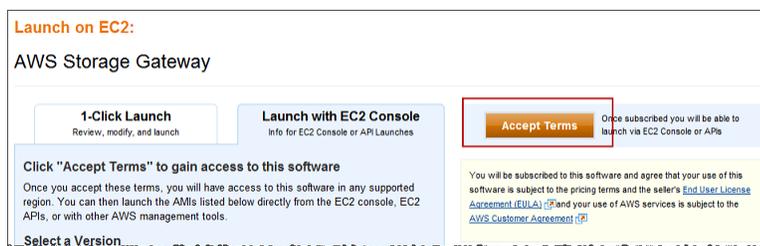
**Launch with EC2 Console**  
Info for EC2 Console or API Launches

Click "Accept Terms & Launch with 1-Click" to launch this software with the settings below

Once you accept the terms, you will have access to launch any version of this software in any supported region. For future launches, you can return to this page or launch directly from the EC2 console.

6. 如果是首次使用 AWS Storage Gateway AMI，则单击接受条款；否则，跳至下一步。

将浏览器页面保持为打开状态。片刻时间内，确认电子邮件会发送到您登录 AWS Marketplace 的账户所用的电子邮箱地址。



7. 在地区列表中，通过单击“地区”旁的与 EC2 控制台一同启动链接，选择要启动实例的地区。

Region	ID	
US East (Virginia)	ami-200c6949	<a href="#">Launch with EC2 Console</a>
US West (Oregon)	ami-4a7ae7a	<a href="#">Launch with EC2 Console</a>
US West (Northern California)	ami-ee96bbab	<a href="#">Launch with EC2 Console</a>
EU West (Ireland)	ami-6804111c	<a href="#">Launch with EC2 Console</a>
Asia Pacific (Singapore)	ami-60b0fc32	<a href="#">Launch with EC2 Console</a>
Asia Pacific (Sydney)	ami-aad84890	<a href="#">Launch with EC2 Console</a>
Asia Pacific (Tokyo)	ami-9867e499	<a href="#">Launch with EC2 Console</a>
South America (Sao Paulo)	ami-87974d9a	<a href="#">Launch with EC2 Console</a>

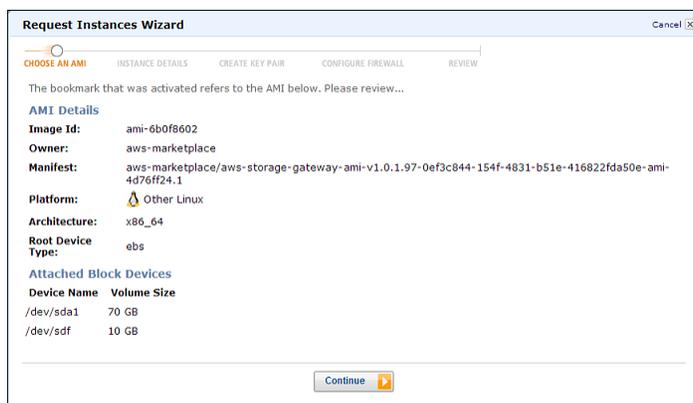
现在，将进入 Amazon EC2 控制台以进行部署 AMI 的下一步。

8. 单击左侧导航窗格中的所有实例类型链接。现在，可看到所有 Amazon EC2 实例类型。

### 步骤 2：选择实例类型

您必须指定至少一个 Standard XL (m1.xlarge) 实例类型，或者该实例不会启动。有关详细信息，请在 AWS Marketplace 中转到 [AWS Storage Gateway](#)。

1. 在选择一个实例类型页上，单击所有实例类型，然后选择某个实例类型。



2. 完成操作后，单击下一步：在页面底部配置实例详细信息。

### 步骤 3：配置实例详细信息

1. 在配置实例详细信息页上，对于实例有若干配置选项，包括要从 AMI 启动多少个实例、要在 EC2-Classic 中还是在 VPC 中启动实例。如果创建网关作测试用途，则可保留默认设置，然后转到下一步。



#### Note

如果您的 AWS 账户是默认 VPC 账户，则网络下拉列表中将为默认 VPC 网络设置，因此，您的网关将启动至默认 VPC 中。这种情况下，将无法启动至 EC2 Classic 中。



#### Note

如果您的 AWS 账户是默认 VPC 账户，则网络下拉列表中将为默认 VPC 网络设置，因此，您的网关将启动至默认 VPC 中。这种情况下，将无法启动至 EC2 Classic 中。



#### Note

如果您的 AWS 账户是默认 VPC 账户，则网络下拉列表中将为默认 VPC 子网设置，因此，您的网关将启动至默认 VPC 中。这种情况下，将无法启动至 EC2 Classic 中。如果您具有 EC2 Classic 账户，则可为您的账户创建 VPC，然后将实例启动至该 VPC 中。有关如何创建 VPC 的信息，请转到 *Amazon Virtual Private Cloud Getting Started Guide* 中的 [Amazon VPC 入门](#)。



2. 完成操作后，单击下一步：添加存储。

#### 步骤 4：添加存储

必须附加其他 EBS 卷用作缓存存储和上传缓冲区。有关更多信息，请参阅 [卷网关（网关缓存和网关存储）架构 \(p. 3\)](#)。有关调整这两个存储类型大小的详细信息，请参阅 [配置上传缓冲区的大小（网关缓存） \(p. 97\)](#)和[配置缓存存储空间的大小（网关缓存） \(p. 93\)](#)。

1. 出于测试用途，可创建两个存储卷，一个 10 GB 用于上传缓冲区，一个 20 GB 用于缓存存储。



#### Important

请勿删除任何现有 EBS 卷。



2. 单击添加新卷以添加 EBS 卷。
3. 完成操作后，单击下一步：标签实例。

#### 步骤 5：标签实例

1. 在标签实例页上，定义一个标签，其名称相对于实例要比较易记。例如，Name=MyGatewaycachedOnEC2。然后，在 Amazon EC2 控制台中所有出现 EC2 实例的地方显示此标签。



2. 完成操作后，单击下一步：配置安全组。

#### 步骤 6：配置安全组

安全组必须至少允许端口 (80) 进行激活。要允许连接网关的 iSCSI 存储目标，则必须同时允许端口 3260 的流量。您可能需要查看现有的安全组，或者在启动实例前为网关实例创建一个新的安全组。有关安全组要求的详细信息，请参阅 [Amazon EC2 网关实例配置安全组 \(p. 142\)](#)。

- 在配置安全组页上，添加以下规则。如果创建网关进行测试，则可新建一个安全组，分配组名称，然后添加这些规则。





### Caution

如果在源中指定 `0.0.0.0/0`，则您允许所有 IP 地址使用 SSH 访问您的实例。在测试环境下短时间内，这种情况尚可接受，但它对于生产环境并不安全。在生产中，请仅授权特定 IP 地址或地址范围访问您的实例。

在检查并启动页上，单击启动。

### 步骤 7：查看和启动

1. 在 7. 检查并启动页上，单击启动。
2. 在选择现有密钥对或新建密钥对窗口的下拉列表中选择相应的选项。如果新建密钥对，则先向该密钥对给出一个名称并下载该密钥对，然后再单击启动实例。



3. 在启动状态中，记下实例 ID，然后单击查看实例以打开 Amazon EC2 控制台。



4. 在 Amazon EC2 控制台中，选择该实例，然后记下公共 DNS 值。通过这个 DNS，可推断出下一步激活网关时将需要的 IP 地址。例如，如果公共 DNS 值为 `ec2-11-22-33-44.compute-1.amazonaws.com`，则 `11.22.33.44` 为 IP 地址。



### 步骤 8：激活网关

1. 现在，需要返回 AWS Storage Gateway 控制台，在在 Amazon EC2 上设置并激活网关向导中提供该 IP 地址，然后单击继续激活。



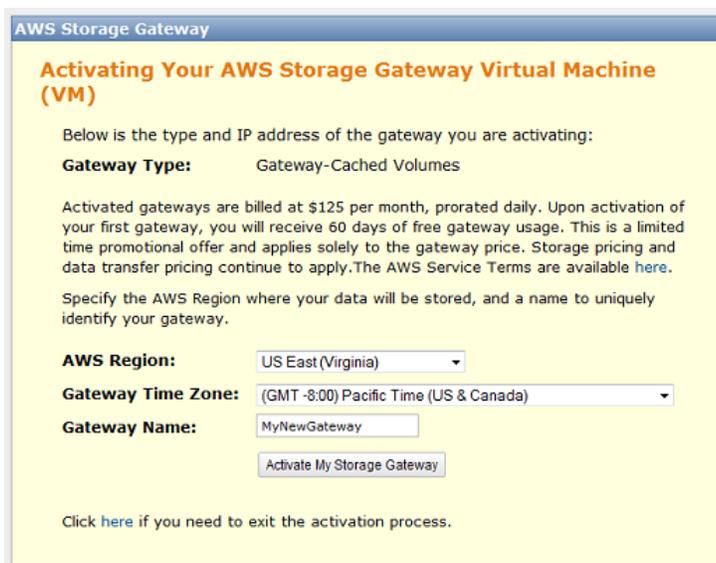
### Note

不支持通过公共 Internet 访问 Amazon EC2 Storage Gateway。无法使用 Amazon EC2 实例的弹性 IP 地址作为目标地址。



2. 在激活页上，提供所需的信息，然后单击激活我的 Storage Gateway。

注意，所选择的 AWS 地区是卷的所在地—即网关将卷数据存储在所选择的 AWS 地区。



3. 成功激活网关后，将在 AWS Storage Gateway 控制台中的卷网关部分下显示该网关。



## 管理您的 Amazon EC2 网关

### Topics

- [从实例中添加和删除 Amazon EBS 卷 \(p. 139\)](#)
- [启用和禁用 AWS Support 的访问 \(p. 141\)](#)
- [为 Amazon EC2 网关实例配置安全组 \(p. 142\)](#)
- [删除部署在 Amazon EC2 上的网关后清除资源 \(p. 142\)](#)

在本节中，我们回顾可怎样管理部署在 Amazon Elastic Compute Cloud (Amazon EC2) 上的网关。将对网关执行的管理任务包括添加和删除 Amazon EBS 卷、允许和禁止 AWS Support 访问您的网关、配置安全组以及在完成对网关的操作后清理 AWS 资源。

有关管理本地部署的网关的详细信息，请参阅[管理已激活的卷网关（网关缓存和网关存储）\(p. 166\)](#)。

### 从实例中添加和删除 Amazon EBS 卷

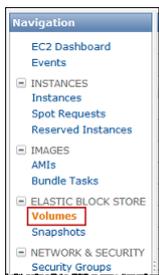
在 Amazon Elastic Compute Cloud (Amazon EC2) 上部署并激活网关（请参阅[在 Amazon EC2 上部署并激活 AWS Storage Gateway \(p. 133\)](#)）后，随着应用程序需求的变化，可能需要配置其他存储以用作上传缓冲区和缓存存储容量。或者，也可能必须减少上传缓冲区或者缓冲存储。无论是哪种情况，都将使用 Amazon Elastic Block Store (Amazon EBS) 存储，或者添加更多数据块存储，或者减少它。有关 Amazon EBS 的详细信息，请转到《Amazon EC2 用户指南》中的[Amazon Elastic Block Store \(Amazon EBS\)](#)。

在向网关添加更多存储之前，应检查如何根据缓存网关的应用程序需求调整上传缓冲区和缓存存储的大小（[配置上传缓冲区的大小（网关缓存）\(p. 97\)](#)和[配置缓存存储空间的大小（网关缓存）\(p. 93\)](#)）。配置其他本地存储后，使用它如同使用本地网关一样（相关示例请参阅[配置上传缓冲区和缓存存储空间 \(p. 142\)](#)）。对于网关缓存设置，您可以添加高达 18 TiB 的存储空间，其中高达 2 TiB 分配到上传缓冲区，16 TiB 分配到缓存卷。

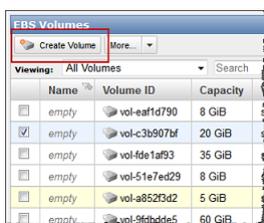
以下任务演示如何在实例上添加和删除 Amazon EBS 卷。尽管对于 Amazon EC2 实例，这是一个简单的任务，但在实例托管 AWS Storage Gateway 时，也需要多谨慎一些。这些步骤假定您已部署并激活了网关。

## 向 Amazon EC2- 托管网关添加 Amazon EBS 卷

1. 在 Amazon EC2 控制台的导航窗格中，单击卷。



2. 单击创建卷。

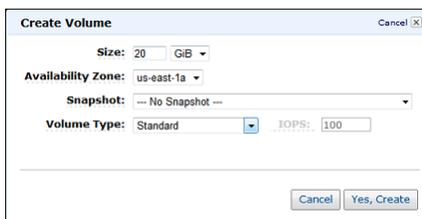


3. 在创建卷对话框中，指定卷的大小，选择可用区域，然后单击是，创建。



### Important

请在与网关相同的可用区域中创建 Amazon EBS 卷；否则，无法将其附加到网关实例。



4. 在 Amazon EC2 控制台导航窗格中的 弹性块存储 下，单击卷。
5. 查找所创建的卷，右键单击该卷，然后选择附加卷。
6. 在附加卷对话框中，指定某个卷; 容量网关实例，然后单击是，附加。

如果您收到该设备已在使用中的错误消息，请选择其他设备连接点。例如，如果已在使用 `/dev/sdg`，则尝试 `/dev/sdh`。有关更多详细，请参阅《Amazon EC2 用户指南》中的[将卷附加到实例](#)。



7. 在 Amazon EC2 控制台的导航窗格中，单击实例，然后选择网关实例以显示其详细信息。  
在实例详细信息的块存储设备部分中确认添加了新设备。



8. 在 AWS Storage Gateway 控制台中，将所添加的 Amazon EBS 卷配置为上传缓冲区或缓存存储。

## 从 Amazon EC2- 托管的网关中删除 Amazon EBS 卷

1. 按[使用 AWS Storage Gateway 控制台关停并启动网关 \(p. 210\)](#)过程中的步骤关闭网关。



### Note

关停网关前，请确保没有正在向该网关写入数据的应用程序正在使用它，并且没有快照进程。可在控制台的快照计划选项卡上检查存储卷的快照计划。有关更多信息，请参阅[编辑快照计划 \(p. 195\)](#)。

2. 在 Amazon EC2 控制台的导航窗格中，单击实例。
3. 找到运行该网关的实例。
4. 记录该实例附加的块储存设备，并找到需要移除的设备。

请注意，根设备和插拔设备都属于 X 和 Y 类，不应予以移除。

5. 在 Amazon EC2 控制台的导航窗格中，单击卷。
6. 找到要从网关中删除的卷，选中并右键单击它，然后选择强制分离。

## 启用和禁用 AWS Support 的访问

在 Amazon EC2 上部署网关后，可允许 AWS Support 访问网关以帮助解决问题。AWS Support 的访问默认为禁用。

### 允许 AWS Support 访问部署在 Amazon EC2 上的网关

1. 如果您启动实例时指定的安全组不包含运行 SSH ( 端口 22 ) 访问的规则，请添加该规则。

有关安全组以及如何添加安全组规则的详细信息，请转到《Amazon EC2 用户指南》中的[Amazon EC2 安全组](#)。



### Note

如果您要向现有安全组添加新规则，应理解所有使用安全组的实例的蕴含式。

2. 要允许 AWS Support 进行访问，请使用以下命令。

```
ssh -i IDENTITY_FILE sguser@INSTANCE_IP_ADDRESS grant-aws-support-access
```

其中 *IDENTITY\_FILE* 是在创建该实例时所用密钥对的 .pem 私钥文件，而 *INSTANCE\_IP\_ADDRESS* 是该网关的 IP 地址。

## 禁止 AWS Support 访问部署在 Amazon EC2 上的网关

- 要禁止 AWS Support 进行访问，请使用以下命令。

```
ssh -i IDENTITY_FILE sguser@INSTANCE_IP_ADDRESS revoke-aws-support-access
```

其中 *IDENTITY\_FILE* 是在创建该实例时所用密钥对的 .pem 私钥文件，而 *INSTANCE\_IP\_ADDRESS* 是该网关的 IP 地址。

## 为 Amazon EC2 网关实例配置安全组

安全组控制发往 Amazon EC2 网关实例的流量。从 AWS Marketplace 提供的 AWS Storage Gateway AMI 创建实例时，可选择两种方法启动实例。在 [在 Amazon EC2 上部署并激活 AWS Storage Gateway \(p. 133\)](#) 中，我们展示了使用 AWS Marketplace 的与 EC2 控制台一同启动功能启动实例。推荐您使用这种方法。也可使用 AWS Marketplace 中的单键启动功能启动实例。在这种情况下，将创建自动生成的安全组 `AWS Storage Gateway-1-0-AutogenByAWSMP-`。这个安全组拥有正确的端口 (80) 规则，可让您激活您的网关。有关安全组的详细信息，请转到《Amazon Elastic Compute Cloud 用户指南》中的 [安全组概念](#)。

无论您使用的是何种安全组，我们建议：

- 安全组不应该允许从外部 Internet 传入的连接；它应该只允许该装置的安全组与该装置“交谈”。如果您必须允许实例从该装置的安全组外面连接该装置，我们建议您只允许端口 3260（适用于 iSCSI）和端口 80（适用于激活）上的连接。
- 您应该仅在使用 AWS Support 进行故障诊断用途时，允许端口 22 上的访问。有关更多信息，请参阅 [启用和禁用 AWS Support 的访问 \(p. 141\)](#)。
- 如果您希望从设备安全组外的主机激活设备，就需要允许该主机的 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，可以打开端口 80、激活网关并在完成激活后关闭端口上的访问。

如果要使用 Amazon EC2 实例作为发起程序，即连接到在 Amazon EC2 上部署的网关上的 iSCSI 目标，则有两种方法。您可以将启动程序放在网关所在的同一安全组中，或者配置相应的访问，以便启动程序与网关进行通信。

## 删除部署在 Amazon EC2 上的网关后清除资源

如果使用部署在 Amazon EC2 上的网关完毕，则建议清除曾用于该网关的 AWS 资源，尤其是 Amazon EC2 实例和任何 Amazon EBS 卷。完成此操作有助于避免产生非故意的使用费用。我们建议您采取下列操作删除您的网关和清理相关的资源：

- 在 AWS Storage Gateway 控制台中，删除该网关，如 [使用 AWS Storage Gateway 控制台删除网关 \(p. 217\)](#) 所示。
- 如果打算再次使用该网关，则在 Amazon EC2 控制台中，停止该实例。如果您不打算再次使用该实例，请终止该实例。在终止实例前，如果您打算删除卷，可记录该实例上说附加的块储存设备及其标识符。
- 如果不打算再次使用曾附加到该实例的任何 Amazon EBS 卷，则在 Amazon EC2 控制台中，删除这些卷。

## 配置上传缓冲区和缓存存储空间

### Topics

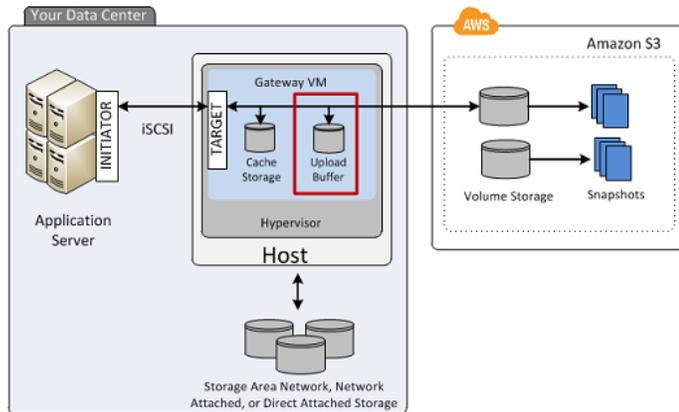
- [配置上传缓冲区（网关缓存）\(p. 143\)](#)
- [配置缓存存储空间（网关缓存）\(p. 145\)](#)
- [配置上传缓冲区（网关存储）\(p. 146\)](#)

为提供场内环境和 AWS 存储基础设施之间的无缝融合，每个网关都需要本地存储空间，用来缓冲和缓存数据。本部分讨论如何为网关配置本地磁盘存储空间。对于网关缓存卷的设置，您将本地磁盘存储空间配置为上传缓冲区和缓存存储空间。对于网关存储卷的设置，您将本地磁盘存储空间配置为上传缓冲区。有关可为网关选择的不同架构的详细信息，请参阅 [AWS Storage Gateway 的运行原理（架构）](#) (p. 3)。

创建卷供应用程序使用前，需要配置上传缓冲区和缓存存储空间。通过为网关 VM 配置的本地磁盘创建上传缓冲区和缓存存储（请参阅 [AWS Storage Gateway VM 配置本地磁盘存储](#) (p. 90)）。

## 配置上传缓冲区（网关缓存）

本部分描述如何配置网关的上传缓冲区。您的网关在将卷数据上传到 AWS 前，需要上传缓冲区临时缓冲您的卷数据。下图在 AWS Storage Gateway 网关缓存架构的大图中突出显示了上传缓冲区（请参阅 [AWS Storage Gateway 的运行原理（架构）](#) (p. 3)）。



您需要确保网关 VM 上有可供使用的本地磁盘，才能配置上传缓冲区。有关向 VM 添加更多本地磁盘的说明，请参阅 [预配置本地磁盘（网关缓存）](#) (p. 92)。

如需将本地磁盘配置为网关的上传缓冲区

1. 在 AWS Storage Gateway 控制台中：

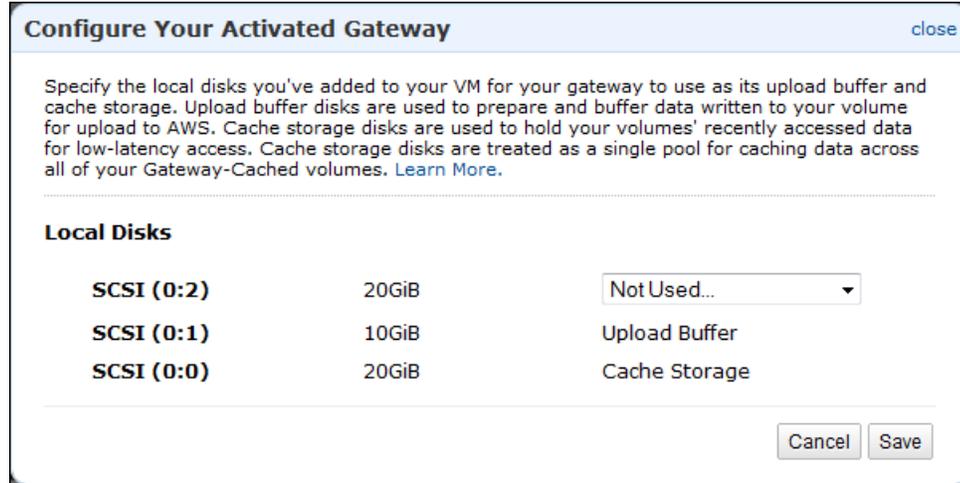
如果...	那么...
您正要首次在网关上配置卷。	您将自动转入配置已激活的网关向导。前往步骤 2。
您的网关已有定义的卷。	打开配置已激活的网关向导。 <ol style="list-style-type: none"> <li>a. 在导航窗格中单击该网关。</li> <li>b. 选择网关选项卡。</li> <li>c. 单击配置本地存储。</li> </ol>

The screenshot shows the AWS Management Console for a Storage Gateway named 'MyNewGateway'. The 'Gateway' tab is selected. There are three buttons: 'Shut Down', 'Delete Gateway', and 'Configure Local Storage'. The 'Configure Local Storage' button is highlighted with a red rectangular box. Below the buttons, the gateway's name and ID are displayed: 'Name: MyNewGateway (edit name)' and 'Gateway ID: sgw-37BE5B5E'.

- 在配置已激活的网关向导中，确认有本地磁盘可配置为上传缓冲区。

向导显示您的本地 VM 上的可用磁盘列表。如果没有本地磁盘可用，您必须向网关 VM 添加本地磁盘。有关更多信息，请参阅 [为上传缓冲区添加虚拟磁盘（网关缓存）](#) (p. 98)。

在下例中，有 SCSI (0:2) 磁盘可配置为上传缓冲区。



Local Disks		
SCSI (0:2)	20GiB	Not Used...
SCSI (0:1)	10GiB	Upload Buffer
SCSI (0:0)	20GiB	Cache Storage

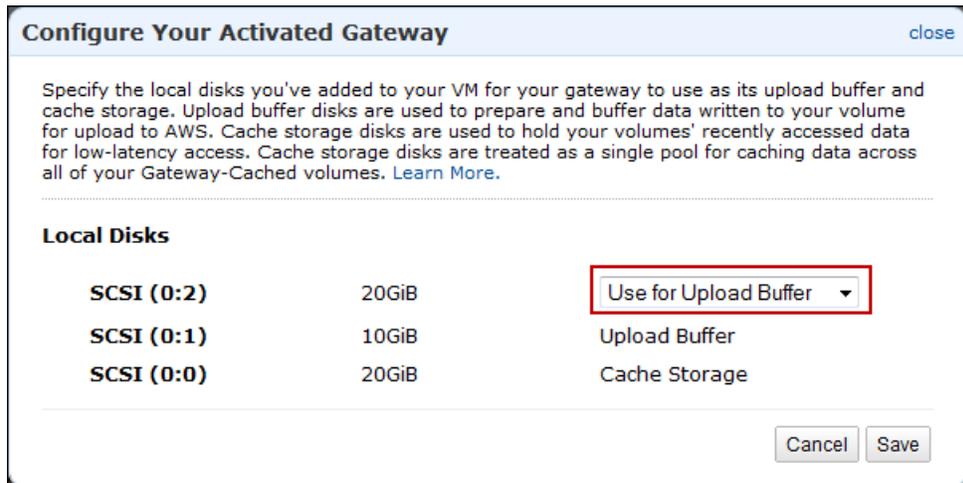
- 如果有磁盘可供配置为上传缓冲区，请配置网关以使用这些磁盘。

- 选择您希望作为上传缓冲区分配给网关的磁盘旁边的下拉列表。



**Important**

将磁盘配置为上传缓冲区后，磁盘上任何先前的数据都会丢失。



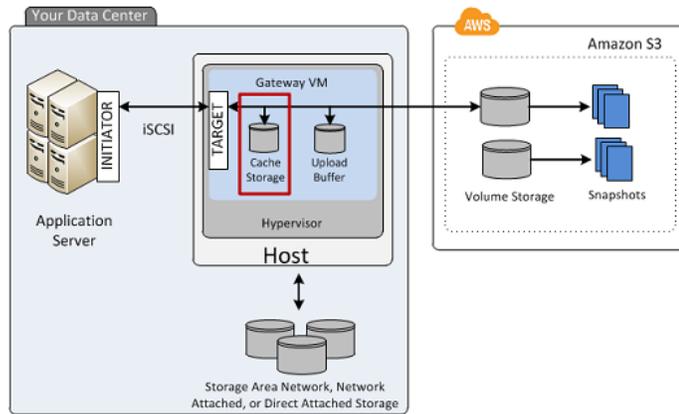
Local Disks		
SCSI (0:2)	20GiB	Use for Upload Buffer
SCSI (0:1)	10GiB	Upload Buffer
SCSI (0:0)	20GiB	Cache Storage

- 单击保存。

此操作将磁盘分配为网关的上传缓冲区。

## 配置缓存存储空间 ( 网关缓存 )

本部分描述了如何配置网关的缓存存储空间。您的网关需要缓存存储空间来缓存最近访问的应用程序数据。下图在 AWS Storage Gateway 网关缓存架构的大图中突出显示了缓存存储 ( 请参阅 [AWS Storage Gateway 的运行原理 \( 架构 \) \(p. 3\)](#) )。



如需将本地磁盘配置为网关的缓存存储空间

1. 在 AWS Storage Gateway 控制台中：

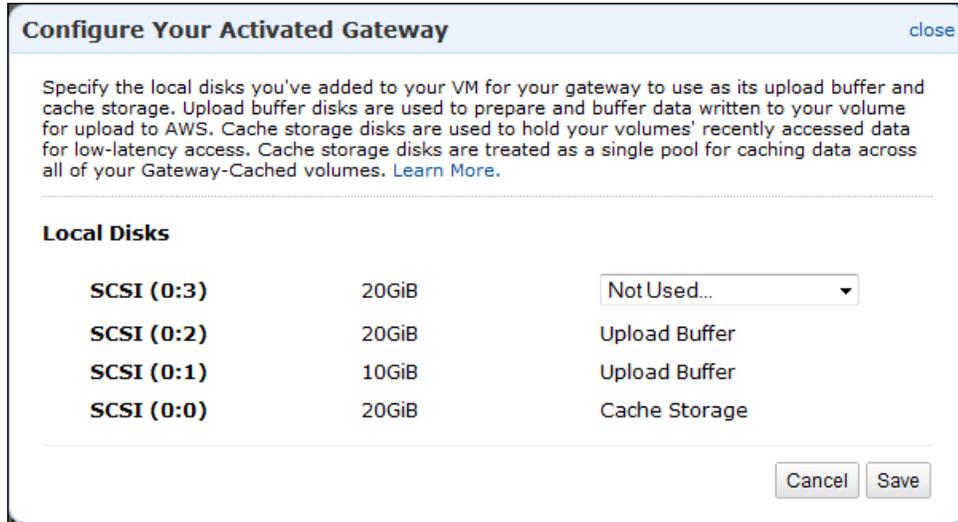
如果...	那么...
您正要首次在网关上配置卷。	您将自动转入配置已激活的网关向导。前往步骤 2。
您的网关已有定义的卷。	打开配置已激活的网关向导。 <ol style="list-style-type: none"> <li>在导航窗格中单击该网关。</li> <li>选择网关选项卡。</li> <li>单击配置本地存储。</li> </ol>

The screenshot shows the AWS Storage Gateway console for a gateway named 'MyNewGateway'. The 'Gateway' tab is selected. In the top navigation bar, the 'Configure Local Storage' button is highlighted with a red box. Below the navigation bar, the gateway's Name and Gateway ID are displayed.

2. 在配置已激活的网关向导中，确认有本地磁盘可配置为缓存存储。

向导显示您的本地 VM 上的可用磁盘列表。如果没有本地磁盘可供配置为缓存存储空间，您就必须向网关 VM 添加本地磁盘。有关更多信息，请参阅 [为缓存存储空间添加虚拟磁盘 \( 网关缓存 \) \(p. 93\)](#)。

在下例中，有 SCSI (0:3) 磁盘可配置为缓存存储。



3. 如果有磁盘可供配置为缓存存储空间，请配置网关以使用这些磁盘。
  - a. 选择您希望作为缓冲存储分配给网关的磁盘旁边的下拉列表。



**Important**

将磁盘配置为缓存存储空间后，磁盘上任何先前的数据都会丢失。

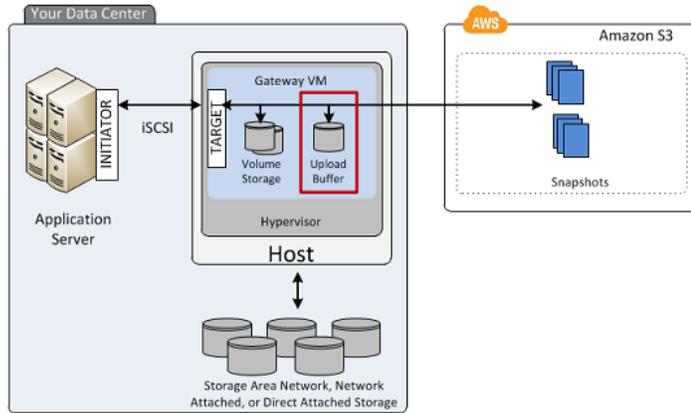


- b. 单击保存。

此操作将磁盘分配为网关的缓存存储空间。

## 配置上传缓冲区（网关存储）

本部分描述如何配置网关的上传缓冲区。您的网关在将卷数据上传到 AWS 前，需要上传缓冲区临时缓冲您的卷数据。下图在 AWS Storage Gateway 网关存储架构的大图中突出显示了上传缓冲区（请参阅 [AWS Storage Gateway 的运行原理（架构）](#)（p. 3））。



如需将本地磁盘配置为网关的上传缓冲区

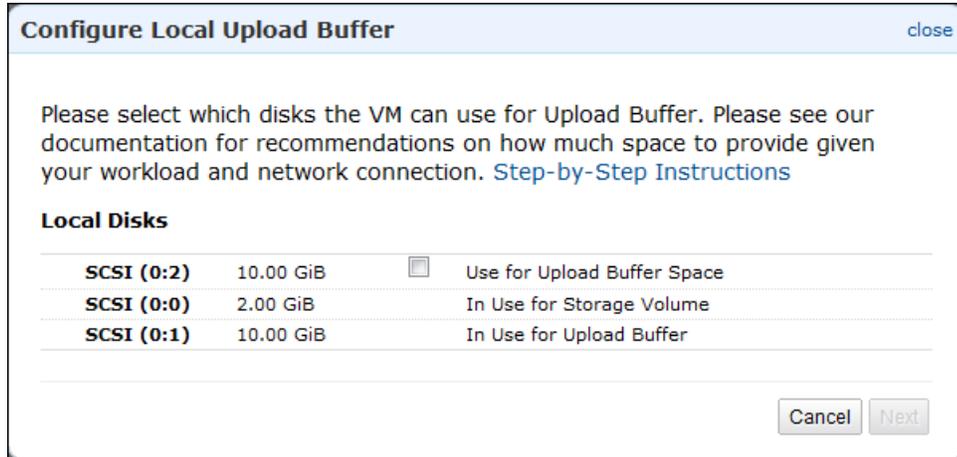
1. 在 AWS Storage Gateway 控制台中：

如果...	那么...
您正要首次在网关上配置卷。	您将自动转入配置已激活的网关向导。前往步骤 2。
您的网关已有定义的卷。	<p>打开配置已激活的网关向导。</p> <ol style="list-style-type: none"> <li>a. 在导航窗格中单击该网关。</li> <li>b. 选择网关选项卡。</li> <li>c. 单击配置本地存储。</li> </ol>

2. 在配置本地上传缓冲区向导中，确认有本地磁盘可配置为上传缓冲区。

向导显示您的本地 VM 上的可用磁盘列表。如果没有本地磁盘可用，您必须向网关 VM 添加本地磁盘。有关更多信息，请参阅 [为上传缓冲区添加虚拟磁盘（网关存储）](#) (p. 105)。

在下示例中，有 SCSI (0:2) 磁盘可配置为上传缓冲区空间。

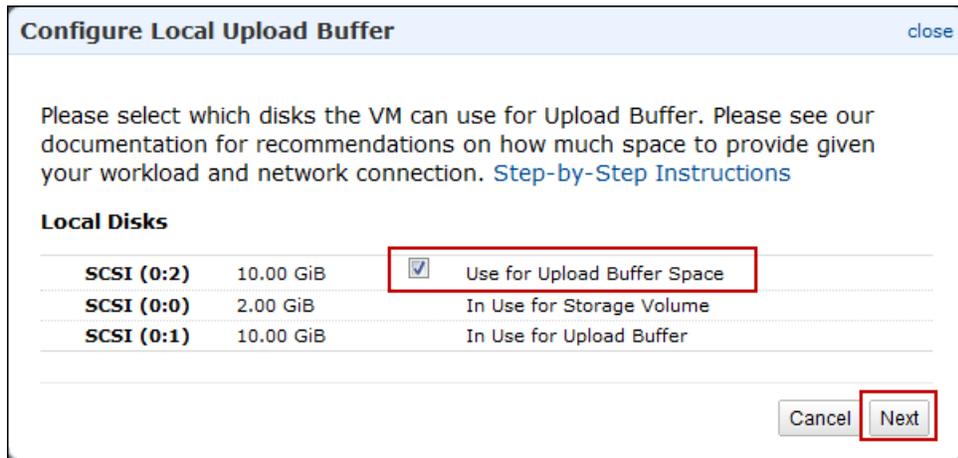


3. 如果有磁盘可供配置为上传缓冲区，请配置网关以使用这些磁盘。
  - a. 选中要分配给网关作为上传缓冲区的磁盘旁的复选框，然后单击下一步。仅在选择至少一个磁盘后，才会启用下一步按钮。

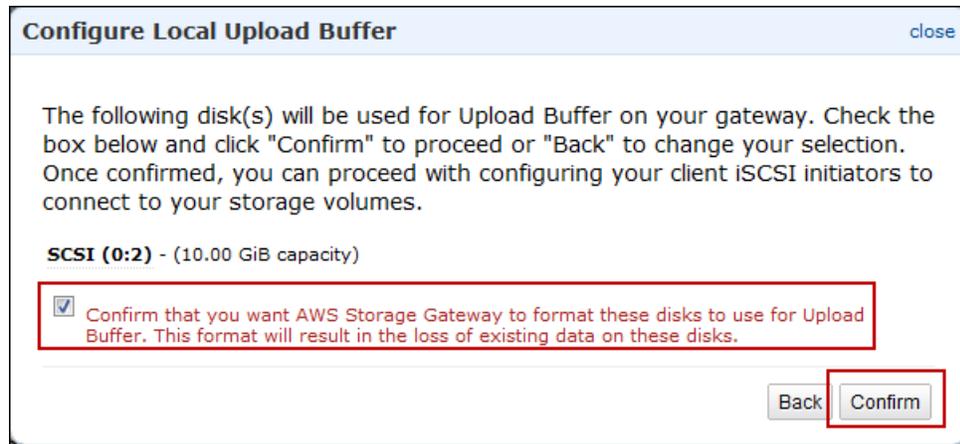


**Important**

将磁盘配置为上传缓冲区后，磁盘上任何先前的数据都会丢失。



- b. 在确认对话框中，阅读并选中确认复选框，然后单击确认。  
此操作将磁盘分配为网关的上传缓冲区。



## 创建存储卷

### Topics

- [创建存储卷 \( 网关缓存 \)](#) (p. 149)
- [创建存储卷 \( 网关存储 \)](#) (p. 151)

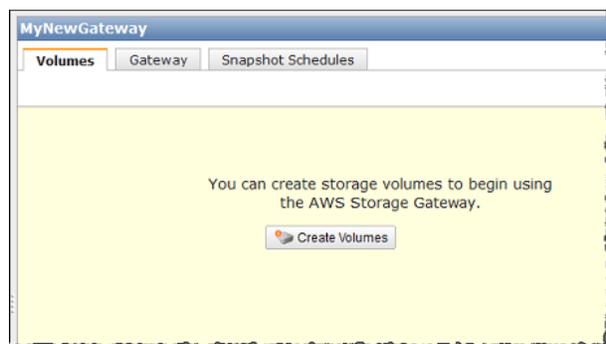
您的应用程序数据存储存储在存储卷中。在本部分中，您将了解将存储卷创建为网关缓存卷架构或网关存储卷架构的过程。有关不同 AWS Storage Gateway 架构的详细信息，请参阅 [AWS Storage Gateway 的运行原理 \( 架构 \)](#) (p. 3)。

## 创建存储卷 ( 网关缓存 )

可使用 AWS Storage Gateway API ( 请参阅 [CreateCachediSCSIVolume](#) ) 或 AWS Storage Gateway 控制台创建网关缓存卷。下面的任务展示了使用控制台创建卷的过程。该任务假定您已部署并激活了网关。

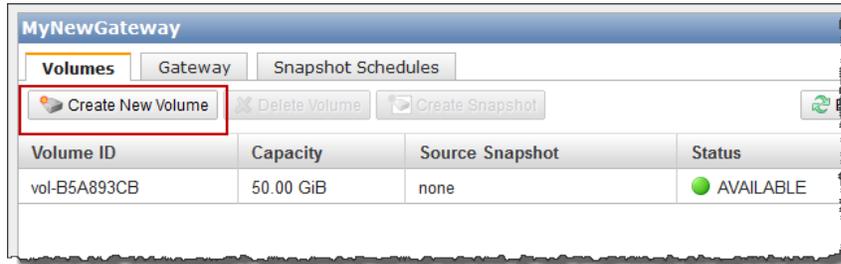
如需使用控制台创建存储卷

1. 在 AWS Storage Gateway 控制台的导航窗格中，选择该网关。
2. 如果网关已激活但没有存储卷。
  - a. 单击创建卷。

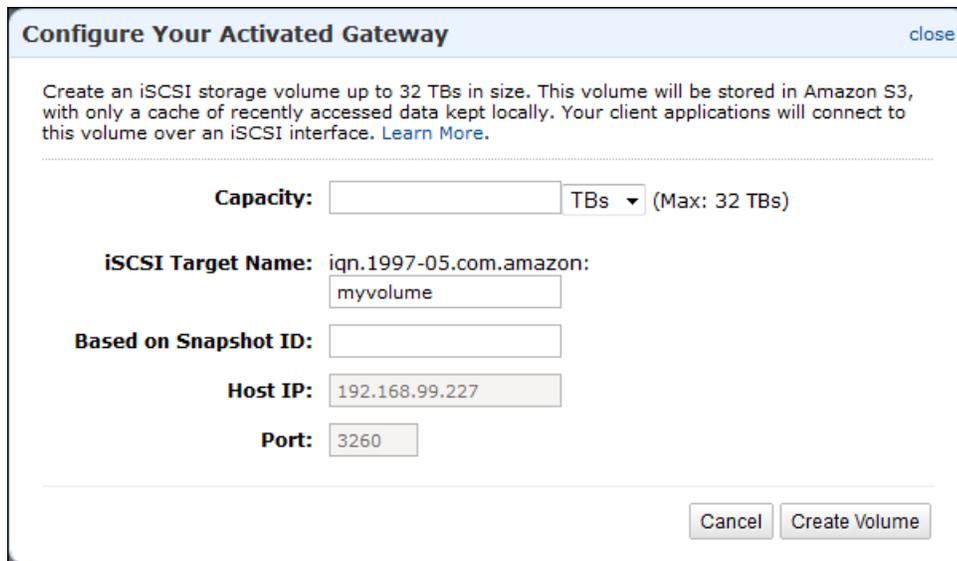


- b. 按“入门”一节中[在本地磁盘上创建缓存存储和上传缓冲区并配置可选警报](#) (p. 63) 中的步骤指定缓存存储和上传缓冲区。

3. 如果网关已有一个或多个存储卷。
  - 在卷选项卡中，单击创建新卷。



4. 在配置已激活的网关向导中，配置该卷。



- a. 在容量字段中，输入要创建的存储卷的大小。



**Note**

不支持存储卷创建后的调整大小。稍后如需更改卷的大小，您必须创建该卷的快照，然后从该快照创建新缓存卷。有关更多信息，请参阅 [管理存储卷（网关缓存）](#) (p. 171)。

- b. 在容量字段旁的大小下拉列表中，选择该卷的相应大小，单位为 GiB 或 TiB。
- c. 在 iSCSI 目标名称字段中输入一个名称。

目标名称可包含小写字母、数字句点 (.) 和连词符 (-)。经过发现后，在 iSCSI Microsoft 发起程序用户界面的目标选项卡中，此目标名称显示为 iSCSI 目标节点名称。例如，名称 target1 将显示为 iqn.1997-05.com.amazon:target1。确保目标名称在 SAN 网络内具有全局唯一性。

- d. 如果要通过快照创建卷，则指定基于快照 ID 字段。

您可以指定现有 AWS Storage Gateway 或此前创建的 Amazon EBS 快照的 ID。在此情况下，网关仅在首次访问数据时创建存储卷并将数据下载到本地缓存卷。要了解如何查找要使用的快照，请参阅 [查找快照](#) (p. 188)。

- e. 主机 IP 字段中显示的 IP 地址显示您的网关 IP 地址。

如果您已配置了有多个网络接口卡 (NIC) 的本地网关主机，可指定希望将哪一 IP 地址用于该存储卷。

- f. 注意，端口字段显示用于映射 iSCSI 目标的端口。

AWS Storage Gateway 仅支持端口 3260。

- g. 单击创建卷。

此操作创建存储卷，并且将您的磁盘作为 iSCSI 目标，供应用程序连接并存储数据。有关连接到 iSCSI 目标的信息，请参阅[配置应用程序对存储卷的访问](#) (p. 153)。



#### Note

如果您想要该卷的快照，可以拍摄临时快照，也可以为该卷设置快照计划。有关更多信息，请参阅[编辑快照计划](#) (p. 195)。

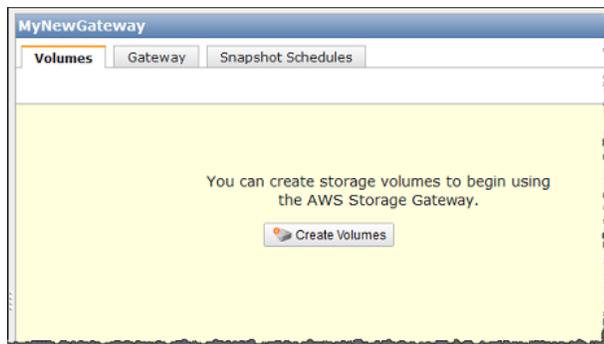
## 创建存储卷 ( 网关存储 )

可使用 AWS Storage Gateway API ( 请参阅 [CreateStorediSCSIVolume](#) ) 或 AWS Storage Gateway 控制台创建网关存储卷。下面的任务展示了使用控制台创建卷的过程。该任务假定您已部署并激活了网关。另外，该任务假定至少有一个本地预配置的网关磁盘，该磁盘尚未使用并且将配置为网关存储卷。要为应用程序存储配置本地磁盘，请参阅[预配置本地磁盘 \( 网关存储 \)](#) (p. 100)。

如需使用控制台创建存储卷

1. 在 AWS Storage Gateway 控制台的导航窗格中，选择该网关。

控制台显示网关专属信息。如果该网关已激活，但没有存储卷，则控制台显示以下页，其中含有创建卷按钮。



2. 单击创建新卷。

**Create Storage Volume** close

**CREATE VOLUMES** **CONFIGURE LOCAL UPLOAD BUFFER**

Create a storage volume for each disk in your VM on which you plan to store application data. Your client applications will connect to these volumes over an iSCSI interface. A default snapshot schedule will be set up for each volume you create. [Step-by-Step Instructions](#).

**Disk:** select..  Preserve existing data

**iSCSI Target Name:** iqn.1997-05.com.amazon:  
myvolume

**Based on Snapshot ID:**

**Size:** --

**Host IP:** 192.168.99.183

**Port:** 3260

Cancel Create Volume

3. 在创建存储卷向导中，输入以下信息：

- a. 在磁盘下拉列表中，选择为该网关配置的本地虚拟磁盘。

有关配置磁盘的详细信息，请参阅为 [AWS Storage Gateway VM 配置本地磁盘存储 \(p. 90\)](#)。

- b. 如果要将数据保留在磁盘上，则选中保留现有数据复选框。

AWS Storage Gateway 在创建后即自举您的卷，保存卷的现有数据并将其上传到 AWS。

- c. 在 iSCSI 目标名称字段中输入一个名称。

目标名称可包含小写字母、数字句点 (.) 和连字符 (-)。经过发现后，在 iSCSI Microsoft 发起程序用户界面的目标选项卡中，此目标名称显示为 iSCSI 目标节点名称。例如，名称 target1 将显示为 iqn.1997-05.com.amazon:target1。确保目标名称在 SAN 网络内具有全局唯一性。

- d. 如果要通过快照创建卷，则指定基于快照 ID 字段。

可指定现有 AWS Storage Gateway 或以前创建的 Amazon EBS 快照的 ID。如果您希望还原另一存储卷的快照，这是一个有用的场景。在这种情况下，网关会创建存储卷并将您现有的快照数据下载到该卷。不过，在您的应用程序开始访问卷及其所有数据前，无需等到所有的数据从 Amazon S3 传输到您的卷。要详细了解快照，请参阅 [使用快照 \(p. 187\)](#)。

通过现有快照创建卷时，将不保留磁盘上的任何现有数据，因此必须取消选中保留现有数据复选框。

- e. 主机 IP 字段中显示的 IP 地址显示您的网关 IP 地址。

如果您已配置了有多个网络接口卡 (NIC) 的本地网关主机，可指定希望将哪一 IP 地址用于该存储卷。

- f. 注意，端口字段显示用于映射 iSCSI 目标的端口。

AWS Storage Gateway 仅支持端口 3260。

- g. 单击创建卷。

此操作创建存储卷，并且将您的磁盘作为 iSCSI 目标，供应用程序连接并存储数据。

单击该按钮也会为您的新卷创建快照计划。默认情况下，AWS Storage Gateway 每天拍摄一次快照。您可以修改每天拍摄快照的时间以及频率（每 1、2、4、8、12 或 24 小时）。有关更多信息，请参阅 [编辑快照计划 \(p. 195\)](#)。



#### Note

快照为增量压缩式备份。对于给定的卷，网关仅保存自上次快照拍摄以来发生变化的数据块。这样可以用于备份的存储空间减少到最低限度。如需确保网关能够跟上传入写入的速率，请注意至少每天拍摄一次快照。

## 配置应用程序对存储卷的访问

### Topics

- [从 Windows 客户端连接到您的存储卷 \(p. 154\)](#)
- [从 Red Hat 连接到您的存储卷 \(p. 156\)](#)
- [为存储卷配置 CHAP 验证 \(p. 159\)](#)

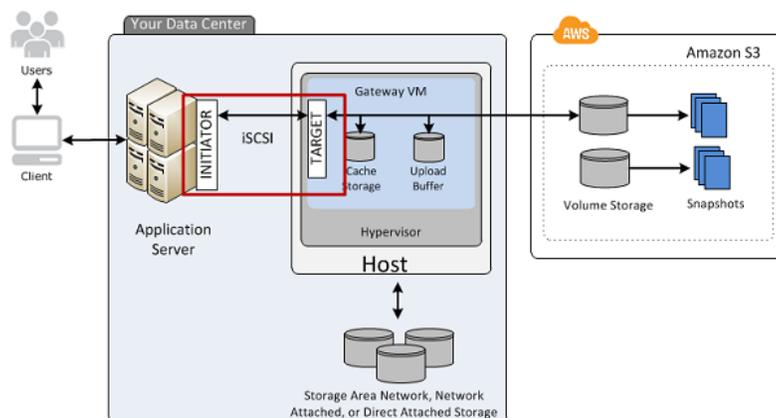
向 VM 添加本地磁盘并创建存储卷后，网关将这些磁盘作为 iSCSI 目标公布。您的客户端应用程序连接到这些 iSCSI 目标以存储数据。对每个 iSCSI 目标仅连接一个应用程序。AWS Storage Gateway 支持可让您连接到这些目标的 Red Hat 和 Windows 客户端 iSCSI 启动程序。要详细了解向 VM 添加本地磁盘，请参阅 [AWS Storage Gateway VM 配置本地磁盘存储 \(p. 90\)](#)。要详细了解创建存储卷，请参阅 [管理 AWS Storage Gateway 中的存储卷 \(p. 167\)](#)。



#### Note

如需连接到存储卷目标，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，那么您的存储卷的状态就会显示为 UPLOAD BUFFER NOT CONFIGURED。要为存储卷网关配置上传缓冲区，请参阅 [如需使用控制台为网关配置上传缓冲区 \(p. 184\)](#)。要为缓存卷网关配置上传缓冲区，请参阅 [如需使用控制台为您的网关将本地磁盘配置为上传缓冲区 \(p. 179\)](#)。

下图在 AWS Storage Gateway 架构的大图中突出显示了 iSCSI 目标（请参阅 [AWS Storage Gateway 的运行原理（架构） \(p. 3\)](#)）。



Internet 小型计算机系统接口 (iSCSI) 是基于 Internet 协议 (IP) 的存储联网标准，用来启动和管理基于 IP 的存储设备和客户端之间的连接。

下表列出用于描述连接和相关组件的一些 iSCSI 术语。

术语	说明
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。启动程序可在软件或硬件中实施。AWS 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。每个存储卷均公布为一个 iSCSI 目标。仅对每个 iSCSI 目标连接一个 iSCSI 启动程序。
Microsoft iSCSI 启动程序	Windows 计算机上的软件程序，可让您使用主计算机的以太网网络适配卡将客户端计算机（例如运行您希望将其数据写入网关的应用程序的计算机）来连接到外部基于 iSCSI 数组（即网关）。Microsoft iSCSI 启动程序在软件中实施。Microsoft iSCSI 启动程序已安装在 Windows Server 2008 R2、Windows 7、Windows Server 2008 和 Windows Vista 上。在上述操作系统中，您不需要安装该启动程序。
Red Hat iSCSI 启动程序	包含 iscsi /启动程序/实用程序的资源包管理器 (RPM) 包为您提供实施在适用于 Red Hat 的软件中的 iSCSI 启动程序。该包含有用于 iSCSI 协议的服务器守护进程。

您可以从 Windows 或 Red Hat 客户端连接到存储卷。您可以针对两种客户端类型有选择地配置质询握手身份验证协议 (CHAP)。

如需...	请参见...
从 Windows 连接到您的存储卷。	<a href="#">步骤 3：访问您的 AWS Storage Gateway 卷 (p. 72)</a> 入门教程中的
从 Red Hat Linux 连接到您的存储卷。	<a href="#">从 Red Hat 连接到您的存储卷 (p. 156)</a>
为 Windows 和 Red Hat Linux 配置 CHAP 验证。	<a href="#">为存储卷配置 CHAP 验证 (p. 159)</a>

## 从 Windows 客户端连接到您的存储卷

使用 Windows 客户端时，您用 Microsoft iSCSI 启动程序连接到您的网关存储卷。

本练习说明如何连接到存储卷。有关更多信息，请参阅 [步骤 3：访问您的 AWS Storage Gateway 卷 \(p. 72\)](#)。

### 自定义您的 Windows iSCSI 设置

设置您的启动程序后，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。通过提高下列步骤中所示的超时值，您可以改善应用程序处理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性能。



#### Note

修改注册表前，您应该制作一份备份副本。有关在使用注册表时需要遵循的制作备份副本及其他最佳操作的信息，请参阅 *Windows Server TechCenter* 中的 [注册表最佳操作](#)。

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. 导航到设备类别全局唯一标识符 (GUID) 密钥，其中包含 iSCSI 控制器设置。



**Warning**

确保处于 CurrentControlSet 子项内，而非 ControlSet001 或 ControlSet002 等其他控制集内。

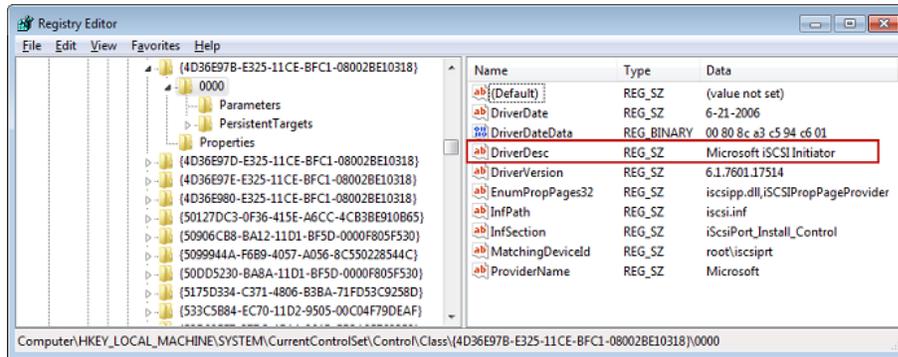
```
HK_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFCl-08002BE10318}
```

- c. 找到 Microsoft iSCSI 启动程序的子项。

将按 0000 或 00001 等四位数字表示该项。

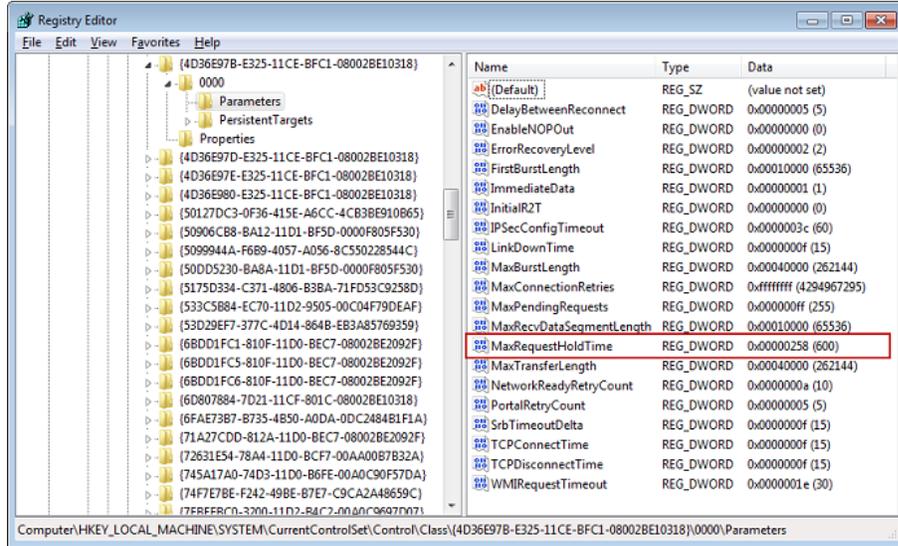
```
HK_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFCl-08002BE10318}\<Instance Number>
```

根据计算机上所装硬件的不同，Microsoft iSCSI 发起程序可能不是子项 0000。可通过确认字符串 DriverDesc 具有下列所示的 Microsoft iSCSI Initiator 值，确保已选择正确的子项。



- d. 单击参数子项以显示 iSCSI 设置。  
e. 右键单击 MaxRequestHoldTime DWORD ( 32 位 ) 值，选择“修改”，然后将其值改为 600。

该值表示 600 秒的保持时间。下列显示值为 600 的 MaxRequestHoldTime 字符串值。

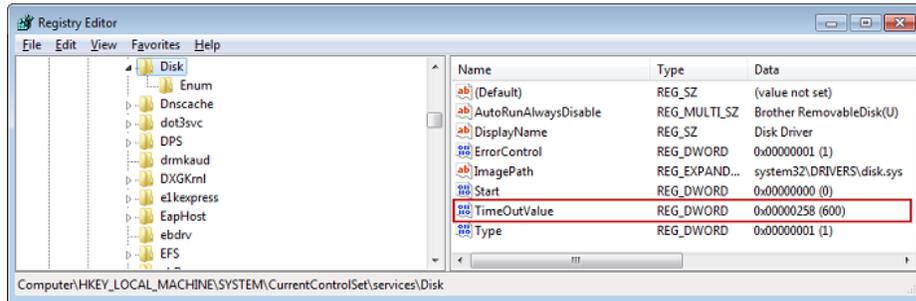


2. 提高磁盘超时值。

- a. 启动注册表编辑器 (Regedit.exe)。
- b. 导航到 CurrentControlSet 的服务子项中的磁盘子项。

HK\_Local\_Machine\SYSTEM\CurrentControlSet\Services\Disk

- c. 右键单击 TimeoutValue DWORD ( 32 位 ) 值，单击“修改”，然后将其值改为 600。  
该值表示 600 秒的超时值。



3. 重启系统以确保新配置的值生效。

重启前，您必须确保对存储卷的所有写入均刷新。要这样做，请在重启前将任何映射的存储卷磁盘脱机。

## 从 Red Hat 连接到您的存储卷

使用 Red Hat Linux 时，您用 iscsi /启动程序/实用程序 RPM 包连接到您的网关存储卷。

如需将 Linux 客户端连接到存储卷

1. 如果 `iscsi` /启动程序/实用程序 RPM 包尚未安装到您的客户端，请安装。

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. 使用下面的命令验证 iSCSI 守护进程正在运行。

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

- b. 如果 `status` 命令未返回 `running` 状态，则使用以下命令启动守护程序。

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

3. 发现针对网关定义的存储卷目标。

使用下面的发现命令列出网关目标。

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

将上一命令中的 `GATEWAY_IP` 变量替换为网关的 IP 地址。可在 AWS Storage Gateway 控制台卷的 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。

```
GATEWAY_IP:3260, 1 iqn.1997-05.com.amazon:myvolume
```

您的 iSCSI 限定名称 (IQN) 与以上所示不同，因为每个组织的 IQN 值是不同的。目标名称是您创建存储卷时指定的名称。在 AWS Storage Gateway 控制台中选择存储卷后，还可在 iSCSI 目标信息属性窗格中找到此目标名称。

4. 连接到目标。

您需要在连接命令中指定正确的 `GATEWAY_IP` 和 IQN。



#### Warning

对于部署在 Amazon EC2 实例上的 Amazon Storage Gateway，不支持通过公共 Internet 访问网关。无法使用 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:myvolume --portal GATEWAY_IP:3260,1 --login
```

5. 验证卷是否已连接到客户机 (启动程序)。

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

设置发起程序后，我们强烈建议您按[自定义您的 Linux iSCSI 设置 \(p. 158\)](#)中讨论的方式自定义 iSCSI 设置。

## 自定义您的 Linux iSCSI 设置

设置您的启动程序后，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。通过按如下所示提高 iSCSI 超时值，您可以改善应用程序处理需要较长时间的写入以及网络中断等暂时问题的性能。

### 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

必须在发现网关前进行 `iscsid.conf` 的设置。如果您已发现网关并且/或者登录到目标，您可以使用下面的命令从发现数据库删除该项，然后重新发现/登录，从而使新设置生效。

```
iscsiadm -m discoverydb -t sendtargets -p gateway_ip:3260 -o delete
```

2. 提高磁盘超时值。
  - a. 打开 `/etc/udev/rules.d/50-udev.rules` 文件，然后找到下面这行。

```
ACTION=="add", SUBSYSTEM=="scsi", SYSFS{type}=="0|7|14", \ RUN+="/bin/sh
-c 'echo [timeout] > /sys$$DEVPATH/timeout'
```

- b. 将 `timeout` 值设为 600。

该值表示 600 秒的超时值。

3. 重启系统以确保新配置的值生效。

重启前，您必须确保对存储卷的所有写入均刷新。要这样做，请在重启前卸载存储卷。

## 为存储卷配置 CHAP 验证

AWS Storage Gateway 支持通过 CHAP (质询握手身份验证协议) 在网关和 iSCSI 启动程序间进行身份验证。CHAP 通过定期验证 iSCSI 发起程序的身份是否具有访问存储卷目标的权限, 预防反演攻击。如需建立 CHAP, 您必须在 AWS Storage Gateway 控制台中和用来连接到该目标的 iSCSI 启动程序中进行配置。

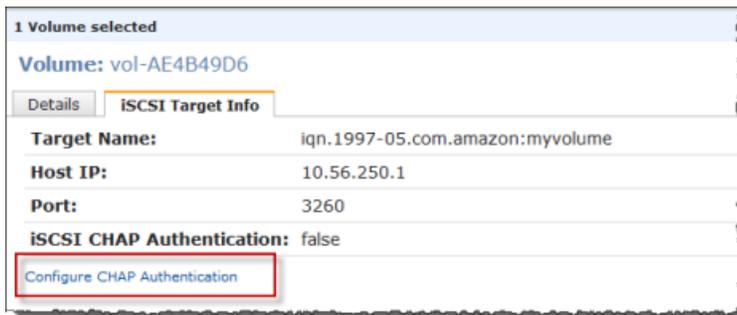
本部分讨论双向 CHAP, 即启动程序验证目标身份的同时, 目标也验证启动程序。如需使用双向 CHAP, 您需要执行两个步骤:

- 首先, 在 AWS Storage Gateway 控制台中配置 CHAP。
  - 如需在 [AWS Storage Gateway 控制台中配置 CHAP \(p. 159\)](#)
- 其次, 在客户端启动程序软件中, 完成 CHAP 设置。
  - 在 [Windows 客户端上配置双向 CHAP。 \(p. 160\)](#)
  - 如需在 [Red Hat Linux 客户端上配置双向 CHAP \(p. 165\)](#)

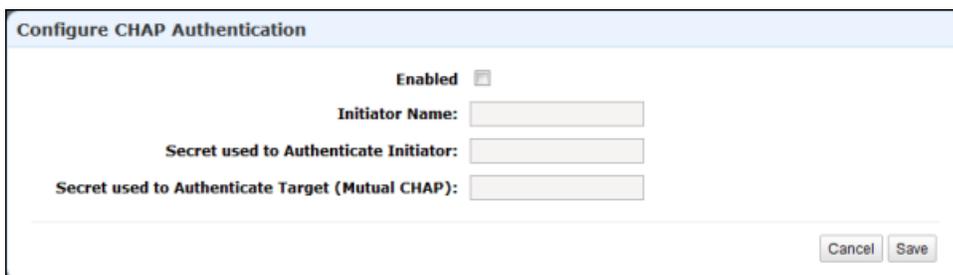
如需在 AWS Storage Gateway 控制台中配置 CHAP

在本步骤中, 您指定两个用来读取和写入存储卷的私有密钥。这两个密钥也用来在本步骤中配置客户端启动程序。

1. 转到要为其配置 CHAP 的卷的 iSCSI 目标信息选项卡。
2. 单击配置 CHAP 身份验证链接。



3. 在配置 CHAP 身份验证对话框中配置 CHAP。



- a. 选中已启用框。
- b. 指定发起程序名称。

启动程序名称可利用 iSCSI 启动程序软件找到。例如, 对于 Windows 客户端, 该名称为 iSCSI 发起程序的配置选项卡中的值。有关更多信息, 请参阅 [在 Windows 客户端上配置双向 CHAP。 \(p. 160\)](#)。



**Note**

如需更改启动程序名称，您必须先禁用 CHAP，在 iSCSI 启动程序软件中更改启动程序名称，然后使用新名称启用 CHAP。

- c. 指定用于验证发起程序身份的密钥字段。

该私有密钥的长度至少为 12 个字符。启动程序（例如 Windows 客户端）要加入与目标的 CHAP 中，必须知道该私有密钥。

- d. 在用于验证目标身份的私有密钥(双向 CHAP) 字段中指定私有密钥。

该私有密钥的长度至少为 12 个字符。启动程序要加入与目标的 CHAP 中，必须知道该私有密钥。



**Note**

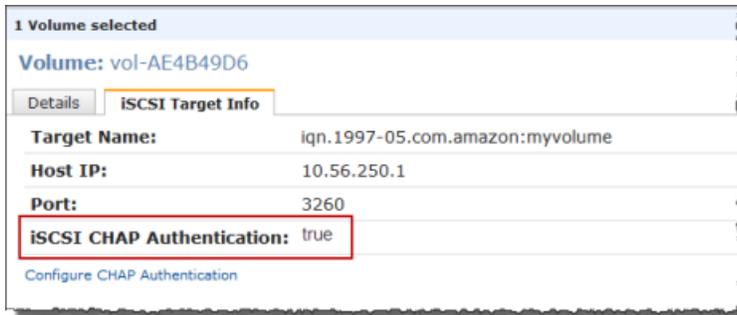
用来验证目标身份的私有密钥必须不同于用来验证启动程序的私有密钥。

- e. 单击保存。
- f. 在确认对话框中单击关闭。

iSCSI 目标信息选项卡指示使用 CHAP 身份验证。

- 4. 确认 CHAP 已启用。

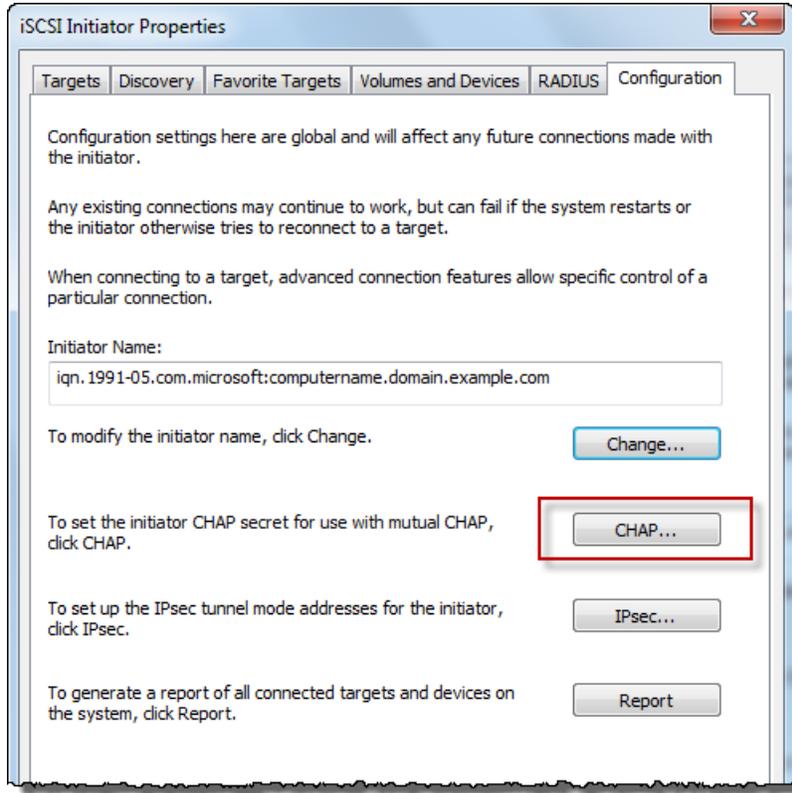
iSCSI 目标信息选项卡指示使用 CHAP 身份验证。



在 Windows 客户端上配置双向 CHAP。

本步骤中，您使用在控制台中为存储卷配置 CHAP 所用的相同密钥在 Microsoft iSCSI 启动程序中配置 CHAP。

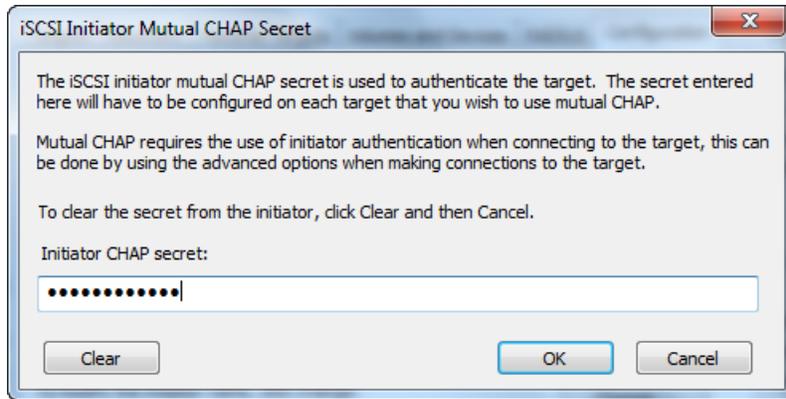
- 1. 如果 iSCSI 发起程序尚未启动，则在 Windows 客户端计算机的开始菜单中，键入 `iscsicpl.exe` 并运行该程序。
- 2. 配置启动程序 ( Windows 客户端 ) 的双向 CHAP。
  - a. 单击配置选项卡。



- b. 注意，发起程序名称字段对于您的发起程序和公司必须独一无二。此处显示的名称是在 AWS Storage Gateway 控制台的配置 CHAP 身份验证对话框中使用的值。

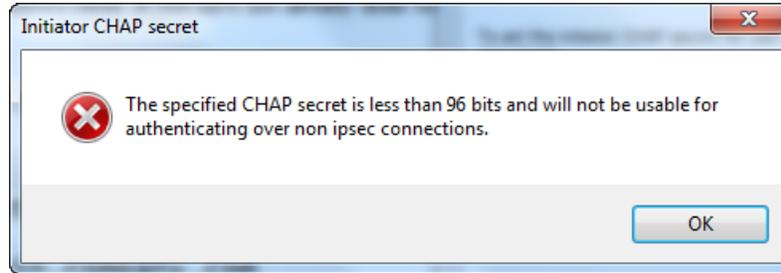
示例图像中所示名称仅作示范用途。

- c. 单击 CHAP 按钮。
- d. 在 iSCSI 发起程序双向 CHAP 私有密钥对话框中，输入双向 CHAP 私有密钥值。



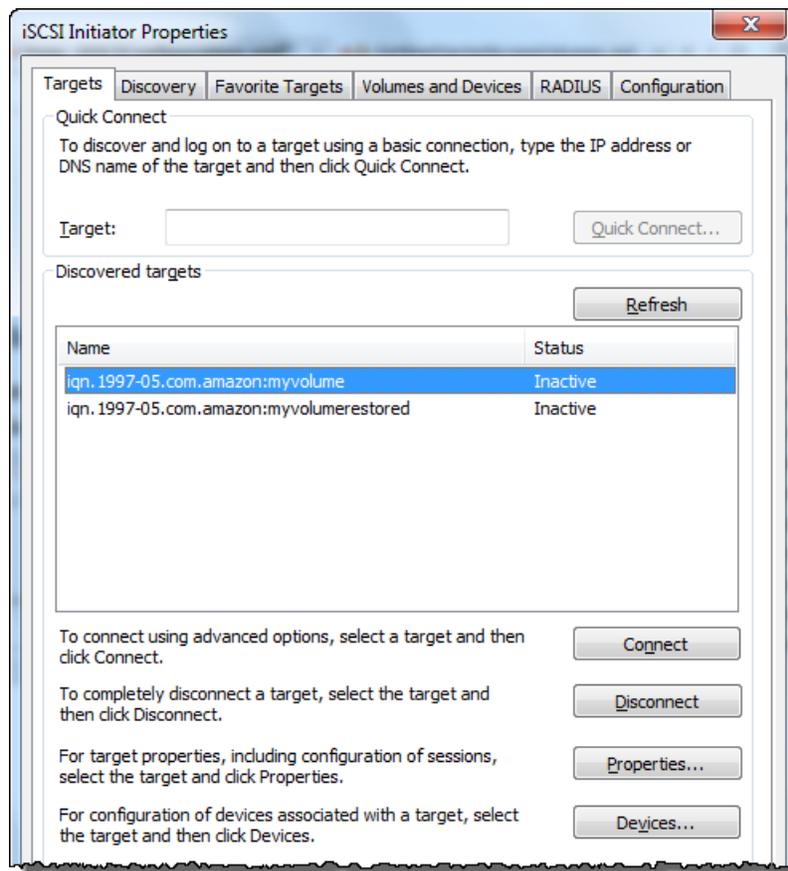
在此对话框中，输入启动程序（Windows 客户端）用来验证目标（存储卷）的私有密钥。该私有密钥允许目标读取并写入启动程序。此私有密钥映射到配置 CHAP 身份验证对话框中的用于验证目标身份的私有密钥(双向 CHAP)字段。有关更多信息，请参阅[为存储卷配置 CHAP 验证 \(p. 159\)](#)。

- e. 如果您输入的密钥少于 12 个字符，则显示发起程序 CHAP 私有密钥错误对话框。  
单击确定，然后尝试重新输入密钥。



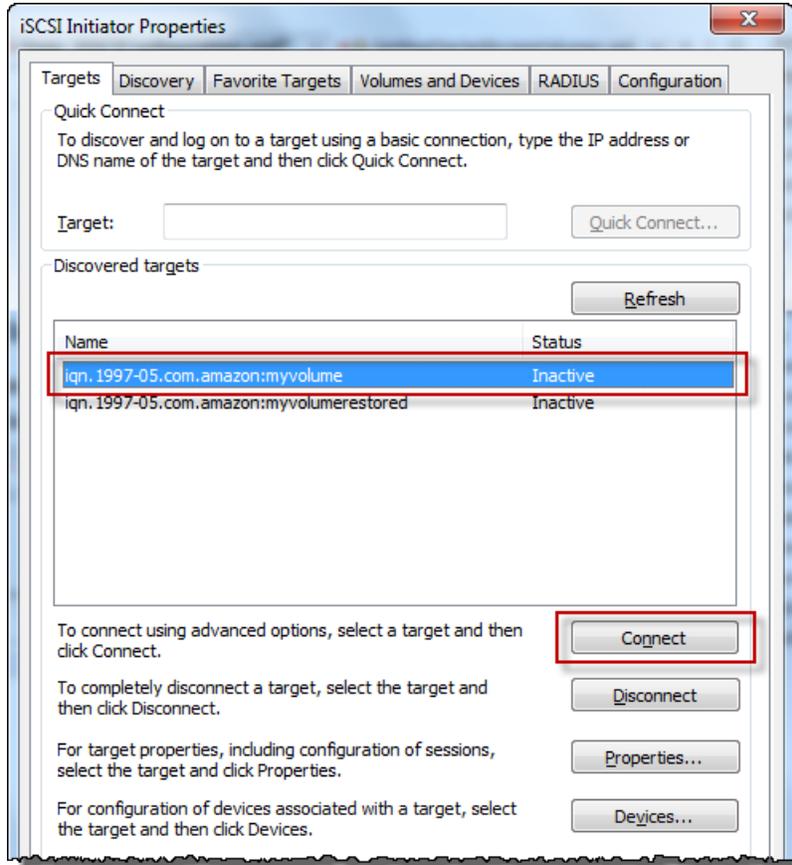
3. 使用启动程序的密钥进行配置，完成双向 CHAP 配置。

a. 单击目标选项卡。

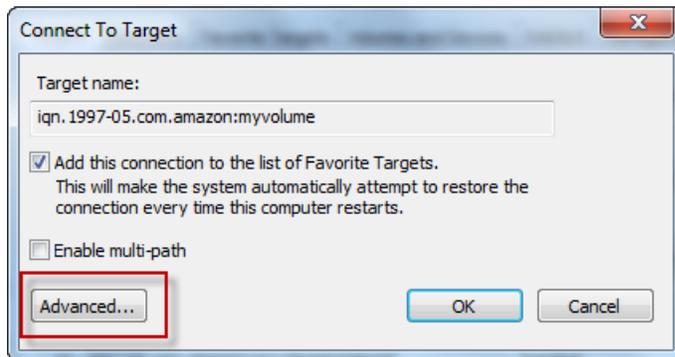


b. 如果当前连接了要为 CHAP 配置的目标，则通过选择该目标并单击断开连接，断开该目标。

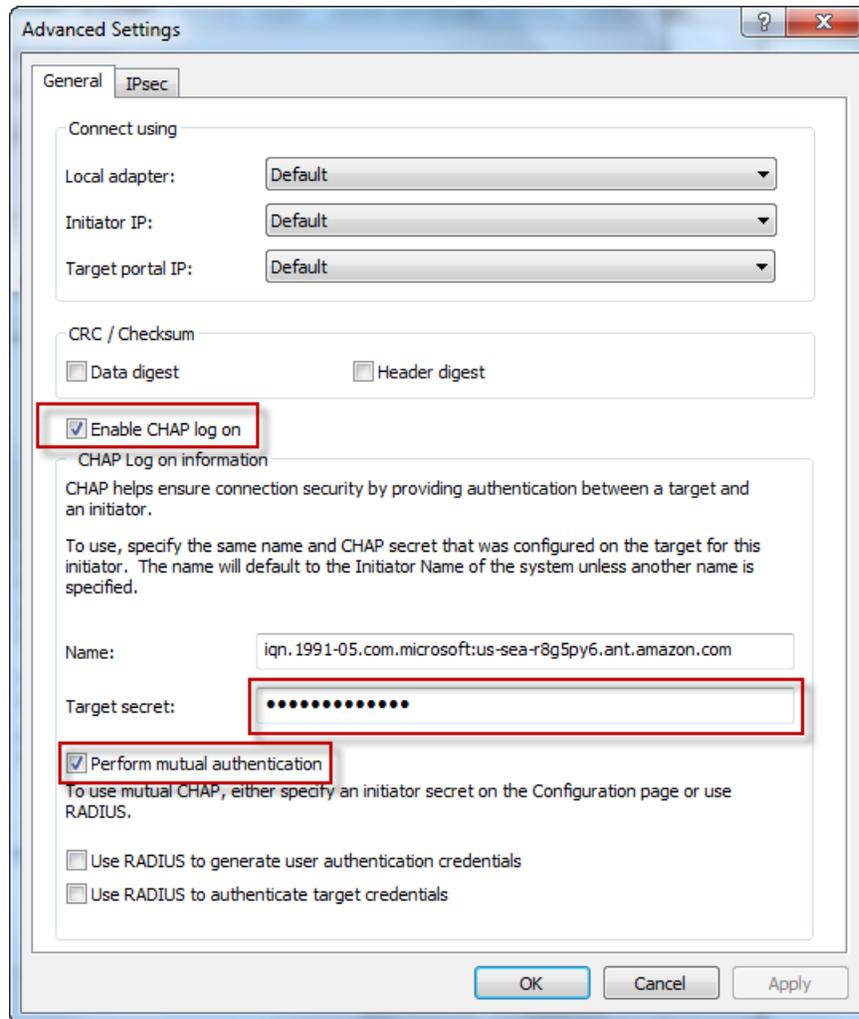
c. 选择要为 CHAP 配置的目标，然后单击连接。



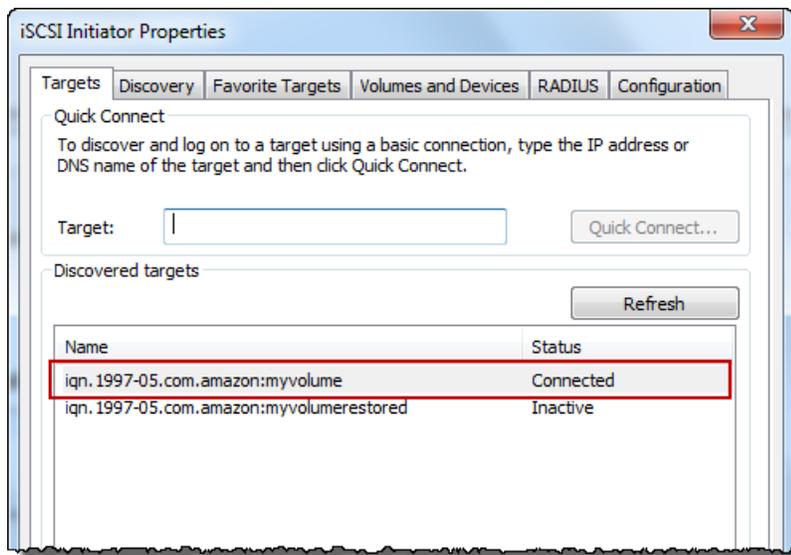
- d. 在连接到目标对话框中，单击高级。



- e. 在高级设置对话框中，配置 CHAP。



- i. 选择启用 CHAP 登录。
  - ii. 输入验证启动程序所需的该私有密钥。此私有密钥映射到配置 CHAP 身份验证对话框中的用于验证发起程序身份的私有密钥字段。有关更多信息，请参阅 [为存储卷配置 CHAP 验证 \(p. 159\)](#)。
  - iii. 选择执行双向身份验证。
  - iv. 单击确定以应用更改。
- f. 在连接到目标对话框中，单击确定。
4. 如果提供的私有密钥正确无误，则目标将显示已连接状态。



下列步骤假定 iSCSI 守护进程正在运行并且您已连接到了目标。如果尚未完成这两个任务，则参阅[从 Red Hat 连接到您的存储卷 \(p. 156\)](#)。

如需在 Red Hat Linux 客户端上配置双向 CHAP

本步骤中，您使用在控制台中为存储卷配置 CHAP 所用的相同密钥在 Linux iSCSI 启动程序中配置 CHAP。

1. 断开并移除您即将为其配置 CHAP 的目标的任何现有配置。
  - a. 列出已保存的配置以找到目标名称，并确保其为已定义配置。

```
sudo /sbin/iscsiadm --mode node
```

- b. 从目标断开。

以下命令从 Amazon IQN 上定义的名称为 *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。

以下命令删除 *myvolume* 目标的配置。

```
sudo /sbin/iscsiadm --mode node --op delete --targetname iqn.1997-05.com.amazon:myvolume
```

2. 编辑 iSCSI 文件以启用 CHAP。

- a. 获取启动程序的名称（您正在使用的客户端）。

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如下所示：

```
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代码注释，然后指定正确的用户名称和密码（私有访问密钥）。

```
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
```

将下表作为指导，填写前面的项目。

配置设置	值
username	使用您在本步骤中的上一步中找到的启动程序名称。该值将以“iqn”起始。例如， <code>iqn.1994-05.com.redhat:8e89b27b5b8</code> 是有效的 username。
password	这是用来在启动程序与存储卷通信时，验证启动程序（您正在使用的客户端）的私有密钥。
username_in	使用目标存储卷的 IQN。该值以“iqn”开头，以目标名称结尾。例如， <code>iqn.1997-05.com.amazon:myvolume</code> 是有效的 username_in。
password_in	这是用来在目标与启动程序通信时，验证目标（存储卷）的私有访问密钥。

- d. 保存配置文件中的更改并关闭文件。

### 3. 发现并登录到目标。

可按照从 [Red Hat 连接到您的存储卷 \(p. 156\)](#) 中提供的步骤发现并登录到目标。

## 管理已激活的卷网关（网关缓存和网关存储）

### Topics

- [管理 AWS Storage Gateway 中的存储卷 \(p. 167\)](#)
- [管理上传缓冲区和缓存存储空间（网关缓存） \(p. 177\)](#)
- [配置上传缓冲区（网关存储） \(p. 182\)](#)
- [使用快照 \(p. 187\)](#)
- [执行卷网关（网关缓存和网关存储）维护任务 \(p. 208\)](#)
- [卷网关（网关缓存或网关存储）问题排查 \(p. 236\)](#)
- [优化 AWS Storage Gateway 性能 \(p. 242\)](#)
- [监控 AWS Storage Gateway \(p. 243\)](#)
- [相关部分 \(p. 328\)](#)

本部分中，我们讨论您如何在部署并激活 AWS Storage Gateway 后对其进行管理。您将要对网关执行的管理任务包括配置存储卷和上传缓冲区、使用快照、一般维护、问题排查和网关监控。如果尚未设置网关，请参阅[设置卷网关（网关缓存和网关存储）](#)（p. 89）。

## 管理 AWS Storage Gateway 中的存储卷

### Topics

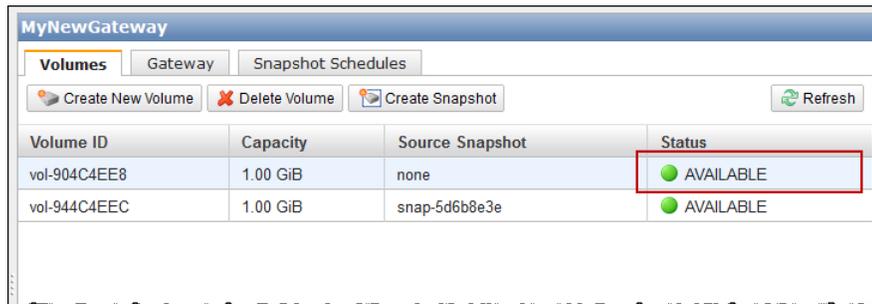
- [理解存储卷状况](#) (p. 167)
- [管理存储卷（网关缓存）](#) (p. 171)
- [管理存储卷（网关存储）](#) (p. 173)

本部分讨论如何管理您的存储卷，包括查看卷状况、添加新卷、以及移除现有卷。

### 理解存储卷状况

每个卷均有相关联的状况，让您一目了然地了解卷的运行状况。状况大多数时候将会显示卷运行正常，无需您采取任何行动。少数情况下，状况显示卷有问题，可能需要您执行相关操作，也可能不需要。本部分帮助您决定何时采取行动。

卷状态可在控制台中查看，也可使用 AWS Storage Gateway API 操作查看。有关示例，请参见 [DescribeCachediSCSIVolumes](#) 或 [DescribeStorediSCSIVolumes](#)。以下示例在 AWS Storage Gateway 控制台中显示卷状态。卷状态显示在网关中各个存储卷的状态字段中。在示例中，突出显示的卷运行正常，因为其状况为 AVAILABLE。



下表描述了各个卷的状况，以及您是否需要以及在何时应采取行动。AVAILABLE 状况是卷的正常状况，卷应该在使用的全部或大部分期间处于此状况。

状态	说明
AVAILABLE	卷的正常运行状况。

状态	说明
BOOTSTRAPPING	<p>该状况意为网关正在本地同步数据，同时将数据的副本存储在 AWS 中。您一般不需要对该状况采取任何行动，因为存储卷会在大多数情况下自动转为 AVAILABLE。</p> <p>以下是卷状况为 BOOTSTRAPPING 的三种场景。</p> <ul style="list-style-type: none"> <li>• 存储卷可在网关意外关停后、网关的上传缓冲区容量超出后或者在您创建网关存储卷并选择保存本地磁盘数据时，进行自举。</li> <li>• 超出了网关的上传缓冲区。在此场景中，自举会在您的卷处于 PASS THROUGH 状况以及自由上传缓冲区空间足够增加时发生。您可以提供额外的上传缓冲区，作为提高自由上传缓冲区空间比例的一种方式。在此特定场景中，存储卷从 PASS THROUGH 转为 BOOTSTRAPPING，再到 AVAILABLE。您可以在自举期间继续使用该卷；不过，您不能拍摄快照。</li> <li>• 您正在创建网关存储卷并保存现有磁盘数据。在此场景中，您的网关开始将所有数据上传到 AWS 并且卷仍然处于 BOOTSTRAPPING 状况，直至所有数据从本地磁盘复制到 AWS。您可以在自举期间使用该卷；不过，您不能拍摄快照。</li> </ul>
创建	该卷正在创建并且尚未可供使用。这是一个过渡状态；无需采取行动。
删除	卷当前正在删除。无需采取行动。
IRRECOVERABLE	发生错误，卷无法从其还原。有关在此情况下采取措施的信息，请参见 <a href="#">排查存储卷问题 (p. 239)</a> 。
PASS THROUGH	<p>该状况表示本地维护的数据与 AWS 中存储的数据未同步。这一卷状况可因各种原因发生。</p> <ul style="list-style-type: none"> <li>• 可导致 PASS THROUGH 状况发生的一个原因是您的网关用完了上传缓冲区空间。您的应用程序可在存储卷处于 PASS THROUGH 状况时继续从/向这些卷读写数据；但是网关不将您的任何卷数据写入其上传缓冲区，也不将任何此类数据上传到 AWS。网关将继续上传进入 PASS THROUGH 状况前写入到卷的任何数据。任何待拍摄或计划的存储卷快照将会在 PASS THROUGH 模式中失效。有关因超出上传缓冲区导致存储卷处于 PASS THROUGH 的情况下应执行的操作的信息，请参见 <a href="#">排查存储卷问题 (p. 239)</a>。</li> <li>• 卷显示 PASS THROUGH 状况的另一原因是有一个以上的存储卷在同时自举。同一时间只能有一个存储卷进行自举。例如，如果您创建两个存储卷并选择保存两个存储卷上的现有数据，那么第二个存储卷就会显示 PASS THROUGH 状况，直到第一个存储卷完成自举。在此场景中，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 AVAILABLE 状况。您可以在存储卷处于 PASS THROUGH 或 BOOTSTRAPPING 状况时向其读写数据。</li> <li>• PASS THROUGH 状况偶尔也可能表示分配作上传缓冲区的某磁盘发生故障。有关在此场景中应采取何种行动的信息，请参见 <a href="#">排查存储卷问题 (p. 239)</a>。</li> </ul>
还原	<p>卷正在从现有快照还原。该状态仅适用于网关存储卷设置中的存储卷（请参见 <a href="#">AWS Storage Gateway 的运行原理（架构）(p. 3)</a>）。</p> <p>如果您同时还原两个存储卷，两个存储卷均会显示 RESTORING 状况。各个存储卷将会在创建完成后自动转为 AVAILABLE 状况。您可以在存储卷处于 RESTORING 状况时向其读写数据并拍摄其快照。</p>

状态	说明
RESTORING_PASS_THROUGH	<p>该卷正在从现有快照还原，并且遇到了上传缓冲区问题。该状态仅适用于网关存储卷设置中的存储卷（请参见 <a href="#">AWS Storage Gateway 的运行原理（架构）</a> (p. 3)）。</p> <p>可导致 RESTORING_PASS_THROUGH 状况的一个原因是您的网关已用完了上传缓冲区空间。您的应用程序可在存储卷处于 RESTORING_PASS_THROUGH 状况时继续从/向其读写数据，但是 RESTORING_PASS_THROUGH 状况下不会创建任何存储卷快照。有关存储卷因超出上传缓冲区容量而处于 RESTORING_PASS_THROUGH 状态时应采取的行动，请参见 <a href="#">排查存储卷问题</a> (p. 239)。</p> <p>RESTORING_PASS_THROUGH 偶尔也可能表示分配作上传缓冲区的某磁盘发生故障。有关在此场景中应采取何种行动的信息，请参见 <a href="#">排查存储卷问题</a> (p. 239)。</p>
UPLOAD_BUFFER_NOT_CONFIGURED	<p>由于网关未配置上传缓冲区，卷无法创建或使用。如需为缓存卷网关添加上传缓冲区容量，请参见 <a href="#">添加并移除上传缓冲区容量（网关缓存）</a> (p. 179)。如需为存储卷网关添加上传缓冲区容量，请参见 <a href="#">配置上传缓冲区（网关存储）</a> (p. 182)。</p>

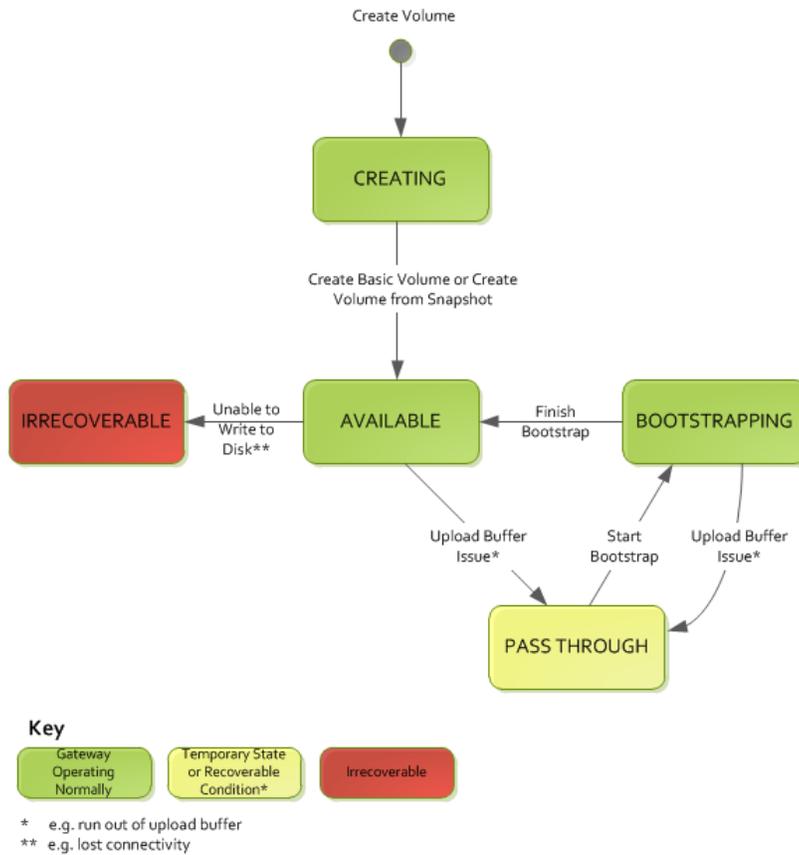
## 缓存卷状况过渡（网关缓存）

以下状态示意图描述网关缓存卷状况间最常见的过渡状态。您无需详细理解示意图以有效使用网关。示意图只是在您希望更多了解 AWS Storage Gateway 工作方式的情况下，为您提供详细信息。

该示意图不显示 UPLOAD\_BUFFER\_NOT\_CONFIGURED 状况，也不显示 DELETING 状况。示意图中的卷状态分别由绿、黄和红框表示。框的色彩含义说明如下。

- 绿色 – 网关运行正常。卷状况为 AVAILABLE，或者最终转为 AVAILABLE。
- 黄色 – 黄色 (PASS THROUGH) 表示存储卷可能存在问题。如果该状况是由于上传缓冲区已充满，那么在部分情况下可能会有更多缓冲区可供。此时，存储卷会自我更正并转为 AVAILABLE 状况。在另一些情况下，您可能需要添加更多的上传缓冲区到您的网关，以便让存储卷状况转为 AVAILABLE。如需在超出上传缓冲区容量时进行问题排查，请参见 [排查存储卷问题](#) (p. 239)。如需添加上传缓冲区容量，请参见 [添加并移除上传缓冲区容量（网关缓存）](#) (p. 179)。
- 红色 – 存储卷已转为 IRRECOVERABLE 状态。在此情况下，您应删除卷（请参见 [如需移除存储卷](#) (p. 173)）。

示意图中，两种状态简单过渡状态使用标记线表示。例如，从 CREATING 状态到 AVAILABLE 状态的转换将标记为 [创建基本卷](#) 或 [从快照中创建卷](#)，表示正在创建缓存卷。有关创建存储卷的更多信息，请参见 [添加存储卷](#) (p. 172)。



### Note

卷状态 PASS THROUGH 在该示意图中表示为黄色，这与 AWS Storage Gateway 控制台的状态字段中的此状态图标颜色不匹配。

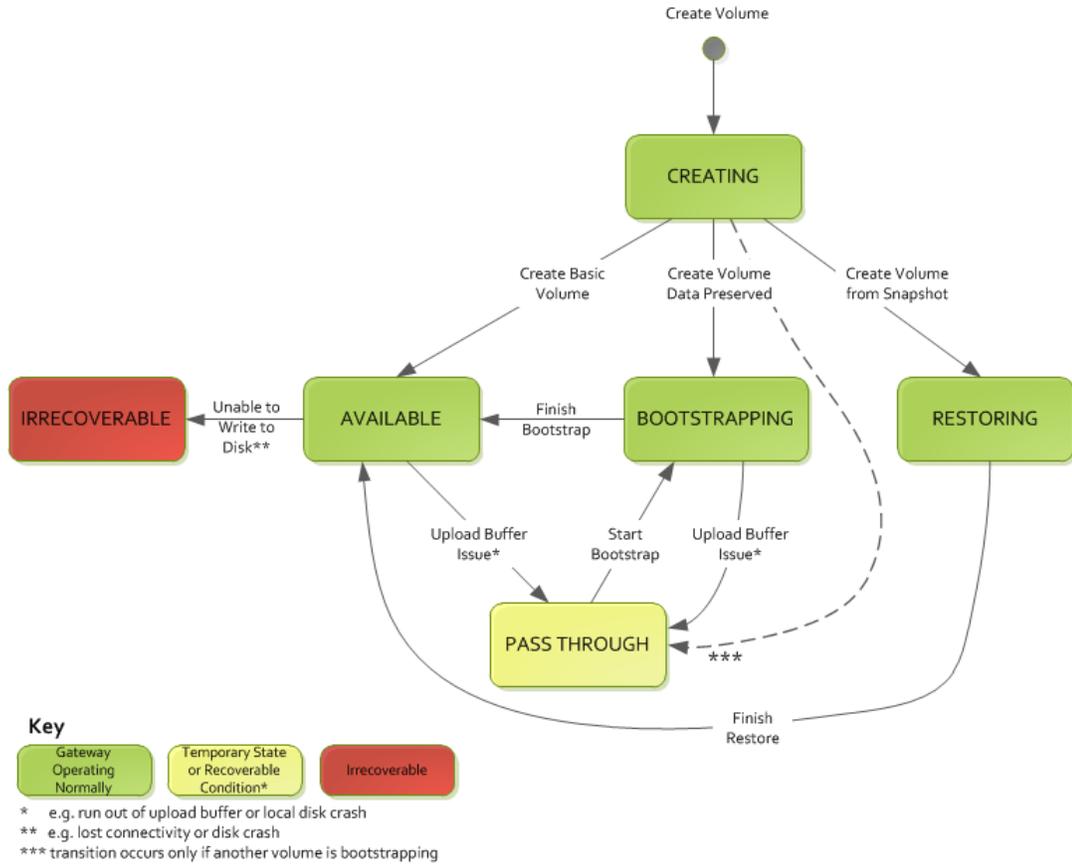
## 存储卷状况过渡 ( 网关存储 )

以下状态示意图描述网关存储卷状况间最常见的过渡状态。您无需详细理解示意图以有效使用网关。示意图只是在您希望更多了解 AWS storage Gateway 工作方式的情况下，为您提供详细信息。

该示意图不显示 UPLOAD BUFFER NOT CONFIGURED 状况，也不显示 DELETING 状况。示意图中的卷状态分别由绿、黄和红框表示。这些色彩的含义说明如下。

- 绿色—网关运行正常。卷状况为 AVAILABLE，或者最终转为 AVAILABLE。
- 黄色—在您创建存储卷并保存数据时，在另一个卷进行自举时会发生从 CREATING 到 PASS THROUGH 的路径。在此情况下，处于 PASS THROUGH 状况的卷就会在第一个卷完成自举后转为 BOOTSTRAPPING 后再转为 AVAILABLE。除了所述具体场景外，黄色 (PASS THROUGH) 表示存储卷可能存在问题，最常见的问题是上传缓冲区问题。如果超出了上传缓冲区容量，部分情况下可能有更多的空间可供使用。此时，存储卷会自我更正并转为 AVAILABLE 状况。在其他情况下，您需要向网关添加更多的上传缓冲区容量，以便让存储卷状态转为 AVAILABLE。如需在超出上传缓冲区容量时进行问题排查，请参见 [排查存储卷问题 \(p. 239\)](#)。如需添加上传缓冲区容量，请参见 [配置上传缓冲区 \( 网关存储 \) \(p. 182\)](#)。
- 红色—存储卷已转为 IRRECOVERABLE 状态。在此情况下，您应删除卷 ( 请参见 [移除底层本地磁盘 \(VMware ESXi\) \(p. 175\)](#) ) 。

在下面的示意图中，两种状态间的过渡状态用标记线表示。例如，从 CREATING 状态到 AVAILABLE 状态的转换标记为 *创建基本卷*，表示在不保存数据或从快照进行创建的情况下创建存储卷。有关创建存储卷的更多信息，请参见 [如需使用控制台创建存储卷 \(p. 151\)](#)。



### Note

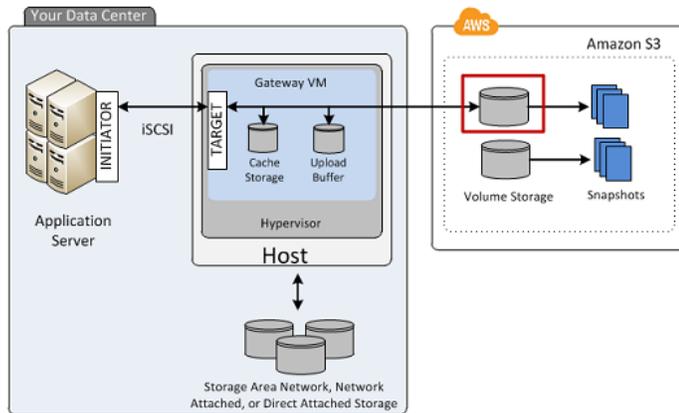
卷状态 PASS THROUGH 在该示意图中表示为黄色，这与 AWS Storage Gateway 控制台的状态字段中的此状态图标颜色不匹配。

## 管理存储卷 ( 网关缓存 )

### Topics

- [添加存储卷 \(p. 172\)](#)
- [移除存储卷 \(p. 173\)](#)

网关缓存卷是 Amazon S3 中公布为 iSCSI 目标的存储卷，您可以用来存储应用程序数据。以下示意图突出显示网关缓存设置中的存储卷 ( 请参见 [AWS Storage Gateway 的运行原理 \( 架构 \) \(p. 3\)](#) )。



您的网关使用您指定的名称将各个卷公布为 iSCSI 目标，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，请参见 [配置应用程序对存储卷的访问 \(p. 153\)](#)。



#### Note

存储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。每个网关可支持高达 20 个缓存卷以及 150 TiB 的缓存卷总存储空间。

不支持重新配置存储卷的大小。如需更改卷的大小，请创建该卷的快照，然后从该快照创建新缓存卷。新卷可大于快照所创建的卷。有关描述如何移除存储卷的步骤，请参见 [如需移除存储卷 \(p. 173\)](#)。有关描述如何添加存储卷和保存现有数据的步骤，请参见 [如需使用控制台创建存储卷 \(p. 149\)](#)。



#### Important

由于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全部数据的进程。例如，我们强烈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还是按计划，都会导致存储在 Amazon S3 中的所有数据为扫描进行本地下载，由此导致高带宽使用率和废数据缓存。作为进行整个磁盘扫描的替代方法，您可以使用实时病毒扫描，即扫描从/向缓存卷读写的数据。

所有的网关缓存卷数据和快照数据均保存在 Amazon S3 中，并使用服务器端加密 (SSE) 进行安全加密。不过，您不能使用 Amazon S3 API 或借助 Amazon S3 等其他工具访问这些数据。

## 添加存储卷

您在初始网关设置过程中创建存储卷。有关示例，请参见 [卷网关入门 \(网关缓存卷和网关存储卷\) \(p. 10\)](#)。随着应用程序需求的增长，您可能需要向网关添加更多的存储卷。随着向网关添加更多的存储卷，您必须考虑分配给网关的缓存存储空间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，请参见 [管理上传缓冲区和缓存存储空间 \(网关缓存\) \(p. 177\)](#)。

您可以使用 API (请参见 [CreateCachediSCSIVolume](#)) 或控制台添加存储卷。以下任务展示控制台的使用过程，并假定您已部署并激活了网关。

### 如需使用控制台创建存储卷

- 按照 [创建存储卷 \(网关缓存\) \(p. 149\)](#) 中您用来创建初始卷的步骤操作。

## 移除存储卷

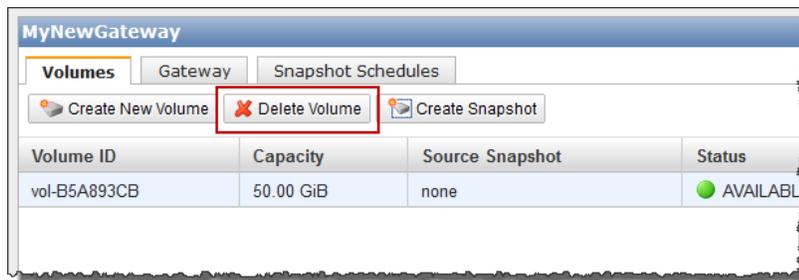
随着应用程序需求的变化，您可能需要移除存储卷，例如在迁移应用程序以便使用更大存储卷的情况下。移除存储卷前，请确保没有应用程序正在写入卷。另外，请确保该卷没有快照正在进程中。如果已为卷定义快照计划，则可在控制台的快照计划选项卡中进行查看。有关更多信息，请参见 [编辑快照计划 \(p. 195\)](#)。

移除存储卷前，请确保没有应用程序正在写入卷。另外，请确保该卷没有快照正在进程中。可在控制台的快照计划选项卡上检查存储卷的快照计划。有关更多信息，请参见 [编辑快照计划 \(p. 195\)](#)。执行以下任务，在网关运行的情况下移除存储卷。

您可以使用 API ( 请参见 [API\\_DeleteVolume](#) ) 或控制台移除存储卷。以下任务展示控制台的使用过程。在网关运行的情况下执行任务。

### 如需移除存储卷

1. 在 AWS Storage Gateway 控制台的卷选项卡中，选择该存储卷。



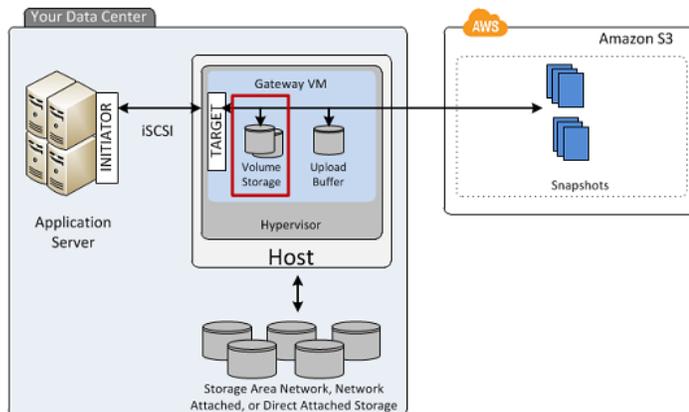
2. 单击删除卷。

## 管理存储卷 ( 网关存储 )

### Topics

- [添加存储卷 \(p. 174\)](#)
- [移除存储卷 \(p. 174\)](#)

网关存储卷是公布为 iSCSI 目标的存储卷，您可以用来存储应用程序数据。在您添加到网关 VM 的本地虚拟磁盘上创建存储卷 ( 请参见 [预配置本地磁盘 \( 网关存储 \) \(p. 100\)](#) )。以下示意图突出显示网关存储设置中的存储卷 ( 请参见 [AWS Storage Gateway 的运行原理 \( 架构 \) \(p. 3\)](#) )。



您的网关使用您指定的名称将各个卷公布为 iSCSI 目标，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，请参见 [配置应用程序对存储卷的访问](#) (p. 153)。您的网关将应用程序数据本地存储在存储卷的磁盘上，同时将您的数据异步上传到 AWS。



#### Note

存储卷的大小范围可以是 1 GiB 到 1 TiB。大小取决于您从创建存储卷的本地磁盘。本地磁盘的大小应四舍五入到最近的 GiB 值（请参见 [为存储卷添加本地磁盘（网关存储）](#) (p. 101)）。每个网关可支持高达 12 个卷以及高达 12 TiB 的本地存储。

不支持重新配置存储卷底层磁盘的大小。如需更改底层磁盘的大小，请删除使用该磁盘的存储卷，重新配置磁盘大小，然后从重新配置了大小的磁盘创建新存储卷。重新创建存储卷时，请务必保存磁盘上的数据。有关描述如何移除存储卷的步骤，请参见 [移除底层本地磁盘（VMware ESXi）](#) (p. 175) 或 [移除底层本地磁盘（Microsoft Hyper-V）](#) (p. 176)。有关描述如何添加存储卷和保存现有数据的步骤，请参见 [如需使用控制台创建存储卷](#) (p. 151)。

## 添加存储卷

您在初始网关设置过程中创建存储卷，有关示例，请参见 [卷网关入门（网关缓存卷和网关存储卷）](#) (p. 10)。随着应用程序需求的增长，您可能需要向网关添加更多的存储卷。随着添加更多的存储卷，您必须考虑分配给网关的上传缓冲区的大小。网关必须有充足的缓冲区空间。有关更多信息，请参见 [管理上传缓冲区（网关存储）](#) (p. 183)。

您可以使用 API（请参见 [CreateStorediSCSIVolume](#)）或控制台添加存储卷。以下任务展示控制台的使用过程，并假定您已部署并激活了网关。另外，假定的前提是至少有一个本地预配置的网关磁盘，该磁盘未被使用并且可分配为存储卷。若要为应用程序存储配置本地磁盘，请参见 [预配置本地磁盘（网关存储）](#) (p. 100)。

### 如需添加存储卷

- 按 [创建存储卷（网关存储）](#) (p. 151) 中的步骤操作。

## 移除存储卷

随着应用程序需求的变化，您可能需要移除存储卷，例如迁移应用程序以便使用更大的存储卷并且您希望回收旧存储卷的底层本地磁盘空间时。您需要将本地磁盘从 VM 移除，才能回收本地磁盘空间。

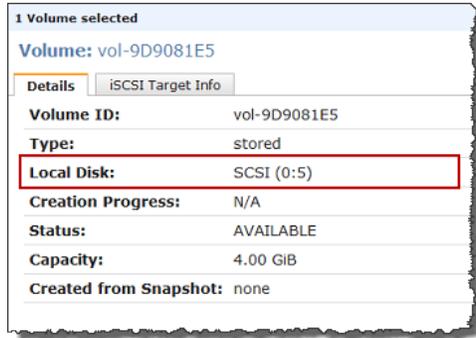
移除存储卷前，请确保没有应用程序正在写入卷。另外，请确保该卷没有快照正在进程中。可在控制台的快照计划选项卡上检查存储卷的快照计划。有关更多信息，请参见 [编辑快照计划](#) (p. 195)。

您可以使用 API（请参见 [DeleteVolume](#)）或控制台移除存储卷。以下任务演示如何使用控制台、VMware ESXi 平台上所部署网关的 vSphere 客户端或者 Microsoft Hyper-V 平台上所部署网关的 Microsoft Hyper-V Manager。执行以下任务，在网关运行的情况下移除存储卷。

### 移除 AWS Storage Gateway 控制台中的存储卷

- 在 AWS Storage Gateway 控制台的卷选项卡中，选择该存储卷。
- 如果您计划从 VM 移除支持存储卷的磁盘，请在详细信息属性选项卡中，记下本地磁盘字段中的值。

该值是磁盘的虚拟设备节点值，您可在管理程序客户端中使用该值以确保移除正确的磁盘。



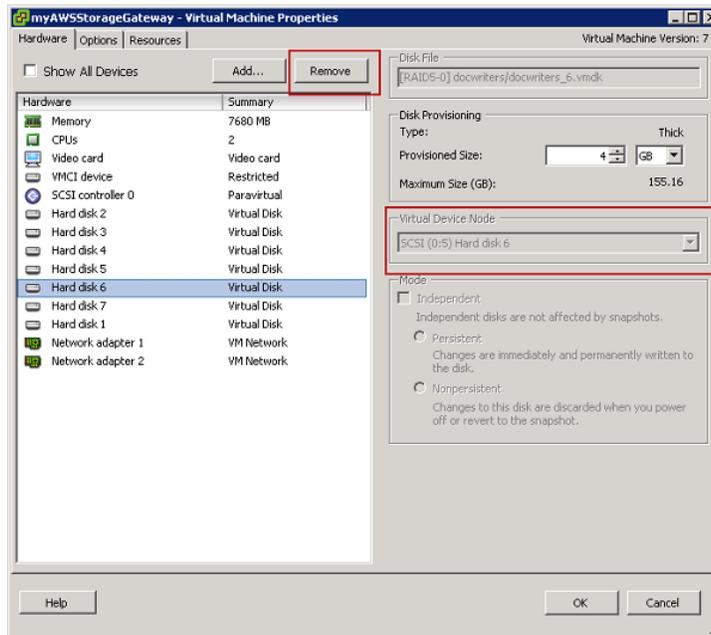
- 单击删除卷。
- 如果您希望移除底层本地磁盘，请执行下列操作之一：

对于下列托管网关...	请执行此操作...
VMware ESXi	按 <a href="#">移除底层本地磁盘 (VMware ESXi)</a> (p. 175) 中的步骤操作。
Microsoft Hyper-V	按 <a href="#">移除底层本地磁盘 (Microsoft Hyper-V)</a> (p. 176) 中的步骤操作。

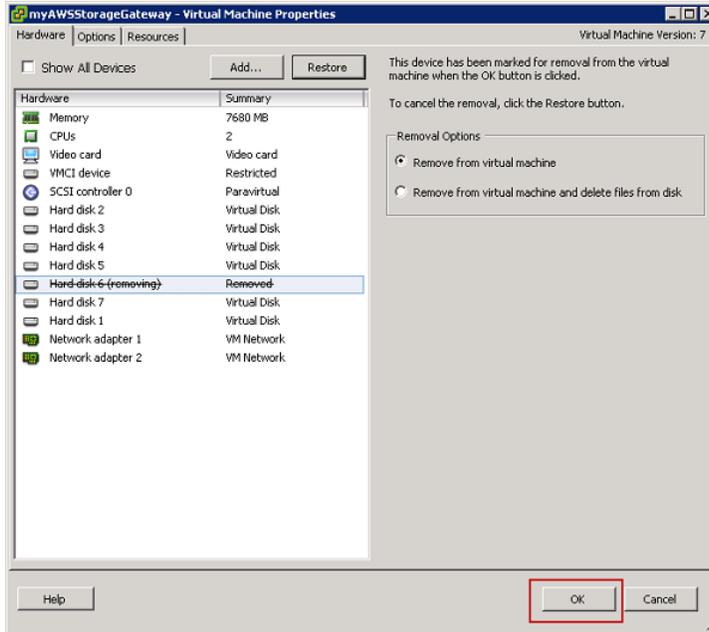
### 移除底层本地磁盘 (VMware ESXi)

- 在 vSphere 客户端中，右键单击网关 VM 的名称，然后单击编辑设置...
- 在虚拟机属性对话框的硬件选项卡中，选择要移除的磁盘，然后单击移除。

确认虚拟机属性对话框中的虚拟设备节点值与从上一步中记录的值相同。这项操作确保您移除了要移除的磁盘。在 Microsoft Hyper-V Manager 中显示的第一个 SCSI Controller 是控制器 0。



- 在删除选项面板中选择一个选项，然后单击确定以完成删除磁盘的过程。



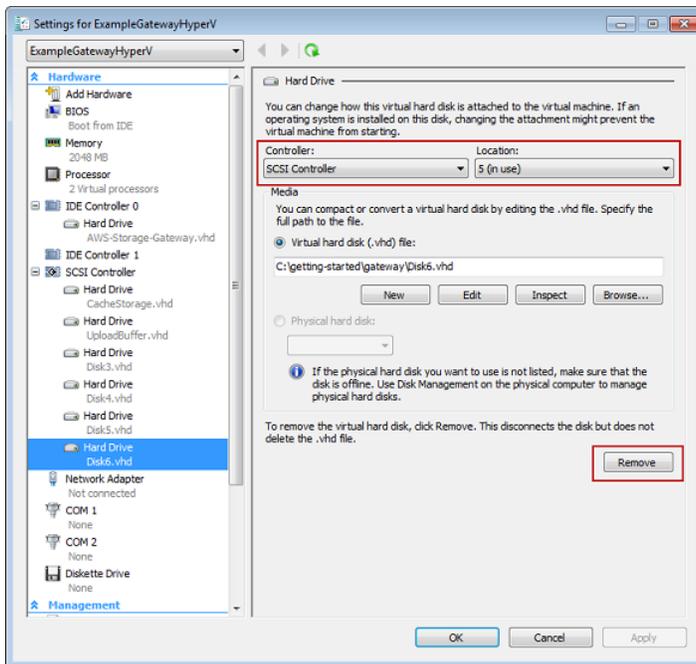
### 移除底层本地磁盘 (Microsoft Hyper-V)

1. 在 Microsoft Hyper-V 管理器中，右键单击网关 VM 的名称，然后单击设置...
2. 在设置对话框的硬件列表中，选择要删除的磁盘，然后单击删除。

添加到网关的磁盘在硬件列表中的 SCSI 控制器条目下。

验证控制器和位置值与上一步中记录的值相同。这项操作确保您移除了要移除的磁盘。

在 Microsoft Hyper-V Manager 中显示的第一个 SCSI Controller 是控制器 0。



- 单击确定以应用更改。

## 管理上传缓冲区和缓存存储空间 ( 网关缓存 )

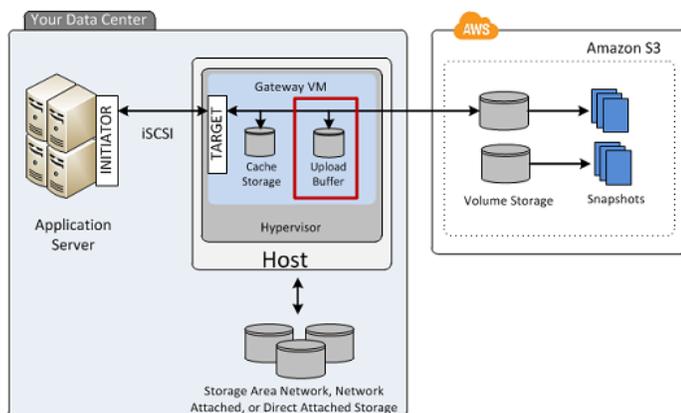
### Topics

- [管理上传缓冲区 \( 网关缓存 \) \(p. 177\)](#)
- [管理缓存存储空间 \( 网关缓存 \) \(p. 178\)](#)
- [添加并移除上传缓冲区容量 \( 网关缓存 \) \(p. 179\)](#)
- [添加缓存存储空间 \( 网关缓存 \) \(p. 182\)](#)

在初步部署过程中，您需要为网关配置上传缓冲区和缓存存储空间。在添加存储卷以便为应用程序数据提供更多存储空间的同时，您可能需要给网关添加更多的上传缓冲区或缓存存储空间容量。举例而言，由于希望替换已失效的本地磁盘，您可能还要移除分配为上传缓冲区的本地磁盘。本部分探讨如何确定您是否需要添加更多上传缓冲区或缓存存储空间，以及如何添加。

### 管理上传缓冲区 ( 网关缓存 )

您的网关在将卷数据上传到 AWS 前，使用上传缓冲区临时缓冲这些数据。下图在网关缓存架构的大图中突出显示了上传缓冲区 ( 请参阅 [AWS Storage Gateway 的运行原理 \( 架构 \) \(p. 3\)](#) )。



您的网关需要的上传缓冲区空间量的大小取决于数种因素，例如向存储卷传入数据的速率，向 AWS 传出数据的速率，您的网络带宽等。如果应用程序持续向存储卷快速写入数据，而网络吞吐量不足够网关上传数据到 AWS，那么您的上传缓冲区最终就会填满等待上传到 AWS 的数据。下面是可以帮助您避免出现这种情况的一些指导：

- 使用调整大小公式—随着应用程序需求的变化，应定期检查建议用于调整上传缓冲区大小的公式。有关更多信息，请参阅 [配置上传缓冲区的大小 \( 网关缓存 \) \(p. 97\)](#)。
- 使用 Amazon CloudWatch 指标— 可通过在一段时间后监控网关使用上传缓冲区空间的百分比，主动避免上传缓冲区填满。Amazon CloudWatch 提供 `UploadBufferPercentUsed` 指标等用量指标用于监控网关的上传缓冲区 ( 请参阅 [监控上传缓冲区 \(p. 249\)](#) )。您可以设置一个阈值，在上传缓冲区使用率超过该阈值时，触发向您发送的通知。如果上传缓冲区填充的数据量接近容量，您可以考虑向网关添加更多缓冲区容量。有关 AWS Storage Gateway 指标的完整列表，请参阅 [理解 AWS Storage Gateway 指标 \(p. 253\)](#)。有关 AWS Storage Gateway 指标的完整列表，请参阅 [理解 AWS Storage Gateway 指标 \(p. 253\)](#)。

可在 AWS Storage Gateway 控制台的网关选项卡中看到上传缓冲区用量的当前百分比。

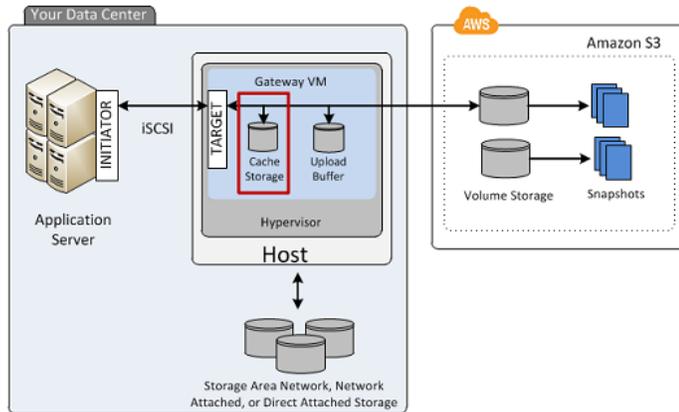
- 监控卷状态—卷状态可指示上传缓冲区的问题。例如，如果达到上传缓冲区最大容量，则受影响的存储卷进入 [PASS THROUGH \(p. 169\)](#) 模式，并且尽管应用程序可继续运行，向存储卷写入或从其读取数据，但这段时间内不拍摄快照。
- 优化所处环境—如果传入写入的速度与传出网络带宽相比过高，则无论将上传缓冲区容量配置为多大，网关可能都跟不上该速度。在此情况下，请考虑优化网关以提高性能 ( 请参阅 [优化 AWS Storage Gateway 性能 \(p. 242\)](#) )。

如果您确定需要改变上传缓冲区的容量，请执行下列操作。

如需...	请执行此操作...
向您的网关添加更多上传缓冲区容量。	按 <a href="#">添加上传缓冲区容量 (p. 179)</a> 中的步骤进行操作。
移除分配为上传缓冲区的磁盘。	按 <a href="#">移除上传缓冲区容量 (p. 179)</a> 中的步骤进行操作。

## 管理缓存存储空间 ( 网关缓存 )

您的网关使用缓存存储空间来缓存最近访问的应用程序数据。下图在 AWS Storage Gateway 网关缓存架构的大图中突出显示了缓存存储 ( 请参阅 [AWS Storage Gateway 的运行原理 \( 架构 \) \(p. 3\)](#) )。



您的网关需要的缓存存储空间大小取决于您希望提供低延迟访问的应用程序数据量。缓存存储空间的大小不得少于上传缓冲区的大小。这样可以保证缓存存储空间有足够的大小来持续承载尚未上传到 Amazon S3 的全部数据。缓存存储空间充满废数据时，直到更多缓存存储空间可用时才会解除屏蔽应用程序向存储卷的写入。不过，仍然允许应用程序从存储卷读取数据。下面是可以帮助您避免出现这种情况的一些指导：

- 使用调整大小公式—随着应用程序需求的变化，应定期检查建议用于调整缓存存储大小的公式。有关更多信息，请参阅 [配置缓存存储空间的大小 \( 网关缓存 \) \(p. 93\)](#)。
- 使用 Amazon CloudWatch 指标—可通过监控正在如何使用缓存存储—特别是通过检查缓存未命中次数，主动避免将缓存存储填满无效数据。Amazon CloudWatch 提供 `CachePercentDirty` 和 `CacheHitPercent` 指标等用量指标用于监控网关的缓存存储中有多少数据尚未上传到 Amazon S3。您可以设置阈值，在缓存废数据百分率超过某阈值或缓存命中率低于某阈值时触发向您发送的通知，两者均有可能表示缓存存储空间不够网关使用。有关 AWS Storage Gateway 指标的完整列表，请参阅 [理解 AWS Storage Gateway 指标 \(p. 253\)](#)。

如果决定需要增加网关的缓存存储容量，请按 [添加缓存存储空间 \( 网关缓存 \) \(p. 182\)](#) 中的步骤操作。

## 添加并移除上传缓冲区容量 (网关缓存)

最初配置网关上传缓冲区 (请参阅[配置上传缓冲区 \(网关缓存\)](#) (p. 143)) 后, 可随应用程序需求的变化配置额外的上传缓冲区容量。要详细了解如何根据应用程序需求调整上传缓冲区大小, 请参阅[配置上传缓冲区的大小 \(网关缓存\)](#) (p. 97)。

您可以向网关添加更多缓冲区空间, 无需中断现有的网关功能。请注意, 您需要在网关 VM 开启的情况下才能添加更多上传缓冲区容量; 但是减少上传缓冲区容量时, 则必须先关闭 VM。

### 添加上传缓冲区容量

随着应用程序需求的变化以及更多存储卷空间的添加, 您可能需要增加网关的上传缓冲区容量。可使用 AWS Storage Gateway API (请参阅 [AddUploadBuffer](#)) 或 AWS Storage Gateway 控制台添加更多缓冲区容量。下列步骤介绍了如何使用控制台添加更多缓冲区容量。这些步骤假定您的已激活网关在其 VM 上至少有一个本地磁盘可用, 可供您将其分配为网关的上传缓冲区。

如需使用控制台为您的网关将本地磁盘配置为上传缓冲区

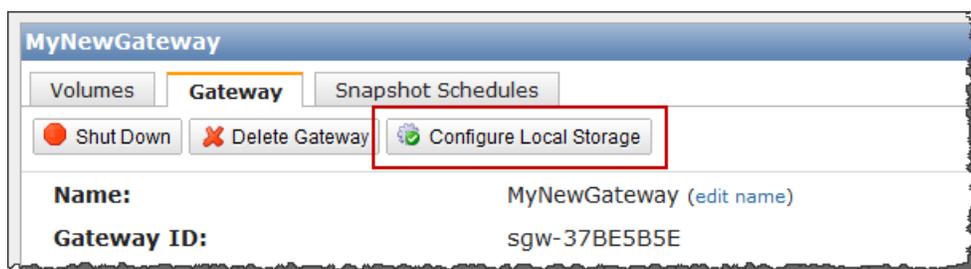
- 按[如需将本地磁盘配置为网关的上传缓冲区](#) (p. 143) 中的步骤进行操作。

### 移除上传缓冲区容量

由于应用程序需求的变化以及对网关的存储卷配置的更改, 您可能需要减少网关的上传缓冲区容量。分配为上传缓冲区的本地磁盘也有可能失效, 导致您需要从上传缓冲区移除该磁盘并分配新的本地磁盘。在两种情况下, 均可使用 AWS Storage Gateway 控制台删除更多缓冲区容量。下列步骤假定您已激活的网关至少有一个本地磁盘分配为网关的上传缓冲区。这些步骤以 AWS Storage Gateway 控制台为开始, 随后离开控制台, 使用 VMware vSphere 客户端或 Microsoft Hyper-V Manager 移除磁盘, 然后返回到控制台。

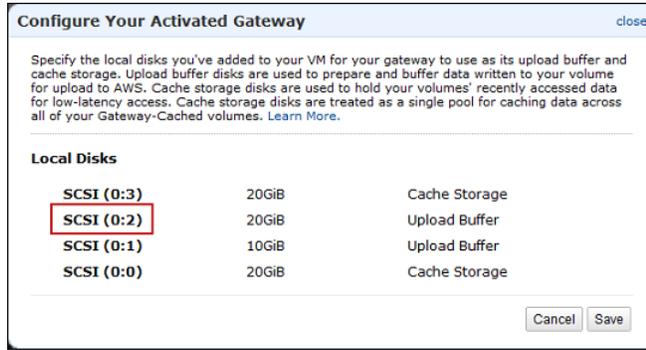
使用控制台查找已分配为上传缓冲区的磁盘 ID

- 在 AWS Storage Gateway 控制台的网关选项卡中, 单击配置本地存储。



- 在配置已激活的网关对话框中, 记下要删除的本地磁盘的虚拟设备节点值。可在本地磁盘列中找到节点值。例如, 在下面的对话框中, 突出显示设备节点 SCSI (0:2)。

您在 vSphere 客户端中使用磁盘的虚拟设备节点来确保移除了需要移除的磁盘。



- 按使用 [AWS Storage Gateway 控制台](#) 关停并启动网关 (p. 210) 过程中的步骤关闭网关。



#### Note

关停网关前，请确保没有正在向该网关写入数据的应用程序正在使用它，并且没有快照进程。可在控制台的快照计划选项卡上检查存储卷的快照计划。有关更多信息，请参阅 [编辑快照计划](#) (p. 195)。

- 要移除底层本地磁盘，请执行下列操作之一，然后转到下一步：

对于下列托管网关...	请执行此操作...
VMware ESXi	按 <a href="#">移除已分配为上传缓冲区磁盘的底层磁盘 ( VMware ESXi )</a> (p. 180) 中的步骤进行操作。
Microsoft Hyper-V	按 <a href="#">移除已分配为上传缓冲区磁盘的底层磁盘 (Microsoft Hyper-V)</a> (p. 181) 中的步骤进行操作。

- 在 AWS Storage Gateway 控制台中，打开网关。



#### Important

移除了用作上传缓冲区的磁盘后，您必须在向 VM 添加新磁盘前重新开启网关。

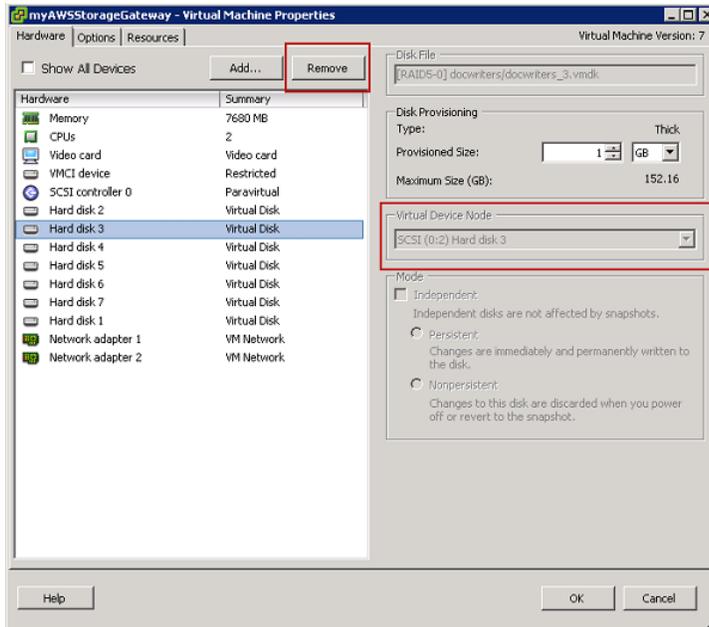
- 在 AWS Storage Gateway 控制台的卷选项卡中，确认所有存储卷的状态均为 [AVAILABLE](#) (p. 169)。

网关重新启动后，存储卷可能在网关适应您删除的上传缓冲区磁盘时经历 [PASS THROUGH](#) (p. 169) 和 [BOOTSTRAPPING](#) (p. 169) 状态。经历这两个状态的存储卷最终将变为 [AVAILABLE](#) (p. 169) 状态。您可以在状态转换以及自举状态的过程中使用存储卷，但不能拍摄快照。

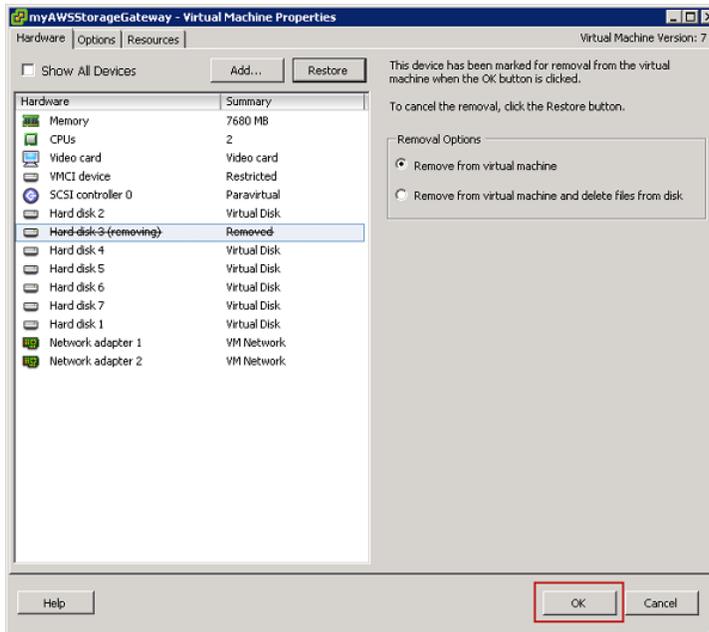
#### 移除已分配为上传缓冲区磁盘的底层磁盘 ( VMware ESXi )

- 在 vSphere 客户端中，右键单击网关 VM 的名称，然后单击编辑设置...
- 在虚拟机属性对话框的硬件选项卡中，选择分配为上传缓冲区的磁盘，然后单击删除。

确认虚拟机属性对话框中的虚拟设备节点值与从上一步中记录的值相同。这样可以确保您移除需要移除的网关。



3. 在删除选项面板中选择一个选项，然后单击确定以完成删除磁盘的过程。

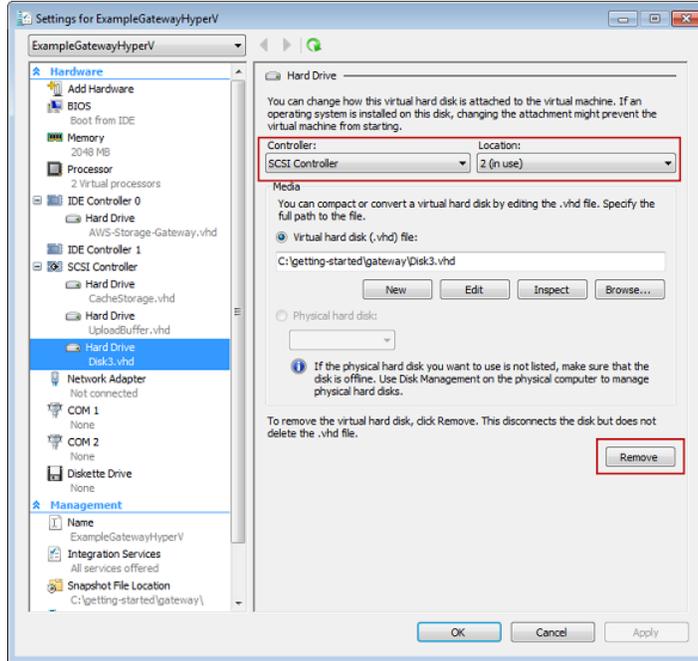


### 移除已分配为上传缓冲区磁盘的底层磁盘 (Microsoft Hyper-V)

1. 在 Microsoft Hyper-V 管理器中，右键单击网关 VM 的名称，然后单击设置...。
2. 在设置对话框的硬件列表中，选择要删除的磁盘，然后单击删除。

添加到网关的磁盘在硬件列表中的 SCSI 控制器条目下。验证控制器和位置值与上一步中记录的相同。这项操作确保您移除了要移除的磁盘。

在 Microsoft Hyper-V Manager 中显示的第一个 SCSI Controller 是控制器 0。



3. 单击确定以应用更改。

## 添加缓存存储空间 ( 网关缓存 )

最初配置网关缓存存储 ( 请参阅 [配置缓存存储空间 \( 网关缓存 \)](#) (p. 145) ) 后, 可随应用程序需求的变化为网关配置额外的缓存存储。要详细了解如何根据应用程序需求调整缓存存储大小, 请参阅 [配置缓存存储空间的大小 \( 网关缓存 \)](#) (p. 93)。

您可以在网关 VM 开启的情况下向网关添加更多的缓存存储空间, 无需打断现有的网关功能。



### Note

当前不支持移除分配为缓存存储空间的磁盘。

可使用 AWS Storage Gateway API ( 请参阅 [AddCache](#) ) 或 AWS Storage Gateway 控制台添加更多缓存存储。以下过程假定您激活的网关在其 VM 上至少有一个本地磁盘可分配为网关的缓存存储。

如需将本地磁盘配置为网关的缓存存储空间

- 按 [如需将本地磁盘配置为网关的缓存存储空间](#) (p. 145) 中的步骤进行操作。

## 配置上传缓冲区 ( 网关存储 )

### Topics

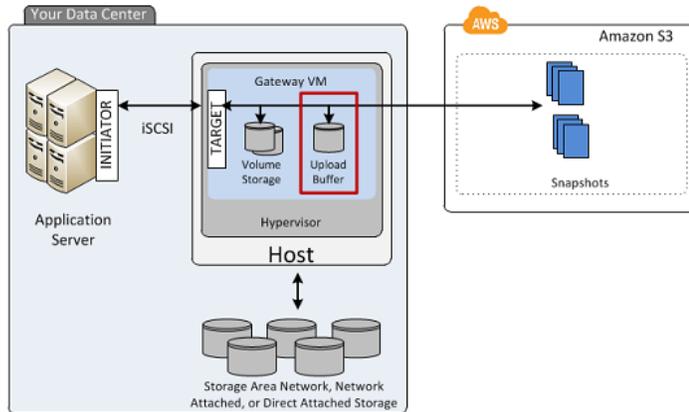
- [管理上传缓冲区 \( 网关存储 \)](#) (p. 183)
- [添加和移除上传缓冲区容量 \( 网关存储 \)](#) (p. 184)

为网关配置上传缓冲区是初步部署的部分内容。在添加存储卷以便为应用程序数据提供更多存储空间的同时, 您可能需要向网关添加更多的上传缓冲区容量。举例而言, 由于希望替换已失效的本地磁盘, 您可能

还要移除分配为上传缓冲区的本地磁盘。本部分探讨如何确定您是否需要添加更多的上传缓冲区容量，以及如何添加。

## 管理上传缓冲区 ( 网关存储 )

您的网关在将卷数据上传到 AWS 前，使用上传缓冲区临时缓冲这些数据。下图在网关存储架构的大图中突出显示了上传缓冲区 ( 请参阅 [AWS Storage Gateway 的运行原理 \( 架构 \)](#) (p. 3) )。



您的网关需要的上传缓冲区空间量的大小取决于数种因素，例如向存储卷传入数据的速率，向 AWS 传出数据的速率，您的网络带宽等。如果应用程序持续向存储卷快速写入数据，而网络吞吐量不足够网关上传数据到 AWS，那么您的上传缓冲区最终就会填满等待上传到 AWS 的数据。下面是可以帮助您避免出现这种情况的一些指导：

- 使用调整大小公式—随着应用程序需求的变化，应定期检查建议用于调整上传缓冲区大小的公式。有关更多信息，请参阅 [配置上传缓冲区的大小 \( 网关存储 \)](#) (p. 104)。
- 使用 Amazon CloudWatch 指标—可通过在一段时间后监控网关使用上传缓冲区空间的百分比，主动避免上传缓冲区填满。Amazon CloudWatch 提供 UploadBufferPercentUsed 指标等用量指标用于监控网关的上传缓冲区用量 ( 请参阅 [监控上传缓冲区](#) (p. 249) )。您可以设置一个阈值，在上传缓冲区使用率超过该阈值时，触发向您发送的通知。如果上传缓冲区填充的数据量接近容量，您可以考虑向网关添加更多缓冲区容量。

可在 AWS Storage Gateway 控制台的网关选项卡中看到上传缓冲区百分比用量的当前值。

- 监控卷状态—如果达到上传缓冲区最大容量，则受影响的存储卷进入 [PASS THROUGH](#) (p. 169) 模式，并且尽管应用程序可继续运行，向存储卷写入或从其读取数据，但这段时间内不拍摄快照。
- 优化所处环境—如果传入写入的速度与传出网络带宽相比过高，则无论将上传缓冲区容量配置为多大，网关可能都跟不上该速度。在此情况下，应考虑优化网关以提高性能 ( 请参阅 [优化 AWS Storage Gateway 性能](#) (p. 242) )。

如需...	请执行此操作...
向您的网关添加更多上传缓冲区容量。	按 <a href="#">添加上传缓冲区容量 ( 网关存储 )</a> (p. 184) 中的步骤进行操作。
移除分配为上传缓冲区的磁盘。	按 <a href="#">移除上传缓冲区容量 ( 网关存储 )</a> (p. 184) 中的步骤进行操作。

## 添加和移除上传缓冲区容量 ( 网关存储 )

最初配置网关上传缓冲区 ( 请参阅 [配置上传缓冲区 \( 网关存储 \)](#) (p. 146) ) 后, 可随应用程序需求的变化配置额外的上传缓冲区容量。要详细了解如何根据应用程序需求调整上传缓冲区大小, 请参阅 [配置上传缓冲区的大小 \( 网关存储 \)](#) (p. 104)。

您可以向网关添加更多缓冲区空间, 无需中断现有的网关功能。请注意, 您需要在网关 VM 开启的情况下才能添加更多上传缓冲区容量; 但是减少上传缓冲区容量时, 则必须先关闭 VM。

### 添加上传缓冲区容量 ( 网关存储 )

随着应用程序需求的变化以及更多存储卷空间的添加, 您可能需要增加网关的上传缓冲区容量。可使用 AWS Storage Gateway API ( 请参阅 [AddUploadBuffer](#) ) 或 AWS Storage Gateway 控制台添加更多缓冲区容量。下列步骤介绍了如何使用控制台添加更多缓冲区容量。这些步骤假定您的已激活网关在其 VM 上至少有一个本地磁盘可用, 可供您将其分配为网关的上传缓冲区。

如需使用控制台为网关配置上传缓冲区

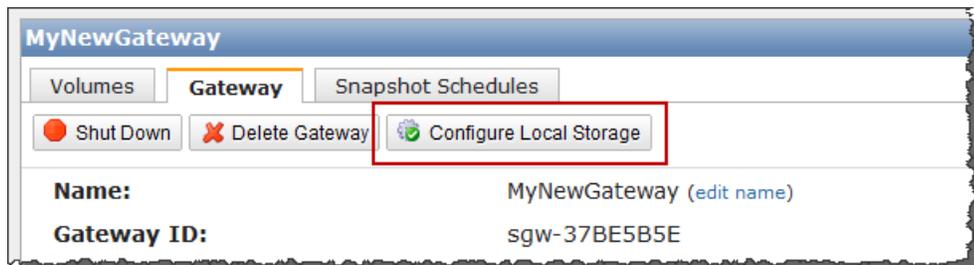
- 按 [如需将本地磁盘配置为网关的上传缓冲区 \(p. 147\)](#) 中的步骤进行操作。

### 移除上传缓冲区容量 ( 网关存储 )

由于应用程序需求的变化以及对网关的存储卷配置的更改, 您可能需要减少网关的上传缓冲区容量。分配到上传缓冲区的本地磁盘也有可能失效, 导致您需要从上传缓冲区移除该磁盘并分配新的本地磁盘。在两种情况下, 均可使用 AWS Storage Gateway 控制台删除更多缓冲区容量。下列步骤假定您已激活的网关至少有一个本地磁盘分配为网关的上传缓冲区。在该过程中, 首先在 AWS Storage Gateway 控制台进行操作, 然后离开控制台, 使用 VMware vSphere 客户端或 Microsoft Hyper-V 管理器删除磁盘, 再返回控制台。

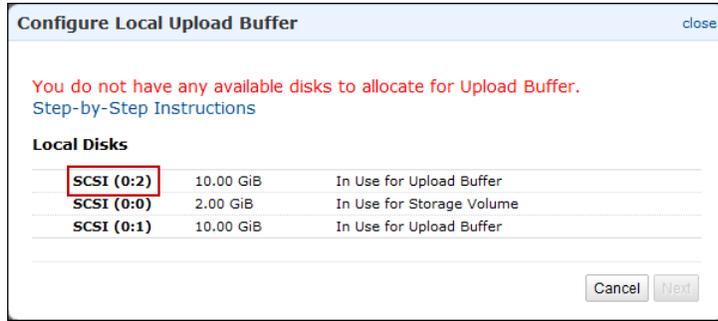
使用控制台查找已分配为上传缓冲区的磁盘 ID

- 在 AWS Storage Gateway 控制台的网关选项卡中, 单击配置本地存储。



- 在配置本地上传缓冲区对话框中, 记下要删除的本地磁盘的虚拟设备节点值。可在本地磁盘列中找到节点值。例如, 在下面的对话框中, 突出显示设备节点 SCSI (0:2)。

您在管理程序客户端中使用磁盘的虚拟设备节点来确保移除了需要移除的磁盘。



- 按使用 [AWS Storage Gateway 控制台](#) 关停并启动网关 (p. 210) 过程中的步骤关闭网关。



#### Note

关停网关前，请确保没有正在向该网关写入数据的应用程序正在使用它，并且没有快照进程。可在控制台的快照计划选项卡上检查存储卷的快照计划。有关更多信息，请参阅 [编辑快照计划](#) (p. 195)。

- 要移除底层本地磁盘，请执行下列操作之一，然后转到下一步：

对于下列托管网关...	请执行此操作...
VMware ESXi	按 <a href="#">删除分配为上传缓冲区的底层磁盘 (VMware ESXi)</a> (p. 185) 中的步骤进行操作。
Microsoft Hyper-V	按 <a href="#">删除分配为上传缓冲区的底层磁盘 (Microsoft Hyper-V)</a> (p. 186) 中的步骤进行操作。

- 在 AWS Storage Gateway 控制台中，打开网关。



#### Important

移除用作上传缓冲区的磁盘后，您必须在向 VM 添加新磁盘前重新开启网关。

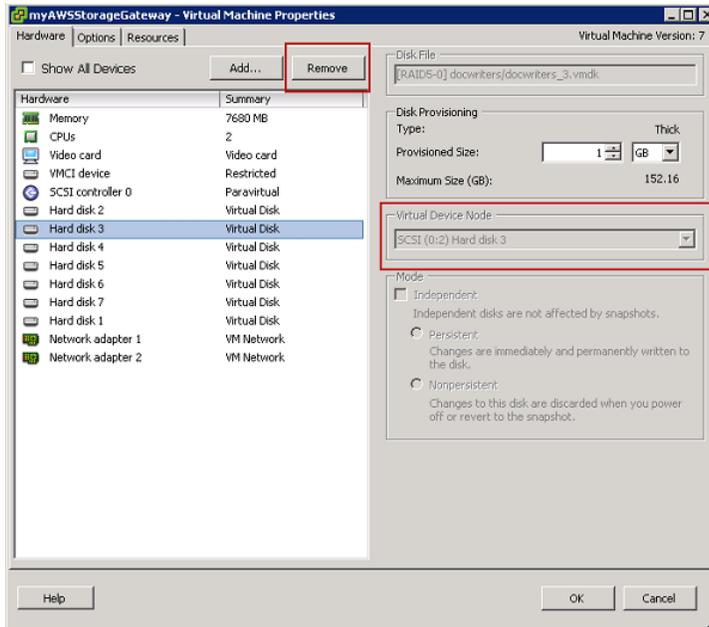
- 在 AWS Storage Gateway 控制台的卷选项卡中，确认所有存储卷的状态均为 [AVAILABLE](#) (p. 169)。

网关重新启动后，存储卷可能在网关适应您删除的上传缓冲区磁盘时经历 [PASS THROUGH](#) (p. 169) 和 [BOOTSTRAPPING](#) (p. 169) 状态。经历这两个状态的存储卷最终将变为 [AVAILABLE](#) (p. 169) 状态。您可以在状态转换以及自举状态的过程中使用存储卷，但不能拍摄快照。

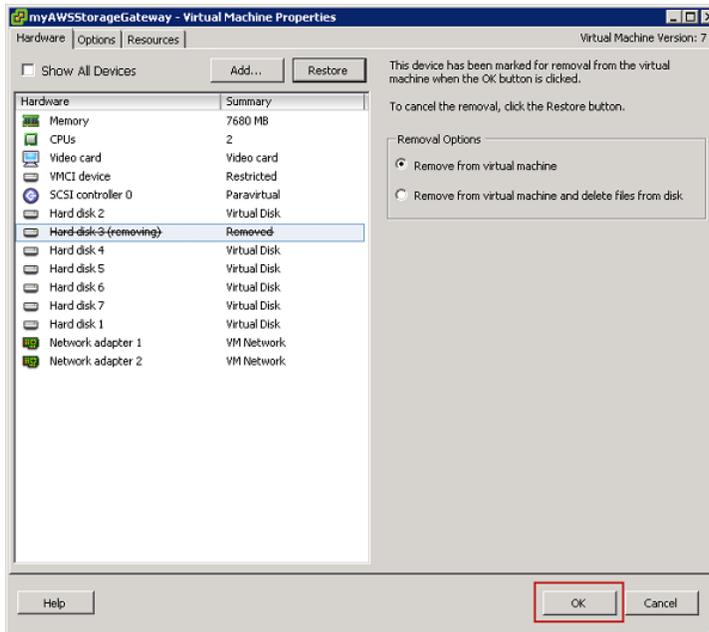
#### 删除分配为上传缓冲区的底层磁盘 (VMware ESXi)

- 在 vSphere 客户端中，右键单击网关 VM 的名称，然后单击编辑设置...
- 在虚拟机属性对话框的硬件选项卡中，选择分配为上传缓冲区的磁盘，然后单击删除。

确认虚拟机属性对话框中的虚拟设备节点值与从上一步中记录的值相同。这样可以确保您移除需要移除的网关。



3. 在删除选项面板中选择一个选项，然后单击确定以完成删除磁盘的过程。

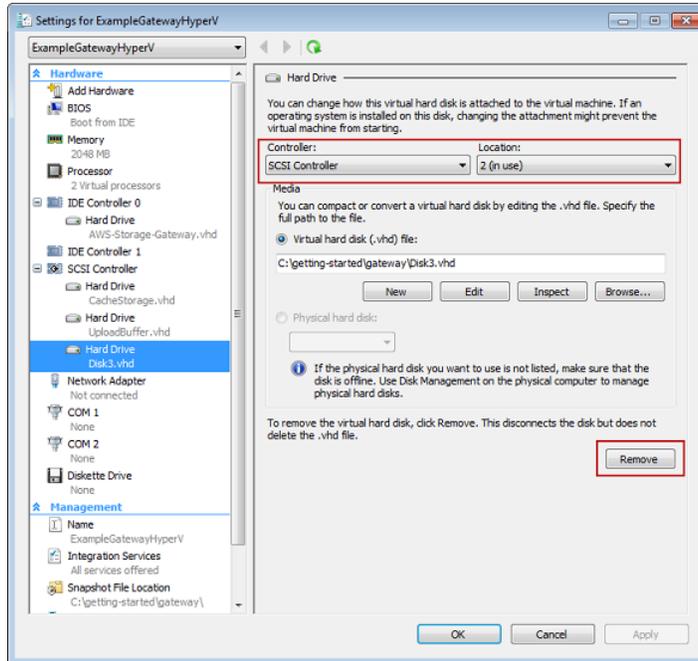


### 删除分配为上传缓冲区的底层磁盘 (Microsoft Hyper-V)

1. 在 Microsoft Hyper-V 管理器中，右键单击网关 VM 的名称，然后单击设置...。
2. 在设置对话框的硬件列表中，选择要删除的磁盘，然后单击删除。

添加到网关的磁盘在硬件列表中的 SCSI 控制器条目下。验证控制器和位置值与上一步中记录的相同。这项操作确保您移除了要移除的磁盘。

在 Microsoft Hyper-V Manager 中显示的第一个 SCSI Controller 是控制器 0。



3. 单击确定以应用更改。

## 使用快照

### Topics

- [概述 \(p. 187\)](#)
- [查找快照 \(p. 188\)](#)
- [编辑快照计划 \(p. 195\)](#)
- [创建临时快照 \(p. 196\)](#)
- [删除快照 \(p. 197\)](#)
- [还原快照 \(p. 205\)](#)

## 概述

AWS Storage Gateway 具有将数据的时间点快照备份到 Amazon S3 的功能，从而获得持久的还原能力，可随后在场内或 Amazon EC2 中使用。您可以按预定或临时方式拍摄快照。本部分中，我们向您介绍可以对快照执行的最常见任务，包括创建快照并将快照还原为随后可作为 iSCSI 设备安装的卷，以及将快照还原为随后可连接到 Amazon EC2 实例的 Amazon EBS 卷。

AWS Storage Gateway 将数据持续异步上传到 AWS，以便让您的本地数据与存储在 AWS 中的副本保持同步。这样做的好处是快照开始拍摄时，部分或所有数据已经上传，并且快照可快速完成。此外，快照是增量的。亦即，网关仅上传自上次快照拍摄以来您的卷中发生变化的数据块。例如，如果您有 100 GiB 的数据且自上次快照拍摄以来仅有 5 GiB 数据发生变化，那么网关仅上传发生变化的 5 GiB 数据。您可以删除任何快照。AWS Storage Gateway 仅移除其他快照不需要的快照数据，以便您能够从任一活动快照还原卷。

快照在 AWS Storage Gateway 设置中的有效使用方式取决于您设置的网关类型，亦即网关缓存或网关存储架构（请参见 [AWS Storage Gateway 的运行原理（架构）\(p. 3\)](#)）

- 对于网关缓存卷，您的卷数据已存储在 Amazon S3 中，因此快照可用来保存数据的旧版本。

- 对于网关存储卷，您的卷数据在场内存储，因此快照提供 Amazon S3 中的持久异地备份。

## 快照任务摘要

由于快照对于 AWS Storage Gateway 服务的使用非常重要，您应该在宏观层面理解每个快照操作的内容以及执行原因。每项任务在连接部分均有详述。

如需执行任务，您应该有已运行了足够时间的一个或多个网关，以便有快照可用。您可以借助 AWS Storage Gateway 控制台、AWS 软件开发工具包 (SDK) 或 AWS Storage Gateway REST API 使用快照（请参见 [AWS Storage Gateway 中的操作 \(p. 438\)](#)）。本部分中，我们主要介绍如何利用控制台执行网关任务。

快照操作	常见场景
查找	建议您查找快照，确认其是否已完成、拍摄于何时、快照大小，或者快照所从拍摄的卷的名称。有关更多信息，请参见 <a href="#">查找快照 (p. 188)</a> 。
计划设定	首次设置存储卷时，默认计划设定为每天拍摄一次。您可以更改拍摄频率和快照计划的时间安排，以便满足您的应用程序需求。有关更多信息，请参见 <a href="#">编辑快照计划 (p. 195)</a> 。
创建	存储卷的快照默认按计划拍摄，您可以修改快照计划。不过，您也可以随时对存储和缓存卷随拍摄即时快照。有关更多信息，请参见 <a href="#">创建临时快照 (p. 196)</a> 。
还原	您可以将快照本地还原为新的 AWS Storage Gateway 卷，也可以用快照来创建 Amazon Elastic Block Store (EBS) 卷并将其连接到 Amazon EC2 实例。有关更多信息，请参见 <a href="#">将快照还原为 AWS Storage Gateway 卷 (p. 206)</a> 和 <a href="#">将快照还原为 Amazon EBS 卷 (p. 208)</a> 。
删除	如果您不再需要快照，可将其删除。由于快照是增量备份，删除某个快照的操作仅删除其他快照不需要的数据。有关更多信息，请参见 <a href="#">删除快照 (p. 197)</a> 。

## 快照一致性

快照提供已写入 AWS Storage Gateway 卷的数据的时间点视图。不过，快照仅抓取已写入存储卷的数据，可能会排除客户端应用程序或操作系统已缓冲的数据。您的应用程序和操作系统最终会将这些缓存数据刷新到存储卷。如果您需要确保应用程序数据已在快照拍摄前刷新到磁盘，应查询具体应用程序的文档以理解应用程序是否以及如何缓冲数据，以及如何刷新这些数据。如果您需要在快照拍摄前确保操作系统和文件系统已将缓冲的数据刷新到磁盘，可在拍摄快照前让存储卷脱机，从而做到这一点。这样可以确保您的操作系统已将数据刷新到磁盘。快照完成后，您可以让卷重新联机。在 Windows 中，使用磁盘管理 (diskmgmt.msc) 来选中存储卷并让其联机或脱机。若要在 Windows 中执行该过程的脚本，您可以使用命令行工具，例如 [Diskpart.exe](#)。在 Linux 中，使用 `mount` 和 `umount` 命令。

## 查找快照

希望将快照还原为新卷时，您需要查找与卷关联的快照（例如在灾难恢复场景中），或者还原应用程序数据的上一版本。如需还原快照，您需要知道其快照 ID。有数种方法可用来查找快照 ID，包括使用 AWS Storage Gateway 控制台、Amazon Elastic Compute Cloud (EC2) 控制台，或者用 AWS 软件开发工具包 (SDK) 以编程方式查找。

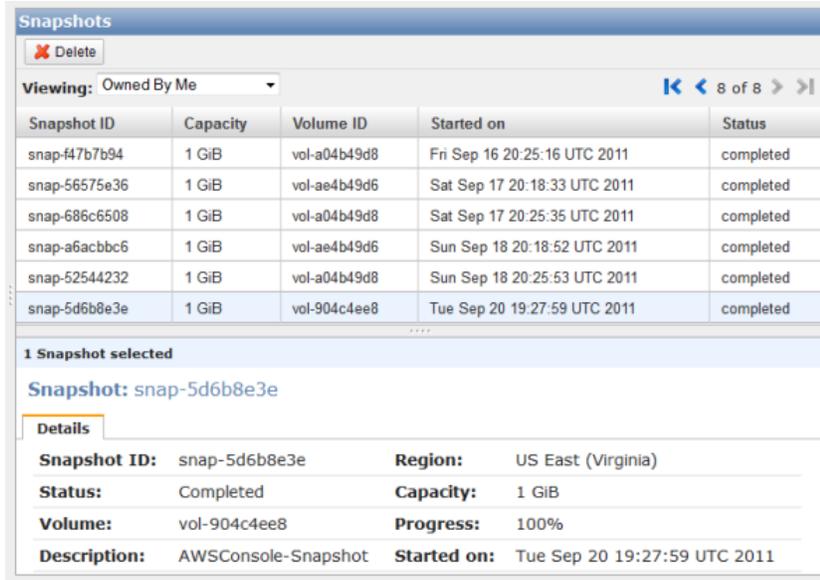
如果您使用 AWS Storage Gateway 列出快照，列表将包括由网关生成的所有快照以及您可能从 Amazon Elastic Block Storage (EBS) 卷生成的快照。如果您在 Amazon EC2 控制台中列出快照，会有更多的快照属性显示出来，以帮助您查找快照和搜索筛选条件功能。两种控制台的体验描述如下。在某些场景中，您可能需要同时使用数种快照属性进行搜索，例如状态、起始日期和描述。在本例中，您可以使用编程方法。有关示例，请参见 [使用适用于 Java 的 AWS 软件开发工具包查找快照 \(p. 190\)](#)、[使用适用于 .NET 的 AWS 软件开发工具包查找快照 \(p. 192\)](#) 或 [使用适用于 Windows PowerShell 的 AWS 工具查找快照 \(p. 194\)](#)。

找到快照后，您可以查看器详细信息，包括快照起始日期和时间以及快照所从创建的网关存储卷。

如需使用 AWS Storage Gateway 控制台查找卷的快照

1. 在 AWS 存储网关控制台的导航窗格中，单击快照。

快照窗口显示您的快照列表。



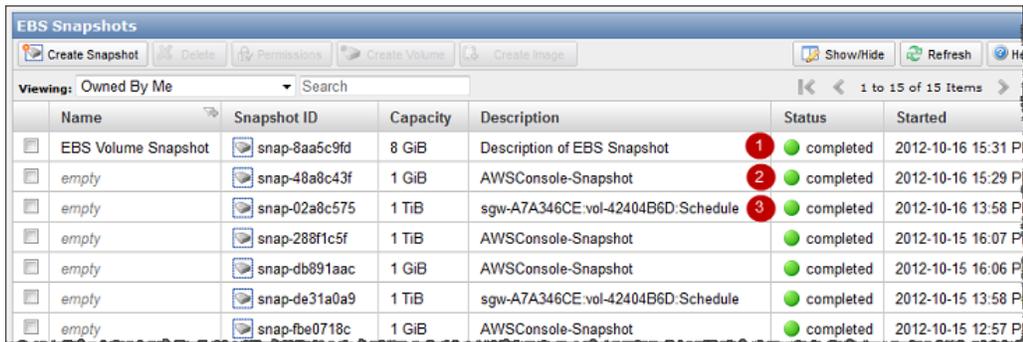
2. 在卷 ID 栏中查找卷 ID，从而在列表中找到您查找的快照。
3. 单击快照行以显示快照详细信息。

如需使用 Elastic Block Store 控制台找到卷的快照

1. 在 Amazon EC2 Management 控制台的导航窗格中，单击弹性块存储下的快照。

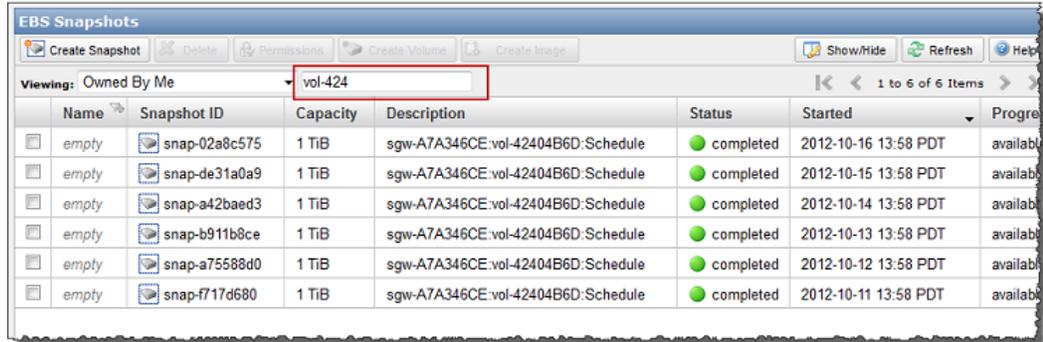
EBS 快照窗口显示您的快照列表。此快照视图提供查找快照的更多功能。具体而言，该视图显示可用来筛选结果的描述，例如，其中有您可以用来协助查找快照的模式。例如，在下面的控制台图像中

- 标记为 1 的行是从 EBS 卷拍摄的快照。名称和描述字段在快照创建过程中指定。该快照并非创建自 AWS Storage Gateway 操作。
- 标记为 2 的行是从 AWS Storage Gateway 控制台拍摄的临时快照。临时快照的描述包含“AWSConsole-Snapshot”。
- 标记为 3 的行是 AWS Storage Gateway 按快照计划拍摄的卷快照。预定快照的描述提供存储网关 ID、卷 ID 以及模式“*gatewayID:volumeID:Schedule*”中的词语“Schedule”。



2. 将部分或全部卷 ID 键入搜索字段，从而在列表中找到您查找的快照。

在下面的实例中，仅显示包含“vol-424”的结果。您可以在 AWS Storage Gateway 控制台中的卷选项卡找到卷 ID。



3. 单击快照行以显示快照详细信息。

### 使用适用于 Java 的 AWS 软件开发工具包查找快照

您可以使用编程方法快速查找快照，并使用快照状况、描述和快照创建日期等快照属性筛选返回的结果。以下示例展示了如何借助数种快照属性，使用适用于 Java 的 AWS 软件开发工具包查找快照。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，请参见“适用于 Java 的 AWS 软件开发工具包开发人员指南”中的入门部分。

**Example :使用适用于 Java 的 AWS 软件开发工具包查找快照**

以下 Java 代码示例使用快照的数种属性筛选返回的结果，查找指定网关卷的快照。该示例使用适用于 Java 的 AWS 软件开发工具包和 Amazon Elastic Compute Cloud (EC2) API。Amazon EC2 API 包括使用快照的数种操作。

您需要更新代码并提供服务终端节点、完整的或部分卷 ID、快照状况和天数来指明快照返回的截止日期。有关可用于 Amazon EC2 的 AWS 服务终端部分点的列表，请查看“Amazon Web Services 术语表”中的[地区和终端部分点部分](#)。

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

import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.PropertiesCredentials;
import com.amazonaws.services.ec2.AmazonEC2Client;
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;

public class FindingSnapshotsExample {

    static AmazonEC2Client ec2Client;
    // A full volume id or partial fragment with "*".
    static String volumeID = "vol-424*";
    // Snapshot status to filter on: "completed", "pending", "error".
    static String status = "completed";
    // The number of days before which to not return snapshot results.
    static int daysBack = 10;
    // Service end point. Should be same region as volume/gateway.
    public static String serviceURLEC2 = "https://ec2.us-east-1.amazonaws.com";

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

        ec2Client = new AmazonEC2Client(new PropertiesCredentials(
            FindingSnapshotsExample.class.getResourceAsStream("AwsCreden
tials.properties")));
        ec2Client.setEndpoint(serviceURLEC2);

        FindingSnapshotsForAVolume();

    }

    private static void FindingSnapshotsForAVolume() {

        try {
            Filter[] filters = new Filter[2];
            filters[0] = new Filter().withName("volume-id").withValues(volumeID);

            filters[1] = new Filter().withName("status").withValues(status);

            DescribeSnapshotsRequest describeSnapshotsRequest =
```

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

List<Snapshot> snapshots = describeSnapshotResult.getSnapshots();
System.out.println("volume-id = " + volumeID);
for (Snapshot s : snapshots) {
    if (CompareDates(daysBack, s.getStartTimestamp())) {
        StringBuilder sb = new StringBuilder();
        sb.append(s.getSnapshotId() + ", " + s.getStartTimestamp() + ", "
            + s.getDescription());
        System.out.println(sb.toString());
    }
}
} catch (AmazonClientException ace) {
    System.err.println(ace.getMessage());
}
}

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 查找快照

您可以使用编程方法快速查找快照，并使用快照状况、描述和快照创建日期等快照属性筛选返回的结果。以下示例展示了如何借助数种快照属性，使用适用于 .NET 的 AWS 软件开发工具包查找快照。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，请参见“适用于 .NET 的 AWS 软件开发工具包开发人员指南”中的[入门](#)部分。

**Example :使用适用于 .NET 的 AWS 软件开发工具包 查找快照**

以下 C# 代码示例使用快照的数种属性筛选返回的结果，查找指定网关卷的快照。该示例使用适用于 .NET 的 AWS 软件开发工具包和 Amazon Elastic Compute Cloud (EC2) API。Amazon EC2 API 包括使用快照的数种操作。

您需要更新代码并提供服务终端节点、完整的或部分卷 ID、快照状况和天数来指明快照返回的截止日期。有关可用于 Amazon EC2 的 AWS 服务终端部分点的列表，请查看“Amazon Web Services 术语表”中的[地区和终端部分点部分](#)。

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

namespace AWSStorageGateway
{
    class FindingSnapshotsExample
    {
        static AmazonEC2Config ec2Config;
        static AmazonEC2Client ec2Client;
        // A full volume id or partial fragment with "*".
        static String volumeID = "vol-424*";
        // Snapshot status to filter on: "completed", "pending", "error".
        static String status = "completed";
        // The number of days before which to not return snapshot results.
        static int daysBack = 4;
        // Service endpoint. Should be same region as volume/gateway.
        static String serviceURLEC2 = "https://ec2.us-east-1.amazonaws.com";

        public static void Main(string[] args)
        {
            //Create a ec2 client
            ec2Config = new AmazonEC2Config();
            ec2Config.ServiceURL = serviceURLEC2;
            ec2Client = new AmazonEC2Client(ec2Config);

            FindingSnapshotsForAVolume();

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

        private static void FindingSnapshotsForAVolume()
        {
            try
            {
                Filter[] filters = new Filter[2];
                filters[0] = new Filter().WithName("volume-id").With
Value(volumeID);
                filters[1] = new Filter().WithName("status").WithValue(status);

                DescribeSnapshotsRequest describeSnapshotsRequest =
                    new DescribeSnapshotsRequest().WithFilter(filters);
                DescribeSnapshotsResponse describeSnapshotsResponse =
```

```
        ec2Client.DescribeSnapshots(describeSnapshotsRequest);

        List<Snapshot> snapshots = describeSnapshotsResponse.Describe
SnapshotsResult.Snapshot;
        Console.WriteLine("volume-id = " + volumeID);
        foreach (Snapshot s in snapshots)
        {
            if (CompareDates(daysBack, s.StartTime))
            {
                StringBuilder sb = new StringBuilder();
                sb.Append(s.SnapshotId + ", " + s.StartTime + ", " +
s.Description);
                Console.WriteLine(sb.ToString());
            }
        }
    }
    catch (AmazonEC2Exception ex)
    {
        Console.WriteLine(ex.Message);
    }
}

public static Boolean CompareDates(int daysBack, String d)
{
    DateTime snapshotDate = DateTime.Parse(d);
    DateTime cutoffDate = DateTime.Now.Add(new TimeSpan(-daysBack, 0,
0, 0));
    return (DateTime.Compare(snapshotDate, cutoffDate) < 0) ? true :
false;
}
}
```

## 使用适用于 Windows PowerShell 的 AWS 工具查找快照

您可以使用编程方法快速查找快照，并使用快照状况、描述和快照创建日期等快照属性筛选返回的结果。以下示例展示了如何借助数种快照属性，使用适用于 Windows PowerShell 的 AWS 工具查找快照。如需使用示例代码，您应该熟悉 PowerShell 脚本控制台应用程序的运行方式。有关更多信息，请参见“适用于 Windows PowerShell 的 AWS 工具用户指南”中的[入门](#)部分。

### Example :使用适用于 Windows PowerShell 的 AWS 工具查找快照

以下 PowerShell 脚本示例使用数种快照属性筛选返回的结果，查找指定网关卷的快照。该示例使用适用于 Windows PowerShell 的 AWS 工具和 Amazon Elastic Compute Cloud (EC2) Cmdlet。Amazon EC2 Cmdlet 包括快照相关操作。

您需要更新脚本并提供完整的或部分卷 ID、快照状况和天数来指明返回快照的截止日期。

```
<# .DESCRIPTION Finds snapshots for a given volume and criteria about the
snapshot. .NOTES PREREQUISITES: 1) AWS Tools for PowerShell from ht
tp://aws.amazon.com/powershell/ 2) Credentials and region stored in session
using Initialize-AWSDefault. For more info, see http://docs.aws.amazon.com/power
shell/latest/userguide/specifying-your-aws-credentials.html .EXAMPLE power
shell.exe .\SG_FindSnapshots.ps1 #> # Criteria to use to filter the results
returned. $volumeID = "vol-424*" $status = "completed" $daysBack = 4 # Define
filters. $filter1 = New-Object Amazon.EC2.Model.Filter $filter1.Name = "volume-
id" $filter1.Value.Add($volumeID) $filter2 = New-Object Amazon.EC2.Model.Filter
$filter2.Name = "status" $filter2.Value.Add($status) $snapshots = get-
EC2Snapshot -Filter $filter1, $filter2 $count = 0 foreach ($s in $snapshots) {
  $d = ([DateTime]::Now).AddDays(-$daysBack) if ([DateTime]::Compare($d,
$s.StartTime) -gt 0) { # Meets criteria. $count +=1 $sb = $s.SnapshotId + ", "
  + $s.StartTime + ", " + $s.Description Write-Output($sb) } } Write-Output
("Found " + $count + " snapshots that matched the criteria.")
```

## 编辑快照计划

对于网关存储卷，AWS Storage Gateway 创建一天一次的默认快照计划。这样可以确保您的网关可跟上对本地存储卷的传入写入的速率。您可以更改默认的快照计划，例如通过制定快照每天的创建时间和频率（每 1、2、4、8、12 或 24 个小时）。

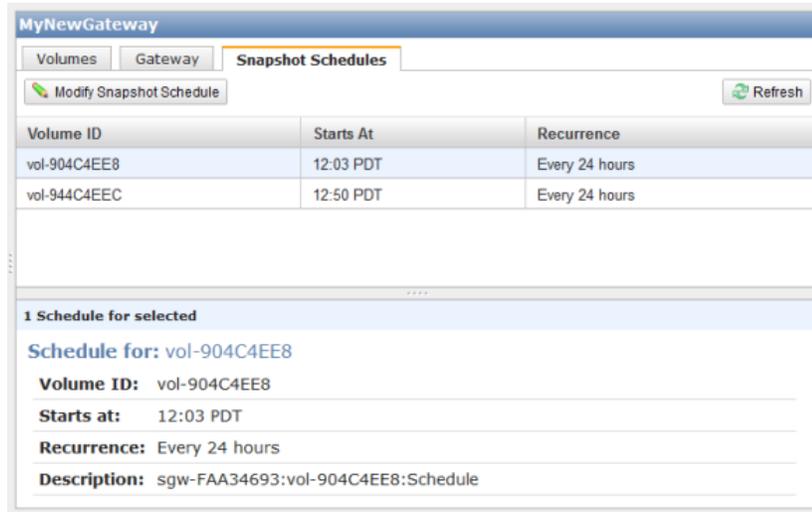
对于网关缓存卷，AWS Storage Gateway 并不创建默认快照计划；不过，您在需要的情况下可随时设置快照计划。对于网关缓存卷而言，由于您的数据存储于 Amazon S3 中，就无需用于灾难恢复用途的快照（以及快照计划）。

在下列步骤中，我们向您介绍如何编辑卷的快照计划。

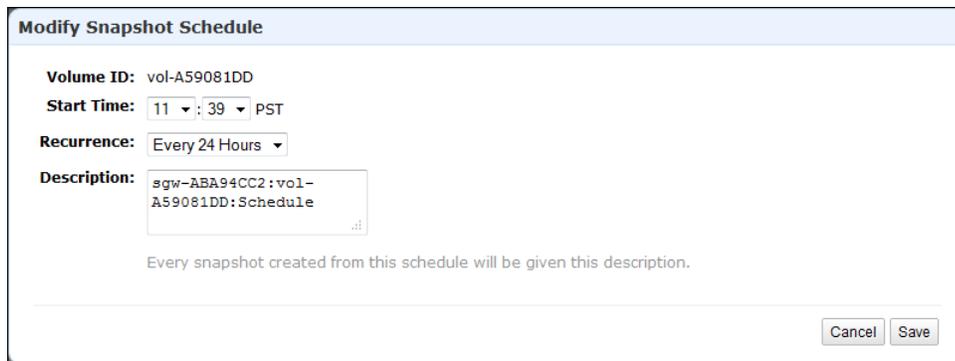
### 如需编辑快照计划

1. 在AWS 存储网关控制台中，选定包含您希望编辑的卷快照计划的网关。
2. 单击快照计划选项卡。

该选项卡显示选定网关上的存储卷列表。



3. 选择一个卷。  
AWS Storage Gateway 显示该卷的快照计划详情。
4. 单击修改快照计划。



5. 在修改快照计划对话框中，按需更新计划字段。例如，您可以提高默认为一天一次的快照频率或更改快照拍摄时间。
6. 单击保存以保存快照计划更新。

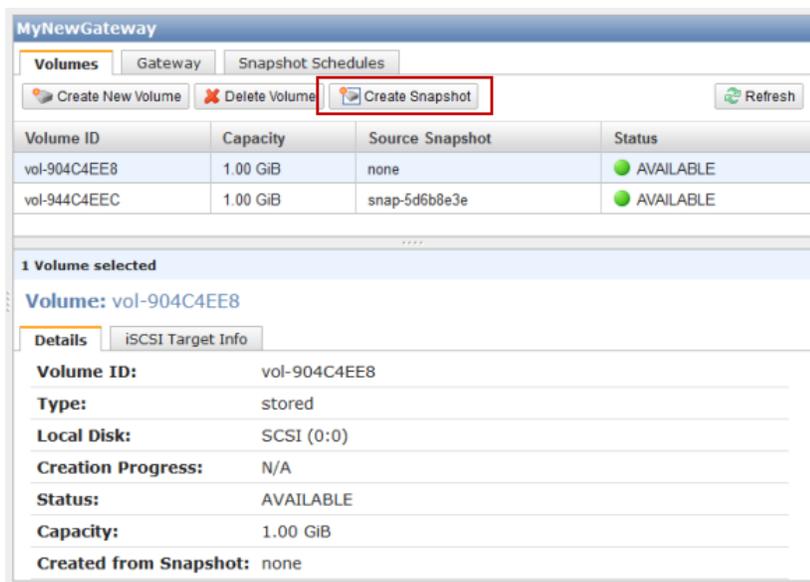
## 创建临时快照

除预定快照外，AWS Storage Gateway 还允许您拍摄临时快照，以便您立即备份存储卷，而无需等待下次预定快照。

如需拍摄存储卷的临时快照

1. 在AWS 存储网关控制台中，选择包含要拍摄快照的存储卷的网关。
2. 单击卷选项卡。
3. 从该列表中选择一个卷，然后单击创建快照。

AWS Storage Gateway 立即开始快照拍摄过程。



4. 在控制台验证快照。有关更多信息，请参见 [查找快照](#) (p. 188)。

## 删除快照

### Topics

- [使用适用于 Java 的 AWS 软件开发工具包删除快照](#) (p. 198)
- [使用适用于 .NET 的 AWS 软件开发工具包删除快照](#) (p. 201)
- [使用适用于 Windows PowerShell 的 AWS 工具删除快照](#) (p. 204)

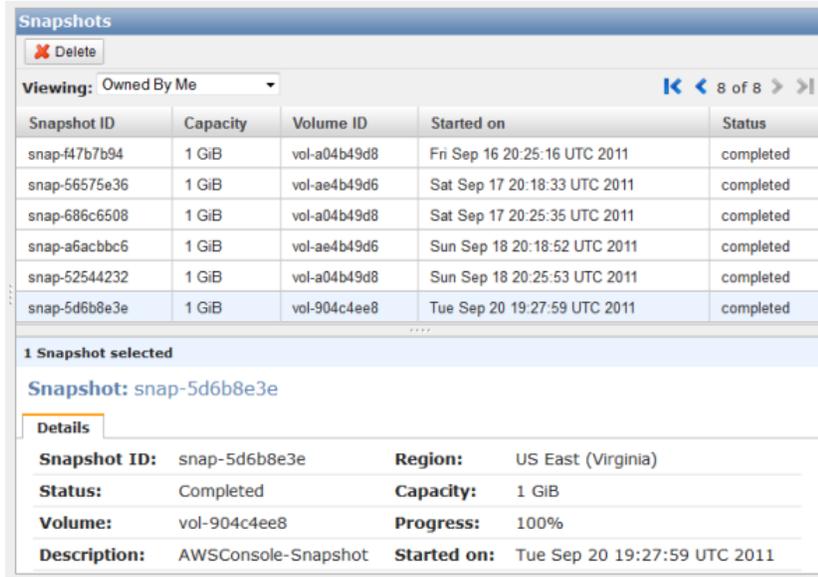
举例而言，如果您在一段时间内拍摄了存储卷的多个快照且不再需要较旧的快照，您可能希望删除快照。由于快照是增量备份，删除某个快照的操作仅删除其他快照不需要的数据。

在 AWS Storage Gateway 控制台中，您逐次逐个删除快照。如需删除多个快照，请使用支持 AWS Storage Gateway 操作的 AWS 软件开发工具包。有关示例，请参见 [使用适用于 Java 的 AWS 软件开发工具包删除快照](#) (p. 198)、[使用适用于 .NET 的 AWS 软件开发工具包删除快照](#) (p. 201) 或 [使用适用于 Windows PowerShell 的 AWS 工具删除快照](#) (p. 204)。

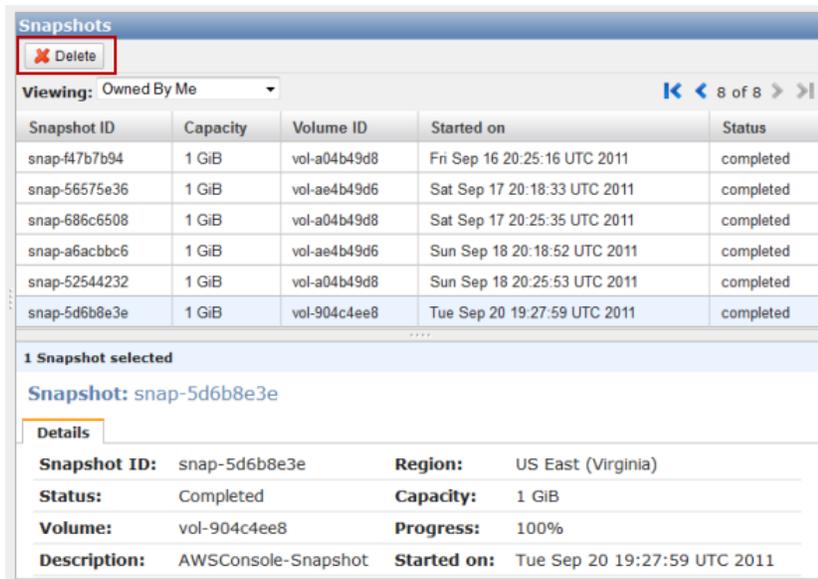
### 如需使用控制台删除快照

1. 在 AWS Storage Gateway 控制台中，在导航窗格中单击快照。

快照列表显示在窗格中。



- 选中要删除的快照并单击删除。



- 单击确定以确认您要删除快照。

## 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。以下示例展示了如何使用适用于 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，请参见“适用于 Java 的 AWS 软件开发工具包开发人员指南”中的入门部分。如果您只需删除少量快照，请按 [如需使用控制台删除快照 \(p. 197\)](#) 中所述使用控制台。

**Example :使用适用于 Java 的 AWS 软件开发工具包删除快照**

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。该示例使用适用于 Java 的 AWS 软件开发工具包和 AWS Storage Gateway 以及 Amazon Elastic Compute Cloud (EC2) API。Amazon EC2 API 包括使用快照的多种操作。

您需要更新代码并提供服务终端部分点、网关的亚马逊资源名称 (ARN) 以及快照将被删除前的天数。您还需要指定布尔 `viewOnly`，表明是否要查看将被删除的内容或是否要实际执行快照删除。您需要仅利用查看选项先运行代码 (`viewOnly` 设置为 `true`) 以查看代码将删除什么内容。有关您可用于 AWS Storage Gateway 的 AWS 服务终端部分点，请参见“Amazon Web Services 术语表”中的[地区和终端部分点](#)部分。

```
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().to
String());

```

```

        sb.append(", meets criteria for delete? " + meetsCriteria);
        sb.append(", deleted? ");
        if (!viewOnly & meetsCriteria) {
            sb.append("yes");
            DeleteSnapshotRequest deleteSnapshotRequest =
                new DeleteSnapshotRequest().withSnapshotId(s.getSnap
shotId());
            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。以下示例展示了如何使用适用于 .NET 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 .NET 控制台应用程序的运行方式。有关更多信息，请参见“适用于 .NET 的 AWS 软件开发工具包开发人员指南”中的[入门](#)部分。如果您只需删除少量快照，请按[如需使用控制台删除快照 \(p. 197\)](#)中所述使用控制台。

**Example :使用适用于 .NET 的AWS 软件开发工具包删除快照**

以下 C# 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。该示例使用适用于 .NET 的 AWS 软件开发工具包和 AWS Storage Gateway 以及 Amazon Elastic Compute Cloud (EC2) API。Amazon EC2 API 包括使用快照的多种操作。

您需要更新代码并提供服务终端部分点、网关的亚马逊资源名称 (ARN) 以及快照将被删除前的天数。您还需要指定布尔 `viewOnly`，表明是否要查看将被删除的内容或是否要实际执行快照删除。您需要仅利用查看选项先运行代码 (`viewOnly` 设置为 `true`) 以查看代码将删除什么内容。有关您可用于 AWS Storage Gateway 的 AWS 服务终端部分点，请参见“Amazon Web Services 术语表”中的[地区和终端部分点](#)部分。

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

namespace AWSStorageGateway
{
    class ListDeleteVolumeSnapshotsExample
    {
        static AmazonStorageGatewayClient sgClient;
        static AmazonStorageGatewayConfig sgConfig;
        static AmazonEC2Config ec2Config;
        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)
        {
            // Create a storage gateway client
            sgConfig = new AmazonStorageGatewayConfig();
            sgConfig.ServiceURL = serviceURLSG;
            sgClient = new AmazonStorageGatewayClient(sgConfig);

            //Create a ec2 client
            ec2Config = new AmazonEC2Config();
            ec2Config.ServiceURL = serviceURLEC2;
            ec2Client = new AmazonEC2Client(ec2Config);

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

```

        Console.WriteLine("\nTo continue, press Enter.");
        Console.Read();
    }
    public static List<VolumeInfo> ListVolumesForGateway()
    {
        ListVolumesRequest request = new ListVolumesRequest().WithGatewayARN(gatewayARN);
        ListVolumesResponse response = sgClient.ListVolumes(request);
        ListVolumesResult volumes = response.ListVolumesResult;

        foreach (VolumeInfo vi in volumes.VolumeInfos)
        {
            Console.WriteLine(OutputVolumeInfo(vi));
        }

        return volumes.VolumeInfos;
    }

    public static void DeleteSnapshotsForVolumes(List<VolumeInfo> volumes,
        int cutoffDays)
    {
        foreach (VolumeInfo vi in volumes)
        {
            String volumeARN = vi.VolumeARN;
            String volumeId = volumeARN.Substring(volumeARN.LastIndexOf("/")
+ 1).ToLower();
            Filter[] filters = new Filter[1];
            filters[0] = new Filter().WithName("volume-id").WithValue(volumeId);

            DescribeSnapshotsRequest describeSnapshotsRequest =
                new DescribeSnapshotsRequest().WithFilter(filters);
            DescribeSnapshotsResponse describeSnapshotsResponse =
                ec2Client.DescribeSnapshots(describeSnapshotsRequest);

            List<Snapshot> snapshots = describeSnapshotsResponse.DescribeSnapshotsResult.Snapshot;
            Console.WriteLine("volume-id = " + volumeId);
            foreach (Snapshot s in snapshots)
            {
                StringBuilder sb = new StringBuilder();
                Boolean meetsCriteria = CompareDates(daysBack, s.StartTime);

                sb.Append(s.SnapshotId + ", " + s.StartTime);
                sb.Append(", meets criteria for delete? " + meetsCriteria);

                sb.Append(", deleted? ");
                if (!viewOnly & meetsCriteria)
                {
                    sb.Append("yes");
                    DeleteSnapshotRequest deleteSnapshotRequest =
                        new DeleteSnapshotRequest().WithSnapshotId(s.SnapshotId);
                    ec2Client.DeleteSnapshot(deleteSnapshotRequest);
                }
                else
                {

```

```
        sb.Append("no");
    }
    Console.WriteLine(sb.ToString());
}

}

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;
}

public static Boolean CompareDates(int daysBack, String d)
{
    DateTime snapshotDate = DateTime.Parse(d);
    DateTime cutoffDate = DateTime.Now.Add(new TimeSpan(-daysBack, 0,
0, 0));
    return (DateTime.Compare(snapshotDate, cutoffDate) < 0) ? true :
false;
}

}

}
```

## 使用适用于 Windows PowerShell 的 AWS 工具删除快照

如需删除与卷关联的多个快照，您可以使用编程方法。以下示例展示了如何使用适用于 Windows PowerShell 的 AWS 工具删除快照。如需使用示例脚本，您应该熟悉如何运行 Powershell 脚本。有关更多信息，请参见“适用于 Windows PowerShell 的 AWS 工具”中的[入门](#)部分。如果您只需要删除少量快照，请按[如需使用控制台删除快照 \(p. 197\)](#)中所述使用控制台。

### Example :使用适用于 Windows PowerShell 的 AWS 工具删除快照

以下 PowerShell 脚本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。该示例使用适用于 Windows PowerShell 的 AWS 工具和 AWS Storage Gateway 和 Amazon Elastic Compute Cloud (Amazon EC2) Cmdlet。Amazon EC2 API 包括使用快照的多种操作。

您需要更新脚本并提供服务终端部分点、网关的亚马逊资源名称 (ARN) 以及快照将被删除前的天数。您还需要指定布尔 `viewOnly`，表明是否要查看将被删除的内容或是否要实际执行快照删除。您需要仅利用查看选项先运行代码 (`viewOnly` 设置为 `true`) 以查看代码将删除什么内容。

```
<# .DESCRIPTION Delete Snapshots of a specified volume that match given criteria.
.NOTES PREREQUISITES: 1) AWS Tools for PowerShell from http://aws.amazon.com/powershell/ 2) Credentials and region stored in session
using Initialize-AWSDefault. For more info see, http://docs.aws.amazon.com/power
shell/latest/userguide/specifying-your-aws-credentials.html .EXAMPLE power
shell.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 = $volumesResult.VolumeInfos Write-Output("`nVolume List") foreach
($vi in $volumes) { Write-Output("`nVolume Info:") Write-Output("ARN: " +
$vi.VolumeARN) write-Output("Type: " + $vi.VolumeType) } Write-Output("`nWhich
snapshots meet the criteria?") foreach ($vi in $volumes) { $volumeARN =
$vi.VolumeARN $volumeId = $volumeARN.Substring($volumeARN.LastIndexOf("/")+1).To
Lower() $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 = $false if ([Date
Time]::Compare($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) } }
```

## 还原快照

### Topics

- [将快照还原为 AWS Storage Gateway 卷 \(p. 206\)](#)
- [将快照还原为 Amazon EBS 卷 \(p. 208\)](#)

您可以将卷的快照还原为新的 AWS Storage Gateway 卷，也可以使用快照创建 Amazon Elastic Block Store (EBS) 卷并将该卷连接到 Amazon EC2 实例。将快照还原为新的 AWS Storage Gateway 卷后，您可以将该卷作为 AWS Storage Gateway 卷设备安装到场内应用程序服务器并在创建新卷时访问该快照类似的内容。

还原快照的使用案例取决于您设置的网关类型（请参见 [AWS Storage Gateway 的运行原理（架构）](#) (p. 3)）。

- 对于网关缓存卷，您的卷数据以存储在 Amazon S3 中，因此快照一般用来保存数据的较旧版本。在快照还原为网关缓存卷的过程开始后，快照数据仅在首次访问数据时下载到本地缓存。
- 对于网关存储卷，您的卷数据在场内存储，因此快照提供 Amazon S3 中的持久异地备份。例如，如果分配为存储卷的本地磁盘崩溃，您可以配置新的本地磁盘并在卷的创建过程中将快照还原到该磁盘（请参见 [创建存储卷（网关存储）](#) (p. 151)）。

在快照还原为网关缓存卷的过程开始后，快照数据在后台下载。也就是说，在您从快照创建卷后，无需等到所有数据从 Amazon S3 传输到您的卷，您的应用程序即可访问卷及其所有数据。如果您的应用程

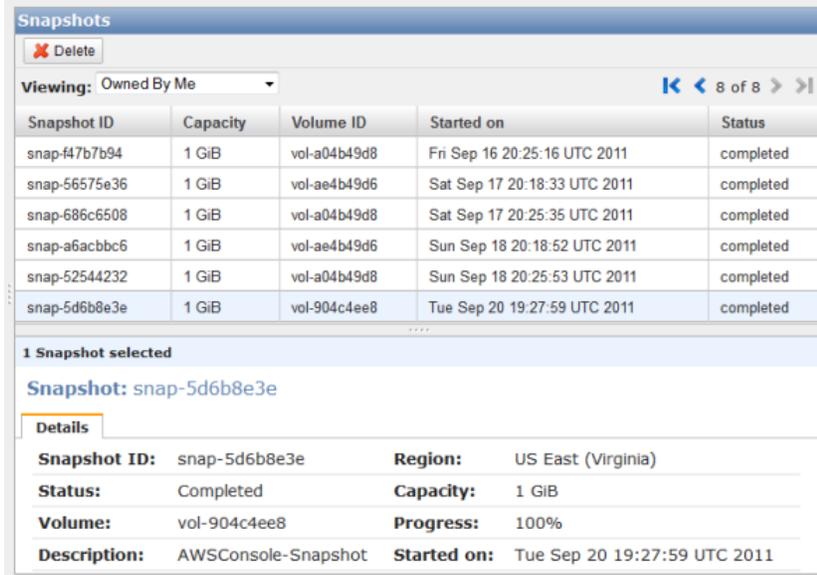
序访问了尚未装载的某个数据，网关就会立即从 Amazon S3 下载请求的数据，然后继续后台装载卷的其余数据。

## 将快照还原为 AWS Storage Gateway 卷

下列步骤适用于网关缓存和网关存储卷。

如需从现有快照创建卷

1. 在 AWS Storage Gateway 控制台中，单击快照。



The screenshot shows the AWS Storage Gateway Snapshots console. At the top, there is a 'Delete' button and a 'Viewing: Owned By Me' dropdown. Below this is a table of snapshots with columns for Snapshot ID, Capacity, Volume ID, Started on, and Status. The selected snapshot is 'snap-5d6b8e3e'. Below the table, the details for this snapshot are shown, including its ID, Region (US East (Virginia)), Status (Completed), Capacity (1 GiB), Volume (vol-904c4ee8), Progress (100%), and Description (AWSConsole-Snapshot).

Snapshot ID	Capacity	Volume ID	Started on	Status
snap-f47b7b94	1 GiB	vol-a04b49d8	Fri Sep 16 20:25:16 UTC 2011	completed
snap-56575e36	1 GiB	vol-ae4b49d6	Sat Sep 17 20:18:33 UTC 2011	completed
snap-686c6508	1 GiB	vol-a04b49d8	Sat Sep 17 20:25:35 UTC 2011	completed
snap-a6acb6c6	1 GiB	vol-ae4b49d6	Sun Sep 18 20:18:52 UTC 2011	completed
snap-52544232	1 GiB	vol-a04b49d8	Sun Sep 18 20:25:53 UTC 2011	completed
snap-5d6b8e3e	1 GiB	vol-904c4ee8	Tue Sep 20 19:27:59 UTC 2011	completed

**1 Snapshot selected**

**Snapshot: snap-5d6b8e3e**

**Details**

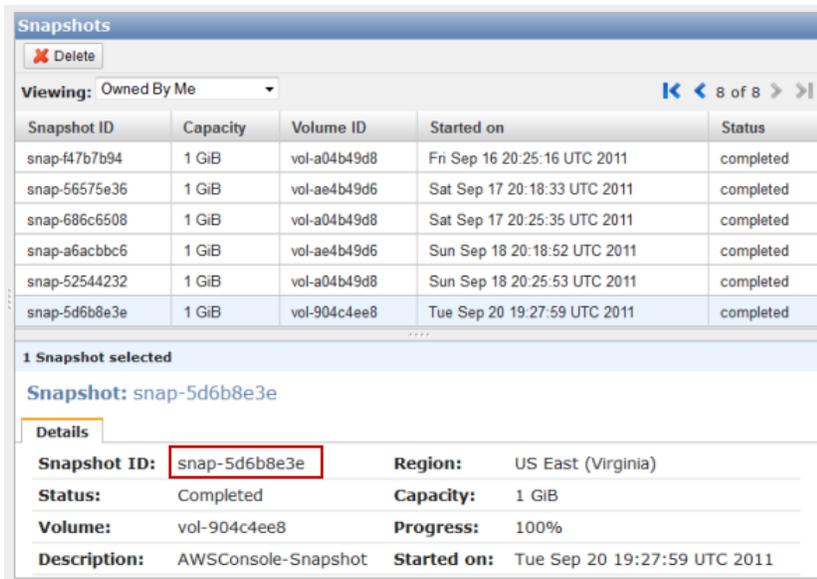
**Snapshot ID:** snap-5d6b8e3e      **Region:** US East (Virginia)

**Status:** Completed      **Capacity:** 1 GiB

**Volume:** vol-904c4ee8      **Progress:** 100%

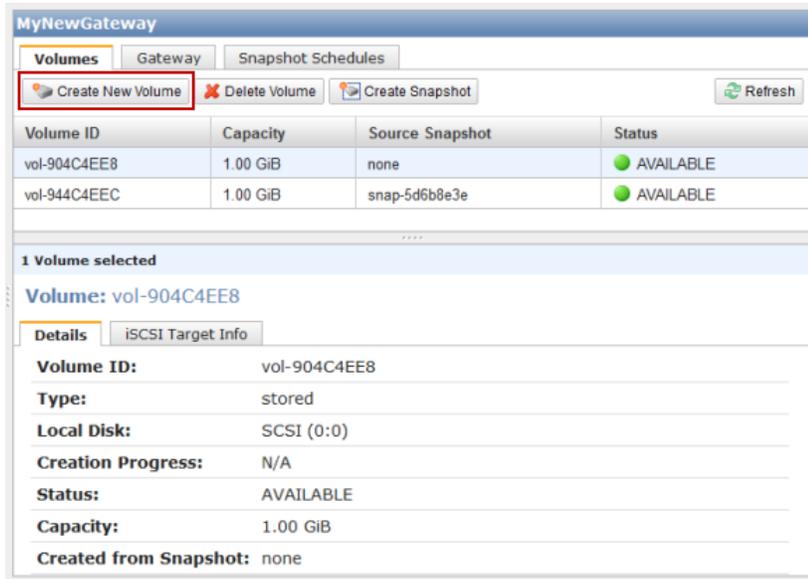
**Description:** AWSConsole-Snapshot      **Started on:** Tue Sep 20 19:27:59 UTC 2011

2. 在快照列表中，选中要创建存储卷的快照并记下快照 ID，以备后续步骤使用。



This screenshot is identical to the previous one, but the 'Snapshot ID' field in the details section is highlighted with a red rectangular box, indicating that the user should note this ID for later use.

3. 在导航窗格中，选中您希望还原快照的网关。
4. 单击创建卷。



5. 根据配置的网关类型的不同，选择下列步骤之一。

a. 如需创建网关存储卷。

i. 在创建存储卷对话框中，将先前复制的快照 ID 粘贴到基于快照 ID 字段中。

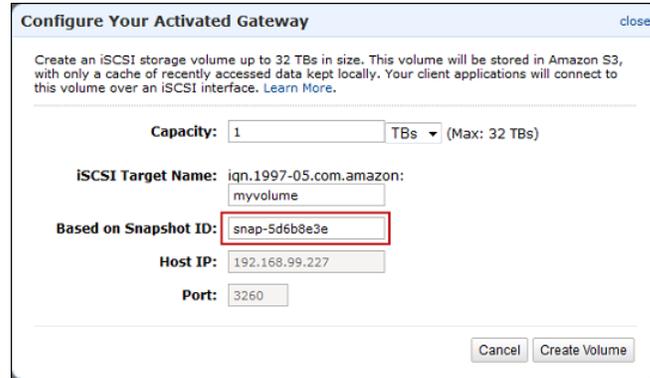


ii. 选择一个磁盘和唯一目标名称，然后单击创建卷。

存储卷的大小必须大于或等于快照大小。若要将磁盘添加到可用作存储卷的网关 VM，请参见 [为存储卷添加本地磁盘（网关存储）](#) (p. 101)。您现在可以从场内应用程序访问该卷的内容（请参见 [配置应用程序对存储卷的访问](#) (p. 153)）。

b. 如需创建网关缓存卷。

i. 在配置您的网关对话框中，将先前复制的快照 ID 粘贴到基于快照 ID 字段中。



- ii. 选择磁盘容量和唯一目标名称，然后单击创建卷。

存储卷的大小必须大于或等于快照大小。您现在可以从场内应用程序访问该卷的内容（请参见 [配置应用程序对存储卷的访问](#) (p. 153)）。

## 将快照还原为 Amazon EBS 卷

AWS Storage Gateway 拍摄的本地存储卷的快照以 Amazon EBS 快照的形式存储在 Amazon S3 中。对于大小高达 1 TiB 的快照，您可以将本地存储卷的快照还原为 Amazon EBS 卷，然后将该卷连接到 Amazon EC2 实例。这样有助于您在需要针对灾难恢复或数据处理而利用 Amazon EC2 计算能力的情况下，轻松地将数据从场内应用程序迁移到运行在 Amazon EC2 中的应用程序。若要查看 Amazon EC2 和 Amazon EBS 的详细定价信息，请转到 [Amazon EC2 定价](#) 页面。

如需将快照还原为 Amazon EBS 卷

1. 创建 Amazon EBS 卷。

- 按“Amazon Elastic Compute Cloud 用户指南”中的 [创建 Amazon EBS 卷](#) 中的说明进行操作。

您指定的卷大小必须大于或等于快照大小。在 Amazon EC2 控制台的 EBS 卷窗格中，在创建卷向导的下拉列表中选择快照 ID。另外，您还可以使用 Amazon EC2 API 创建 Amazon EBS 卷。

2. 将 Amazon EBS 卷连接到 Amazon EC2 实例。有关更多信息，请参见“Amazon Elastic Compute Cloud 用户指南”中的 [将卷连接到实例](#)。

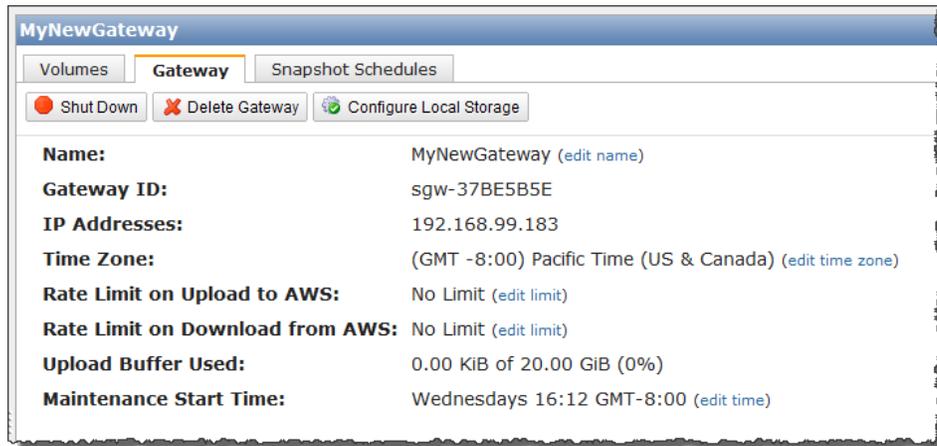
## 执行卷网关（网关缓存和网关存储）维护任务

Topics

- [使用 AWS Storage Gateway 控制台关停并启动网关](#) (p. 210)
- [使用 AWS Storage Gateway 控制台管理网关更新](#) (p. 212)
- [更新网关速率限制](#) (p. 213)
- [使用 AWS Storage Gateway 控制台删除网关](#) (p. 217)
- [登录到 AWS Storage Gateway 本地控制台](#) (p. 218)
- [将 AWS Storage Gateway 的路由选为通过代理](#) (p. 222)
- [允许通过防火墙和路由器进行 AWS Storage Gateway 访问](#) (p. 223)
- [将您的 AWS Storage Gateway 配置为使用静态 IP 地址](#) (p. 224)

- [测试 AWS Storage Gateway 到 Internet 的连接 \(p. 226\)](#)
- [同步您的网关 VM 时间 \(p. 227\)](#)
- [针对多个网络适配器 \(NIC\) 配置 AWS Storage Gateway \(p. 229\)](#)
- [使用多个网络适配器在 AWS Storage Gateway 中创建存储卷 \(p. 235\)](#)

您可以在 AWS Storage Gateway 控制台的网关选项卡中执行许多与网关维护相关的任务。以下示例显示网关选项卡。



下表总结了网关选项卡上可更新的字段。单击字段末尾的编辑链接，可编辑该链接来更改值。

维护项目	注释
名称	您可以有选择地修改网关名称。如果使用 Amazon CloudWatch 查看网关指标（请参见 <a href="#">使用 Amazon CloudWatch 控制台 (p. 244)</a> ），建议您记下前一名称以及新名称以免混淆，或者仅使用网关 ID，该 ID 保持不变。
Gateway ID	AWS Storage Gateway 会为每个网关分配一个唯一标识符。该值不能更改。
IP Addresses	如果网关托管在配有一个以上网络接口卡的服务器上，那么您的存储应用程序可以使用一个以上的 IP 地址访问网关的存储卷。在此场景中，可用来与网关通信的所有地址均列出。
Time Zone	AWS Storage Gateway 在显示来自 AWS 和快照调度的维护消息等基于时间的信息时，使用时区。
Rate Limit on Upload to AWS	您可以选择限制从网关到 AWS 的上传吞吐量。对您的网关实行带宽限制，从而限制网络带宽的使用量。以千位每秒为单位制定速率限制 (kbps)。默认对上传没有速率限制。有关更新此带宽的更多信息，请参见 <a href="#">更新网关速率限制 (p. 213)</a> 。
Rate Limit on Download from AWS	您可以选择限制从 AWS 到网关的下载吞吐量。对您的网关实行带宽限制，从而限制网络带宽的使用量。以千位每秒为单位制定速率限制 (kbps)。默认对下载没有速率限制。有关更新此带宽的更多信息，请参见 <a href="#">更新网关速率限制 (p. 213)</a> 。
Upload Buffer Used	显示已使用的上传缓冲区。有关如何监控上传缓冲区及其如何随时间变化的信息，请参见 <a href="#">监控上传缓冲区 (p. 249)</a> 。

维护项目	注释
Maintenance Start Time	每个网关的维护窗口期为每周一次。激活期间，默认时间分配到您的网关。如需更改时间，请单击编辑并指定网关时区中一星期中的某一天以及一天中的某个时间。
Apply Update Now	如果 AWS Storage Gateway 有更新，控制台中将显示消息。单击立即应用更新以立即应用更新。如果您不应用更新，AWS Storage Gateway 将根据您的维护起始时间设置应用更新。有关更多信息，请参见 <a href="#">使用 AWS Storage Gateway 控制台管理网关更新</a> (p. 212)。

## 使用 AWS Storage Gateway 控制台关停并启动网关

本部分介绍如何关闭和打开网关。举例来说，您可能需要关停网关来将补丁应用到您的管理程序主机。关停网关时，您的应用程序无法访问存储卷，因此不能向这些存储卷写入任何数据。网关也会停止向 AWS 上传任何数据。

关停网关前，您必须通过关停 iSCSI 启动程序的连接来停止正在向存储卷写入的任何应用程序。如果关停网关时快照正在进程中，快照将会在网关重启后继续。可在控制台的快照计划选项卡上检查存储卷的快照计划。有关更多信息，请参见 [编辑快照计划](#) (p. 195)。

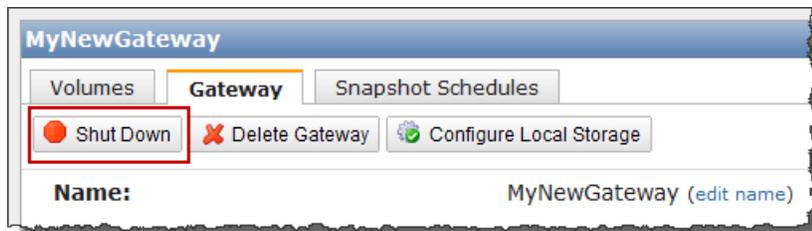


### Note

请注意，当您使用 AWS Storage Gateway 控制台关停网关时，即意味着您在停止该网关。不过，网关 VM 会继续开启。如果您需要关闭 VM，请使用 VMware vSphere 客户端或 Microsoft Hyper-V Manager 连接到您的主机然后关闭具体的 VM。在您激活后使用网关的大多普通场景中，您不需要关停网关 VM。

### 关停网关

1. 在 AWS Storage Gateway 控制台的导航窗格中，选择网关。
2. 单击关停。



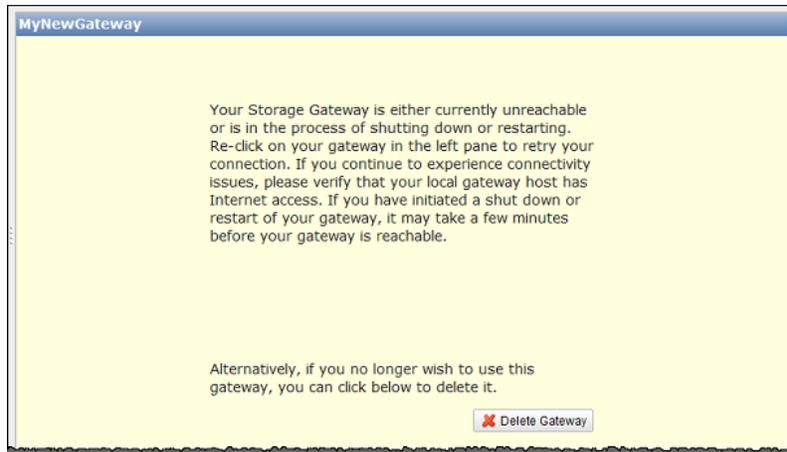
3. 在确认对话框中，单击确定。



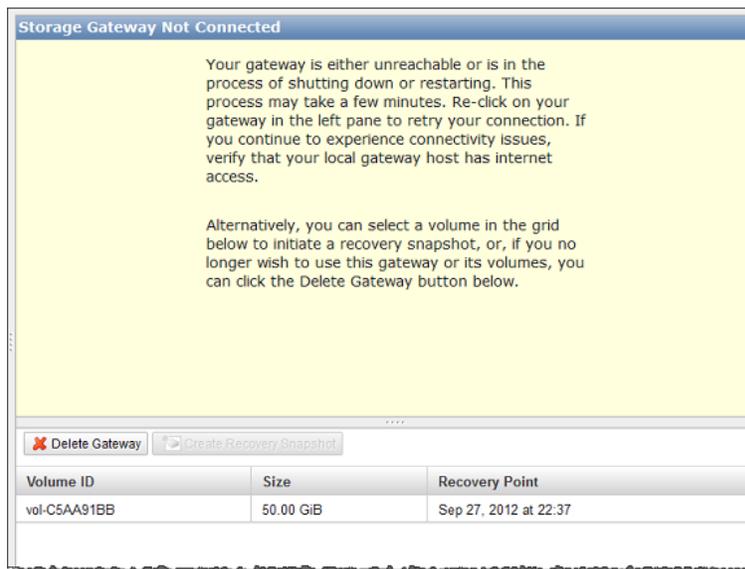
4. 在网关关闭对话框中，单击关闭。



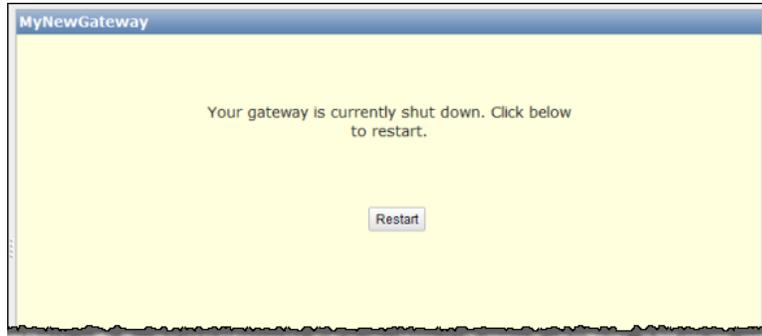
5. 在网关关停的过程中，您可能会看到网关正在关停进程中的消息。  
您在此时拥有的选项取决于网关类型（缓存卷或存储卷）。
  - a. 对于存储卷网关，您可以选择删除网关。如果您计划重启并继续使用该网关，请勿删除该网关。



- b. 对于缓存卷网关，您可以选择删除网关或者从还原点创建快照。  
有关卷还原点的更多信息，请参见 [使用还原快照（网关缓存）](#) (p. 241)。



6. 在左侧导航窗格中选择网关。  
将显示重启按钮。



### 打开网关

1. 在 AWS Storage Gateway 控制台的导航窗格中，选择要重新启动的网关。
2. 单击重启。

## 使用 AWS Storage Gateway 控制台管理网关更新

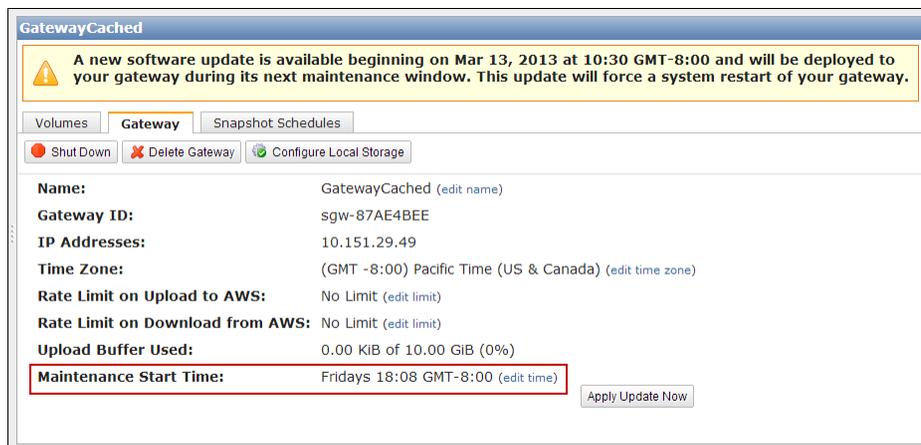
AWS Storage Gateway 定期向您的网关部署必须应用的重要更新和补丁。亚马逊会在任何网关更新前通过 AWS Storage Gateway 控制台和电子邮件通知您。软件更新会强制重新启动您的网关，这通常需要花费几分钟时间完成。您无需进行任何行动，尤其是不应该手动重新启动 VM。在更新后，您的网关及其卷的状态会和更新前相同。在应用软件更新的时，系统会缓冲处理应用程序从启动程序到网关存储卷的读取与写入操作；网关会在更新完成后处理这些操作。您可以通过提高 iSCSI 启动程序的超时值将应用程序的中断几率降到最低。有关针对 Windows 和 Linux 提高 iSCSI 启动程序超时值的更多信息，请分别参见 [自定义您的 Windows iSCSI 设置 \(p. 154\)](#) 和 [自定义您的 Linux iSCSI 设置 \(p. 158\)](#)。

您可以选择让 AWS Storage Gateway 根据您的网关维护计划应用更新，也可以自行应用更新。部署并激活网关后，将设置默认的周度维护计划。您可以随时通过单击网关选项卡中维护起始时间旁的编辑来修改该计划。以下示例显示了用来应用更新的含有维护消息和用户界面中的按钮的网关维护选项卡。



### Important

软件更新强制网关系统重启。您可以通过提高 iSCSI 启动程序的超时值将应用程序的中断几率降到最低。有关针对 Windows 和 Linux 提高 iSCSI 启动程序超时值的更多信息，请分别参见 [自定义您的 Windows iSCSI 设置 \(p. 154\)](#) 和 [自定义您的 Linux iSCSI 设置 \(p. 158\)](#)。



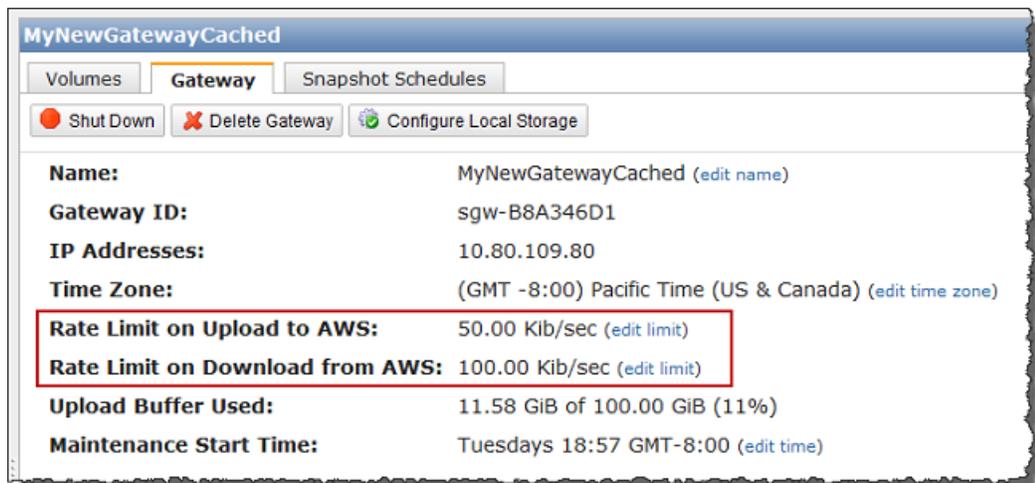
## 更新网关速率限制

您可以限制（或限定）从网关到 AWS 的上传吞吐量或者从 AWS 到网关的下载吞吐量。使用带宽限制可以帮助您控制网关所用的网络带宽量。已激活的网关按默认不对上传或下载进行速率限制。

您可以使用 AWS 管理控制台或以编程方式使用 AWS API（请参见 [UpdateBandwidthRateLimit](#)）指定速率限制，也可以使用 AWS 软件开发工具包 (SDK) 进行指定。以编程方式更改限定值的功能可以让您自动更改一天中的限制，例如安排任务时间来更改带宽。有关以编程方式更改带宽速率限制的示例，请参见 [使用适用于 Java 的 AWS 软件开发工具包更新网关速率限制 \(p. 213\)](#)、[使用适用于 .NET 的 AWS 软件开发工具包更新网关速率限制 \(p. 215\)](#) 或 [使用适用于 Windows PowerShell 的 AWS 工具更新网关速率限制 \(p. 217\)](#)。

如需使用控制台更改网关的带宽限制

1. 在 AWS Storage Gateway 控制台的导航窗格中，选择您要管理的网关。
2. 在右侧窗格中单击网关选项卡。
3. 单击要更改的限制旁的编辑限制文本。



4. 在编辑速率限制对话框中，输入新的限制值，然后单击保存。



## 使用适用于 Java 的 AWS 软件开发工具包更新网关速率限制

以编程方式更新带宽速率限制可为您提供在一段时间内自动调整限制的途径，例如可通过安排任务时间进行调整。下面的示例介绍了如何使用适用于 Java 的 AWS 软件开发工具包 (SDK) 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，请参见“适用于 Java 的 AWS 软件开发工具包开发人员指南”中的 [入门](#) 部分。

Example :使用适用于 Java 的 AWS 软件开发工具包更新网关带宽限制

以下 Java 代码示例更新网关的带宽速率限制。您需要更新代码并提供服务终端节点、网关的亚马逊资源名称 (ARN) 以及上传和下载限制。有关可用于 AWS Storage Gateway 的 AWS 服务终端部分点的列表，请查看“Amazon Web Services 术语表”中的[地区和终端部分点](#)。

```
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(
            ListDeleteVolumeSnapshotsExample.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 " + re
turnGatewayARN);
        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 bandwidth.\n" + ex.to
String());
    }
}
}
```

### 使用适用于 .NET 的 AWS 软件开发工具包更新网关速率限制

以编程方式更新带宽速率限制可为您提供在一段时间内自动调整限制的途径，例如可通过安排任务时间进行调整。下面的示例介绍了如何使用适用于 .NET 的 AWS 软件开发工具包 (SDK) 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，请参见“适用于 .NET 的 AWS 软件开发工具包开发人员指南”中的[入门](#)部分。

Example :使用适用于 .NET 的 AWS 软件开发工具包更新网关带宽限制

以下 C# 代码示例更新网关的带宽速率限制。您需要更新代码并提供服务终端节点、网关的亚马逊资源名称 (ARN) 以及上传和下载限制。有关可用于 AWS Storage Gateway 的 AWS 服务终端部分点的列表，请查看“Amazon Web Services 一般参考”中的[地区和终端部分点](#)。

```
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
```



EBS 快照。如果您不愿意取消 Amazon EC2 订阅，则可使用 Amazon EC2 控制台删除快照。有关更多信息，请参见 [AWS Storage Gateway 详细信息页面](#)。

如果您意外删除了网关，可激活新的网关（请参见 [激活 AWS Storage Gateway \(p. 109\)](#)）并将其配置为匹配已删除网关的设置。为新的网关创建一个新的 VM。对于网关存储设置，使用与已删除网关相同的上传缓冲区创建新网关。对于网关缓存设置，使用与已删除网关相同的上传缓冲区和缓存存储空间创建新网关。针对网关缓存设置在新网关上创建存储卷时，请在 Amazon S3 中创建新卷并从快照还原。对于网关存储设置，您可以使用与已删除网关相同的底层磁盘并将数据保存在这些磁盘上。有关更多信息，请参见 [管理存储卷（网关存储） \(p. 173\)](#)。

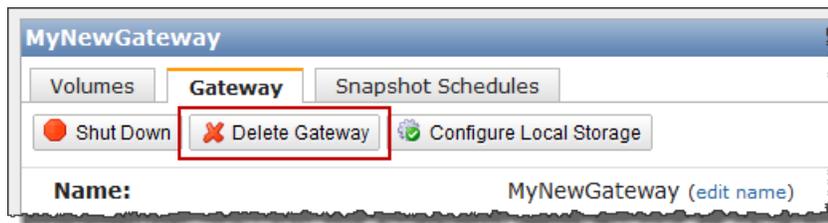
#### 如需删除网关

1. 在 AWS Storage Gateway 控制台的导航窗格中，选择要删除的网关。
2. 在网关选项卡中，单击删除网关。



#### Important

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，可能会造成数据丢失。



3. 单击确定来确认删除。

至此，删除的网关不再是已激活的网关。不过，网关 VM 会仍然在您的虚拟环境中。如需移除 VM，请使用 VMware vSphere 客户端或 Microsoft Hyper-V Manager 连接到主机并移除 VM。

## 登录到 AWS Storage Gateway 本地控制台

某些网关维护任务需要您登录到网关的本地控制台。本地控制台可通过管理程序客户端软件访问。用户为 *sguser*，密码为 *sgpassword*。这些登录证书授予您访问配置菜单的权限，您可以在这些菜单中配置网络网关设置。

在这个主题中，我们向您介绍如何访问 VMware ESXi（请参见 [访问您的网关本地控制台（VMware ESXi） \(p. 218\)](#)）或 Microsoft Hyper-V（请参见 [访问您的网关本地控制台（Microsoft Hyper-V） \(p. 219\)](#)）中托管的网关的本地控制台。在访问控制台后，您可以登录到控制台中（请参见 [登录网关本地控制台 \(p. 221\)](#)）。

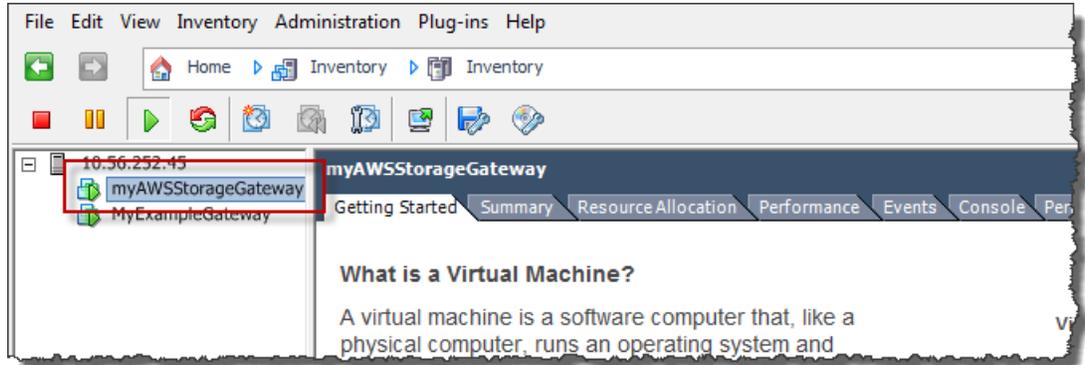
#### 访问您的网关本地控制台（VMware ESXi）

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

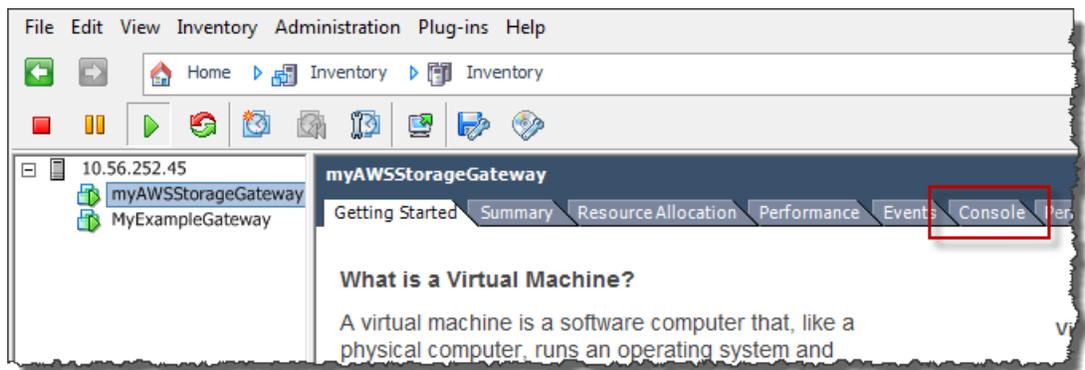


#### Note

如果您的网关 VM 已开启，绿色箭头图标会随 VM 图标显示，如下例所示。如果您的网关 VM 未开启，则可通过单击工具栏菜单中的开机图标，将其开启。



- 单击控制台选项卡。

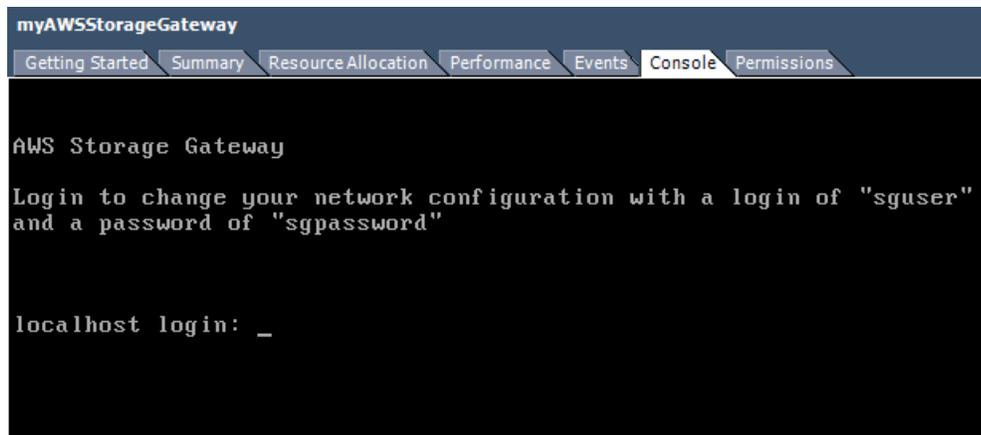


- 在过几分钟时间后，虚拟机就会准备就绪，供您登录了。



**Note**

要从控制台窗口中释放光标，请按 Ctrl+Alt.



- 要登录，请继续执行过程 [登录网关本地控制台 \(p. 221\)](#)。

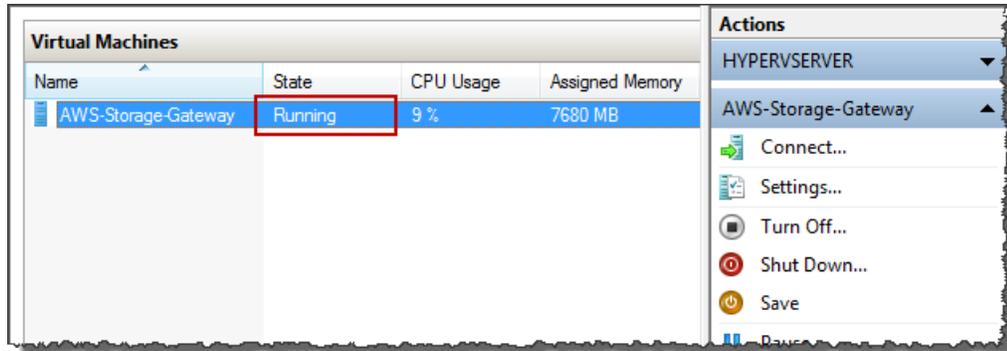
访问您的网关本地控制台 (Microsoft Hyper-V)

- 在 Microsoft Hyper-V Manager 的虚拟机列表中，选择您的网关 VM。
- 确保网关已开启。



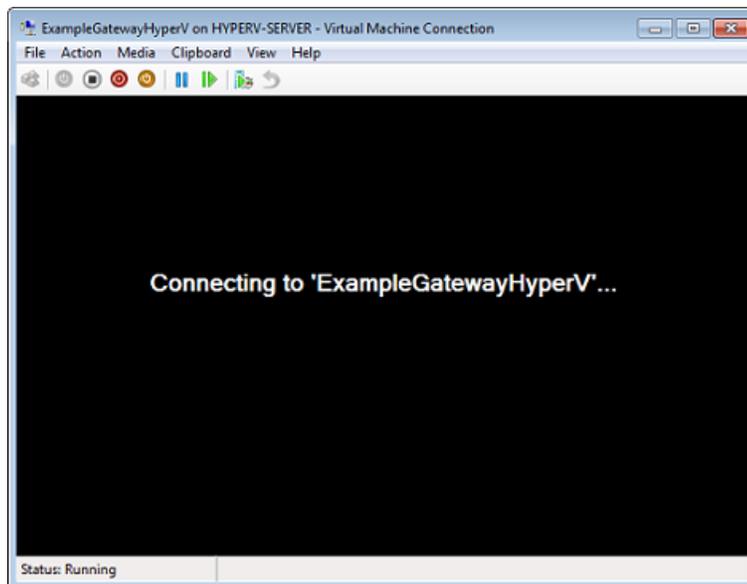
### Note

如果您的网关 VM 已打开，Running 会显示为 VM 的状态，如下例所示。如果您的网关 VM 未开启，则可通过单击操作窗格中的开始，将其开启。

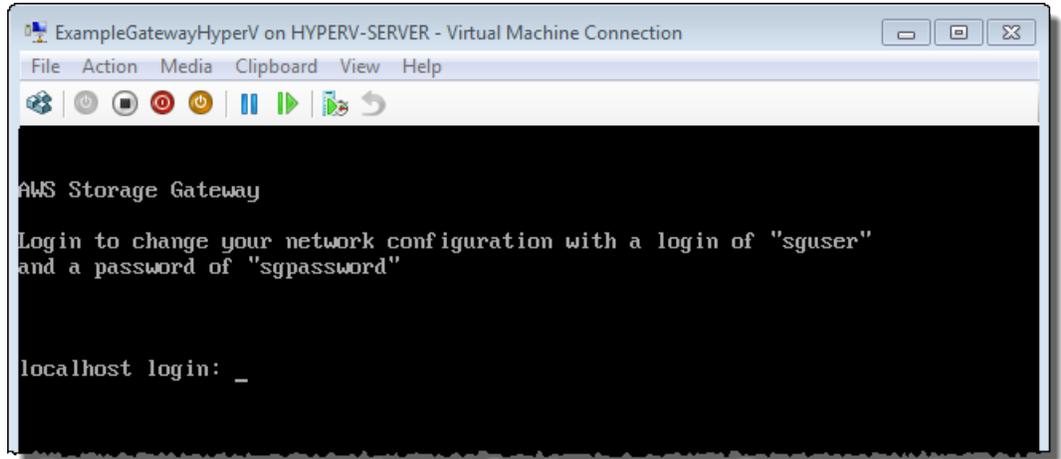


3. 在操作窗格中，选择连接...

随后将显示虚拟机连接窗口。如果显示身份验证窗口，请输入管理程序管理员向您提供的用户名称和密码。



4. 在过几分钟时间后，虚拟机就会准备就绪，供您登录了。



5. 要登录，请继续执行过程 [登录网关本地控制台 \(p. 221\)](#)。

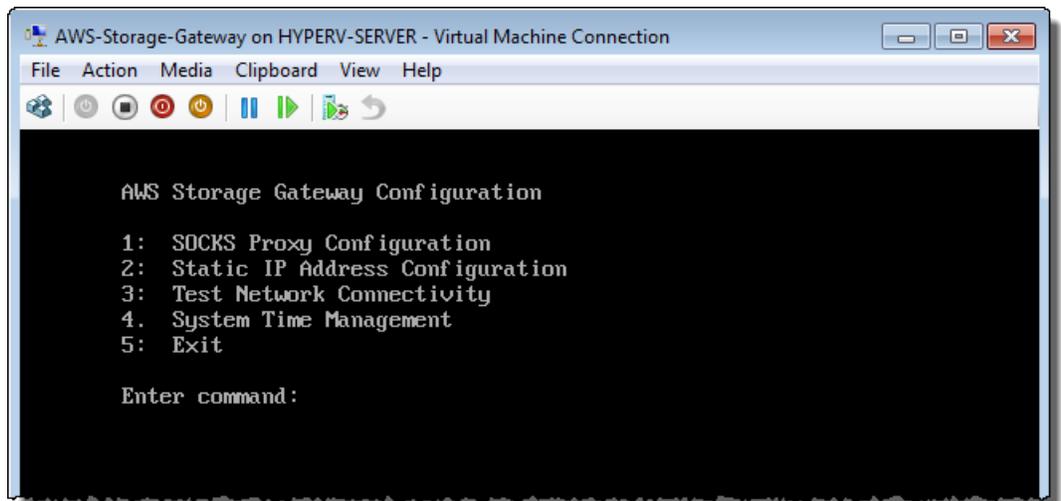
#### 登录网关本地控制台

1. 在登录屏幕中，使用“Console”窗口中指定的用户名称和密码登录到 VM。
2. 登录后，您将看到 AWS Storage Gateway 配置主菜单。



#### Note

对于部署在 Microsoft Hyper-V 上的网关，您还将看到一个用于系统时间管理的菜单项，部署在 VMware ESXi 上的网关没有该菜单项。



如需...	请参见...
为您的网关配置 SOCKS 代理	<a href="#">将 AWS Storage Gateway 的路由选为通过代理 (p. 222)</a>
为您的网关接口配置静态 IP 地址	<a href="#">将您的 AWS Storage Gateway 配置为使用静态 IP 地址 (p. 224)</a>

如需...	请参见...
测试网关连接性	<a href="#">测试 AWS Storage Gateway 到 Internet 的连接 (p. 226)</a>
管理 VM 时间 ( 仅限 Microsoft Hyper-V )	<a href="#">同步您的网关 VM 时间 (p. 227)</a>

## 将 AWS Storage Gateway 的路由选为通过代理

AWS Storage Gateway 支持在网关和 AWS 间配置 SOCKS5 代理。如果您的网关必须使用代理服务器与 Internet 通信，那么您就需要为网关配置 SOCKS 代理服务器设置。您可以通过为运行代理的主机指定 IP 地址和端口号来进行上述操作，AWS Storage Gateway 会将所有的 HTTPS 流量引导为通过代理服务器。

如需将网关的 Internet 流量引导为通过本地代理服务器

1. 登录到网关的本地控制台。有关说明，请参见[登录到 AWS Storage Gateway 本地控制台 \(p. 218\)](#)。
2. 在 AWS Storage Gateway 配置主菜单中，输入选项 1。



### Note

对于部署在 Microsoft Hyper-V 上的网关，您还将看到一个用于系统时间管理的菜单项，部署在 VMware ESXi 上的网关没有该菜单项。

```
AWS Storage Gateway Configuration

1: SOCKS Proxy Configuration
2: Static IP Address Configuration
3: Test Network Connectivity
4: Exit

Enter command: _
```

3. 选择 AWS Storage Gateway SOCKS 代理配置菜单中的以下某个选项：

```
AWS Storage Gateway SOCKS Proxy Configuration

1: Configure SOCKS Proxy
2: View Current SOCKS Proxy Configuration
3: Remove SOCKS Proxy Configuration
4: Exit

Enter command: _
```

如需...	请执行此操作...
配置 SOCKS 代理	输入选项 1。  您需要提供主机名称和端口以完成配置。

如需...	请执行此操作...
查看当前的 SOCKS 代理配置	输入选项 2。  如果 SOCKS 代理未配置，“SOCKS Proxy not configured”消息将会显示。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	输入选项 3。  消息“SOCKS Proxy Configuration Removed”显示。
退出该菜单并返回到上一菜单。	输入选项 4。

## 允许通过防火墙和路由器进行 AWS Storage Gateway 访问

您的本地部署网关需要访问下列终端节点，以便与 AWS 进行通信。如果您使用防火墙或者路由器筛选或者限制网络流量，则必须配置防火墙和路由器，以允许这些服务终端节点与 AWS 进行出站通信。

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

下表提供了针对可用地区的地区字符串列表。

Region name	Region string
US East (Northern Virginia)	us-east-1
US West (Northern California)	us-west-1
US West (Oregon)	us-west-2
EU (Ireland)	eu-west-1
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1
South America (Sao Paulo)	sa-east-1

根据您的网关地区，可将终端部分点中的 *region* 替换为相应的地区字符串。例如，如果在美国西部（俄勒冈）地区创建一个网关，则 Storage Gateway 终端节点将类似于此：

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



### Note

稍后，可以更改这些终端节点，或者添加新的终端节点。

## 将您的 AWS Storage Gateway 配置为使用静态 IP 地址

网关的默认网络配置是动态主机配置协议 (DHCP)。借助 DHCP，您的网关可获得自动分配的 IP 地址。在某些情况中，您可能需要手动将网关的 IP 地址分配为静态 IP 地址。本主题说明如何进行该配置。

如需将您的网关配置为使用静态 IP 地址。

1. 登录到网关的本地控制台。有关说明，请参见[登录到 AWS Storage Gateway 本地控制台 \(p. 218\)](#)。
2. 在 AWS Storage Gateway 配置主菜单中，选择选项 2。



### Note

对于部署在 Microsoft Hyper-V 上的网关，您还将看到一个用于系统时间管理的菜单项，部署在 VMware ESXi 上的网关没有该菜单项。

```
AWS Storage Gateway Configuration

1: SOCKS Proxy Configuration
2: Static IP Address Configuration
3: Test Network Connectivity
4: Exit

Enter command: _
```

3. 选择 AWS Storage Gateway 静态 IP 地址配置菜单中的以下某个选项：

```
AWS Storage Gateway Static IP Address Configuration

1: View Network Configuration
2: Configure Static IP
3: View DNS Configuration
4: Reset to DHCP
5: Set Default Route Adapter
6: View Routes
7: Exit

Enter command: _
```

如需...	请执行此操作...
查看网关的网络配置	<p>输入选项 1。</p> <p>适配器列表名称将会显示，并且系统会提示您输入一个适配器名称，例如“eth0”。如果您指定的适配器正在使用中，有关该适配器的下列信息就会显示：</p> <ul style="list-style-type: none"> <li>• MAC 地址</li> <li>• IP 地址</li> <li>• 网络掩码</li> <li>• 网关 IP 地址</li> <li>• DHCP 启用状态</li> </ul> <p>配置静态 IP 地址（选项 2）或设置网关的默认路由适配器（选项 5）时，您使用相同的适配器名称。</p>
为网关配置静态 IP 地址	<p>输入选项 2。</p> <p>系统会提示您输入下列信息以配置静态 IP 地址。</p> <ul style="list-style-type: none"> <li>• 网络适配器名称</li> <li>• IP 地址</li> <li>• 网络掩码</li> <li>• 默认网关地址</li> <li>• 主 DNS 地址</li> <li>• 备用 DNS 地址</li> </ul> <p> <b>Important</b></p> <p>如果已激活您的网关，则必须从 AWS Storage Gateway 控制台中关闭再重新启动网关以使这些设置生效。有关更多信息，请参见 <a href="#">使用 AWS Storage Gateway 控制台关停并启动网关 (p. 210)</a>。</p> <p>如果网关使用一个以上的网络接口，您必须将所有启用的接口设置为使用 DHCP 或静态 IP 地址。举例而言，如果网关使用两个配置为 DHCP 的接口，并且您随后将一个接口设置为静态 IP，另一个接口就会禁用。如需启用另一接口，您必须将其设置为静态 IP。如果两个接口最初都设置为使用静态 IP 地址并且您之后将网关设置为使用 DHCP，那么两个接口都必须使用 DHCP。</p>
查看网关的 DNS 配置	<p>输入选项 3。</p> <p>主 DNS 和备用 DND 域名服务器的 IP 地址将会显示。</p>

如需...	请执行此操作...
将网关的网络配置重设为 DHCP	输入选项 4。  所有网络接口均设置为使用 DHCP。   <b>Important</b>  如果已激活您的网关，则必须从 AWS Storage Gateway 控制台中关闭再重新启动网关以使这些设置生效。有关更多信息，请参见 <a href="#">使用 AWS Storage Gateway 控制台关停并启动网关 (p. 210)</a> 。
设置网关的默认路由适配器	输入选项 5。  可供网关使用的适配器将会显示，系统会提示您选择任意适配器，例如“eth0”。
查看路由表	输入选项 6。  网关的默认路由将会显示。
退出该菜单并返回到上一菜单。	输入选项 7。

## 测试 AWS Storage Gateway 到 Internet 的连接

AWS Storage Gateway 配置菜单还能让您测试网关到 Internet 的连接。排查网关相关问题时，该测试可能会很有用处。网关的连接性测试不计入可能已配置的任何 SOCKS 代理。

如需测试网关到 Internet 的连接

1. 登录到网关的本地控制台。有关说明，请参见 [登录到 AWS Storage Gateway 本地控制台 \(p. 218\)](#)。
2. 在 AWS Storage Gateway 配置主菜单中，选择选项 3。



### Note

对于部署在 Microsoft Hyper-V 上的网关，您还将看到一个用于系统时间管理的菜单项，部署在 VMware ESXi 上的网关没有该菜单项。

```
AWS Storage Gateway Configuration
1: SOCKS Proxy Configuration
2: Static IP Address Configuration
3: Test Network Connectivity
4: Exit

Enter command: _
```

网络连接性的测试结果可能是下列各项之一。

连接性是...	消息
成功	AWS Storage Gateway 具有 Internet 连接
不成功	AWS Storage Gateway 没有 Internet 连接

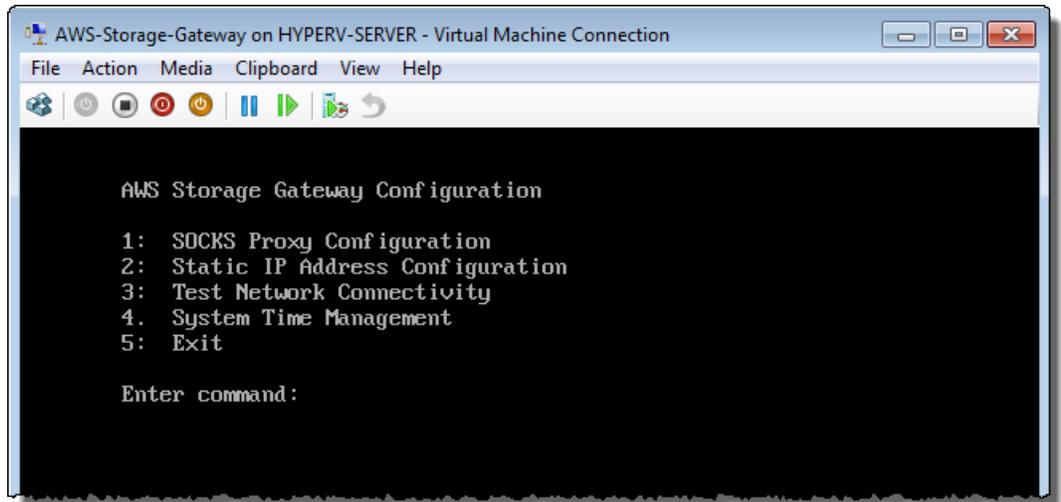
## 同步您的网关 VM 时间

在部署并运行网关后，会存在一些网关 VM 时间出现漂移的情况。例如，如果网络中断时间延长，而您的管理程序主机和网关没有获取时间更新，那么网关 VM 的时间会偏离真正的时间。当出现时间漂移时，操作（如网关更新或者快照）预计出现的时间和操作实际出现的时间之间会出现差异。

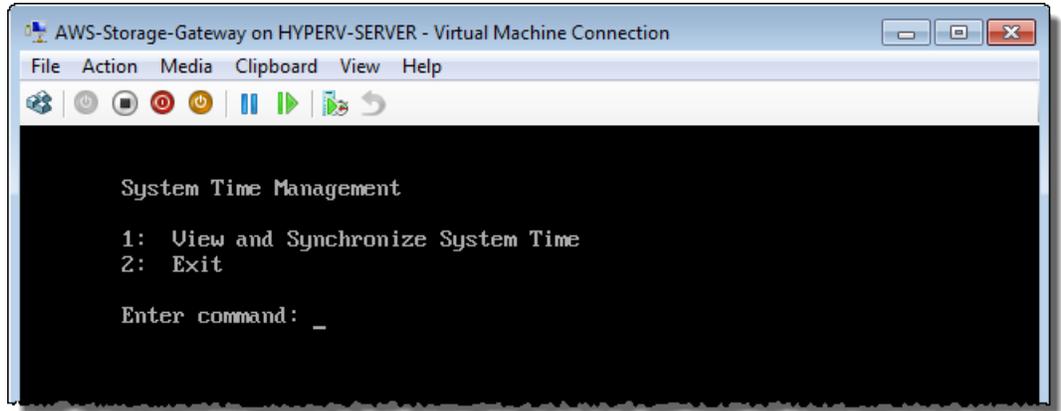
对于 VMware ESXi 上部署的网关，设置管理程序主机的时间和将 VM 时间同步到主机，就足以避免时钟漂移。有关详细信息，请参见 [将 VM 时间与主机时间同步 \(p. 18\)](#)。对于 Microsoft Hyper-V 上部署的网关，您应该定期地使用本部分介绍的操作步骤查看 VM 的时间。

查看 Hyper-V 网关 VM 的时间并将其同步到 NTP 服务器

1. 登录到网关的本地控制台。有关说明，请参见 [登录到 AWS Storage Gateway 本地控制台 \(p. 218\)](#)。
2. 在 AWS Storage Gateway 配置主菜单中，选择选项 4 系统时间管理。



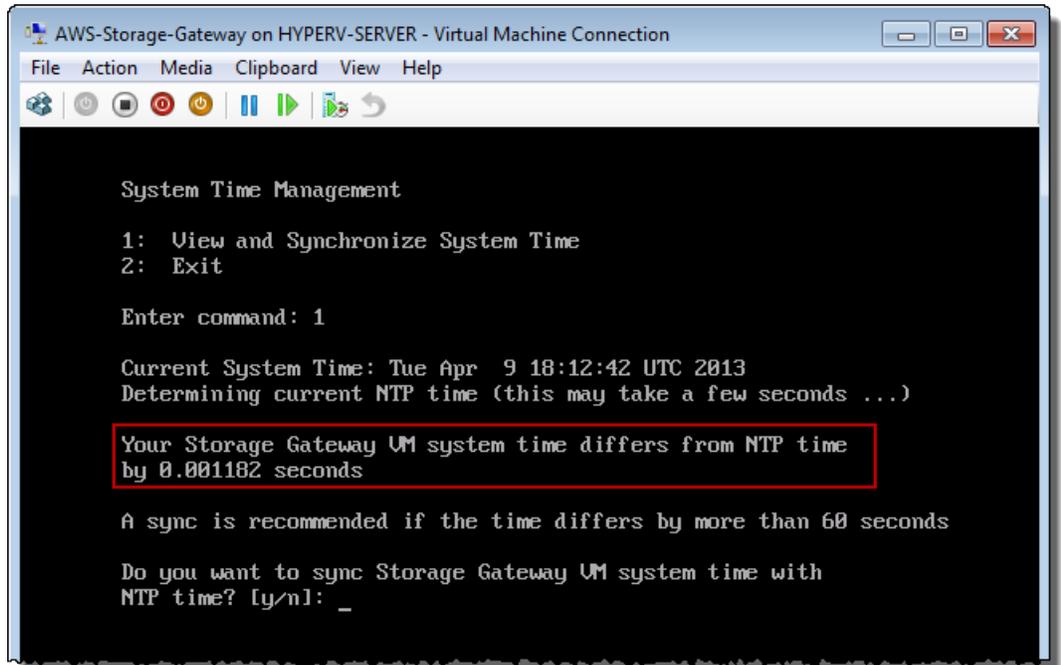
3. 在系统时间管理菜单中，选择选项 1 查看和同步系统时间。



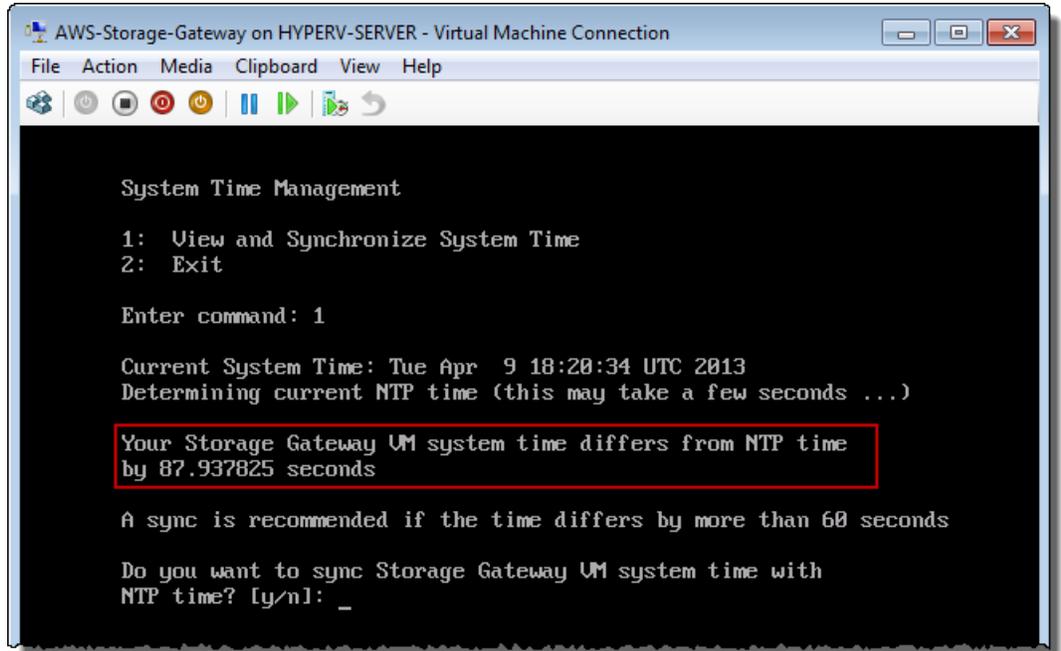
4. 如果结果指示您应同步您的时间，则输入 y；否则输入 n。

如果输入 y 进行同步，则同步可能需要消耗一段时间。

下例介绍的 VM 不需要进行时间同步。



下例介绍的 VM 需要进行时间同步。



## 针对多个网络适配器 (NIC) 配置 AWS Storage Gateway

如果您将网关配置为使用多个网络适配器，网关就可由一个以上的 IP 地址访问。当您希望通过配置网关使用多个网络适配器时，可使用案例，包括：

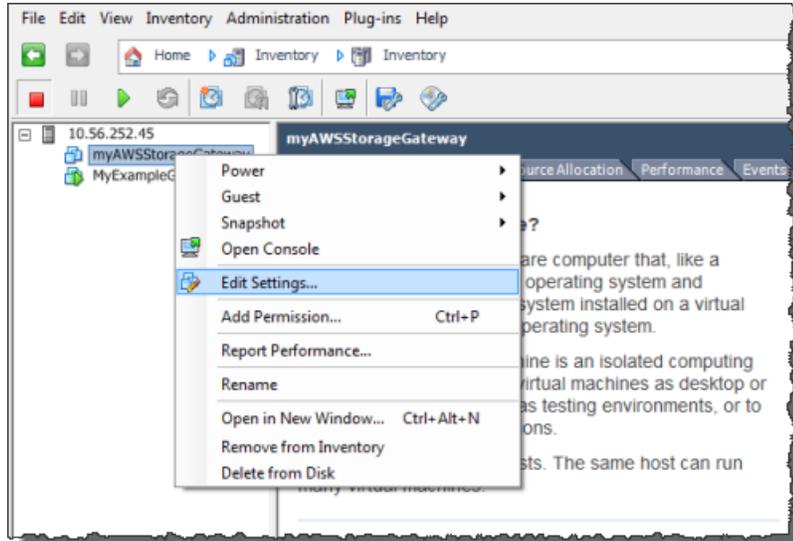
- 使吞吐量达到最大 – 当网络适配器成为瓶颈时，可能要使网关的吞吐量达到最大。
- 应用程序分隔 – 可能需要分隔应用程序及其如何写入网关的存储卷。举例而言，您可以选择让至关重要的存储应用程序单独使用针对网关定义的一个适配器。
- 网络约束 – 应用程序环境可能需要将 iSCSI 目标及连接到这些目标的发起程序保留在与网关用于与 AWS 通信的网络不同的一个独立网络中。

在典型的多适配器使用案例中，一个适配器会配置为路径，供网关与 AWS 通信使用（默认网关）。除这个适配器外，启动程序所在的子网必须与（包含所连接的 iSCSI 目标的）适配器的相同；否则，可能无法与预定目标通信。如果在用于 AWS 通信的同一个适配器上配置了目标，那么，该目标的 iSCSI 流量和 AWS 流量都将通过同一个适配器。

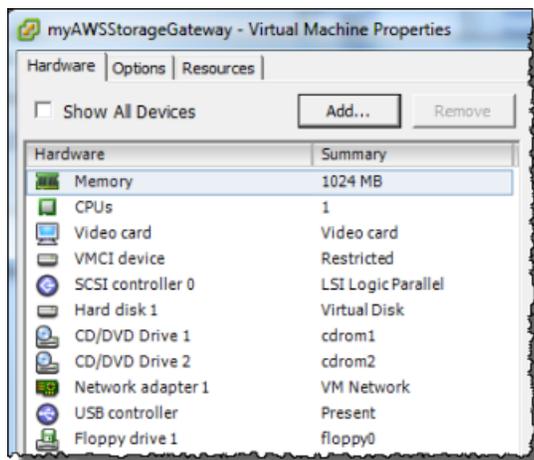
下列步骤假定您的网关 VM 已定义了一个网络适配器，并且您将添加第二个适配器。第一个过程介绍了如何给 VMware ESXi 添加适配器，第二个过程介绍了如何给 Microsoft Hyper-V 添加适配器。

如需将网关配置为使用另一个适用于 VMware ESXi 的网络适配器

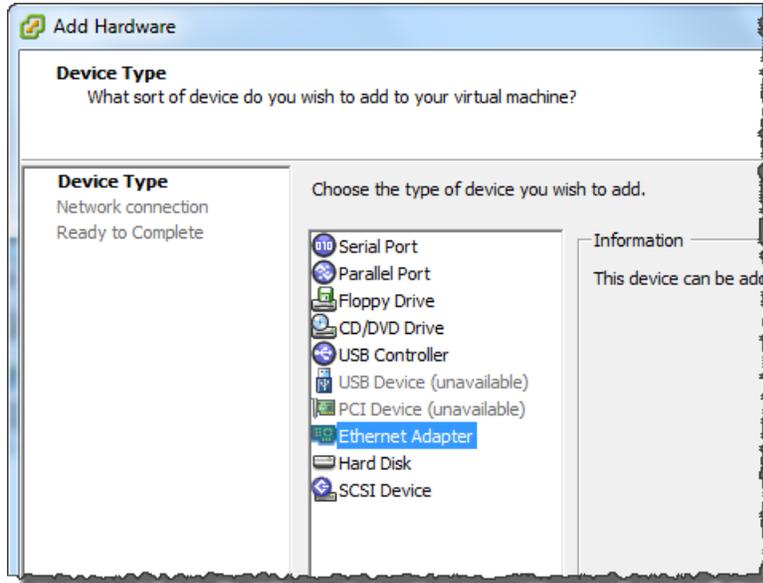
1. 在 AWS Storage Gateway 控制台中，关闭网关。  
执行 [关停网关 \(p. 210\)](#) 中的步骤，返回到此处，然后转到下一步。
2. 在 VMware vSphere 客户端中，选择您的网关 VM。  
VM 可在执行这些步骤期间保持开启。
3. 在客户端中，右键单击网关 VM 的名称，然后单击编辑设置。



4. 在虚拟机属性对话框的硬件选项卡中，单击添加以添加一个设备。

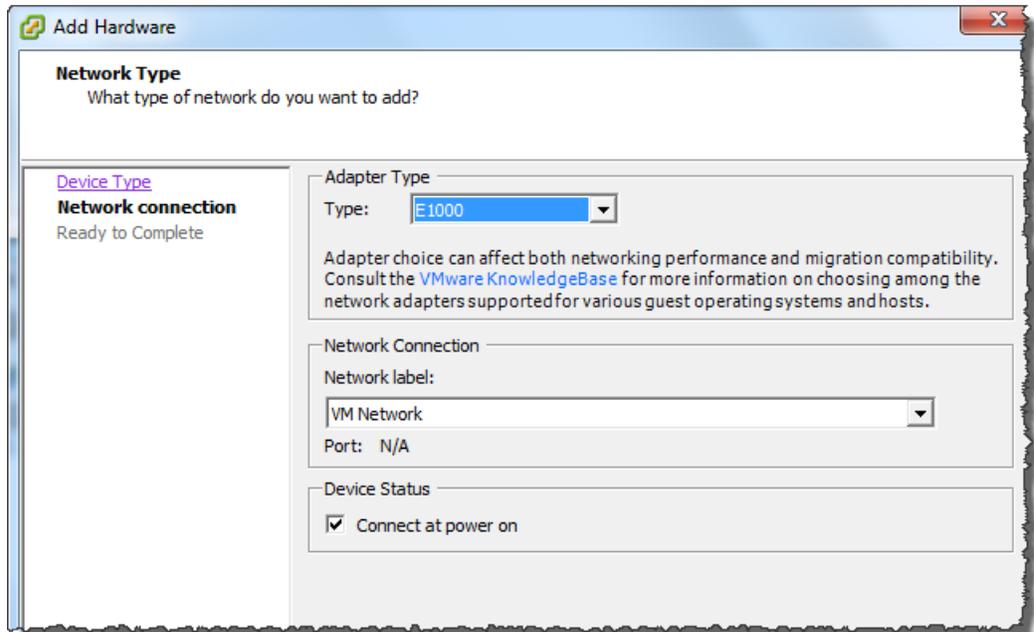


5. 按添加硬件向导添加网络适配器：
  - a. 在设备类型窗格中，单击以太网适配器以添加适配器，然后单击下一步。

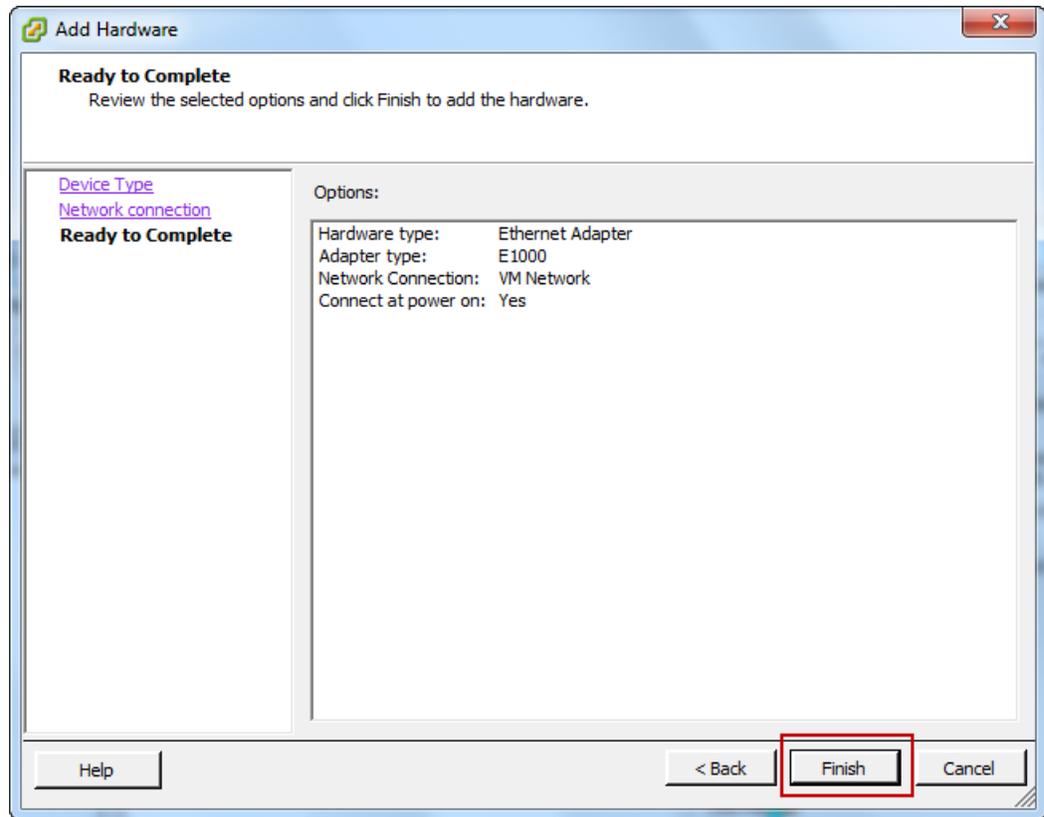


- b. 在网络类型窗格的类型下拉列表中，选择一种适配器类型，确保选中启动时连接，然后单击下一步。

我们建议您将 E1000 网络适配器与 AWS Storage Gateway 一起使用。有关适配器列表中可能出现的适配器类型的详细信息，请参阅 [ESXi 和 vCenter 服务器文档](#) 中的“网络适配器类型”。



- c. 在已准备好完成窗格中，检查相关信息，然后单击完成。



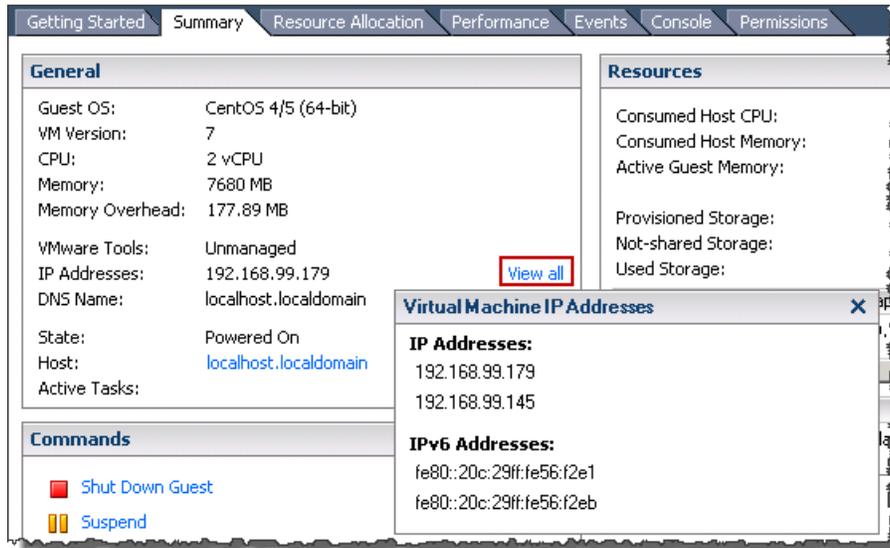
- 单击 VM 的摘要选项卡，然后单击 IP 地址字段旁的查看全部。虚拟机 IP 地址窗口显示所有可用于访问网关的 IP 地址。确认第二个 IP 地址已针对该网关列出。



#### Note

适配器更改生效和 VM 摘要信息刷新可能需要少许时间。

下例仅用于举例说明。在实际工作中，其中的 IP 地址之一将是网关与 AWS 通信的地址，而另一个会是另一子网中的地址。

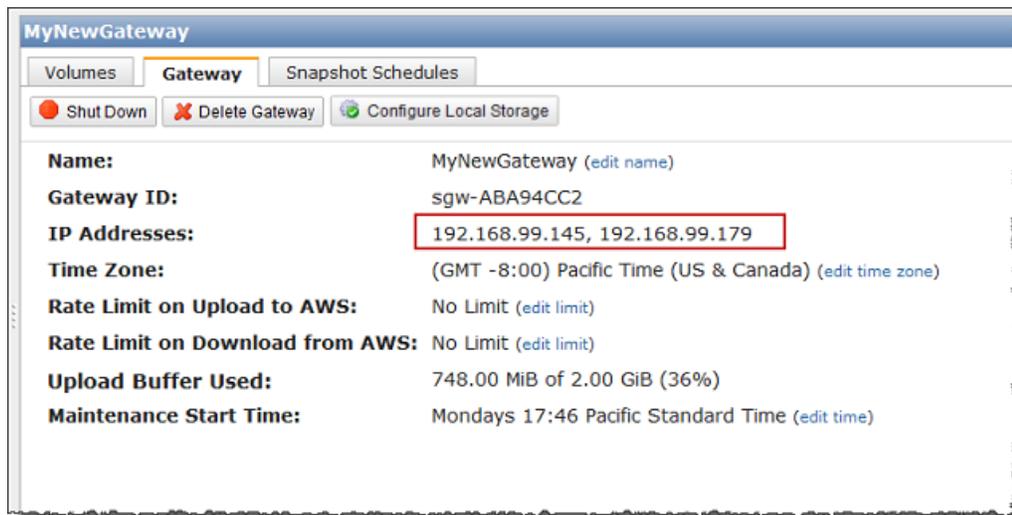


7. 在 AWS Storage Gateway 控制台中，打开网关。

执行 [打开网关](#) (p. 212) 中的步骤，返回到此处，然后转到下一步。

8. 在 AWS Storage Gateway 控制台的导航窗格中，选择将适配器添加到的网关，然后选中网关选项卡。

确认 IP 地址字段中列出了第二个 IP 地址。



如需将网关配置为使用另一个适用于 Microsoft Hyper-V 的网络适配器

1. 在 AWS Storage Gateway 控制台中，关闭网关。

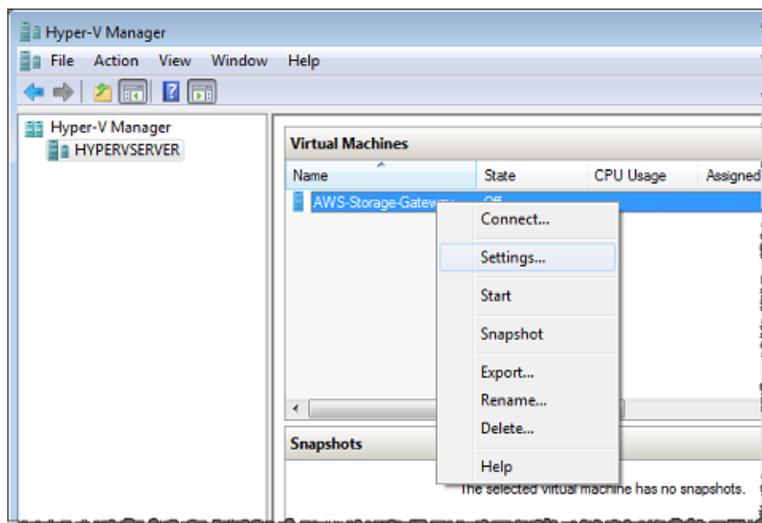
执行 [关停网关](#) (p. 210) 中的步骤，返回到此处，然后转到下一步。

2. 在 Microsoft Hyper-V Manager 中，选择您的网关 VM。

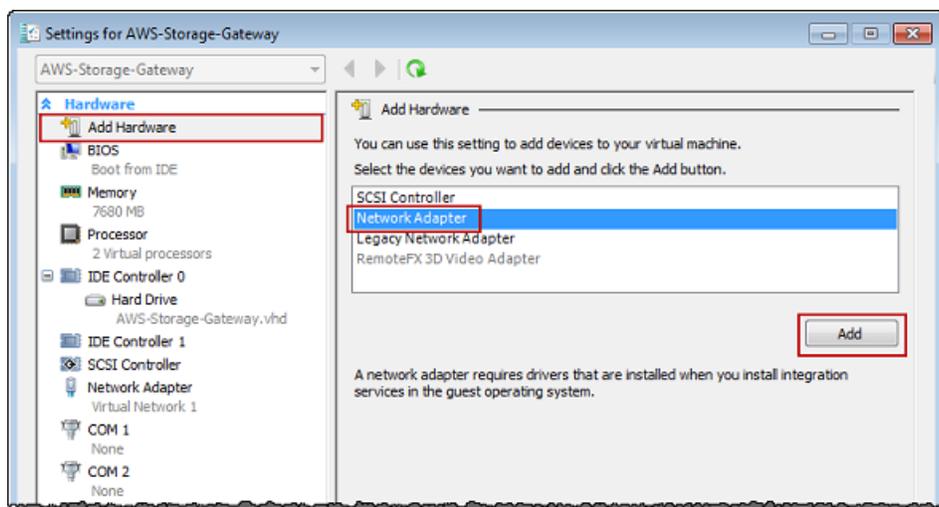
3. 如果没有关闭 VM，请予以关闭。

- 右键单击网关，然后选择关闭...

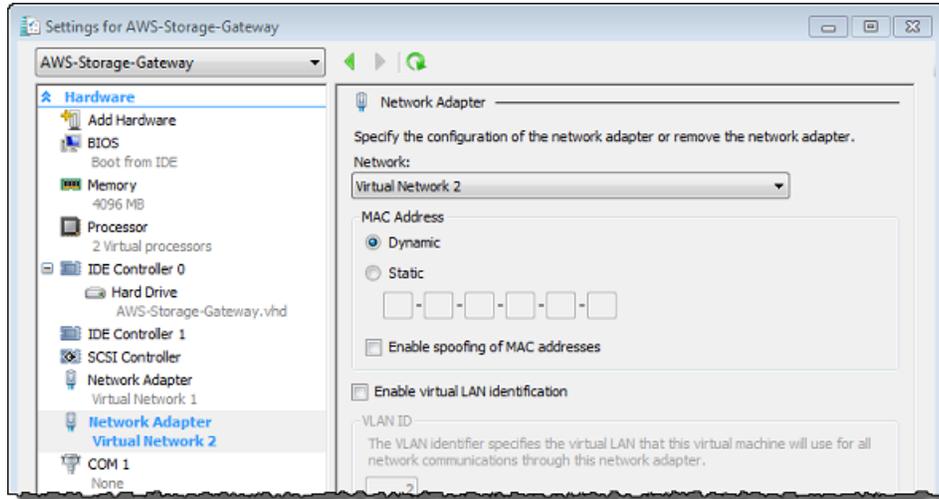
4. 在客户端中，右键单击您的网关 VM 的名称，然后单击设置...



5. 在 VM 的设置对话框的硬件列表下，单击添加硬件。
6. 在添加硬件窗格中，选择网络适配器，然后单击添加以添加设备。

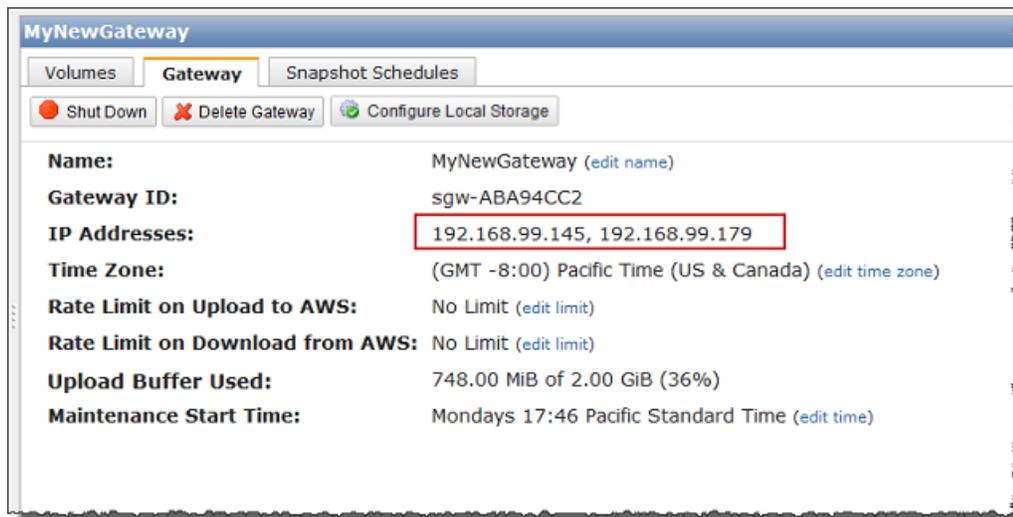


7. 配置网络适配器，然后单击应用。  
在下例中，选择了虚拟网络 2 用于新适配器。



- 在设置对话框的硬件列表中，确认已添加第二个适配器，然后单击确定。
- 在 AWS Storage Gateway 控制台中，打开网关。  
执行 [打开网关 \(p. 212\)](#) 中的步骤，返回到此处，然后转到下一步。
- 在 AWS Storage Gateway 控制台的导航窗格中，选择将适配器添加到的网关，然后选中网关选项卡。

确认 IP 地址字段中列出了第二个 IP 地址。



## 使用多个网络适配器在 AWS Storage Gateway 中创建存储卷

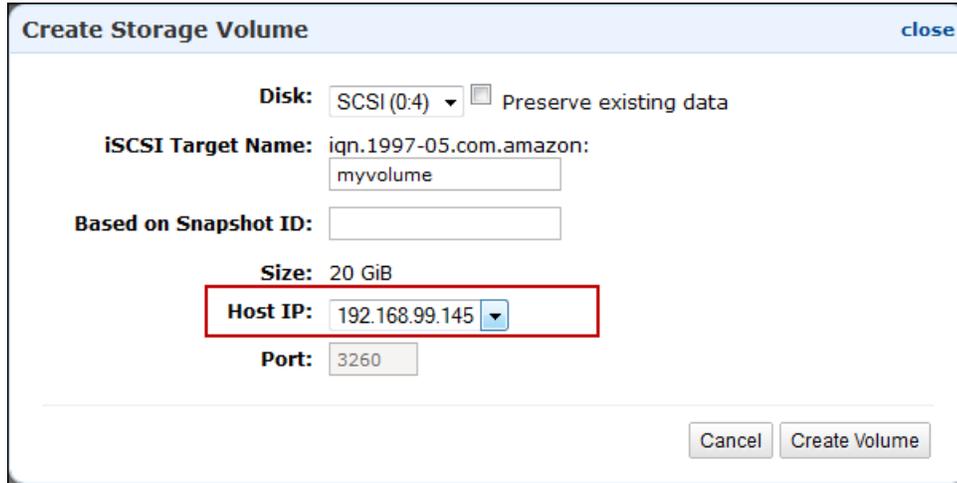
如果您已将网关定义为使用多个网络适配器，那么当您为该网关创建存储卷时，就必须选择让存储应用程序用哪一 IP 地址来访问存储卷。针对网关定义的每个网络适配器代表您可以选择的一个 IP 地址。有关如何向网关添加网络适配器的信息，请参见 [针对多个网络适配器 \(NIC\) 配置 AWS Storage Gateway \(p. 229\)](#)。

如需使用指定的网络适配器创建存储卷。

- 在 AWS Storage Gateway 控制台的导航窗格中，选择您希望使用的网关，然后选择卷选项卡。

2. 单击创建新卷。
3. 按 [管理存储卷 \(网关缓存\)](#) (p. 171) 或 [管理存储卷 \(网关存储\)](#) (p. 173) 步骤中所述配置存储卷。
4. 选择要使用的 IP 地址以访问卷。

请注意，创建存储卷对话框将显示主机 IP 的下拉列表，针对网关 VM 为每个适配器配置一个 IP 地址。如果网关 VM 仅针对一个网络适配器配置，由于仅有一个 IP 地址，下拉列表将会禁用。



The screenshot shows a 'Create Storage Volume' dialog box with the following fields and values:

- Disk: SCSI (0:4) (with a 'Preserve existing data' checkbox)
- iSCSI Target Name: iqn.1997-05.com.amazon:myvolume
- Based on Snapshot ID: (empty)
- Size: 20 GiB
- Host IP: 192.168.99.145 (highlighted with a red box)
- Port: 3260

Buttons: Cancel, Create Volume

5. 单击创建卷。

若要创建到存储卷的连接，请参见 [配置应用程序对存储卷的访问](#) (p. 153)。

## 卷网关 ( 网关缓存或网关存储 ) 问题排查

本部分讨论排查网关相关以及存储卷相关的问题。网关问题排查分为两个部分：本地网关和部署到 Amazon EC2 的网关。场内网关故障诊断问题涵盖 VMware ESXi 或者 Microsoft Hyper-V 平台上部署的网关。存储卷的故障诊断问题适用于所有网关类型。

### Topics

- [排查场内网关问题](#) (p. 236)
- [Amazon EC2 网关问题诊断](#) (p. 238)
- [排查存储卷问题](#) (p. 239)
- [使用还原快照 \(网关缓存\)](#) (p. 241)

## 排查场内网关问题

下表列出了您在使用场内网关时可能遇到的典型问题。

问题	措施
<p>您找不到网关的 IP 地址。</p>	<p>请使用管理程序客户端连接主机，以便查找网关 IP 地址。</p> <ul style="list-style-type: none"> <li>对于 VMware ESXi，可在摘要选项卡上的 vSphere 客户端中找到 VM 的 IP 地址（请参见 <a href="#">激活 AWS Storage Gateway (p. 109)</a>）。</li> <li>对于 Microsoft Hyper-V，可登录本地控制台查找 VM 的 IP 地址（请参见 <a href="#">激活 AWS Storage Gateway (p. 128)</a>）。</li> </ul> <p>如果您仍然难以找到网关 IP 地址：</p> <ul style="list-style-type: none"> <li>检查 VM 是否已启动。仅在 VM 已启动的情况下，IP 地址才会分配给您的网关。</li> <li>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顺序。</li> </ul>
<p>当您单击 AWS Storage Gateway 控制台中的继续激活按钮时，网关的激活过程将失败。</p>	<ul style="list-style-type: none"> <li>检查网关 VM 是否可通过从客户端 ping 通。</li> <li>检查 VM 是否有到 Internet 的网络连接；如果没有，您可能需要配置 SOCKS 代理。有关更多信息，请参见 <a href="#">将 AWS Storage Gateway 的路由选为通过代理 (p. 222)</a>。</li> <li>检查一下主机的时间是否准确，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，请参见 <a href="#">同步您的网关 VM 时间 (p. 227)</a>。</li> <li>执行这些步骤后，您可以使用 AWS Storage Gateway 控制台和设置并激活网关向导重新尝试网关部署。</li> <li>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，请参见 <a href="#">要求 (p. 7)</a>。</li> </ul>
<p>您需要移除分配为上传缓冲区的一个磁盘，因为您希望降低网关上传缓冲区空间的量或者您需要替换用作上传缓冲区的已失效磁盘。</p>	<p>有关移除分配为上传缓冲区空间的磁盘的说明，请参见 <a href="#">移除上传缓冲区容量 (p. 179)</a> 或 <a href="#">移除上传缓冲区容量 (网关存储) (p. 184)</a>。</p>
<p>您需要提高网关和 AWS 之间的带宽。</p>	<p>您可以在 NIC 上设置一个独立于您的应用程序和网关 VM 之间的连接的通往 AWS 的 Internet 连接，从而提高网关到 AWS 之间的带宽。在您拥有到 AWS 的高带宽连接并且希望避免带宽争用的情况下（尤其是在快照还原期间），这样做很有用处。对于高吞吐量工作负载需求，您可以使用 <a href="#">AWS Direct Connect</a> 在本地网关和 AWS 间建立专用网络连接。若要测量从网关到 AWS 的连接带宽，请使用网关的 <code>CloudBytesDownloaded</code> 和 <code>CloudBytesUploaded</code> 指标（请参见 <a href="#">衡量网关和 AWS 间的性能 (p. 246)</a>）。提高 Internet 连接性能有助于确保您的上传缓冲区不被填满。</p>

问题	措施
往返您的网关的吞吐量将为零。	<ul style="list-style-type: none"> <li>在 AWS Storage Gateway 控制台中的网关选项卡上，验证网关 VM 的 IP 地址是否与您在使用管理程序客户端软件（即 VMware vSphere 客户端或者 Microsoft Hyper-V Manager）中看到的相同。如果您发现了不一致，请从 AWS Storage Gateway 控制台重启网关，如 <a href="#">使用 AWS Storage Gateway 控制台关停并启动网关 (p. 210)</a> 中所述。在重新启动后，AWS Storage Gateway 控制台的网关选项卡中的 IP 地址字段应匹配您通过管理程序客户端确定的网关的 IP 地址。</li> <li>对于 VMware ESXi，可在摘要选项卡上的 vSphere 客户端中找到 VM 的 IP 地址（请参见 <a href="#">激活 AWS Storage Gateway (p. 109)</a>）。</li> <li>对于 Microsoft Hyper-V，可登录本地控制台查找 VM 的 IP 地址（请参见 <a href="#">激活 AWS Storage Gateway (p. 128)</a>）。</li> <li>按 <a href="#">测试 AWS Storage Gateway 到 Internet 的连接 (p. 226)</a> 中所述，检查网关到 AWS 的连接性。</li> <li>检查网关的网络适配器配置，同时确保您打算为网关启动的所有接口均已启用。若要查看网关的网络适配器配置，请遵循 <a href="#">将您的 AWS Storage Gateway 配置为使用静态 IP 地址 (p. 224)</a> 的指示并选择用于查看网关的网络配置的选项。</li> </ul> <p>您可以从 Amazon CloudWatch 控制台查看往返网关的吞吐量。有关测量网关到 AWS 之间吞吐量的更多信息，请参见 <a href="#">衡量网关和 AWS 间的性能 (p. 246)</a>。</p>
您在 Microsoft Hyper-V 上导入（部署）AWS Storage Gateway 是遇到问题。	请参见附录中的 <a href="#">故障诊断 Microsoft Hyper-V 设置 (p. 453)</a> 。那里的提示涵盖一些您在 Microsoft Hyper-V 上部署网关时遇到的常见问题。

## Amazon EC2 网关问题诊断

下表列出了您在使用 Amazon Elastic Compute Cloud (Amazon EC2) 上部署的网关时可能遇到的典型问题。有关本地网关和 Amazon EC2 中部署的网关之间的差异的更多信息，请参见 [在 Amazon EC2 上部署并激活 AWS Storage Gateway \(p. 133\)](#)。

问题	措施
当您单击 AWS Storage Gateway 控制台中的继续激活按钮时，Amazon EC2 网关的激活过程将失败。	<p>如果过了一会激活仍未出现，请在 Amazon EC2 控制台中检查下列内容：</p> <ul style="list-style-type: none"> <li>已在实例关联的安全组中启用端口 80。有关添加安全组规则的详细信息，请转到 <i>Amazon Elastic Compute Cloud 用户指南</i> 中的 <a href="#">添加安全组规则</a>。</li> <li>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”。</li> </ul> <p>在纠正问题后，请转到 AWS Storage Gateway 控制台，单击在 Amazon EC2 上部署新网关，并重新输入实例的 IP 地址来重新尝试激活网关。</p>

问题	措施
您在实例的列表中找不到 Amazon EC2 网关实例。	<p>例如，如果您没有为实例提供资源标签，同时还有许多实例在运行，因此很难了解您在网关中部署了哪些实例，那么可以采取下列操作查找网关实例：</p> <ul style="list-style-type: none"> <li>在实例的说明选项卡中，查看亚马逊系统映像 (AMI) 名称。基于 AWS Storage Gateway AMI 的实例应该以“aws-storage-gateway-ami”文本开头。</li> <li>如果您的实例不是基于 AWS Storage Gateway AMI，请查看实例的启动时间查找正确的实例。</li> </ul>
您创建了 Amazon EBS 卷，但不能将其附加到 Amazon EC2 网关实例。	查看与网关实例在同一可用区域中的有问题的 Amazon EBS 卷。如果可用区域中存在不一致，请在您的实例所在的同一可用区域中创建一个新的 Amazon EBS 卷。
您不能将启动程序附加到 Amazon EC2 网关的存储卷目标上。	查看启动实例时使用的安全组，其中包括的规则是否允许使用针对 iSCSI 的端口。端口通常设置为 3260。有关连接到存储卷的更多信息，请参见 <a href="#">配置应用程序对存储卷的访问 (p. 153)</a> 。
您激活了 Amazon EC2 网关，但在添加存储卷时，收到错误消息，表示您没有可用的磁盘空间。	没有为新激活的网关定义卷存储。在定义卷存储前，必须将本地磁盘分配给网关，以使用作上传缓冲区空间和缓冲存储。对于部署到 Amazon EC2 的网关，本地磁盘是附加到实例的 Amazon EBS 卷。这个错误消息很可能是因为未为实例定义 Amazon EBS 卷而出现。查看为运行网关的实例所定义的块存储设备。如果只存在两个块存储设备 (AMI 具有的默认设备)，那么应该添加存储 (请参见 <a href="#">在 Amazon EC2 上部署并激活 AWS Storage Gateway (p. 133)</a> )。在附加两个或更多的 Amazon EBS 卷后，尝试在网关上创建卷存储。
您必须移除为用作上传缓冲区空间而分配的磁盘，因为要减少上传缓冲区空间大小。	按 <a href="#">从 Amazon EC2-托管的网关中删除 Amazon EBS 卷 (p. 141)</a> 中的步骤操作。
往返您的 Amazon EC2 网关的吞吐量将下降为零。	<ul style="list-style-type: none"> <li>验证网关实例是否在运行。例如，如果实例因为重新启动而正在启动，请等待该实例重新启动。</li> <li>验证是否尚未更改网关 IP。如果实例停止然后重新启动，那么实例的 IP 地址可能会出现更改。在这种情况下，您必须重新激活新的网关。</li> </ul> <p>您可以从 Amazon CloudWatch 控制台查看往返网关的吞吐量。有关测量网关到 AWS 之间吞吐量的更多信息，请参见 <a href="#">衡量网关和 AWS 间的性能 (p. 246)</a>。</p>



#### Warning

对于部署在 Amazon EC2 实例上的 Amazon Storage Gateway，不支持通过公共 Internet 访问网关。无法使用 EC2 实例的弹性 IP 地址作为目标地址。

## 排查存储卷问题

下表列出了您在使用存储卷时可能遇到的最典型问题。

问题	措施
AWS Storage Gateway 控制台指示您卷的状态为 <a href="#">UPLOAD BUFFER NOT CONFIGURED</a> (p. 169)。	向网关添加上传缓冲区空间。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，请参见资源： <a href="#">如需使用控制台为您的网关将本地磁盘配置为上传缓冲区</a> (p. 179) 或 <a href="#">如需使用控制台为网关配置上传缓冲区</a> (p. 184)。
AWS Storage Gateway 控制台指示您卷的状态为 <a href="#">IRRECOVERABLE</a> (p. 169)。	<p>存储卷无法再使用。您可以尝试在 AWS Storage Gateway 控制台中删除卷。如果卷上有数据，您就可以根据最初用来创建存储卷的 VM 本地磁盘还原这些数据。创建新的存储卷时，选择保留现有数据。有关更多信息，请参见 <a href="#">管理 AWS Storage Gateway 中的存储卷</a> (p. 167)。删除存储卷前，请删除卷的待创建快照。有关更多信息，请参见 <a href="#">删除快照</a> (p. 197)。</p> <p>如果在 AWS Storage Gateway 控制台中删除该卷不起作用，那么分配作存储卷的该磁盘可能已从 VM 错误移除，并且无法从设备移除。</p>
AWS Storage Gateway 控制台指示您卷的状态为 <a href="#">PASS THROUGH</a> (p. 169)。	<p>卷可能因数种原因处于 <a href="#">PASS THROUGH</a> (p. 169) 状态。应针对部分原因采取行动，而另一些原因无需行动。</p> <p>在存储卷处于 PASS THROUGH 且网关用完上传缓冲区空间的情形中，您应该采取相应的行动。若要验证过去是否超出了上传缓冲区，可以查看 Amazon CloudWatch 控制台中的 <code>UploadBufferPercentUsed</code> 指标（请参见 <a href="#">监控上传缓冲区</a> (p. 249)）。如果网关由于用完了上传缓冲区空间而处于 PASS THROUGH 状况，您应该向网关分配更多的上传缓冲区空间。添加更多的上传缓冲区空间将会导致您的存储卷自动从 PASS THROUGH 转为 <a href="#">BOOTSTRAPPING</a> (p. 169) 后再转为 <a href="#">AVAILABLE</a> (p. 169)。在 BOOTSTRAPPING 状况期间，网关从存储卷的磁盘读取数据，将这些数据上传到 Amazon S3，然后根据需要赶上变化。网关紧跟着将存储卷数据保存到 Amazon S3 之后，卷状况即转为 AVAILABLE，并且可重新开始拍摄快照。请注意当存储卷处于 PASS THROUGH 或 BOOTSTRAPPING 状态时，您可以从存储卷磁盘读取和写入数据。有关添加更多上传缓冲区空间的更多信息，请参见 <a href="#">管理上传缓冲区（网关存储）</a> (p. 183)。</p> <p>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，请参见 <a href="#">如需为网关的上传缓冲区设置阈值警报</a> (p. 249)。</p> <p>另一个无需采取行动的情形是存储卷处于 PASS THROUGH，且该存储卷因为另一个卷目前正处于引导中而在排队等待。网关在同一时间自举一个卷。</p> <p>PASS THROUGH 状况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，请参见 <a href="#">移除上传缓冲区容量</a> (p. 179) 或 <a href="#">移除上传缓冲区容量（网关存储）</a> (p. 184)。</p>
您的存储卷 iSCSI 目标不在磁盘管理控制台 (Windows) 中显示。	检查您是否为网关配置了上传缓冲区。有关更多信息，请参见 <a href="#">如需使用控制台为您的网关将本地磁盘配置为上传缓冲区</a> (p. 179) 或 <a href="#">如需使用控制台为网关配置上传缓冲区</a> (p. 184)。
建议您更改存储卷的 iSCSI 目标名称。	未删除卷且未使用新目标名称添加卷的情况下，无法配置目标名称。您可以将数据保存在卷上。有关创建存储卷的信息，请参见 <a href="#">管理存储卷（网关缓存）</a> (p. 171) 或 <a href="#">管理存储卷（网关存储）</a> (p. 173)。

问题	措施
您计划的存储卷快照未创建。	<p>检查您的卷是否处于 <a href="#">PASS THROUGH (p. 169)</a>，或者网关的上传缓冲区是否在安排快照拍摄前被填满。您可以在 Amazon CloudWatch 控制台中检查网关的 <code>UploadBufferPercentUsed</code> 指标，并针对该指标创建警报。有关更多信息，请参见 <a href="#">监控上传缓冲区 (p. 249)</a> 和 <a href="#">如需为网关的上传缓冲区设置上阈值警报 (p. 249)</a>。</p>
您需要移除存储卷，因为该卷不再需要，或者您需要替换已失效的存储卷。	<p>您应该首先使用 AWS Storage Gateway 控制台移除该卷（请参见 <a href="#">如需移除存储卷 (p. 173)</a>），然后使用管理程序客户端移除备份存储。</p> <ul style="list-style-type: none"> <li>对于 VMware ESXi，请按照 <a href="#">移除底层本地磁盘 (VMware ESXi) (p. 175)</a> 中的说明移除备份存储。</li> <li>对于 Microsoft Hyper-V，请按照 <a href="#">移除底层本地磁盘 (Microsoft Hyper-V) (p. 176)</a> 中的说明移除备份存储。</li> </ul>
从应用程序到存储卷的吞吐量降为零。	<ul style="list-style-type: none"> <li>检查存储卷的主机 IP 地址是否匹配显示在 vSphere 客户端的摘要选项卡中的地址。您可以在 AWS Storage Gateway 控制台的存储卷的 iSCSI 目标信息选项卡中找到存储卷的主机 IP 字段。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 AWS Storage Gateway 控制台重启您的网关，如 <a href="#">使用 AWS Storage Gateway 控制台关停并启动网关 (p. 210)</a> 中所述。重启后，存储卷的 iSCSI 目标信息选项卡中的主机 IP 地址应该匹配 vSphere 客户端的网关摘要选项卡中的 IP 地址。</li> <li>检查 <a href="#">未找到 IP 地址</a> 是否出现在该存储卷的主机 IP 字段中。举例来说，当您创建一个与配有两个或以上网络适配器的网关中的某个网络适配器的 IP 地址关联的存储卷时，可能会发生这种情况。当您移除或禁用存储卷关联的网络适配器时，将显示未找到 IP 地址消息。要解决这一问题，请在保存现有数据的同时删除存储卷然后重新创建。有关更多信息，请参见 <a href="#">管理 AWS Storage Gateway 中的存储卷 (p. 167)</a>。</li> <li>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，请参见 <a href="#">配置应用程序对存储卷的访问 (p. 153)</a>。</li> </ul> <p>您可以查看存储卷的吞吐量并从 Amazon CloudWatch 控制台创建警报。有关测量应用程序到存储卷的吞吐量的更多信息，请参见 <a href="#">衡量您的应用程序和网关间的性能 (p. 245)</a>。</p>

## 使用还原快照（网关缓存）

AWS Storage Gateway 在网关缓存卷架构中提供各个卷的还原点。卷的还原点是一个时间点，在这样的点上该卷的所有数据均一致，并且您可以从该点创建快照。您可以在网关无法到达或网关存储卷无法还原时，使用快照来创建新卷。

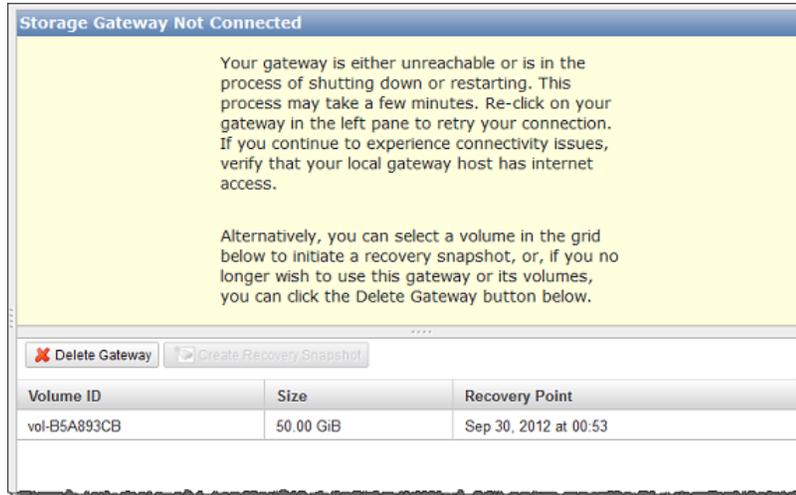
每个网关缓存卷的卷还原点是自动维护的，您还可以根据特定情况拍摄快照，或者为该卷设置快照计划。有关快照的更多信息，请参见 [使用快照 \(p. 187\)](#)。

网关无法到达时（例如关停网关后），您可以选择从卷的还原点创建快照。

如需创建并使用无法到达的网关的卷的还原快照

1. 在 AWS 存储网关控制台的导航窗格中，选择无法到达的网关。

网关卷的列表显示。



2. 选择还原快照所从创建的卷。
3. 单击创建恢复快照按钮。

AWS Storage Gateway 初始化快照进程。



4. 在已创建恢复点对话框中，单击关闭。



5. 使用 [查找快照](#) (p. 188) 过程中的步骤查找快照。
6. 使用 [还原快照](#) (p. 205) 中的某个步骤还原快照。

## 优化 AWS Storage Gateway 性能

本部分提供有关如何优化网关性能的信息。向网关添加资源以及向应用程序服务器添加资源是这些指导的基础。

## 向您的网关添加资源

- 使用更高性能的磁盘—您可以添加串行连接 SCSI (SAS) 磁盘和固态硬盘 (SSD) 等高性能磁盘，也可以直接从 SAN 连接虚拟磁盘到您的 VM，而不用通过 VMware 的 VMFS 层或 Microsoft Hyper-V 的 NTFS 层连接。更好的磁盘性能一般可取得更好的吞吐量和每秒输入/输出操作 (IOPS)。如需测量吞吐量，请将 ReadBytes 和 WriteBytes 指标与 Samples Amazon CloudWatch 统计数据结合使用。例如，ReadBytes 指标的 Samples 统计数据在五分钟的采样周期内除以 300 秒，可得出每秒输入/输出操作 (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。有关网关指标的更多信息，请参见 [衡量网关和 AWS 间的性能 \(p. 246\)](#)。
- 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。您应该确认分配到网关 VM 的四个虚拟处理器由四个核心支持，并且您没有超额预订主机服务器的 CPU。将更多 CPU 添加到网关虚拟服务器时，您并行增加网关处理两方面的能力，即存储应用程序到本地存储器的数据的能力以及上传这些数据到 Amazon S3 的能力。更多 CPU 也可确保您的网关在主机与其他 VM 共享时获得足够的 CPU 资源。这样做一般可以取得更加吞吐量的效果。
- 更改存储卷配置—如果您发现向网关添加更多的存储卷降低了到网关的吞吐量，就应该考虑添加存储卷到另一网关。尤其在存储卷用于高吞吐量应用程序的情况下，您就应该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。若要测量存储卷吞吐量，请使用 ReadBytes 和 WriteBytes 指标（请参见 [衡量您的应用程序和网关间的性能 \(p. 245\)](#)）。
- 使用独立物理磁盘支持网关虚拟磁盘—在网关缓存卷设置中预配置网关缓存卷设置时，我们强烈建议您不要为使用相同的底层物理磁盘的上传缓冲区和缓存存储空间预配置本地磁盘。同样地，对于网关存储卷设置，强烈建议您不要为使用相同的底层物理磁盘的上传缓冲区和应用程序存储空间预配置本地磁盘。例如，对于 VMware ESXi，底层物理存储资源表示为 VMware ESXi 中的数据存储器。部署网关 VM 时，您选择用来存储 VM 文件的数据存储器。预配置虚拟磁盘时（例如要用作上传缓冲区），您可以选择将虚拟磁盘存储在和 VM 一样的数据存储中。如果您有一个以上的数据存储器，强烈建议您选择将一个数据存储器用于正在创建的各类型本地存储器。仅由一个底层物理磁盘支持，或者仅由一个 RAID 1 等低性能 RAID 配置支持的数据存储器可能在某些情况下导致性能不佳，例如在同时用来支持一个网关缓存卷设置中的缓存存储空间和上传缓冲区的情况下。

## 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—确保应用程序和网关之间的带宽可维持您的应用程序需求。您可以使用网关的 ReadBytes 和 WriteBytes 指标（请参见 [衡量网关和 AWS 间的性能 \(p. 246\)](#)）来测量总数据吞吐量。将测得的吞吐量与预期的吞吐量比较（针对您的应用程序）。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，您可以提高 VM 和本地磁盘见的带宽（如果非直连）。
- 向应用程序环境添加 CPU 资源—如果您的应用程序可利用更多的 CPU 资源，那么添加更多的 CPU 可让您的应用程序扩展 IO 负载。

## 监控 AWS Storage Gateway

### Topics

- [使用 Amazon CloudWatch 控制台 \(p. 244\)](#)
- [衡量您的应用程序和网关间的性能 \(p. 245\)](#)
- [衡量网关和 AWS 间的性能 \(p. 246\)](#)
- [监控上传缓冲区 \(p. 249\)](#)
- [监控缓存卷 \(p. 252\)](#)
- [理解 AWS Storage Gateway 指标 \(p. 253\)](#)

在本部分，我们讨论如何监控您的 gateway，包括其与网关关联的卷（网关缓存和网关存储）以及上传缓冲区。使用 AWS 管理控制台查看 gateway 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、从 AWS 云检索数据的时间。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。

AWS Storage Gateway 提供 Amazon CloudWatch 指标，而不另外收费。AWS Storage Gateway 指标的记录期限为两周，便于您访问历史信息并协助您更好地了解 gateway 和卷的运行状况。有关 Amazon CloudWatch 的详细信息，请转到 [Amazon CloudWatch 开发人员指南](#)。

## 使用 Amazon CloudWatch 控制台

您可以利用 AWS 管理控制台或 Amazon CloudWatch API 获得 gateway 的监控数据。控制台根据来自 Amazon CloudWatch API 的原始数据显示一系列的图表。Amazon CloudWatch API 也可通过一项 [Amazon AWS 软件开发工具包 \(SDK\)](#) 或 [Amazon CloudWatch API](#) 工具使用。根据您的需求差异，您可能倾向于使用控制台中显示的图表，也可能倾向于检索自 API 的图表。

无论选择何种方法使用指标，您都必须指定下列信息。

- 首先，指定使用的指标维度。维度是帮助您对某指标进行唯一标识的名称/值对。AWS Storage Gateway 的维度是 GatewayId、GatewayName 和 VolumeId。Amazon CloudWatch 控制台中提供 Gateway Metrics 和 Volume Metrics 视图，便于选择与网关和卷相关的维度。有关维度的更多信息，请参见“Amazon CloudWatch 开发人员指南”中的 [维度](#)。
- 其次，指定指标值，例如 ReadBytes。



### Tip

如果 gateway 的名称在您希望查看指标的时间段内进行了更改，则应使用 GatewayId 来指定供您分析的指标。

下表总结了可供您使用的 AWS Storage Gateway 指标数据的类型。

Amazon CloudWatch 命名空间	维度	说明
AWS/StorageGateway	GatewayId, GatewayName	这些维度筛选描述 gateway 各个方面的指标数据。您使用 GatewayId 或 GatewayName 标识要使用的网关。  网关的吞吐量和延迟数据基于 gateway 中的所有卷。  数据在 5 分钟期间内自动可用，无需收费。
	VolumeId	该维度筛选存储卷专属指标数据。通过 VolumeId 标识要使用的存储卷。  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。许多常见任务在 Amazon CloudWatch 中进行了概述，并在下文列出，便于您使用：

- [列出可用指标](#)
- [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是您用来理解使用 AWS Storage Gateway 的应用程序存储性能状况的衡量指标。可使用 AWS Storage Gateway 指标衡量这三种值，这些指标在您使用正确的集合统计数据时为您提供。一项统计数据是某指标在指定时间内的集合。当您在 Amazon CloudWatch 中查看某指标的值时，将 Average 统计数据用于数据延迟（毫秒），将 Sum 统计数据用于数据吞吐量（每秒字节数），并且将 Samples 统计数据用于每秒操作 (IOPS)。有关更多信息，请参见“Amazon CloudWatch 开发人员指南”中的[统计数据](#)。

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

关注项	如何衡量
吞吐量	将 ReadBytes 和 WriteBytes 指标与 Sum Amazon CloudWatch 统计数据结合使用。例如，五分钟采样周期内的 ReadBytes 的 Sum 除以 300 秒可以得出以每秒字节数为速率单位的吞吐量。
延迟	将 ReadTime 和 WriteTime 指标与 Average Amazon CloudWatch 统计数据结合使用。例如，ReadTime 的 Average 为您提供采样周期内的每个操作的延迟时间。
IOPS	将 ReadBytes 和 WriteBytes 指标与 Samples Amazon CloudWatch 统计数据结合使用。例如，五分钟采样周期内的 ReadBytes 的 Samples 除以 300 秒，得出每秒输入/输出操作 (IOPS)。

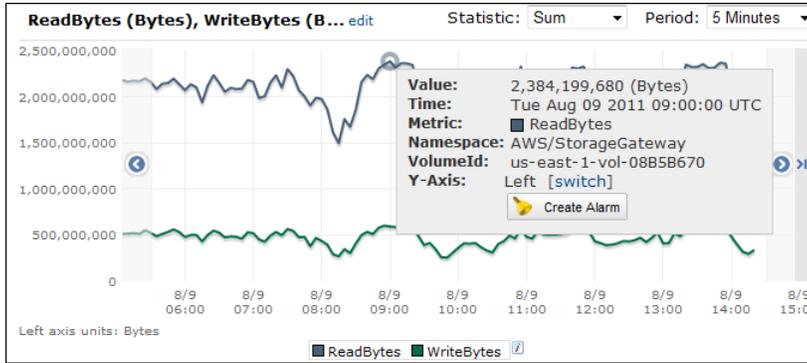
对于平均延迟图表和平均大小图表，平均值通过该期间内完成的操作（读取或写入，以适用于图表者为准）总数计算得出。

下面的任务假定您从 Amazon CloudWatch 控制台开始。

### 如需衡量应用程序到存储卷的数据吞吐量

1	选择 StorageGateway:卷指标并找出要使用的存储卷。
2	选择 ReadBytes 和 WriteBytes 指标。
3	选择一个时间范围。
4	选择 Sum 统计数据。
5	选择一个 5 分钟或更长的周期。
6	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。

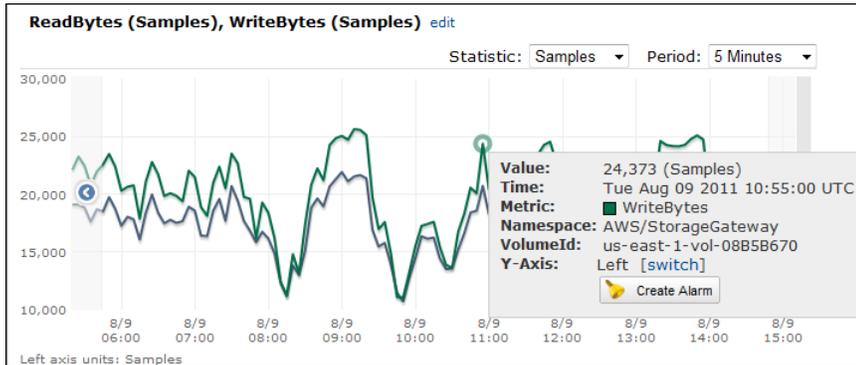
下面的示例使用 Sum 统计数据显示了存储卷的 ReadBytes 和 WriteBytes 指标。在示例中，将光标悬浮在数据点上就会显示该数据点信息，包括数值和字节数。将字节值除以周期（5 分钟）得出采样点当时的数据吞吐量。对于高亮点，读取吞吐量是 2 384 199 680 字节除以 300 秒，即 7.6 MB/s。



如需衡量从应用程序到存储卷的每秒输入/输出操作

1	选择 StorageGateway:卷指标并找出要使用的存储卷。
2	选择 ReadBytes 和 WriteBytes 指标。
3	选择一个时间范围。
4	选择 Samples 统计数据。
5	选择一个 5 分钟或更长的周期。
6	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）得出每秒输入/输出操作。

下面的示例使用 Samples 统计数据显示了存储卷的 ReadBytes 和 WriteBytes 指标。在示例中，将光标悬浮在数据点上就会显示该数据点的信息，包括其数值和样本数。用周期（5 分钟）除字节值以得出采样点当时的每秒操作数。对于高亮点，写入操作数是 24 373 字节除以 300 秒，即每秒 81 次写入操作。



## 衡量网关和 AWS 间的性能

数据吞吐量、数据延迟和每秒操作是您用来理解使用 AWS Storage Gateway 的应用程序存储性能状况的衡量指标。这三种值均可使用 AWS Storage Gateway 指标衡量，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 IOPS 的指标和相应统计数据。

关注项	如何衡量
吞吐量	将 ReadBytes 和 WriteBytes 指标与 Sum Amazon CloudWatch 统计数据结合使用。例如，五分钟采样周期内的 ReadBytes 的 Sum 除以 300 秒可以得出以每秒字节数为速率单位的吞吐量。

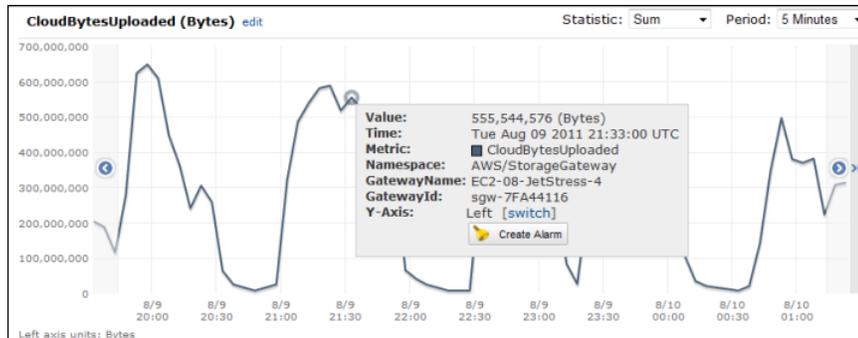
关注项	如何衡量
延迟	将 ReadTime 和 WriteTime 指标与 Average Amazon CloudWatch 统计数据结合使用。例如，ReadTime 的 Average 为您提供采样周期内的每个操作的延迟时间。
IOPS	将 ReadBytes 和 WriteBytes 指标与 Samples Amazon CloudWatch 统计数据结合使用。例如，五分钟样本周期内的 Samples 的 ReadBytes 除以 300 秒，得出每秒输入/输出操作 (IOPS)。
到 AWS 的吞吐量	将 CloudBytesDownloaded 和 CloudBytesUploaded 指标与 Sum Amazon CloudWatch 统计数据结合使用。例如，五分钟样本周期内的 CloudBytesDownloaded 的 Sum 除以 300 秒可得出以每秒字节数为单位的从 AWS 到网关的吞吐量。
到 AWS 的数据延迟	将 CloudDownloadLatency 指标与 Average 统计数据结合使用。例如，CloudDownloadLatency 指标的 Average 统计数据为您提供每次操作的延迟。

下面的任务假定您从 Amazon CloudWatch 控制台开始。

#### 如需衡量网关到 AWS 的上传数据吞吐量

1	选择 StorageGateway:Gateway Metrics 维度并找出要使用的网关。
2	选择 CloudBytesUploaded 指标。
3	选择一个时间范围。
4	选择 Sum 统计数据。
5	选择一个 5 分钟或更长的周期。
6	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。

下面的示例使用 Sum 统计数据显示了网关存储卷的 CloudBytesUploaded 指标。在示例中，将光标悬浮在数据点上，就会显示有关该数据点的信息，包括值和已上传的字节数。将该值除以周期（5 分钟），可得出样本点的吞吐量。对于高亮点，从网关到 AWS 的吞吐量为 555 544 576 字节除以 300 秒，即 1.7 MB/s。



#### 如需衡量网关的每操作延迟

1	选择 StorageGateway:Gateway Metrics 维度并找出要使用的网关。
---	------------------------------------------------

2	选择 ReadTime 和 WriteTime 指标。
3	选择一个时间范围。
4	选择 Average 统计数据。
5	选择一个 5 分钟的周期以匹配默认报告时间。
6	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。

如需衡量从网关到 AWS 的数据延迟

1	选择 StorageGateway:GatewayMetrics 维度并找出要使用的网关。
2	选择 CloudDownloadLatency 指标。
3	选择一个时间范围。
4	选择 Average 统计数据。
5	选择一个 5 分钟的周期以匹配默认报告时间。
6	得出的按时间排序的数据点集包含以秒为单位的延迟。

如需对网关到 AWS 的吞吐量设置上阈值

1	启动创建警报向导。
2	选择 StorageGateway:Gateway Metrics 维度并找出要使用的网关。
3	选择 CloudBytesUploaded 指标。
4	通过定义 CloudBytesUploaded 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 CloudBytesUploaded 指标在 60 分钟内大于 10 MB 时的警报状态。
5	针对该警报状态配置要采取的行动。
6	创建警报。

如需设置从 AWS 读取数据的上阈值警报

1	启动创建警报向导。
2	选择 StorageGateway:Gateway Metrics 维度并找出要使用的网关。
3	选择 CloudDownloadLatency 指标。
4	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 60,000 毫秒时的警报状态。
5	针对该警报状态配置要采取的行动。
6	创建警报。

## 监控上传缓冲区

以下部分讨论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。这样可以让您能够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，主动添加缓冲区容量。

监控上传缓冲区适用于网关缓存和网关存储架构。有关更多信息，请参见 [AWS Storage Gateway 的运行原理 \(架构\) \(p. 3\)](#)。



### Note

WorkingStoragePercentUsed、WorkingStorageUsed 和 WorkingStorageFree 指标代表 AWS Storage Gateway 缓存卷功能发行前，仅适用于网关存储卷设置的上传缓冲区。现在您应使用等效上传缓冲区指标：适用于两种网关架构的 UploadBufferPercentUsed、UploadBufferUsed 和 UploadBufferFree。

关注项	如何衡量
上传缓冲区使用率	将 UploadBufferPercentUsed、UploadBufferUsed、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。

下面的任务假定您从 Amazon CloudWatch 控制台开始。

### 如需测量上传缓冲区使用率

1	选择 StorageGateway:Gateway Metrics 维度并找出要使用的网关。
2	选择 UploadBufferPercentUsed 指标。
3	选择一个时间范围。
4	选择 Average 统计数据。
5	选择一个 5 分钟的周期以匹配默认报告时间。
6	得出的按时间排序的数据点集包含上传缓冲区的使用率。

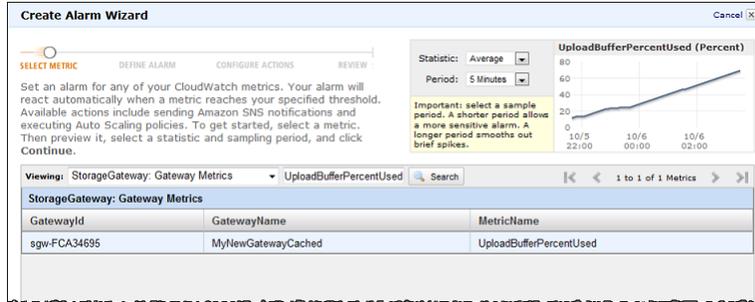
下面的上传缓冲区任务向您介绍如何使用 Amazon CloudWatch 控制台和创建警报向导创建警报。若要了解警报和阈值的更多信息，请参见 [创建 CloudWatch 警报](#)。

### 如需为网关的上传缓冲区设置上阈值警报

1. 启动创建警报向导。
  - a. 在 Amazon CloudWatch 控制台中，单击导航窗格中的警报链接。
  - b. 在您的 CloudWatch 警报窗格中，单击创建警报。



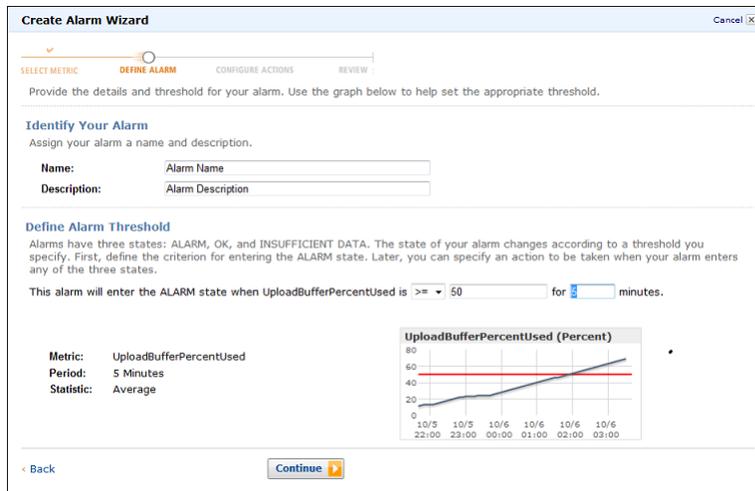
2. 为您的警报指定指标。
  - a. 在创建警报向导的选择指标页面中，选择 `AWS/StorageGateway:GatewayId,GatewayName` 维度并找出您希望使用的网关。
  - b. 选择 `UploadBufferPercentUsed` 指标。使用 `Average` 统计数据 and 5 分钟的周期。



- c. 单击继续。

3. 定义警报名称、描述和阈值。
  - a. 在创建警报向导的定义警报页面中，通过分别在名称和描述字段中给您的警报命名和描述来标识警报。
  - b. 定义警报阈值。

在下面的示例中，警报状态针对 5 分钟内大于或等于 50% 的 `UploadBufferPercentUsed` 定义。



- c. 单击继续。

4. 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中，从警报状态下拉列表选择警报。
  - b. 从主题下拉列表选择选择或创建电子邮件主题...

定义电子邮件主题即设置子 Amazon SNS 主题。有关 Amazon SNS 的更多信息，请参见[设置 Amazon SNS](#)。

- c. 在主题字段中，输入主题的描述名。

- d. 单击添加操作。

When Alarm state is	Take action	Action details
ALARM	Send Notification	Topic: my-alarm-topic    Email(s): user@example.com

- e. 单击继续。

5. 核查警报设置并创建警报。

- a. 在创建警报向导的审核页面中，审核警报定义、指标以及此步骤的关联操作。

**Alarm Definition**

Name: Alarm Name  
Description: Alarm Description  
In ALARM state when: the value is  $\geq 50$  for 5 minutes

**Metric**

Namespace: AWS/StorageGateway  
MetricName: UploadBufferPercentUsed  
GatewayName: MyNewGatewayCached  
GatewayId: sgw-FCA34695  
Period / Statistic: 5 Minutes / Average

**Alarm Actions**

Actions: When alarm state is **ALARM**  
Action Type: Send Notification to New Topic  
Action: Notify topic: my-alarm-topic (user@example.com)

- b. 检查警报摘要后，单击保存警报。

6. 确认您对警报主题的订阅。

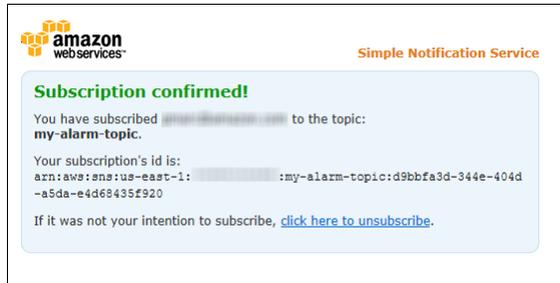
- a. 打开发送到您创建主题时提供的电子邮箱地址的 Amazon Simple Notification Service (Amazon SNS) 电子邮件。

以下示例显示通知。



b. 单击电子邮件中的链接，确认您的订阅。

订阅确认显示。



## 监控缓存卷

以下部分讨论如何监控网关的缓存卷以及如何创建警报，以便您在缓存参数超过指定阈值时收到通知。这样可以让您主动向网关添加缓存卷。

监控缓存卷仅适用于网关缓存架构。有关更多信息，请参见 [AWS Storage Gateway 的运行原理（架构）](#) (p. 3)。

关注项	如何衡量
缓存总使用率	将 CachePercentUsed 和 TotalCacheSize 指标结合 Average 统计数据使用。例如，将 CachePercentageUsed 结合 Average 统计数据使用以分析一段时间内的缓存使用率。  TotalCacheSize 指标仅在您向网关添加缓存时变化。
网关送达的读取请求百分率。	将 CacheHitPercent 指标与 Average 统计数据结合使用。  一般而言，您会希望 CacheHitPercent 保持较高。
缓存废数据率，亦即含有未上传到 AWS 的内容。	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。

下面的任务假定您从 Amazon CloudWatch 控制台开始。

如需测量网关及其所有卷的废数据率

1	选择 StorageGateway:Gateway Metrics 维度并找出要使用的网关。
2	选择 CachePercentDirty 指标。

3	选择一个时间范围。
4	选择 Average 统计数据。
5	选择一个 5 分钟的周期以匹配默认报告时间。
6	得出的按时间排序的数据点集，包含缓存的废数据使用率。

如需测量卷的缓存废数据使用率

1	选择 StorageGateway:卷指标并找出要使用的卷。
2	选择 CachePercentDirty 指标。
3	选择一个时间范围。
4	选择 Average 统计数据。
5	选择一个 5 分钟的周期以匹配默认报告时间。
6	得出的按时间排序的数据点集，包含缓存的废数据使用率。

## 理解 AWS Storage Gateway 指标

Topics

- [网关指标 \(p. 253\)](#)
- [存储卷指标 \(p. 255\)](#)

### 网关指标

对于此处的讨论，我们将网关指标定义为范围限定到网关的指标，即这些指标用来衡量网关的某个方面。由于 gateway 包含一个或多个卷，gateway 专属的指标代表 gateway 上的所有卷。例如，CloudBytesUploaded 指标是在报告期间 gateway 发送给云的总字节数。它包括 gateway 上所有卷的活动。

使用 gateway 指标数据时，将指定您希望查看其指标的 gateway 的唯一标识。要这样做，您可以指定 GatewayId 或 GatewayName。需要使用网关的指标时，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，请参见 [使用 Amazon CloudWatch 控制台 \(p. 244\)](#)。

下表描述了可用于获取有关您的 gateway 信息的 AWS Storage Gateway 指标。表中的项根据功能按度量分组。

指标	说明
CacheHitPercent	缓存传送的应用程序读取率。该指标仅适用网关缓存卷的设置。样本在报告周期结束时采用。  单位：百分比
CachePercentageUsed	网关的缓存存储空间的百分使用率。该指标仅适用网关缓存卷的设置。样本在报告周期结束时采用。  单位：百分比

指标	说明
CachePercentDirty	<p>尚未持续到 AWS 的网关缓存百分率。该指标仅适用网关缓存卷的设置。样本在报告周期结束时采用。</p> <p>单位：百分比</p>
CloudBytesDownloaded	<p>gateway 在报告期间从 AWS 下载的预压缩总字节数。</p> <p>将此指标与 Sum 统计数据结合使用可衡量吞吐量，而与 Samples 统计数据结合可衡量每秒操作数 (IOPS)。</p> <p>单位：字节</p>
CloudDownloadLatency	<p>报告期间从 AWS 读取数据耗费的总毫秒数。</p> <p>将此指标与 Average 统计数据结合使用可测量延迟。</p> <p>单位：毫秒</p>
CloudBytesUploaded	<p>gateway 在报告期间上传到 AWS 的预压缩总字节数。</p> <p>将此指标与 Sum 统计数据结合使用可衡量吞吐量，而与 Samples 统计数据结合可衡量每秒操作数 (IOPS)。</p> <p>单位：字节</p>
UploadBufferFree	<p>网关的上传缓冲区未使用字节的总量。样本在报告周期结束时采用。</p> <p>单位：字节</p>
UploadBufferPercentUsed	<p>网关上传缓冲区的使用率。样本在报告周期结束时采用。</p> <p>单位：百分比</p>
UploadBufferUsed	<p>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。</p> <p>单位：字节</p>
QueuedWrites	<p>等待写入 AWS 的字节数，gateway 中的所有卷在报告周期结束时采样所得。这些字节保存在网关的工作存储空间中。</p> <p>单位：字节</p>
ReadBytes	<p>报告周期内 gateway 中的所有卷从场内应用程序读取的总字节数。</p> <p>将此指标与 Sum 统计数据结合使用可衡量吞吐量，而与 Samples 统计数据结合可衡量每秒操作数 (IOPS)。</p> <p>单位：字节</p>
ReadTime	<p>报告周期内 gateway 中所有卷从场内应用程序进行读取所耗费的总毫秒数。</p> <p>将此指标与 Average 统计数据结合使用可测量延迟。</p> <p>单位：毫秒</p>
TotalCacheSize	<p>以字节为单位的缓存总大小。该指标仅适用网关缓存卷的设置。样本在报告周期结束时采用。</p> <p>单位：字节</p>

指标	说明
WriteBytes	<p>报告周期内 gateway 中所有卷写入场内应用程序的总字节数。</p> <p>将此指标与 Sum 统计数据结合使用可衡量吞吐量，而与 Samples 统计数据结合可衡量每秒操作数 (IOPS)。</p> <p>单位：字节</p>
WriteTime	<p>报告周期内 gateway 中所有卷从场内应用程序进行写入所消耗的总毫秒数。</p> <p>将此指标与 Average 统计数据结合使用可测量延迟。</p> <p>单位：毫秒</p>
WorkingStorageFree	<p>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。</p> <p> <b>Note</b></p> <p>工作存储空间仅适用于网关存储卷设置。上传缓冲区适用于网关存储和网关缓存卷设置。如果您要使用两种类型的网关设置，可能会发现仅使用相应的上传缓冲区指标 UploadBufferFree 更为方便。</p> <p>单位：字节</p>
WorkingStoragePercentageUsed	<p>网关上传缓冲区的使用率。样本在报告周期结束时采用。</p> <p> <b>Note</b></p> <p>工作存储空间仅适用于网关存储卷设置。上传缓冲区适用于网关存储和网关缓存卷设置。如果您要使用两种类型的网关设置，可能会发现仅使用相应的上传缓冲区指标 UploadBufferPercentUsed 更为方便。</p> <p>单位：百分比</p>
WorkingStorageUsed	<p>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。</p> <p> <b>Note</b></p> <p>工作存储空间仅适用于网关存储卷设置。上传缓冲区适用于网关存储和网关缓存卷设置。如果您要使用两种类型的网关设置，可能会发现仅使用相应的上传缓冲区指标 UploadBufferUsed 更为方便。</p> <p>单位：字节</p>

## 存储卷指标

在本部分，我们讨论 AWS Storage Gateway 指标，这些指标为您提供网关存储卷的相关信息。gateway 的每个卷均有与其关联的一组指标。请注意，部分卷专属指标具有和网关专属指标相同的名称。这些指标代表同样种类的度量，但其范围限于卷，而非网关。您在使用指标前必须首先指定希望使用网关还是存储卷指标。尤其是使用卷指标时，您必须指定希望查看其指标的存储卷的 *VolumelId*。有关更多信息，请参见 [使用 Amazon CloudWatch 控制台 \(p. 244\)](#)。

下表描述了用来获取存储卷相关信息的 AWS Storage Gateway 指标。

指标	说明
CacheHitPercent	<p>应用程序从卷的读取百分率，由缓存传送。该指标仅适用于缓存卷。样本在报告周期结束时采用。</p> <p>在没有应用程序从卷读取的情况下，该指标报告 100%。</p> <p>单位：百分比</p>
CachePercentageUsed	<p>卷对网关缓存存储空间的总体使用率占比。该指标仅适用于缓存卷。样本在报告周期结束时采用。</p> <p>使用网关的 CachePercentageUsed 指标来查看网关缓存卷的总体使用率。有关更多信息，请参见 <a href="#">网关指标 (p. 253)</a>。</p> <p>单位：百分比</p>
CachePercentDirty	<p>卷对尚未传送到 AWS 的网关缓存总体比例的占比。该指标仅适用于缓存卷。样本在报告周期结束时采用。</p> <p>使用网关的 CachePercentDirty 指标来查看尚未传送到 AWS 的网关缓存总体比例。有关更多信息，请参见 <a href="#">网关指标 (p. 253)</a>。</p> <p>单位：百分比</p>
ReadBytes	<p>报告周期内从场内应用程序读取的总字节数。</p> <p>将此指标与 Sum 统计数据结合使用可衡量吞吐量，而与 Samples 统计数据结合可衡量每秒操作数 (IOPS)。</p> <p>单位：字节</p>
ReadTime	<p>报告周期内从场内应用程序进行读取所消耗的总毫秒数。</p> <p>将此指标与 Average 统计数据结合使用可测量延迟。</p> <p>单位：毫秒</p>
WriteBytes	<p>报告周期内写入到场内应用程序的总字节数。</p> <p>将此指标与 Sum 统计数据结合使用可衡量吞吐量，而与 Samples 统计数据结合可衡量每秒操作数 (IOPS)。</p> <p>单位：字节</p>
WriteTime	<p>报告周期内从场内应用程序进行写入所消耗的总毫秒数。</p> <p>将此指标与 Average 统计数据结合使用可测量延迟。</p> <p>单位：毫秒</p>
QueuedWrites	<p>等待写入到 AWS 的字节数，采样于报告周期结束时。</p> <p>单位：字节</p>

## 相关部分

- [AWS Storage Gateway 的 API 参考 \(p. 418\)](#)

## 网关 - 虚拟磁带库 ( 网关 VTL )

---

网关 VTL 提供了一种持久且经济实用的脱机数据归档解决方案。利用该解决方案提供的 VTL 接口，您可以通过现有的基于磁带的备份应用程序基础设施来将数据存储到您在网关 VTL 上创建的虚拟磁带盒上。使用媒体转换器和磁带驱动器预配置每个网关 VTL，可将这些媒体转换器和磁带驱动器作为 iSCSI 设备用于现有客户端备份应用程序。根据需要添加磁带盒以存档数据。

有关网关 VTL 架构的更多信息，请参见 [网关 - 虚拟磁带库 \( 网关 VTL \) 架构 \(p. 5\)](#)。有关提供的网关概念和存储解决方案的信息，请参见 [什么是 AWS Storage Gateway ? \(p. 1\)](#)。

以下部分提供了有关设置和管理网关 VTL 的信息。“入门”部分提供了端对端示例设置。您可以使用 AWS Storage Gateway 控制台执行这些任务，如下列主题所述。还可以使用 AWS Storage Gateway API ( 请参见 [AWS Storage Gateway 的 API 参考 \(p. 418\)](#) ) 或 AWS SDK 库以编程方式执行这些任务。

### Topics

- [入门 \( 网关 VTL \) \(p. 257\)](#)
- [设置网关 VTL \(p. 313\)](#)
- [管理已激活的网关 VTL \(p. 361\)](#)

## 入门 ( 网关 VTL )

本入门部分向 AWS Storage Gateway 新用户展示如何设置和使用全功能网关 VTL。

在尝试示例设置前，我们建议您阅读本指南中的以下各节：

- [什么是 AWS Storage Gateway ? \(p. 1\)](#)
- [AWS Storage Gateway 的运行原理 \( 架构 \) \(p. 3\)](#)

### Topics

- [注册 AWS Storage Gateway \(p. 258\)](#)
- [尝试示例虚拟磁带库 \(VTL\) 设置 \(p. 258\)](#)
- [我从这里可以继续进行哪些内容 ? \(p. 312\)](#)

### 下一步

注册 AWS : [注册 AWS Storage Gateway \(p. 258\)](#)

## 注册 AWS Storage Gateway

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

如需注册 AWS Storage Gateway

1. 请转至 <http://aws.amazon.com>，然后单击“注册”。
2. 按照屏幕上的说明进行操作。

在注册过程中，您会接到一个电话，需要您使用电话按键输入 PIN 码。

下一步

[尝试示例虚拟磁带库 \(VTL\) 设置 \(p. 258\)](#)

## 尝试示例虚拟磁带库 (VTL) 设置

在按本入门部分中的步骤进行操作时，将使用 AWS Storage Gateway 控制台中的设置并激活网关向导。在该向导的若干步骤中，您将在控制台以外执行任务，然后返回控制台。如果会话超时或浏览器关闭，您可以返回到控制台，从上一步继续执行。

Topics

- [在您开始之前 \(p. 258\)](#)
- [步骤 1：部署 VM 并激活网关 VTL \(p. 259\)](#)
- [步骤 2：配置本地存储和警报 \(p. 300\)](#)
- [步骤 3：使用 AWS Storage Gateway 控制台创建虚拟磁带 \(p. 301\)](#)
- [步骤 4：将网关 VTL 设备连接到 Windows 客户端 \(p. 302\)](#)
- [步骤 5：测试网关 VTL 设置 \(p. 304\)](#)
- [步骤 6：在示例练习后进行清除 \(p. 312\)](#)

在开始本练习前，请检查最低网关和 VM 要求。有关更多信息，请参阅 [要求 \(p. 7\)](#)。

下面总结了激活网关 VTL 和备份数据要遵循的步骤：

- 选择网关 VTL 配置
- 下载并配置主机 (VMware 或 Hyper-V)
- 配置本地存储
- 激活网关 VTL
- 配置本地存储
- 创建虚拟磁带
- 配置 VTL 设备作为 iSCSI 目标
- 配置备份软件以访问您的 VTL 设备
- 使用备份软件备份数据

## 在您开始之前

在开始练习之前，确保已安装以下软件：

- 虚拟机监控程序—将需要决定要将网关 VM 部署到 VMware ESXi 虚拟机监控程序还是 Microsoft Hyper-V 上。

有关更多信息，请参阅 [要求 \(p. 7\)](#)。

- 虚拟机监控程序客户端—根据虚拟机监控程序主机的不同，将需要安装相应的客户端。

有关更多信息，请参阅 [要求 \(p. 7\)](#)。

- 对于网关 VTL，还将需要安装客户端备份软件。

本指南中的示例使用 Symantec NetBackup 7.5 软件。有关 NetBackup 的信息，请转到 [Symantec NetBackup](#)。

本练习假定使用动态主机配置协议 (DHCP) 自动配置网关 IP 地址。如果部署 AWS Storage Gateway 的环境要求为网关指定静态 IP 地址，则可照做。有关配置网关以使用静态 IP 地址的详细信息，请参阅[将您的 AWS Storage Gateway 配置为使用静态 IP 地址 \(p. 224\)](#)。



### Important

从 90 天内的虚拟磁带架 (VTS) 检索数据会产生相关成本，因此在本练习中，请备份和检索少量数据以将成本降至最低。有关更多信息，请参阅 [AWS Storage Gateway 定价 \(p. 9\)](#)。

下一步

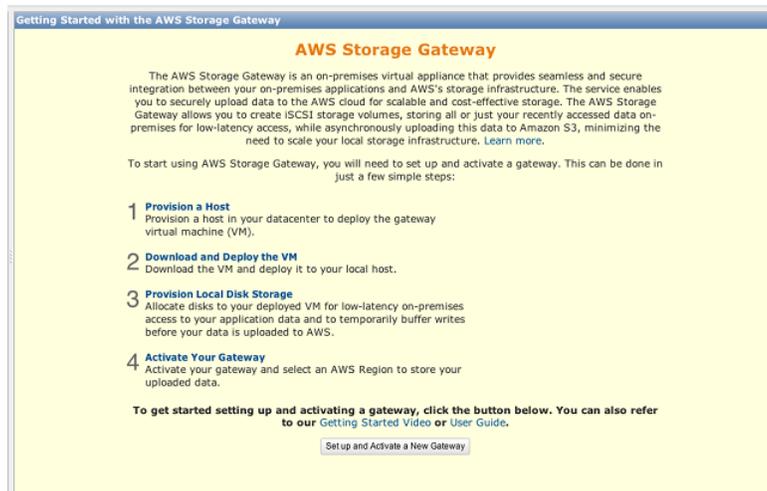
[步骤 1：部署 VM 并激活网关 VTL \(p. 259\)](#)

## 步骤 1：部署 VM 并激活网关 VTL

在本练习中，您下载并部署网关 VM，然后激活网关。转到 <http://console.aws.amazon.com/storagegateway> 上的控制台。如果您注册了服务但尚未激活网关，控制台将在您着手部署网关的情况下显示以下页面。

Topics

- [选择网关 VTL 配置 \(p. 260\)](#)
- [VMware 主机 \(p. 260\)](#)
- [Hyper-V 主机 \(p. 278\)](#)



如果已激活网关，则不会看到上一页。而是可通过在导航窗格中单击部署新网关，部署并激活新网关。



下一步

[选择网关 VTL 配置 \(p. 260\)](#)

## 选择网关 VTL 配置

### 选择网关配置

1. 在设置并激活网关向导中的配置主机步骤中，选择网关虚拟磁带库，然后单击继续。



选择网关配置后，接下来决定要在其上部署网关的虚拟化平台。VMware ESXi [VMware 主机 \(p. 260\)](#) 和 Microsoft Hyper-V 虚拟化 [Hyper-V 主机 \(p. 278\)](#) 支持网关 VTL。

2. 在下一页上，单击继续以选择虚拟化平台。

下一步

选择虚拟化平台：

- 配置 VMware 主机：[VMware 主机 \(p. 260\)](#)
- 配置 Microsoft Hyper-V 主机：[Hyper-V 主机 \(p. 278\)](#)

## VMware 主机

在本部分中，您将预配置场内 VMware 主机、向主机下载和部署网关 VM、配置网关 VM 并进行激活。

要设置 Microsoft Hyper-V 主机，请参阅 [Hyper-V 主机 \(p. 278\)](#) 平台。

Topics

- [配置 VMware 主机以部署 AWS Storage Gateway VM \(p. 260\)](#)
- [下载 AWS Storage Gateway VM 并将其部署在您的主机上 \(p. 261\)](#)
- [为网关 VTL VM 配置本地磁盘存储 \(p. 269\)](#)
- [激活 AWS Storage Gateway-VTL \(p. 275\)](#)

下一步

[配置 VMware 主机以部署 AWS Storage Gateway VM \(p. 260\)](#)

### 配置 VMware 主机以部署 AWS Storage Gateway VM

在本步骤中，您在数据中心创建 VMware 主机，用来部署网关虚拟机 (VM)。

如需预配置主机

1. 查看 [要求 \(p. 7\)](#) 中的最低主机要求。
2. 使用 VMware ESXi 管理程序在数据中心设置主机。

本指南中的附录提供安装管理程序操作系统的最低限度指导。有关更多信息，请参阅 [附录 B：为 AWS Storage Gateway 配置 VMware ESXi 主机 \(p. 442\)](#)。



#### Note

如果计划部署使用 VMware High Availability (HA) 进行故障转移保护的 AWS Storage Gateway，请参阅 [将 AWS Storage Gateway 与 VMware High Availability 配合使用 \(p. 314\)](#)。在本练习中，您将 AWS Storage Gateway VM 部署在未配置集群或故障转移的单个主机上。

下一步

[下载 AWS Storage Gateway VM 并将其部署在您的主机上 \(p. 261\)](#)

[下载 AWS Storage Gateway VM 并将其部署在您的主机上](#)

以 VMware ESX .ova 软件包形式提供 AWS Storage Gateway 虚拟机。本节介绍如何将 .ova 文件下载到本地、将其部署到主机以及将 VM 时间与主机时间同步。

Topics

- [下载 AWS Storage Gateway VM \(p. 261\)](#)
- [将 AWS Storage Gateway VM 部署到您的主机 \(p. 262\)](#)
- [将 VM 时间与主机时间同步 \(p. 266\)](#)



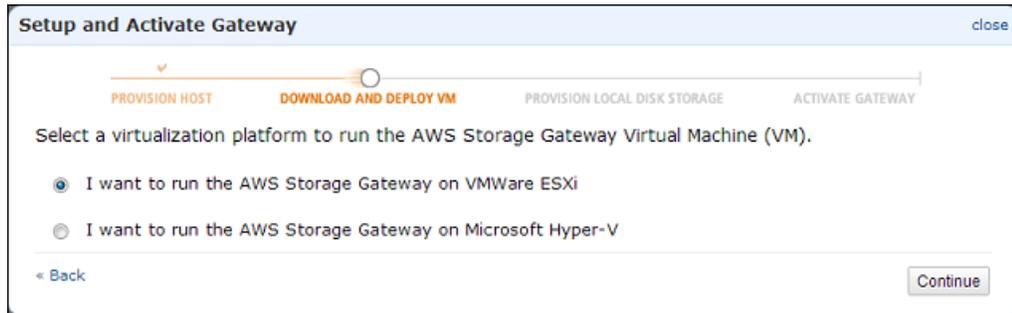
#### Important

要成功激活网关，就需要同步 VM 时间和主机时间。

[下载 AWS Storage Gateway VM](#)

如需下载该 VM

1. 在 [AWS Storage Gateway](#) 控制台的设置并激活网关向导中，导航到下载并部署 VM 页。
2. 选择我要在 VMware ESXi 上运行 AWS Storage Gateway，然后单击继续。



3. 单击下载以下载一个 .zip 文件，其中包含 .ova 文件。将 .zip 文件保存到计算机上的某个位置。



#### Note

.zip 文件的大小超过 500 MB，根据网速的不同，下载该文件可能耗时较长。



## 将 AWS Storage Gateway VM 部署到您的主机

1. 连接到您的管理程序主机：



### Note

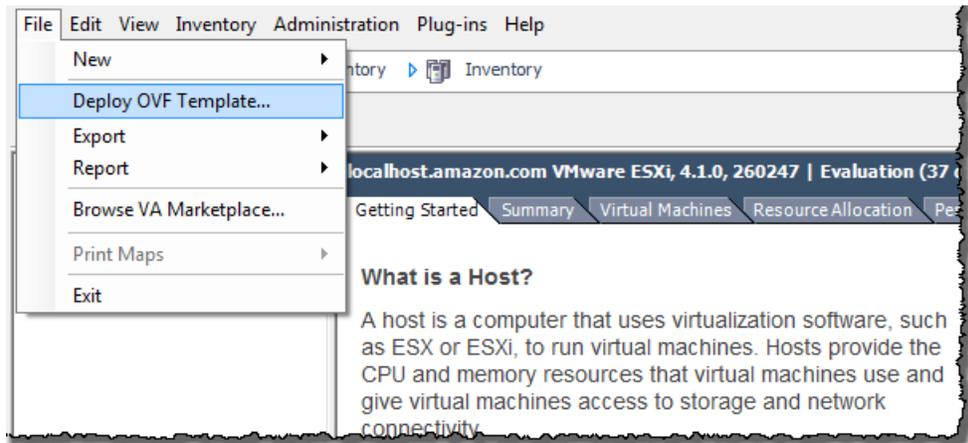
根据所用虚拟机监控程序版本的不同，这些过程中显示的图形用户界面 (GUI) 可能略有不同。

- a. 在您的 Windows 客户端上启动 VMware vSphere client。
- b. 在登录对话框中输入主机 IP 地址并在相应字段中输入登录证书。
- c. 单击登录。

您的 vSphere 客户端现已连接到您的主计算机。

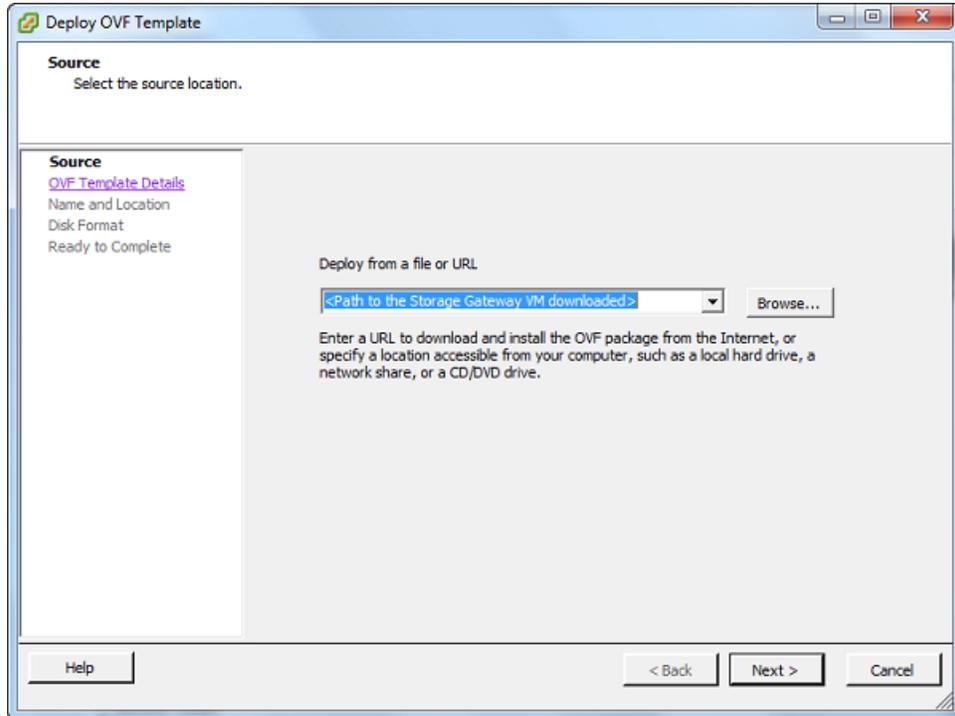
2. 将 AWS Storage Gateway VM 部署到主机上：

- a. 从 vSphere 客户端的文件菜单中，单击部署 OVF 模板。



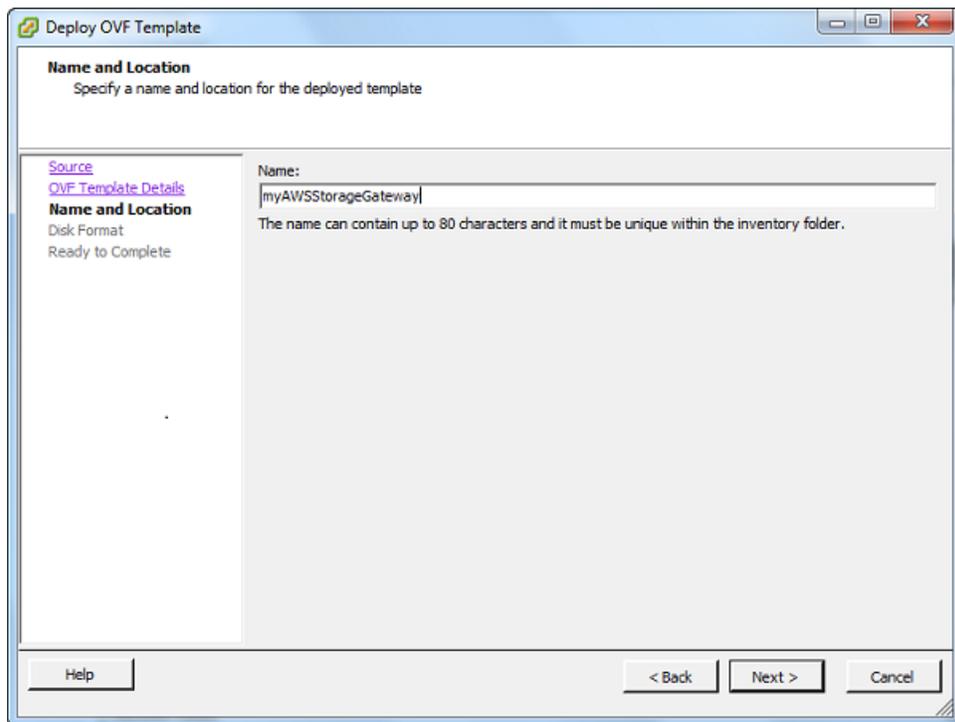
此操作将打开部署 OVF 模板向导。向导是让您提供部署 VM 所需信息的一系列步骤。

- b. 在源窗格中，提供 AWS Storage Gateway .ova 软件包的文件路径，然后单击下一步。



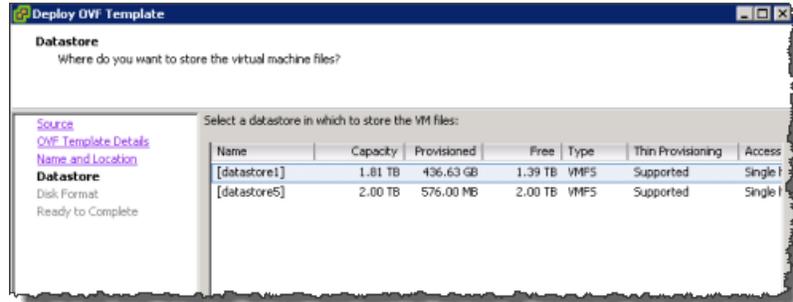
- c. 在 OVF 模板详细信息窗格中，单击下一步。
- d. 在名称和位置窗格中的名称字段中，输入 VM 名称，然后单击下一步。

该 VM 名称显示在 vSphere 客户端中。但是，AWS Storage Gateway 在任何位置均不使用此名称。



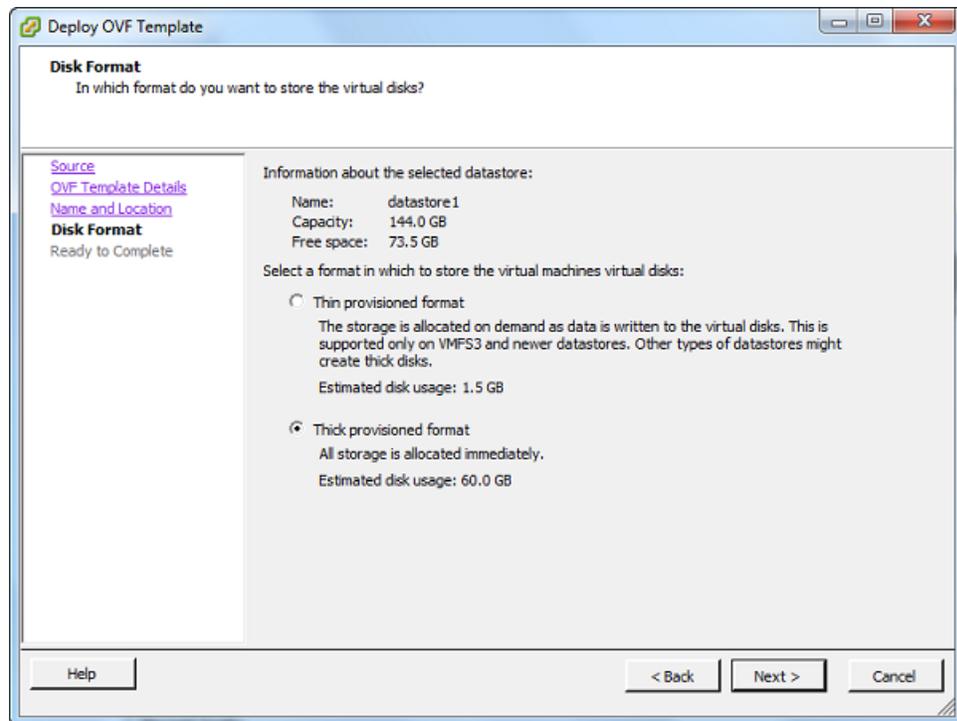
- e. 仅在主机具有多个数据存储时，才会显示以下数据存储窗格。在此窗格中，选择要从中部署 VM 的数据存储，然后单击下一步。如果您的主机仅有一个数据存储，请跳到下一步。

数据存储是底层物理存储资源的虚拟表示形式。下例展示一个主机，它具有两个数据存储：datastore1 和 datastore2。



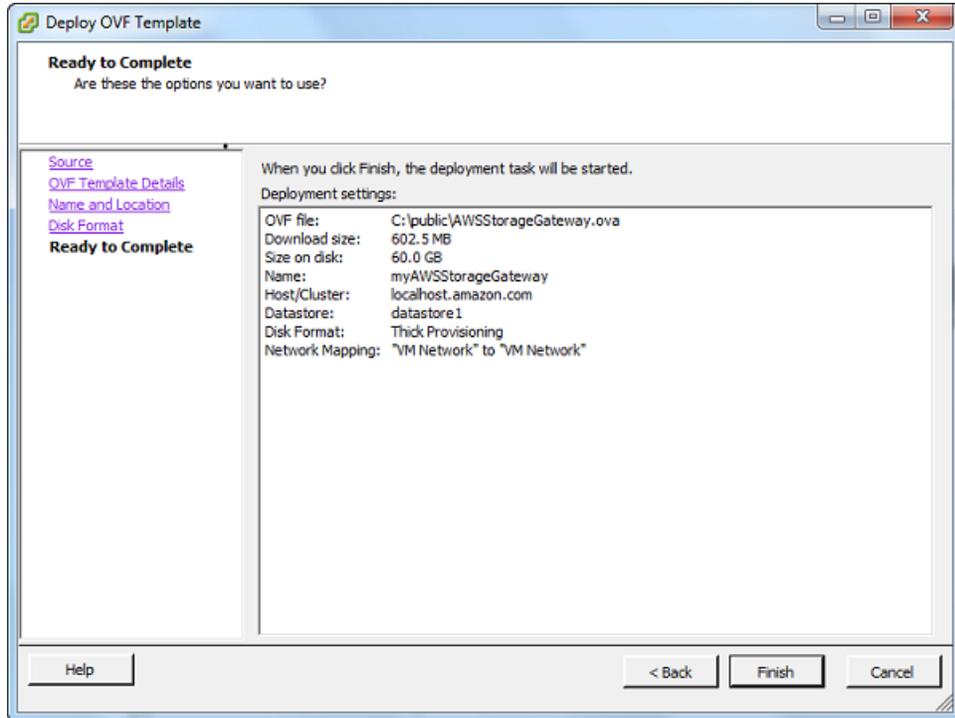
- f. 在磁盘格式化窗格中，选择完全配置格式，然后单击下一步。

选择存储自动配置时，磁盘空间立即分配，从而取得更好的性能。反之，自动精简配置按需分配存储空间。按需分配可能会影响 AWS Storage Gateway 的正常运行。因此，为使 AWS Storage Gateway 正常运行，必须以完全配置格式存储虚拟机磁盘。

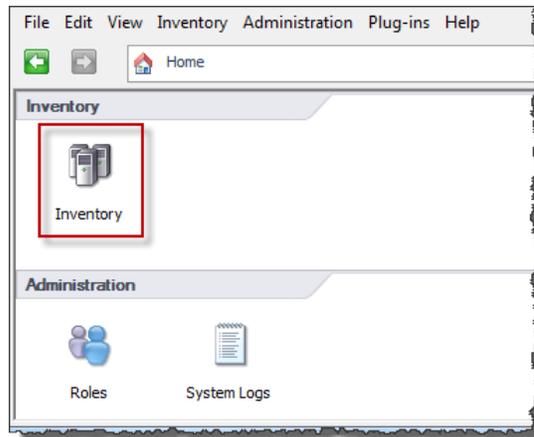


- g. 在已准备好完成窗格中，单击完成。

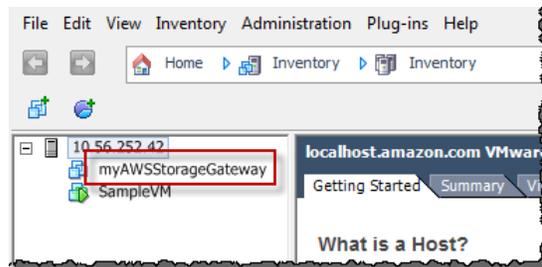
随后开始向您的主机部署 AWS Storage Gateway VM。



- h. 查看新 VM 的详细信息。
- i. 根据 vSphere 客户端状态的不同，可能需要先单击清点图标才能查看包含新 VM 的主机数据元。



- ii. 扩展主机数据元，查看新 VM 的详细信息。



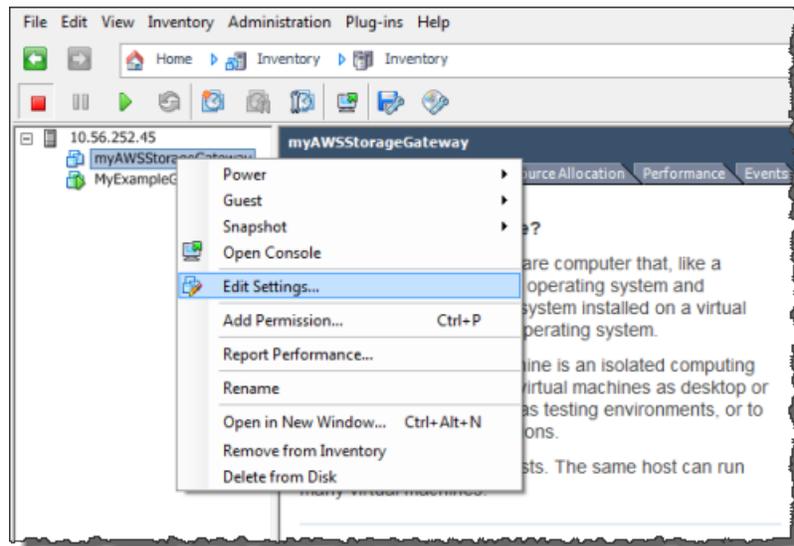
## 将 VM 时间与主机时间同步

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。成功激活网关需要同步 VM 和主机时间。在本步骤中，您首先将 VM 时间与主机时间同步。然后检查主机时间。如果需要，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。

如需将 VM 时间与主机时间同步

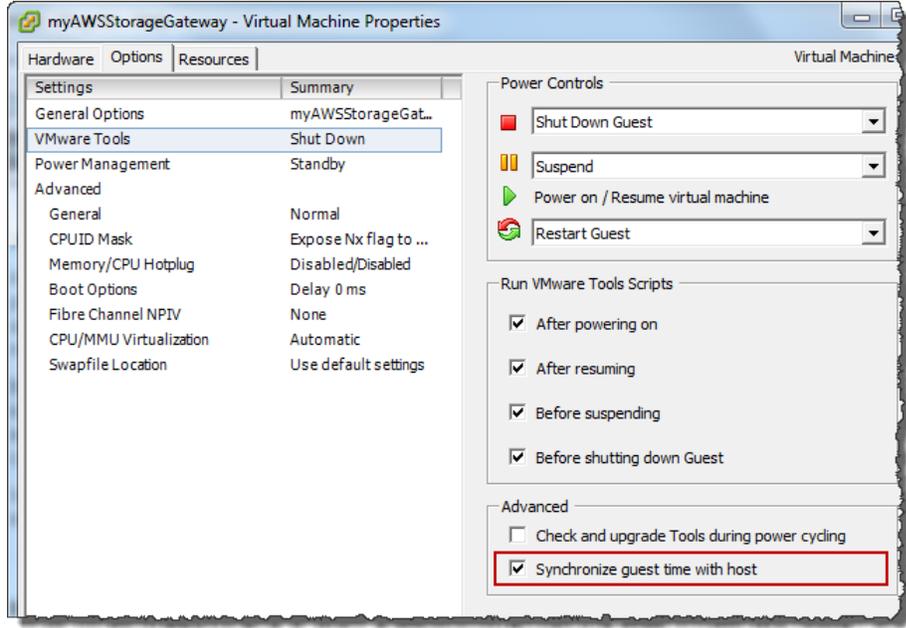
1. 配置您的 VM 时间。
  - a. 在 vSphere 客户端中，右键单击网关 VM 的名称，然后选择编辑设置。

随后将打开虚拟机属性对话框。



- b. 单击选项选项卡，然后从选项列表中选择 VMware 工具。
- c. 选中将来宾时间与主机同步选项，然后单击确定。

VM 时间与主机进行同步。

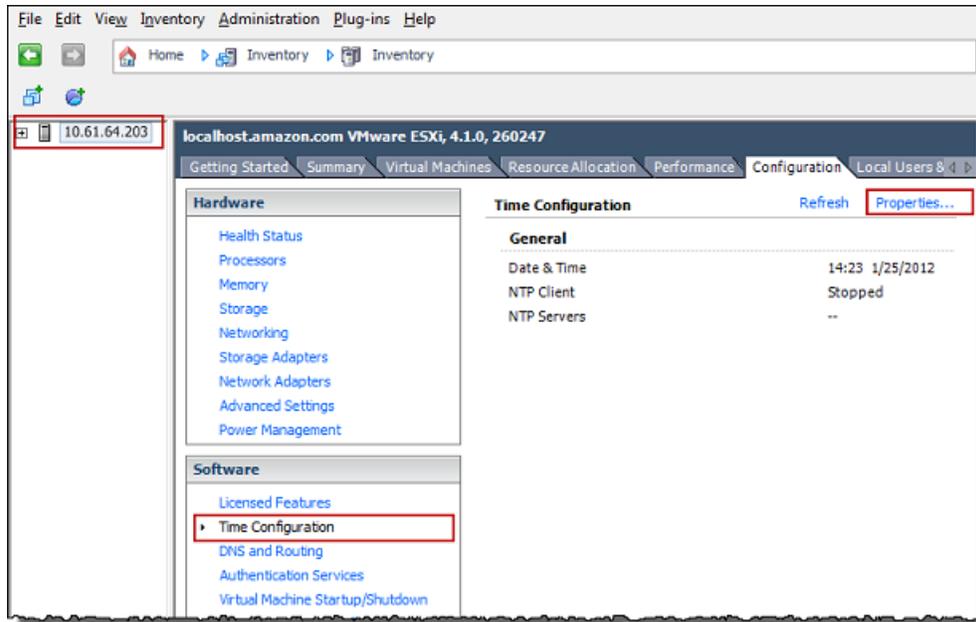


## 2. 配置主机时间。

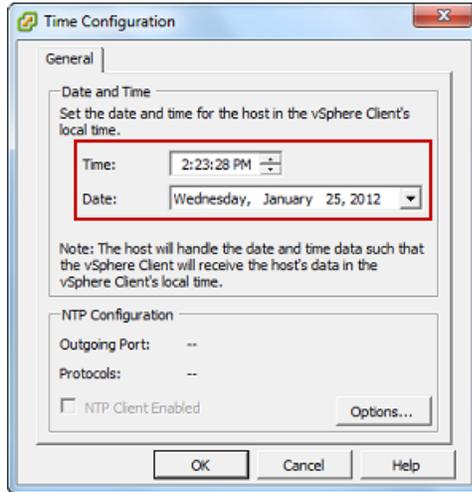
请注意，确保您设置了正确的主机时间。如果尚未配置主机时间，则按以下步骤设置该时间并将其与网络时间协议 (NTP) 服务器同步。

- 在 VMware vSphere 客户端中，在左侧窗格中选择 vSphere 主机节点，然后选择配置选项卡。
- 在软件面板中选择时间配置。
- 单击属性链接。

随后将显示时间配置对话框。

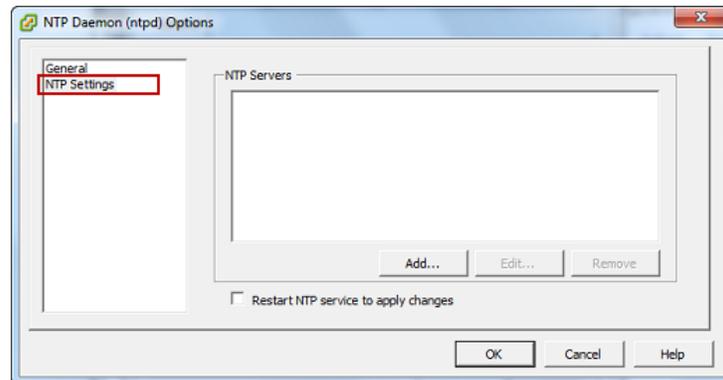


- d. 在日期和时间窗格中设置日期和时间。



- e. 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单击选项。
- ii. 在 NTP 守护程序(ntpd)选项对话框中的左侧窗格中选择 NTP 设置。



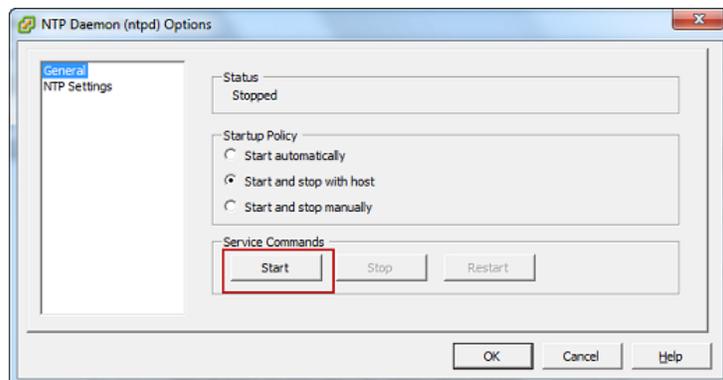
- iii. 单击添加以添加新 NTP 服务器。
- iv. 在添加 NTP 服务器对话框中，输入 NTP 服务器的 IP 地址或完全限定域名，然后单击确定。

可使用 `pool.ntp.org`，如本例所示。



- v. 在 NTP 守护程序(ntpd)选项对话框中的左侧窗格中单击常规。
- vi. 在服务命令窗格中，单击启动以启动服务。

请注意如果您稍后更改或添加另一 NTP 服务器参考，就需要重启服务才能使用新服务器。



- f. 单击确定以关闭 NTP 守护程序(ntpd)选项对话框。
- g. 单击确定以关闭时间配置对话框。

下一步

[为网关 VTL VM 配置本地磁盘存储 \(p. 269\)](#)

[为网关 VTL VM 配置本地磁盘存储](#)

在以下步骤中，您向所部署的网关 VM 分配本地存储。分配虚拟存储空间以用作上传缓冲区和缓存存储。网关通过将用于上传到 AWS 的应用程序数据存储称为上传缓冲区的存储上，准备并缓冲这些数据。经常访问的应用程序数据保留在本地作为缓存数据。此本地存储称为缓存存储。完成这些步骤后，您便成功添加了两个虚拟磁盘。

Topics

- [配置本地磁盘存储 \(网关 VTL\) \(p. 269\)](#)
- [配置 AWS Storage Gateway VM 以使用半虚拟化的磁盘控制器 \(p. 273\)](#)

[配置本地磁盘存储 \(网关 VTL\)](#)

在本练习中，您将向专供网关使用的 VM 分配 10 GiB 作为上传缓冲区，20 GiB 作为缓存存储。



#### Important

在本练习中，为 VM 分配的用作上传缓冲区和缓存存储的虚拟存储的大小不适合真实的工作负载。我们强烈建议您至少分配 150 GiB 的上传缓冲区。要估计网关所需的缓存存储量，可使用计划每天写入虚拟磁带的大致数据。在本教程后面的步骤 ([管理上传缓冲区和缓存存储 \(网关 VTL\) \(p. 379\)](#)) 中，您将了解如何针对真实工作负载适当地调整缓存存储和上传缓冲区的大小。

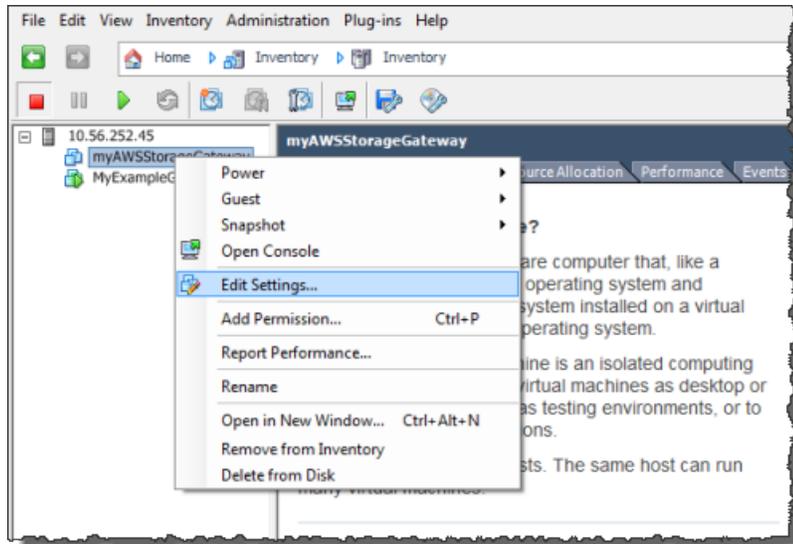
[为上传缓冲区分配本地存储](#)

网关在向 AWS 上传数据时，需要缓冲区空间以临时存储数据。这一空间称为上传缓冲区。您必须给 VM 添加虚拟磁盘，专供 VM 使用。网关需要的上传缓冲区的大小取决于经常访问的数据的缓存。有关相关准则，请参阅[配置上传缓冲区的大小 \(网关 VTL\) \(p. 316\)](#)。

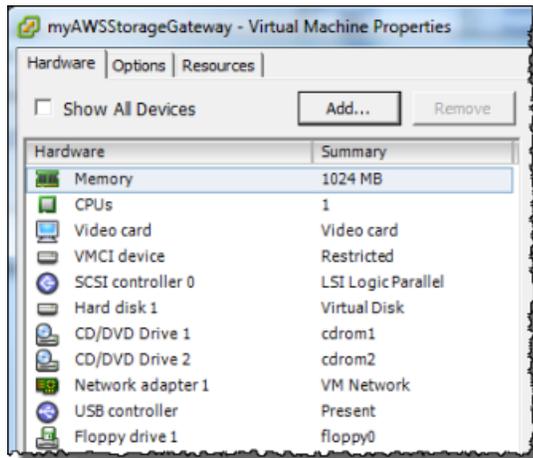
在本练习中，您向专供网关使用的 VM 分配一个 10 GiB 的虚拟磁盘。在向导的创建磁盘窗格中，输入 10 GiB 作为磁盘大小。

如需将本地磁盘分配为上传缓冲区

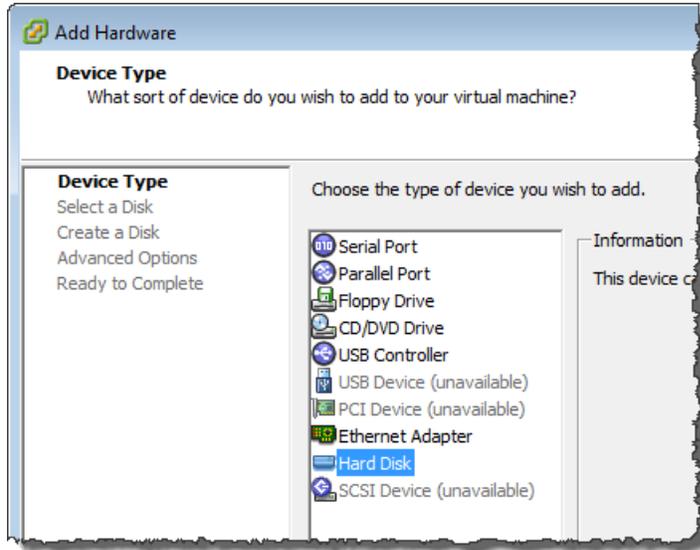
1. 启动 VMware vSphere 客户端并连接到您的主机。
2. 在客户端中，右键单击网关 VM 的名称，然后单击编辑设置。



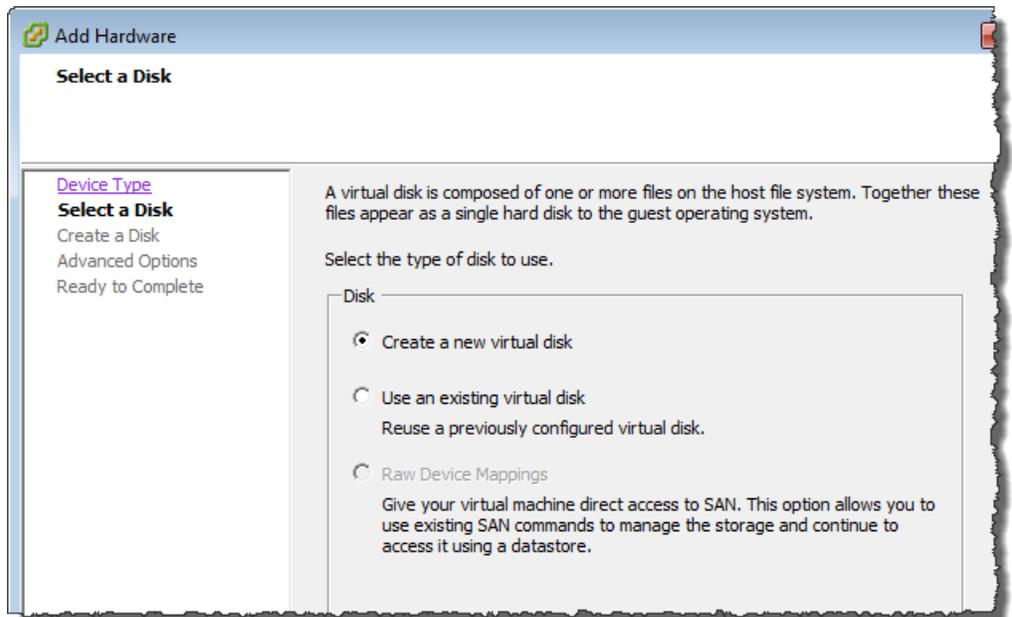
3. 在虚拟机属性对话框的硬件选项卡中，单击添加以添加一个设备。



4. 根据添加硬件向导添加磁盘：
  - a. 在设备类型窗格中，单击硬盘以添加一个磁盘，然后单击下一步。



- b. 在选择磁盘窗格中，选择新建虚拟磁盘，然后单击下一步。



- c. 在创建磁盘窗格中，将磁盘的大小指定为 10 GiB，然后单击下一步。

选择存储自动配置时，磁盘空间立即分配，从而取得更好的性能。反之，自动精简配置按需分配存储空间。按需分配可能会影响 AWS Storage Gateway 的正常运行。因此，为使 AWS Storage Gateway 正常运行，必须以完全配置格式存储虚拟机磁盘。

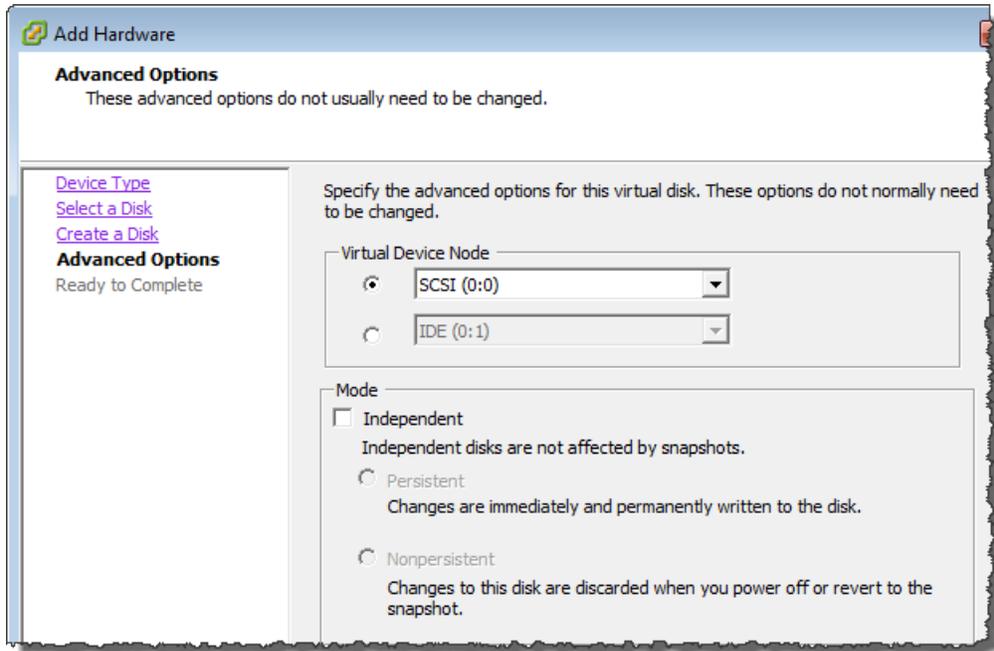


#### Note

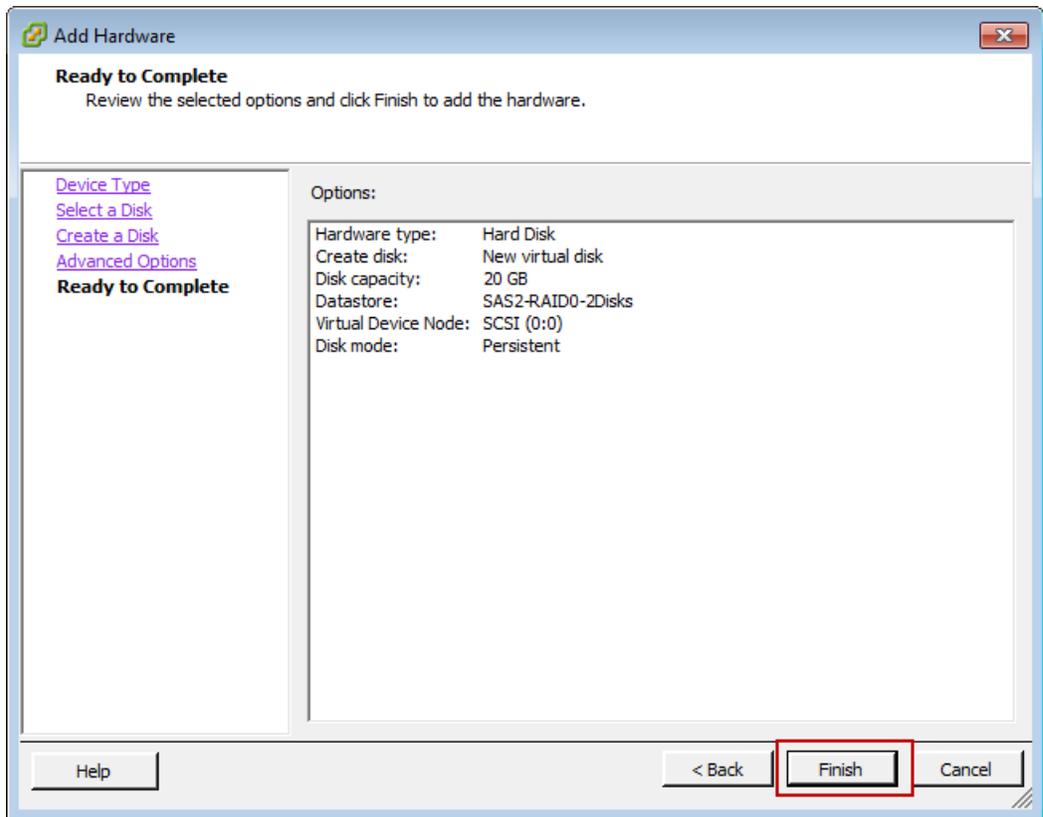
在本例设置中，将磁盘的位置与虚拟机存储在一起。对于实际工作负载，我们强烈建议您不要使用相同的底层物理存储磁盘预配置本地磁盘。根据托管环境的不同，为您在本步骤中预配置的磁盘选择不同的数据存储器可能更好。有关更多信息，请参阅在 [VMware ESXi 主机上为 AWS Storage Gateway VTL VM 配置本地磁盘存储](#) (p. 314)。



- d. 在高级选项窗格中，接受默认值，然后单击下一步。



- e. 在已准备好完成窗格中，接受默认值，然后单击完成。



- f. 在虚拟机属性对话框中，单击确定以完成添加磁盘。

### 为缓存存储分配本地磁盘存储

经常访问的应用程序数据保留在本地作为缓存数据，因此必须分配 VM 上的一个磁盘作为存储这些数据的缓存。本节说明如何从直接连接存储 (DAS) 磁盘添加虚拟磁盘。使用下面的指导预配置一个磁盘，以便存储您的应用程序数据。有关从现有的存储区域网络 (SAN) 连接 iSCSI 卷，以使您可在这一步使用这些卷的说明，请参阅[如需添加新的 iSCSI 目标 \(p. 443\)](#)。

在本练习中，您向 VM 分配一个 20 GiB 的虚拟磁盘。

如需将本地磁盘分配为缓存

- 重复前一节 ([为上传缓冲区分配本地存储 \(p. 269\)](#) 过程) 中的步骤以向网关添加另一个虚拟磁盘，用作缓存存储。

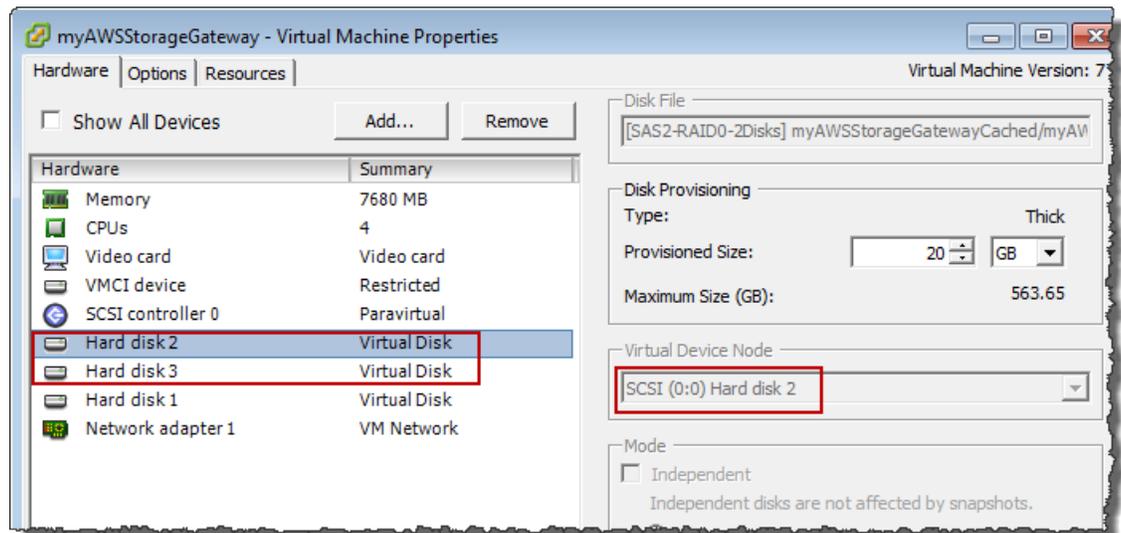
### 验证网关 VM 有两个磁盘

本练习的其余部分要求您已向网关 VM 分配两个磁盘。您可以使用下面的可选步骤验证已给网关 VM 分配好两个磁盘。如果需要分配其他磁盘，则重复为[上传缓冲区分配本地存储 \(p. 269\)](#)过程中的步骤。

如需验证 VM 有两个磁盘

1. 在客户端中，右键单击网关 VM 的名称，然后单击编辑设置。
2. 在虚拟机属性对话框的硬件选项卡中，确认硬件列表中显示硬盘 2 和硬盘 3。

这两个磁盘随后将用于 AWS Storage Gateway 控制台中，并在下拉列表中显示为 SCSI (0:0) 和 SCSI (0:1)。



### 配置 AWS Storage Gateway VM 以使用半虚拟化的磁盘控制器

在本任务中，iSCSI 控制器设置为 VM 采用半虚拟化的模式，在该模式中网关 VM 与主机 OS 协同工作，以便控制台能够正确识别您给 VM 添加的虚拟磁盘。

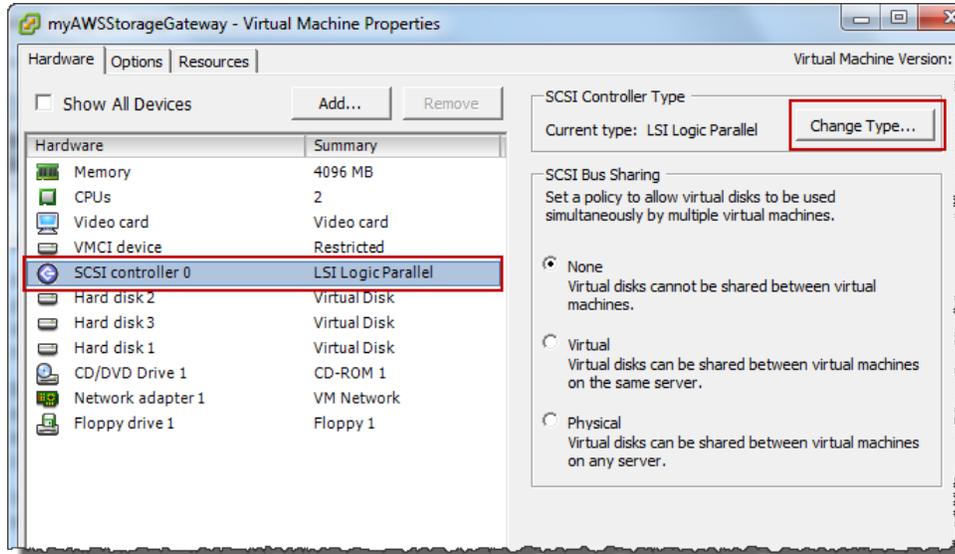


## Note

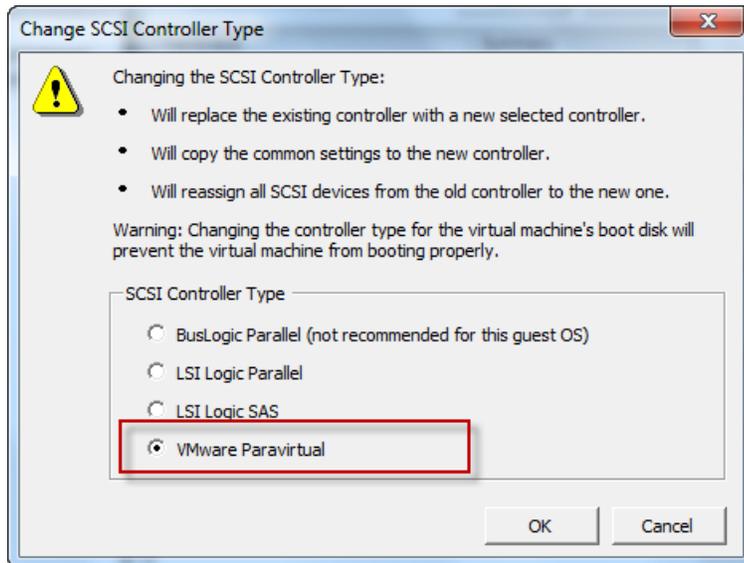
您必须完成本步骤以避免随后在识别这些磁盘时发生问题。

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，右键单击您的网关 VM 名称。
2. 选择编辑设置。
3. 在虚拟机属性对话框中，单击硬件选项卡，选择 SCSI 控制器 0，然后单击更改类型。



4. 在更改 SCSI 控制器类型对话框中，选择 VMware 半虚拟化 SCSI 控制器类型，然后单击确定。



下一步

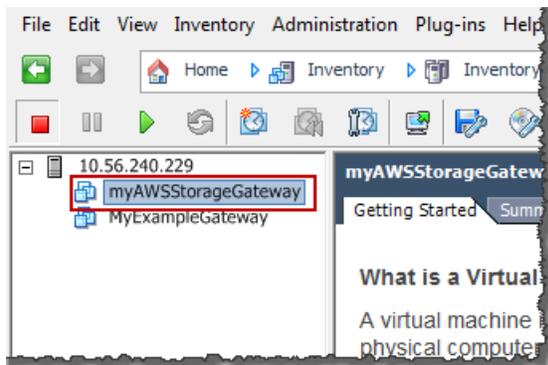
[激活 AWS Storage Gateway-VTL \(p. 275\)](#)

## 激活 AWS Storage Gateway-VTL

现在您已准备好激活您的网关。激活过程将您的网关与 AWS 账户关联。您必须在激活网关前启动网关 VM。

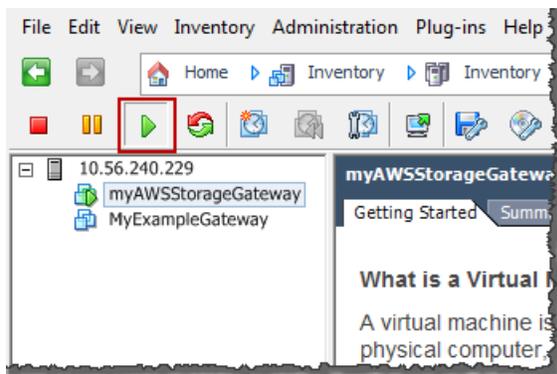
### 如需激活网关

1. 启动 VM。
  - a. 在 vSphere 客户端中，选择网关 VM。



- b. 在工具栏菜单中，单击开机图标。

您的网关 VM 图标现在包含一个绿色箭头图标，表示您已启动 VM。

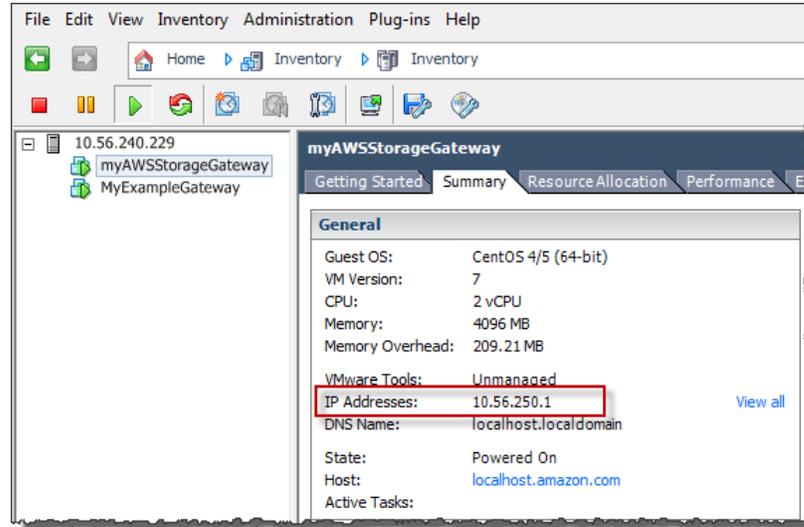


2. 激活网关。
  - a. 取得您的网关的 IP 地址。
    - i. 在 vSphere 客户端中，选择您部署的网关 VM。
    - ii. 单击摘要，然后记下 IP 地址（可能要将其写下来）。您将使用此 IP 地址激活网关。

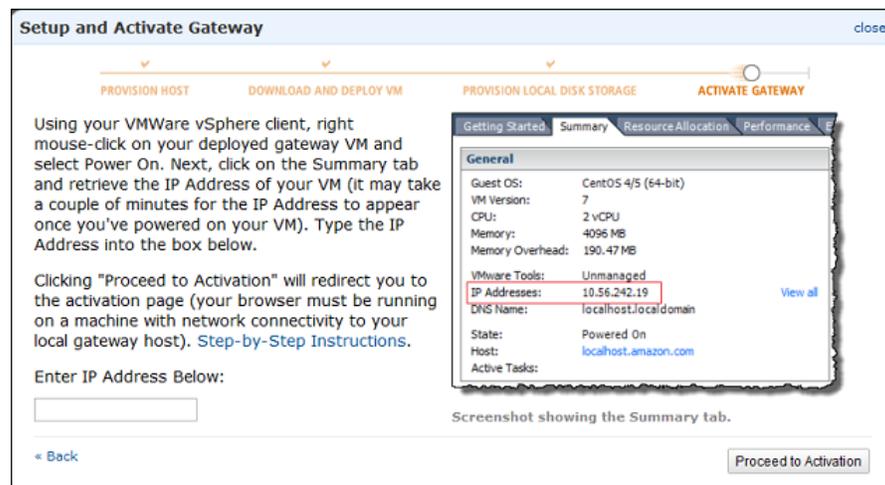


#### Note

网关的 IP 地址显示为摘要的一部分。启动 VM 后，IP 地址可能需要几分钟的时间才能显示。



- b. 将您的网关关联到 AWS 账户。
  - i. 在 AWS Storage Gateway 控制台的设置并激活网关向导中，导航到激活网关页。
    - A. 如果尚未启动该向导，则单击设置并激活新网关按钮。
    - B. 在向导的每个步骤中单击继续，直到抵达激活网关页。
  - ii. 在“输入 IP 地址”文本框中，输入网关的 IP 地址，然后单击继续激活。



 **Note**

激活期间，您的浏览器连接到网关。如果激活失败，则确认输入的 IP 地址正确无误。如果该 IP 地址正确，则确认已将网络配置为允许浏览器访问网关 VM。

- iii. 在激活页上，输入所要求的信息以完成激活过程。
  - AWS 地区决定 AWS 存储虚拟磁带的位置。您不能在网关激活后更改地区。



#### Note

在以下地区支持 AWS Storage Gateway-VTL。

地区

Region name	Region string
US East (Northern Virginia)	us-east-1
US West (Northern California)	us-west-1
US West (Oregon)	us-west-2
EU (Ireland)	eu-west-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1

- 网关时区指定希望用于网关的时区。
- 网关名称在控制台中标识您的网关。您使用该名称在控制台中管理网关，可在激活后更改名称。该名称必须是您账户的唯一名称。
- 介质更换器类型指定此网关使用的介质更换器的类型。
- 磁带驱动器类型指定此网关使用的磁带驱动器的类型。



- iv. 单击激活我的 Storage Gateway。

成功激活网关后，AWS Storage Gateway 控制台在导航窗格的网关部分下显示一个链接，指向已激活的网关。单击您刚刚添加的网关。

随后将显示创建磁带按钮。

如果激活失败，请参阅[网关 VTL 问题排查 \(p. 411\)](#)以了解可能采用的解决方案。



单击创建磁带后，将有向导指导您如何为网关配置本地存储、创建可选警报和创建虚拟磁带。



#### Note

首次为网关 VTL 创建磁带时，必须先为网关配置本地存储，然后才能创建虚拟磁带。

下一步

[步骤 2：配置本地存储和警报 \(p. 300\)](#)

## Hyper-V 主机

在本部分中，您将预配置场内 Microsoft Hyper-V 主机、向主机下载和部署网关 VM、配置网关 VM 并进行激活。

### Topics

- [配置 Hyper-V 主机以部署 AWS Storage Gateway VM \(p. 278\)](#)
- [下载 AWS Storage Gateway VM 并将其部署在您的主机上 \(p. 278\)](#)
- [为 AWS Storage Gateway-VTL VM 配置本地存储 \(p. 288\)](#)
- [激活您的存储网关 VTL \(p. 294\)](#)

### 下一步

[配置 Hyper-V 主机以部署 AWS Storage Gateway VM \(p. 278\)](#)

### 配置 Hyper-V 主机以部署 AWS Storage Gateway VM

在本步骤中，您在数据中心创建 Hyper-V 主机，用来部署网关虚拟机 (VM)。

#### 如需预配置主机

1. 核查最低主机要求。有关更多信息，请参见 [要求 \(p. 7\)](#)。
2. 使用 Microsoft Hyper-V 主机在数据中心设置主机。

本指南中的附录提供安装管理程序操作系统的最低限度指导。有关更多信息，请参阅 [附录 D：为 AWS Storage Gateway 配置 Microsoft Hyper-V 主机 \(p. 447\)](#)。

### 下一步

[下载 AWS Storage Gateway VM 并将其部署在您的主机上 \(p. 278\)](#)

### 下载 AWS Storage Gateway VM 并将其部署在您的主机上

以 Hyper-V 可下载的 .zip 文件形式提供 AWS Storage Gateway 虚拟机。本部分介绍如何将该文件下载到本地，并导入到您的主机。

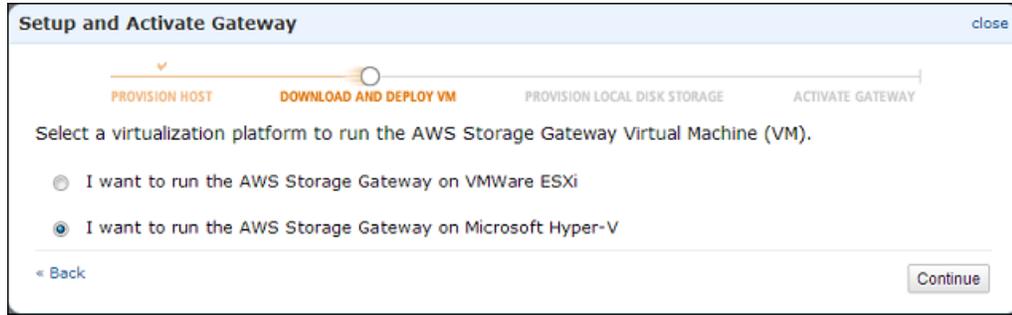
### Topics

- [下载 AWS Storage Gateway VM \(p. 278\)](#)
- [将 AWS Storage Gateway VM 部署到您的主机 \(p. 279\)](#)

### 下载 AWS Storage Gateway VM

#### 如需下载该 VM

1. 在 [AWS Storage Gateway](#) 控制台的设置并激活网关向导中，导航到下载并部署 VM 页。
2. 选择我要在 Microsoft Hyper-V 上运行 AWS Storage Gateway，然后单击继续。



3. 单击下载以下载包含该 VM 的 .zip 文件。

将 .zip 保存到您的计算机上的某个位置。解压缩已下载的文件，并记下已创建的文件夹的位置。



#### Note

该 .zip 文件大小超过 500 MB，根据网速的不同，下载该文件可能需要一些时间。

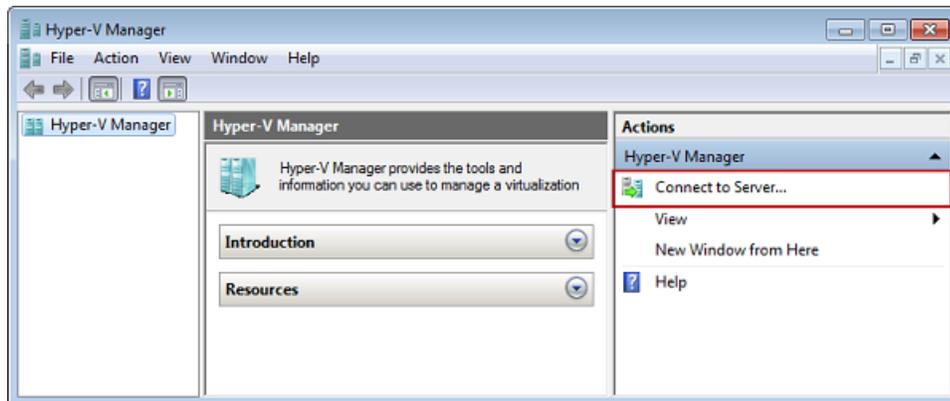


### 将 AWS Storage Gateway VM 部署到您的主机

要使用您的虚拟机监控程序主机，必须连接到它。连接到它之后，您将指定存储 VM 的位置，导入 VM，然后为它配置一个网络。

如需连接到管理程序主机

1. 在您的 Windows 客户端上启动 Microsoft Hyper-V Manager。
2. 在操作窗格中，单击连接到服务器...

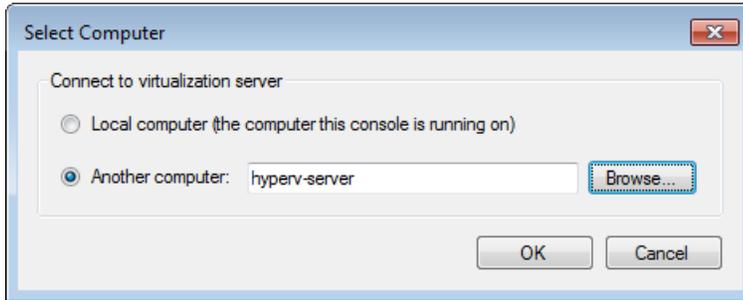


3. 在选择计算机对话框中，选择另一台计算机，输入 IP 地址或主机名，然后单击确定。



### Note

在本练习中，我们使用 `hyperv-server` 作为主机。您的主机名会与此不同。如果在使用选择计算机对话框时找不到您的主机名，则可能需要向 `hosts` 文件添加一个条目，以使 Hyper-V 管理器可解析服务器名称。



您的 Microsoft Hyper-V Manager 现已连接到您的主计算机。

既然您已连接到主机，下一个步骤就是在该主机上创建文件夹，以便存储已下载的源 VM、已导入的正在运行 VM 以及该 VM 所关联的虚拟硬盘。

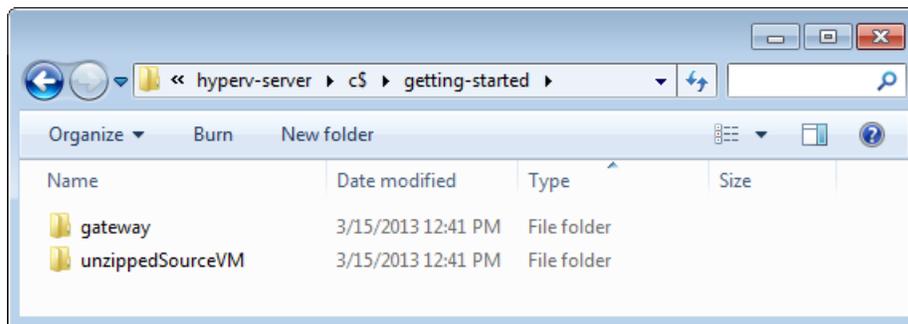
### 指定虚拟硬盘和 VM 的位置

1. 在管理程序主机上为网关虚拟硬盘和 VM 创建位置。

- a. 导航到管理程序所在的驱动器。

例如，使用本练习中主机的名称，并假定 `C` 驱动器对于您的主机有效，则可在开始菜单中键入 `\\hyperv-server\c$`。

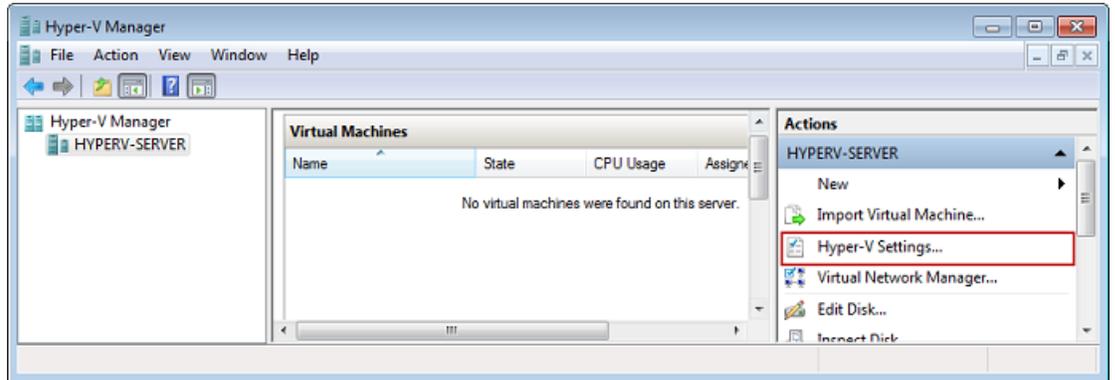
- b. 创建一个名为 `getting-started` 的文件夹，其中含有两个子文件夹 `unzippedSourceVM` 和 `gateway`。



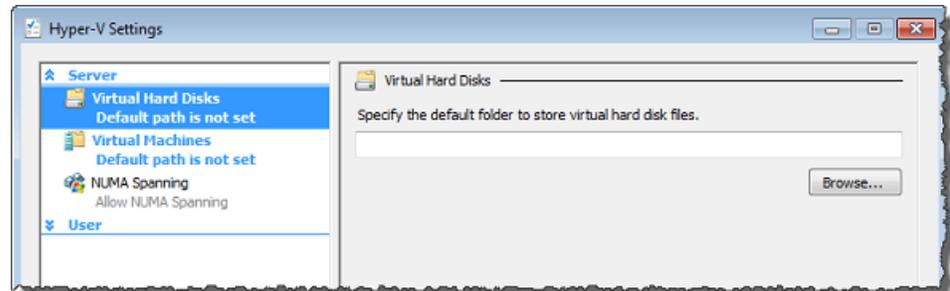
2. 配置 Hyper-V 管理器，使其指向您创建的 `gateway` 文件夹。

这也是正在运行的 VM 将用于存储其配置的文件夹。

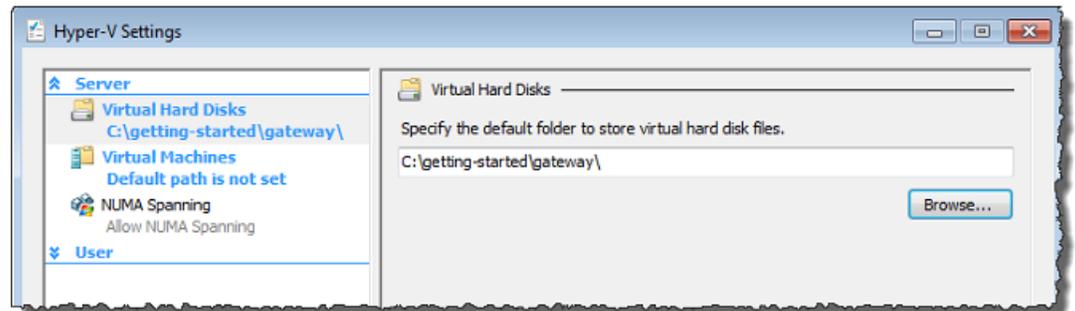
- a. 在操作菜单中，单击 Hyper-V 设置...



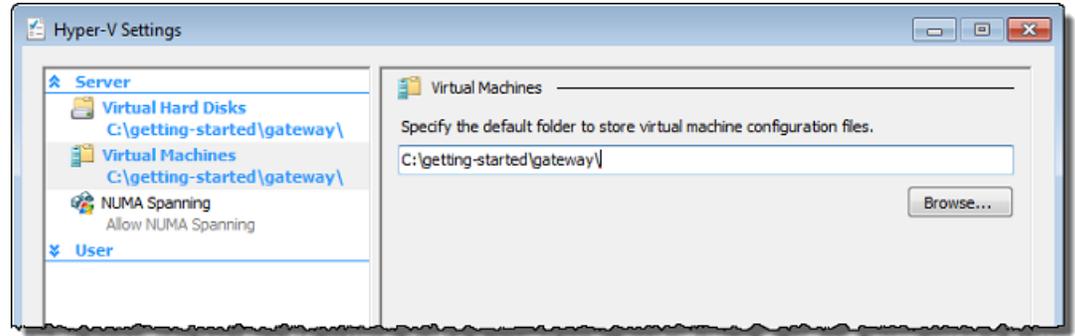
- b. 在 Hyper-V 设置对话框中，配置虚拟硬盘和虚拟机的位置。
  - i. 在左侧窗格中的服务器下，选择虚拟硬盘设置。



- ii. 通过浏览，查找以前创建的 gateway 文件夹。  
您在管理程序（主机）服务器上浏览。

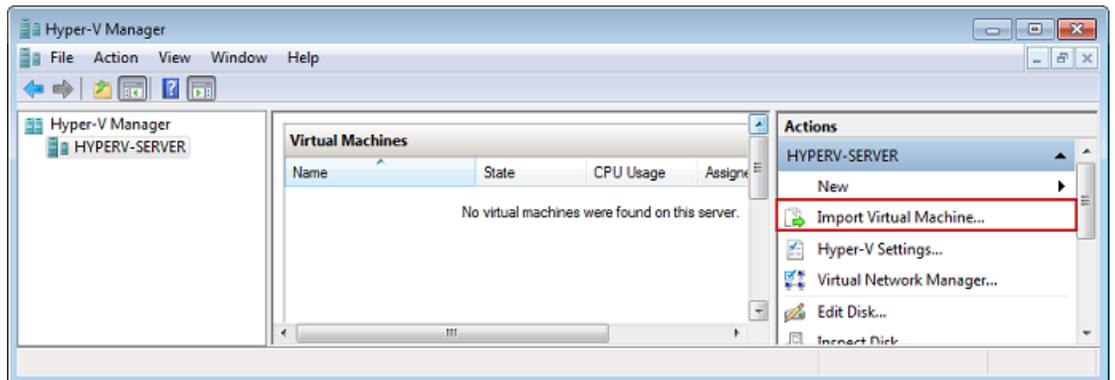


- iii. 在左侧窗格中的服务器下，选择虚拟机设置。
    - iv. 通过浏览，将该位置设为相同的 gateway 文件夹，然后单击确定。



### 导入该 VM

1. 将解压缩的源 VM 文件复制到您在主机计算机上创建的文件夹。在本练习中，该路径为  
\\hyperv-server\c\$\getting-started\unzippedSourceVM\AWS-Storage-Gateway。
2. 将 AWS Storage Gateway VM 导入到主机。
  - a. 在 Hyper-V 管理器的左侧控制台树窗格中，选择主机 hyperv-server。
  - b. 在操作菜单中，单击导入虚拟机...



- c. 在导入虚拟机对话框中：
  - i. 在位置框中，找到以前创建的位置  
\\hyperv-server\c\$\getting-started\unzippedSourceVM\AWS-Storage-Gateway。



### Caution

您必须指向正确的文件夹，导入才会成功。要选择正确文件夹 (AWS-Storage-Gateway) 将包含其他三个文件夹 ( Snapshots、Virtual Hard Disks、Virtual Machines ) 和一个文件 (config.xml)。根据网关源文件的解压缩方式，您最后可能会得到一个额外的文件夹级别。要帮助排除导入方面的故障，请参阅[故障诊断 Microsoft Hyper-V 设置 \(p. 453\)](#)。

- ii. 选择复制虚拟机(新建唯一 ID)。
- iii. 选中复制所有文件以便可以再次导入同一虚拟机。
- iv. 单击导入。



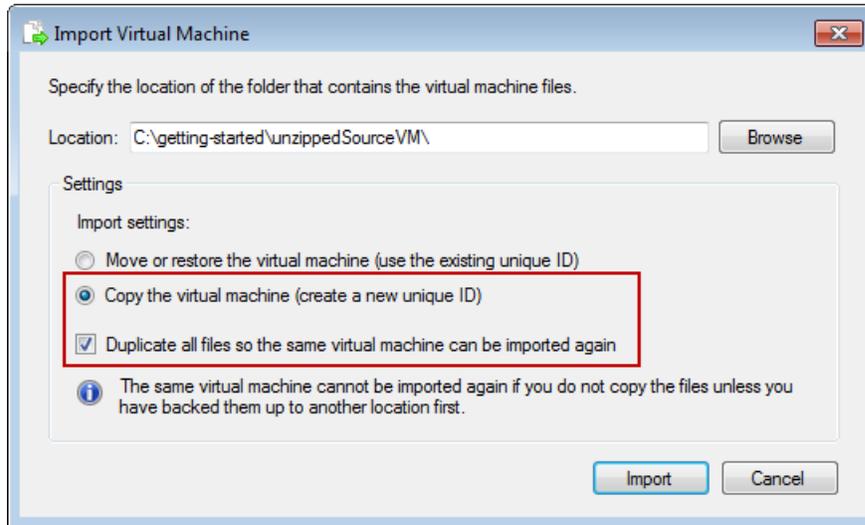
### Caution

选择复制虚拟机(新建唯一 ID)和复制所有文件以便可以再次导入同一虚拟机选项很重要，尤其是要重用解压缩的网关源文件时。



### Important

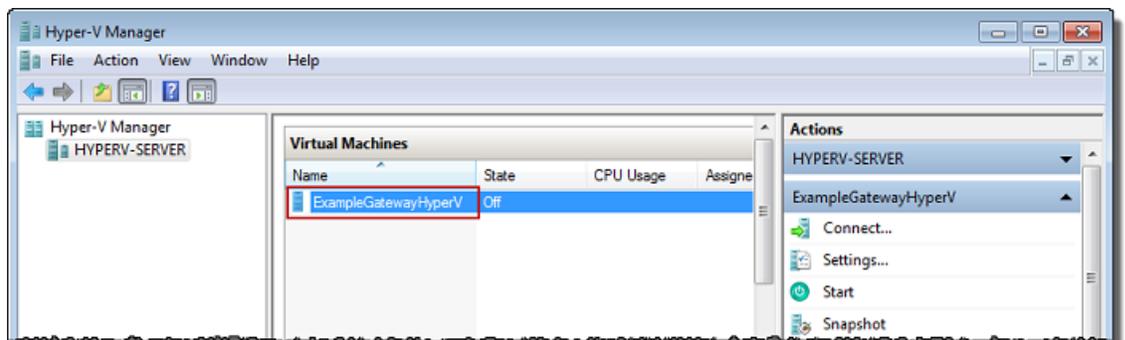
您必须具有 75 GiB 的磁盘空间，以便安装 VM 映像和系统数据。



在导入完成后，会创建名为 AWS-Storage-Gateway 的虚拟机。

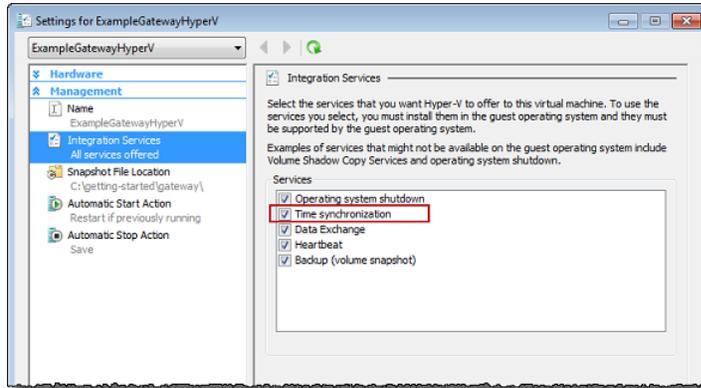
3. 重命名该虚拟机以避免与可能导入到主机的其他虚拟机混淆。
  - a. 选择该虚拟机，单击右键并选择重命名。
  - b. 为虚拟机提供新的名称。

在本练习中，我们将使用 ExampleGatewayHyperV-VTL。



4. 确认在集成服务中为该 VM 选择了时间同步。

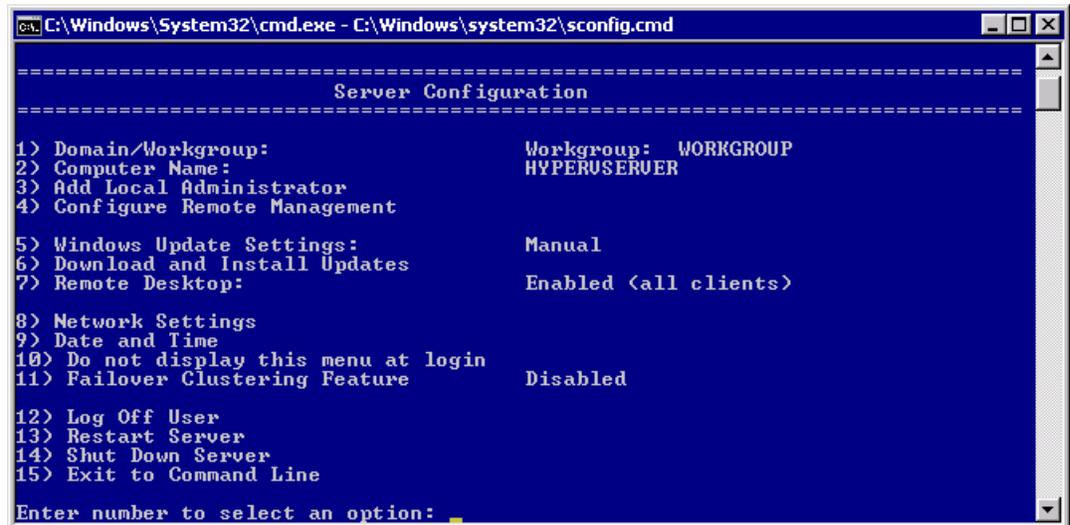
- a. 在虚拟机列表窗格中，选择虚拟机 ExampleGatewayHyperV-VTL。
- b. 在操作菜单中，单击设置...。
- c. 在设置对话框中的管理下，选择集成服务，然后确认选中了时间同步。



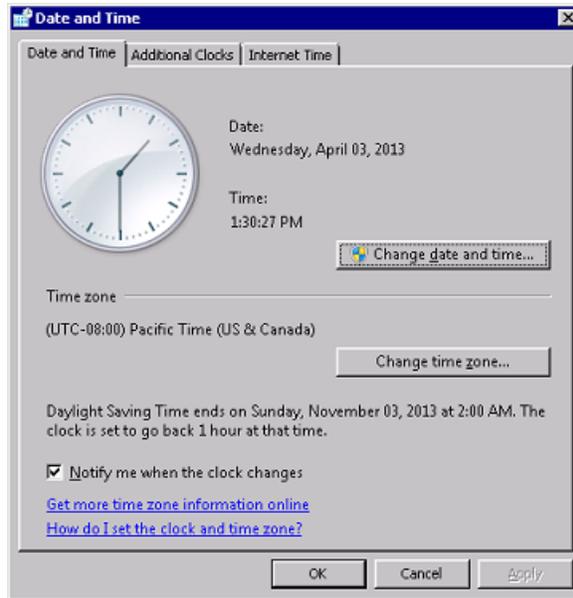
5. 如果尚未配置主机时间，则请照做，然后单击确定。

请注意，确保您设置了正确的主机时间。以下步骤展示如何使用服务器配置工具 (Sconfig.cmd) 设置时间。有关 Sconfig.cmd 的详细信息，请转到[使用 Sconfig.cmd 配置服务器核心服务器](#)。(根据正在运行的 Microsoft Hyper-V 版本，您可以使用其他方式设置该时间。)

- a. 通过访问虚拟机监控程序主机控制台或远程登录，访问 Sconfig.cmd 工具。



- b. 输入选项 9 日期和时间。  
随后将显示日期和时间控制面板。
- c. 配置时间，然后单击确定。



可注销远程计算机。

## 配置虚拟网络并在 VM 上使用

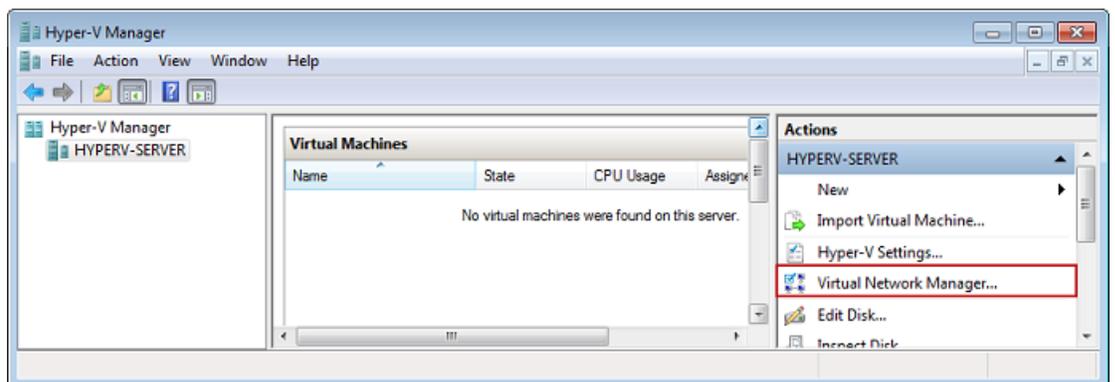
### 1. 配置 Hyper-V 主机的虚拟网络设置。



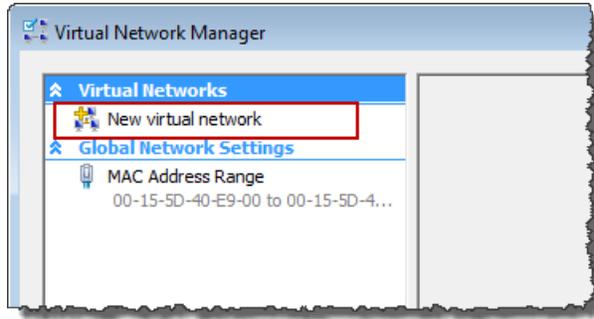
#### Note

在本练习中，我们假定该主机尚未配置虚拟网络设置。如果您已经配置了虚拟网络，请转到步骤 2。

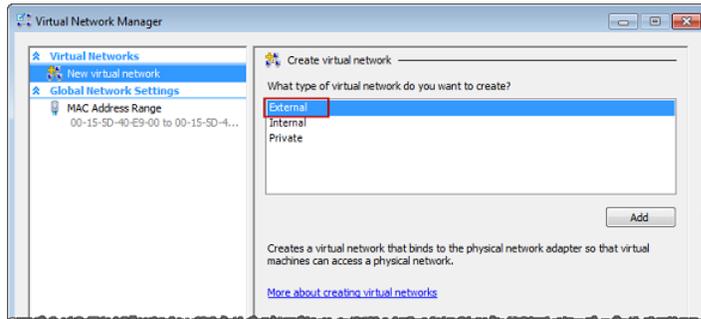
- a. 在操作菜单中的虚拟机监控程序主机名（例如，`hyperv-server`）下，单击虚拟网络管理器...



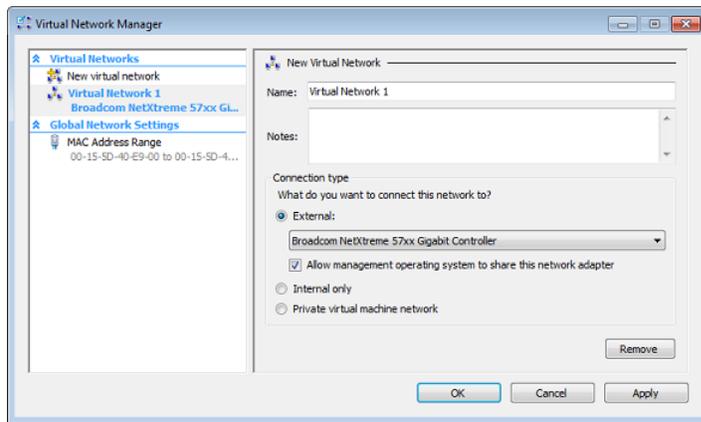
- b. 在虚拟网络管理器对话框中，选择新建虚拟网络。



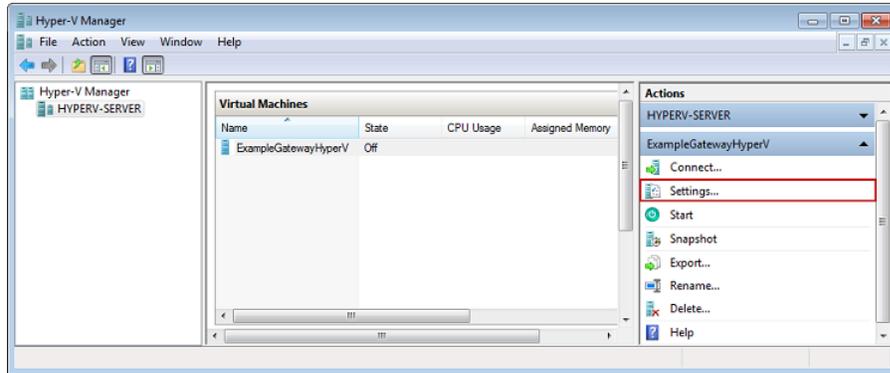
- c. 选择外部作为虚拟网络类型，然后单击添加。



- d. 为该网络提供一个名称，然后单击确定。

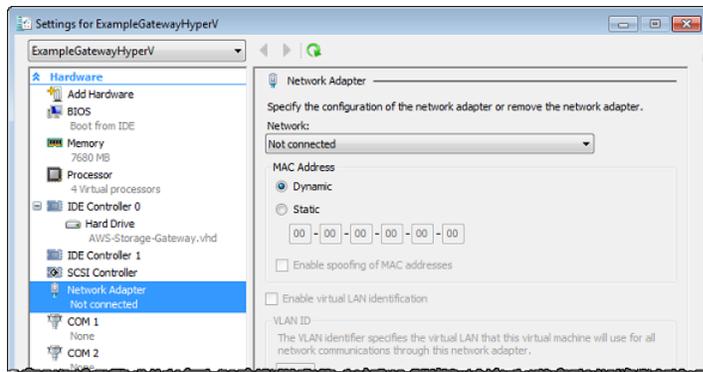


2. 配置虚拟机，以使用虚拟网络。
- a. 在虚拟机列表窗格中，选择虚拟机 ExampleGatewayHyperV。
  - b. 在操作窗格中，选择设置...。



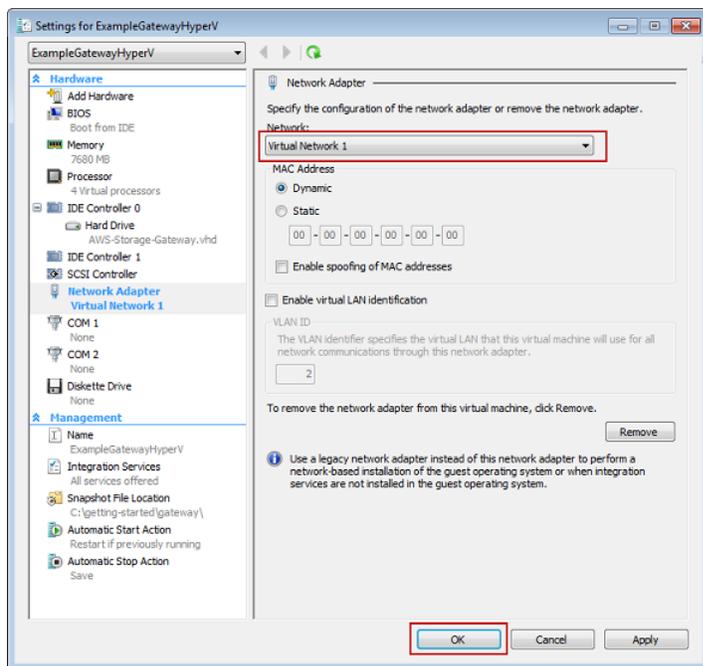
c. 在设置窗口中，选择网络适配器。

网络适配器的状态应为未连接。



d. 在网络框中的右窗格中，选择一个网络。

在下例中，选择了虚拟网络 1。



- e. 单击确定。

下一步

[为 AWS Storage Gateway-VTL VM 配置本地存储 \(p. 288\)](#)

[为 AWS Storage Gateway-VTL VM 配置本地存储](#)

在下面的步骤中，您将给部署的网关 VM 分配本地磁盘。您分配虚拟磁盘以用作上传缓冲区和缓存存储空间。在本练习中，您将分配一个磁盘用于上传缓冲区，另一个用于缓存存储。网关通过将用于上传到 AWS 的应用程序数据存储称为上传缓冲区的磁盘上，准备并缓冲这些数据。经常访问的应用程序数据保留在本地作为缓存数据，并存储在称为缓存存储的磁盘上。分配这些本地磁盘后，您将向所部署的网关添加了两个虚拟磁盘。

Topics

- [为上传缓冲区分配本地磁盘 \(p. 288\)](#)
- [为缓冲存储区分配本地磁盘 \(p. 293\)](#)
- [验证网关 VM 有两个磁盘 \(p. 293\)](#)

在本练习中，您将向专供网关使用的 VM 分配 10 GiB 作为上传缓冲区，20 GiB 作为缓存存储。



#### Important

在本教程中，为 VM 分配的用作上传缓冲区和缓存存储的虚拟磁盘的大小不适合真实的工作负载。我们强烈建议您至少分配 150 GiB 的上传缓冲区。缓存存储空间的大小应根据上传缓冲区的大小而定。在本教程后面的步骤 ([管理上传缓冲区和缓存存储 \(网关 VTL\) \(p. 379\)](#)) 中，您将了解如何针对真实工作负载适当地调整缓存存储和上传缓冲区的大小。

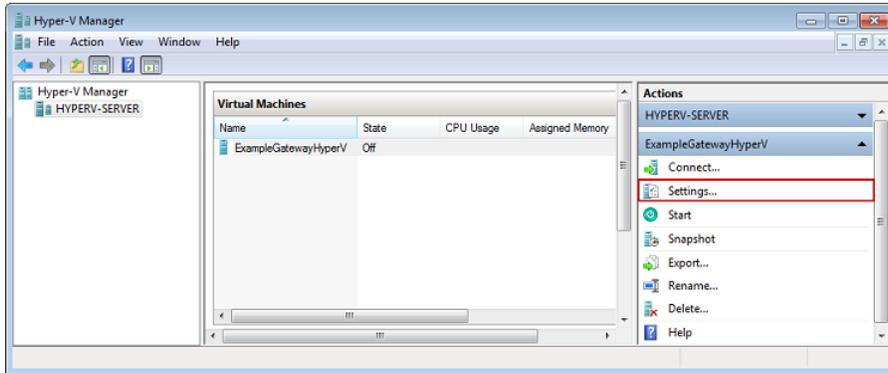
[为上传缓冲区分配本地磁盘](#)

网关在上传快照到 AWS 时，需要缓存空间以临时存储数据。这一空间称为上传缓冲区。您必须给 VM 添加虚拟磁盘，专供 VM 使用。网关需要的上传缓冲区大小取决于您指定的经常访问数据的缓存。有关相关准则，请参阅[配置上传缓冲区的大小 \(网关 VTL\) \(p. 316\)](#)。

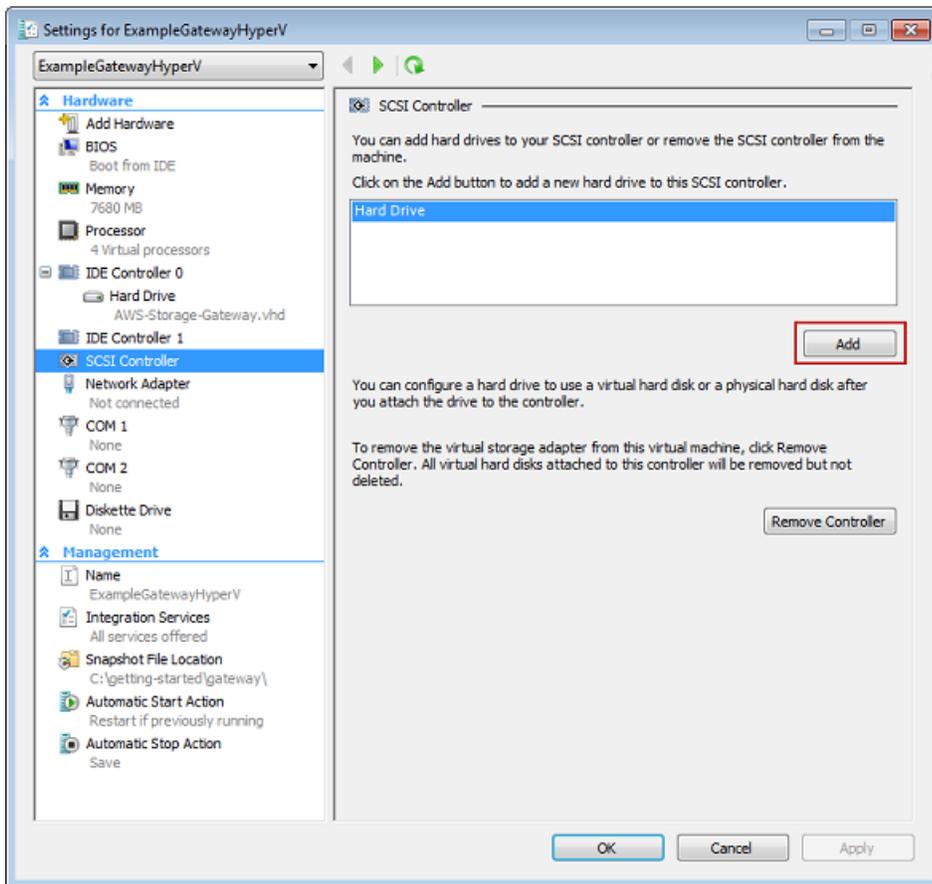
在本练习中，您向专供网关使用的 VM 分配一个 10 GiB 的虚拟磁盘。在向导的创建磁盘窗格中，输入 10 GiB 作为磁盘大小。

分配本地磁盘作为上传缓冲区

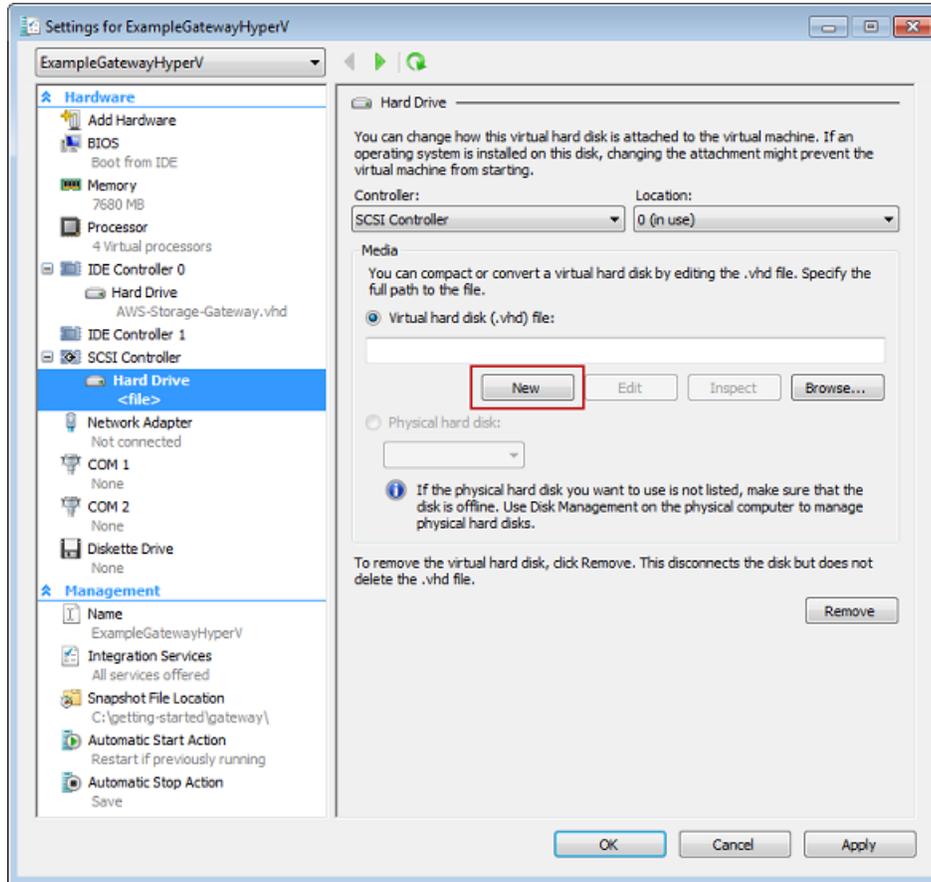
1. 启动 Microsoft Hyper-V Manager，然后连接到虚拟机监控程序。
2. 在虚拟机列表窗格中，选择虚拟机 ExampleGatewayHyperV。
3. 在网关的操作窗格中，选择设置...



4. 在设置窗口中，选择 SCSI 控制器，然后单击添加。

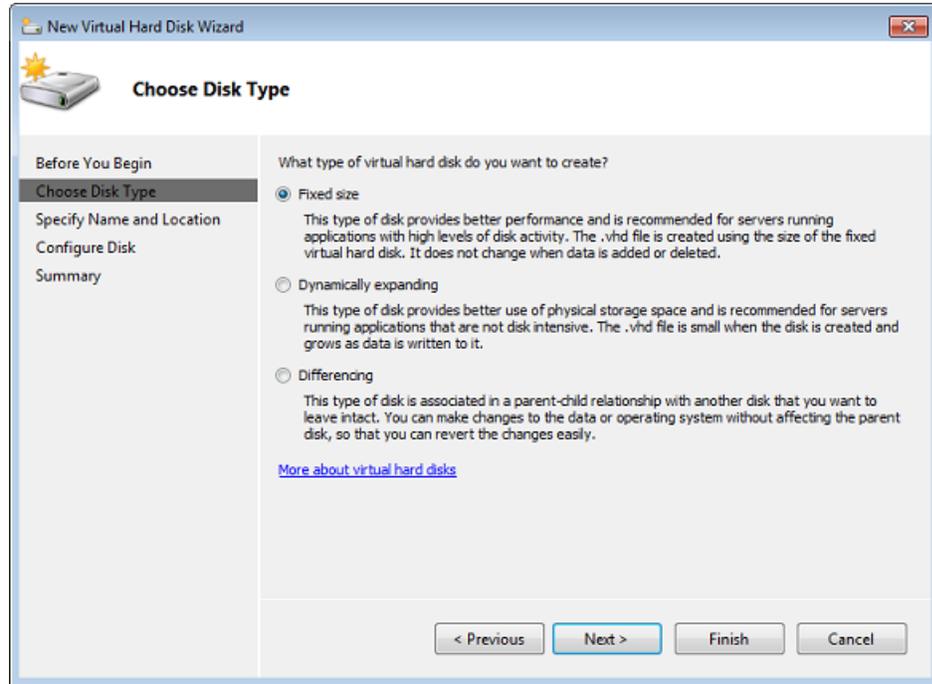


5. 在硬盘驱动器窗格中的介质下，单击新建。



6. 在新建虚拟硬盘向导中，新建一个虚拟硬盘。
  - a. 在开始之前页上，单击下一步。
  - b. 在选择磁盘类型页上，选择固定大小，然后单击下一步。

使用固定大小配置时，将立即分配磁盘存储，这样性能更好。如果不使用固定大小配置，则按需分配存储，这样可能会影响 AWS Storage Gateway 的正常运行。因此，为使 AWS Storage Gateway 正常运行，必须以固定大小配置的格式存储虚拟机磁盘。



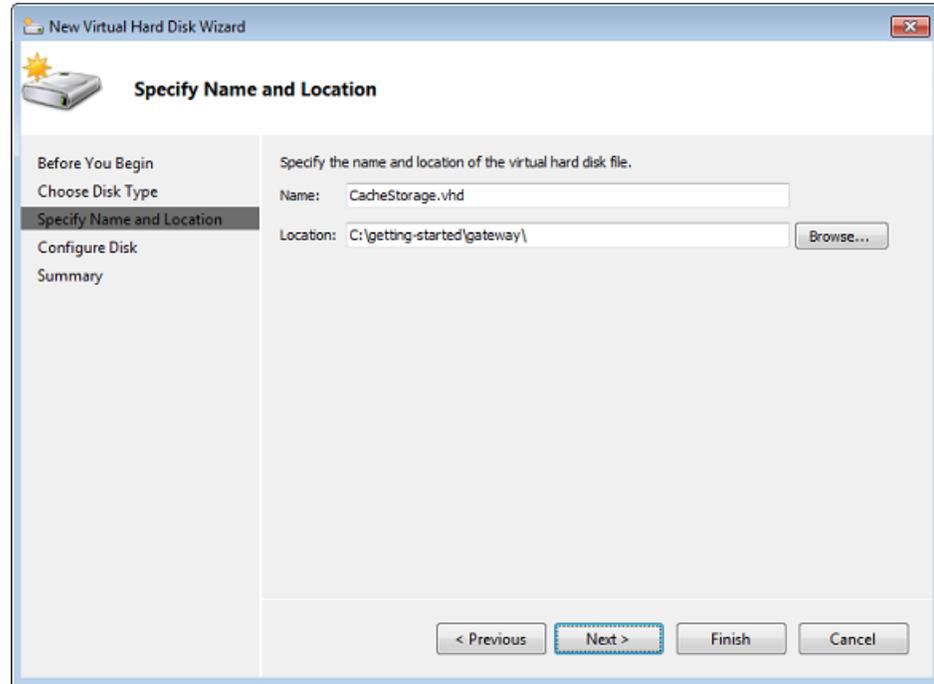
- c. 在指定名称和位置页上，指定该虚拟硬盘的名称和位置。
  - i. 指定 UploadBuffer-vtl.vhd 作为名称。
  - ii. 将位置指定为 c:\getting-started\gateway。



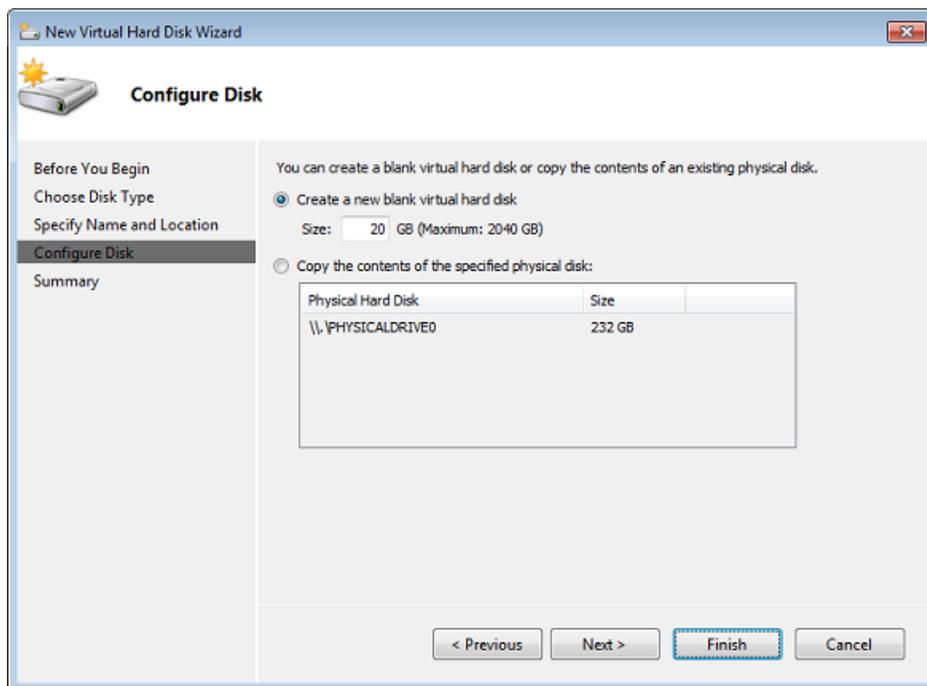
#### Note

在本示例设置中，您使用虚拟机存储虚拟磁盘。对于真实的工作负载，我们强烈建议您不要使用同一底层物理存储磁盘配置本地磁盘。根据主机托管环境、性能和便携性要求，最好在这个步骤选择一个不同的物理磁盘。有关更多信息，请参阅在 [VMware ESXi 主机上为 AWS Storage Gateway VTL VM 配置本地磁盘存储 \(p. 314\)](#)。

- iii. 单击下一步。



- d. 在配置磁盘页中，将磁盘的大小指定为 10 GiB，然后单击完成。

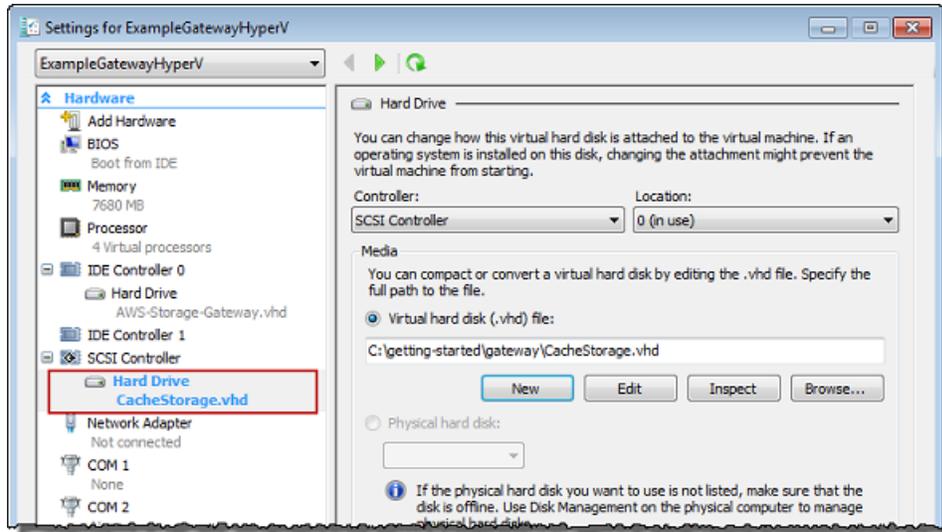


- e. 在创建虚拟磁盘后，确认在 SCSI 控制器下显示硬盘驱动器。  
f. 单击 SCSI 控制器以准备添加另一个硬盘驱动器。



## Warning

在添加另一个硬盘驱动器时，需要先单击 SCSI 控制器，然后再按此过程中的步骤进行操作。在查看现有硬盘驱动器的详细信息时单击新建将替换该现有驱动器。



7. 单击确定。

## 为缓冲存储区分配本地磁盘

您经常访问的应用程序数据在本地维护。您必须在 VM 上分配一个磁盘，作为存储这些数据的缓存。本部分说明如何在主机的物理磁盘上添加虚拟硬盘。在真实的应用程序中，请考虑使用一个单独的物理磁盘作为后备存储。有关使用一个单独的物理磁盘为虚拟硬盘充当后备的说明，请参阅[添加通过硬盘支持的虚拟磁盘 \(p. 452\)](#)。

在本练习中，您向 VM 分配一个 20 GiB 的虚拟磁盘。

## 分配本地磁盘作为缓存存储

- 重复前一节 ([分配本地磁盘作为上传缓冲区 \(p. 288\)](#)) 中的步骤以向网关添加另一个虚拟磁盘。除了使用名称 `CacheStorage-vtl.vhd` 作为磁盘名称，并使用 20 GiB 作为磁盘大小之外，请严格按这些步骤进行操作。

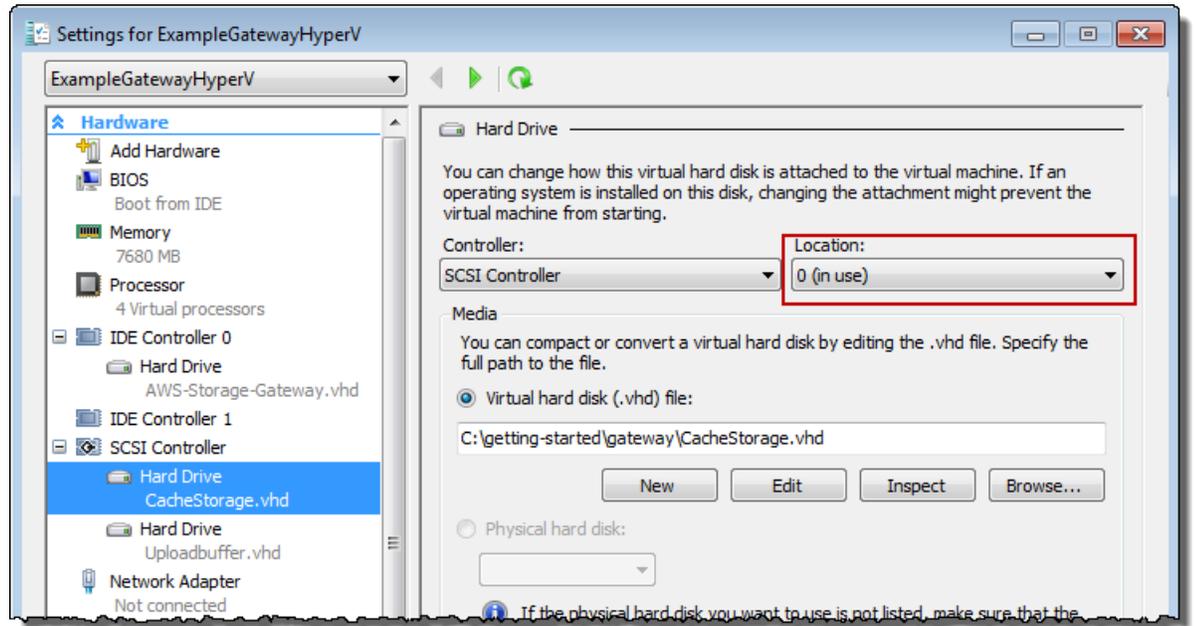
## 验证网关 VM 有两个磁盘

本练习的其余部分要求您已向网关 VM 分配两个磁盘。您可以使用下面的可选步骤验证已给网关 VM 分配好两个磁盘。如果需要分配其他磁盘，则重复[分配本地磁盘作为上传缓冲区 \(p. 288\)](#)过程中的步骤。

## 如需验证 VM 有两个磁盘

1. 如果尚未启动 Microsoft Hyper-V Manager，请启动它并连接到虚拟机监控程序。
2. 在您的虚拟机的虚拟机列表窗格中，选择虚拟机 `ExampleGatewayHyperV`。
3. 在操作窗格中，选择设置...
4. 在设置(您的网关名称)窗口中和硬件窗格中，选择 SCSI 控制器，然后确认 SCSI 控制器下有两个磁盘。

您创建的这两个磁盘随后将用于 AWS Storage Gateway 控制台中，并在下拉列表中显示为 SCSI (0:0) 和 SCSI (0:1)。在下例中，选择 UploadBuffer.vhd 磁盘，并且它为 SCSI (0:0)。



下一步

[激活您的存储网关 VTL \(p. 294\)](#)

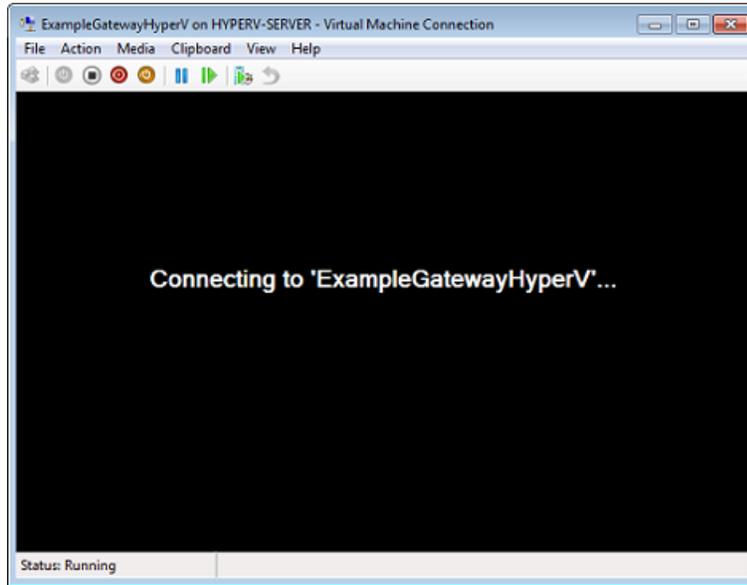
[激活您的存储网关 VTL](#)

现在，您已可随时激活网关。激活过程将您的网关与 AWS 账户关联。您必须在激活网关前启动网关 VM。

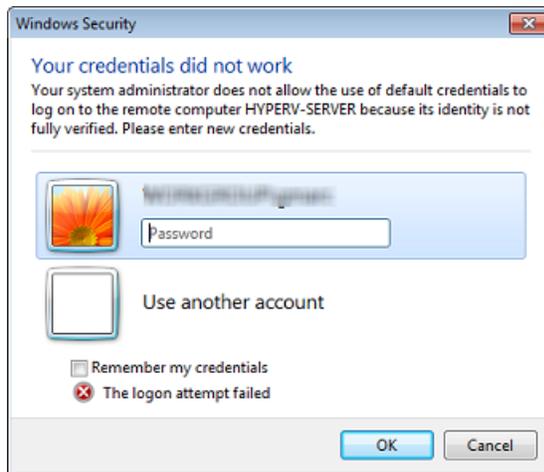
如需激活网关

1. 启动 VM。
  - a. 如果尚未连接 Microsoft Hyper-V Manager，请启动它并连接到虚拟机监控程序。
  - b. 在虚拟机列表窗格中，选择您部署的虚拟机 ExampleGatewayHyperV-VTL。
  - c. 在您的网关的操作窗格中，单击启动。

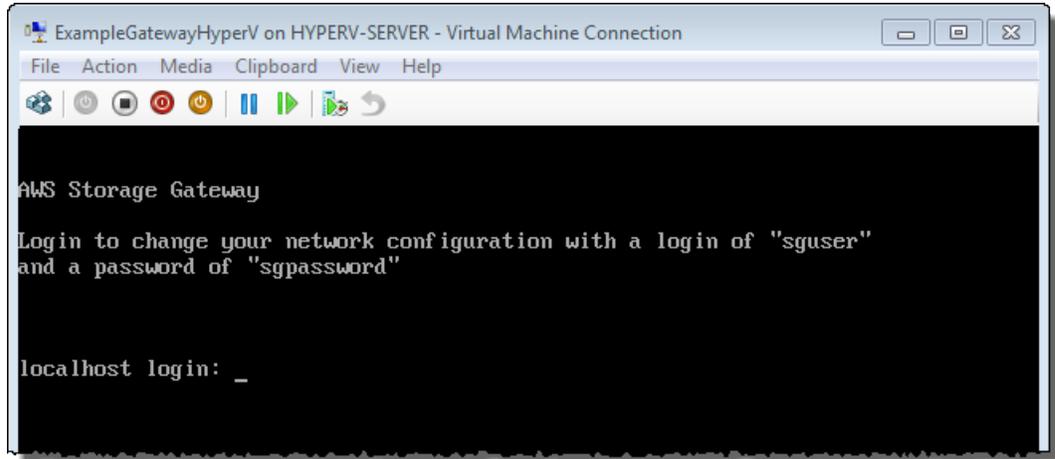
随后将显示虚拟机连接窗口。如果未显示此窗口，则在您的网关的操作窗格中单击连接。



- d. 如果显示身份验证窗口，请输入管理程序管理员向您提供的用户名称和密码。



- e. 在过几分钟时间后，虚拟机就会准备就绪，供您登录了。  
下面的示例介绍了您在 VM 准备就绪时会看到的登录提示。



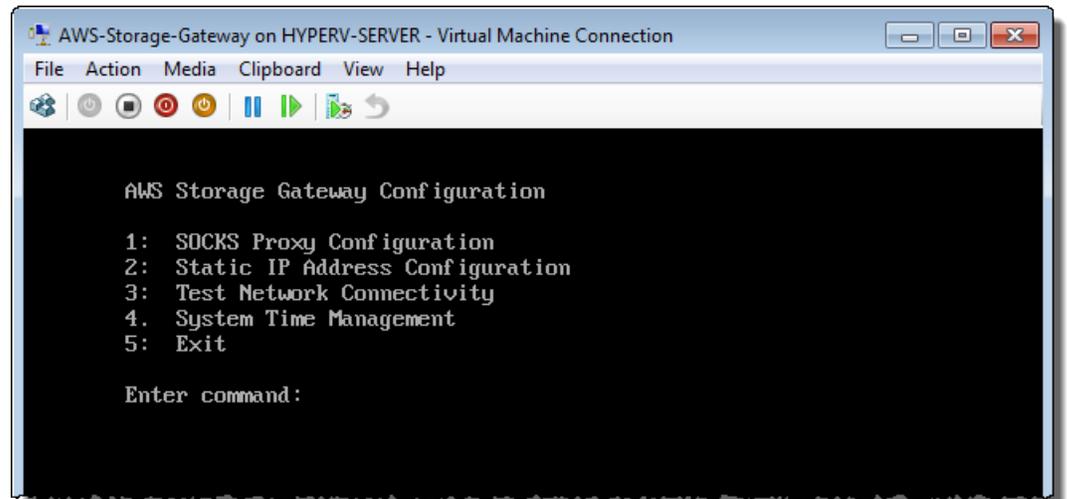
2. 激活网关。

a. 取得您的网关的 IP 地址。

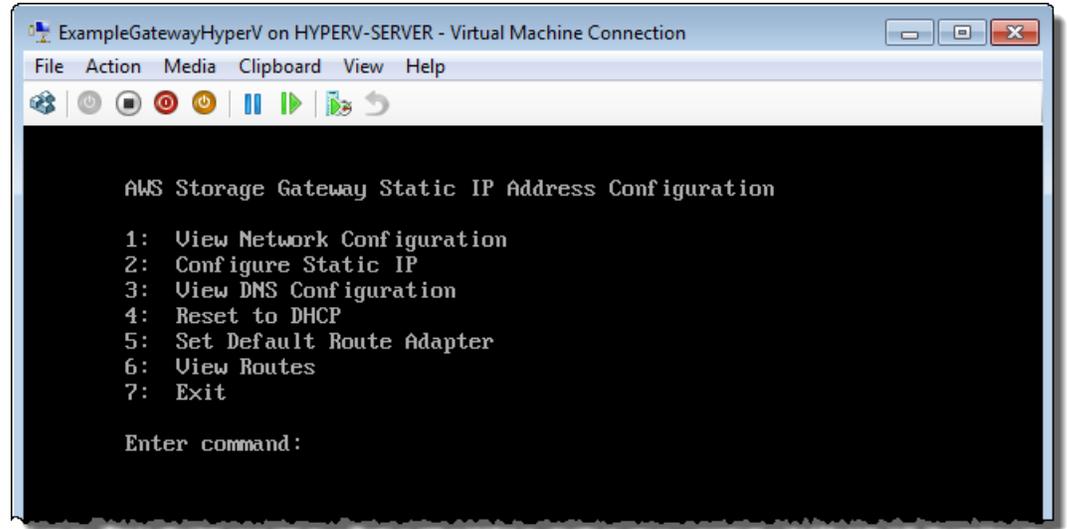
- i. 在 Microsoft Hyper-V 管理器中，选择所部署的网关 VM。
- ii. 在虚拟机列表窗格中，选择虚拟机 ExampleGatewayHyperV。
- iii. 在操作窗格中，单击连接...

随后将显示虚拟机连接窗口。

- iv. 在出现登录提示时，输入用户名 `sguser` 和密码 `sgpassword`。
- v. 在 AWS Storage Gateway 配置菜单中，选择选项 2 静态 IP 地址配置。

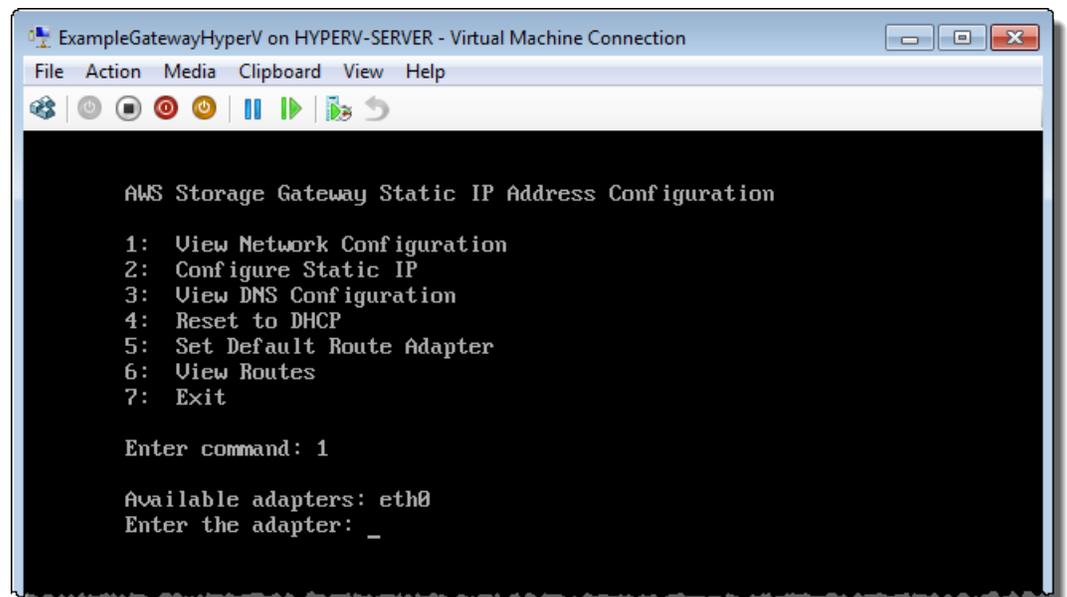


- vi. 在 AWS Storage Gateway 静态 IP 地址配置菜单中，选择选项 1 查看网络配置。



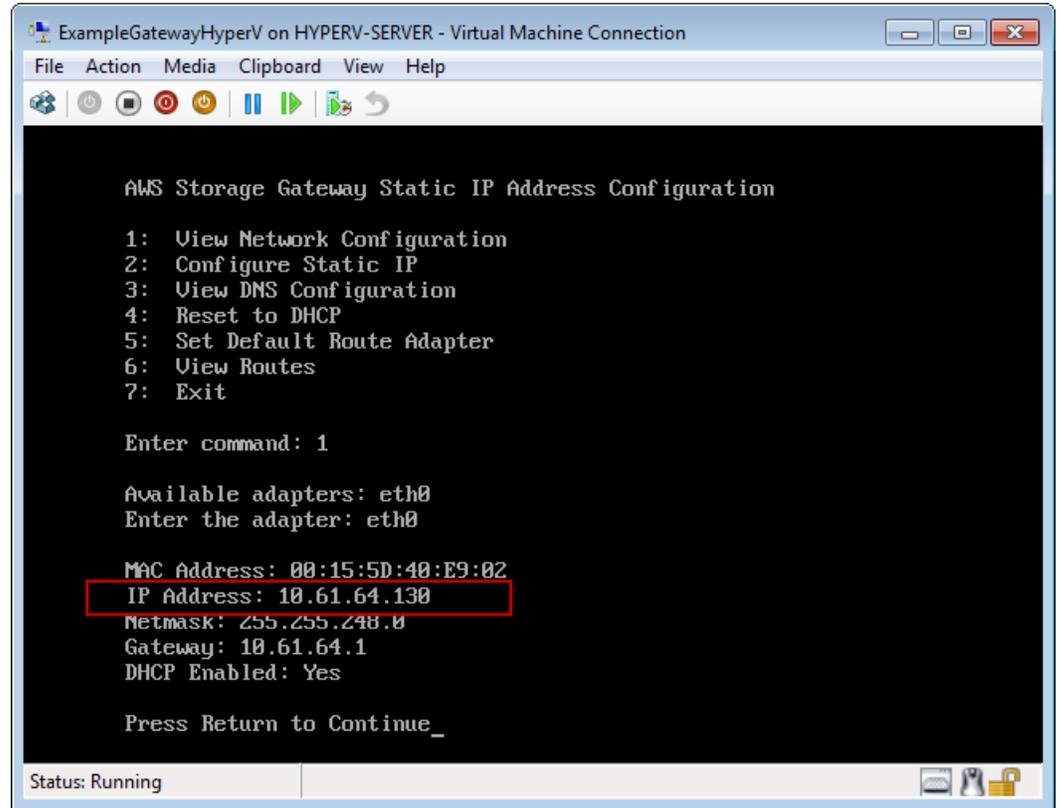
vii. 键入适配器的标识符。

在大多数设置中，eth0 将是适配器标识符。

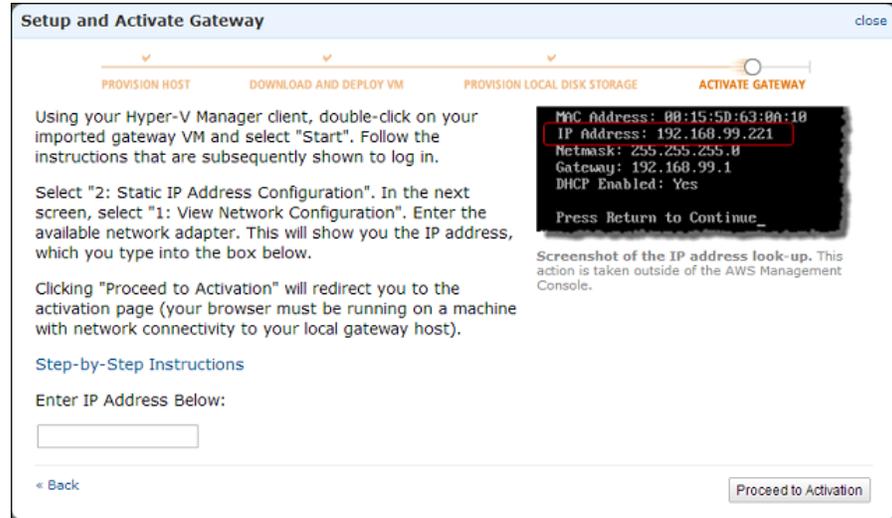


viii. 从适配器信息中获取 IP 地址。

在下例中，IP 地址为 10.61.64.130。您的网关的 IP 地址将会不同。



- ix. 按 Return，然后按提示退出配置菜单。
- b. 将您的网关关联到 AWS 账户。
  - i. 在 AWS Storage Gateway 控制台的设置并激活网关向导中，导航到以下激活网关页。
    - A. 如果尚未启动该向导，则单击设置并激活新网关。
    - B. 在向导的每个步骤中单击继续，直到抵达激活网关页。
  - ii. 输入您的网关的 IP 地址，然后单击继续激活。记下该 IP 地址，因为以后在访问设备时需要该地址。



### Note

激活期间，您的浏览器连接到网关。如果激活失败，则确认输入的 IP 地址正确无误。如果该 IP 地址正确，则确认已将网络配置为允许浏览器访问网关 VM。

iii. 在激活页上，输入所要求的信息以完成激活过程。

- AWS 地区决定 AWS 存储虚拟磁带的位置。您不可以在网关激活后更改地区。

在以下地区提供 AWS Storage Gateway：

Region name	Region string
US East (Northern Virginia)	us-east-1
US West (Northern California)	us-west-1
US West (Oregon)	us-west-2
EU (Ireland)	eu-west-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1

- 网关时区指定希望网关使用的时区。
- 网关名称在控制台中标识您的网关。您使用该名称在控制台中管理网关，可在激活后更改名称。该名称必须是您账户的唯一名称。网关的名称不得含有空格。
- 介质更换器类型指定此网关中使用的机械手的类型。
- 磁带驱动器类型指定此网关中使用的磁带驱动器的类型。



iv. 单击激活我的 Storage Gateway。

成功激活后，AWS Storage Gateway 控制台在导航窗格的网关部分下显示一个链接，指向已激活的网关。单击刚刚部署的网关。如果激活失败，请参阅[网关 VTL 问题排查 \(p. 411\)](#)以了解可能采用的解决方案。

随后将显示创建磁带按钮。



单击创建磁带后，将有向导指导您如何为网关配置本地存储、创建可选警报和创建虚拟磁带。



#### Note

首次为网关 VTL 创建磁带时，必须先为网关配置本地存储，然后才能创建虚拟磁带。

下一步

[步骤 2：配置本地存储和警报 \(p. 300\)](#)

## 步骤 2：配置本地存储和警报

在本练习的前面，您创建了两个磁盘，一个用于上传缓冲区 (10 GiB)，另一个用于缓存存储 (20 GiB)。将网关配置为使用这些磁盘。还可创建可选警报以监控您的磁盘。

配置本地存储（缓存存储和上传缓冲区）

- 在配置已激活的网关向导中，配置本地工作存储。



- 在所配置的两个磁盘中，选择一个作为上传缓冲区，另一个作为缓冲存储，如以下屏幕截图所示。
- 单击下一步。

现在，可创建可选警报以监控已创建的两个磁盘的存储用量。

配置警报

- 在上传缓冲区警报页中，配置上传缓冲区用量的警报。



- 使用两个下拉框，选择用来创建两个上传缓冲区警报的使用率。

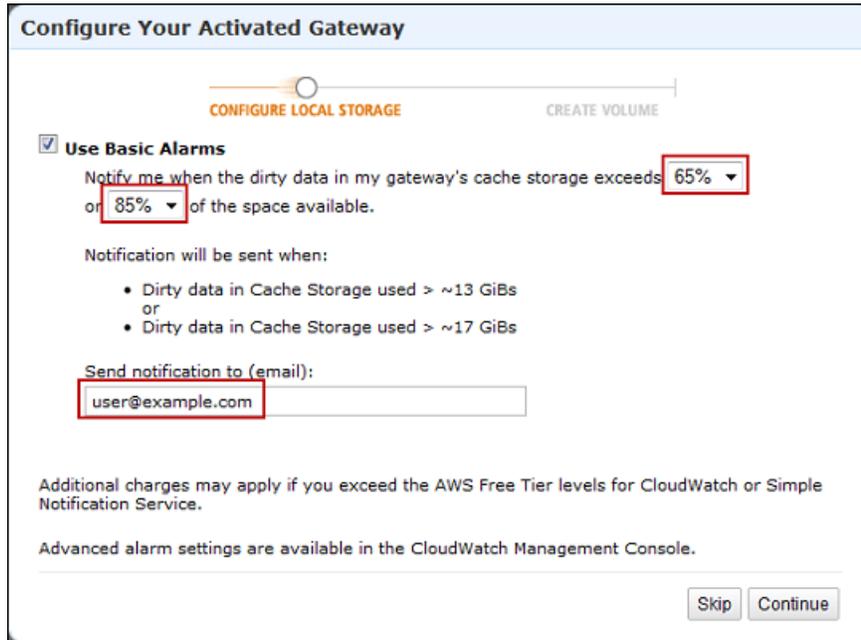
例如，您可以选择阈值，从而让第一个阈值（较低百分率值）代表您希望在其被超过的情况下收到相关警报的上传缓冲区使用率。可以选择第二个阈值来代表这样一个上传缓冲区使用率，即在其超过的情况下成为添加更多上传缓冲区空间等操作的触发原因。

完成此步骤后，可随时转到 Amazon CloudWatch 控制台并更改警报阈值。

- 输入电子邮箱地址。
- 单击继续。

可将警报命名为一例如，*MyGatewayBufferUtilizationAlarm*。

- d. 检查是否向指示的电子邮件地址发送了订阅确认电子邮件，然后按这封电子邮件中的说明确认您对 Amazon Simple Notification Service (Amazon SNS) 主题的订阅。确认订阅后，无论超过了您指定的哪一阈值，都会收到电子邮件。
2. 单击继续以创建警报。
3. 在缓存存储警报页中，配置缓存存储的警报。



按[配置警报 \(p. 300\)](#)过程的第 1 步中的说明配置此警报。

可将警报命名为—例如，*MyGatewayCacheBufferAlarm*。

4. 单击继续以创建警报。

下一步

[步骤 3：使用 AWS Storage Gateway 控制台创建虚拟磁带 \(p. 301\)](#)

## 步骤 3：使用 AWS Storage Gateway 控制台创建虚拟磁带

现在已激活网关 VTL，接下来将创建虚拟磁带。



### Note

只需为写入磁带的数量而非整个磁带容量付费。

以下屏幕截图显示创建虚拟磁带页。



### 创建虚拟磁带

1. 在磁带数量文本框中，输入要创建的磁带数量。在本练习中，可创建三个磁带。

- 在容量文本框中，输入要创建的虚拟磁带的大小。在本练习中，可输入 100 GiB。
- 在条码前缀文本框中，输入要在虚拟磁带的条码之前追加的前缀。在本练习中，可接受默认设置。



Note

条码前缀为可选。

- 单击创建磁带。

确认页显示网关上的 iSCSI 目标。可随时通过选择网关并导航到 VTL 设备选项卡，在 AWS Storage Gateway 控制台中查看此信息。

以下屏幕截图显示为网关创建的设备的配置页。



可关闭确认页。

下一步

[步骤 4：将网关 VTL 设备连接到 Windows 客户端 \(p. 302\)](#)

## 步骤 4：将网关 VTL 设备连接到 Windows 客户端

在此入门练习中，您使用 Windows iSCSI 发起程序连接到网关的 VTL 设备。在此过程结束时，这些设备即成为 Windows 客户端上的本地设备。在此步骤后，配置备份软件以访问这些设备。

将 Windows 客户端连接到虚拟磁带库设备

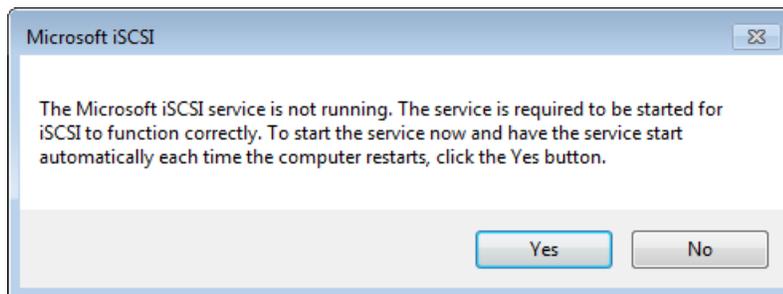
- 在 Windows 客户端计算机的开始菜单中，输入 iscsicpl.exe 并运行该程序。



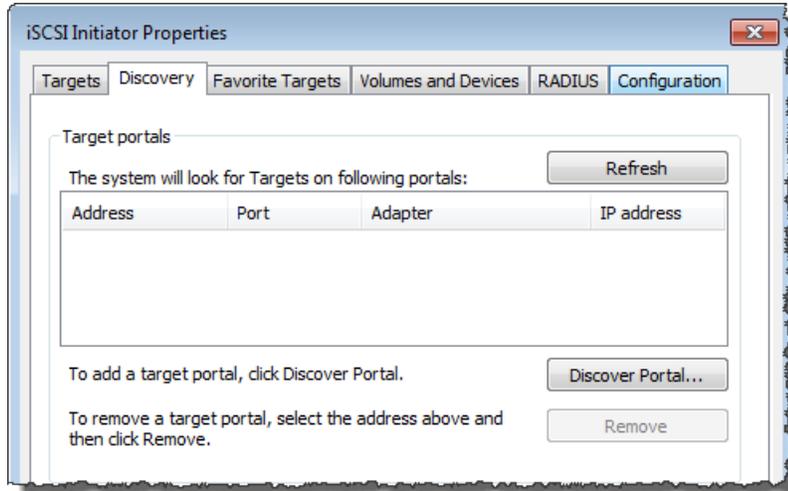
Note

必须具有客户端计算机上的管理员权限才能运行 iSCSI 发起程序。

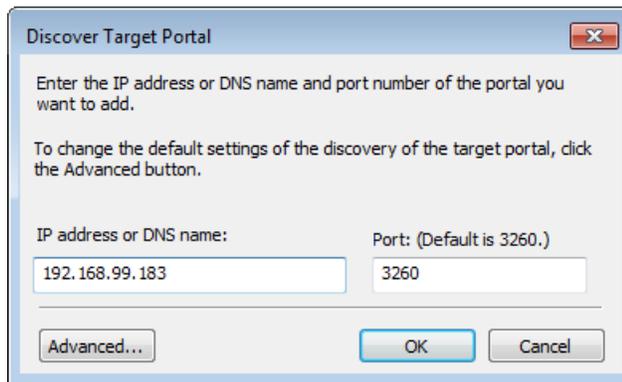
- 如果出现提示，则单击是启动 Microsoft iSCSI 发起程序服务。



- 在 iSCSI 发起程序属性对话框中，单击发现选项卡，然后单击发现门户按钮。

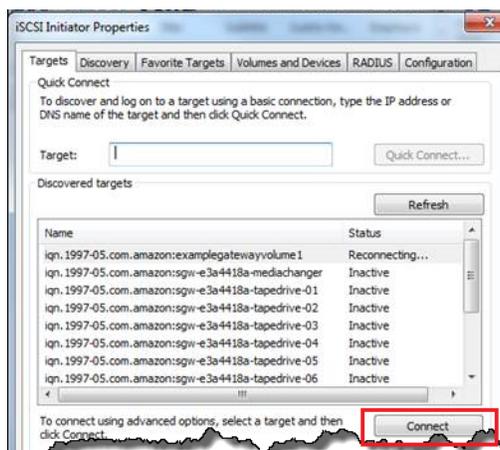


4. 在发现目标门户对话框的 IP 地址或 DNS 名称字段中，输入网关 VTL 的 IP 地址，然后单击确定。



5. 选择目标选项卡，然后单击刷新。随后在发现的目标框中显示所有十个磁带驱动器和介质更换器。目标的状态为不活动。

以下屏幕截图显示所发现的目标。



6. 选择第一个设备，然后单击连接。一次连接一个设备。
7. 在连接到目标对话框中，单击确定。

- 对每个设备重复前两步（第 6 步和第 7 步）以连接这些设备，然后在 iSCSI 发起程序属性窗口中单击确定。
- 在 Windows 客户端上，磁带驱动器的驱动程序提供商必须为 Microsoft。按以下过程验证驱动程序提供商，如有必要，则更新它。

- 在 Windows 客户端上，启动“设备管理器”。
- 展开磁带驱动器，右键单击某个磁带驱动器，然后选择属性。



- 在设备属性对话框的驱动程序选项卡中，确认驱动程序提供商为 Microsoft。



- 如果驱动程序提供商不是 Microsoft，则设置如下值：
  - 单击更新驱动程序
  - 在更新驱动程序软件对话框中，单击浏览计算机以查找驱动程序软件。



- 在更新驱动程序软件对话框中，单击从计算机的设备驱动程序列表中选择。



- 选择 LTO Tape drive，然后单击下一步。



- 关闭更新驱动程序软件窗口，然后确认驱动程序提供商值现在设为 Microsoft。
- 重复步骤 9.2 到 9.5 以更新所有磁带驱动器。

下一步

[步骤 5：测试网关 VTL 设置 \(p. 304\)](#)

## 步骤 5：测试网关 VTL 设置

在此步骤中，通过使用 [Symantec NetBackup 7.5 版](#) 备份软件执行以下任务，测试设置。

- 将示例数据备份到磁带
- 将磁带存档
- 从存档中检索磁带
- 从磁带中读取数据

### Topics

- [配置 NetBackup 存储设备 \(p. 305\)](#)
- [将示例数据备份到网关 VTL 上的磁带 \(p. 306\)](#)
- [将磁带存档 \(p. 310\)](#)
- [将存档的磁带从 VTS 检索回网关 VTL \(p. 310\)](#)
- [从磁带还原数据 \(p. 311\)](#)

下一步

[配置 NetBackup 存储设备 \(p. 305\)](#)

## 配置 NetBackup 存储设备

在此步骤中，配置 NetBackup 以使用在上一步中添加到 Windows 客户端的存储设备。在此步骤后，NetBackup 将在网关 VTL 上使用这些存储设备。

要配置 NetBackup 以在网关 VTL 上使用存储设备

1. 打开 NetBackup 管理控制台并以管理员身份运行它。



2. 单击配置存储设备以打开设备配置向导。
3. 单击下一步。NetBackup 软件将您的计算机检测为设备主机。
4. 在设备主机列中，选择您的计算机，然后单击下一步。NetBackup 软件扫描您的计算机中的设备，并发现所有设备。



5. 在正在扫描主机页中，单击下一步，然后单击下一步。随后在您的计算机上找到您的所有磁带驱动器和介质更换器。



6. 在备份设备窗口中，单击下一步。
7. 在拖放配置窗口中，确认选择了您的介质更换器，然后单击下一步。
8. 在随后显示的对话框中，单击是以将配置保存到您的计算机上。NetBackup 软件更新设备配置。
9. 更新完毕后，单击下一步以使这些设备对 NetBackup 软件可用。NetBackup 软件检测全部十个磁带驱动器和介质更换器。
10. 在已完成! 窗口中，单击完成。

在 NetBackup 软件中验证您的设备

1. 在 NetBackup 管理控制台中，展开媒体和设备管理节点，然后展开设备节点。单击驱动器以显示所有磁带驱动器。



2. 在设备节点中，单击机械手以显示您的所有机械手（介质更换器）。

在 NetBackup 软件中，介质更换器称为“机械手”。

3. 在所有机械手窗格中，右键单击 TLD(0)（您的机械手），然后单击清点机械手。
4. 在机械手清点窗口中，确认从位于选择机械手类别中的设备主机下拉列表中选择了您的主机。
5. 确认从机械手下拉列表中选择了您的机械手。
6. 在机械手清点窗口中，选择更新卷配置，选择预览更改，选择更新前清空介质访问端口，然后单击开始。



此操作将更新并清点您在 NetBackup 企业介质管理 (EMM) 数据库中的机械手（介质更换器）和虚拟磁带。NetBackup 将介质信息、设备配置和磁带状态存储在 EMM 中。

7. 在机械手清点窗口中，单击是。此操作将更新配置，并将在导入/导出插槽中找到的虚拟磁带移至虚拟磁带库。



8. 以下屏幕截图显示在导入/导出插槽中找到的三个虚拟磁带。



关闭机械手清点窗口。

9. 在介质节点中，展开机械手节点，然后单击 TLD(0) 以显示对您的机械手（介质更换器）可用的所有虚拟磁带。



#### Note

如果以前已将其他设备连接到 NetBackup 软件，则可能有多个机械手。确保所选的机械手正确无误。



现在已连接了设备并使其对备份软件可用，已准备好通过将数据备份到所创建的虚拟磁带上，测试网关，并准备好将这些虚拟磁带存档到 Amazon Glacier 支持的虚拟磁带架 (VTS) 中。

下一步

[将示例数据备份到网关 VTL 上的磁带 \(p. 306\)](#)

## 将示例数据备份到网关 VTL 上的磁带

在本节中，您通过将数据备份到虚拟磁带上，测试网关 VTL 设置。



#### Note

应备份本入门练习的少量数据，因为将产生与存储、存档和检索数据关联的成本。有关定价信息，请转到 AWS Storage Gateway 产品详细信息页中的[定价](#)。

## 创建卷池

卷池是要用于备份的虚拟磁带的集合。

1. 启动 NetBackup 管理控制台。
2. 展开介质节点，右键单击卷池，然后单击新建。此操作将打开新建卷池对话框。



3. 在名称文本框中，输入卷池的名称。
4. 在说明文本框中，输入卷池的说明，然后单击确定。刚创建的卷池即添加到卷池列表。

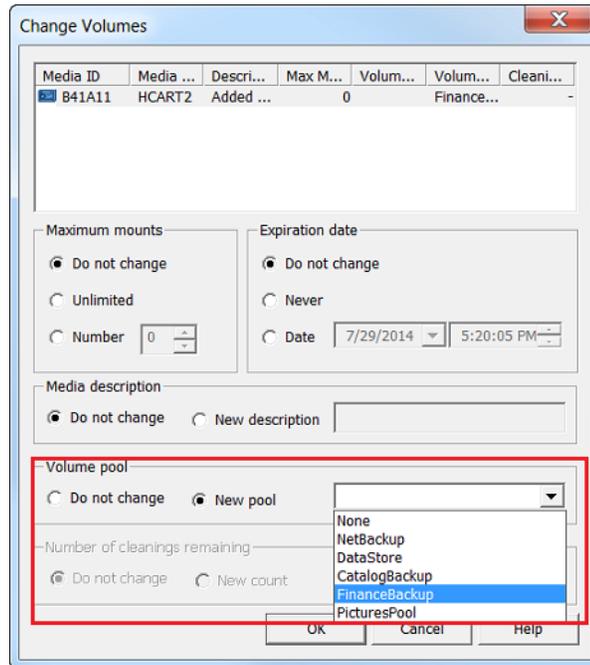
以下屏幕截图显示卷池的列表。



### 将虚拟磁带添加到卷池

1. 展开机械手节点，然后选择 TLD(0) 机械手以显示此机械手识别的虚拟磁带。  
注意，如果以前已连接了机械手，则您的网关 VTL 机械手的名称可能不同。
2. 从虚拟磁带的列表中，右键单击要添加到卷池的磁带，然后单击更改以打开更改卷对话框。

以下屏幕截图显示更改卷对话框。



3. 在卷池类别中，选择新建池。
4. 从新建池下拉列表中，选择刚刚创建的池，然后单击确定。

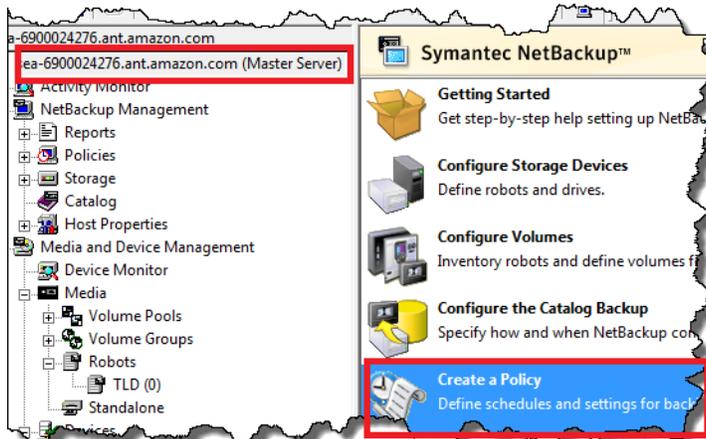
可通过展开介质节点并单击您的卷池，确认您的卷池包含刚刚添加的虚拟磁带。

### 创建备份策略

1. 备份策略指定要备份什么数据、何时备份和要使用哪个卷池。

选择主服务器以返回 Symantec NetBackup 控制台。

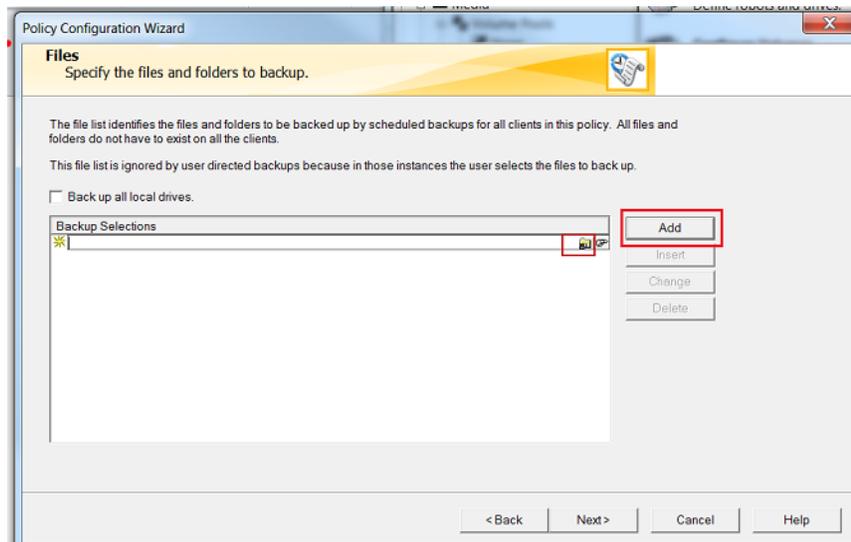
以下屏幕截图显示选择了创建策略的 NetBackup 控制台。



2. 单击创建策略以打开策略配置向导窗口。
3. 选择文件系统、数据库、应用程序，然后单击下一步。
4. 在策略名称文本框中，输入策略的名称，然后确认从选择策略类型下拉列表选择了 MS-Windows，然后单击下一步。
5. 在客户端列表窗口中，单击添加，在名称列中输入您的计算机的主机名，然后单击下一步。此操作将您定义的策略应用于本地主机（客户端计算机）。



6. 在文件窗口中，单击添加，然后单击文件夹图标。



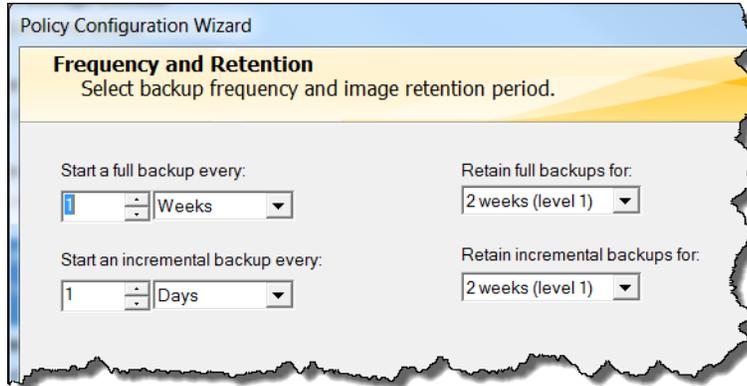
7. 在浏览窗口中，浏览到要备份的文件夹或文件，单击确定，然后单击下一步。
8. 在备份类型窗口中，接受默认值，然后单击下一步。



#### Note

如果要自行开始备份，则选择用户备份。

9. 在频率和保留窗口中，选择要应用于备份的频率和保留策略。在本练习中，可接受所有默认值，然后单击下一步。



10. 在开始时间范围中，选择业余时间，然后单击下一步。此操作指定应仅在业余时间备份您的文件夹。



11. 在策略配置向导中，单击完成。

该策略根据计划运行备份。还可随时手动备份，在下一步中我们将这样做。

#### 进行手动备份

1. 在 NetBackup 控制台的左侧导航窗格中，展开 NetBackup 管理节点。
2. 展开策略节点。
3. 右键单击您的策略，然后单击手动备份。



4. 在手动备份窗口中，选择一个计划，选择一个客户端，然后单击确定。



5. 在随后显示的手动备份已开始对话框中，单击确定。
6. 在左侧导航窗格中，单击活动监视器以按作业 ID 查看备份的状态。



可在作业详细信息窗口中找到备份中使用的虚拟磁带的条码。

#### 查找磁带的条码

我们来查找 NetBackup 写入文件数据的磁带的条码。在下一步中将磁带存档到虚拟磁带架 (VTS)，其中将需要此条码。

1. 在活动监视器中，右键单击备份作业的作业 ID，然后单击详细信息。
2. 在作业详细信息窗口中，单击详细状态选项卡。
3. 在状态框中，找到介质 ID。例如，在以下屏幕截图中，介质为 87A222。此 ID 可帮助您确定已将数据写入到哪个磁带。



您已成功部署了网关 VTL、创建了虚拟磁带并备份了您的数据。现在，可将虚拟磁带存档并尝试从 VTS 检索这些虚拟磁带。

下一步

[将磁带存档 \(p. 310\)](#)

## 将磁带存档

将磁带存档时，AWS Storage Gateway 将磁带从网关的虚拟磁带库 (VTL) 移至虚拟磁带架 (VTS)，后者为离线存储。通过使用备份应用程序弹出磁带，发起磁带存档。

将虚拟磁带存档

1. 在 NetBackup 管理控制台中，展开介质和设备管理节点，然后展开介质节点。
2. 展开机械手，然后单击 TLD(0)。
3. 右键单击要存档的虚拟磁带，然后单击从机械手弹出卷。



4. 在弹出卷窗口中，确保介质 ID 与要弹出的虚拟磁带相符，然后单击弹出。



5. 在随后出现的对话框（从介质访问端口卸下弹出的介质，是否要继续弹出？）中，单击是。



弹出过程完毕后，弹出卷对话框中磁带的状态指示弹出已成功。



可关闭弹出卷窗口。

6. 在 AWS Storage Gateway 控制台中，可验证所存档的磁带的状态。将数据上传到 AWS 可能需要一段时间才能上传完毕。在这段时间内，将在网关的虚拟磁带库 (VTL) 中列出弹出的磁带，状态为“正在中转到 VTS”或“正在存档”。数据上传完毕后，VTL 中即不再列出弹出的磁带。
7. 单击您的网关，然后单击 VTL 盒式磁带；确认您的网关中不再列出该虚拟磁带。
8. 在 AWS Storage Gateway 控制台的导航窗格中，单击虚拟磁带架。确认 VTS 中列出了您的存档磁带，并且状态为“已存档”。

下一步

[将存档的磁带从 VTS 检索回网关 VTL \(p. 310\)](#)

## 将存档的磁带从 VTS 检索回网关 VTL

Topics

存档的磁带存储在虚拟磁带架 (VTS) 中，后者为离线存储。如果要访问磁带数据，必须首先将磁带从 VTS 检索回网关。在此步骤中，将检索在上一步中存档的磁带。



### Note

将磁带从 VTS 检索回网关耗时大约 24 小时。

## 检索存档的磁带

1. 在 AWS Storage Gateway 控制台的导航窗格中，单击虚拟磁带架。随后，控制台显示所有网关已存档的所有虚拟磁带。
2. 选择要检索的虚拟磁带，然后单击检索磁带。



### Note

要检索的虚拟磁带的状态必须为“已存档”。



3. 在检索磁带向导的磁带条码字段中，确认条码标识的是要检索的虚拟磁带。



4. 在网关下拉列表中，选择要将存档的磁带检索到的网关，然后单击继续。

磁带的状态从“已存档”变为“正在检索”。移动所有数据后，VTS 中虚拟磁带的状态变为“已检索”，并且在网关的虚拟磁带库 (VTL) 中显示该磁带。



### Note

检索的虚拟磁带为只读。

## 下一步

[从磁带还原数据 \(p. 311\)](#)

## 从磁带还原数据

在此步骤中，将数据从磁带还原到客户端计算机。



### Note

此步骤不使用在以前步骤中使用的 NetBackup 管理控制台。而是将使用随 Symantec NetBackup 软件一起安装的“备份、存档和还原”软件。

## 还原数据

1. 启动备份、存档和还原软件，并以管理员身份运行它。
2. 单击选择进行还原选项卡。



3. 如果以前备份过数据，则将在 NetBackup 历史记录窗格中看到备份图标。在本例中，仅有一个备份图标。



4. 选择表示要还原的备份的备份图标。
5. 在所有文件夹窗格中，选择要还原的文件夹，然后单击左侧窗格中的还原标记的文件图标（此图标无标签。将鼠标放在此图标上时会显示名称）。



6. 在还原标记的文件窗口中，选中将所有内容还原到其他位置(保持现有结构)按钮。这样可避免覆盖您的原始数据。



7. 在目标框中，浏览到要将数据还原到的文件夹，然后单击开始还原。
8. 在随后显示的对话框中，单击是以查看还原过程的进度。



在查看状态窗口中，可看到还原过程的状态。如果还原成功，则状态变为成功。

下一步

[步骤 6：在示例练习后进行清除 \(p. 312\)](#)

## 步骤 6：在示例练习后进行清除

完成本指南中的练习后，如果不想继续使用您的网关 VTL，请考虑将其清除。这样可避免产生费用。

如果要继续使用您的网关 VTL，则参阅[我从这里可以继续进行哪些内容？ \(p. 312\)](#)中的其他信息。

应按顺序执行以下步骤以确保成功释放资源。

1. 同时从网关的虚拟磁带库 (VTL) 以及虚拟磁带架 (VTS) 中删除磁带。
  - a. 取消从网关的 VTL 中检索任何处于“正在检索”状态的磁带。

有关说明，请参阅[取消磁带检索 \(p. 374\)](#)。
  - b. 从网关的 VTL 中将任何处于“已检索”状态的磁带存档。

有关说明，请参阅[将磁带存档到 VTS \(p. 374\)](#)。
  - c. 从网关的 VTL 中删除任何剩余的磁带。

有关说明，请参阅[从网关 VTL 的虚拟磁带库中删除磁带 \(p. 373\)](#)。
  - d. 删除您在 VTS 中拥有的任何磁带。

有关说明，请参阅[从 VTS 中删除磁带 \(p. 378\)](#)。
2. 如果要使用该网关 VTL，则可保留它。否则，请删除该网关。
  - a. 删除所有处于“正在检索”和“已检索”状态的磁带后，删除该网关。

有关说明，请参阅[删除网关 VTL \(p. 390\)](#)。
  - b. 从本地主机中删除 AWS Storage Gateway VM。

## 我从这里可以继续进行哪些内容？

入门部分提供尝试示例设置的说明。这些步骤未涉及某些设置详细信息，如特定方案需要多少上传缓冲区 and 缓存存储。有关设置的详细信息，请参阅[设置网关 VTL \(p. 313\)](#)。

网关 VTL 处于生产环境后，可执行若干管理任务，如添加和删除磁带、监控和优化网关性能以及故障排除。有关这些管理任务的信息，请参阅[管理已激活的网关 VTL \(p. 361\)](#)。

可在 AWS Management Console 中执行某些网关 VTL 维护任务，如配置网关的带宽速率限制和管理网关软件更新。如果网关 VTL 部署在本地，则可在网关的本地控制台中执行某些维护任务，如通过代理路由网关 VTL 以及配置网关以使用静态 IP 地址。如果正在运行网关作为 Amazon EC2 实例，则可在 Amazon EC2 控制台中执行一些特定的维护任务，如添加和删除 Amazon EBS 卷。有关更多信息，请参阅[执行网关 VTL 维护任务 \(p. 378\)](#)。

## 设置网关 VTL

您可以选择将 AWS Storage Gateway 作为本地虚拟机 (VM) 设备运行，或在云中将其作为 Amazon Elastic Compute Cloud (Amazon EC2) 实例运行。对于托管本地 VM，AWS Storage Gateway 支持 VMware ESXi 管理程序和 Microsoft Hyper-V 2008 R2 管理程序。有关更多信息，请参见 [要求 \(p. 7\)](#)。

### Topics

- [本地部署和激活 AWS Storage Gateway VTL \(p. 313\)](#)
- [在 Amazon EC2 上部署并激活网关 VTL \(p. 341\)](#)
- [配置上传缓冲区和缓存存储空间 \(p. 346\)](#)
- [使用 AWS Storage Gateway 控制台创建虚拟磁带 \(p. 347\)](#)
- [连接到网关上的 VTL 设备 \(p. 348\)](#)

## 本地部署和激活 AWS Storage Gateway VTL

您可以在数据中心的虚拟主机上部署 AWS Storage Gateway 软件设备。有关最低主机要求，请参见 [要求 \(p. 7\)](#)。我们将介绍如何使用 VMware ESXi 和 Microsoft Hyper-V 虚拟环境托管您的网关。

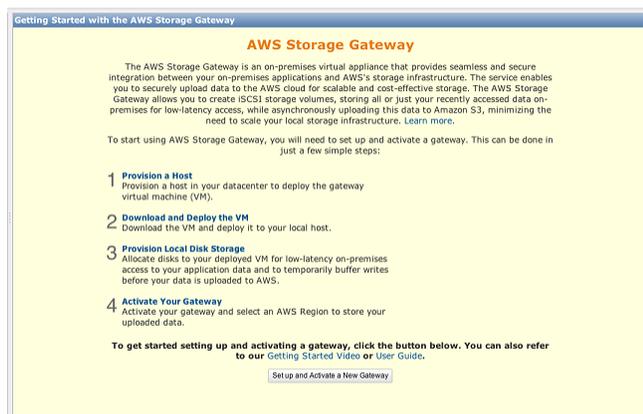
我们建议您在继续本部分之前查阅该指南的入门部分（请参见 [入门 \(网关 VTL\) \(p. 257\)](#)）。

### 如需开始设置

1. 请转到 [AWS Storage Gateway](#) 并单击注册。

下载并部署 AWS Storage Gateway 前，您必须注册该服务。

2. 如果您的 AWS 账户下没有已激活的网关，就需要从下页开始学习使用 AWS Storage Gateway。单击设置并激活新网关按钮以启动设置并激活网关向导。



如果您已激活一个或多个网关，控制台就会显示您的网关列表。在导航窗格中，单击部署新网关以启动设置并激活新网关向导。



## 在 VMware ESXi 主机上部署和激活 AWS Storage Gateway VTL

本部分介绍如何在 VMware ESXi 主机上部署并激活 AWS Storage Gateway 虚拟机 (VM)。激活过程会将网关与您的 AWS 账户关联。



## Note

此处描述的任务假定您已经预配置了 VMware ESXi 主机。如果您尚未完成此操作，请参见“入门”部分中的 [配置 VMware 主机以部署 AWS Storage Gateway VM \(p. 260\)](#)。

## Topics

- [下载 AWS Storage Gateway 虚拟机 \(VM\) 并将其部署在 VMware ESXi 主机上 \(p. 314\)](#)
- [在 VMware ESXi 主机上为 AWS Storage Gateway VTL VM 配置本地磁盘存储 \(p. 314\)](#)
- [激活部署在 VMware ESXi 主机上的 AWS Storage Gateway-VTL \(p. 323\)](#)

## 下载 AWS Storage Gateway 虚拟机 (VM) 并将其部署在 VMware ESXi 主机上

使用 AWS Management Console 中的设置并激活网关向导配置主机后，下一步为下载并部署 VM。在此步骤中，选择要用于部署网关的虚拟化平台，下载 VM，然后部署它。



本入门练习说明如何下载和部署网关。有关说明，请参阅 [下载 AWS Storage Gateway VM 并将其部署在您的主机上 \(p. 261\)](#)。

## 将 AWS Storage Gateway 与 VMware High Availability 配合使用

VMware 高可用性 (HA) 是一种 vSphere 组件，可以在支持网关 VM 的基础结构层提供故障防护。为此，VMware HA 使用配置为集群的多个主机，以使如果一个运行网关 VM 的主机发生故障，则可自动在该集群内的其他主机上重新启动该网关 VM。有关 VMware HA 的详细信息，请转到 [VMware HA：概念和最佳实践](#)。

应该按下列建议做法将 AWS Storage Gateway 与 VMware HA 一起使用。

- 只在群集中的一个主机上部署网关的开放虚拟应用程序 (Open Virtualization Application, OVA)。
- 当部署 OVA 时，选择一个不在主机本地的数据存储器。相反，使用一个可供群集的所有主机访问的数据存储器。如果您选择的是主机本地的数据存储器，而主机发生了故障，那么，群集中的其他主机可能无法访问该数据源，且可能无法进行故障转移。
- 遵循建议的 iSCSI 设置，以防在故障转移期间发起程序从 VTL 设备目标断开连接。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需要花费几秒钟到几分钟的时间。Windows 客户端（请参阅 [建议进行的 Windows iSCSI 设置 \(p. 349\)](#)）和 Linux 客户端（请参阅 [建议进行的 Linux iSCSI 设置 \(p. 352\)](#)）的建议 iSCSI 超时大于进行故障转移通常所需的时间。
- 在使用集群的情况下，如果您给集群部署 OVA，系统会要求您选择主机。或者您也可以直接部署到群集中的主机里。

## 在 VMware ESXi 主机上为 AWS Storage Gateway VTL VM 配置本地磁盘存储

网关 VM 可将您本地分配的本地磁盘用于以下目的：

- 上传缓冲区 – 上传缓冲区提供了一个暂存区域，在网关将数据上传到 Amazon S3 之前，可将写入到磁带的本地数据保存到该区域。
- 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。当应用程序对虚拟磁带执行 I/O 时，网关会将数据保存到缓存存储空间中以实现低延迟访问。当您的应用程序请求磁带中的数据时，网关在从 AWS 下载数据前会先检查缓存存储空间中的数据。

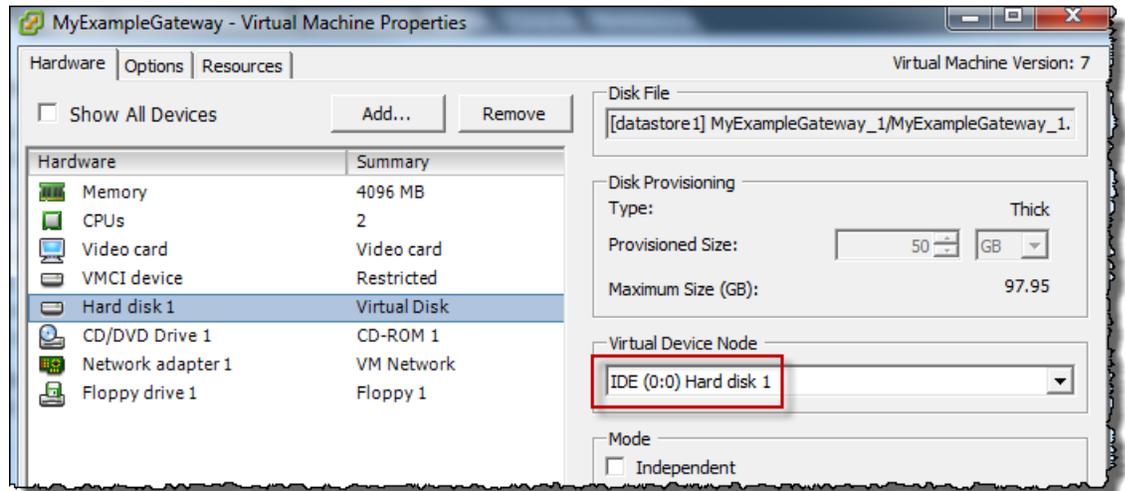
## Topics

- 为上传缓冲区添加本地磁盘 ( 网关 VTL ) ( p. 315)
- 为缓存存储添加本地磁盘 ( 网关 VTL ) ( p. 319)
- 在 VMware ESXi 主机上将 AWS Storage Gateway VM 配置为使用半虚拟化 ( p. 322)



## Note

部署网关 VM 后，它包括预先配置的处理器、内存和承载 VM 基础设施的 IDE 磁盘。该 IDE 磁盘在 vSphere 客户端的虚拟机属性窗口中显示为“IDE (0:0) Hard disk1”，如以下示例屏幕截图所示。不过，您可以直接访问或使用该磁盘。网关用该磁盘来存储系统数据。



## Note

配置磁盘时，强烈建议您不要将本地磁盘配置为使用相同底层物理存储资源（磁盘）的上传缓冲区和缓存存储空间。底层的物理存储资源在 VMware 中表示为数据存储器。部署网关 VM 时，您选择用来存储 VM 文件的数据存储器。预配置本地磁盘时（例如用作缓存存储空间或上传缓冲区），您可以选择将虚拟磁盘存储在与 VM 相同的数据存储器中，也可以选择存储在不同的存储器中。如果您有一个以上的数据存储器，强烈建议为缓存存储空间选择一个数据存储器，为上传缓冲区选择另一个数据存储器。仅由一个底层物理磁盘支持，或者仅由一个 RAID 1 等低性能 RAID 配置支持的数据存储器可能在用来支持缓存存储空间和上传缓冲区的某些情况下导致性能不佳。

## 为上传缓冲区添加本地磁盘 ( 网关 VTL )

上传缓冲区 – 上传缓冲区提供了一个暂存区域，在网关将数据上传到 Amazon S3 之前，可将写入到磁带的数据保存到该区域。

下图以更大幅的 AWS Storage Gateway 架构为背景，突出显示了上传缓冲区（请参见 [AWS Storage Gateway 的运行原理 \( 架构 \) \( p. 3 \)](#)）。



## 配置上传缓冲区的大小 ( 网关 VTL )

您可以利用上传缓冲区公式来确定上传缓冲区的大小。我们强烈建议您至少分配 150 GiB 的上传缓冲区。因此，如果公式得出小于 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 2 TiB 的上传缓冲区。

若要估算上传缓冲区的容量，您可以确定所需的传入和传出数据速率，并将它们插入以下公式中。

- 数据传入速率—该速率指应用程序吞吐量，亦即您的场内应用程序在某段时间内将数据写入到网关的速率。
- 数据传出速率—该速率指网络吞吐量，亦即您的网关将数据上传到 AWS 时可达到的速率。该速率取决于您的网络速度以及您是否启用了带宽限制。该速率应该针对压缩率进行调整。将数据上传到 AWS 时，网关在可能的情况下实施数据压缩。例如，如果您的应用程序为纯文本，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，因而需要更多的网关上传缓冲区。

如果传入速率大于传出速率，或者公式返回的值小于 150 GiB，强烈建议您至少分配 150 GiB 的上传缓冲区空间。

$$\left( \begin{array}{l} \text{Application} \\ \text{Throughput} \\ \text{(MB/s)} \end{array} - \begin{array}{l} \text{Network} \\ \text{Throughput} \\ \text{to AWS (MB/s)} \end{array} \right) \times \begin{array}{l} \text{Compression} \\ \text{Factor} \end{array} \times \begin{array}{l} \text{Duration} \\ \text{of writes} \\ \text{(s)} \end{array} = \begin{array}{l} \text{Upload} \\ \text{Buffer} \\ \text{(MB)} \end{array}$$

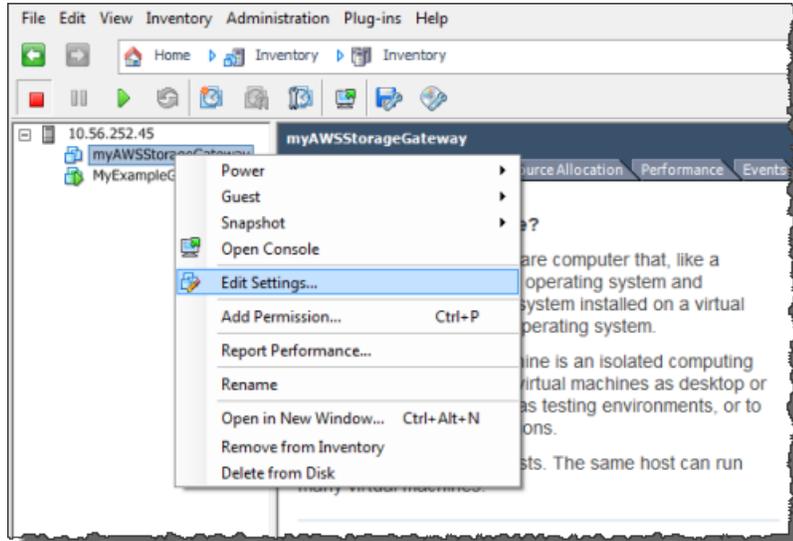
例如，假定您的商业应用程序每天 12 个小时以每秒 40 兆字节的速率向网关写入文本数据并且您的网络吞吐量为每秒 12 兆字节。假定文本数据的压缩系数为 2:1，您就需要为上传缓冲区分配约 690 GB 的空间。

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

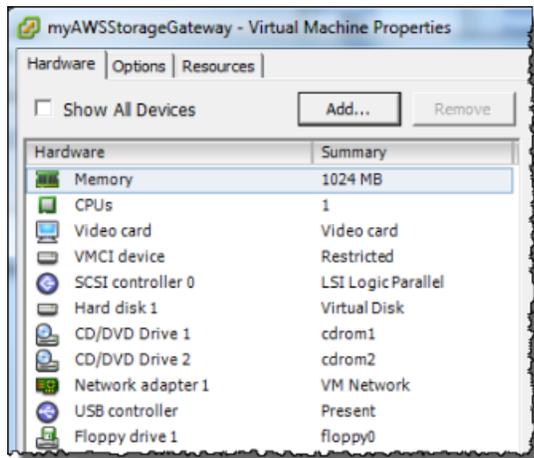
请注意您可以将此近似值用来初步确定您希望分配给网关作为上传缓冲区空间的磁盘大小。使用 AWS Storage Gateway 控制台按需添加更多的上传缓冲区空间。另外，您可以使用 Amazon CloudWatch 运行指标来监控上传缓冲区使用率并确定额外的存储空间需求。有关指标及设置警报的更多信息，请参见 [监控上传缓冲区 \(p. 365\)](#)。

如需向 VM 分配新的虚拟磁盘用作上传缓冲区

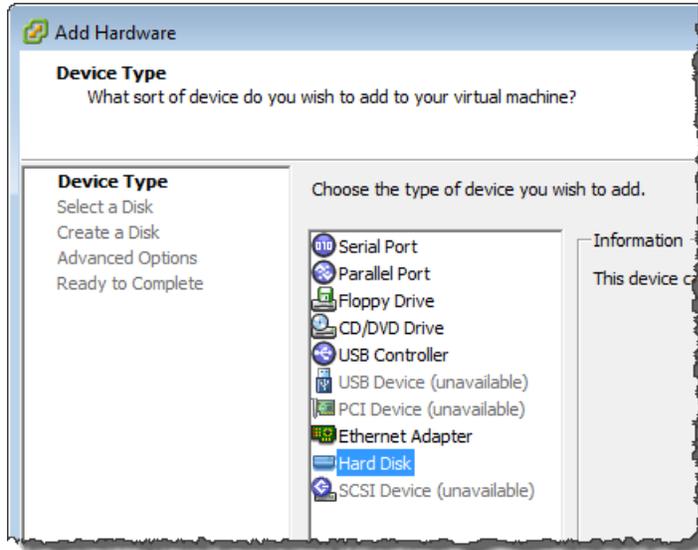
1. Start the VMware vSphere client and connect to your host.
2. In the client, right-click the name of your gateway VM and click Edit Settings...



3. In the Hardware tab of the Virtual Machine Properties dialog box, click Add... to add a device.

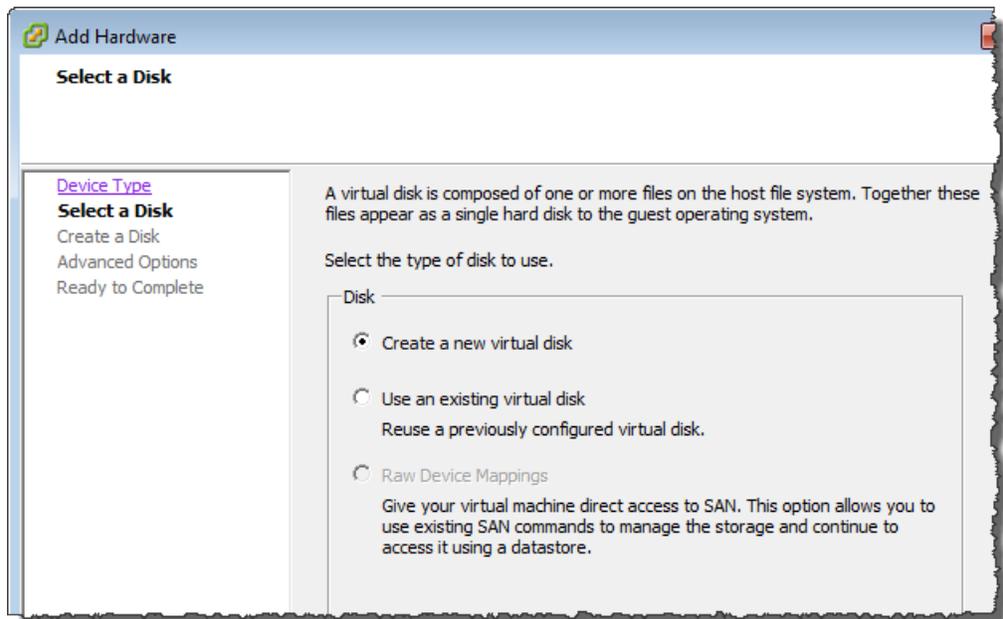


4. Follow the Add Hardware wizard to add a disk:
  - a. In the Device Type pane, click Hard Disk to add a disk, and click Next.



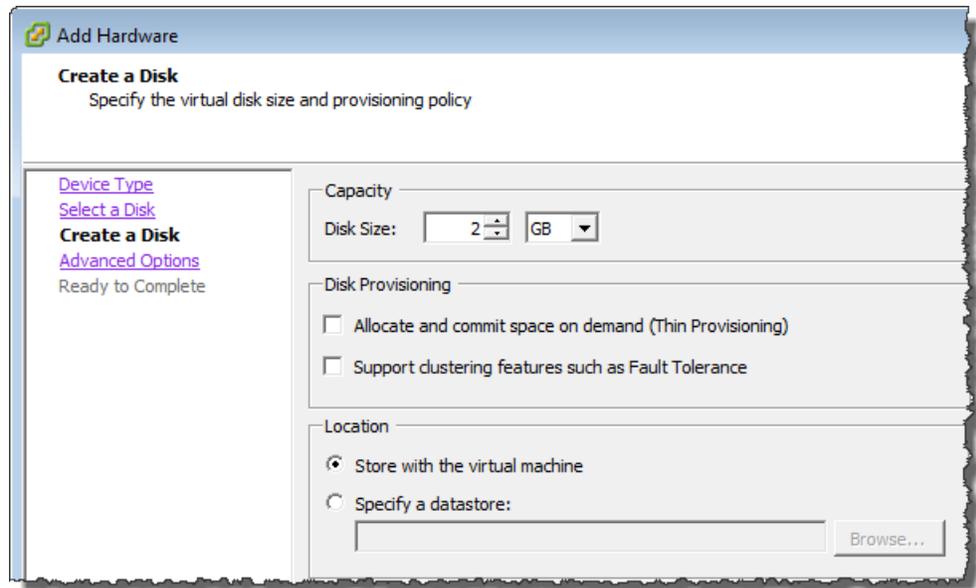
- b. In the Select a Disk pane, select Create a new virtual disk and click Next.

If the disk you are adding for your application storage contains pre-existing data that you want to preserve, select the Use an existing virtual disk option.



- c. In the Create a Disk pane, specify the size of the disk and click Next.

When you use thick provisioning, the disk storage is allocated immediately, resulting in better performance. In contrast, thin provisioning allocates storage on demand. On-demand allocation can affect the normal function of AWS Storage Gateway. Therefore, for AWS Storage Gateway to function properly, the virtual machine disks must be stored in thick-provisioned format.



- d. In the Advanced Options pane, click Next.
  - e. In the Ready to Complete pane, click Finish.
5. If you have not already done so, you must configure your VM to use a paravirtualized controller for your local disks.



#### Important

Configuring your VM for paravirtualization is a critical task. If you do not configure paravirtualization, the AWS Storage Gateway console will not be able to communicate with the disks that you have allocated. For steps on configuring paravirtualization, see [将 AWS Storage Gateway VM 配置为使用半虚拟化 \(p. 108\)](#).

### 为缓存存储添加本地磁盘 ( 网关 VTL )

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。

下图以更大幅的 AWS Storage Gateway 架构为背景，突出显示了缓存存储空间 ( 请参见 [AWS Storage Gateway 的运行原理 \( 架构 \) \(p. 3\)](#) )。



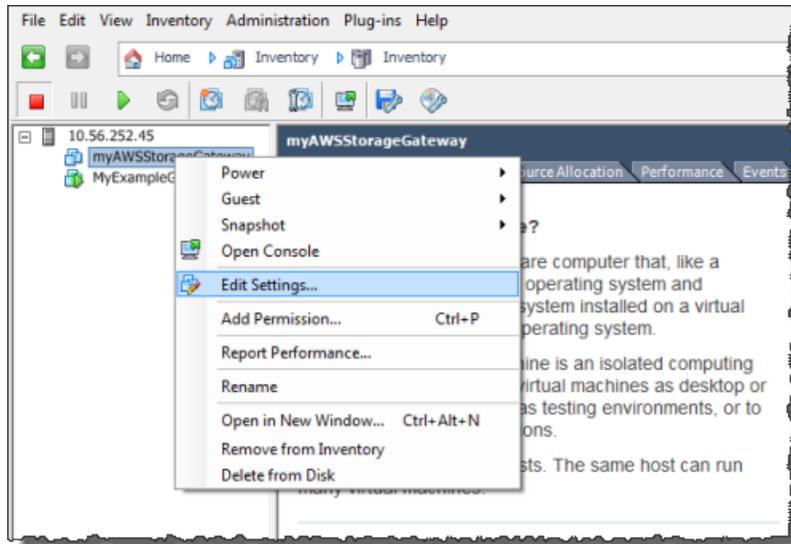
#### 配置缓存存储空间大小

网关使用缓存存储空间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 的数据的场内持久存储器。将缓存存储空间的大小配置为上传缓冲区大小的 1.1 倍。

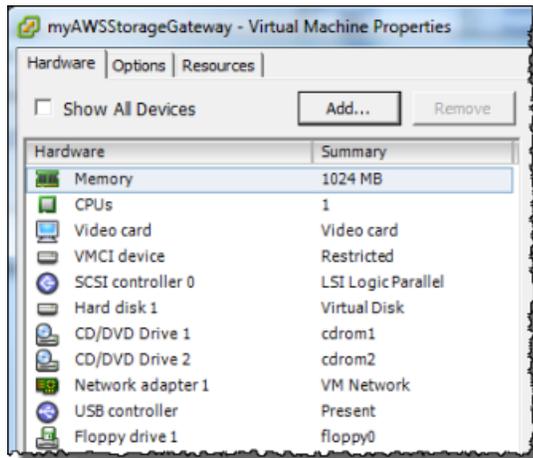
您可以将此近似值用来初步为缓存存储空间预配置磁盘。您然后可以使用 Amazon CloudWatch 运行指标来监控缓存存储空间使用率并使用控制台按需预配置更多的存储空间。有关使用指标和设置警报的过程，请参见 [监控缓存卷 \(p. 368\)](#)。

如需向磁盘分配新的虚拟磁盘以用作缓存存储空间

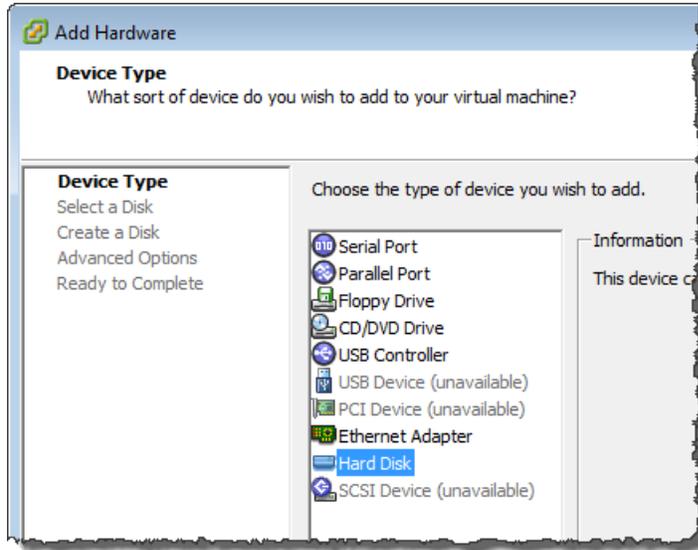
1. Start the VMware vSphere client and connect to your host.
2. In the client, right-click the name of your gateway VM and click Edit Settings....



3. In the Hardware tab of the Virtual Machine Properties dialog box, click Add... to add a device.

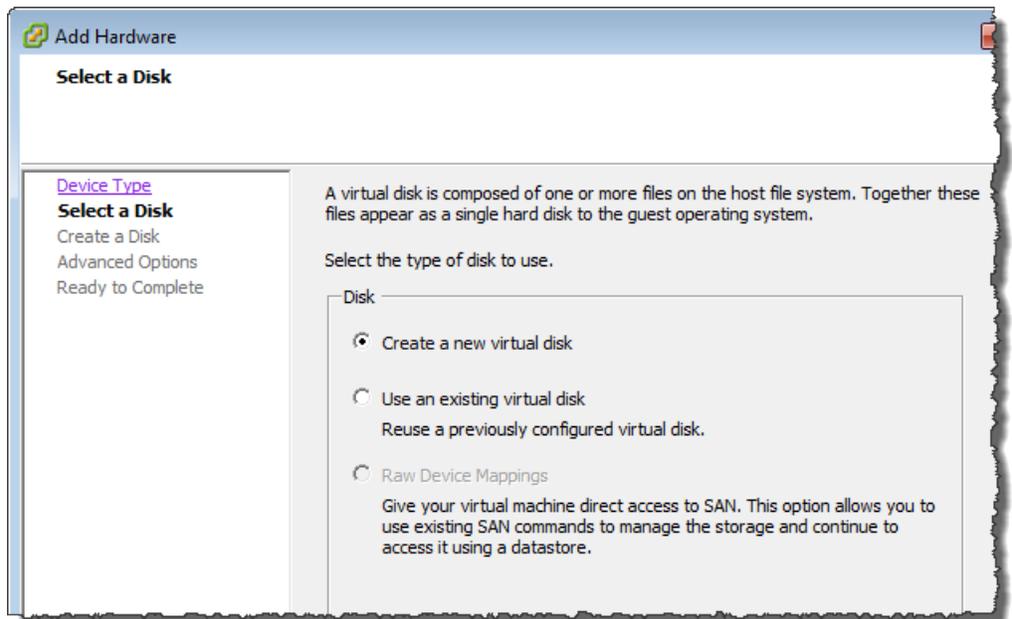


4. Follow the Add Hardware wizard to add a disk:
  - a. In the Device Type pane, click Hard Disk to add a disk, and click Next.



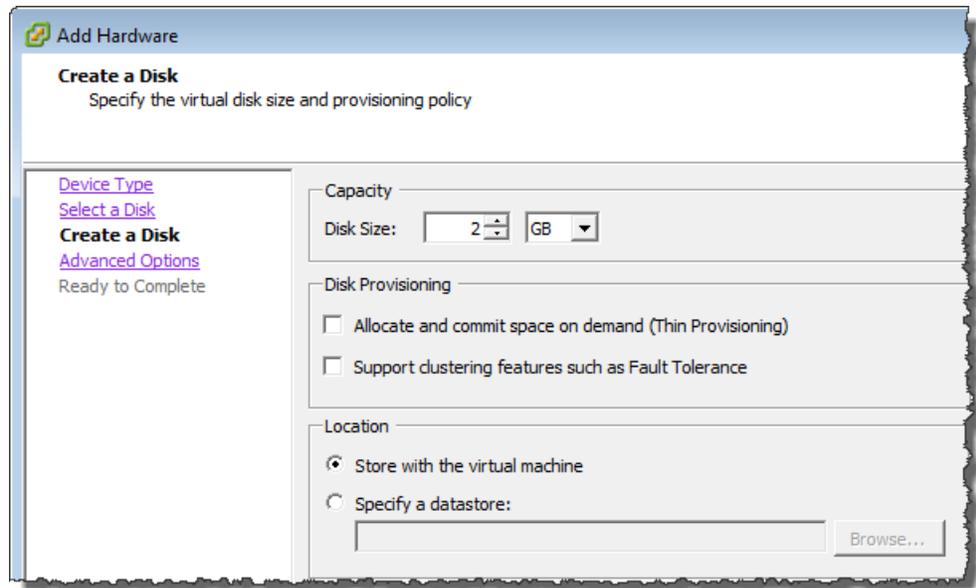
- b. In the Select a Disk pane, select Create a new virtual disk and click Next.

If the disk you are adding for your application storage contains pre-existing data that you want to preserve, select the Use an existing virtual disk option.



- c. In the Create a Disk pane, specify the size of the disk and click Next.

When you use thick provisioning, the disk storage is allocated immediately, resulting in better performance. In contrast, thin provisioning allocates storage on demand. On-demand allocation can affect the normal function of AWS Storage Gateway. Therefore, for AWS Storage Gateway to function properly, the virtual machine disks must be stored in thick-provisioned format.



- d. In the Advanced Options pane, click Next.
  - e. In the Ready to Complete pane, click Finish.
5. If you have not already done so, you must configure your VM to use a paravirtualized controller for your local disks.



#### Important

Configuring your VM for paravirtualization is a critical task. If you do not configure paravirtualization, the AWS Storage Gateway console will not be able to communicate with the disks that you have allocated. For steps on configuring paravirtualization, see [将 AWS Storage Gateway VM 配置为使用半虚拟化 \(p. 108\)](#).

### 在 VMware ESXi 主机上将 AWS Storage Gateway VM 配置为使用半虚拟化

为了让 AWS Storage Gateway 控制台正确识别磁盘，您必须将 VM 配置为使用本地磁盘的半虚拟化控制器。在实际工作中，您可在网关的初始安装期间设置超虚拟，也就是说，在部署 VM 和添加本地磁盘后但在打开 VM 前。要设置超虚拟，必须关闭 VM。



#### Note

如果您给 VM 至少预配置了一个 SCSI 磁盘，那么，只能设置 iSCSI 控制器的虚拟。有关更多信息，请参见 [在 VMware ESXi 主机上为 AWS Storage Gateway VTL VM 配置本地磁盘存储 \(p. 314\)](#)。

#### 如需将 VM 配置为使用半虚拟化的控制器

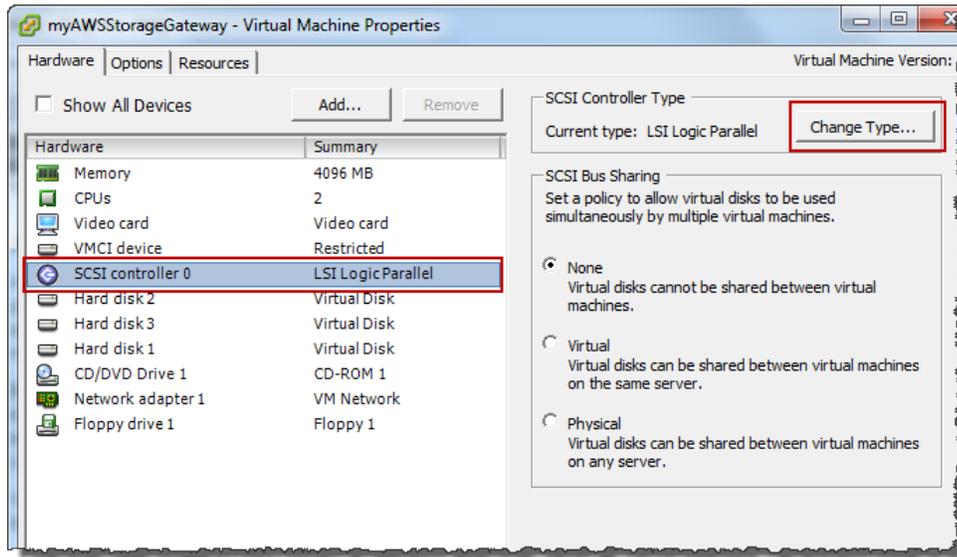
1. 在 VMware vSphere 客户端中，右键单击您的网关虚拟机的名称。

验证是否已关闭 VM。如果没有，请予以关闭。有关更多信息，请参见 [关停网关 \(p. 383\)](#)。在关闭 VM 前，请确保没有使用网关。

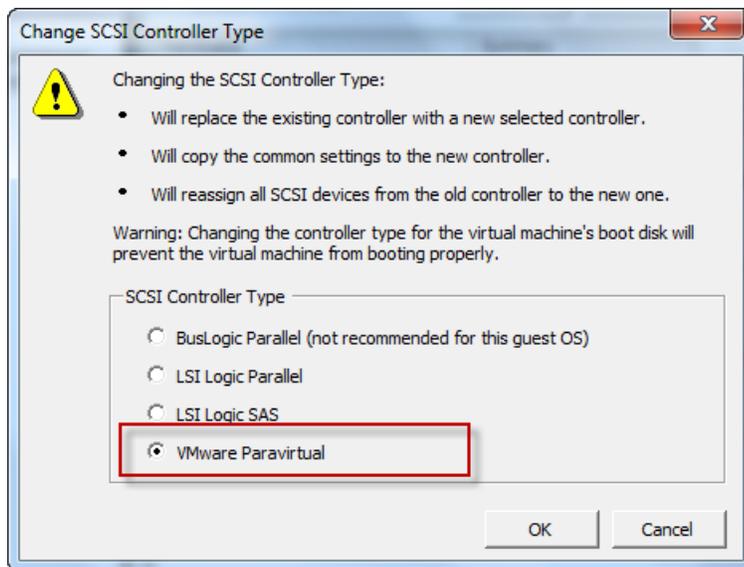
2. 选择编辑设置...

随后将打开虚拟机属性对话框。

3. 在硬件选项卡中，选择硬件列表中的 SCSI 控制器 0 设置，然后单击更改类型...



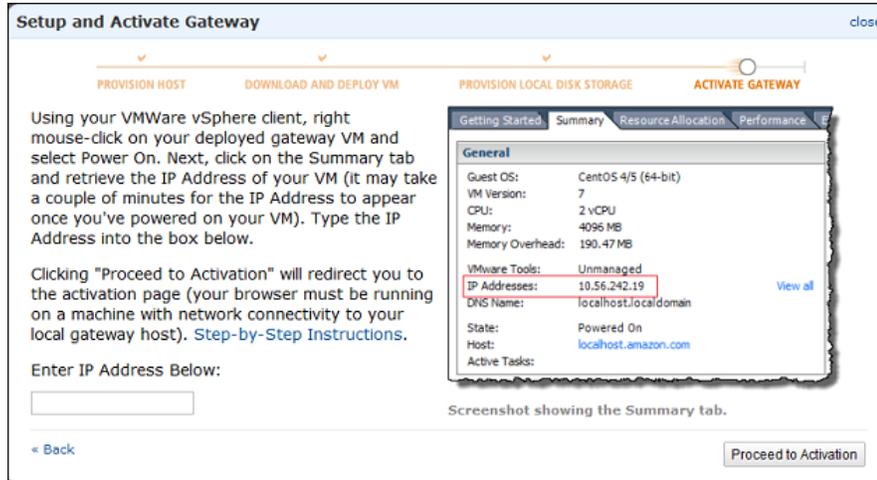
4. 选择 VMware ParaVirtual SCSI 控制器类型，然后单击确定。



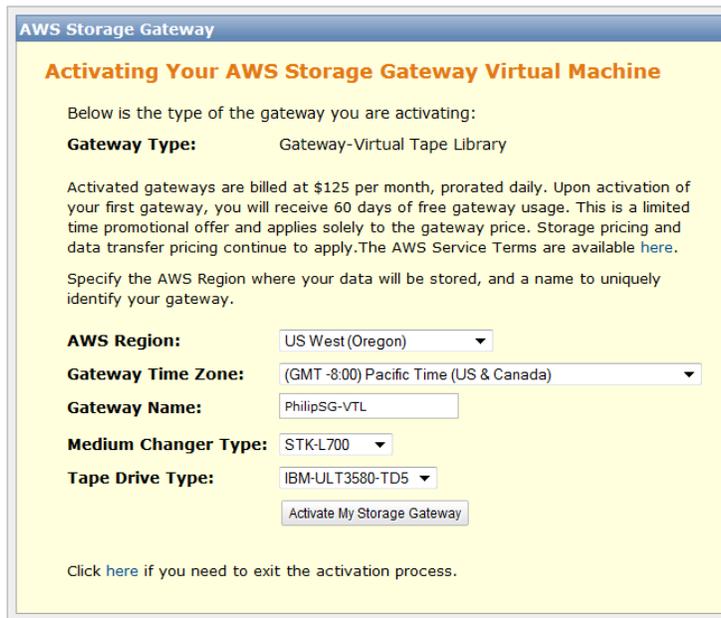
## 激活部署在 VMware ESXi 主机上的 AWS Storage Gateway-VTL

部署 AWS Storage Gateway 虚拟机 (VM) 后，必须使用 AWS Storage Gateway 控制台激活网关。如果按控制台步骤进行操作，则将看到以下激活屏幕。激活过程将您的网关与 AWS 账户关联。

激活后，您开始产生费用。有关定价的信息，请参阅 [AWS Storage Gateway](#)。



指定网关的 IP 地址后，将看到以下屏幕截图，您在其中提供所需信息。



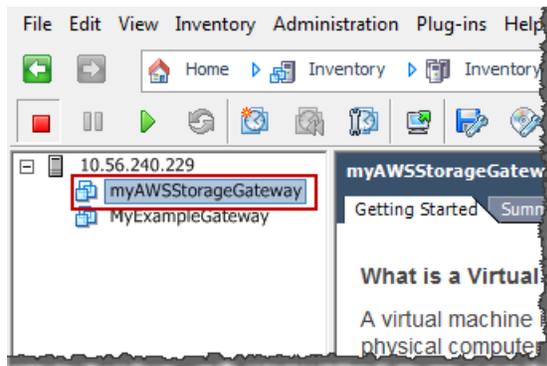
继续激活之前，请确认已完成以下步骤：

步骤	说明
将本地磁盘预配置到 VM	所配置的 VM 没有磁盘，因此，必须配置本地磁盘。为 AWS Storage Gateway-VTL 配置的本地磁盘用于缓存存储和上传缓冲区。有关更多信息，请参阅 <a href="#">预配置本地磁盘（网关缓存）</a> (p. 92)。
将 VM 配置为使用半虚拟化	将 VM 配置为使用半虚拟化是至关重要的任务。如果未配置半虚拟化，则 AWS Storage Gateway 控制台将无法与已分配的磁盘进行通信。有关更多信息，请参阅 <a href="#">将 AWS Storage Gateway VM 配置为使用半虚拟化</a> (p. 108)。

步骤	说明
将 VM 时间与主机时间同步	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。成功激活网关需要同步 VM 和主机时间。有关更多信息，请参阅 <a href="#">将 VM 时间与主机时间同步 (p. 266)</a> 。
确认将运行浏览器以激活网关的客户端可连接到网关 VM 的 IP 地址。	在网关激活期间，Web 浏览器连接到网关 VM 的 80 端口。如果激活失败，可能是因此连接失败。

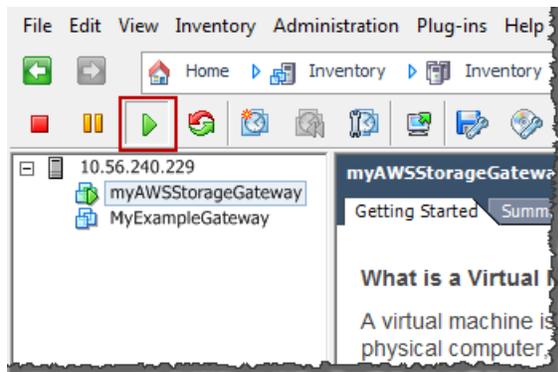
### 如需使用控制台激活网关

1. 启动 VMware vSphere 客户端，然后连接到虚拟机监控程序主机。
2. 如果 VM 尚未启动，请启动。
  - a. 在 vSphere 客户端中，选择网关 VM。



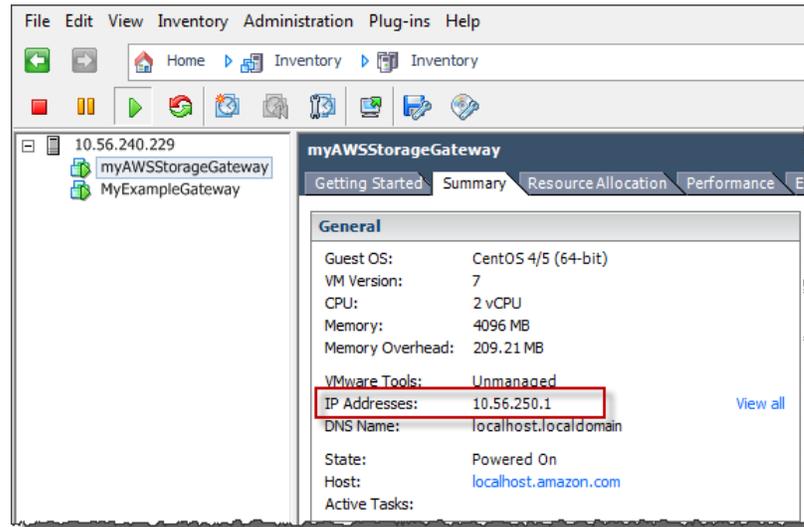
- b. 单击工具栏菜单上的开机图标。

您的网关 VM 图标现在包含一个绿色箭头图标，表示您已启动了 VM。



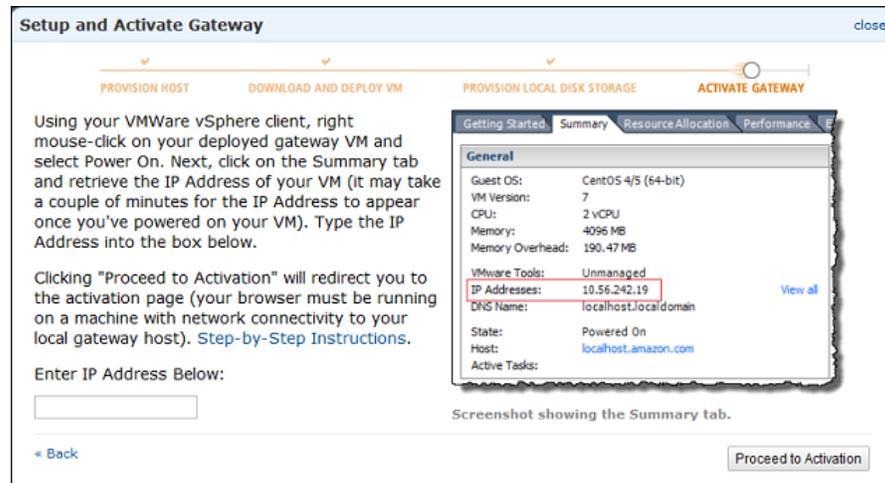
3. 激活网关。
  - a. 取得您的网关的 IP 地址。请注意，启动 VM 后，IP 地址可能需要一段时间才能显示。
    - i. 使用 vSphere 客户端登录您的主机。
    - ii. 选择部署的网关 VM。

- iii. 单击摘要选项卡以获得该 IP 地址。



- b. 将您的网关关联到 AWS 账户

- i. 返回控制台，如果尚未打开设置并激活网关向导，则请照做，继续进行激活网关步骤，输入 IP 地址，然后单击继续激活。您的浏览器必须运行在可通过网络连接本地网关主机的机器上。



**Note**

如果激活失败，请检查您输入的 IP 地址是否正确，然后重试激活。如果 IP 地址正确无误，则确认网关可访问 Internet，如有必要，则还要设置代理（请参阅[将 AWS Storage Gateway 的路由选为通过代理](#) (p. 222)）。

- ii. 在激活页面上，填写请求的信息以完成激活过程。

- AWS 地区决定 AWS 存储虚拟磁带的位置。您不能在网关激活后更改地区。



### Note

在以下地区支持 AWS Storage Gateway-VTL。

地区

Region name	Region string
US East (Northern Virginia)	us-east-1
US West (Northern California)	us-west-1
US West (Oregon)	us-west-2
EU (Ireland)	eu-west-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1

- 网关时区指定要用于网关的时区。它用于调度快照和更新。
- 网关名称在控制台中标识您的网关。您使用该名称在控制台中管理网关，可在激活后更改名称。该名称必须是您账户的唯一名称。
- 介质更换器类型指定此网关使用的介质更换器的类型。
- 磁带驱动器类型指定此网关使用的磁带驱动器的类型。

**AWS Storage Gateway**

### Activating Your AWS Storage Gateway Virtual Machine

Below is the type of the gateway you are activating:

**Gateway Type:** Gateway-Virtual Tape Library

Activated gateways are billed at \$125 per month, prorated daily. Upon activation of your first gateway, you will receive 60 days of free gateway usage. This is a limited time promotional offer and applies solely to the gateway price. Storage pricing and data transfer pricing continue to apply. The AWS Service Terms are available [here](#).

Specify the AWS Region where your data will be stored, and a name to uniquely identify your gateway.

**AWS Region:** US West (Oregon) ▼

**Gateway Time Zone:** (GMT -8:00) Pacific Time (US & Canada) ▼

**Gateway Name:** PhilipSG-VTL

**Medium Changer Type:** STK-L700 ▼

**Tape Drive Type:** IBM-ULT3580-TD5 ▼

[Click here](#) if you need to exit the activation process.

- iii. 单击激活我的 Storage Gateway。

成功激活后，AWS 存储网关-VTL 控制台即显示激活的 gateway 和一个链接，供您创建虚拟磁带。



单击创建磁带后，将有向导指导您如何为网关配置本地存储、创建可选警报和创建虚拟磁带。



#### Note

首次为网关 VTL 创建磁带时，必须先为网关配置本地存储，然后才能创建虚拟磁带。

#### 相关部分

- [AWS Storage Gateway 的 API 参考 \(p. 418\)](#)

## 在 Microsoft Hyper-V 主机上部署和激活场内 AWS Storage Gateway

本部分介绍如何在 Microsoft Hyper-V 主机上部署并激活网关虚拟机 (VM)。激活过程会将网关与您的 AWS 账户关联。



#### Note

此处描述的任务假定您已经预配置了 Microsoft Hyper-V 主机。如果您尚未完成此操作，请参见此练习中的 [配置 Hyper-V 主机以部署 AWS Storage Gateway VM \(p. 278\)](#)。

## 下载 AWS Storage Gateway 虚拟机 (VM) 并将其部署在 Hyper-V 主机上

使用 AWS Management Console 中的设置并激活网关向导配置主机后，下一步为下载并部署 VM。在此步骤中，选择要使用的虚拟化平台，下载 VM，然后部署它。



本入门练习说明如何下载和部署网关。有关说明，请参阅 [下载 AWS Storage Gateway VM 并将其部署在您的主机上 \(p. 278\)](#)。

## 在 Hyper-V 主机上为 AWS Storage Gateway VTL VM 配置本地磁盘存储

网关 VM 可将您本地分配的本地磁盘用于以下目的：

- 上传缓冲区 – 上传缓冲区提供了一个暂存区域，在网关将数据上传到 Amazon S3 之前，可将写入到磁带的的数据保存到该区域。
- 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。当应用程序对虚拟磁带执行 I/O 时，网关会将数据保存到缓存存储空间中以实现低延迟访问。当您的应用程序请求磁带中的数据时，网关在从 AWS 下载数据前会先检查缓存存储空间中的数据。

#### Topics

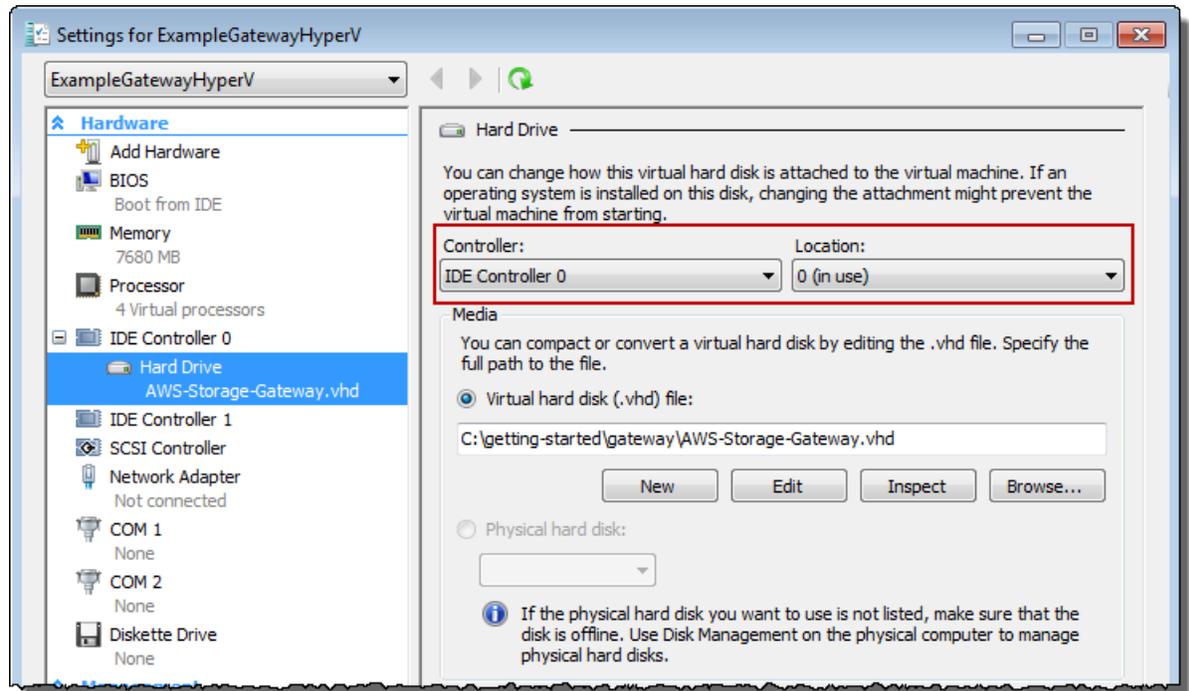
- [为上传缓冲区添加本地磁盘 \(网关 VTL\) \(p. 329\)](#)

- 为缓存存储添加本地磁盘 ( 网关 VTL ) (p. 332)



#### Note

部署 ( 导入 ) 网关 VM 后，它包括预先配置的处理器、内存和承载 VM 基础设施的 IDE 磁盘。在 Microsoft Hyper-V Manager 的设置窗口中，此 IDE 磁盘会显示为 AWS-Storage-Gateway.vhd 和控制器 IDE (0:0)，如下例屏幕截图所示。不过，您可以直接访问或使用该磁盘。网关用该磁盘来存储系统数据。



#### Note

配置磁盘时，强烈建议您不要将本地磁盘配置为使用相同底层物理存储资源 ( 磁盘 ) 的上传缓冲区和缓存存储空间。部署网关 VM 时，您选择用来存储 VM 文件的磁盘位置。预配置本地磁盘时 ( 例如用作缓存存储空间或上传缓冲区 )，您可以选择将虚拟磁盘存储在与 VM 相同的磁盘位置中，也可以选择存储在不同的位置中。如果您有一个以上的磁盘，强烈建议为缓存存储空间选择一个磁盘位置，为上传缓冲区选择另一个磁盘位置。仅由一个底层物理磁盘支持，或者仅由一个 RAID 1 等低性能 RAID 配置支持的一个磁盘位置可能在用来支持缓存存储空间和上传缓冲区的某些情况下导致性能不佳。

### 为上传缓冲区添加本地磁盘 ( 网关 VTL )

上传缓冲区 – 上传缓冲区提供了一个暂存区域，在网关将数据上传到 Amazon S3 之前，可将写入到磁带的的数据保存到该区域。

下图以更大幅的 AWS Storage Gateway 架构为背景，突出显示了上传缓冲区。( 请参见 [AWS Storage Gateway 的运行原理 \( 架构 \)](#) (p. 3) )。



## 配置上传缓冲区

您可以利用上传缓冲区公式来确定上传缓冲区的大小。我们强烈建议您至少分配 150 GiB 的上传缓冲区。因此，如果公式得出小于 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 2 TiB 的上传缓冲区。

若要估算上传缓冲区的容量，您可以确定所需的传入和传出数据速率，并将它们插入以下公式中。

- 数据传入速率—该速率指应用程序吞吐量，亦即您的场内应用程序在某段时间内将数据写入到网关的速率。
- 数据传出速率—该速率指网络吞吐量，亦即您的网关将数据上传到 AWS 时可达到的速率。该速率取决于您的网络速度以及您是否启用了带宽限制。该速率应该针对压缩率进行调整。将数据上传到 AWS 时，网关在可能的情况下实施数据压缩。例如，如果您的应用程序为纯文本，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，因而需要更多的网关上传缓冲区。

如果传入速率大于传出速率，或者公式返回的值小于 150 GiB，强烈建议您至少分配 150 GiB 的上传缓冲区空间。

$$\left( \begin{array}{l} \text{Application} \\ \text{Throughput} \\ \text{(MB/s)} \end{array} - \begin{array}{l} \text{Network} \\ \text{Throughput} \\ \text{to AWS (MB/s)} \end{array} \right) \times \begin{array}{l} \text{Compression} \\ \text{Factor} \end{array} \times \begin{array}{l} \text{Duration} \\ \text{of writes} \\ \text{(s)} \end{array} = \begin{array}{l} \text{Upload} \\ \text{Buffer} \\ \text{(MB)} \end{array}$$

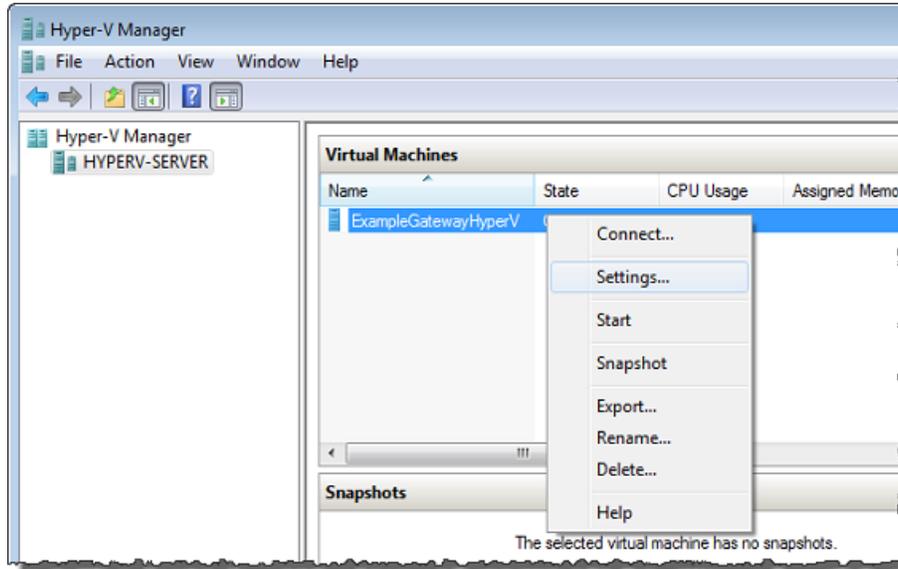
例如，假定您的商业应用程序每天 12 个小时以每秒 40 兆字节的速率向网关写入文本数据并且您的网络吞吐量为每秒 12 兆字节。假定文本数据的压缩系数为 2:1，您就需要为上传缓冲区分配约 690 GB。

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

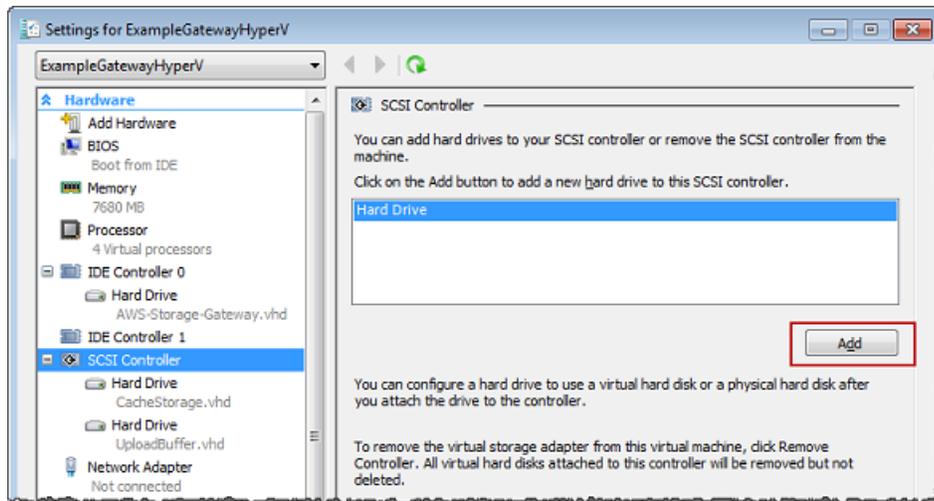
请注意您可以将此近似值用来初步确定您希望分配给网关作为上传缓冲区空间的磁盘大小。使用 AWS Storage Gateway 控制台按需添加更多的上传缓冲区空间。另外，您可以使用 Amazon CloudWatch 运行指标来监控上传缓冲区使用率并确定额外的存储空间需求。有关指标及设置警报的更多信息，请参见 [监控上传缓冲区 \(p. 365\)](#)。

如需向 VM 分配新的虚拟磁盘用作上传缓冲区

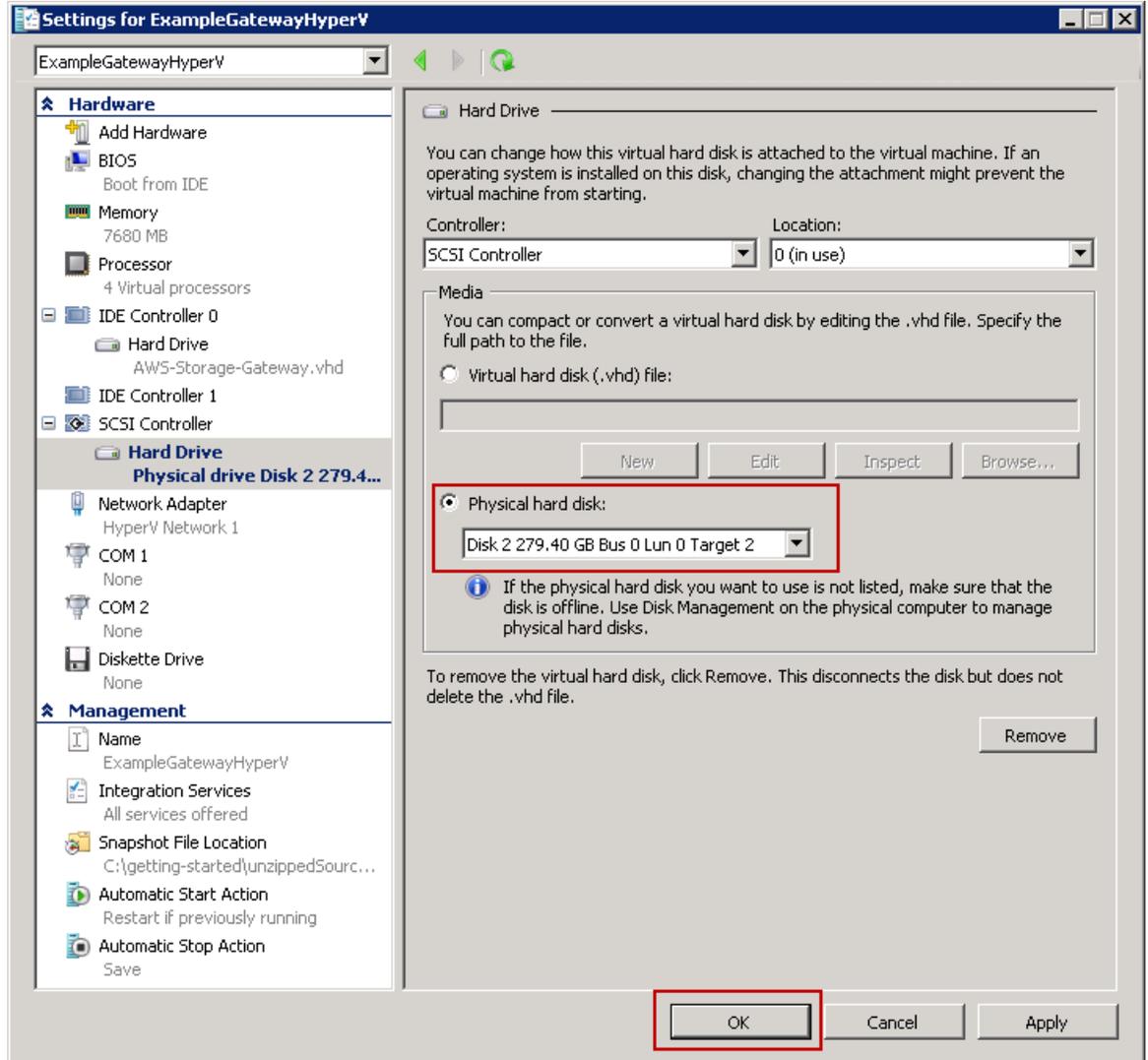
1. Start the Microsoft Hyper-V Manager and connect to your host.
2. In the client, right-click the name of your gateway VM and click Settings....



3. In the Hardware list in the left pane, click SCSI Controller.
4. In the SCSI Controller pane, Click Add.



5. In the Hard Drive pane, in the Media section click Physical hard disk and select a disk from the box.



6. Click OK.

### 为缓存存储添加本地磁盘（网关 VTL）

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。

下图以更大幅的 AWS Storage Gateway 架构为背景，突出显示了缓存存储空间（请参见 [AWS Storage Gateway 的运行原理（架构）](#)（p. 3））。



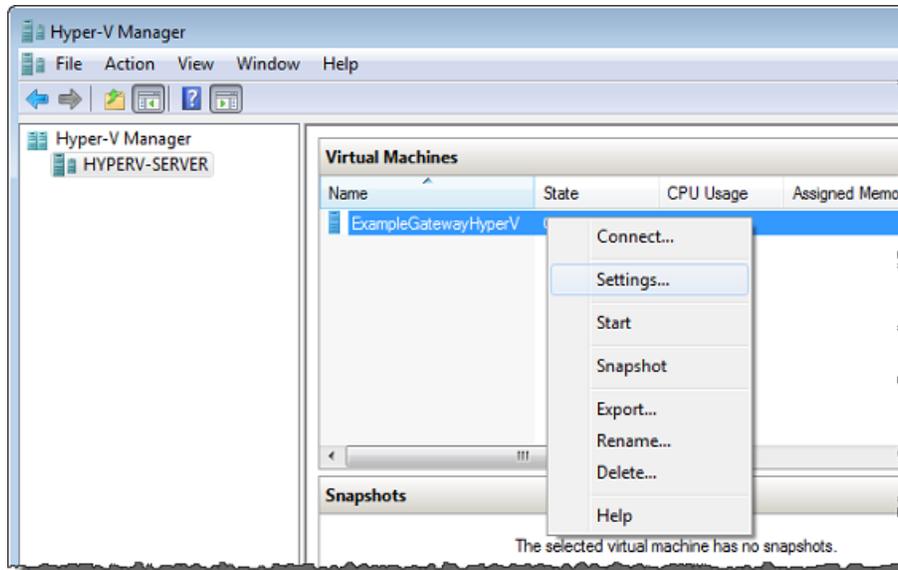
### 配置缓存存储空间的大小（网关 VTL）

网关使用缓存存储空间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 的数据的场内持久存储器。将缓存存储空间的大小配置为上传缓冲区大小的 1.1 倍。

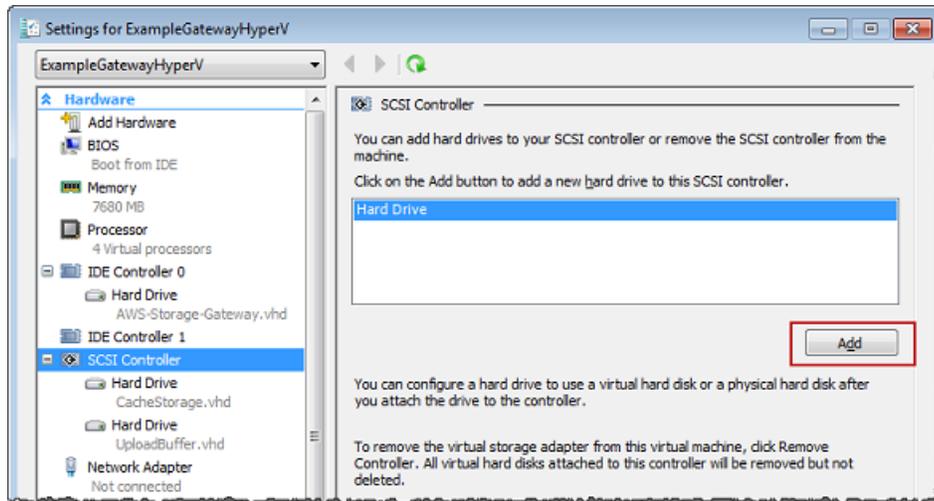
您可以将此近似值用来初步为缓存存储空间预配置磁盘。您然后可以使用 Amazon CloudWatch 运行指标来监控缓存存储空间使用率并使用控制台按需预配置更多的存储空间。有关使用指标和设置警报的过程，请参见 [监控缓存卷](#)（p. 368）。

如需向磁盘分配新的虚拟磁盘以用作缓存存储空间

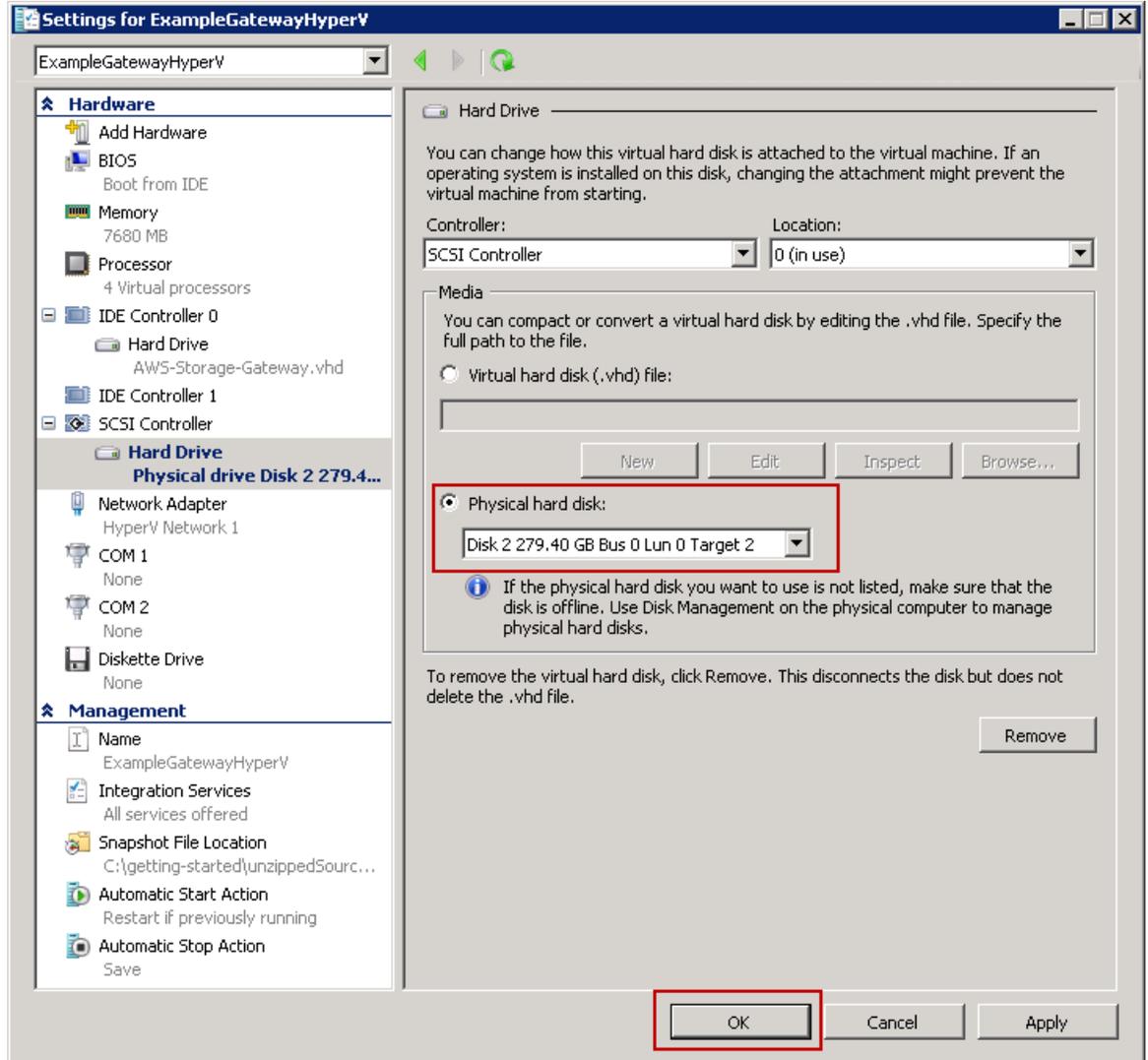
1. Start the Microsoft Hyper-V Manager and connect to your host.
2. In the client, right-click the name of your gateway VM and click Settings....



3. In the Hardware list in the left pane, click SCSI Controller.
4. In the SCSI Controller pane, Click Add.



5. In the Hard Drive pane, in the Media section click Physical hard disk and select a disk from the box.

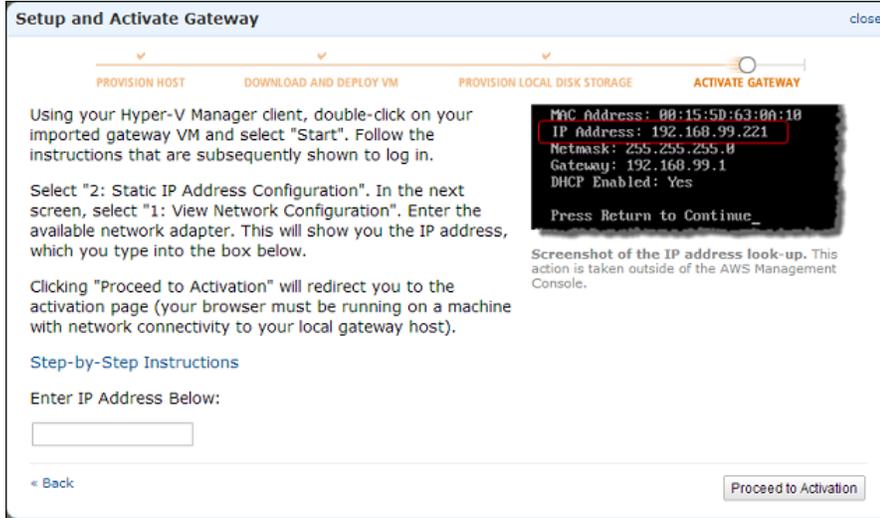


6. Click OK.

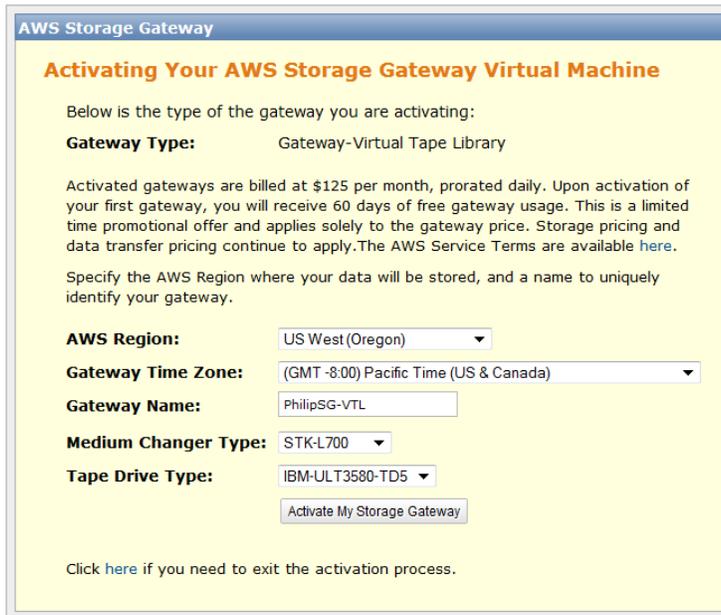
## 激活部署在 Hyper-V 主机上的 AWS Storage Gateway-VTL

部署 AWS Storage Gateway 虚拟机 (VM) 后，必须使用 AWS Storage Gateway 控制台激活网关。如果按控制台步骤进行操作，则将看到以下激活屏幕。激活过程将您的网关与 AWS 账户关联。

激活后，您开始产生费用。有关定价的信息，请参阅 [AWS Storage Gateway](#)。



指定网关的 IP 地址后，将看到以下屏幕截图，您在其中提供所需信息。



继续激活之前，请确认已完成以下步骤：

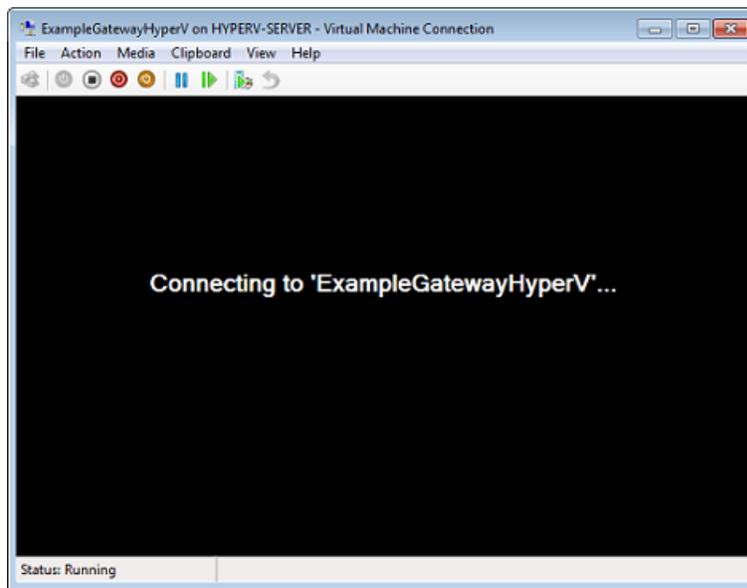
步骤	说明
将本地磁盘预配置到 VM	所配置的 VM 没有磁盘，因此，必须配置本地磁盘。为 AWS Storage Gateway-VTL 配置的本地磁盘用于缓存存储和上传缓冲区。有关更多信息，请参阅 <a href="#">预配置本地磁盘（网关缓存）</a> (p. 92)。
将 VM 配置为使用半虚拟化	将 VM 配置为使用半虚拟化是至关重要的任务。如果未配置半虚拟化，则 AWS Storage Gateway 控制台将无法与已分配的磁盘进行通信。有关更多信息，请参阅 <a href="#">将 AWS Storage Gateway VM 配置为使用半虚拟化</a> (p. 108)。

步骤	说明
将 VM 时间与主机时间同步	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。成功激活网关需要同步 VM 和主机时间。有关更多信息，请参阅 <a href="#">将 VM 时间与主机时间同步 (p. 266)</a> 。
确认将运行浏览器以激活网关的客户端可连接到网关 VM 的 IP 地址。	在网关激活期间，Web 浏览器连接到网关 VM 的 80 端口。如果激活失败，可能是因此连接失败。

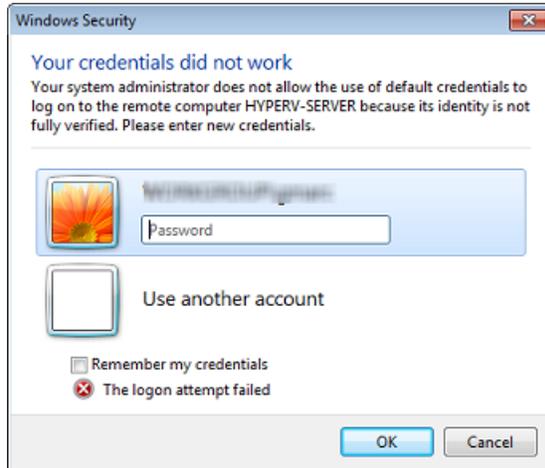
#### 如需激活网关

1. 如果尚未连接 Microsoft Hyper-V Manager，请启动它并连接到虚拟机监控程序。
2. 启动 VM。
  - a. 在虚拟机列表窗格中，选择您部署的虚拟机 ExampleGatewayHyperV-VTL。
  - b. 在您的网关的操作窗格中，单击启动。

随后将显示虚拟机连接窗口。如果未显示此窗口，则在您的网关的操作窗格中单击连接。

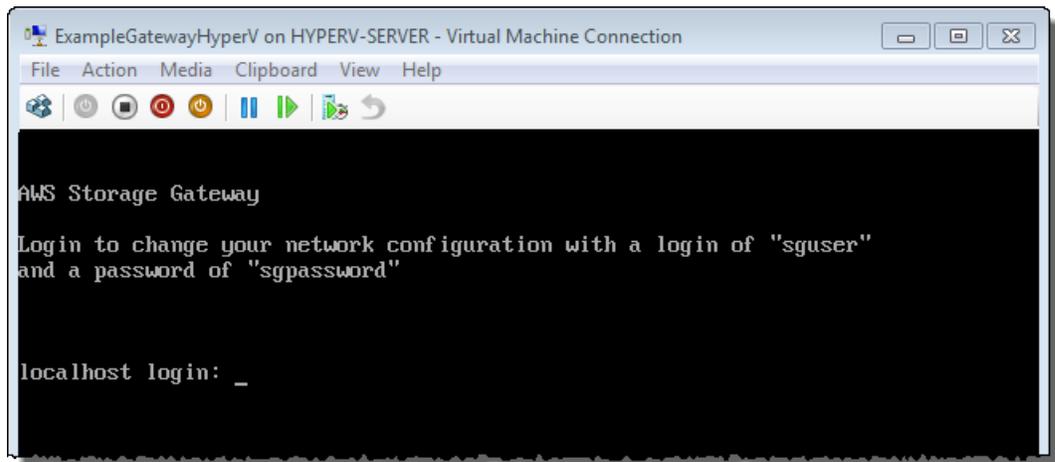


- c. 如果显示身份验证窗口，请输入管理程序管理员向您提供的用户名称和密码。



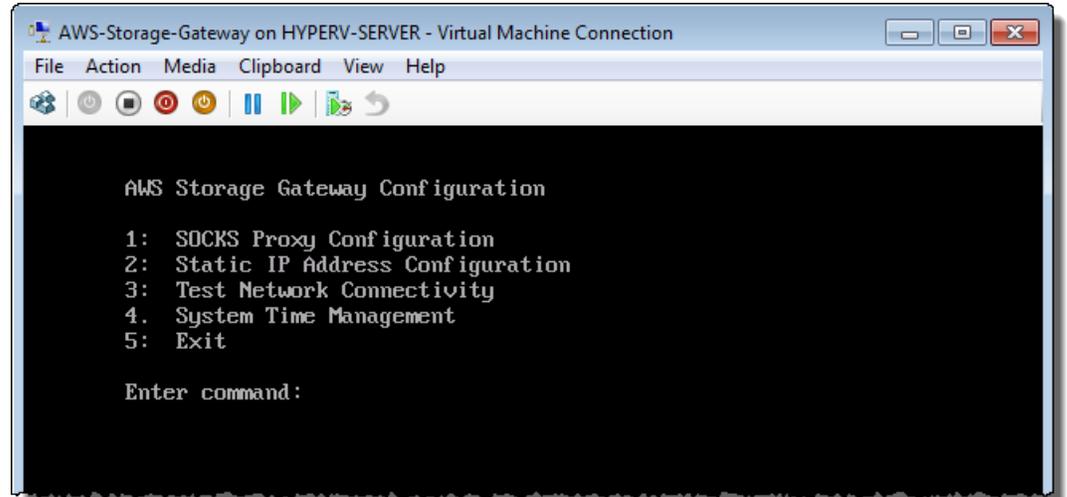
- d. 在过几分钟时间后，虚拟机就会准备就绪，供您登录了。

下面的示例介绍了您在 VM 准备就绪时会看到的登录提示。

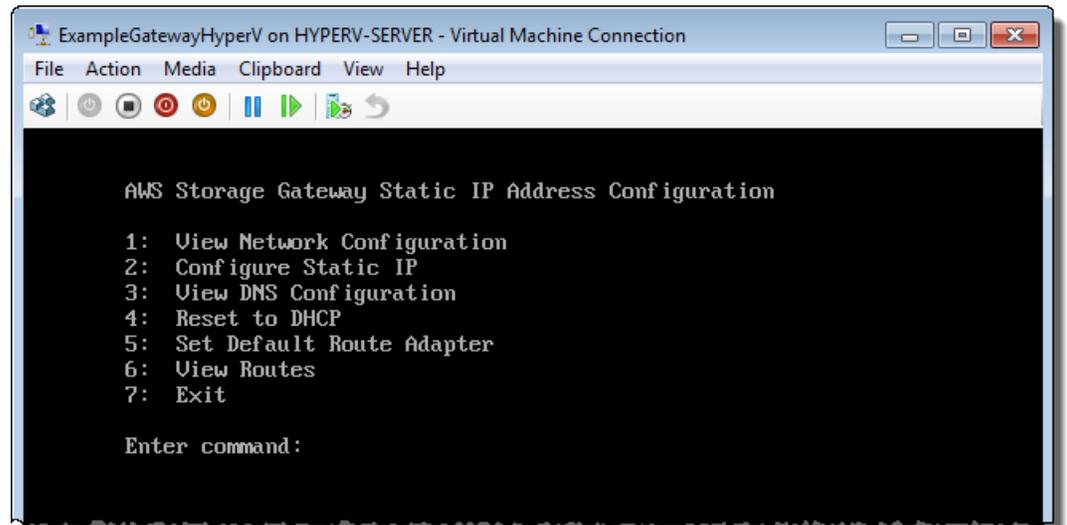


### 3. 激活网关。

- a. 取得您的网关的 IP 地址。
- 在 Microsoft Hyper-V 管理器中，选择所部署的网关 VM。
  - 在虚拟机列表窗格中，选择虚拟机 ExampleGatewayHyperV。
  - 在操作窗格中，单击连接...。
- 随后将显示虚拟机连接窗口。
- 在出现登录提示时，输入用户名 `sguser` 和密码 `sgpassword`。
  - 在 AWS Storage Gateway 配置菜单中，选择选项 2 静态 IP 地址配置。

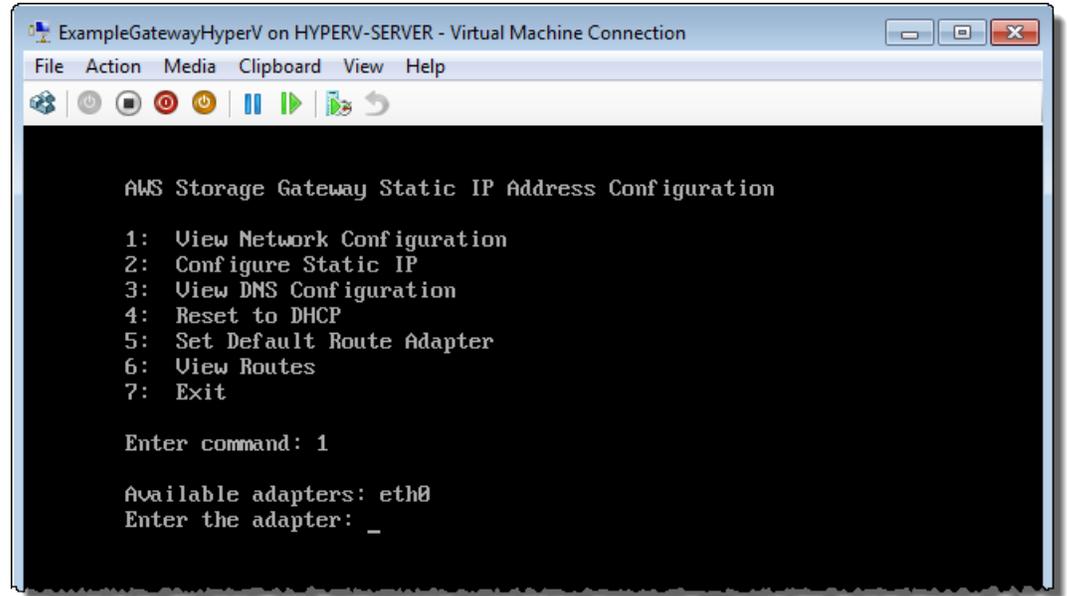


- vi. 在 AWS Storage Gateway 静态 IP 地址配置菜单中，选择选项 1 查看网络配置。



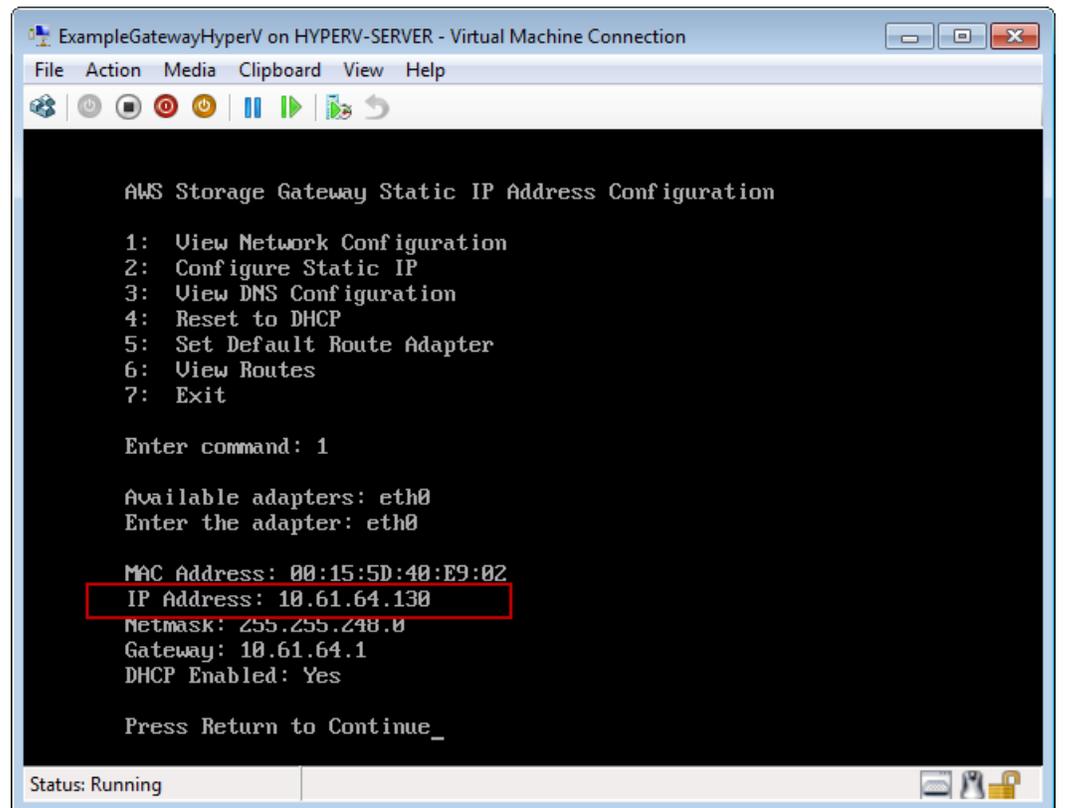
- vii. 键入适配器的标识符。

在大多数设置中，eth0 将是适配器标识符。



viii. 从适配器信息中获取 IP 地址。

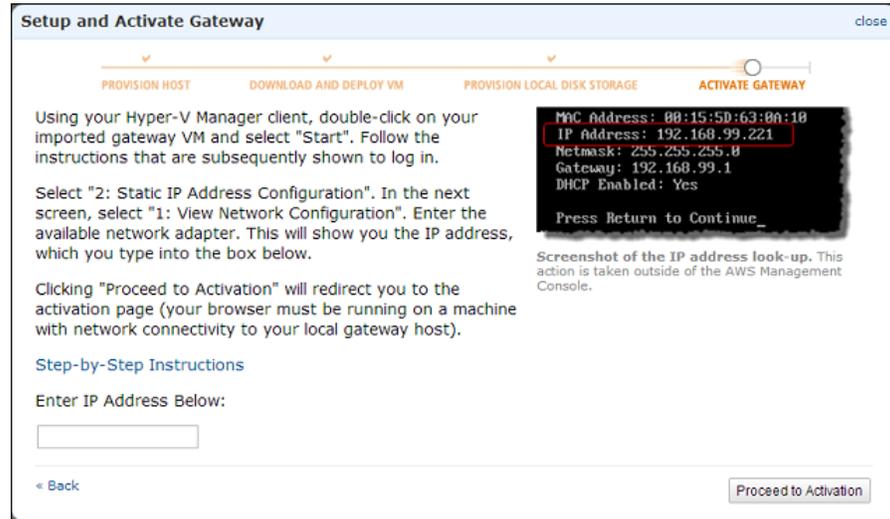
在下例中，IP 地址为 10.61.64.130。您的网关的 IP 地址将会不同。



ix. 按 Return，然后按提示退出配置菜单。

b. 将您的网关关联到 AWS 账户。

- i. 在 AWS Storage Gateway 控制台的设置并激活网关向导中，导航到以下激活网关页。
  - A. 如果尚未启动该向导，则单击设置并激活新网关。
  - B. 在向导的每个步骤中单击继续，直到抵达激活网关页。
- ii. 输入您的网关的 IP 地址，然后单击继续激活。记下该 IP 地址，因为以后在访问设备时需要该地址。



#### Note

激活期间，您的浏览器连接到网关。如果激活失败，则确认输入的 IP 地址正确无误。如果该 IP 地址正确，则确认已将网络配置为允许浏览器访问网关 VM。

- iii. 在激活页上，输入所要求的信息以完成激活过程。
  - AWS 地区决定 AWS 存储虚拟磁带的位置。您不可以在网关激活后更改地区。  
可在以下地区激活 AWS Storage Gateway：

Region name	Region string
US East (Northern Virginia)	us-east-1
US West (Northern California)	us-west-1
US West (Oregon)	us-west-2
EU (Ireland)	eu-west-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1

- 网关时区指定要使用的时区。
- 网关名称在控制台中标识您的网关。您使用该名称在控制台中管理网关，可在激活后更改名称。
- 介质更换器类型指定用于网关 VTL 中的机械手的类型。

- 磁带驱动器类型指定网关 VTL 中使用的磁带驱动器的类型。



- iv. 单击激活我的 Storage Gateway。

成功激活后，AWS Storage Gateway 控制台在导航窗格的网关部分下显示一个链接，指向已激活的网关。单击刚刚部署的网关。

随后将显示创建磁带按钮。



单击创建磁带后，将有向导指导您如何为网关配置本地存储、创建可选警报和创建虚拟磁带。



#### Note

首次为网关 VTL 创建磁带时，必须先为网关配置本地存储，然后才能创建虚拟磁带。

## 在 Amazon EC2 上部署并激活网关 VTL

可在云中以 EC2 实例的形式运行网关 VTL。AWS Storage Gateway 提供一个亚马逊系统映像 (AMI)，其中包含网关 VM 映像。可在 AWS Marketplace ([AWS Storage Gateway](#)) 中获得 AMI，供您从 Amazon EC2 控制台中或从 AWS Storage Gateway 控制台中启动实例。



#### Important

无论采用何种方式访问 AMI，我们都强烈建议您选择 AWS Marketplace 中的与 EC2 控制台一同启动选项用于启动您的实例。下方的过程中记载了执行此操作的步骤。如果决定使用单键启动功能启动该实例，则需要在启动该实例后，作为一个单独的步骤，将 Amazon EBS 卷添加到您的实例（请参阅[从网关 VTL 实例中添加和删除 Amazon EBS 卷 \(p. 408\)](#)）。

本节介绍如何启动 AWS Storage Gateway AMI 和激活网关 VTL。

#### 步骤 1：选择 AWS Storage Gateway AMI

1. 在 AWS Storage Gateway 控制台中，单击在 Amazon EC2 上部署新网关。



2. 在在 Amazon EC2 上设置并激活网关向导的第 1 步中，单击启动网关 AMI。



此操作将在浏览器的新选项卡中打开 AWS Marketplace 页。

3. 在 AMI 的 AWS Marketplace 页上，单击继续。

## AWS Storage Gateway 用户指南 在 Amazon EC2 上部署并激活网关

**AWS Storage Gateway**  
Sold by: [Amazon Web Services](#)

The AWS Storage Gateway is a service connecting a software appliance with cloud-based storage to provide seamless and secure integration between an organization's EC2 instances and AWS's storage infrastructure. The service enables you to securely store data to the AWS cloud for scalable and cost-effective storage. The AWS Storage Gateway supports industry-standard storage protocols that work with your existing applications. It provides low-latency performance by maintaining frequently accessed data locally while securely storing all of your data encrypted in the Amazon Simple Storage Service... [Read more](#)

**Customer Rating** [Be the first to review this product](#)

**Latest Version** 1.0

**Base Operating System** Linux/Unix, Amazon Linux 2012.09

**Delivery Method** 64-bit Amazon Machine Image (AMI) ([Learn more](#))

**Support** [See details below](#)

**AWS Services Required** Amazon EC2, Amazon EBS

**Highlights**

- Secure: The AWS Storage Gateway securely transfers your data to AWS over SSL and stores data encrypted at rest in Amazon S3 using Advanced Encryption Standard (AES) 256, a secure symmetric-key encryption standard using 256-bit encryption keys.
- Durably backed by Amazon S3: The AWS Storage Gateway durably stores your application data by uploading it to Amazon S3. Amazon S3 stores data in multiple facilities and on multiple devices within each facility.

**Pricing Details**  
**Hourly Fees**  
Total hourly fees will vary by instance type and EC2 region.

For region: **US East (Virginia)**

EC2 Instance Type	Software	EC2	Total*
Standard XL (m1.xlarge)	\$0.00/hr	\$0.52/hr	\$0.52/hr
High-Memory XL (m2.xlarge)	\$0.00/hr	\$0.45/hr	\$0.45/hr
High-Memory 2XL (m2.2xlarge)	\$0.00/hr	\$0.90/hr	\$0.90/hr
High-Memory 4XL (m2.4xlarge)	\$0.00/hr	\$1.80/hr	\$1.80/hr
High-CPU XL (c1.xlarge)	\$0.00/hr	\$0.66/hr	\$0.66/hr

\*EBS fees and data transfer fees not included. Assumes On-Demand EC2 pricing; prices for Reserved and Spot Instances will be lower. [See details](#)

[Learn about instance types](#)

4. 在 AMI 的在 EC2 上启动:页上, 选择与 EC2 控制台一同启动选项卡。

**Launch on EC2:**  
AWS Storage Gateway

**1-Click Launch**  
Review, modify, and launch

**Launch with EC2 Console**  
Info for EC2 Console or API Launches

Click "Accept Terms & Launch with 1-Click" to launch this software with the settings below

Once you accept the terms, you will have access to launch any version of this software in any supported region. For future launches, you can return to this page or launch directly from the EC2 console.

5. 如果是首次使用 AWS Storage Gateway AMI, 则单击接受条款; 否则, 跳至下一步。

将浏览器页面保持为打开状态。片刻时间内, 确认电子邮件会发送到您登录 AWS Marketplace 的账户所用的电子邮箱地址。

**Launch on EC2:**  
AWS Storage Gateway

**1-Click Launch**  
Review, modify, and launch

**Launch with EC2 Console**  
Info for EC2 Console or API Launches

**Accept Terms** Once subscribed you will be able to launch via EC2 Console or APIs

Click "Accept Terms" to gain access to this software

Once you accept these terms, you will have access to this software in any supported region. You can then launch the AMIs listed below directly from the EC2 console, EC2 APIs, or with other AWS management tools.

You will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's [End User License Agreement \(EULA\)](#) and your use of AWS services is subject to the [AWS Customer Agreement](#).

Select a Version

6. 在地区列表中, 通过单击“地区”旁的与 EC2 控制台一同启动链接, 选择要启动实例的地区。仅以下这些地区提供网关 VTL AMI。

Region name	Region string
US East (Northern Virginia)	us-east-1
US West (Northern California)	us-west-1
US West (Oregon)	us-west-2
EU (Ireland)	eu-west-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1

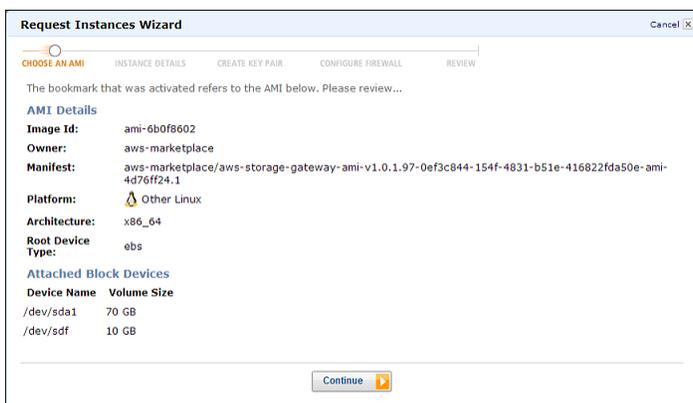
Region	ID	
US East (Virginia)	ami-200c6949	<a href="#">Launch with EC2 Console</a>
US West (Oregon)	ami-4a7aee7a	<a href="#">Launch with EC2 Console</a>
US West (Northern California)	ami-ee96bbab	<a href="#">Launch with EC2 Console</a>
EU West (Ireland)	ami-6804111c	<a href="#">Launch with EC2 Console</a>
Asia Pacific (Singapore)	ami-60b0fc32	<a href="#">Launch with EC2 Console</a>
Asia Pacific (Sydney)	ami-aad84890	<a href="#">Launch with EC2 Console</a>
Asia Pacific (Tokyo)	ami-9867e499	<a href="#">Launch with EC2 Console</a>
South America (Sao Paulo)	ami-87974d9a	<a href="#">Launch with EC2 Console</a>

现在，将进入 Amazon EC2 控制台以进行部署 AMI 的下一步。

## 步骤 2：选择实例类型

您必须指定至少一个 Standard XL (m1.xlarge) 实例类型，或者该实例不会启动。有关详细信息，请在 AWS Marketplace 中转到 [AWS Storage Gateway](#)。

1. 在选择实例类型页上，单击所有实例类型，然后选择实例类型 m1.xlarge 或更大的实例。



2. 完成操作后，单击下一步：在页面底部配置实例详细信息。

## 步骤 3：配置实例详细信息

1. 在配置实例详细信息页上，对于实例有若干配置选项，包括要从 AMI 启动多少个实例、要在 EC2-Classic 中还是在 VPC 中启动实例。如果创建网关作测试用途，则可保留默认设置，然后转到下一步。



### Note

如果您的 AWS 账户是默认 VPC 账户，则网络下拉列表中将为默认 VPC 子网设置，因此，您的网关将启动至默认 VPC 中。这种情况下，将无法启动至 EC2 Classic 中。如果您具有 EC2 Classic 账户，则可为您的账户创建 VPC，然后将实例启动至该 VPC 中。有关如何创建 VPC 的信息，请转到 *Amazon Virtual Private Cloud Getting Started Guide* 中的 [Amazon VPC 入门](#)。



2. 完成操作后，单击下一步：添加存储。

#### 步骤 4：添加存储

必须附加其他 EBS 卷用作缓存存储和上传缓冲区。有关更多信息，请参阅 [网关 - 虚拟磁带库 \(网关 VTL\) 架构 \(p. 5\)](#)。有关调整这两个存储类型大小的详细信息，请参阅 [配置上传缓冲区的大小 \(网关 VTL\) \(p. 316\)](#) 和 [配置缓存存储空间大小 \(p. 319\)](#)。

1. 添加两个 EBS 存储卷。

如果创建此设置作为示例设置，则可添加两个存储卷：一个 10 GB 用于上传缓冲区，一个 10 GB 用于缓存存储。



#### Important

请勿删除任何现有 EBS 卷。



2. 单击添加新卷以添加 EBS 卷。
3. 完成操作后，单击下一步：标签实例。

#### 步骤 5：标签实例

1. 在标签实例页上，定义一个标签，其名称相对于实例要比较易记。例如，Name=MyGatewayVTLonEC2。然后，在 Amazon EC2 控制台中所有出现 EC2 实例的地方显示此标签。



2. 完成操作后，单击下一步：配置安全组。

#### 步骤 6：配置安全组

安全组必须至少允许端口 (80) 进行激活。以允许连接到网关的 iSCSI 存储目标。在启动您的实例之前，您可能要检查现有安全组，或为您的网关实例新建安全组。有关安全组要求的详细信息，请参阅 [为 Amazon EC2 网关 VTL 实例配置安全组 \(p. 410\)](#)。

我们建议网关的安全组仅允许在端口 3260 上通过发往特定主机 (iSCSI 发起程序) 或发往发起程序所属安全组的流量。

- 在配置安全组页上，添加以下规则。如果创建网关进行测试，则可新建一个安全组，分配组名称，然后添加这些规则。



#### Caution

如果在源中指定 (0.0.0.0/0)，则您允许所有 IP 地址使用 SSH 访问您的实例。在测试环境下短时间内，这种情况尚可接受，但它对于生产环境并不安全。在生产中，请仅授权特定 IP 地址或地址范围访问您的实例。

#### 步骤 7：查看和启动

1. 在检查并启动页上，单击启动。

2. 在选择现有密钥对或新建密钥对窗口的下拉列表中选择相应的选项。如果新建密钥对，则先向该密钥对给出一个名称并下载该密钥对，然后再单击启动实例。



3. 在启动状态中，记下实例 ID，然后单击查看实例以打开 Amazon EC2 控制台。



4. 在 Amazon EC2 控制台中，选择该实例，然后记下公共 DNS 值。通过这个 DNS，可推断出下一步激活网关时将需要的 IP 地址。例如，如果公共 DNS 值为 `ec2-11-22-33-44.compute-1.amazonaws.com`，则 `11.22.33.44` 为 IP 地址。



### 步骤 8：激活网关

1. 现在，需要返回 AWS Storage Gateway 控制台，在在 Amazon EC2 上设置并激活网关向导中提供该 IP 地址，选择网关磁带库，然后单击继续激活。



#### Note

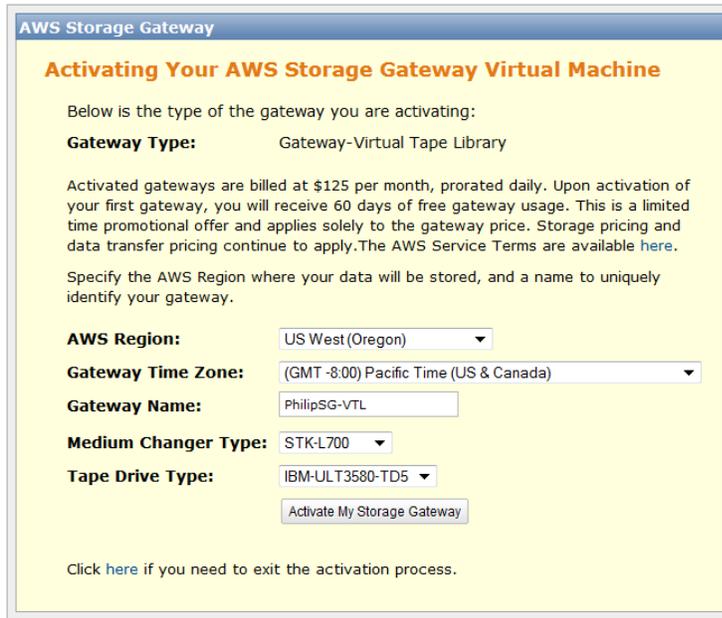
不支持通过公共 Internet 访问 Amazon EC2 Storage Gateway。无法使用 Amazon EC2 实例的弹性 IP 地址作为目标地址。



2. 在激活页上，提供所需的信息，然后单击激活我的 Storage Gateway。

注意，所选择的 AWS 地区是虚拟磁带架的所在地—即网关将磁带数据存储在所选择的 AWS 地区。

Region name	Region string
US East (Northern Virginia)	<code>us-east-1</code>
US West (Northern California)	<code>us-west-1</code>
US West (Oregon)	<code>us-west-2</code>
EU (Ireland)	<code>eu-west-1</code>
Asia Pacific (Sydney)	<code>ap-southeast-2</code>
Asia Pacific (Tokyo)	<code>ap-northeast-1</code>



**AWS Storage Gateway**

### Activating Your AWS Storage Gateway Virtual Machine

Below is the type of the gateway you are activating:

**Gateway Type:** Gateway-Virtual Tape Library

Activated gateways are billed at \$125 per month, prorated daily. Upon activation of your first gateway, you will receive 60 days of free gateway usage. This is a limited time promotional offer and applies solely to the gateway price. Storage pricing and data transfer pricing continue to apply. The AWS Service Terms are available [here](#).

Specify the AWS Region where your data will be stored, and a name to uniquely identify your gateway.

**AWS Region:** US West (Oregon)

**Gateway Time Zone:** (GMT -8:00) Pacific Time (US & Canada)

**Gateway Name:** PhilipSG-VTL

**Medium Changer Type:** STK-L700

**Tape Drive Type:** IBM-ULT3580-TD5

[Activate My Storage Gateway](#)

[Click here](#) if you need to exit the activation process.

- 成功激活网关后，将在 AWS Storage Gateway 控制台中的 VTL 网关部分下显示该网关。



- 单击您刚刚添加的网关。随后将显示创建磁带按钮。



本入门部分说明如何完成其余练习。您将执行以下任务：

- 配置本地磁盘和警报
- 创建虚拟磁带
- 将 VTL 设备连接到 Windows 计算机
- 测试网关 VTL 设置

单击创建磁带后，将有向导指导您如何为网关配置本地存储、创建可选警报和创建虚拟磁带。



#### Note

首次为网关 VTL 创建磁带时，必须先为网关配置本地存储，然后才能创建虚拟磁带。

下一步

[步骤 2：配置本地存储和警报 \(p. 300\)](#)

## 配置上传缓冲区和缓存存储空间

作为设置网关 VTL 的一部分，您将为您网关分配存储空间（磁盘）。在决定磁盘大小时，使用建议的大小配置公式。有关大小配置的更多信息，请参见以下主题

- [配置上传缓冲区的大小（网关 VTL）\(p. 316\)](#)

- [配置缓存存储空间大小 \(p. 319\)](#)

有关本地磁盘在实现网关完全运行方面起到的作用的信息，请参见 [网关 - 虚拟磁带库 \(网关 VTL\) 架构 \(p. 5\)](#)。



本部分介绍如何将网关配置为将这些磁盘用作上传缓冲区和缓存存储空间。

将本地磁盘配置为上传缓冲区和缓存存储空间

1. 在 AWS Storage Gateway 控制台中，单击网关选项卡。
2. 单击配置本地存储选项卡。



3. 在配置已激活的网关向导中，验证是否有可配置为上传缓冲区和缓存存储空间的本地磁盘。

向导显示您的本地 VM 上的可用磁盘列表。如果没有本地磁盘可用，您必须先向网关 VM 添加磁盘。有关更多信息，请参见 [在 VMware ESXi 主机上为 AWS Storage Gateway VTL VM 配置本地磁盘存储 \(p. 314\)](#)。



4. 选择您希望作为上传缓冲区和缓存存储空间分配给网关的磁盘旁边的下拉列表。



#### Important

配置这些磁盘后，磁盘上任何先前的数据都会丢失。

5. 单击保存。

## 使用 AWS Storage Gateway 控制台创建虚拟磁带

### Topics

激活网关 VTL 后，您创建用于备份数据和将数据存档的虚拟磁带。每个网关最多可创建 1500 个磁带。但是，每次最多只能创建 10 个虚拟磁带。有关虚拟磁带限制的详细信息，请参阅 [附录 F：AWS Storage Gateway 限制 \(p. 457\)](#)。由条码唯一地标识虚拟磁带。可向条码添加前缀。该前缀为可选，但是，可将其用于虚拟磁带。该前缀必须为大写字母 (A-Z)，并且其长度必须为 1 到 4 个字符。



#### Note

如果使用 Storage Gateway API 创建虚拟磁带，则其大小必须为整 GB (1024\*1024\*1024 字节)。

有关详细信息，请参阅 [AWS Storage Gateway 的 API 参考 \(p. 418\)](#) 中的 `CreateTapes`



#### Note

只需为写入磁带的的数据量而非整个磁带容量付费。

以下屏幕截图显示创建磁带页。



### 创建虚拟磁带

1. 在 AWS Storage Gateway 控制台上，选择要为其创建虚拟磁带的网关 VTL。
2. 单击 VTL 盒式磁带选项卡，然后单击创建磁带以打开为您的 Storage Gateway 创建虚拟磁带对话框。
3. 填写表单中的值。
4. 单击创建磁带。

已创建的虚拟磁带显示在 AWS Storage Gateway 控制台中。控制台中还显示虚拟磁带的条码、容量和状态。在创建虚拟磁带时，虚拟磁带的状态最初设置为正在创建。创建磁带后，其状态变为可用。有关状态的详细信息，请参阅 ( [在虚拟磁带库 \(VTL\) 中管理磁带 \(p. 371\)](#) )。

## 连接到网关上的 VTL 设备

### Topics

- [从 Windows 客户端连接到您的 VTL 设备 \(p. 349\)](#)
- [从 Red Hat 客户端连接到 VTL 设备 \(p. 351\)](#)
- [为 VTL 设备配置 CHAP 身份验证 \(p. 353\)](#)

网关 VTL 公开若干磁带驱动器和一个介质更换器 ( 统称 VTL 设备 ) 作为 Internet 小型计算机系统接口 (iSCSI) 目标。有关更多信息，请参阅 [要求 \(p. 7\)](#)。



### Note

您向每个 iSCSI 目标仅连接一个应用程序。

下图在 AWS Storage Gateway 架构的大图中突出显示了 iSCSI 目标 ( 请参阅 [AWS Storage Gateway 的运行原理 \( 架构 \) \(p. 3\)](#) )。



iSCSI 标准是一个基于 Internet 协议 (IP) 的存储联网标准，用于在基于 IP 的存储设备和客户端之间发起和管理连接。

下表列出用于描述连接和相关组件的一些 iSCSI 术语。

术语	说明
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。启动程序可在软件或硬件中实施。AWS Storage Gateway 仅支持软件发起程序。
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。以 iSCSI 目标的形式公开每个 VTL 设备。仅对每个 iSCSI 目标连接一个 iSCSI 启动程序。
Microsoft iSCSI 启动程序	Windows 计算机上的软件程序，可让您使用主计算机的以太网网络适配卡将客户端计算机 ( 例如运行您希望将其数据写入网关的应用程序的计算机 ) 来连接到外部基于 iSCSI 数组 ( 即网关 )。Microsoft iSCSI 启动程序在软件中实施。Microsoft iSCSI 启动程序已安装在 Windows Server 2008 R2、Windows 7、Windows Server 2008 和 Windows Vista 上。在上述操作系统中，您不需要安装该启动程序。

术语	说明
Red Hat iSCSI 启动程序	包含 iscsi /启动程序/实用程序的资源包管理器 (RPM) 包为您提供实施在适用于 Red Hat 的软件中的 iSCSI 启动程序。该包包含用于 iSCSI 协议的服务器守护进程。

您可以针对两种客户端类型有选择地配置质询握手身份验证协议 ( CHAP )。

## 从 Windows 客户端连接到您的 VTL 设备

使用 Windows 客户端时，您使用 Microsoft iSCSI 发起程序连接到您的 VTL 设备。这是一个两步过程：

- 将网关 VTL 设备连接到 Windows 客户端。
- 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。

本入门示例设置提供对两步的说明。其中使用 Symantec NetBackup 备份应用程序。有关详细信息，请参阅[步骤 4：将网关 VTL 设备连接到 Windows 客户端 \(p. 302\)](#)和[配置 NetBackup 存储设备 \(p. 305\)](#)。

### 建议进行的 Windows iSCSI 设置

设置您的启动程序后，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。通过提高下列步骤中所示的超时值，您可以改善应用程序处理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性能。



#### Note

修改注册表前，您应该制作一份备份副本。有关在使用注册表时需要遵循的制作备份副本及其他最佳操作的信息，请参阅 *Windows Server TechCenter* 中的[注册表最佳操作](#)。

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. 导航到设备类别全局唯一标识符 (GUID) 密钥，其中包含 iSCSI 控制器设置。



#### Warning

确保处于 CurrentControlSet 子项内，而非 ControlSet001 或 ControlSet002 等其他控制集内。

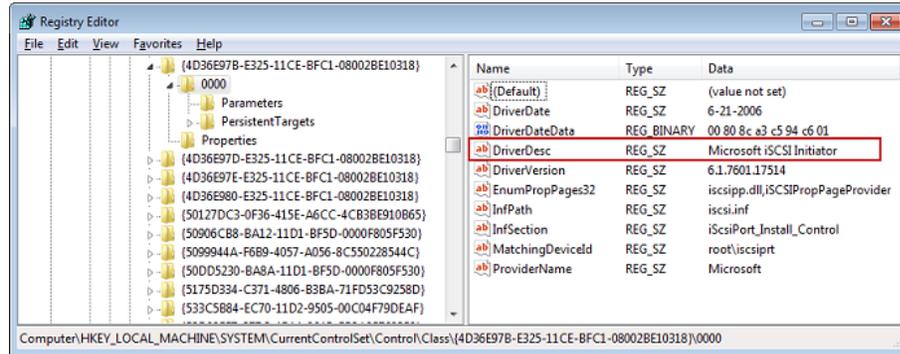
```
HK_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}
```

- c. 找到 Microsoft iSCSI 启动程序的子项。

将按 0000 或 00001 等四位数字表示该项。

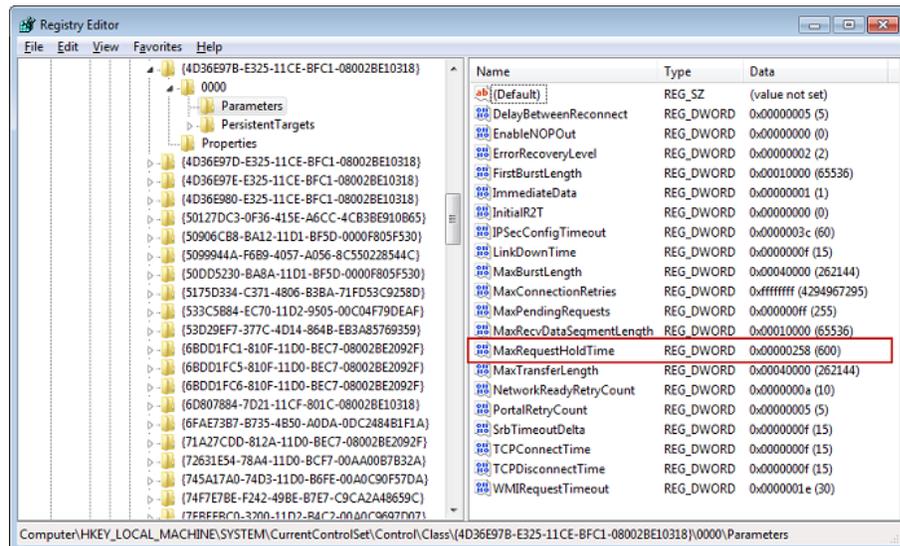
```
HK_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\<Instance Number>
```

根据计算机上所装硬件的不同，Microsoft iSCSI 发起程序可能不是子项 0000。可通过确认字符串 DriverDesc 具有下列所示的 Microsoft iSCSI Initiator 值，确保已选择正确的子项。



- d. 单击参数子项以显示 iSCSI 设置。
- e. 右键单击 MaxRequestHoldTime DWORD ( 32 位 ) 值，选择“修改”，然后将其值改为 600。

该值表示 600 秒的保持时间。下列显示值为 600 的 MaxRequestHoldTime 字符串值。



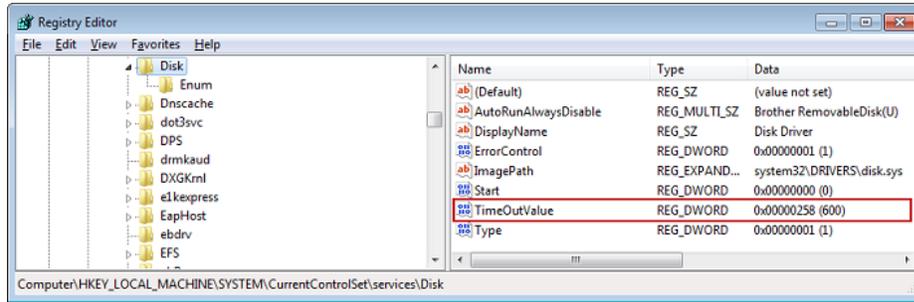
## 2. 提高磁盘超时值。

- a. 启动注册表编辑器 (Regedit.exe)。
- b. 导航到 CurrentControlSet 的服务子项中的磁盘子项。

HK\_Local\_Machine\SYSTEM\CurrentControlSet\Services\Disk

- c. 右键单击 TimeoutValue DWORD ( 32 位 ) 值，单击“修改”，然后将其值改为 600。

该值表示 600 秒的超时值。



3. 重启系统以确保新配置的值生效。

重新启动之前，必须确保刷新了向虚拟磁带进行的所有写入。为此，请使任何映射的虚拟磁带脱机，然后再重新启动。

## 从 Red Hat 客户端连接到 VTL 设备

使用 Red Hat Linux 时，您使用 `iscsi-initiatorutils` RPM 包连接到您的网关存储设备。



### Note

完成以下过程后，如果要使用备份软件，则还将需要将应用程序配置为使用这些设备。

将 Linux 客户端连接到 VTL 设备

1. 如果 `iscsi` /启动程序/实用程序 RPM 包尚未安装到您的客户端，请安装。

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. 使用下面的命令验证 iSCSI 守护进程正在运行。

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

- b. 如果 `status` 命令未返回 `running` 状态，则使用以下命令启动守护程序。

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

3. 发现为网关 VTL 定义的 VTL 设备目标。

使用下面的发现命令列出网关目标。

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

将上一命令中的 `GATEWAY_IP` 变量替换为网关的 IP 地址。可在 AWS Storage Gateway 控制台中 VTL 设备的 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。

```
iqn.1997-05.com.amazon:gatewayId-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 值是不同的。激活网关 VTL 后，为您创建了十个虚拟磁带驱动器和一个介质更换器作为目标。在 AWS Storage Gateway 控制台中选择虚拟磁带驱动器或介质更换器后，可在 iSCSI 目标信息属性窗格上找到该设备的目标名称。

#### 4. 连接到目标。

您需要在连接命令中指定正确的 `GATEWAY_IP` 和 IQN。



#### Warning

对于部署在 Amazon EC2 实例上的 Storage Gateway，不支持通过公共 Internet 访问网关。无法使用 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:mydevice  
--portal GATEWAY_IP:3260,1 --login
```

#### 5. 确认这些设备附加到客户机（发起程序）。

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

设置发起程序后，我们强烈建议您按 [建议进行的 Linux iSCSI 设置 \(p. 352\)](#) 中讨论的方式自定义 iSCSI 设置。

## 建议进行的 Linux iSCSI 设置

设置您的启动程序后，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。通过按如下所示提高 iSCSI 超时值，您可以改善应用程序处理需要较长时间的写入以及网络中断等暂时问题的性能。

### 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

必须在发现网关前进行 `iscsid.conf` 的设置。如果您已发现网关并且/或者登录到目标，您可以使用下面的命令从发现数据库删除该项，然后重新发现/登录，从而使新设置生效。

```
iscsiadm -m discoverydb -t sendtargets -p gateway_ip:3260 -o delete
```

#### 2. 提高磁盘超时值。

- a. 打开 `/etc/udev/rules.d/50-udev.rules` 文件，然后找到下面这行。

```
ACTION=="add", SUBSYSTEM=="scsi", SYSFS{type}=="0|7|14", \ RUN+=" /bin/sh  
-c 'echo [timeout] > /sys$DEVPATH/timeout'
```

- b. 将 `timeout` 值设为 600。

该值表示 600 秒的超时值。

#### 3. 重启系统以确保新配置的值生效。

重新启动之前，必须确保刷新了向虚拟磁带进行的所有写入。为此，请先卸载 VTL 设备，然后再重新启动。

## 为 VTL 设备配置 CHAP 身份验证

AWS Storage Gateway 支持通过 CHAP (质询握手身份验证协议) 在您的网关与 iSCSI 发起程序之间进行身份验证。CHAP 通过定期验证 iSCSI 发起程序的身份是否具有访问 VTL 设备目标的权限，预防反演攻击。要设置 CHAP，您必须同时在 AWS Storage Gateway 控制台中和用于连接到目标的 iSCSI 发起程序软件中配置它。



#### Note

注意，必须单独为每个 VTL 设备配置 CHAP。

本部分讨论双向 CHAP，即启动程序验证目标身份的同时，目标也验证启动程序。如需使用双向 CHAP，您需要执行两个步骤：

- 首先，在 AWS Storage Gateway 控制台中配置 CHAP。
  - [在 AWS Storage Gateway 控制台中配置 CHAP \(p. 353\)](#)
- 其次，在客户端启动程序软件中，完成 CHAP 设置。
  - [在 Windows 客户端上配置双向 CHAP。\(p. 355\)](#)
  - [如需在 Red Hat Linux 客户端上配置双向 CHAP \(p. 360\)](#)

#### 在 AWS Storage Gateway 控制台中配置 CHAP

在此过程中，您指定两个私有密钥，用于读取和写入虚拟磁带驱动器中的虚拟磁带。这两个密钥也用来在本步骤中配置客户端启动程序。

1. 转到要为其配置 CHAP 的虚拟磁带驱动器的 iSCSI 目标信息选项卡。
2. 单击配置 CHAP 身份验证链接。

在此屏幕截图中，所选进行 CHAP 配置的设备为虚拟磁带驱动器 01。



3. 在配置 CHAP 身份验证对话框中配置 CHAP。

- a. 选中已启用框。
- b. 指定发起程序名称。

启动程序名称可利用 iSCSI 启动程序软件找到。例如，对于 Windows 客户端，该名称为 iSCSI 启动程序的配置选项卡中的值。有关更多信息，请参阅 [在 Windows 客户端上配置双向 CHAP](#)。(p. 355)。



#### Note

如需更改启动程序名称，您必须先禁用 CHAP，在 iSCSI 启动程序软件中更改启动程序名称，然后使用新名称启用 CHAP。

- c. 指定用于验证发起程序身份的密钥字段。

该私有密钥的长度至少为 12 个字符。启动程序（例如 Windows 客户端）要加入与目标的 CHAP 中，必须知道该私有密钥。

- d. 在用于验证目标身份的私有密钥(双向 CHAP) 字段中指定私有密钥。

该私有密钥的长度至少为 12 个字符。启动程序要加入与目标的 CHAP 中，必须知道该私有密钥。



#### 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。

- e. 单击保存。
- f. 在确认对话框中单击关闭。

iSCSI 目标信息选项卡指示使用 CHAP 身份验证。

4. 确认 CHAP 已启用。

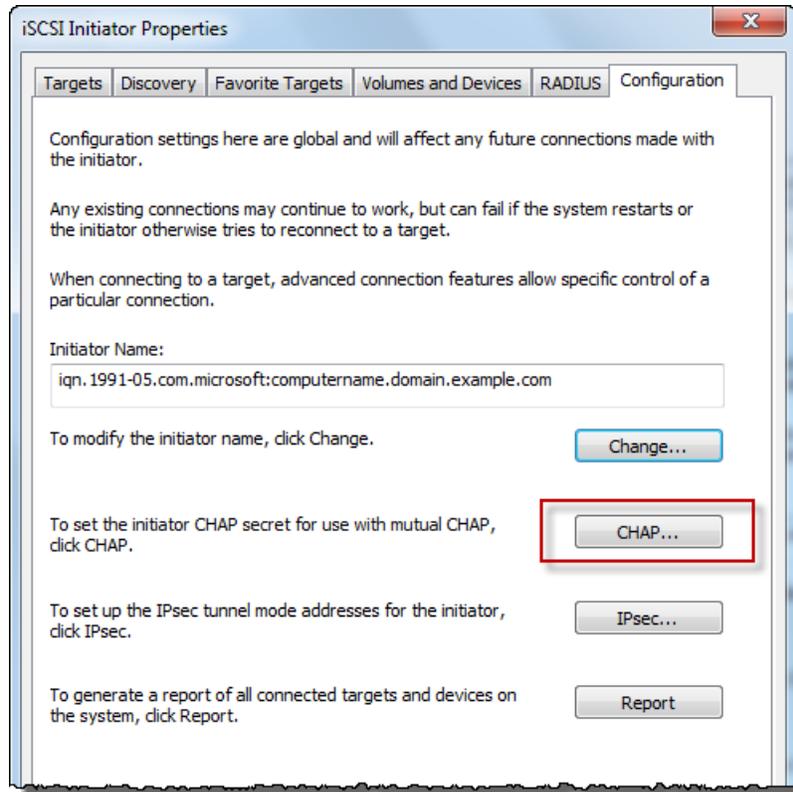
iSCSI 目标信息选项卡指示使用 CHAP 身份验证。

在 iSCSI 目标信息选项卡中，确认将 iSCSI CHAP 身份验证设置为 *true*。

在 Windows 客户端上配置双向 CHAP。

在此过程中，使用在控制台中用于为虚拟磁带驱动器配置 CHAP 的相同密钥，在 Microsoft iSCSI 发起程序中配置 CHAP。

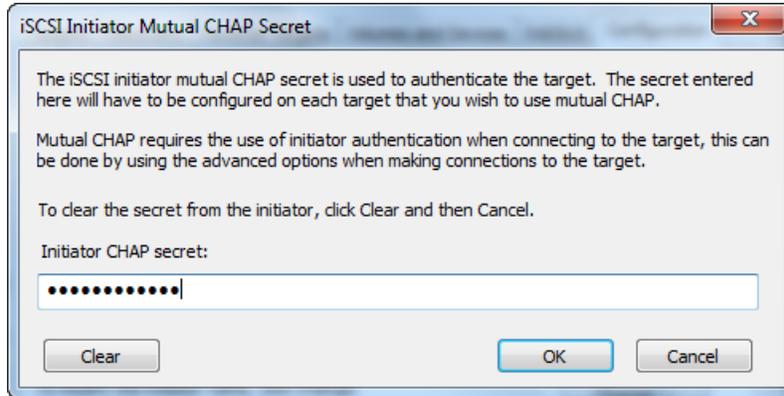
1. 如果 iSCSI 发起程序尚未启动，则在 Windows 客户端计算机的开始菜单中，键入 `iscsicpl.exe` 并运行该程序。
2. 配置启动程序 ( Windows 客户端 ) 的双向 CHAP。
  - a. 单击配置选项卡。



- b. 注意，发起程序名称字段对于您的发起程序和公司必须独一无二。此处显示的名称是在 AWS 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为示范用途。

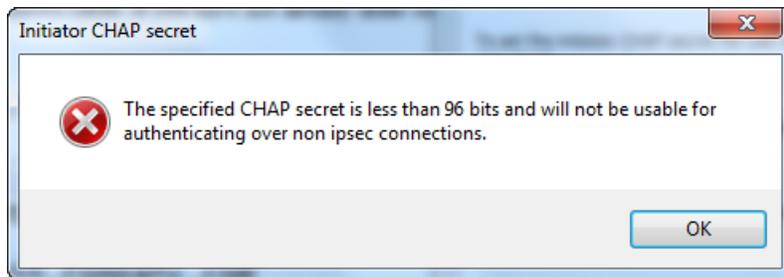
- c. 单击 CHAP 按钮。
      - d. 在 iSCSI 发起程序双向 CHAP 私有密钥对话框中，输入双向 CHAP 私有密钥值。



在此对话框中，您要输入发起程序（Windows 客户端）用于验证目标（VTL 设备）身份的私有密钥。该私有密钥允许目标读取并写入启动程序。此私有密钥映射到配置 CHAP 身份验证对话框中的用于验证目标身份的私有密钥(双向 CHAP)字段。有关更多信息，请参阅为 [VTL 设备配置 CHAP 身份验证](#) (p. 353)。

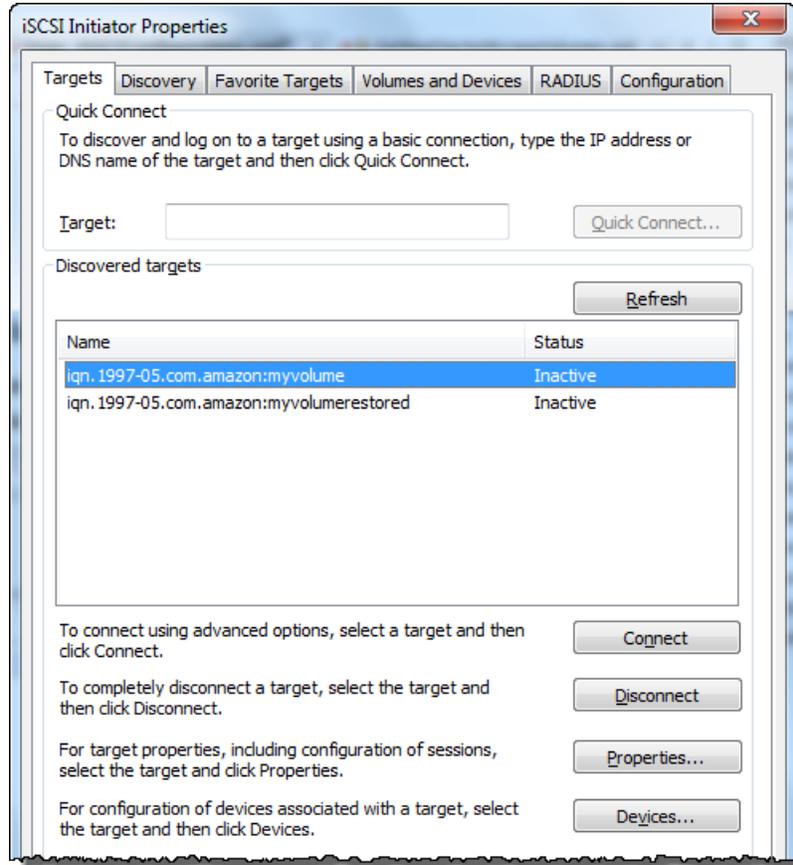
- e. 如果您输入的密钥少于 12 个字符，则显示发起程序 CHAP 私有密钥错误对话框。

单击确定，然后尝试重新输入密钥。

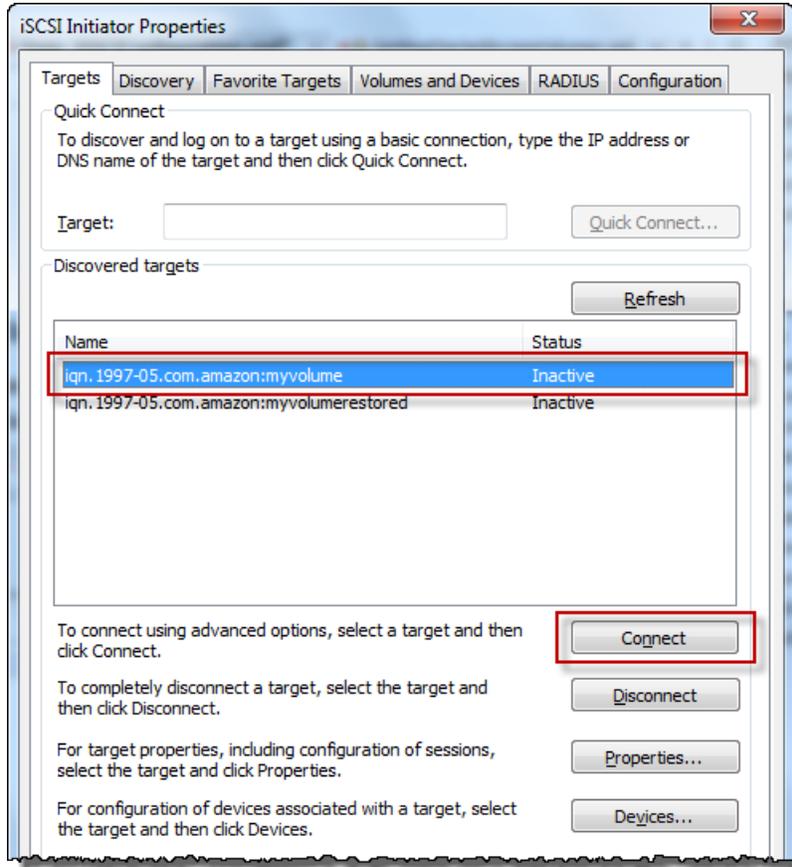


- 3. 使用启动程序的密钥进行配置，完成双向 CHAP 配置。

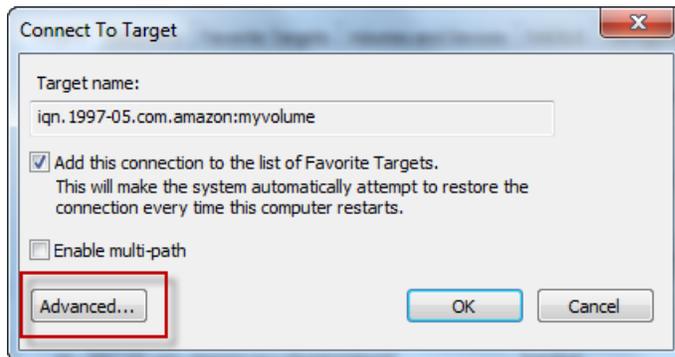
- a. 单击目标选项卡。



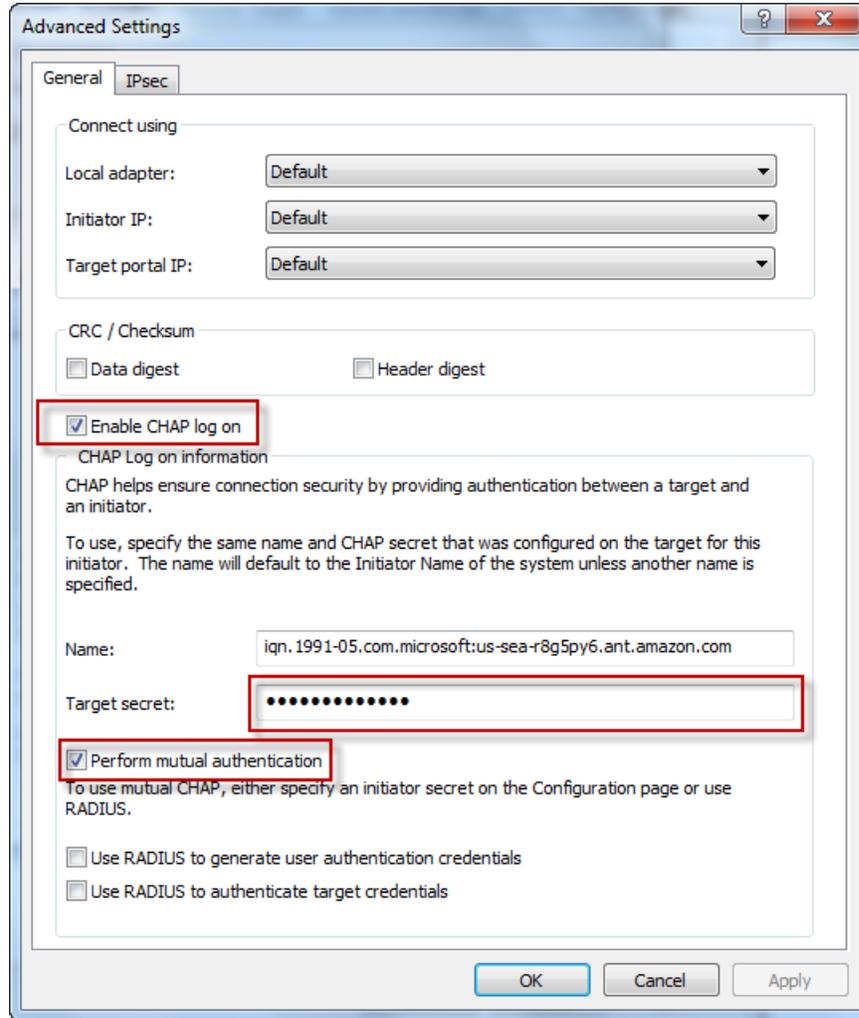
- b. 如果当前连接了要为 CHAP 配置的目标，则通过选择该目标并单击断开连接，断开该目标。
- c. 选择要为 CHAP 配置的目标，然后单击连接。



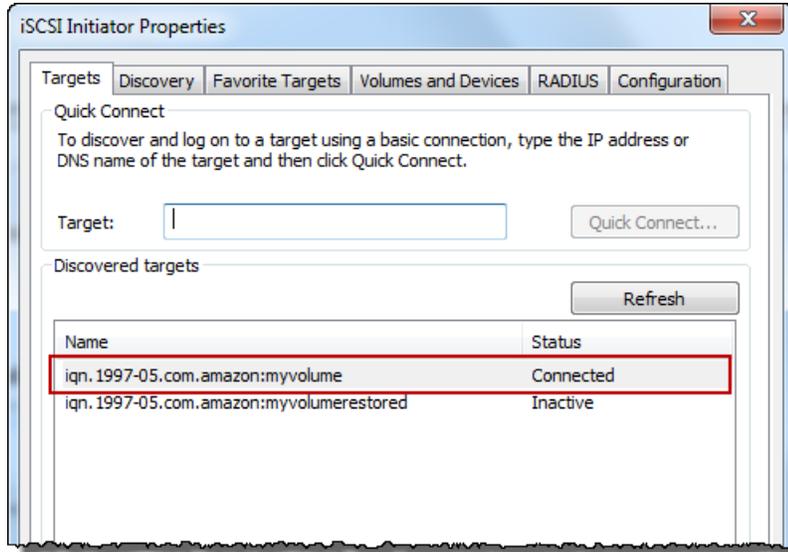
- d. 在连接到目标对话框中，单击高级。



- e. 在高级设置对话框中，配置 CHAP。



- i. 选择启用 CHAP 登录。
  - ii. 输入验证启动程序所需的该私有密钥。此私有密钥映射到配置 CHAP 身份验证对话框中的用于验证发起程序身份的私有密钥字段。有关更多信息，请参阅 [为 VTL 设备配置 CHAP 身份验证 \(p. 353\)](#)。
  - iii. 选择执行双向身份验证。
  - iv. 单击确定以应用更改。
- f. 在连接到目标对话框中，单击确定。
4. 如果提供的私有密钥正确无误，则目标将显示已连接状态。



下列步骤假定 iSCSI 守护进程正在运行并且您已连接到了目标。如果尚未完成这两个任务，则参阅[从 Red Hat 客户端连接到 VTL 设备](#) (p. 351)。

如需在 Red Hat Linux 客户端上配置双向 CHAP

在此过程中，使用在控制台中用于为虚拟磁带驱动器配置 CHAP 的相同密钥，在 Linux iSCSI 发起程序中配置 CHAP。

1. 断开并移除您即将为其配置 CHAP 的目标的任何现有配置。

a. 列出已保存的配置以找到目标名称，并确保其为已定义配置。

```
sudo /sbin/iscsiadm --mode node
```

b. 从目标断开。

以下命令从 Amazon IQN 上定义名为 *mydevice* 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:mydevice
```

c. 移除目标的配置。

以下命令删除 *mydevice* 目标的配置。

```
sudo /sbin/iscsiadm --mode node --op delete --targetname iqn.1997-05.com.amazon:mydevice
```

2. 编辑 iSCSI 文件以启用 CHAP。

a. 获取启动程序的名称（您正在使用的客户端）。

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如下所示：

```
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代码注释，然后指定正确的用户名和密码（私有访问密钥）。

```
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
```

将下表作为指导，填写前面的项目。

配置设置	值
username	使用您在本步骤中的上一步中找到的启动程序名称。该值将以“iqn”起始。例如，iqn.1994-05.com.redhat:8e89b27b5b8 是有效的 username。
password	这是用于在发起程序与 VTL 设备通信时，验证发起程序（您正在使用的客户端）身份的私有密钥。
username_in	使用目标 VTL 设备的 IQN。该值以“iqn”开头，以目标名称结尾。例如，iqn.1997-05.com.amazon:mydevice 是有效的 username_in。
password_in	这是用于在目标（VTL 设备）与发起程序通信时，验证目标身份的私有密钥。

- d. 保存配置文件中的更改并关闭文件。

### 3. 发现并登录到目标。

可按照从 [Red Hat 客户端连接到 VTL 设备 \(p. 351\)](#) 中提供的步骤发现并登录到目标。

## 管理已激活的网关 VTL

本节讨论如何能够在已部署并激活网关 VTL 后管理它。管理网关包括配置缓存存储和上传缓冲区空间、使用虚拟磁带、进行常规维护、排除故障和监控网关性能等任务。如果尚未设置网关，请参阅[尝试示例虚拟磁带库 \(VTL\) 设置 \(p. 258\)](#)。

### Topics

- [监控 AWS Storage Gateway 虚拟磁带库 \(VTL\) \(p. 362\)](#)
- [管理虚拟磁带 \(p. 371\)](#)
- [执行网关 VTL 维护任务 \(p. 378\)](#)
- [网关 VTL 问题排查 \(p. 411\)](#)

## 监控 AWS Storage Gateway 虚拟磁带库 (VTL)

### Topics

- [使用 Amazon CloudWatch 控制台 \(p. 362\)](#)
- [衡量网关 VTL 和 AWS 间的性能 \(p. 363\)](#)
- [监控上传缓冲区 \(p. 365\)](#)
- [监控缓存卷 \(p. 368\)](#)
- [理解 AWS Storage Gateway 指标 \(p. 369\)](#)

在本部分，我们讨论如何监控您 gateway、与网关关联的虚拟磁带、缓存存储和上传缓冲区。使用 AWS Management Console 可查看您的 gateway 的指标。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。

AWS Storage Gateway 将提供 Amazon CloudWatch 指标而不会加收任何费用。AWS Storage Gateway 指标将会保留两周的时间。这让您能够访问历史信息并为您提供更好的视角来了解您 gateway 和虚拟磁带的运行情况。有关 Amazon CloudWatch 的详细信息，请转到 [Amazon CloudWatch 开发者指南](#)。

### 使用 Amazon CloudWatch 控制台

您可以使用 AWS Management Console 或 Amazon CloudWatch API 来获得您的 gateway 监控数据。控制台将根据来自 Amazon CloudWatch API 的原始数据显示一系列图表。Amazon CloudWatch API 也可以通过 [Amazon AWS 软件开发工具包 \(SDKs\)](#) 或 [Amazon CloudWatch API 工具](#) 之一来使用。

无论选择何种方法使用指标，您都必须指定下列信息。

- 首先，指定使用的指标维度。维度是帮助您对某指标进行唯一标识的名称/值对。AWS Storage Gateway 的维度是 GatewayId 和 GatewayName。Amazon CloudWatch 控制台中提供了 Gateway Metrics 视图以便轻松地选择特定于网关和磁带的维度。有关维度的更多信息，请参见 [Amazon CloudWatch 开发者指南](#) 中的 [维度](#)。
- 其次，指定指标值，例如 ReadBytes。



#### Tip

如果 gateway 的名称在您希望查看指标的时间段内进行了更改，则应使用 GatewayId 来指定供您分析的指标。

下表总结了可供您使用的 AWS Storage Gateway 指标数据的类型。

Amazon CloudWatch 命名空间	维度	说明
AWS/StorageGateway	GatewayIdGatewayName	这些维度筛选描述 gateway 各个方面的指标数据。您可以通过 GatewayId 或 GatewayName 标识要使用的网关。  网关的吞吐量和延迟数据基于 gateway 中的所有虚拟磁带。  数据在 5 分钟期间内自动可用，无需收费。

网关和磁带指标的使用方式类似于其他服务指标。Amazon CloudWatch 文档对许多常见任务进行了概述。以下是常用任务的列表：

- [列出可用指标](#)

- [获取指标的数据](#)
- [创建 CloudWatch 警报](#)

## 衡量网关 VTL 和 AWS 间的性能

数据吞吐量、数据延迟和每秒操作数是您可用来理解使用 AWS Storage Gateway 的应用程序存储的性能状况的衡量指标。当您使用正确的聚合统计数据时，可使用提供给您 AWS Storage Gateway 指标来衡量这三个值。下表总结了用来衡量您的网关和 AWS 之间的吞吐量、延迟和 IOPS 的指标以及相应的统计数据。

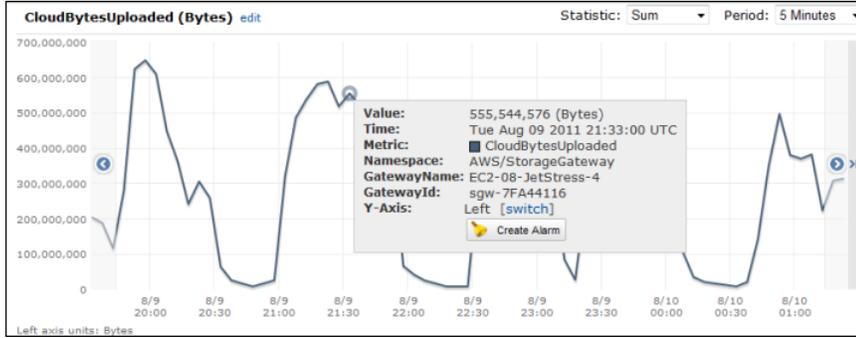
关注项	如何衡量
吞吐量	将 ReadBytes 和 WriteBytes 指标与 Sum Amazon CloudWatch 统计数据结合使用。例如，五分钟采样周期内的 ReadBytes 的 Sum 除以 300 秒可以得出以每秒字节数为速率单位的吞吐量。
延迟	将 ReadTime 和 WriteTime 指标与 Average Amazon CloudWatch 统计数据结合使用。例如，ReadTime 的 Average 为您提供采样周期内的每个操作的延迟时间。
到 AWS 的吞吐量	将 CloudBytesDownloaded 和 CloudBytesUploaded 指标与 Sum Amazon CloudWatch 统计数据结合使用。例如，五分钟样本周期内的 CloudBytesDownloaded 的 Sum 除以 300 秒可得出以每秒字节数为单位的从 AWS 到网关的吞吐量。
到 AWS 的数据延迟	将 CloudDownloadLatency 指标与 Average 统计数据结合使用。例如，CloudDownloadLatency 指标的 Average 统计数据为您提供每次操作的延迟。

下面的任务假定您从 Amazon CloudWatch 控制台开始。

### 如需衡量网关到 AWS 的上传数据吞吐量

1	选择 StorageGateway:Gateway Metrics 维度并找出要使用的网关。
2	选择 CloudBytesUploaded 指标。
3	选择一个时间范围。
4	选择 Sum 统计数据。
5	选择一个 5 分钟或更长的周期。
6	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。

下面的示例使用 Sum 统计数据显示网关磁带的 CloudBytesUploaded 指标。在示例中，将光标悬浮在一个数据点上即可显示有关该数据点的信息，包括它的值和已上传的字节数。将该值除以周期（5 分钟），可得出样本点的吞吐量。对于高亮点，从网关到 AWS 的吞吐量为 555 544 576 字节除以 300 秒，即 1.7 MB/s。



如需衡量从网关到 AWS 的数据延迟

1	选择 StorageGateway:GatewayMetrics 维度并找出要使用的网关。
2	选择 CloudDownloadLatency 指标。
3	选择一个时间范围。
4	选择 Average 统计数据。
5	选择一个 5 分钟的周期以匹配默认报告时间。
6	得出的按时间排序的数据点集包含以秒为单位的延迟。

如需对网关到 AWS 的吞吐量设置上阈值

1	启动创建警报向导。
2	选择 StorageGateway:Gateway Metrics 维度并找出要使用的网关。
3	选择 CloudBytesUploaded 指标。
4	通过定义 CloudBytesUploaded 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 CloudBytesUploaded 指标在 60 分钟内大于 10 MB 时的警报状态。
5	针对该警报状态配置要采取的行动。
6	创建警报。

如需设置从 AWS 读取数据的上阈值警报

1	启动创建警报向导。
2	选择 StorageGateway:Gateway Metrics 维度并找出要使用的网关。
3	选择 CloudDownloadLatency 指标。
4	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 60,000 毫秒时的警报状态。
5	针对该警报状态配置要采取的行动。
6	创建警报。

## 监控上传缓冲区

本部分讨论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。这样可以让您能够在缓冲区存储空间充满并且存储应用程序停止备份到 AWS 之前，主动为网关添加缓冲区容量。

关注项	如何衡量
上传缓冲区使用率	将 UploadBufferPercentUsed、UploadBufferUsed、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。

下面的任务假定您从 Amazon CloudWatch 控制台开始。

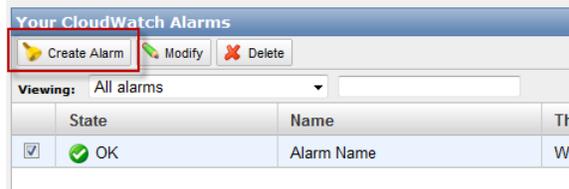
### 如需测量上传缓冲区使用率

1	选择 StorageGateway:Gateway Metrics 维度并找出要使用的网关。
2	选择 UploadBufferPercentUsed 指标。
3	选择一个时间范围。
4	选择 Average 统计数据。
5	选择一个 5 分钟的周期以匹配默认报告时间。
6	得出的按时间排序的数据点集包含上传缓冲区的使用率。

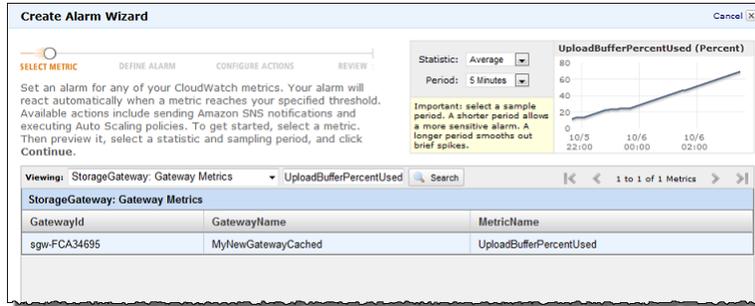
下面的任务向您介绍如何使用 Amazon CloudWatch 控制台和创建警报向导创建警报。若要了解警报和阈值的更多信息，请参见 [创建 CloudWatch 警报](#)。

### 如需为网关的上传缓冲区设置上阈值警报

1. 启动创建警报向导。
  - a. 在 Amazon CloudWatch 控制台中，单击导航窗格中的警报链接。
  - b. 在您的 CloudWatch 警报窗格中，单击创建警报。



2. 为您的警报指定指标。
  - a. 在创建警报向导的选择指标页面中，选择 AWS/StorageGateway:GatewayId,GatewayName 维度并找出您希望使用的网关。
  - b. 选择 UploadBufferPercentUsed 指标。使用 Average 统计数据 and 5 分钟的周期。

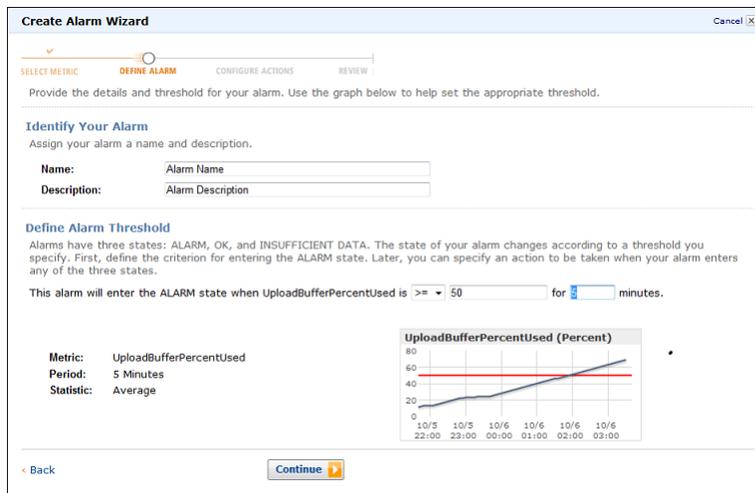


c. 单击继续。

3. 定义警报名称、描述和阈值。

- 在创建警报向导的定义警报页面中，通过分别在名称和描述字段中给您的警报命名和描述来标识警报。
- 定义警报阈值。

以下屏幕截图显示了为在 5 分钟内大于或等于 50% 的 UploadBufferPercentUsed 定义的警报状态的示例。



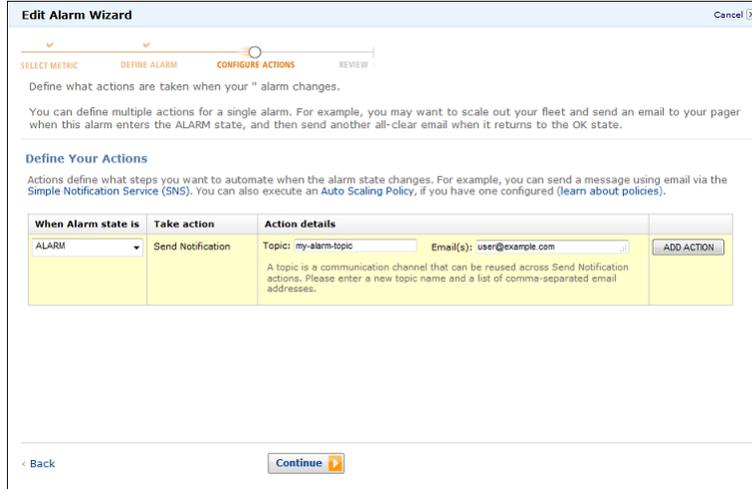
c. 单击继续。

4. 针对该警报配置电子邮件操作。

- 在创建警报向导的配置操作页面中，从警报状态下拉列表选择警报。
- 从主题下拉列表选择选择或创建电子邮件主题...

定义电子邮件主题即设置子 Amazon SNS 主题。有关 Amazon SNS 的更多信息，请参见[设置 Amazon SNS](#)。

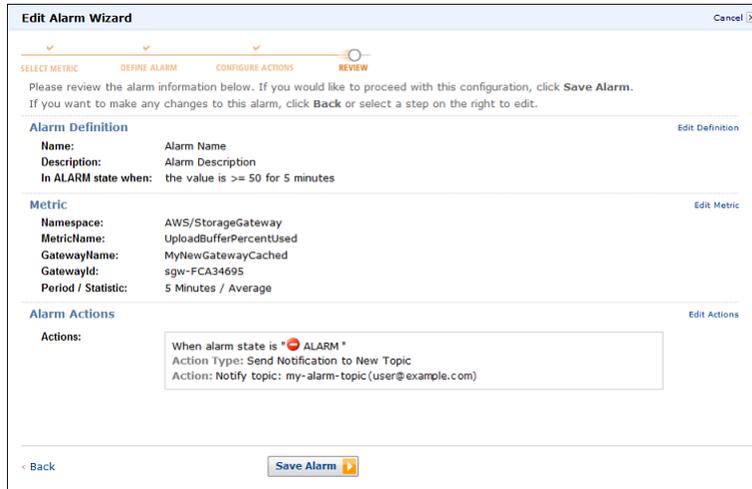
- 在主题字段中，输入主题的描述名。
- 单击添加操作。



e. 单击继续。

5. 核查警报设置并创建警报。

a. 在创建警报向导的审核页面中，审核警报定义、指标以及此步骤的关联操作。



b. 检查警报摘要后，单击保存警报。

6. 确认您对警报主题的订阅。

a. 打开发送到您在创建主题时提供的电子邮件地址的 Amazon Simple Notification Service (Amazon SNS) 电子邮件。

以下示例显示了一个通知。



- b. 单击电子邮件中的链接，确认您的订阅。

订阅确认显示。



## 监控缓存卷

下一部分讨论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存储的参数超过指定阈值时收到通知。这样可以让您主动向网关添加缓存卷。

关注项	如何衡量
缓存总使用率	将 CachePercentUsed 和 TotalCacheSize 指标结合 Average 统计数据使用。例如，将 CachePercentageUsed 结合 Average 统计数据使用以分析一段时间内的缓存使用率。  TotalCacheSize 指标仅在您向网关添加缓存时变化。
网关送达的读取请求百分率。	将 CacheHitPercent 指标与 Average 统计数据结合使用。  一般而言，您会希望 CacheHitPercent 保持较高。如果这个指标不高，并且您正在重新使用旧磁带并覆盖陈旧数据，则我们建议您删除旧磁带并创建新磁带。
缓存废数据率，亦即含有未上传到 AWS 的内容。	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。如果这个指标不低，则我们建议添加缓存或增加硬件资源。有关更多信息，请参见 <a href="#">优化 AWS Storage Gateway VTL 性能 (p. 407)</a> 。

下面的任务假定您从 Amazon CloudWatch 控制台开始。

测量网关及其所有虚拟磁带的缓存废数据百分率

1	选择 StorageGateway:Gateway Metrics 维度并找出要使用的网关。
---	------------------------------------------------

2	选择 CachePercentDirty 指标。
3	选择一个时间范围。
4	选择 Average 统计数据。
5	选择一个 5 分钟的周期以匹配默认报告时间。
6	得出的按时间排序的数据点集，包含缓存的废数据使用率。

#### 测量虚拟磁带的缓存废数据百分比

1	选择 StorageGateway:TapeMetrics 维度并找到您希望使用的网关。
2	选择 CachePercentDirty 指标。
3	选择一个时间范围。
4	选择 Average 统计数据。
5	选择一个 5 分钟的周期以匹配默认报告时间。
6	得出的按时间排序的数据点集，包含缓存的废数据使用率。

## 理解 AWS Storage Gateway 指标

### Topics

- [网关指标 \(p. 369\)](#)

### 网关指标

在本部分，我们将网关指标定义为网关范围内的指标，即，这些指标用来衡量网关的某个方面。由于 gateway 包含一个或多个虚拟磁带，因此 gateway 特定指标可代表 gateway 上的所有虚拟磁带。例如，CloudBytesUploaded 指标是在报告期间 gateway 发送给云的总字节数。这包括 gateway 上的所有磁带的活动。

使用 gateway 指标数据时，将指定您希望查看其指标的 gateway 的唯一标识。要这样做，您可以指定 GatewayId 或 GatewayName。当您需要使用网关指标时，可在指标命名空间中指定网关维度，这样可将网关特定指标与磁带特定指标区分开。有关更多信息，请参见 [使用 Amazon CloudWatch 控制台 \(p. 362\)](#)。

下表描述了可用于获取有关您的 gateway 信息的 AWS Storage Gateway 指标。表中的项根据功能按度量分组。

指标	说明
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
CachePercentageUsed	网关的缓存存储空间的百分使用率。样本在报告周期结束时采用。 单位：百分比
CachePercentDirty	尚未持续到 AWS 的网关缓存百分率。样本在报告周期结束时采用。 单位：百分比

指标	说明
CloudBytesDownloaded	<p>gateway 在报告期间从 AWS 下载的预压缩总字节数。</p> <p>将此指标与 Sum 统计数据结合使用可衡量吞吐量，而与 Samples 统计数据结合可衡量每秒操作数 (IOPS)。</p> <p>单位：字节</p>
CloudDownloadLatency	<p>报告期间从 AWS 读取数据耗费的总毫秒数。</p> <p>将此指标与 Average 统计数据结合使用可测量延迟。</p> <p>单位：毫秒</p>
CloudBytesUploaded	<p>gateway 在报告期间上传到 AWS 的预压缩总字节数。</p> <p>将此指标与 Sum 统计数据结合使用可衡量吞吐量，而与 Samples 统计数据结合可衡量每秒操作数 (IOPS)。</p> <p>单位：字节</p>
UploadBufferFree	<p>网关的上传缓冲区未使用字节的总量。样本在报告周期结束时采用。</p> <p>单位：字节</p>
UploadBufferPercentUsed	<p>网关上传缓冲区的使用率。样本在报告周期结束时采用。</p> <p>单位：百分比</p>
UploadBufferUsed	<p>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。</p> <p>单位：字节</p>
QueuedWrites	<p>等待写入 AWS 的字节数（在报告周期结束时对 gateway 中的所有磁带采样所得）。这些字节保存在网关的工作存储空间中。</p> <p>单位：字节</p>
ReadBytes	<p>在报告周期内为 gateway 中的所有磁带从网关读取的总字节数。</p> <p>将此指标与 Sum 统计数据结合使用可衡量吞吐量，而与 Samples 统计数据结合可衡量每秒操作数 (IOPS)。</p> <p>单位：字节</p>
ReadTime	<p>报告周期内为 gateway 中的所有磁带进行从网关进行读取的操作所耗费的总毫秒数。</p> <p>将此指标与 Average 统计数据结合使用可测量延迟。</p> <p>单位：毫秒</p>
TotalCacheSize	<p>以字节为单位的缓存总大小。样本在报告周期结束时采用。</p> <p>单位：字节</p>

指标	说明
WriteBytes	<p>在报告周期内为 gateway 中的所有磁带写入到网关的总字节数。</p> <p>将此指标与 Sum 统计数据结合使用可衡量吞吐量，而与 Samples 统计数据结合可衡量每秒操作数 (IOPS)。</p> <p>单位：字节</p>
WriteTime	<p>报告周期内为 gateway 中的所有磁带进行写入到网关的操作所消耗的总毫秒数。</p> <p>将此指标与 Average 统计数据结合使用可测量延迟。</p> <p>单位：毫秒</p>

## 管理虚拟磁带

### Topics

- [在虚拟磁带库 \(VTL\) 中管理磁带 \(p. 371\)](#)
- [管理虚拟磁带架 \(VTS\) 上的磁带 \(p. 376\)](#)

部署网关 VTL 后，可创建磁带。这些磁带显示在网关 VTL 的虚拟磁带库 (VTL) 中。每个网关 VTL 都仅有一个 VTL。备份应用程序可访问 VTL 中的磁带以读取和写入数据。这些磁带由 Amazon S3 提供支持。即，在写入这些磁带时，网关将数据存储到 Amazon S3 中。

AWS Storage Gateway 还提供一个虚拟磁带架 (VTS)，从中可将 VTL 中的磁带存档。VTS 类似于真实磁带库中的场外存档位置。

将磁带存档时，AWS Storage Gateway 将磁带从 VTL 移至虚拟磁带架 (VTS)。AWS Storage Gateway 为 AWS 账户的每个 AWS 地区提供一个磁带架。如果设置多个网关，则这些网关使用同一磁带架将磁带存档。可从磁带架将磁带检索到该地区内的任何网关 VTL。



### Note

在 AWS 账户中创建的每个网关 VTL 都有一个磁带库，但账户中的每个 AWS 地区只有一个虚拟架。

VTS 中的磁带由 Amazon Glacier 提供支持。即，将磁带存档时，AWS Storage Gateway 将磁带数据从 Amazon S3 移至 Amazon Glacier 进行长期存档。

以下小节介绍对于网关 VTL 上或磁带架上的磁带可执行的管理操作。

### Topics

- [在虚拟磁带库 \(VTL\) 中管理磁带 \(p. 371\)](#)
- [管理虚拟磁带架 \(VTS\) 上的磁带 \(p. 376\)](#)

## 在虚拟磁带库 (VTL) 中管理磁带

AWS Storage Gateway 为所激活的每个网关 VTL 提供一个虚拟磁带库 (VTL)。最初，该库不含任何磁带，但可在需要时创建磁带。应用程序可读取和写入网关 VTL 上提供的磁带。这些磁带由 Amazon S3 提供支持。即，在写入这些磁带时，网关将数据存储到 Amazon S3 中。磁带状态必须为“可用”，您才能写入该磁带。有关更多信息，请参阅 [磁带状态信息 \(p. 372\)](#)。

## Topics

- [磁带状态信息 \(p. 372\)](#)
- [在网关虚拟磁带库 \(VTL\) 中创建虚拟磁带 \(p. 373\)](#)
- [从网关 VTL 的虚拟磁带库中删除磁带 \(p. 373\)](#)
- [将磁带存档到 VTS \(p. 374\)](#)
- [取消磁带检索 \(p. 374\)](#)
- [取消磁带存档 \(p. 375\)](#)
- [发生故障的网关恢复虚拟磁带 \(p. 375\)](#)

控制台在 VTL 盒式磁带选项卡中显示对您的网关可用的磁带。



当库中有大量磁带时，控制台支持按条码和/或状态搜索磁带。当按条码进行搜索时，可按状态进行筛选。

### 按条码和状态进行搜索

1. 在 AWS Storage Gateway 控制台中，选择一个网关 VTL，然后要在搜索条码文本框中输入要查找的虚拟磁带的条码。默认情况下，AWS Storage Gateway 搜索所有虚拟磁带。但是，可按状态筛选搜索结果。
2. 在状态下拉列表中，选择要查找的虚拟磁带的状态。随后将在 AWS Storage Gateway 控制台中显示符合条件的磁带。



### 按状态进行搜索

- 在 AWS Storage Gateway 控制台中，从状态下拉列表中选择要查找的磁带的状态。随后将在 AWS Storage Gateway 控制台中显示所有具有指定状态的磁带。



#### Note

默认情况下，AWS Storage Gateway 显示所有磁带，无论其状态是什么。

## 磁带状态信息

磁带状态必须为“可用”，您才能读取或写入该磁带。如前面的控制台屏幕截图所示，VTS 中的每个磁带都有一个相关状态。下表列出并介绍可能存在的状态值。

虚拟磁带状态	说明	磁带数据的存储位置
正在创建	正在创建虚拟磁带。正在创建磁带，因此无法将其载入磁带驱动器。	—
可用	已创建磁带，并准备好载入磁带驱动器	Amazon S3
正在中转到 VTS	磁带已弹出并正在上传到虚拟磁带架 (VTS) 进行存档。您的网关 VTL 正在向 AWS 上传数据。上传完毕时，状态变为“已存档”。	Amazon S3

虚拟磁带状态	说明	磁带数据的存储位置
正在存档	上传完毕后，AWS Storage Gateway 开始将磁带移至由 Amazon Glacier 提供支持的虚拟磁带架 (VTS)。	正在将数据从 Amazon S3 移至 Amazon Glacier
正在删除	正在删除磁带。	正在从 Amazon S3 删除
已删除	已成功删除磁带。	—
正在检索	正在将虚拟磁带从 VTS 检索到您的网关 VTL。   <b>Note</b>  只能将虚拟磁带检索到网关 VTL。	正在将数据从 Amazon Glacier 移至 Amazon S3
已检索	已从 VTS 检索了虚拟磁带。所检索的磁带具有写保护。	Amazon S3
已恢复	虚拟磁带已恢复并为只读。  因任何原因无法访问网关时，可将与该网关关联的虚拟磁带恢复到另一个网关 VTL。必须先禁用无法访问的网关，然后才能恢复虚拟磁带。	Amazon S3
无法恢复	无法从虚拟磁带读取或向其写入。指示网关中有错。	Amazon S3

## 在网关虚拟磁带库 (VTL) 中创建虚拟磁带

可随时在网关 VTL 的虚拟磁带库中根据需要新建磁带。有关网关磁带限制的信息，请参阅[附录 F : AWS Storage Gateway 限制](#) (p. 457)。

### 创建虚拟磁带

1. 在 AWS Storage Gateway 控制台中，选择新磁带的网关 VTL，然后单击 VTL 盒式磁带选项卡。
2. 单击创建磁带以打开为您的 Storage Gateway 创建虚拟磁带窗口。



3. 填写表单，然后单击创建磁带。

当磁带状态变为“可用”后，您的备份应用程序可访问这些磁带。

## 从网关 VTL 的虚拟磁带库中删除磁带

可使用 AWS Storage Gateway 控制台从网关 VTL 的虚拟磁带库中删除虚拟磁带。

### 删除虚拟磁带

1. 在控制台 AWS Storage Gateway 中，选择该网关，然后单击 VTL 盒式磁带选项卡。
2. 选择要删除的虚拟磁带，然后单击删除磁带按钮。



删除磁带后，该磁带将从网关虚拟磁带库 (VTL) 中消失。



#### Note

如果要从网关 VTL 中删除状态为“正在检索”的磁带，则必须先取消检索。有关更多信息，请参阅 [取消磁带检索 \(p. 374\)](#)。取消磁带检索后，虚拟磁带架 (VTS) 中的磁带状态变回“已存档”。此后即可删除该磁带。

如果要从网关 VTL 中删除的磁带为“已检索”状态，则必须先使用备份应用程序弹出磁带。例如，本指南的入门部分说明如何从 Symantec Netbackup 软件中弹出磁带。（请参阅 [将磁带存档 \(p. 310\)](#)）。弹出磁带后，VTS 中的磁带状态变回“已存档”。此后即可删除该磁带。

## 将磁带存档到 VTS

可将网关的虚拟磁带库 (VTL) 中的磁带存档。将磁带存档时，AWS Storage Gateway 将该磁带移至虚拟磁带架 (VTS)。VTS 类似于一个真实的场外磁带存储设备。

AWS Storage Gateway 对于每个 AWS 地区每个账户提供一个 VTS。如果在账户中同时设置多个网关，则所有这些网关均使用同一 VTS 进行存档。

可通过使用备份软件弹出磁带，开始存档过程。已存档的磁带将显示在虚拟磁带架 (VTS) 中。

磁带存档过程由三个阶段组成，其中磁带状态分别显示为“正在中转到 VTS”、“正在存档”和“已存档”。

- 使用备份应用程序弹出磁带后，磁带状态变为“正在中转到 VTS”，并且备份应用程序无法再访问磁带。在此阶段，网关 VTL 正在将数据上传到 AWS，如果需要，还可取消正在进行的存档。有关取消存档的详细信息，请参阅 [取消磁带存档 \(p. 375\)](#)。
- 将数据上传到 AWS 完毕后，磁带状态变为“正在存档”，而 AWS Storage Gateway 开始将磁带移至 VTS。此时无法取消存档。
- 将磁带移至 VTS 后，其状态变为“已存档”。现在磁带在 VTS 中可见，并且现在可将磁带检索到该地区内的任何网关。有关磁带检索的详细信息，请参阅 [将磁带从 VTS 检索到网关 \(p. 377\)](#)。

本入门部分说明如何使用 NetBackup 软件将磁带存档。有关更多信息，请参阅 [将磁带存档 \(p. 310\)](#)。

## 取消磁带检索

开始将磁带从虚拟磁带架 (VTS) 检索到网关后，检索完毕前，可能决定不需要检索磁带。可取消正在进行的检索。此操作将磁带放回 VTS。

以下过程展示如何取消检索过程。

### 取消磁带检索

1. 从 AWS Storage Gateway 控制台中，单击 VTL 盒式磁带选项卡，然后选择要停止检索的磁带。

有关如何在控制台中查找磁带的信息，请参阅 [在虚拟磁带库 \(VTL\) 中管理磁带 \(p. 371\)](#)。

2. 在详细信息选项卡的状态行中，单击停止。



3. 在随后显示的对话框中，单击确定。取消检索后，AWS Storage Gateway 从 VTL 的磁带列表中删除该磁带，然后将 VTS 中的磁带状态从“正在检索”改为“已存档”。



#### Note

在取消磁带检索之前从 VTS 检索的部分数据将向您收费。

## 取消磁带存档

开始将磁带存档到虚拟磁带架 (VTS) 后，可能决定需要磁带恢复原状。例如，可能要取消存档过程，因存档过程耗时过长而取回磁带，或从磁带读取数据。正在存档的磁带经历三种状态。

- “正在中转到 VTS”– 网关正在将数据上传到 AWS。
- “正在存档”– 数据上传完毕，网关正在将磁带移至虚拟磁带架 (VTS)。
- “已存档”– 已移动磁带，VTS 可供检索。

仅在磁带的状态为“正在中转到 VTS”时可取消存档。根据上传带宽和所上传的数据量等因素，可能在控制台 AWS Storage Gateway 中看到或看不到此状态。

### 取消存档

1. 在 AWS Storage Gateway 控制台中，单击 VTL 盒式磁带选项卡，然后选择要停止存档的磁带。磁带的状态必须为“正在中转到 VTS”。
2. 在详细信息选项卡的状态行中，单击停止。



3. 单击取消存档按钮。取消存档后，磁带的状态恢复为其原始状态。

## 发生故障的网关恢复虚拟磁带

如果网关或虚拟机监控程序主机遇到无法恢复的故障，则可将磁带从该网关的虚拟磁带库 (VTL) 恢复到另一网关。

AWS Storage Gateway 定期拍摄库中所有磁带的时间点快照。这些快照称为恢复点。可将磁带从最新恢复点恢复到另一网关。要将磁带从发生故障的网关恢复到另一网关，请按以下步骤进行操作：

1. 新建一个网关 VTL 或找出一个正常运行的现有网关 VTL 以充当恢复目标网关。
2. 禁用发生故障的网关。这样将永久终止网关 VTL 的正常功能，并公开所有可用的恢复点。
3. 向目标网关恢复所需的任何磁带。
4. 删除发生故障的网关以免向您收费。



### Note

可读取、存档和删除恢复的磁带，但无法向其写入。

### 将磁带恢复到另一网关

1. 如果没有网关可恢复磁带，则激活一个新网关。
2. 在 AWS Storage Gateway 控制台的导航窗格中，单击要禁用的网关 VTL。随后将显示所有与该网关相关的虚拟磁带。
3. 选择该虚拟磁带和要恢复的恢复点。一个虚拟磁带可有多个恢复点。



4. 单击创建恢复磁带。
5. 在创建恢复磁带对话框中，验证要恢复的虚拟磁带的条码。



6. 在网关下拉列表中，选择要将虚拟磁带恢复到的网关。

7. 单击创建恢复磁带。

AWS Storage Gateway 将该磁带从发生故障的网关移至所指定的网关。网关将该磁带状态标为“已恢复”。

## 管理虚拟磁带架 (VTS) 上的磁带

VTS 类似于实际磁带库中的场外存档位置。AWS Storage Gateway 针对您的 AWS 账户为每个 AWS 区域提供一个磁带架。如果设置多个网关 VTL，则所有这些网关 VTL 将共享同一个磁带架，并且通过这些网关存档的磁带将转到同一磁带架上。这允许您检索磁带架上的磁带并将其转到该区域中的任何网关 VTL。



### Note

在 AWS 账户中创建的每个网关 VTL 都有一个磁带库，但账户中的每个 AWS 地区只有一个虚拟架。

VTS 中的磁带由 Amazon Glacier 支持。也就是说，当您将磁带存档到 VTS 中时，AWS Storage Gateway 会将磁带数据从 Amazon S3 移至 Amazon Glacier 中以进行长期存档。您必须先检索已存档的磁带，然后才能访问磁带上的数据，并且只能读取已存档磁带中的数据。



VTS 中的每个磁带都有一个关联的状态。有关更多信息，请参见 [磁带状态信息 \(p. 376\)](#)。经过一段时间后，磁带架上可能会有大量磁带，而控制台支持根据条码和/或状态搜索磁带。当按条码进行搜索时，可按状态进行筛选。

### 按条码和状态进行搜索

1. 在 AWS Storage Gateway 控制台导航面板中，单击虚拟磁带架，并在搜索条码文本框中输入要查找的虚拟磁带的条码。默认情况下，AWS Storage Gateway 将搜索所有虚拟磁带。但您可以按状态筛选搜索。
2. 在状态下拉列表框中，选择要查找的磁带的状态。符合条件的磁带将显示在网格中。



### 按状态进行搜索

1. 在 AWS Storage Gateway 控制台中，单击虚拟磁带架，然后从状态下拉列表框中选择状态。拥有您指定的状态的所有虚拟磁带将显示在 VTS 中。

有关 VTS 中的磁带状态的信息，请参见 [磁带状态信息 \(p. 376\)](#)。

2. 如果未找到虚拟磁带，则需要单击刷新。

## 磁带状态信息

如前面的控制台屏幕截图所示，VTS 中的每个磁带都有一个相关状态。下表列出并描述了可能的状态值。

### 确定虚拟磁带的状态

1. 在 AWS Storage Gateway 控制台中，单击虚拟磁带架。
2. 在网格的状态列中，您可查看每个磁带的状态。

磁带状态还会显示在每个虚拟磁带的详细信息选项卡中。

该表列出了

VTS 中的虚拟磁带状态	说明
ARCHIVED	磁带已弹出并将上传到 VTS。
正在检索	正在从 VTS 中检索虚拟磁带。   <b>Note</b> 虚拟磁带只能检索到网关 VTL 中
已检索	已从 VTS 检索了虚拟磁带。已检索的磁带是只读的。

## 将磁带从 VTS 检索到网关

### Topics

若要访问 VTL 中的磁带数据，则必须先将磁带从 VTS 检索到您的网关 VTL 中。AWS Storage Gateway 将为每个网关提供一个 VTL，但每个地区的每个帐户只有一个 VTS。您可以将磁带从某个地区中的 VTL 还原到同一地区中的网关 VTL 中。

如果您在某个地区中部署了多个网关 VTL，则只能将磁带检索到一个网关中。

已检索的磁带是受写入保护的，您只能读取磁带上的数据。



### Important

需经过最多 24 个小时后，磁带才在您的网关 VTL 中可用。

### 将磁带检索到网关中

1. 在 AWS Storage Gateway 控制台的导航窗格中，单击虚拟磁带架。随后，控制台显示所有网关已存档的所有虚拟磁带。
2. 选择要检索的虚拟磁带，然后单击检索磁带。



### Note

要检索的虚拟磁带的状态必须为 *ARCHIVED*



3. 在检索磁带向导的磁带条码字段中，确认条码标识的是要检索的虚拟磁带。



4. 在网关下拉列表中，选择要将存档的磁带检索到的网关，然后单击继续。

磁带的状态从“已存档”变为“正在检索”。此时，将您的数据从虚拟磁带架（受 Amazon Glacier 支持）移至虚拟磁带库（受 Amazon S3 支持）中。在移动所有数据后，VTS 中的虚拟磁带状态将变为 *RETRIEVED*。



#### Note

检索的虚拟磁带为只读。

## 从 VTS 中删除磁带

如果您不再需要虚拟磁带，则可从虚拟磁带架中将其删除。

从 VTS 中删除虚拟磁带

1. 在 AWS Storage Gateway 控制台中，单击虚拟磁带架。
2. 选择要删除的虚拟磁带，然后单击删除磁带按钮。



如果虚拟磁带的状态为 *RETRIEVING*，则必须先取消检索，然后再删除磁带。有关更多信息，请参见 [取消磁带检索 \(p. 374\)](#)。如果磁带状态为 *RETRIEVED*，则必须先存档磁带，然后再将其删除。有关更多信息，请参见 [将磁带存档到 VTS \(p. 374\)](#)。

## 执行网关 VTL 维护任务

在激活网关后，AWS Storage Gateway 将支持多个维护任务。本部分对这些任务进行了分组，如下所示：

- 在 AWS Storage Gateway 控制台中执行的任务 - 有关更多信息，请参见 [常见网关 VTL 维护任务 \(p. 378\)](#)。
- 在本地执行的任务 - 如果在本地部署网关 VTL，则在网关的本地控制台中执行大多数维护任务。有关更多信息，请参见 [网关 VTL 在本地运行时的维护任务 \(p. 390\)](#)。
- 当网关 VTL 作为 EC2 实例运行时执行的任务 - 有关更多信息，请参见 [以 Amazon EC2 实例的形式运行时网关 VTL 的维护任务 \(p. 408\)](#)。

## 常见网关 VTL 维护任务

本部分描述了可在 AWS Storage Gateway 控制台中执行的网关 VTL 维护任务。有关特定于 Amazon EC2 实例上运行的网关 VTL 的维护任务，请参见 [以 Amazon EC2 实例的形式运行时网关 VTL 的维护任务 \(p. 408\)](#)。

### Topics

- [管理上传缓冲区和缓存存储 \(网关 VTL\) \(p. 379\)](#)
- [关停并启动网关 VTL \(p. 383\)](#)
- [管理网关 VTL 更新 \(p. 384\)](#)
- [为您的网关 VTL 更新带宽速率限制 \(p. 384\)](#)
- [禁用网关 VTL \(p. 389\)](#)
- [删除网关 VTL \(p. 390\)](#)

您可以在 AWS Storage Gateway 控制台的网关选项卡中执行许多与网关维护相关的任务。以下屏幕截图显示网关选项卡。



下表总结了网关选项卡上的字段。可以更改某些字段中的值。若要更改值，请单击可编辑的字段末尾的编辑链接。

维护项目	注释
名称	您可以有选择地修改网关名称。如果使用 Amazon CloudWatch 查看网关指标 ( 请参见 <a href="#">使用 Amazon CloudWatch 控制台 (p. 362)</a> ) , 建议您记下前一名称以及新名称以免混淆, 或者仅使用网关 ID, 该 ID 保持不变。
Gateway ID	AWS Storage Gateway 会为每个网关分配一个唯一标识符。该值不能更改。
IP Addresses	这是您在网关上将启动程序连接到 VTL 设备时使用的 IP 地址。如果您可以将网关配置为使用多个网络接口卡 (NIC), 则所有这些 IP 地址将在此处显示。
Time Zone	AWS Storage Gateway 在显示基于时间的信息时使用区。对于网关 VTL, 将指定时区用于维护起始时间。
Rate Limit on Upload to AWS	您可以选择限制从网关到 AWS 的上传吞吐量以便管理您的网络流量。对您的网关实行带宽限制, 从而限制网络带宽的使用量。以千位每秒为单位制定速率限制 (kbps)。默认对上传没有速率限制。有关更新此带宽的更多信息, 请参见 <a href="#">为您的网关 VTL 更新带宽速率限制 (p. 384)</a> 。
Rate Limit on Download from AWS	您可以选择限制从 AWS 到网关的下载吞吐量以便管理您的网络流量。对您的网关实行带宽限制, 从而限制网络带宽的使用量。以千位每秒为单位制定速率限制 (kbps)。默认对下载没有速率限制。有关更新此带宽的更多信息, 请参见 <a href="#">为您的网关 VTL 更新带宽速率限制 (p. 384)</a> 。这会从磁带读取时的性能
Upload Buffer Used	显示已使用的上传缓冲区。有关如何监控上传缓冲区及其如何随时间变化的信息, 请参见 <a href="#">监控上传缓冲区 (p. 365)</a> 。
Maintenance Start Time	这标识每周维护窗口的起始时间。激活期间, 默认时间分配到您的网关。如需更改时间, 请单击编辑并指定网关时区中一星期中的某一天以及一天中的某个时间。
Apply Update Now	如果 AWS Storage Gateway 有更新, 控制台将显示消息。单击立即应用更新以立即应用更新。如果您不应用更新, AWS Storage Gateway 将根据您的维护起始时间设置应用更新。有关更多信息, 请参见 <a href="#">管理网关 VTL 更新 (p. 384)</a> 。

## 管理上传缓冲区和缓存存储 ( 网关 VTL )

最初配置并部署网关后, 可能会发现需要通过添加或删除用于上传缓冲区的磁盘或添加用于缓存存储的磁盘, 调整本地存储。



### Important

AWS Storage Gateway 不支持删除分配用于缓存存储的磁盘。

网关所需的上传缓冲区空间量取决于若干因素, 如向虚拟磁带传入数据的速率、向 AWS 传出数据的速率以及网络带宽等。如果应用程序持续向虚拟磁带快速写入数据, 而网络吞吐量不足以让网关将数据上传到 AWS, 则上传缓冲区最终将填满等待上传到 AWS 的数据。网关能否定期获得磁带的恢复点取决于是否正确配置了上传缓冲区。如果上传缓冲区太小, 则可能在写入磁带时将其填满, 而这样可能会影响网关能够以多快速度获得下一个恢复点。有关调整上传缓冲区大小的信息, 请参见在 [VMware ESXi 主机上为 AWS Storage Gateway VTL VM 配置本地磁盘存储 \(p. 314\)](#)。有关恢复点的详细信息, 请参见 [发生故障的网关恢复虚拟磁带 \(p. 375\)](#)

缓存存储容量大小至少应达到上传缓冲区的大小。这样可确保缓存存储够大，可持续不断地容纳所有尚未上传到 Amazon S3 的数据。缓存存储填满无效数据后，直到有更多缓存存储可用时，才不会阻止应用程序向虚拟磁带进行写入。但是，仍允许应用程序从虚拟磁带进行读取。

可遵照下面的一些指南以确保为网关的上传缓冲区和缓存存储分配的存储空间可满足需要：

- 使用 Amazon CloudWatch 指标
  - 可通过在一段时间后监控网关使用上传缓冲区空间的百分比，主动避免上传缓冲区填满。Amazon CloudWatch 提供 UploadBufferPercentUsed 指标等用量指标用于监控网关的上传缓冲区（请参阅[监控上传缓冲区 \(p. 365\)](#)）。可对 UploadBufferPercentUsed 指标设置警报，在上传缓冲区用量超出阈值时通知您。如果上传缓冲区填充得接近最大容量，则可考虑向网关添加更多上传缓冲区容量。
  - 可通过监控正在如何使用缓存存储—特别是通过检查缓存未命中次数，主动避免将缓存存储填满无效数据。Amazon CloudWatch 提供提供 CachePercentDirty 和 CacheHitPercent 指标等用量指标用于监控网关的缓存存储中有多少数据尚未上传到 Amazon S3。您可以设置阈值，在缓存废数据百分率超过某阈值或缓存命中率低于某阈值时触发向您发送的通知，两者均有可能表示缓存存储空间不够网关使用。有关 AWS Storage Gateway 指标的完整列表，请参阅[理解 AWS Storage Gateway 指标 \(p. 369\)](#)。
  - 优化所处环境—如果传入写入的速度与传出网络带宽相比过高，则无论将上传缓冲区容量配置为多大，网关可能都跟不上该速度。在这种情况下，可通过为网关分配更好的硬件资源，改善这种情况（请参阅[优化 AWS Storage Gateway VTL 性能 \(p. 407\)](#)）。
  - 使用调整大小公式—您使用建议的公式决定如何调整配置为上传缓冲区和缓存存储的本地存储（磁盘）的大小。随着应用程序需求的变化，应定期检查建议用于调整上传缓冲区和缓存存储大小的公式。有关详细信息，请参阅[配置上传缓冲区的大小（网关 VTL） \(p. 316\)](#)和[配置缓存存储空间大小 \(p. 319\)](#)。

有关说明，请参阅[添加和删除上传缓冲区容量（网关 VTL） \(p. 380\)](#)。

### 添加和删除上传缓冲区容量（网关 VTL）

无需中断现有的网关功能，即可向网关添加更多上传缓冲区容量。注意，在添加更多上传缓冲区容量时，可在开启网关 VM 后这样做；但是，在减少上传缓冲区容量时，必须先关闭 VM。

### 添加上传缓冲区或缓存存储容量（网关 VTL）

为网关配置额外存储作为上传缓冲区或缓存存储是一个两步过程

1. 添加一个所需大小的磁盘。
  - 有关在 VMware ESXi 主机上添加磁盘用于上传缓冲区的详细信息，请参阅[为上传缓冲区添加本地磁盘（网关 VTL） \(p. 315\)](#)，而对于 Hyper-V 主机，请参阅[为上传缓冲区添加本地磁盘（网关 VTL） \(p. 329\)](#)。
  - 有关在 VMware ESXi 主机上添加磁盘用于缓存存储的详细信息，请参阅[为缓存存储添加本地磁盘（网关 VTL） \(p. 319\)](#)，而对于 Hyper-V 主机，请参阅[为缓存存储添加本地磁盘（网关 VTL） \(p. 332\)](#)。
2. 配置网关以使用其他磁盘作为上传缓冲区。有关更多信息，请参阅[配置上传缓冲区和缓存存储空间 \(p. 346\)](#)。

### 删除上传缓冲区容量（网关 VTL）

随着应用程序需求的变化以及更改网关的本地存储磁盘配置，可能需要减少网关的上传缓冲区容量。分配为上传缓冲区的本地磁盘也有可能失效，导致您需要从上传缓冲区移除该磁盘并分配新的本地磁盘。在两种情况下，均可使用 AWS Storage Gateway 控制台删除更多缓冲区容量。

AWS Storage Gateway 不支持删除分配用于缓存存储的磁盘。

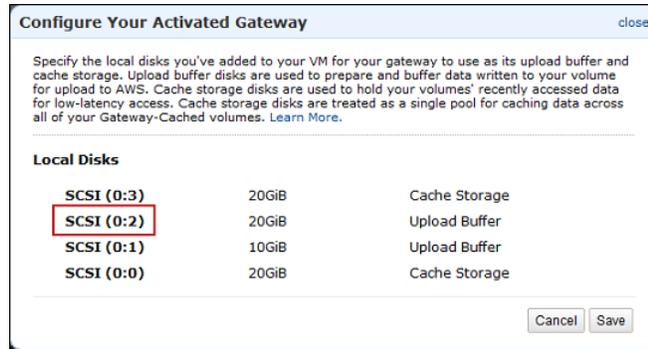
## 删除分配为上传缓冲区的磁盘

1. 在 AWS Storage Gateway 控制台的网关选项卡中，单击配置本地存储。



2. 在配置已激活的网关对话框中，记下要删除的本地磁盘的虚拟设备节点值。可在本地磁盘列中找到节点值。例如，在下面的对话框中，突出显示设备节点 SCSI (0:2)。

您在 VM 客户端中使用磁盘的虚拟设备节点以确保删除的磁盘正确无误。



3. 按**关停并启动网关 VTL (p. 383)**过程中的步骤关闭网关。



### Note

关闭网关之前，请确保没有向该网关写入数据的应用程序正在使用它，并且没有在进行存档。可在控制台的状态列中检查磁带的状态。

4. 要移除底层本地磁盘，请执行下列操作之一，然后转到下一步：

对于下列托管网关...	请执行此操作...
VMware ESXi	按 <b>删除分配为上传缓冲区磁盘的本地磁盘 (VMware ESXi) (p. 381)</b> 中的步骤进行操作。
Microsoft Hyper-V	按 <b>删除分配为上传缓冲区磁盘的本地磁盘 (Microsoft Hyper-V) (p. 382)</b> 中的步骤进行操作。

5. 在 AWS Storage Gateway 控制台中，打开网关。



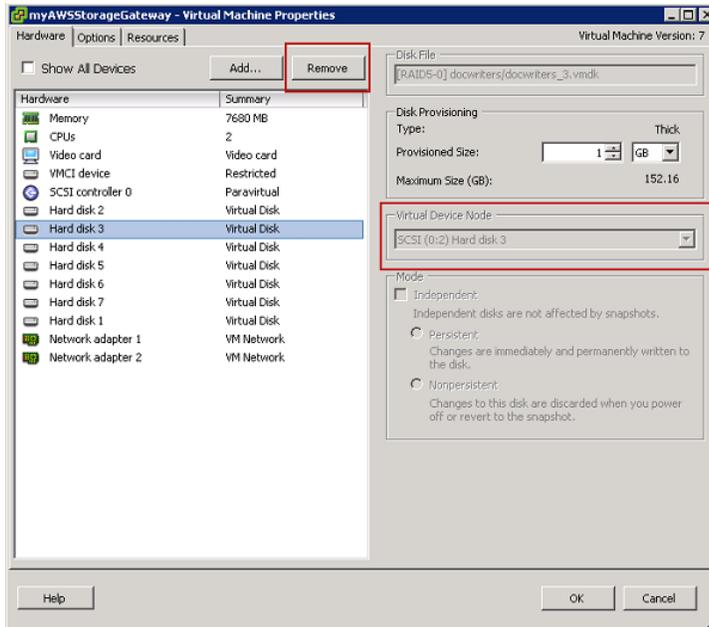
### Important

移除了用作上传缓冲区的磁盘后，您必须在向 VM 添加新磁盘前重新开启网关。

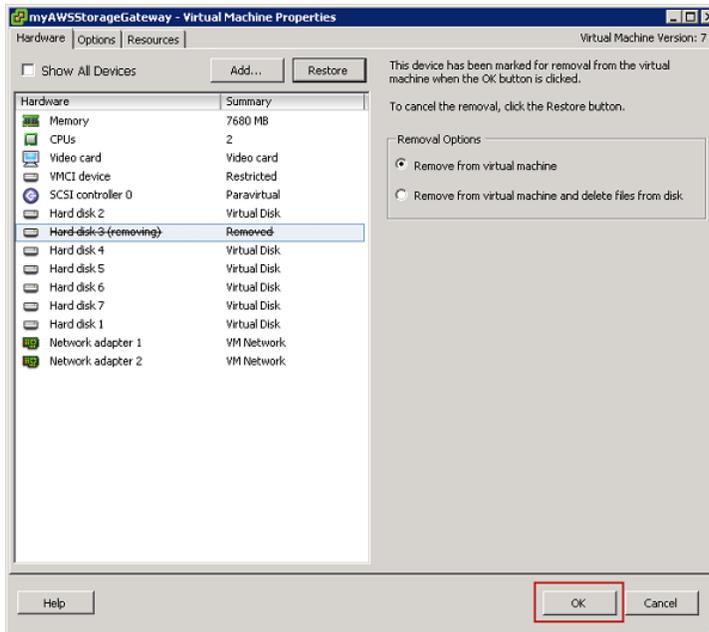
## 删除分配为上传缓冲区磁盘的本地磁盘 (VMware ESXi)

1. 在 vSphere 客户端中，右键单击网关 VM 的名称，然后单击编辑设置...。
2. 在虚拟机属性对话框的硬件选项卡中，选择分配为上传缓冲区的磁盘，然后单击删除。

确认虚拟机属性对话框中的虚拟设备节点值与从上一步中记录的值相同。这样可以确保您移除需要移除的网关。



3. 在删除选项面板中选择一个选项，然后单击确定以完成删除磁盘的过程。

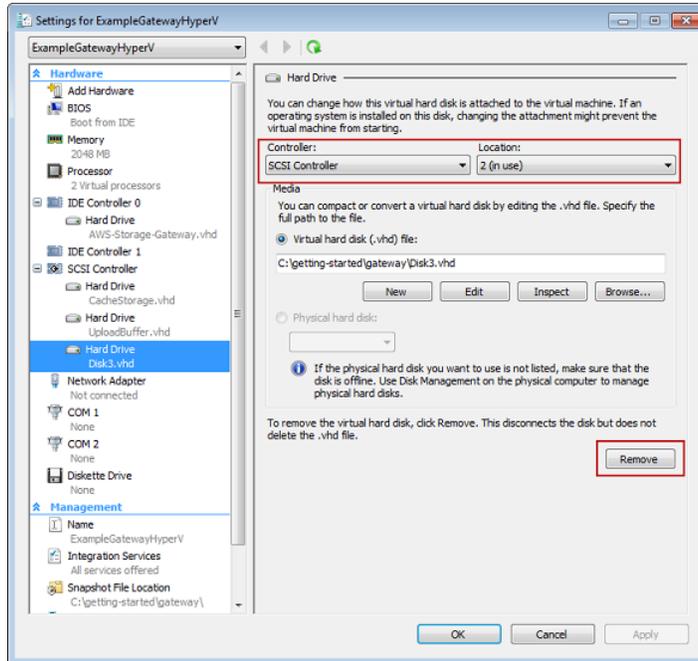


### 删除分配为上传缓冲区磁盘的本地磁盘 (Microsoft Hyper-V)

1. 在 Microsoft Hyper-V 管理器中，右键单击网关 VM 的名称，然后单击设置...。
2. 在设置对话框的硬件列表中，选择要删除的磁盘，然后单击删除。

添加到网关的磁盘在硬件列表中的 SCSI 控制器条目下。验证控制器和位置值与上一步中记录的相同。这项操作确保您移除了要移除的磁盘。

在 Microsoft Hyper-V Manager 中显示的第一个 SCSI Controller 是控制器 0。



3. 单击确定以应用更改。

## 关停并启动网关 VTL

您可能需要关闭您的网关 VM 以进行主机维护。例如，关闭网关以将修补程序应用于您的管理程序。在关闭网关 VM 之前，您应关停该网关。

请注意，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关停网关，则无法完成该任务。关停之前，您应检查备份软件中所有正在进行中的任务，并检查备份计划。

### 关停网关

1. 在 AWS Storage Gateway 控制台的导航窗格中，选择网关。
2. 单击关停。



3. 在确认对话框中，单击确定。



4. 在网关关闭对话框中，单击关闭。



在网关关停的过程中，您可能会看到网关正在关停进程中的消息。

5. 在左侧导航窗格中选择网关。

将显示重启按钮。



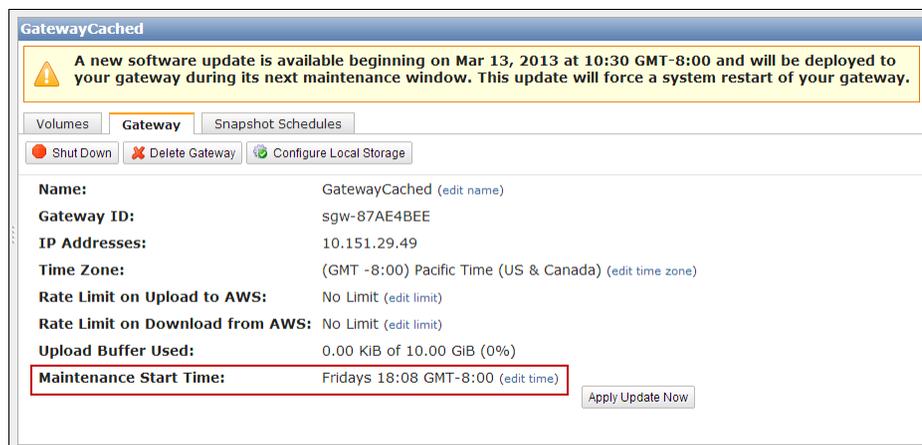
### 启动网关

1. 在 AWS Storage Gateway 控制台的导航窗格中，选择要重新启动的网关。
2. 单击重启。

### 管理网关 VTL 更新

AWS Storage Gateway 将定期发布需要应用于网关的重要更新。AWS 会在发布任何网关更新前通过 AWS Storage Gateway 控制台和电子邮件通知您。软件更新会强制重新启动您的网关，这通常需要花费几分钟时间完成。在此更新过程中，您无需执行任何操作。您可以通过提高 iSCSI 启动程序的超时值将应用程序的中断几率降到最低。有关针对 Windows 和 Linux 提高 iSCSI 启动程序超时值的更多信息，请分别参见 [建议进行的 Windows iSCSI 设置 \(p. 349\)](#) 和 [建议进行的 Linux iSCSI 设置 \(p. 352\)](#)。

您可以在收到通知后立即应用更新。否则，网关将在计划维护时间自动应用更新。部署并激活网关后，将设置默认的周度维护计划。您可以随时通过单击网关选项卡中维护起始时间旁的编辑链接来修改该计划。以下示例显示了含有维护消息的网关选项卡和立即应用更新按钮。



### 为您的网关 VTL 更新带宽速率限制

#### Topics

- [使用 AWS SDK for Java 更新 AWS Storage Gateway VTL 带宽速率限制 \(p. 385\)](#)
- [使用 AWS SDK for .NET 更新 AWS Storage Gateway VTL 带宽速率限制 \(p. 387\)](#)

- [使用 AWS Tools for Windows PowerShell 更新 AWS Storage Gateway VTL 带宽速率限制 \(p. 389\)](#)

您可以限制（或限定）从网关到 AWS 的上传吞吐量或者从 AWS 到网关的下载吞吐量。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 AWS Management Console 或以编程方式使用 AWS Storage Gateway API（请参见 [UpdateBandwidthRateLimit](#)）指定速率限制，也可以使用 AWS 软件开发工具包 (SDK) 进行指定。以编程方式更改限定值的功能可以让您自动更改一天中的限制，例如安排任务时间来更改带宽。本部分介绍了如何使用 AWS Storage Gateway 控制台更改这些限制。有关以编程方式配置这些值的信息，请单击本主题开头提供的主题链接。

如需使用控制台更改网关的带宽限制

1. 在 AWS Storage Gateway 控制台的导航窗格中，选择要管理的网关。
2. 在右侧窗格中单击网关选项卡。
3. 单击要更改的限制旁的编辑限制文本。



4. 在编辑速率限制对话框中，输入新的限制值，然后单击保存。

The screenshot shows a dialog box titled "Edit Rate Limits". It contains two rows of input fields. The first row is labeled "Upload Rate Limit:" and has a text input field containing the number "50" followed by the unit "Kilobits/sec". The second row is labeled "Download Rate Limit:" and has a text input field containing the number "100" followed by the unit "Kilobits/sec". At the bottom right of the dialog box, there are two buttons: "Cancel" and "Save".

### 使用 AWS SDK for Java 更新 AWS Storage Gateway VTL 带宽速率限制

以编程方式更新带宽速率限制可为您提供在一段时间内自动调整限制的途径，例如可通过安排任务时间进行调整。以下示例演示如何使用 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，请参见 *AWS SDK for Java Developer Guide* 中的入门部分。

## Example :使用 AWS SDK for Java 更新网关带宽限制

以下 Java 代码示例更新网关的带宽速率限制。您需要更新代码并提供服务终端节点、网关的亚马逊资源名称 (ARN) 以及上传和下载限制。有关可用于 AWS Storage Gateway 的 AWS 服务终端部分点的列表，请参见 *AWS General Reference* 中的 [地区和终端部分点](#)。

```
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(
            ListDeleteVolumeSnapshotsExample.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 " + re
turnGatewayARN);
        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 bandwidth.\n" + ex.to
String());
    }
}
```

### 使用 AWS SDK for .NET 更新 AWS Storage Gateway VTL 带宽速率限制

以编程方式更新带宽速率限制可为您提供在一段时间内自动调整限制的途径，例如可通过安排任务时间进行调整。下面的示例介绍了如何使用适用于 .NET 的 AWS 软件开发工具包 (SDK) 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，请参见 *AWS SDK for .NET Developer Guide* 中的 [入门](#) 部分。

Example :使用 AWS SDK for .NET 更新网关带宽限制

以下 C# 代码示例更新网关的带宽速率限制。您需要更新代码并提供服务终端节点、网关的亚马逊资源名称 (ARN) 以及上传和下载限制。有关可用于 AWS Storage Gateway 的 AWS 服务终端部分的列表，请参见 *AWS General Reference* 中的[地区和终端部分点](#)。

```
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.amazon
aws.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 bandwidth.\n" + ex.ToString());
}
}
}
}

```

### 使用 AWS Tools for Windows PowerShell 更新 AWS Storage Gateway VTL 带宽速率限制

以编程方式更新带宽速率限制可为您提供在一段时间内自动调整限制的途径，例如可通过安排任务时间进行调整。以下示例演示如何使用 AWS Tools for Windows PowerShell 更新网关的带宽速率限制。如需使用示例代码，您应该熟悉 PowerShell 脚本 控制台应用程序的运行方式。有关更多信息，请参见 *AWS Tools for Windows PowerShell User Guide* 中的 [入门](#) 部分。

#### Example :使用 AWS Tools for Windows PowerShell 更新网关带宽限制

以下 PowerShell 脚本示例更新网关的带宽速率限制。您需要更新脚本并提供服务终端节点、网关的亚马逊资源名称 (ARN) 以及上传和下载限制。

```

<# .DESCRIPTION Update Gateway bandwidth limits. .NOTES PREREQUISITES: 1) AWS Tools for PowerShell from http://aws.amazon.com/powershell/ 2) Credentials and region stored in session using Initialize-AWSDefault. For more info see, http://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)

```

### 禁用网关 VTL

禁用网关将锁定磁带。也就是说，不会将您可写入到这些磁带中的任何数据发送到 AWS。如果您的网关出现故障，并且您需要将磁带恢复到另一个网关中，则必须先禁用出现故障的网关。有关恢复磁带的更多信息，请参见 [发生故障的网关恢复虚拟磁带 \(p. 375\)](#)。

请注意，您只能在网关未连接到 AWS 时使用控制台禁用网关。否则，控制台上将不会显示禁用网关按钮。

#### 禁用网关

1. 在 AWS Storage Gateway 控制台中，选择出现故障的网关，然后单击禁用网关。



2. 在随后显示的对话框中，单击确定。

## 删除网关 VTL

删除操作将停用网关。您可以在 AWS Storage Gateway 控制台中或以编程方式删除网关。删除网关时，您会遇到两种情况。

- 网关已连接到 AWS - 如果网关已连接到 AWS，并且您已关停网关，则 iSCSI 目标将不再可用。
- 网关未连接到 AWS - 如果网关出于任何原因（例如，已关闭 VM 或网络中断）未连接到 AWS，则您无法关停该网关。在重新启动并运行环境后，您可能拥有在本地运行的、具有可用的 iSCSI 目标的网关。不过，将不会在 AWS 中上传或下载任何数据。



### Note

如果网关无法正常工作，您必须先禁用网关并删除处于 *RETRIEVING* 或 *RETRIEVED* 状态的磁带，然后再删除该网关。

在控制台中删除网关后，应从您的主机中删除 VM。

删除网关后，您将不再需要为其付费。如果已在 VTS 中对磁带进行存档，则会保留这些磁带，并且您需要继续为存储付费。在删除网关前，必须从 VTL 中删除磁带，如下所示。

- 如果磁带状态为 *RETRIEVING*，则必须取消检索过程。有关说明，请参见[取消磁带检索 \(p. 374\)](#)。
- 如果磁带状态为 *RETRIEVED*，则可使用备份软件弹出磁带。有关说明，请参见[将磁带存档 \(p. 310\)](#)。

在删除网关前，您必须取消所有 *RETRIEVING* 操作并弹出所有已检索的磁带。

## 删除网关 VTL

1. 在 AWS Storage Gateway 控制台的导航窗格中，选择要删除的网关。
2. 在网关选项卡中，单击删除网关。



### Important

请确保当前没有应用程序正在写入到网关 VTL。如果您在网关使用期间删除网关，可能会造成数据丢失。



3. 单击确定来确认删除。

至此，删除的网关不再是已激活的网关。不过，网关 VM 会仍然在您的虚拟环境中。如需移除 VM，请使用 VMware vSphere 客户端或 Microsoft Hyper-V Manager 连接到主机并移除 VM。

## 网关 VTL 在本地运行时的维护任务

对于在本地部署的网关 VTL，本节介绍可使用本地网关控制台执行的维护任务。有关其他维护任务，请参阅[以 Amazon EC2 实例的形式运行时网关 VTL 的维护任务 \(p. 408\)](#)。

### Topics

- [登录到您的网关 VTL 本地控制台 \(p. 391\)](#)

- [通过代理路由网关 VTL \(p. 394\)](#)
- [允许您的网关 VTL 通过防火墙和路由器进行访问 \(p. 396\)](#)
- [将您的 AWS Storage Gateway-VTL 配置为使用静态 IP 地址 \(p. 396\)](#)
- [测试您的网关 VTL 与 Internet 的连接 \(p. 399\)](#)
- [同步您的网关 VM 时间 \(p. 399\)](#)
- [配置您的 AWS Storage Gateway-VTL 以使用多个网络适配器 \(NIC\) \(p. 401\)](#)
- [优化 AWS Storage Gateway VTL 性能 \(p. 407\)](#)

## 登录到您的网关 VTL 本地控制台

某些网关维护任务需要您登录到网关的本地控制台。登录后，本地控制台类似于如下所示：



可通过虚拟机监控程序客户端访问本地控制台。您将需要在本地控制台中提供以下登录凭据。

用户: `sguser`

密码: `sgpassword`

登录后，可使用本地控制台中的菜单执行配置任务。

在本主题中，我们向您展示如何访问在 VMware ESXi（请参阅[访问您的网关本地控制台 \(VMware ESXi\) \(p. 391\)](#)）中或 Microsoft Hyper-V（请参阅[访问您的网关本地控制台 \(Microsoft Hyper-V\) \(p. 392\)](#)）中托管的网关的本地控制台。访问控制台后，可登录到控制台（请参阅[登录网关本地控制台 \(p. 394\)](#)）。

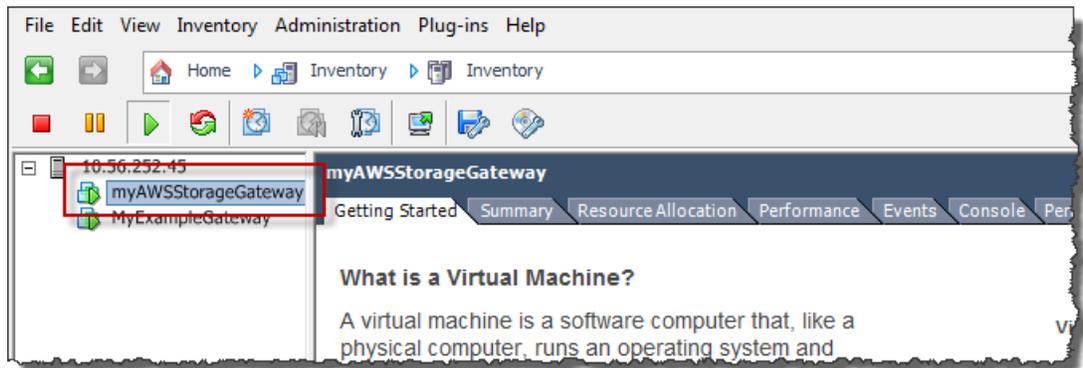
### 访问您的网关本地控制台 (VMware ESXi)

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

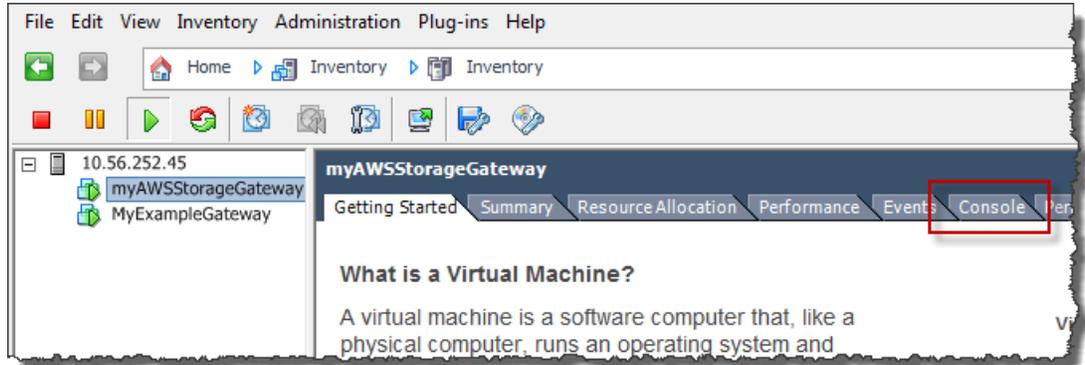


#### Note

如果您的网关 VM 已开启，则有一个绿色箭头图标与 VM 图标一同显示，如下例所示。如果您的网关 VM 未开启，则可通过单击工具栏菜单中的开机图标，将其开启。



3. 单击控制台选项卡。

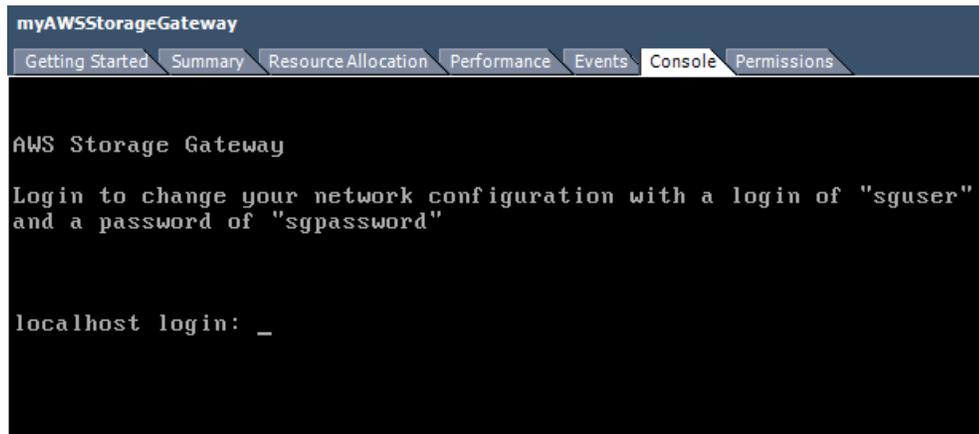


4. 在过几分钟时间后，虚拟机就会准备就绪，供您登录了。



**Note**

要从控制台窗口中释放光标，请按 Ctrl+Alt.



5. 要登录，请继续进行过程[登录网关本地控制台 \(p. 394\)](#)。

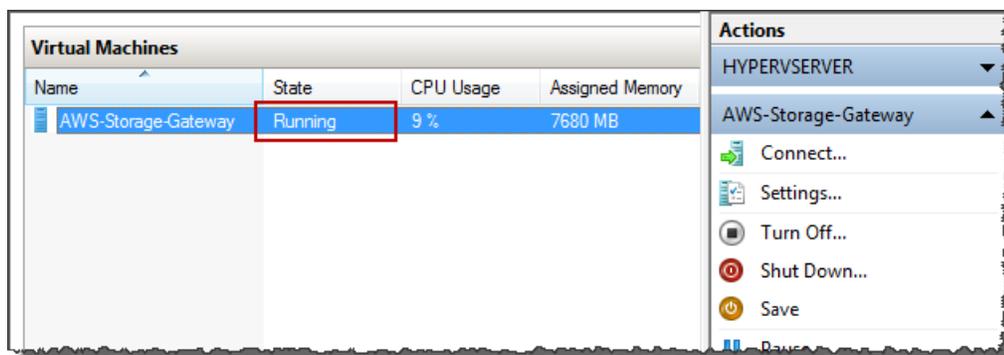
访问您的网关本地控制台 (Microsoft Hyper-V)

1. 在 Microsoft Hyper-V 管理器的虚拟机列表中，选择您的网关 VM。
2. 确保网关已开启。



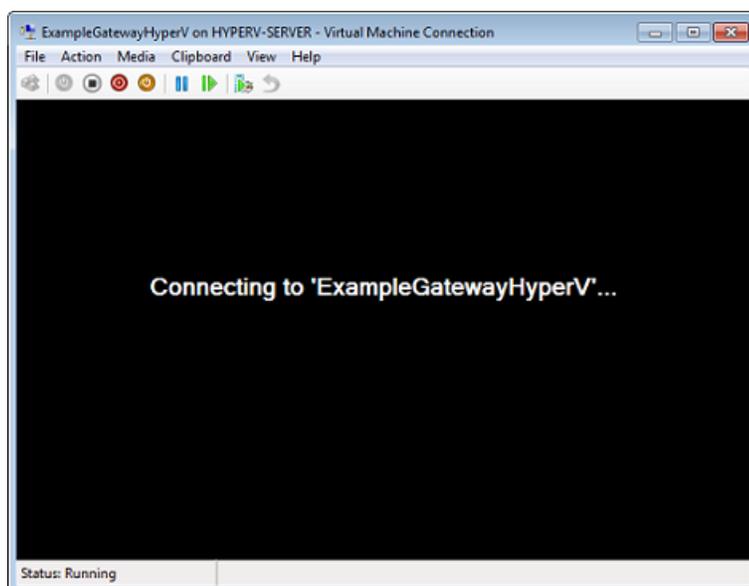
**Note**

如果您的网关 VM 已开启，则显示 `Running` 作为 VM 的状态，如下例所示。如果您的网关 VM 未开启，则可通过单击操作窗格中的开始，将其开启。

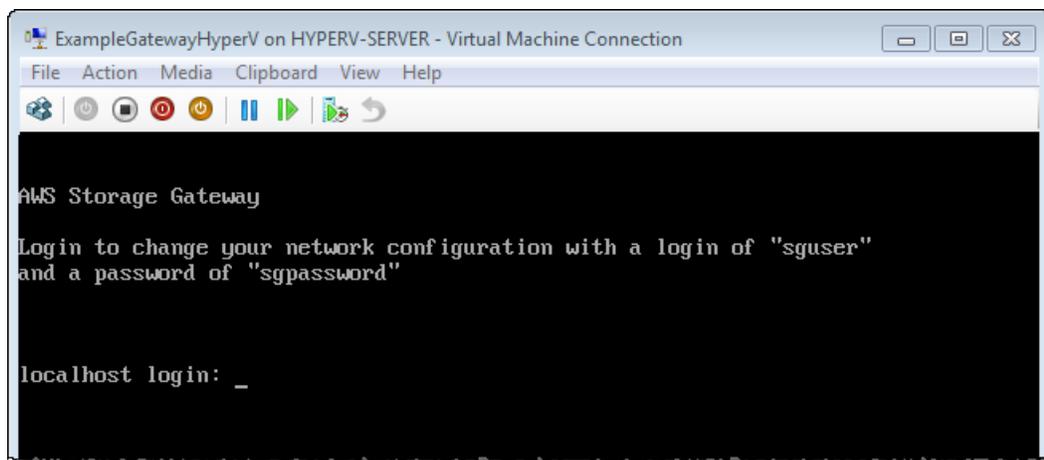


3. 在操作窗格中，选择连接...

随后将显示虚拟机连接窗口。如果显示身份验证窗口，请输入管理程序管理员向您提供的用户名称和密码。



4. 在过几分钟时间后，虚拟机就会准备就绪，供您登录了。



5. 要登录，请继续进行过程[登录网关本地控制台](#) (p. 394)。

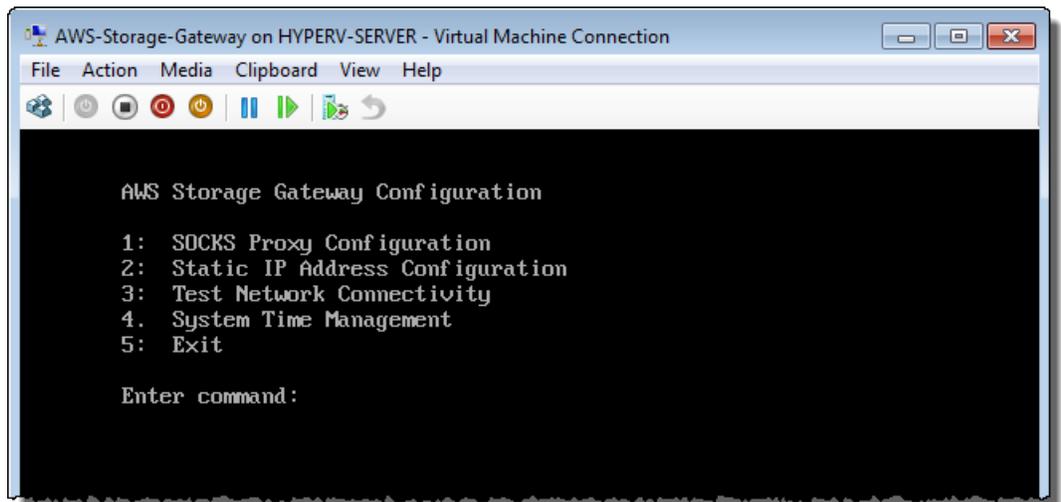
#### 登录网关本地控制台

1. 在登录屏幕中，使用“Console”窗口中指定的用户名称和密码登录到 VM。
2. 登录后，您将看到 AWS Storage Gateway 配置主菜单。



#### Note

对于部署在 Microsoft Hyper-V 上的网关，您还将看到一个用于系统时间管理的菜单项，部署在 VMware ESXi 上的网关没有该菜单项。



如需...	请参见...
为您的网关配置 SOCKS 代理	<a href="#">通过代理路由网关 VTL</a> (p. 394)
为您的网关接口配置静态 IP 地址	<a href="#">将您的 AWS Storage Gateway-VTL 配置为使用静态 IP 地址</a> (p. 396)
测试网关连接性	<a href="#">测试您的网关 VTL 与 Internet 的连接</a> (p. 399)
管理 VM 时间 (仅限 Microsoft Hyper-V)	<a href="#">同步您的网关 VM 时间</a> (p. 399)

## 通过代理路由网关 VTL

AWS Storage Gateway 支持在您的网关 VTL 与 AWS 之间配置 SOCKS5 代理。



#### Note

AWS Storage Gateway 仅支持为 SOCKS5 代理配置。

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 SOCKS 代理设置。为此，请为运行代理的主机指定 IP 地址和端口号，然后 AWS Storage Gateway 将路由所有 HTTPS 流量，使其通过您的代理服务器。

如需将网关的 Internet 流量引导为通过本地代理服务器

1. 登录到网关的本地控制台。有关说明，请参阅[登录到您的网关 VTL 本地控制台 \(p. 391\)](#)。
2. 在 AWS Storage Gateway 配置主菜单中，输入选项 1。



**Note**

对于部署在 Microsoft Hyper-V 上的网关，您还将看到一个用于系统时间管理的菜单项，部署在 VMware ESXi 上的网关没有该菜单项。

```
AWS Storage Gateway Configuration
1: SOCKS Proxy Configuration
2: Static IP Address Configuration
3: Test Network Connectivity
4: Exit

Enter command: _
```

3. 选择 AWS Storage Gateway SOCKS 代理配置菜单中的以下某个选项：

```
AWS Storage Gateway SOCKS Proxy Configuration
1: Configure SOCKS Proxy
2: View Current SOCKS Proxy Configuration
3: Remove SOCKS Proxy Configuration
4: Exit

Enter command: _
```

如需...	请执行此操作...
配置 SOCKS 代理	输入选项 1。 您需要提供主机名称和端口以完成配置。
查看当前的 SOCKS 代理配置	输入选项 2。 如果 SOCKS 代理未配置，“SOCKS Proxy not configured”消息将会显示。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	输入选项 3。 消息“SOCKS Proxy Configuration Removed”显示。
退出该菜单并返回到上一菜单。	输入选项 4。

## 允许您的网关 VTL 通过防火墙和路由器进行访问

您的本地部署网关需要访问下列终端节点，以便与 AWS 进行通信。如果使用防火墙或路由器筛选或限制网络流量，则必须配置防火墙和路由器以允许这些服务终端节点出站与 AWS 通信。

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

下表提供了针对可用地区的地区字符串列表。

地区名称	地区字符串
美国东部 ( 弗吉尼亚北部 )	us-east-1
美国西部 ( 加利福尼亚北部 )	us-west-1
美国西部 ( 俄勒冈 )	us-west-2
欧洲 ( 爱尔兰 )	eu-west-1
亚太地区 ( 东京 )	ap-northeast-1

根据网关地区的不同，可将终端节点中的 *region* 替换为相应的地区字符串。例如，如果在美国西部 ( 俄勒冈 ) 地区创建一个网关，则 Storage Gateway 终端节点将类似于此：

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



### Note

稍后，可以更改这些终端节点，或者添加新的终端节点。

## 将您的 AWS Storage Gateway-VTL 配置为使用静态 IP 地址

网关的默认网络配置是动态主机配置协议 (DHCP)。借助 DHCP，您的网关可获得自动分配的 IP 地址。在某些情况中，您可能需要手动将网关的 IP 地址分配为静态 IP 地址。本主题说明如何进行该配置。

如需将您的网关配置为使用静态 IP 地址。

1. 登录到网关的本地控制台。有关说明，请参阅[登录到您的网关 VTL 本地控制台 \(p. 391\)](#)。
2. 在 AWS Storage Gateway 配置主菜单中，选择选项 2。



### Note

对于部署在 Microsoft Hyper-V 上的网关，您还将看到一个用于系统时间管理的菜单项，部署在 VMware ESXi 上的网关没有该菜单项。

```
AWS Storage Gateway Configuration
1: SOCKS Proxy Configuration
2: Static IP Address Configuration
3: Test Network Connectivity
4: Exit
Enter command: _
```

3. 选择 AWS Storage Gateway 静态 IP 地址配置菜单中的以下某个选项：

```
AWS Storage Gateway Static IP Address Configuration
1: View Network Configuration
2: Configure Static IP
3: View DNS Configuration
4: Reset to DHCP
5: Set Default Route Adapter
6: View Routes
7: Exit
Enter command: _
```

如需...	请执行此操作...
查看网关的网络配置	<p>输入选项 1。</p> <p>适配器列表名称将会显示，并且系统会提示您输入一个适配器名称，例如“eth0”。如果您指定的适配器正在使用中，有关该适配器的下列信息就会显示：</p> <ul style="list-style-type: none"><li>• MAC 地址</li><li>• IP 地址</li><li>• 网络掩码</li><li>• 网关 IP 地址</li><li>• DHCP 启用状态</li></ul> <p>配置静态 IP 地址（选项 2）或设置网关的默认路由适配器（选项 5）时，您使用相同的适配器名称。</p>

如需...	请执行此操作...
<p>为网关配置静态 IP 地址</p>	<p>输入选项 2。</p> <p>系统会提示您输入下列信息以配置静态 IP 地址。</p> <ul style="list-style-type: none"> <li>• 网络适配器名称</li> <li>• IP 地址</li> <li>• 网络掩码</li> <li>• 默认网关地址</li> <li>• 主 DNS 地址</li> <li>• 备用 DNS 地址</li> </ul> <p> <b>Important</b></p> <p>如果已激活您的网关，则必须从 AWS Storage Gateway 控制台中关闭再重新启动网关以使这些设置生效。有关更多信息，请参阅 <a href="#">关停并启动网关 VTL (p. 383)</a>。</p> <p>如果网关使用一个以上的网络接口，您必须将所有启用的接口设置为使用 DHCP 或静态 IP 地址。举例而言，如果网关使用两个配置为 DHCP 的接口，并且您随后将一个接口设置为静态 IP，另一个接口就会禁用。如需启用另一接口，您必须将其设置为静态 IP。如果两个接口最初都设置为使用静态 IP 地址并且您之后将网关设置为使用 DHCP，那么两个接口都必须使用 DHCP。</p>
<p>查看网关的 DNS 配置</p>	<p>输入选项 3。</p> <p>主 DNS 和备用 DND 域名服务器的 IP 地址将会显示。</p>
<p>将网关的网络配置重设为 DHCP</p>	<p>输入选项 4。</p> <p>所有网络接口均设置为使用 DHCP。</p> <p> <b>Important</b></p> <p>如果已激活您的网关，则必须从 AWS Storage Gateway 控制台中关闭再重新启动网关以使这些设置生效。有关更多信息，请参阅 <a href="#">关停并启动网关 VTL (p. 383)</a>。</p>
<p>设置网关的默认路由适配器</p>	<p>输入选项 5。</p> <p>可供网关使用的适配器将会显示，系统会提示您选择任意适配器，例如“eth0”。</p>
<p>查看路由表</p>	<p>输入选项 6。</p> <p>网关的默认路由将会显示。</p>
<p>退出该菜单并返回到上一菜单。</p>	<p>输入选项 7。</p>

## 测试您的网关 VTL 与 Internet 的连接

可使用网关的本地控制台测试 Internet 连接。在解决网络问题时，此测试可能很有用。网关的连接性测试不计入可能已配置的任何 SOCKS 代理。

如需测试网关到 Internet 的连接

1. 登录到网关的本地控制台。有关说明，请参阅[登录到您的网关 VTL 本地控制台 \(p. 391\)](#)。
2. 在 AWS Storage Gateway 配置主菜单中，选择选项 3。



### Note

对于部署在 Microsoft Hyper-V 上的网关，您还将看到一个用于系统时间管理的菜单项，部署在 VMware ESXi 上的网关没有该菜单项。

```
AWS Storage Gateway Configuration
1: SOCKS Proxy Configuration
2: Static IP Address Configuration
3: Test Network Connectivity
4: Exit

Enter command: _
```

网络连接性的测试结果可能是下列各项之一。

连接性是...	消息
成功	AWS Storage Gateway 具有 Internet 连接
不成功	AWS Storage Gateway 没有 Internet 连接

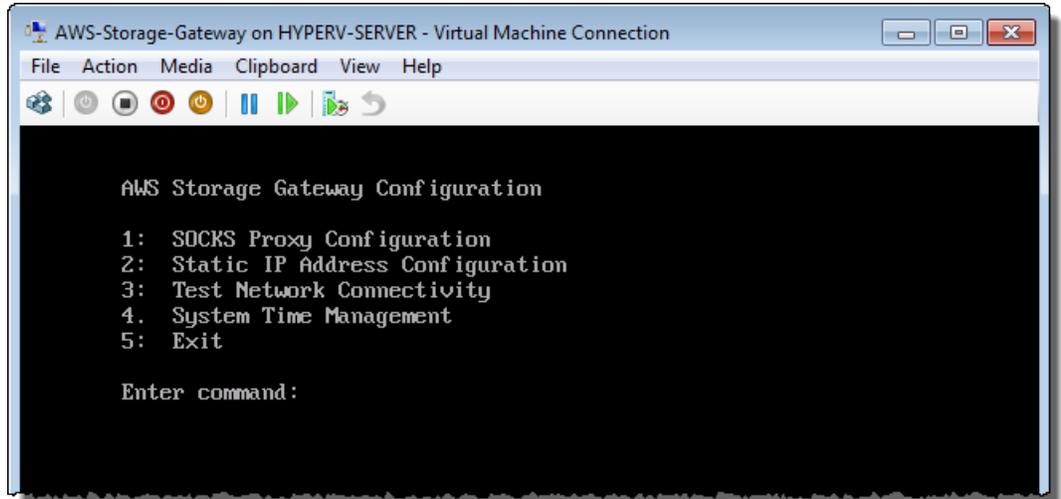
## 同步您的网关 VM 时间

在部署并运行网关后，会存在一些网关 VM 时间出现漂移的情况。例如，如果网络中断时间延长，而您的管理程序主机和网关没有获取时间更新，那么网关 VM 的时间会偏离真正的时间。当出现时间漂移时，操作（如网关更新或者快照）预计出现的时间和操作实际出现的时间之间会出现差异。

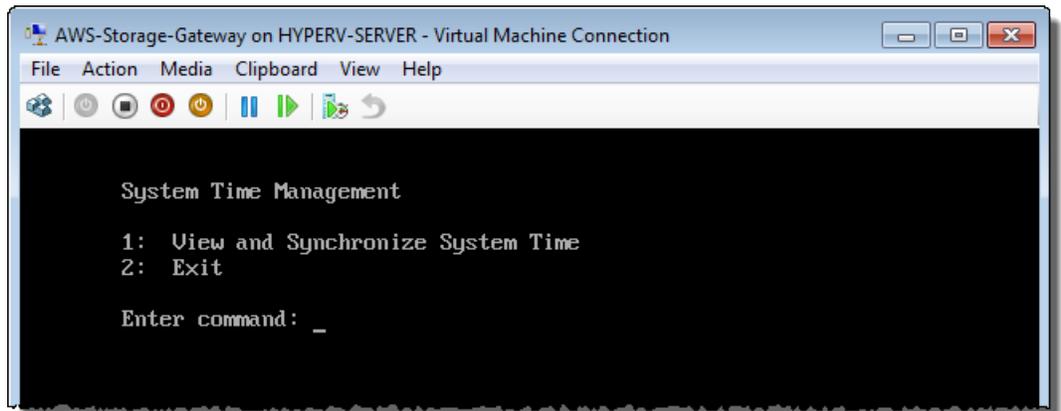
对于 VMware ESXi 上部署的网关，设置管理程序主机的时间和将 VM 时间同步到主机，就足以避免时钟漂移。有关详细信息，请参阅[将 VM 时间与主机时间同步 \(p. 266\)](#)。对于 Microsoft Hyper-V 上部署的网关，您应该定期地使用本部分介绍的操作步骤查看 VM 的时间。

查看 Hyper-V 网关 VM 的时间并将其同步到 NTP 服务器

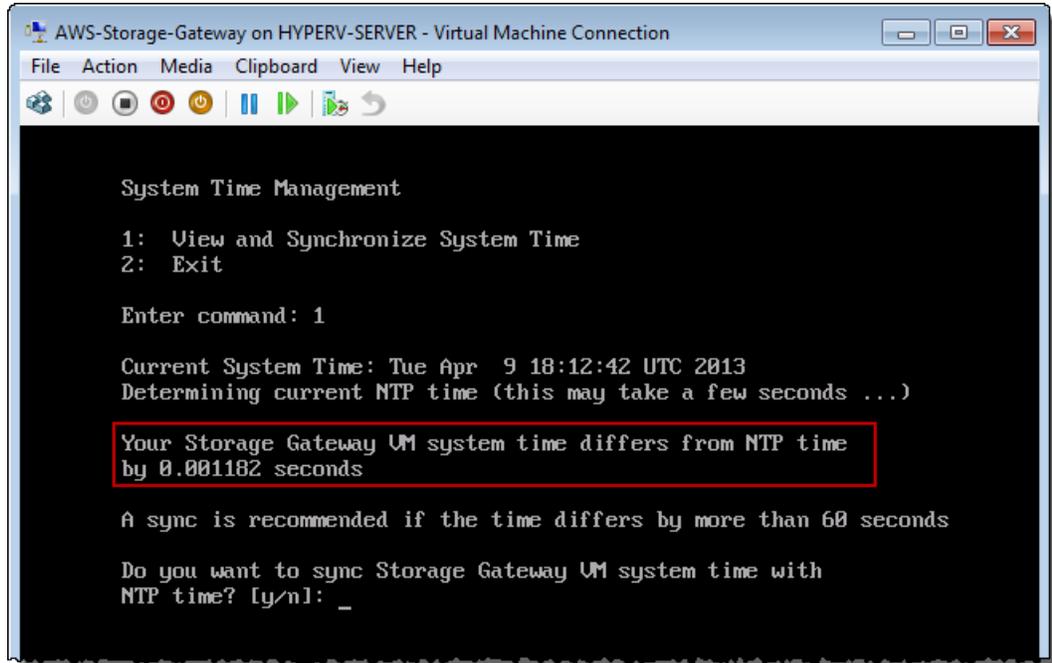
1. 登录到网关的本地控制台。有关说明，请参阅[登录到您的网关 VTL 本地控制台 \(p. 391\)](#)。
2. 在 AWS Storage Gateway 配置主菜单中，选择选项 4 系统时间管理。



3. 在系统时间管理菜单中，选择选项 1 查看和同步系统时间。

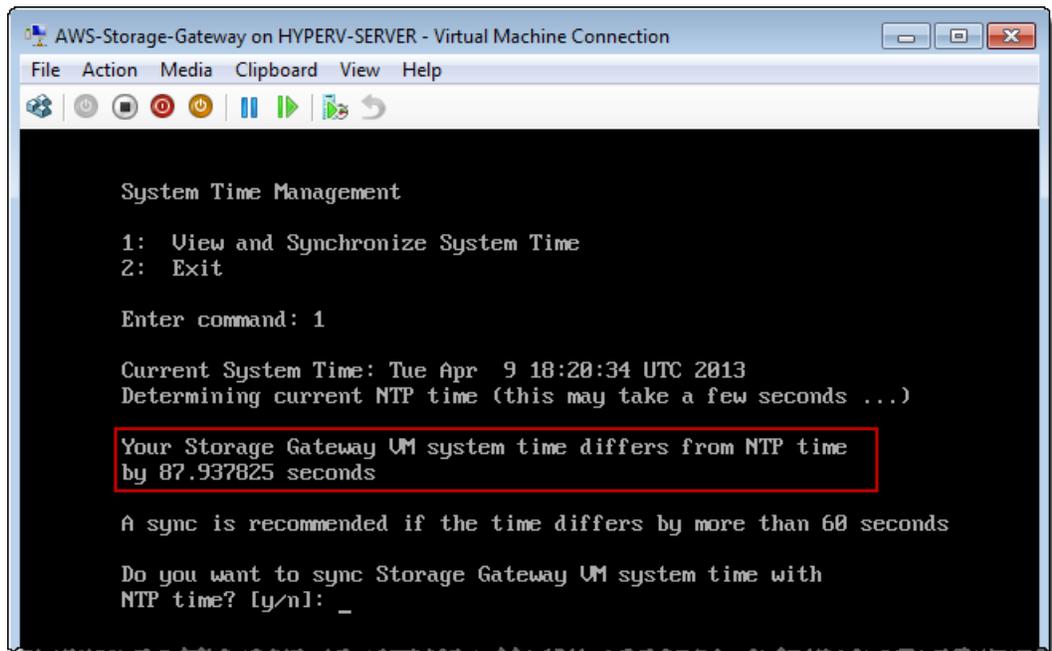


4. 如果结果指示您应同步您的时间，则输入 y；否则输入 n。  
如果输入 y 进行同步，则同步可能需要消耗一段时间。  
下例介绍的 VM 不需要进行时间同步。



```
AWS-Storage-Gateway on HYPERV-SERVER - Virtual Machine Connection
File Action Media Clipboard View Help
System Time Management
1: View and Synchronize System Time
2: Exit
Enter command: 1
Current System Time: Tue Apr 9 18:12:42 UTC 2013
Determining current NTP time (this may take a few seconds ...)
Your Storage Gateway VM system time differs from NTP time
by 0.001182 seconds
A sync is recommended if the time differs by more than 60 seconds
Do you want to sync Storage Gateway VM system time with
NTP time? [y/n]: _
```

下例介绍的 VM 需要进行时间同步。



```
AWS-Storage-Gateway on HYPERV-SERVER - Virtual Machine Connection
File Action Media Clipboard View Help
System Time Management
1: View and Synchronize System Time
2: Exit
Enter command: 1
Current System Time: Tue Apr 9 18:20:34 UTC 2013
Determining current NTP time (this may take a few seconds ...)
Your Storage Gateway VM system time differs from NTP time
by 87.937825 seconds
A sync is recommended if the time differs by more than 60 seconds
Do you want to sync Storage Gateway VM system time with
NTP time? [y/n]: _
```

## 配置您的 AWS Storage Gateway-VTL 以使用多个网络适配器 (NIC)

如果您将网关配置为使用多个网络适配器，网关就可由一个以上的 IP 地址访问。当您希望通过配置网关使用多个网络适配器时，可使用案例，包括：

- 使吞吐量达到最大 – 当网络适配器成为瓶颈时，可能要使网关的吞吐量达到最大。

- 应用程序分隔 – 可能需要分隔应用程序及其如何写入网关的存储卷。举例而言，您可以选择让至关重要的存储应用程序单独使用针对网关定义的一个适配器。
- 网络约束 – 应用程序环境可能需要将 iSCSI 目标及连接到这些目标的发起程序保留在与网关用于与 AWS 通信的网络不同的一个独立网络中。

在典型的多适配器使用案例中，一个适配器会配置为路径，供网关与 AWS 通信使用（默认网关）。除这个适配器外，启动程序所在的子网必须与（包含所连接的 iSCSI 目标的）适配器的相同；否则，可能无法与预定目标通信。如果在用于 AWS 通信的同一个适配器上配置了目标，那么，该目标的 iSCSI 流量和 AWS 流量都将通过同一个适配器。

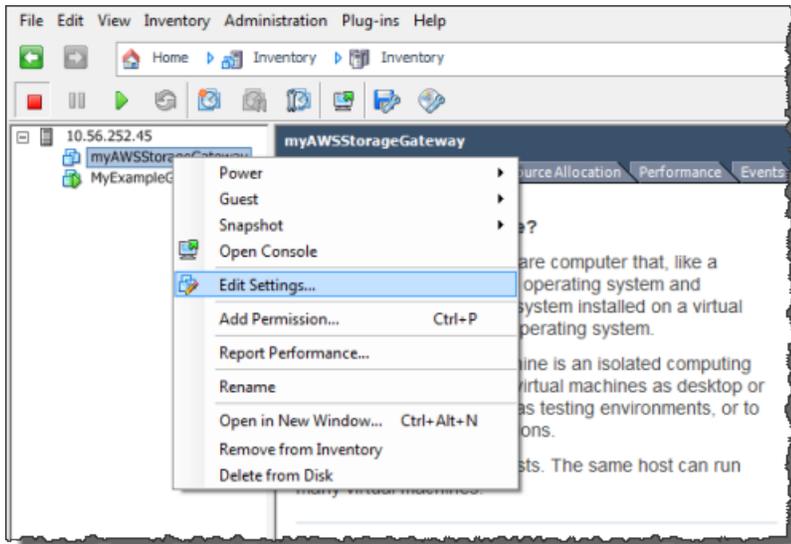
下列步骤假定您的网关 VM 已定义了一个网络适配器，并且您将添加第二个适配器。第一个过程介绍了如何给 VMware ESXi 添加适配器，第二个过程介绍了如何给 Microsoft Hyper-V 添加适配器。

如需将网关配置为使用另一个适用于 VMware ESXi 的网络适配器

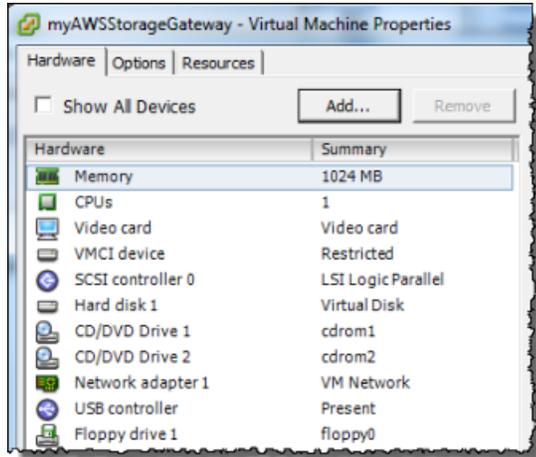
1. 关闭网关。有关详细信息，请参阅 [关停网关 \(p. 383\)](#)。
2. 在 VMware vSphere 客户端中，选择您的网关 VM。

VM 可在执行这些步骤期间保持开启。

3. 在客户端中，右键单击网关 VM 的名称，然后单击编辑设置。

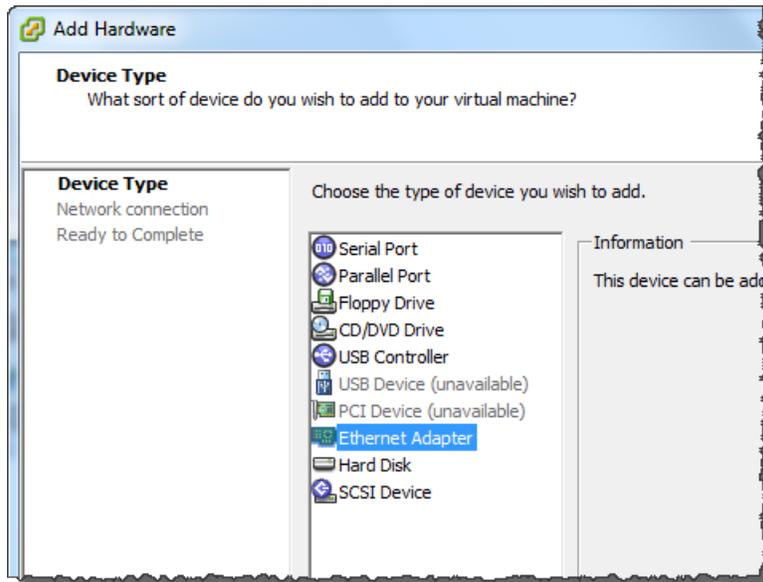


4. 在虚拟机属性对话框的硬件选项卡中，单击添加以添加一个设备。



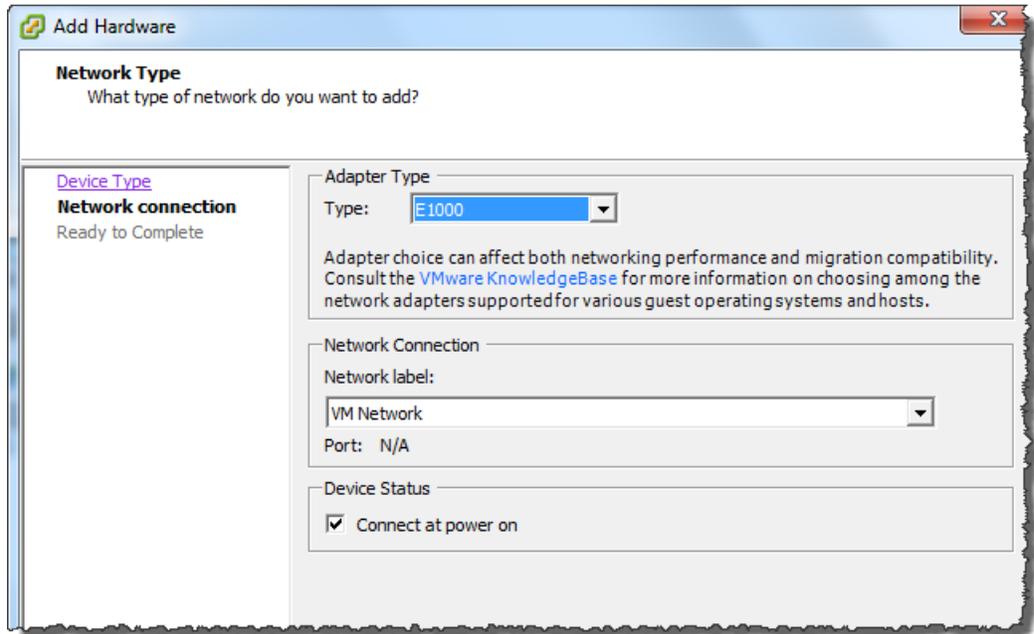
5. 按添加硬件向导添加网络适配器：

- a. 在设备类型窗格中，单击以太网适配器以添加适配器，然后单击下一步。

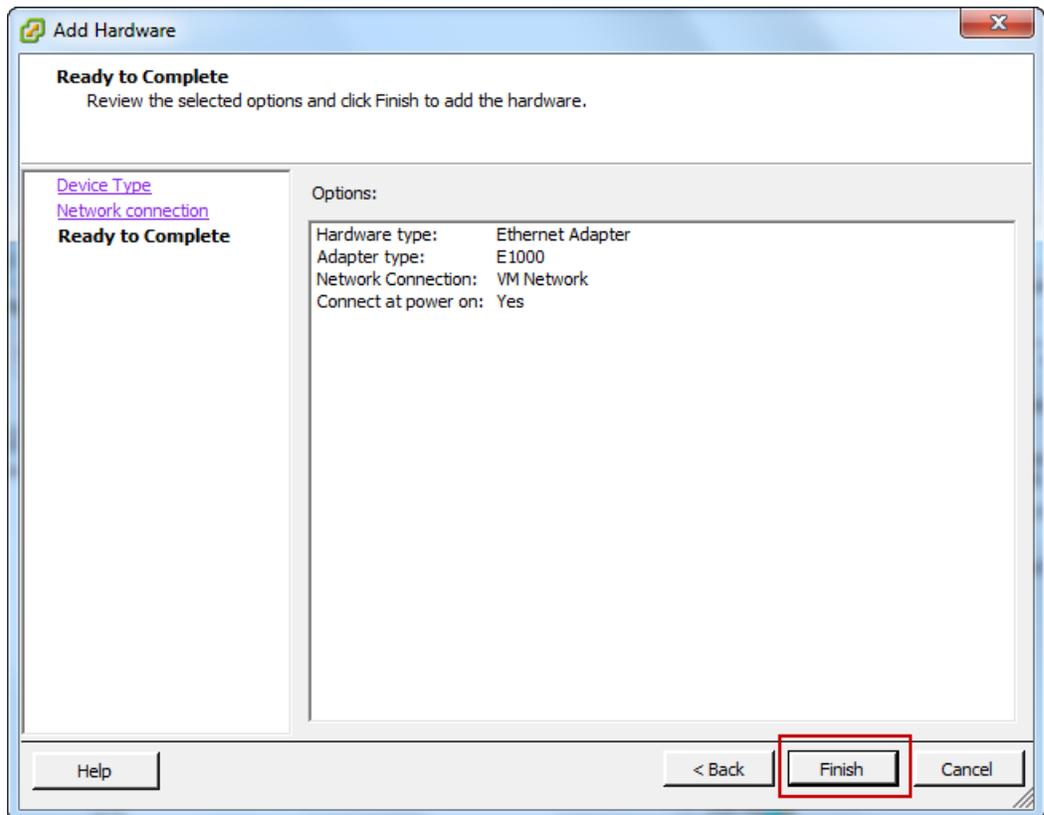


- b. 在网络类型窗格的类型下拉列表中，选择一种适配器类型，确保选中启动时连接，然后单击下一步。

我们建议您将 E1000 网络适配器与 AWS Storage Gateway 一起使用。有关适配器列表中可能出现的适配器类型的详细信息，请参阅 [ESXi](#) 和 [vCenter 服务器文档](#) 中的“网络适配器类型”。



- c. 在已准备好完成窗格中，检查相关信息，然后单击完成。



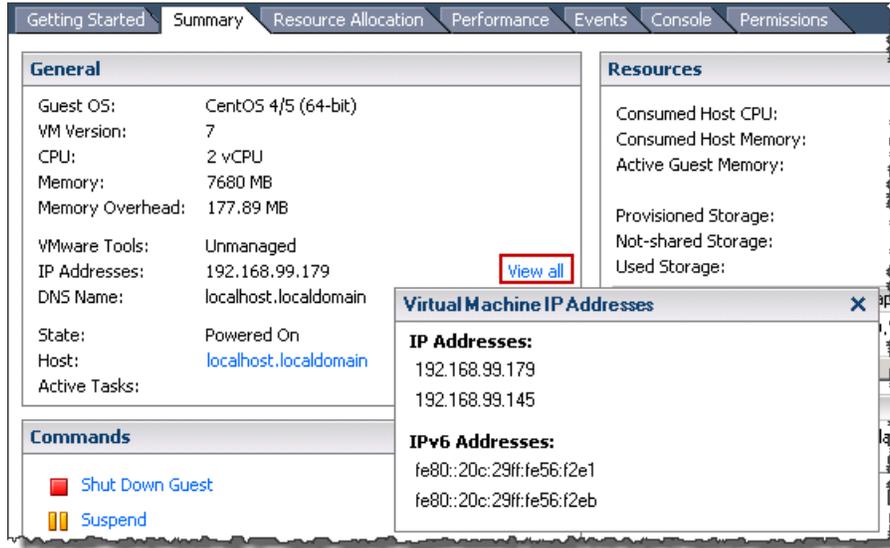
6. 单击 VM 的摘要选项卡，然后单击 IP 地址字段旁的查看全部。虚拟机 IP 地址窗口显示所有可用于访问网关的 IP 地址。确认第二个 IP 地址已针对该网关列出。



### Note

适配器更改生效和 VM 摘要信息刷新可能需要少许时间。

下例仅用于举例说明。在实际工作中，其中的 IP 地址之一将是网关与 AWS 通信的地址，而另一个会是另一子网中的地址。

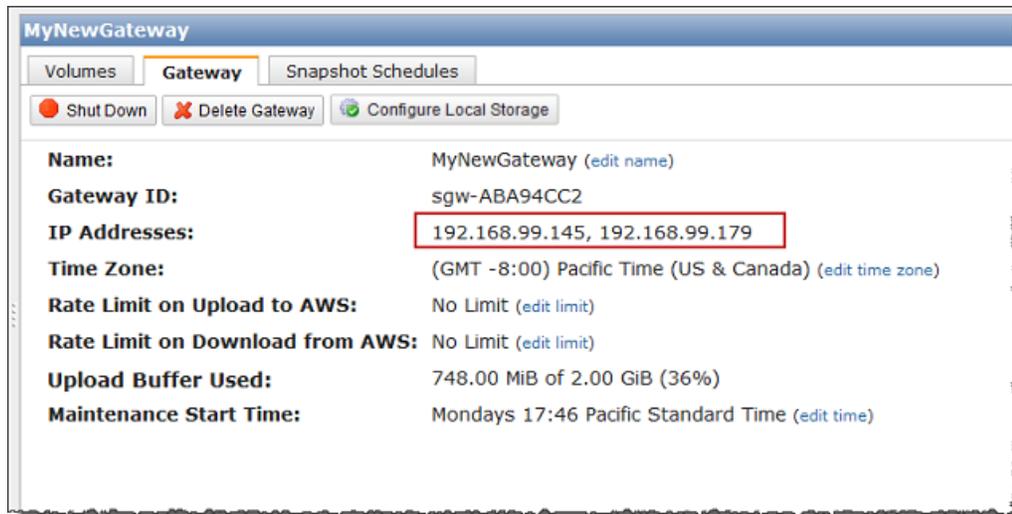


7. 在 AWS Storage Gateway 控制台中，打开网关。

按 [启动网关 \(p. 384\)](#) 中的步骤进行操作，返回此处，然后转到下一步。

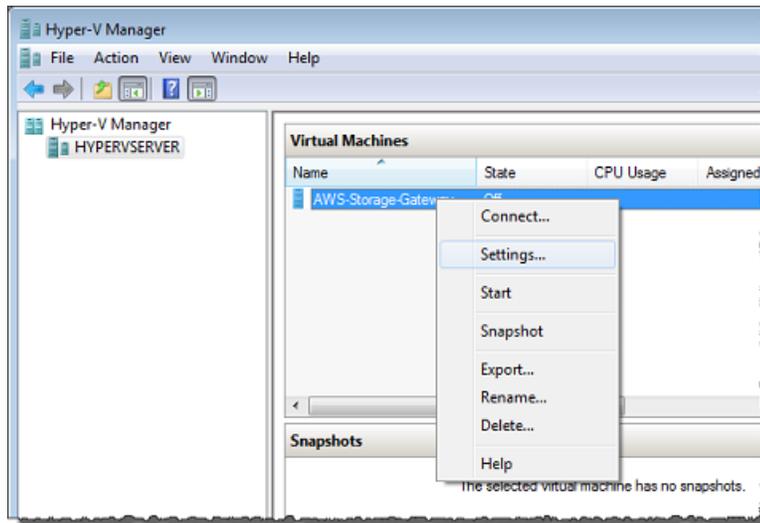
8. 在 AWS Storage Gateway 控制台的导航窗格中，选择将适配器添加到的网关，然后选中网关选项卡。

确认 IP 地址字段中列出了第二个 IP 地址。

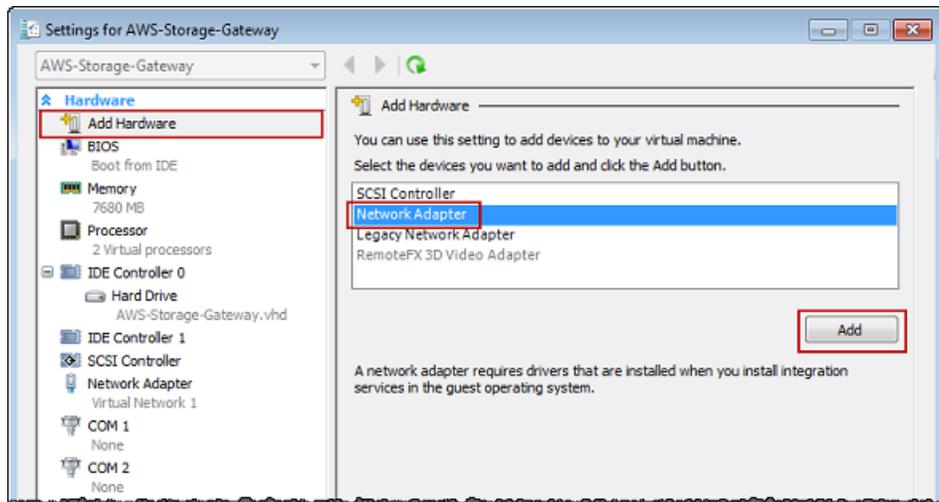


如需将网关配置为使用另一个适用于 Microsoft Hyper-V 的网络适配器

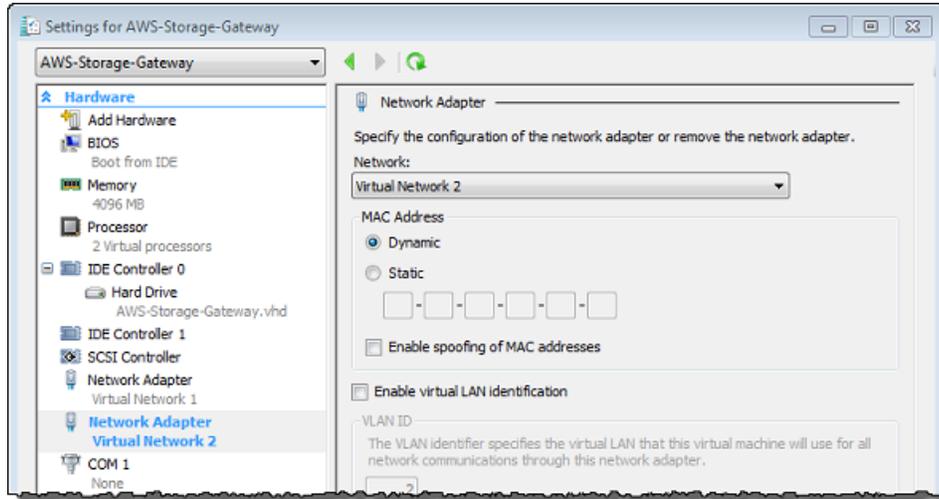
1. 在 AWS Storage Gateway 控制台中，关闭网关。  
按[关闭网关 \(p. 383\)](#)中的步骤进行操作，返回此处，然后转到下一步。
2. 在 Microsoft Hyper-V Manager 中，选择您的网关 VM。
3. 如果没有关闭 VM，请予以关闭。
  - 右键单击网关，然后选择关闭...
4. 在客户端中，右键单击您的网关 VM 的名称，然后单击设置...



5. 在 VM 的设置对话框的硬件列表下，单击添加硬件。
6. 在添加硬件窗格中，选择网络适配器，然后单击添加以添加设备。

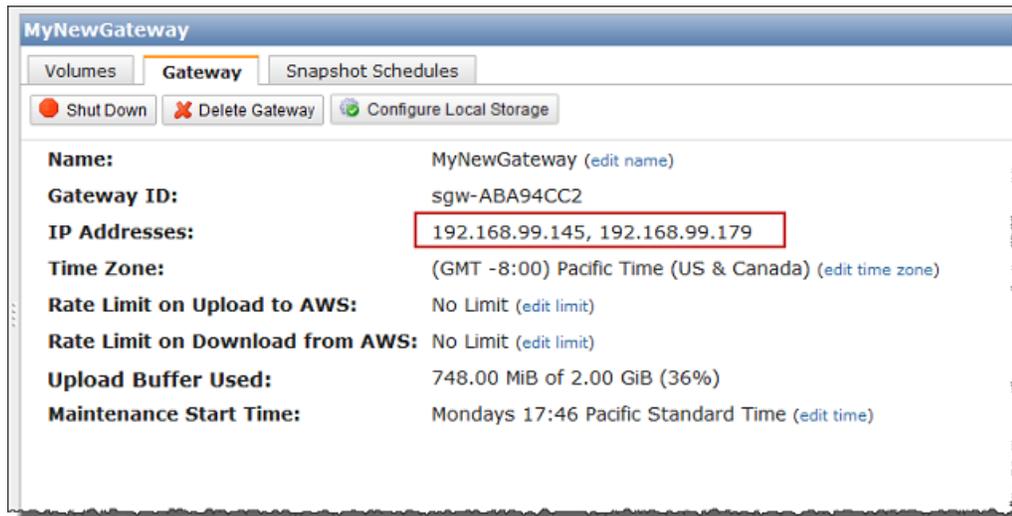


7. 配置网络适配器，然后单击应用。  
在下例中，选择了虚拟网络 2 用于新适配器。



8. 在设置对话框的硬件列表中，确认已添加第二个适配器，然后单击确定。
9. 关闭网关。有关详细信息，请参阅[启动网关 \(p. 384\)](#)
10. 在 AWS Storage Gateway 控制台的导航窗格中，选择将适配器添加到的网关，然后选中网关选项卡。

确认 IP 地址字段中列出了第二个 IP 地址。



## 优化 AWS Storage Gateway VTL 性能

本部分提供有关如何优化网关性能的信息。向网关添加资源以及向应用程序服务器添加资源是这些指导的基础。

### 向您的网关添加资源

- 使用更高性能的磁盘—您可以添加串行连接 SCSI (SAS) 磁盘和固态硬盘 (SSD) 等高性能磁盘，也可以直接从 SAN 连接虚拟磁盘到您的 VM，而不用通过 VMware 的 VMFS 层或 Microsoft Hyper-V 的 NTFS 层连接。更好的磁盘性能一般可取得更好的吞吐量和每秒输入/输出操作 (IOPS)。如需测量吞吐量，请将 ReadBytes 和 WriteBytes 指标与 Samples Amazon CloudWatch 统计数据结合使用。例如，ReadBytes 指标的 Samples 统计数据在五分钟的采样周期内除以 300 秒，可得出每秒输入/输出操作

(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。有关网关指标的更多信息，请参见 [衡量网关 VTL 和 AWS 间的性能 \(p. 363\)](#)。

- 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。您应该确认分配到网关 VM 的四个虚拟处理器由四个核心支持，并且您没有超额预订主机服务器的 CPU。将更多 CPU 添加到网关虚拟服务器时，您并行增加网关处理两方面的能力，即存储应用程序到本地存储器的数据的能力以及上传这些数据到 Amazon S3 的能力。更多 CPU 也可确保您的网关在主机与其他 VM 共享时获得足够的 CPU 资源。这样做一般可以取得更加吞吐量的效果。
- 使用独立物理磁盘支持网关虚拟磁盘—在网关 VTL 设置中配置磁盘时，我们强烈建议您不要为使用相同的底层物理磁盘的上传缓冲区和缓存存储空间配置本地磁盘。同样地，对于网关存储卷设置，强烈建议您不要为使用相同的底层物理磁盘的上传缓冲区和应用程序存储空间预配置本地磁盘。例如，对于 VMware ESXi，底层物理存储资源表示为 VMware ESXi 中的数据存储器。部署网关 VM 时，您选择用来存储 VM 文件的数据存储器。预配置虚拟磁盘时（例如要用作上传缓冲区），您可以选择将虚拟磁盘存储在和 VM 一样的数据存储中。如果您有一个以上的数据存储，强烈建议您选择将一个数据存储用于正在创建的各类本地存储器。仅由一个底层物理磁盘支持，或者仅由一个 RAID 1 等低性能 RAID 配置支持的数据存储器可能在某些情况下导致性能不佳，例如，在同时用来支持一个网关 VTL 设置中的缓存存储空间和上传缓冲区的情况下。

### 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—确保应用程序和网关之间的带宽可维持您的应用程序需求。您可以使用网关的 `ReadBytes` 和 `WriteBytes` 指标（请参见 [衡量网关 VTL 和 AWS 间的性能 \(p. 363\)](#)）来测量总数据吞吐量。将测得的吞吐量与预期的吞吐量比较（针对您的应用程序）。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，您可以提高 VM 和本地磁盘见的带宽（如果非直连）。
- 向应用程序环境添加 CPU 资源—如果您的应用程序可利用更多的 CPU 资源，那么添加更多的 CPU 可让您的应用程序扩展 IO 负载。

## 以 Amazon EC2 实例的形式运行时网关 VTL 的维护任务

本节介绍以 Amazon EC2 实例的形式运行的网关 VTL 的维护任务。有关其他维护任务，请参见 [以 Amazon EC2 实例的形式运行时网关 VTL 的维护任务 \(p. 408\)](#)。

任务	说明
从 EC2 实例中添加或删除 Amazon EBS 卷	可添加或删除卷用于缓存存储和上传缓冲区。（请参见 <a href="#">从网关 VTL 实例中添加和删除 Amazon EBS 卷 (p. 408)</a> ）。
允许或禁止 AWS Support 访问网关	AWS Support 可能需要访问您的网关才能调查和解决问题。（请参见 <a href="#">允许和禁止 AWS Support 访问在 Amazon EC2 实例上运行的网关 (p. 409)</a> ）。
配置安全组	网关需要进行某些端口配置才能正常运行。在安全组中配置这些设置以拒绝或允许访问您的 EC2 实例（请参见 <a href="#">为 Amazon EC2 网关 VTL 实例配置安全组 (p. 410)</a> ）。
清除	如果不打算继续使用网关，则应释放所有 AWS 资源，以使您不再产生费用。（请参见 <a href="#">在 EC2 网关 VTL 练习后进行清除 (p. 410)</a> ）。

### 从网关 VTL 实例中添加和删除 Amazon EBS 卷

最初配置网关 VTL 以 EC2 实例的形式运行时，分配了 EBS 卷用作缓存存储和上传缓冲区。根据应用程序需求随时间的变化，可添加 EBS 卷用作上传缓冲区和缓存存储。还可通过删除以前分配的 EBS 卷，减

少存储。有关 Amazon EBS 的详细信息，请转到 *Amazon Elastic Compute Cloud 用户指南* 中的 [Amazon 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 VTL 的应用程序需求调整上传缓冲区和缓存存储的大小（[配置上传缓冲区的大小（网关 VTL）](#)（p. 316）和[配置缓存存储空间大小](#)（p. 319））。

可分配为上传缓冲区和缓存存储的最大存储受到限制。可向实例附加所需数量的 EBS 卷，但是，将这些卷配置为上传缓冲区和缓存存储时必须遵守这些限制。有关更多信息，请参阅 [附录 F：AWS Storage Gateway 限制](#)（p. 457）。

创建 Amazon EBS 卷，附加它，并为网关 VTL 配置它

1. 创建一个 EBS 卷。有关说明，请转到 *Amazon Elastic Compute Cloud 用户指南* 中的 [创建或还原 Amazon EBS 卷](#)。
2. 将该 EBS 卷附加到您的 Amazon EC2 实例。有关说明，请转到 *Amazon Elastic Compute Cloud 用户指南* 中的 [将 Amazon EBS 卷附加到实例](#)。
3. 将所添加的 Amazon EBS 卷配置为上传缓冲区或缓存存储。有关说明，请参阅 [配置上传缓冲区和缓存存储空间](#)（p. 346）。

删除 Amazon EBS 卷

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。



#### Warning

这些步骤仅适用于分配为上传缓冲区的 EBS 卷。如果删除分配为缓存存储的 EBS 卷，则网关上的磁带将变为“无法恢复”，而您将面临丢失数据的风险（请参阅 [磁带状态信息](#)（p. 372））。

1. 按照 [关停并启动网关 VTL](#)（p. 383）中的步骤关闭网关。
2. 从您的 EC2 实例中分离该 EBS 卷。有关说明，请转到 *Amazon Elastic Compute Cloud 用户指南* 中的 [从实例中分离 Amazon EBS 卷](#)。
3. 删除该 EBS 卷。有关说明，请转到 *Amazon Elastic Compute Cloud 用户指南* 中的 [删除 Amazon EBS 卷](#)。
4. 按 [关停并启动网关 VTL](#)（p. 383）中的步骤启动网关。

## 允许和禁止 AWS Support 访问在 Amazon EC2 实例上运行的网关

可允许 AWS Support 访问网关以帮助解决问题。

允许 AWS Support 访问 Amazon EC2 实例上的网关 VTL

1. 如果您启动实例时指定的安全组不包含运行 SSH（端口 22）访问的规则，请添加该规则。

有关如何向安全组添加规则的说明，请转到 *Amazon Elastic Compute Cloud 用户指南* 中的 [Amazon EC2 安全组](#)。

2. 要允许 AWS Support 进行访问，请使用以下命令。

```
ssh -i IDENTITY_FILE sguser@INSTANCE_IP_ADDRESS grant-aws-support-access
```

其中 *IDENTITY\_FILE* 是在创建该实例时所用密钥对的 .pem 私钥文件，而 *INSTANCE\_IP\_ADDRESS* 是该网关的公共 IP 地址。有关如何查找公用 IP 地址的信息，请参阅在 [Amazon EC2 上部署并激活网关 VTL](#)（p. 341）中的第 7 步。

## 禁止 AWS Support 访问部署在 Amazon EC2 上的网关

1. 要禁止 AWS Support 进行访问，请使用以下命令。

```
ssh -i IDENTITY_FILE sguser@INSTANCE_IP_ADDRESS revoke-aws-support-access
```

其中 *IDENTITY\_FILE* 是在创建该实例时所用密钥对的 .pem 私钥文件，而 *INSTANCE\_IP\_ADDRESS* 是该网关的 IP 地址。

2. 如果配置安全组时添加了任何规则，则应删除这些规则。有关说明，请转到 *Amazon Elastic Compute Cloud 用户指南* 中的[从安全组中删除规则](#)。

## 为 Amazon EC2 网关 VTL 实例配置安全组

安全组控制发往 Amazon EC2 网关实例的流量。从 AWS Marketplace 提供的 AWS Storage Gateway AMI 创建实例时，可选择两种方法启动实例。在[在 Amazon EC2 上部署并激活网关 VTL \(p. 341\)](#)中，我们展示了使用 AWS Marketplace 的与 EC2 控制台一同启动功能启动实例。推荐您使用这种方法。也可使用 AWS Marketplace 中的单键启动功能启动实例。在这种情况下，将创建自动生成的安全组 `AWS Storage Gateway-1-0-AutogenByAWSMP-`。这个安全组拥有正确的端口 (80) 规则，可让您激活您的网关。有关安全组的详细信息，请转到 *Amazon Elastic Compute Cloud 用户指南* 中的[安全组概念](#)。

无论您使用的是何种安全组，我们建议：

- 安全组不应该允许从外部 Internet 传入的连接；它应该只允许该装置的安全组与该装置“交谈”。如果您必须允许实例从该装置的安全组外面连接该装置，我们建议您只允许端口 3260（适用于 iSCSI）和端口 80（适用于激活）上的连接。
- 您应该仅在使用 AWS Support 进行故障诊断用途时，允许端口 22 上的访问。有关更多信息，请参阅[允许和禁止 AWS Support 访问在 Amazon EC2 实例上运行的网关 \(p. 409\)](#)。
- 如果您希望从设备安全组外的主机激活设备，就需要允许该主机的 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，可以打开端口 80、激活网关并在完成激活后关闭端口上的访问。

如果要使用 Amazon EC2 实例作为发起程序，即连接到在 Amazon EC2 上部署的网关上的 iSCSI 目标，则有两种方法。

1. 可将发起程序实例放入与网关相同的安全组。
2. 将需要配置访问权限，以使发起程序可与网关通信。

## 在 EC2 网关 VTL 练习后进行清除

如果曾使用本指南中的练习部署并激活 EC2 网关 VTL，并且不想继续使用您的网关 VTL，则要考虑删除网关和相关资源。有关信息，请参阅[在 Amazon EC2 上部署并激活网关 VTL \(p. 341\)](#)。

我们建议按以下操作顺序删除以 EC2 实例的形式运行的网关和相关资源。删除多余的资源可帮助减少每月支出。

1. 从网关中删除所有状态为“正在检索”的虚拟磁带 – 请参阅[取消磁带检索 \(p. 374\)](#)。
2. 删除所有已检索到网关的磁带 – 请参阅[从网关 VTL 的虚拟磁带库中删除磁带 \(p. 373\)](#)。
3. 从虚拟磁带库 (VTL) 中删除虚拟磁带 – 请参阅[从网关 VTL 的虚拟磁带库中删除磁带 \(p. 373\)](#)。
4. 删除网关 VTL – 请参阅[删除网关 VTL \(p. 390\)](#)。
5. 终止所有 Amazon EC2 实例并删除所有 EBS 卷 – 请参阅 *Amazon Elastic Compute Cloud 用户指南* 中的[清除实例和卷](#)。
6. 从虚拟磁带架 (VTS) 中删除所有已存档的虚拟磁带 – 请参阅[从 VTS 中删除磁带 \(p. 378\)](#)。



### Important

在 VTS 中存储 90 天内检索磁带将收取最低 90 天的存储费用。

## 网关 VTL 问题排查

本部分讨论排查网关相关以及存储卷相关的问题。网关问题排查分为两个部分：本地网关和部署到 Amazon EC2 的网关。场内网关故障诊断问题涵盖 VMware ESXi 或者 Microsoft Hyper-V 平台上部署的网关。存储卷的故障诊断问题适用于所有网关类型。

### Topics

- [排查场内网关问题 \(p. 411\)](#)
- [排查 Amazon EC2 网关问题 \(p. 412\)](#)

## 排查场内网关问题

下表列出了您在使用本地网关时可能遇到的典型问题。

问题	措施
您找不到网关的 IP 地址。	<p>请使用管理程序客户端连接主机，以便查找网关 IP 地址。</p> <ul style="list-style-type: none"><li>• 对于 VMware ESXi，可在摘要选项卡上的 vSphere 客户端中找到 VM 的 IP 地址（请参见 <a href="#">激活部署在 VMware ESXi 主机上的 AWS Storage Gateway-VTL (p. 323)</a>）。</li><li>• 对于 Microsoft Hyper-V，可登录本地控制台查找 VM 的 IP 地址。</li></ul> <p>如果您仍然难以找到网关 IP 地址：</p> <ul style="list-style-type: none"><li>• 检查 VM 是否已启动。仅在 VM 已启动的情况下，IP 地址才会分配给您的网关。</li><li>• 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顺序。</li></ul>
当您单击 AWS Storage Gateway 控制台中的继续激活按钮时，网关的激活过程将失败。	<ul style="list-style-type: none"><li>• 检查网关 VM 是否可通过从客户端 ping 通。</li><li>• 检查 VM 是否有到 Internet 的网络连接；如果没有，您可能需要配置 SOCKS 代理。有关更多信息，请参见 <a href="#">通过代理路由网关 VTL (p. 394)</a>。</li><li>• 检查主机是否具有正确的时间且配置为自动将其时间同步到网络时间协议 (NTP) 服务器，并检查网关 VM 是否具有正确的时间。有关同步管理程序主机和 VM 时间的信息，请参见 <a href="#">同步您的网关 VM 时间 (p. 399)</a>。</li><li>• 执行这些步骤后，您可以使用 AWS Storage Gateway 控制台和设置并激活网关向导重新尝试网关部署。</li><li>• 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，请参见 <a href="#">要求 (p. 7)</a>。</li></ul>

问题	措施
您需要移除分配为上传缓冲区的一个磁盘，因为您希望降低网关上传缓冲区空间的量或者您需要替换用作上传缓冲区的已失效磁盘。	有关移除分配为上传缓冲区的磁盘的指导，请参见 <a href="#">删除上传缓冲区容量 (网关 VTL)</a> (p. 380)
您需要提高网关和 AWS 之间的带宽。	您可以在 NIC 上设置一个独立于您的应用程序和网关 VM 之间的连接的通往 AWS 的 Internet 连接，从而提高网关到 AWS 之间的带宽。在您拥有到 AWS 的高带宽连接并且希望避免带宽争用的情况下（尤其是在快照还原期间），这样做很有用处。对于高吞吐量工作负载需求，您可以使用 <a href="#">AWS Direct Connect</a> 在本地网关和 AWS 间建立专用网络连接。若要测量从网关到 AWS 的连接带宽，请使用网关的 CloudBytesDownloaded 和 CloudBytesUploaded 指标（请参见 <a href="#">衡量网关 VTL 和 AWS 间的性能</a> (p. 363)）。提高 Internet 连接性能有助于确保您的上传缓冲区不被填满。
往返您的网关的吞吐量将为零。	<ul style="list-style-type: none"> <li>在 AWS Storage Gateway 控制台中的网关选项卡上，验证网关 VM 的 IP 地址是否与您在使用管理程序客户端软件（即 VMware vSphere 客户端或者 Microsoft Hyper-V Manager）中看到的相同。如果您发现了不一致，请从 AWS Storage Gateway 控制台重启网关，如 <a href="#">关停并启动网关 VTL</a> (p. 383) 中所述。在重新启动后，AWS Storage Gateway 控制台的网关选项卡中的 IP 地址字段应该匹配您从管理程序客户端中确定的网关 IP 地址。</li> <li>对于 VMware ESXi，可在摘要选项卡上的 vSphere 客户端中找到 VM 的 IP 地址（请参见 <a href="#">激活部署在 VMware ESXi 主机上的 AWS Storage Gateway-VTL</a> (p. 323)）。</li> <li>对于 Microsoft Hyper-V，可登录本地控制台查找 VM 的 IP 地址。</li> <li>按 <a href="#">测试您的网关 VTL 与 Internet 的连接</a> (p. 399) 中所述，检查网关到 AWS 的连接性。</li> <li>检查网关的网络适配器配置，同时确保您打算为网关启动的所有接口均已启用。若要查看网关的网络适配器配置，请遵循 <a href="#">将您的 AWS Storage Gateway-VTL 配置为使用静态 IP 地址</a> (p. 396) 的指示并选择用于查看网关的网络配置的选项。</li> </ul> <p>您可以从 Amazon CloudWatch 控制台查看往返网关的吞吐量。有关测量网关到 AWS 之间吞吐量的更多信息，请参见 <a href="#">衡量网关 VTL 和 AWS 间的性能</a> (p. 363)。</p>
您在 Microsoft Hyper-V 上导入（部署）AWS Storage Gateway 时遇到问题。	请参见附录中的 <a href="#">故障诊断 Microsoft Hyper-V 设置</a> (p. 453)。那里的提示涵盖一些您在 Microsoft Hyper-V 上部署网关时遇到的常见问题。

## 排查 Amazon EC2 网关问题

下表列出了您在使用部署到 Amazon Elastic Compute Cloud (Amazon EC2) 的网关时可能遇到的典型问题。有关本地网关和 Amazon EC2 中部署的网关之间的区别的详细信息，请参见 [在 Amazon EC2 上部署并激活 AWS Storage Gateway](#) (p. 133)。

问题	措施
当您单击 AWS Storage Gateway 控制台中的继续激活按钮时，Amazon EC2 网关的激活过程将失败。	<p>如果过了一会激活仍未出现，请在 Amazon EC2 控制台中检查下列内容：</p> <ul style="list-style-type: none"> <li>已在实例关联的安全组中启用端口 80。有关添加安全组规则的详细信息，请转到 <i>Amazon Elastic Compute Cloud 用户指南</i> 中的<a href="#">添加安全组规则</a>。</li> <li>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”。</li> </ul> <p>在纠正问题后，请转到 AWS Storage Gateway 控制台，单击在 Amazon EC2 上部署新的网关，并重新输入实例的 IP 地址来尝试再次激活网关。</p>
您在实例的列表找不到 Amazon EC2 网关实例。	<p>例如，如果您没有为实例提供资源标签，同时还有许多实例在运行，因此很难了解您在网关中部署了哪些实例，那么可以采取下列操作查找网关实例：</p> <ul style="list-style-type: none"> <li>在实例的说明选项卡中，查看亚马逊系统映像 (AMI) 名称。基于 AWS Storage Gateway AMI 的实例应该以“aws-storage-gateway-ami”文本开头。</li> <li>如果您的实例不是基于 AWS Storage Gateway AMI，请查看实例的启动时间以查找正确的实例。</li> </ul>
您创建了 Amazon EBS 卷，但不能将其附加到 Amazon EC2 网关实例。	<p>查看与网关实例在同一可用区域中的有问题的 Amazon EBS 卷。如果可用区域中存在不一致，请在您的实例所在的同一可用区域中创建一个新的 Amazon EBS 卷。</p>
您不能将启动程序附加到 Amazon EC2 网关的存储卷目标上。	<p>查看启动实例时使用的安全组，其中包括的规则是否允许使用针对 iSCSI 的端口。端口通常设置为 3260。有关连接到存储卷的更多信息，请参见<a href="#">配置应用程序对存储卷的访问 (p. 153)</a>。</p>
您激活了 Amazon EC2 网关，但在添加存储卷时，收到错误消息，表示您没有可用的磁盘空间。	<p>没有为新激活的网关定义卷存储。在定义卷存储前，必须将本地磁盘分配给网关，以便用作上传缓冲区空间和缓冲存储。对于部署到 Amazon EC2 的网关，本地磁盘是附加到实例的 Amazon EBS 卷。这个错误消息很可能是因为没有为实例定义 Amazon EBS 卷而出现。查看为运行网关的实例所定义的块存储设备。如果只存在两个块存储设备（AMI 具有的默认设备），那么应该添加存储（请参见在<a href="#">Amazon EC2 上部署并激活 AWS Storage Gateway (p. 133)</a>）。在附加两个或更多的 Amazon EBS 卷后，尝试在网关上创建卷存储。</p>
您必须移除为用作上传缓冲区空间而分配的磁盘，因为要减少上传缓冲区空间大小。	<p>按<a href="#">从 Amazon EC2-托管的网关中删除 Amazon EBS 卷 (p. 141)</a> 中的步骤操作。</p>
往返您的 Amazon EC2 网关的吞吐量将为零。	<ul style="list-style-type: none"> <li>验证网关实例是否在运行。例如，如果实例因为重新启动而正在启动，请等待该实例重新启动。</li> <li>验证是否尚未更改网关 IP。如果实例停止然后重新启动，那么实例的 IP 地址可能会出现更改。在这种情况下，您必须重新激活新的网关。</li> </ul> <p>您可以从 Amazon CloudWatch 控制台查看往返网关的吞吐量。有关测量网关到 AWS 之间吞吐量的更多信息，请参见<a href="#">衡量网关和 AWS 间的性能 (p. 246)</a>。</p>



### Warning

对于部署在 Amazon EC2 实例上的 Amazon Storage Gateway，不支持通过公共 Internet 访问网关。无法使用 EC2 实例的弹性 IP 地址作为目标地址。

# 使用 AWS Identity and Access Management (IAM) 进行访问控制

AWS Identity and Access Management (IAM) 帮助您安全地控制对 Amazon Web Services 和账户资源的访问。借助 IAM，您可以在 AWS 账户下创建多个用户。要详细了解 IAM 及其功能，请转到 [IAM 是什么？](#)

您在 IAM 系统中创建的每个用户起初均没有任何权限。换言之，用户按默认不能进行任何操作。“权限”是一个通用术语，我们用它表示可针对某个资源执行某项操作。通过 AWS Storage Gateway API（请参阅 [AWS Storage Gateway 的 API 参考 \(p. 418\)](#)），可执行一系列操作。但是，除非您明确向某用户授予权限，该用户就不能执行任何这些操作。您借助策略向用户授予权限。策略是一个文档，其中正式声明一项或多项权限。有关 IAM 策略的详细信息，请转到 [策略概述](#)。

您使用 IAM 用户所用的访问策略语言编写策略。然后可以将该策略关联到 AWS 账户中的某个用户或组。有关策略语言的详细信息，请参阅 [使用 IAM](#) 中的 [访问策略语言](#)。

[使用 IAM 的元素描述](#) 一节介绍可在策略中使用的元素。下列有关部分策略要素的信息专属于 AWS Storage Gateway：

- 资源—策略涉及的数据元。您使用下面的亚马逊资源名称 (ARN) 格式标识资源。

```
arn:aws:<vendor>:<region>:<namespace>:<relative-id>
```

在此格式中，*vendor* 为产品名称“storagegateway”，*namespace* 为账户 ID。在 AWS Storage Gateway 中，有三种类型的资源：gateway、volume 和 iSCSITarget。下表显示了各类型资源的示例 ARN。

资源	说明
网关 ARN	arn:aws:storagegateway:us-east-1:111122223333:gateway/mygateway
卷 ARN	arn:aws:storagegateway:us-east-1:111122223333:gateway/mygateway/volume/vol-1122AABB
目标 ARN (iSCSI 目标名称)	arn:aws:storagegateway:us-east-1:111122223333:gateway/mygateway/target/qn.1997-05.com:amazon:myvolume

- 操作—允许或拒绝的特定操作类型。有关 AWS Storage Gateway 操作的完整列表，请参阅 [AWS Storage Gateway 中的操作 \(p. 438\)](#)。

**Note**

从 AWS Storage Gateway 生成的 Amazon EBS 快照作为 Amazon EC2 资源和相应 EC2 操作进行管理。

本部分提供了示例 IAM 策略，描述如何向用户授予权限以执行具体的 AWS Storage Gateway 操作。然后您可以将这些策略附加到您希望授予访问权限的用户。

## 示例策略

### Example 1: 允许所有操作

下面的策略允许用户执行所有的 AWS Storage Gateway 操作。该策略还允许用户对从 AWS Storage Gateway 生成的 Amazon EBS 快照执行 Amazon EC2 操作 ([DescribeSnapshots](#) 和 [DeleteSnapshot](#))。

```
{ "Statement": [ { "Action": [ "storagegateway:*" ], "Effect": "Allow", "Resource": "*" }, { "Action": [ "ec2:DescribeSnapshots", "ec2:DeleteSnapshot" ], "Effect": "Allow", "Resource": "*" } ] }
```

### Example 2: 允许对网关进行只读访问

以下策略允许对所有资源进行所有 List\* 和 Describe\* 操作。请注意这些操作是读取操作。因此，该策略不允许用户更改任何资源的状态—即该策略不允许用户执行 DeleteGateway、ActivateGateway 和 ShutdownGateway 等操作。

该策略还允许进行 DescribeSnapshots Amazon EC2 操作。有关详细信息，请转到 *Amazon Elastic Compute Cloud API Reference* 中的 [DescribeSnapshots](#)。

```
{ "Statement": [ { "Action": [ "storagegateway:List*", "storagegateway:Describe*" ], "Effect": "Allow", "Resource": "*" }, { "Action": [ "ec2:DescribeSnapshots" ], "Effect": "Allow", "Resource": "*" } ] }
```

在上一策略中，除使用通配符外，您也可以将该策略涵盖的资源范围限定到某个具体网关。然后，该策略将仅在具体网关上允许这些操作。

```
"Resource": "arn:aws:storagegateway:us-east-1:111122223333:gateway/[Gateway Name]/*"
```

在网关内，您可以进一步将资源范围仅限制网关卷。

```
"Resource": "arn:aws:storagegateway:us-east-1:111122223333:gateway/[Gateway Name]/volume/*"
```

### Example 3: 允许访问某个特定的网关

下面的策略允许对具体网关的所有操作。也就是说，该用户对您部署的其他网关的访问受限制。

```
{ "Statement": [ { "Action": [ "storagegateway:*" ], "Effect": "Allow", "Resource": "arn:aws:storagegateway:[AWS Region]:[AWS Account]:gateway/[Gateway Name]/*" } ] }
```

如果策略关联的用户使用 API 或 AWS 软件开发工具包访问网关，上一策略就会起效。但是，如果此用户计划使用 AWS Storage Gateway 控制台，则还必须授予进行 `ListGateways` 操作的权限。

```
{ "Statement": [ { "Action": [ "storagegateway:*" ], "Effect": "Allow", "Resource": "arn:aws:storagegateway:[AWS Region]:[AWS Account]:gateway/[Gateway Name]/*" }, { "Action": [ "storagegateway:ListGateways" ], "Effect": "Allow", "Resource": "*" } ] }
```

另外，如果用户计划激活该特定网关，则还必须授予进行 `ActivateGateway` 操作的权限。

```
{ "Statement": [ { "Action": [ "storagegateway:*" ], "Effect": "Allow", "Resource": "arn:aws:storagegateway:[AWS Region]:[AWS Account]:gateway/[Gateway Name]/*" }, { "Action": [ "storagegateway:ListGateways", "storagegateway:ActivateGateway" ], "Effect": "Allow", "Resource": "*" } ] }
```

### Example 4: 授予访问某个特定卷的权限

以下策略允许用户对网关上的具体卷执行所有操作。由于用户按默认没有任何权限，该策略将用户限定到仅能访问某个具体的卷。

```
{ "Statement": [ { "Action": [ "storagegateway:*" ], "Effect": "Allow", "Resource": "arn:aws:storagegateway:[AWS Region]:[AWS Account]:gateway/[Gateway Name]/volume/[Volume Name]" } ] }
```

如果策略关联的用户使用 API 或 AWS 软件开发工具包访问卷，上一策略就会起效。但是，如果此用户计划使用 AWS Storage Gateway 控制台，则还必须授予进行 `ListGateways` 操作的权限。

```
{ "Statement": [ { "Action": [ "storagegateway:*" ], "Effect": "Allow", "Resource": "arn:aws:storagegateway:[AWS Region]:[AWS Account]:gateway/[Gateway Name]/volume/[Volume Name]" }, { "Action": [ "storagegateway:ListGateways" ], "Effect": "Allow", "Resource": "*" } ] }
```

### Example 5: 允许对具有特定前缀的网关进行所有操作

以下策略允许用户对名称以“DeptX”起始的网关执行所有操作。该策略还允许进行 `DescribeSnapshots` Amazon EC2 操作。

```
{ "Statement": [ { "Action": [ "storagegateway:*" ], "Effect": "Allow", "Resource": "arn:aws:storagegateway:[AWS Region]:[AWS Account]:gateway/[Gateway Name Prefix]*" }, { "Action": [ "ec2:DescribeSnapshots" ], "Effect": "Allow", "Resource": "*" } ] }
```

如果策略关联的用户使用 API 或 AWS 软件开发工具包访问网关，上一策略就会起效。但是，如果此用户计划使用 AWS Storage Gateway 管理控制台，则必须授予其他权限，如 [3: 允许访问某个特定的网关 \(p. 417\)](#) 中所述。

# AWS Storage Gateway 的 API 参考

---

除了使用控制台之外，还可使用 AWS Storage Gateway API 以编程方式配置和管理网关。本节介绍 AWS Storage Gateway 操作、为身份验证进行的请求签名和错误处理。有关对 AWS Storage Gateway 可用的地区和终端节点的信息，请参阅[地区和终端节点](#)。



## Note

通过 AWS Storage Gateway 开发应用程序时，也可使用 AWS 开发工具包。适用于 Java、.NET 和 PHP 的 AWS 开发工具包含有底层 AWS Storage Gateway API，可简化您的编程任务。有关开发工具包库文件的信息，请参阅[示例代码库](#)。

## Topics

- [AWS Storage Gateway 必需的请求标头 \(p. 418\)](#)
- [签名请求 \(p. 420\)](#)
- [错误响应 \(p. 421\)](#)
- [AWS Storage Gateway 中的操作 \(p. 438\)](#)

## AWS Storage Gateway 必需的请求标头

本部分描述您每次向 AWS Storage Gateway 发送 POST 请求时必须使用的标头。您将 HTTP 标头包含在内以识别有关请求的密钥信息，包括您希望调用的操作、请求的日期以及表示您拥有请求发送者授权的信息。标头区分大小写，其次序不重要。

下例展示在 [API\\_ActivateGateway](#) 操作中使用的标头。

```
POST / HTTP/1.1
Host: storagegateway.us-east-1.amazonaws.com
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120425/us-east-1/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 AWS Storage Gateway 发送的 POST 请求中的标头。以下所示标头以“x-amz”为开头，是 AWS 专属的标头。列出的其他所有标头均为 HTTP 事务中使用的普通标头。

标头	说明
Authorization	<p>授权标头包含有关请求的数种信息，这些信息可以让 AWS 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）：</p> <pre>Authorization: AWS4-HMAC_SHA456 Credentials=<i>YourAccessKey</i>/<i>yyymmdd</i>/<i>region</i>/storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature=<i>CalculatedSignature</i></pre> <p>在前面的语法中，您指定 <i>YourAccessKey</i>、年、月、日 (<i>yyymmdd</i>)、<i>region</i> 和 <i>CalculatedSignature</i>。授权标头的格式由 AWS V4 签名过程的要求规定。主题<a href="#">签名请求 (p. 420)</a>中讨论了签名的详细信息。</p>
Content-Type	<p>使用 application/x-amz-json-1.1 作为所有向 AWS Storage Gateway 提出的请求的内容类型。</p> <pre>Content-Type: application/x-amz-json-1.1</pre>
Host	<p>使用主机标头指定向其发送请求的 AWS Storage Gateway 网关终端节点。例如，storagegateway.us-east-1.amazonaws.com 是美国东部地区的终端节点。有关对 AWS Storage Gateway 可用的终端节点的详细信息，请参见<a href="#">地区和终端节点</a>。</p> <pre>Host: storagegateway.<i>region</i>.amazonaws.com</pre>
x-amz-date	<p>必须在 HTTP Date 标头或 AWS x-amz-date 标头中提供时间戳。（部分 HTTP 客户端库文件不允许您设置 Date 标头。）存在 x-amz-date 标头时，AWS Storage Gateway 将在验证请求的身份期间忽略任何 Date 标头。x-amz-date 格式必须为 ISO8601 Basic 的 YYYYMMDD'T'HHMMSS'Z' 格式。如果同时使用 Date 和 x-amz-date 标头，则 Date 标头的格式不必为 ISO8601。</p> <pre>x-amz-date: <i>YYYYMMDD'T'HHMMSS'Z'</i></pre>
x-amz-target	<p>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。</p> <pre>x-amz-target: StorageGateway_<i>APIVersion</i>.<i>operationName</i></pre> <p>可从 API 列表 <a href="#">AWS Storage Gateway 的 API 参考 (p. 418)</a>中找到 <i>operationName</i> 值（例如“ActivateGateway”）。</p>

## 签名请求

AWS 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。要对请求进行签名，请使用加密哈希函数计算数字签名。加密哈希是根据输入内容返回唯一哈希值的函数。对哈希函数的输入内容包括您的请求文本和私有访问密钥。哈希函数返回哈希值，您将该值包含在请求中，作为签名。签名是请求的 `Authorization` 标头的一部分。

收到您的请求后，AWS Storage Gateway 使用与您用于对该请求进行签名的相同哈希函数和输入重新计算签名。如果所得签名与该请求中的签名相匹配，则 AWS Storage Gateway 处理该请求。否则，请求将被拒绝。

AWS 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 AWS 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：创建用于待签字符串**

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”，由哈希算法名称、请求日期、“证书范围”字符串以及来自上一任务的规范化请求组合而成。“证书范围”字符串本身由日期、地区和服务信息组合而成。

- **任务 3：创建签名**

使用接受两种输入字符串的加密哈希函数为您的请求创建签名：您的“待签字符串”和“派生密钥”。计算“派生密钥”时首先采用您的私有访问密钥，然后使用“证书范围”字符串创建一系列基于哈希的消息身份验证代码 (HMAC)。

## 实例签名计算

下例演练为 [API\\_ListGateways](#) 创建签名的详细步骤。该示例可用作核查您的签名计算方法的参考。Amazon Web Services 术语表的 [签名版本 4 测试套件](#) 中包括其他参考计算方法。

示例假定以下各项：

- 请求的时间戳为“Mon, 10 Sep 2012 00:00:00”GMT。
- 终端节点为美国东部（弗吉尼亚北部）地区。

通用请求语法（包括 JSON 正文）为：

```
POST / HTTP/1.1 Host: storagegateway.us-east-1.amazonaws.com x-amz-Date:
20120910T000000Z Authorization: SignatureToBeCalculated
Content-type: application/x-amz-json-1.1 x-amz-target: StorageGate
way_20120630.ListGateways {}
```

为 [任务 1：创建规范请求](#) (p. 420) 计算的请求的规范格式为：

```
POST / content-type:application/x-amz-json-1.1 host:storagegateway.us-east-
1.amazonaws.com x-amz-date:20120910T000000Z x-amz-target:StorageGate
way_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 AWS Storage Gateway API ) 没有查询参数。

**任务 2 : 创建用于待签字符串 (p. 420) 的“待签字符串”为 :**

```
AWS4-HMAC-SHA256 20120910T000000Z 20120910/us-east-1/storagegateway/aws4_request
92c0effa6f9224ac752ca179a04cecbede3038b0959666a8160ab452c9e51b3e
```

“待签字符串”的第一行是算法，第二行是时间戳，第三行是“证书范围”，最后一行是来自任务 1 的规范请求的哈希值。

对于 **任务 3 : 创建签名 (p. 420)**，“派生密钥”可表示为：

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey, "20120910"), "us-
east-1"), "storagegateway"), "aws4_request")
```

如果使用私有访问密钥 wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY，则计算得到的签名为：

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

最后一步是构造 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 ) 为：

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120910/us-
east-1/storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-
amz-target, Signature=6d4c40b8f2257534dbd
ca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

## 错误响应

### Topics

- [例外 \(p. 421\)](#)
- [操作错误代码 \(p. 422\)](#)
- [错误响应 \(p. 437\)](#)

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，如果请求签名有问题，则任何 API 响应均返回错误例外 `InvalidSignatureException`。但是，仅返回 `ActivateGateway` API 的操作错误代码 `ActivationKeyInvalid`。

根据错误类型的情况，AWS Storage Gateway 可能只返回例外，或者同时返回例外和操作错误代码。[错误响应 \(p. 437\)](#) 中显示误差响应的示例。

## 例外

下表列出 AWS Storage Gateway API 例外。当 AWS Storage Gateway 操作返回错误响应时，响应正文包含其中一个例外。`InternalServerError` 和 `InvalidGatewayRequestException` 返回一个操作错误代码 消息代码，该代码给出具体的操作错误代码。

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	500 内部服务器错误
InvalidAction	所请求的操作或操作无效。	400 错误请求
InvalidClientTokenId	在我们的记录中没有所提供的 X.509 证书或 AWS 访问密钥 ID。	403 禁止访问
InvalidGatewayRequestException	一个操作错误代码消息。	400 错误请求
InvalidSignatureException	我们计算出的请求签名与您提供的签名不匹配。请检查您的 AWS 私有访问密钥和签名方法。	400 错误请求
MissingAction	请求中遗漏了一个操作或运行参数。	400 错误请求
MissingAuthenticationToken	请求中必须包含有效的（已注册的）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 需要订阅产品。	400 错误请求
ThrottlingException	费率已超。	400 错误请求
UnknownOperationException	指定了未知操作。 <a href="#">AWS Storage Gateway 中的操作 (p. 438)</a> 中列出有效的操作。	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 AWS Storage Gateway 操作错误代码与可返回这些代码的 API 之间的映射。所有操作错误代码均与[例外 \(p. 421\)](#)中所述的两个常规例外 —`InternalServerError` 和 `InvalidGatewayRequestException`— 中的一个一并返回。

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。	<a href="#">ActivateGateway</a>
ActivationKeyInvalid	指定的激活密钥无效。	<a href="#">ActivateGateway</a>
ActivationKeyNotFound	找不到指定的激活密钥。	<a href="#">ActivateGateway</a>

操作错误代码	消息	返回此错误代码的操作
BandwidthThrottleScheduleNotFound	找不到指定的带宽限制。	<a href="#">DeleteBandwidthRateLimit</a>
CannotExportSnapshot	无法导出指定的快照。	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a>
InitiatorNotFound	找不到指定的启动程序。	<a href="#">DeleteChapCredentials</a>
DiskAlreadyAllocated	指定的磁盘已分配。	<a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateStorediSCSIVolume</a>
DiskDoesNotExist	指定的磁盘不存在。	<a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateStorediSCSIVolume</a>
DiskSizeNotGigAligned	指定的磁盘没有以 GB 为整单位。	<a href="#">CreateStorediSCSIVolume</a>
DiskSizeGreaterThanVolumeMaxSize	指定的磁盘大小超过最高卷大小。	<a href="#">CreateStorediSCSIVolume</a>
DiskSizeLessThanVolumeSize	指定的磁盘大小低于最高卷大小。	<a href="#">CreateStorediSCSIVolume</a>
DuplicateCertificateInfo	指定的证书信息是副本。	<a href="#">ActivateGateway</a>

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。	<a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateSnapshot</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">DeleteBandwidthRateLimit</a> <a href="#">DeleteChapCredentials</a> <a href="#">DeleteVolume</a> <a href="#">DescribeBandwidthRateLimit</a> <a href="#">DescribeCache</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeChapCredentials</a> <a href="#">DescribeGatewayInformation</a> <a href="#">DescribeMaintenanceStartTime</a> <a href="#">DescribeSnapshotSchedule</a> <a href="#">DescribeStorediSCSIVolumes</a> <a href="#">DescribeWorkingStorage</a> <a href="#">ListLocalDisks</a> <a href="#">ListVolumes</a> <a href="#">ListVolumeRecoveryPoints</a> <a href="#">ShutdownGateway</a> <a href="#">StartGateway</a> <a href="#">UpdateBandwidthRateLimit</a> <a href="#">UpdateChapCredentials</a> <a href="#">UpdateMaintenanceStartTime</a> <a href="#">UpdateGatewaySoftwareNow</a> <a href="#">UpdateSnapshotSchedule</a>

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。	<a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateSnapshot</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">DeleteBandwidthRateLimit</a> <a href="#">DeleteChapCredentials</a> <a href="#">DeleteVolume</a> <a href="#">DescribeBandwidthRateLimit</a> <a href="#">DescribeCache</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeChapCredentials</a> <a href="#">DescribeGatewayInformation</a> <a href="#">DescribeMaintenanceStartTime</a> <a href="#">DescribeSnapshotSchedule</a> <a href="#">DescribeStorediSCSIVolumes</a> <a href="#">DescribeWorkingStorage</a> <a href="#">ListLocalDisks</a> <a href="#">ListVolumes</a> <a href="#">ListVolumeRecoveryPoints</a> <a href="#">ShutdownGateway</a> <a href="#">StartGateway</a> <a href="#">UpdateBandwidthRateLimit</a> <a href="#">UpdateChapCredentials</a> <a href="#">UpdateMaintenanceStartTime</a> <a href="#">UpdateGatewaySoftwareNow</a> <a href="#">UpdateSnapshotSchedule</a>

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。	<a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateSnapshot</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteBandwidthRateLimit</a> <a href="#">DeleteChapCredentials</a> <a href="#">DeleteGateway</a> <a href="#">DeleteVolume</a> <a href="#">DescribeBandwidthRateLimit</a> <a href="#">DescribeCache</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeChapCredentials</a> <a href="#">DescribeGatewayInformation</a> <a href="#">DescribeMaintenanceStartTime</a> <a href="#">DescribeSnapshotSchedule</a> <a href="#">DescribeStorediSCSIVolumes</a> <a href="#">DescribeWorkingStorage</a> <a href="#">ListLocalDisks</a> <a href="#">ListVolumes</a> <a href="#">ListVolumeRecoveryPoints</a> <a href="#">ShutdownGateway</a> <a href="#">StartGateway</a> <a href="#">UpdateBandwidthRateLimit</a> <a href="#">UpdateChapCredentials</a> <a href="#">UpdateMaintenanceStartTime</a> <a href="#">UpdateGatewaySoftwareNow</a> <a href="#">UpdateSnapshotSchedule</a>

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。	<a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateSnapshot</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteBandwidthRateLimit</a> <a href="#">DeleteChapCredentials</a> <a href="#">DeleteVolume</a> <a href="#">DescribeBandwidthRateLimit</a> <a href="#">DescribeCache</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeChapCredentials</a> <a href="#">DescribeGatewayInformation</a> <a href="#">DescribeMaintenanceStartTime</a> <a href="#">DescribeSnapshotSchedule</a> <a href="#">DescribeStorediSCSIVolumes</a> <a href="#">DescribeWorkingStorage</a> <a href="#">ListLocalDisks</a> <a href="#">ListVolumes</a> <a href="#">ListVolumeRecoveryPoints</a> <a href="#">ShutdownGateway</a> <a href="#">StartGateway</a> <a href="#">UpdateBandwidthRateLimit</a> <a href="#">UpdateChapCredentials</a> <a href="#">UpdateMaintenanceStartTime</a> <a href="#">UpdateGatewaySoftwareNow</a> <a href="#">UpdateSnapshotSchedule</a>

操作错误代码	消息	返回此错误代码的操作
InternalServerError	出现内部错误。	

操作错误代码	消息	返回此错误代码的操作
		<a href="#">ActivateGateway</a> <a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateSnapshot</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteBandwidthRateLimit</a> <a href="#">DeleteChapCredentials</a> <a href="#">DeleteGateway</a> <a href="#">DeleteVolume</a> <a href="#">DescribeBandwidthRateLimit</a> <a href="#">DescribeCache</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeChapCredentials</a> <a href="#">DescribeGatewayInformation</a> <a href="#">DescribeMaintenanceStartTime</a> <a href="#">DescribeSnapshotSchedule</a> <a href="#">DescribeStorediSCSIVolumes</a> <a href="#">DescribeWorkingStorage</a> <a href="#">ListLocalDisks</a> <a href="#">ListGateways</a> <a href="#">ListVolumes</a> <a href="#">ListVolumeRecoveryPoints</a> <a href="#">ShutdownGateway</a> <a href="#">StartGateway</a> <a href="#">UpdateBandwidthRateLimit</a> <a href="#">UpdateChapCredentials</a> <a href="#">UpdateMaintenanceStartTime</a>

操作错误代码	消息	返回此错误代码的操作
		<a href="#">UpdateGatewayInformation</a> <a href="#">UpdateGatewaySoftwareNow</a> <a href="#">UpdateSnapshotSchedule</a>

操作错误代码	消息	返回此错误代码的操作
InvalidParameters	指定的请求中包含无效参数。	

操作错误代码	消息	返回此错误代码的操作
		<a href="#">ActivateGateway</a> <a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateSnapshot</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteBandwidthRateLimit</a> <a href="#">DeleteChapCredentials</a> <a href="#">DeleteGateway</a> <a href="#">DeleteVolume</a> <a href="#">DescribeBandwidthRateLimit</a> <a href="#">DescribeCache</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeChapCredentials</a> <a href="#">DescribeGatewayInformation</a> <a href="#">DescribeMaintenanceStartTime</a> <a href="#">DescribeSnapshotSchedule</a> <a href="#">DescribeStorediSCSIVolumes</a> <a href="#">DescribeWorkingStorage</a> <a href="#">ListLocalDisks</a> <a href="#">ListGateways</a> <a href="#">ListVolumes</a> <a href="#">ListVolumeRecoveryPoints</a> <a href="#">ShutdownGateway</a> <a href="#">StartGateway</a> <a href="#">UpdateBandwidthRateLimit</a> <a href="#">UpdateChapCredentials</a> <a href="#">UpdateMaintenanceStartTime</a>

操作错误代码	消息	返回此错误代码的操作
		<a href="#">UpdateGatewayInformation</a> <a href="#">UpdateGatewaySoftwareNow</a> <a href="#">UpdateSnapshotSchedule</a>
LocalStorageLimitExceeded	已超过本地存储限制。	<a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a>
LunInvalid	指定的 LUN 无效。	<a href="#">CreateStorediSCSIVolume</a>
MaximumVolumeCountExceeded	已超过最大卷计数。	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeStorediSCSIVolumes</a>
NetworkConfigurationChanged	已更改网关网络配置。	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a>

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。	

操作错误代码	消息	返回此错误代码的操作
		<a href="#">ActivateGateway</a> <a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateSnapshot</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteBandwidthRateLimit</a> <a href="#">DeleteChapCredentials</a> <a href="#">DeleteGateway</a> <a href="#">DeleteVolume</a> <a href="#">DescribeBandwidthRateLimit</a> <a href="#">DescribeBandwidthRateLimit</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeChapCredentials</a> <a href="#">DescribeGatewayInformation</a> <a href="#">DescribeMaintenanceStartTime</a> <a href="#">DescribeSnapshotSchedule</a> <a href="#">DescribeStorediSCSIVolumes</a> <a href="#">DescribeWorkingStorage</a> <a href="#">ListLocalDisks</a> <a href="#">ListGateways</a> <a href="#">ListVolumes</a> <a href="#">ListVolumeRecoveryPoints</a> <a href="#">ShutdownGateway</a> <a href="#">StartGateway</a> <a href="#">UpdateBandwidthRateLimit</a> <a href="#">UpdateChapCredentials</a> <a href="#">UpdateMaintenanceStartTime</a>

操作错误代码	消息	返回此错误代码的操作
		<a href="#">UpdateGatewayInformation</a> <a href="#">UpdateGatewaySoftwareNow</a> <a href="#">UpdateSnapshotSchedule</a>
OutdatedGateway	指定的网关已过时。	<a href="#">ActivateGateway</a>
SnapshotInProgressException	指定的快照正在进行中。	<a href="#">DeleteVolume</a>
SnapshotIdInvalid	指定的快照无效。	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a>
StagingAreaFull	暂存区域已满。	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a>
TargetAlreadyExists	已存在指定的目标。	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a>
TargetInvalid	指定的目标无效。	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteChapCredentials</a> <a href="#">DescribeChapCredentials</a> <a href="#">UpdateChapCredentials</a>
TargetNotFound	找不到指定的目标。	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteChapCredentials</a> <a href="#">DescribeChapCredentials</a> <a href="#">DeleteVolume</a> <a href="#">UpdateChapCredentials</a>

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。	<a href="#">AddCache</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteSnapshotSchedule</a> <a href="#">DescribeCache</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeStorediSCSIVolumes</a> <a href="#">DescribeUploadBuffer</a> <a href="#">DescribeWorkingStorage</a> <a href="#">ListVolumeRecoveryPoints</a>
VolumeAlreadyExists	已存在指定的卷。	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a>
VolumeIdInvalid	指定的卷无效。	<a href="#">DeleteVolume</a>
VolumeInUse	指定的卷已在使用中。	<a href="#">DeleteVolume</a>
VolumeNotFound	找不到指定的卷。	<a href="#">CreateSnapshot</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">DeleteVolume</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeSnapshotSchedule</a> <a href="#">DescribeStorediSCSIVolumes</a> <a href="#">UpdateSnapshotSchedule</a>
VolumeNotReady	指定的卷没有准备好。	<a href="#">CreateSnapshot</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a>

## 错误响应

当存在错误时，响应头信息会包含：

- Content-Type : application/x-amz-json-1.1
- 相应的 4xx 或 5xx HTTP 状态代码

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

例外 (p. 421) 中的一个例外。

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

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

如果使用 DescribeStorediSCSIVolumes API 并指定不存在的网关 ARN 请求输入，则返回以下 JSON 正文。

```
{ "__type": "InvalidGatewayRequestException", "message": "The specified volume was not found.", "error": { "errorCode": "VolumeNotFound" } }
```

如果 AWS 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." }
```

# AWS Storage Gateway 中的操作

有关 AWS Storage Gateway 操作的列表，请转到 *AWS Storage Gateway API Reference* 中的 [操作](#)。

# AWS Storage Gateway 文档历史记录

下表描述了自 *AWS Storage Gateway User Guide* 上一次发布以来对文档所做的重要修改。

- API 版本:2013-06-30
- 文档最新更新时间:2013 年 11 月 5 日

变更	说明	修改日期
支持虚拟磁带库 (VTL) 并引入 API 版本 2013-06-30	<p>AWS Storage Gateway 将本地软件设备与基于云的存储连接起来，以将本地 IT 环境与 AWS 存储基础设施集成。除了卷网关（网关缓存和网关存储）之外，AWS Storage Gateway 现在还支持网关虚拟磁带库 (VTL)。对于每个网关，最多可为网关 VTL 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。有关详细信息，请参阅 <i>AWS Storage Gateway User Guide</i> 中的以下主题。</p> <ul style="list-style-type: none"> <li>• 有关体系架构概述，请参阅<a href="#">网关 - 虚拟磁带库（网关 VTL）架构</a> (p. 5)。</li> <li>• 要开始使用网关 VTL，请参阅<a href="#">入门（网关 VTL）</a> (p. 257)。</li> </ul>	在此次发行版本中。
支持 Microsoft Hyper-V	<p>AWS 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<a href="#">设置和激活（Hyper-V 主机）</a> (p. 35)。</p>	2013 年 4 月 10 日
支持将网关部署在 Amazon EC2 上	<p>AWS Storage Gateway 现在可将网关部署在 Amazon Elastic Compute Cloud (Amazon EC2) 中。可使用 <a href="#">AWS Marketplace</a> 中提供的 AWS Storage Gateway AMI 在 Amazon EC2 中启动网关实例。要使用 AWS Storage Gateway AMI 开始部署网关，请转到<a href="#">在 Amazon EC2 上部署并激活 AWS Storage Gateway</a> (p. 133)。</p>	2013 年 1 月 15 日

变更	说明	修改日期
支持缓存卷并推出了 API 版本 2012-06-30	<p>在此版本中，AWS Storage Gateway 引入了对网关缓存卷的支持。网关缓存卷可尽量避免扩展内部存储基础设施，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。写入网关缓存卷的数据存储在 Amazon Simple Storage Service (Amazon S3) 中，并缓存最近写入和最近读取的数据，存储在本地存储硬件上。通过网关缓存卷，可将 Amazon S3 用于可承受更高检索延迟的数据（如不常访问的旧数据），同时仍将本地存储用于要求低延迟访问的数据。</p> <p>在此版本中，AWS 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，还提供新操作以支持网关缓存卷。</p> <p>有关两种 AWS Storage Gateway 解决方案的详细信息，请参阅<a href="#">AWS Storage Gateway 的运行原理（架构）</a> (p. 3)。</p> <p>您也可以尝试测试设置。有关说明，请转到<a href="#">the section called “入门（卷网关）”</a> (p. 10)。</p>	2012 年 10 月 29 日
API 和 IAM 支持	<p>在此版本中，AWS Storage Gateway 引入了对 API 的支持和对 AWS Identity and Access Management(IAM) 的支持。</p> <ul style="list-style-type: none"> <li>• API 支持—现在可按编程方式配置和管理 AWS Storage Gateway 资源。有关 API 的详细信息，请参阅 <a href="#">AWS Storage Gateway User Guide</a> 中的 <a href="#">AWS Storage Gateway 的 API 参考</a> (p. 418)。</li> <li>• IAM Support – 通过 (IAM)，可创建用户并通过 IAM 策略管理用户对您的 AWS Storage Gateway 资源的访问权限。有关 IAM 策略的示例，请转到<a href="#">使用 AWS Identity and Access Management (IAM) 进行访问控制</a> (p. 415)。有关 IAM 的详细信息，请转到 <a href="#">AWS Identity and Access Management (IAM) 详细信息</a> 页。</li> </ul>	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 <a href="#">将您的 AWS Storage Gateway 配置为使用静态 IP 地址</a> (p. 224)。	2012 年 3 月 5 日
新指南	这是 <i>AWS Storage Gateway User Guide</i> 的第一版。	2012 年 1 月 24 日

# AWS Storage Gateway 附录

此附录包括下列部分。

## Topics

- [附录 A : vSphere 环境中用于 AWS Storage Gateway 的组件 \(p. 441\)](#)
- [附录 B : 为 AWS Storage Gateway 配置 VMware ESXi 主机 \(p. 442\)](#)
- [附录 C : Hyper-V 环境中用于 AWS Storage Gateway 的组件 \(p. 446\)](#)
- [附录 D : 为 AWS Storage Gateway 配置 Microsoft Hyper-V 主机 \(p. 447\)](#)
- [附录 E : AWS Storage Gateway 资源 \(p. 456\)](#)
- [附录 F : AWS Storage Gateway 限制 \(p. 457\)](#)

## 附录 A : vSphere 环境中用于 AWS Storage Gateway 的组件

使用 VMware 创建一个虚拟机，其中托管 AWS Storage Gateway。您使用 VMware 客户端与 VMware Server 交互，并创建虚拟机。可从 [AWS Storage Gateway 详细信息页](#) 获得网关虚拟机定义（即模板），其中包含用于新建 gateway 的所有文件和数据。以部署在 VMware 服务器上的单个 .ova 文件的形式分发该模板。本节讨论 VMware vSphere 环境中为使用 AWS Storage Gateway service 而需要了解的组件。

下表介绍在使用 AWS Storage Gateway service 时通常会涉及到的一部分 vSphere 组件。

组建	说明
VMware vSphere	用于管理虚拟计算基础设施的 VMware 虚拟平台，包括客户端和服务端。
VMware ESXi 管理程序操作系统 (vSphere Server)	托管网关虚拟机的 VMware Server 操作系统。您可以通过 vSphere 客户端 GUI 与操作系统交互。要配置 AWS Storage Gateway，只需在激活网关期间访问主机即可。对于所有其他管理和维护方面的功能，您可以使用 AWS 管理控制台。
VMware vSphere 客户端 (vSphere 客户端)	在计算机上用于访问和管理 VMware 环境的 VMware 软件。您管理使用客户端的虚拟机（其中包含网关）。

组建	说明
VMware 高可用性	VMware 高可用性 (HA) 是一种 vSphere 组件，可以在支持网关 VM 的基础结构层提供故障防护。为此，VMware HA 使用配置为集群的多个主机，以使如果一个运行网关 VM 的主机发生故障，则可自动在该集群内的其他主机上重新启动该网关 VM。AWS Storage Gateway 可以与 VMware HA 一起使用。有关 VMware HA 的详细信息，请转到 <a href="#">VMware HA：概念和最佳实践</a> 。有关将 VM HA 和 AWS Storage Gateway 配合使用的详细信息，请参阅 <a href="#">AWS Storage Gateway 和 VMware High Availability 一起使用 (p. 90)</a> 。
虚拟机	包含 AWS Storage Gateway 组件的计算机软件实施。虚拟机 (VM) 在 VMware vSphere 平台上运行。
OVA、OVF	代表自定义虚拟机的模板。AWS Storage Gateway 设备是在开放式虚拟化应用程序 (OVA) 中分发的开放式虚拟化格式 (OVF) 软件包。OVA 模板包含配置和启动 gateway 所需的全部信息。您可以使用 VMware Server 连接的客户端部署该模板。有关下载 AWS Storage Gateway 的 OVA 模板的说明，请转到 <a href="#">AWS Storage Gateway 详细信息页</a> 。
数据存储	vSphere 上的存储，其中存储了用于定义虚拟机的文件。这些文件来源于 OVA 文件，而 OVA 文件是作为服务的一部分提供的。在部署 OVA 时，如果存在不止一个适用于 VMware Server 的数据存储，那么，您应选择用于存储文件。

## 附录 B：为 AWS Storage Gateway 配置 VMware ESXi 主机

本部分提供您设置虚拟主机所需的基本信息。在基本设置后，我们还讨论了一些可选主机配置。

AWS Storage Gateway service 包括一个本地软件设备，后者与 AWS 的云存储基础设施进行通信。该设备打包为虚拟机，您将该虚拟机部署在运行 VMware ESX/ESXi 虚拟化软件的主机上。有关 VMware 虚拟软件的详细信息，请转到 [VMware vSphere 虚拟机监控程序](#)。有关 VMware 环境为运行 AWS Storage Gateway 而必须满足的要求，请参阅 [要求 \(p. 7\)](#)。

如需在主机上安装 VMware vSphere 管理程序操作系统

1. 将 VMware vSphere hypervisor 磁盘插入磁盘驱动器。
2. 重启计算机。

根据您的计算机 Bios 设置的不同，计算机可能会自动关闭您的磁盘。如果未自动关闭，请检查相关配置，以便从管理程序磁盘启动计算机。

3. 按监视器上的指示安装 VMware 管理程序操作系统。

这项操作会擦除磁盘上的任何现有内容，并且安装管理程序。



#### Tip

VMware 管理程序主机成功安装后，监视器会显示主计算机的 IP 地址。记录该 IP 地址。您使用该 IP 地址连接到主机。

#### 4. 在主机上设置时间。

有关说明，请参阅[将 VM 时间与主机时间同步 \(p. 18\)](#)。

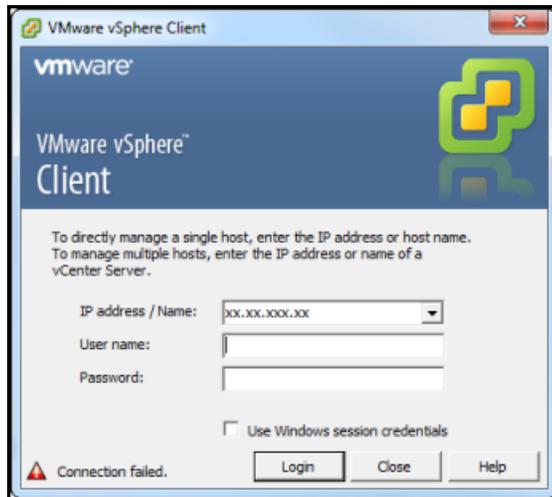
在前面的步骤中，您使用 VMware 管理程序预配置了主机。管理程序了解主计算机配置，例如可用处理器、内存和本地硬盘。主机向 AWS Storage Gateway 提供这些资源。

您可以通过添加更多存储空间，例如直接连接的磁盘或 SAN 磁盘，有选择地配置该主机。以下步骤说明如何向该主机添加一个或多个 SAN 磁盘。

#### 如需连接到管理程序主机

##### 1. 启动 VMware vSphere 客户端，然后使用主机 IP 地址连接到主机。

VMware vSphere 客户端对话框显示。



2. 在 IP 地址字段中输入主机的 IP 地址。
3. 在用户名和密码字段中输入凭据。
4. 单击登录。

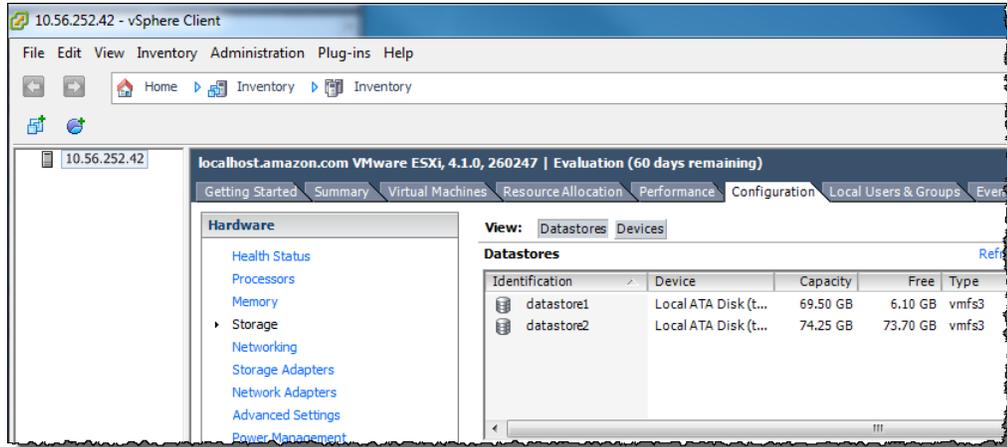
此项操作将您的客户端连接到主机。您现在可随时配置主机。

#### 如需添加新的 iSCSI 目标

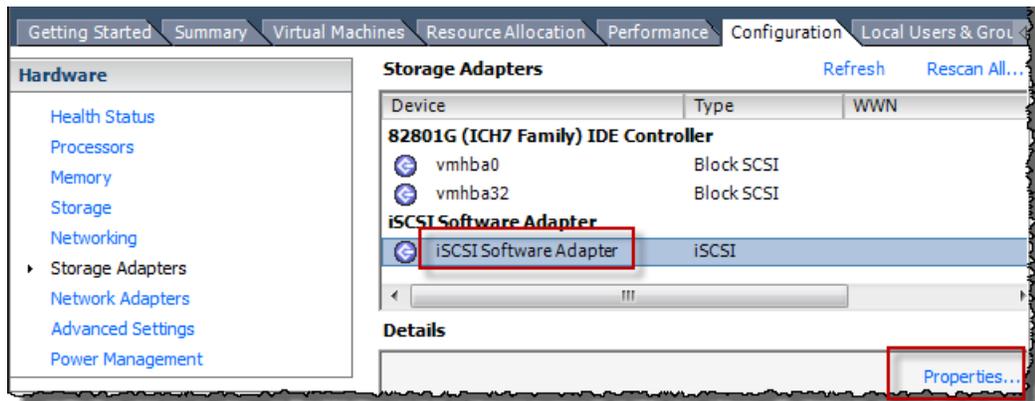
##### 1. 通过虚拟机监控程序连接到远程设备后，转到主机的配置选项卡，然后单击硬件列表中的存储。

数据存储窗格显示可用的数据存储。

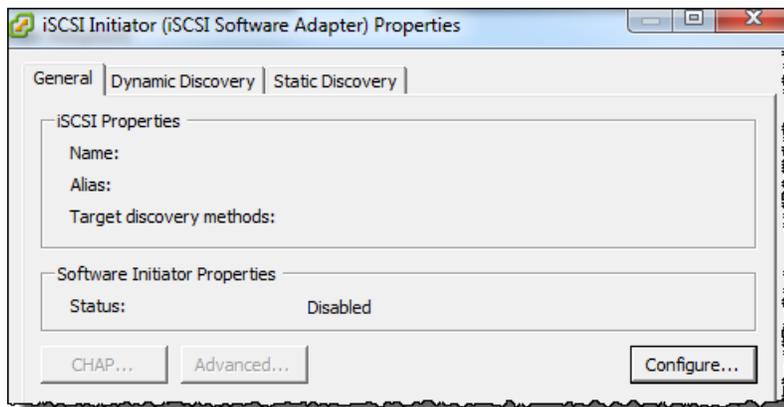
例如，以下示例显示主机有两个本地硬盘可用，分别是 datastore1 和 datastore2。



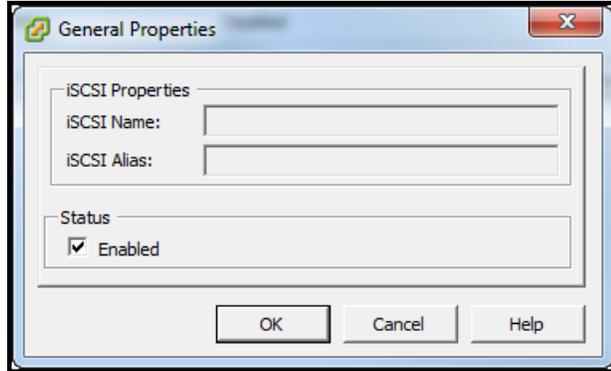
2. 在硬件列表中，单击存储适配器。
3. 在存储适配器窗格中，选择 iSCSI 软件适配器，然后单击详细信息面板中的属性链接。



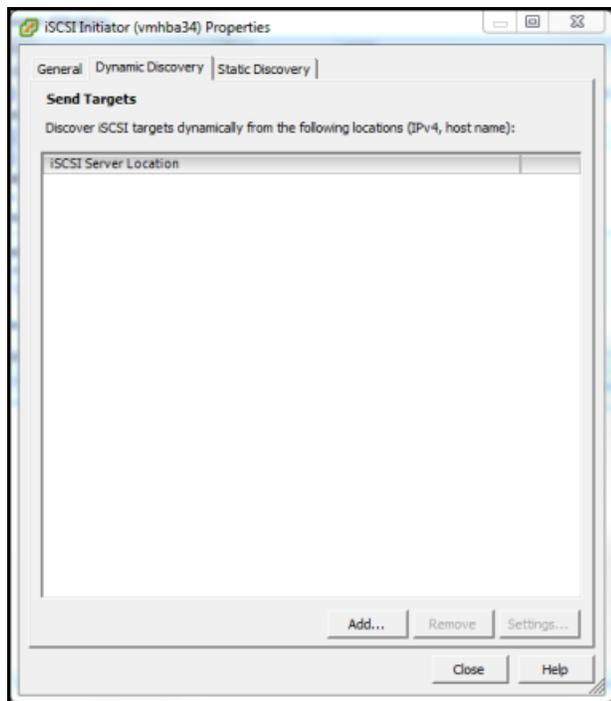
4. 在 iSCSI 发起程序 (iSCSI 软件适配器) 属性对话框中，单击配置。



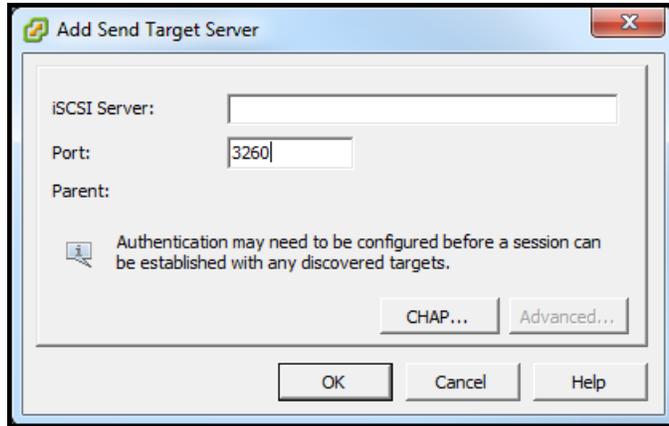
5. 在常规属性对话框中，选择已启用以将软件发起程序状态设置为已启用，然后单击确定。



6. 在 iSCSI 发起程序 (iSCSI 软件适配器) 属性对话框中，选择动态发现选项卡，然后单击添加以添加 iSCSI 目标。



7. 在添加发送目标服务器对话框中，在 iSCSI 服务器字段内输入名称，在端口字段输入端口，然后单击确定。



输入存储系统的 IP 地址或 DNS 名称。

随即在动态发现选项卡上的发送目标列表中显示在此处输入的新 iSCSI 服务器位置。

- 单击关闭以关闭 iSCSI 发起程序 (iSCSI 软件适配器) 属性对话框。

至此，您已在主机配置中添加了新 iSCSI 目标。

## 附录 C : Hyper-V 环境中用于 AWS Storage Gateway 的组件

使用 Microsoft Hyper-V 创建一个本地虚拟机，其中托管 Storage Gateway。您使用 Hyper-V Manager 与 Hyper-V 服务器交互，并创建虚拟机。可从 AWS Storage Gateway 控制台获得网关虚拟机定义（即模板），其中包含用于新建 gateway 的所有文件和数据。以导入到 Hyper-V 服务器的单个 .zip 文件的形式分发该模板。本节讨论 Microsoft Hyper-V 环境中为使用 AWS Storage Gateway 而需要了解的组件。

下表介绍在使用 AWS Storage Gateway 时通常会涉及到的一部分 Hyper-V 组件。

组建	说明
Microsoft Hyper-V	用于管理虚拟计算基础设施的 Microsoft 虚拟平台，包括客户端和服务端。
Hyper-V 管理程序操作系统	托管网关虚拟机的 Hyper-V 服务器操作系统 (OS)。可通过 Microsoft Hyper-V 管理器图形用户界面与操作系统进行交互。要配置 Storage Gateway，只需在激活网关期间访问主机即可。对于所有其他与管理与维护相关的功能，可使用 AWS Management Console。
Hyper-V Manager	在计算机上用于访问和管理 Hyper-V 环境的 Hyper-V 客户端软件。您管理使用客户端的虚拟机（其中包含网关）。
虚拟机	包含 AWS Storage Gateway 组件的计算机的软件实现。虚拟机 (VM) 在 Microsoft Hyper-V 平台上运行。

组建	说明
导入文件 ( VM 封装 )	<p>以压缩目录的形式分发 AWS Storage Gateway 设备，该目录包含以下各项：</p> <ul style="list-style-type: none"><li>• Snapshots 文件夹，对于 AWS Storage Gateway，该文件夹将为空。</li><li>• Virtual Hard Disks 文件夹，其中包含一个名为 AWS-Storage-Gateway.vhd 的虚拟磁盘文件。</li><li>• Virtual Machines 文件夹，其中包含一个导出的配置文件 <i>GUID</i>.exp，其中 GUID 为虚拟机 ID。</li><li>• config.xml，其中包含用于导入的配置信息。</li></ul> <p>通过首先解压缩该目录，然后使用 Hyper-V 管理器导入解压缩后的文件夹，将 AWS Storage Gateway 部署到 Hyper-V。</p>

## 附录 D：为 AWS Storage Gateway 配置 Microsoft Hyper-V 主机

本附录提供有关设置、配置 [Microsoft Hyper-V 2008 R2](#) 虚拟化主机和排除其故障的基本信息，其中包括：

- 设置和配置
  - [安装 Microsoft Hyper-V \(p. 447\)](#)
  - [连接 Microsoft Hyper-V 主机 \(p. 449\)](#)
  - [配置虚拟网络设置 \(p. 450\)](#)
  - [添加通过硬盘支持的虚拟磁盘 \(p. 452\)](#)
- 故障排除
  - [故障诊断 Microsoft Hyper-V 设置 \(p. 453\)](#)

### 设置和配置 Microsoft Hyper-V 主机

AWS Storage Gateway service 包括一个本地软件设备，后者与 AWS 的云存储基础设施进行通信。该设备打包为虚拟机，您将该虚拟机部署在运行 Microsoft Hyper-V 虚拟软件的主机上。有关 Microsoft Hyper-V 软件的详细信息，请转到 [Microsoft 服务器虚拟化](#)。有关 Hyper-V 环境为运行 AWS Storage Gateway 而必须满足的要求，请参阅 [要求 \(p. 7\)](#)。

### 安装 Microsoft Hyper-V

本节介绍安装 Microsoft Hyper-V 的过程。如果已有 Microsoft Hyper-V 虚拟化环境，或将由熟悉该平台的管理员设置环境，则不需要详细了解这些步骤。

有关安装 Hyper-V 的详细信息，请参阅 [Microsoft TechNet](#) 网站上的 [Hyper-V 入门指南](#)。

如需在主机上安装 Microsoft Hyper-V 管理程序操作系统

1. 在磁盘驱动器中插入 Microsoft Hyper-V 磁盘。

2. 重启计算机。

根据您计算机的 Bios 设置的不同，计算机可能会自动关闭您的磁盘。如果未自动关闭，请检查相关配置，以便从管理程序磁盘启动计算机。

3. 按监视器上的指示安装 Hyper-V 管理程序操作系统。

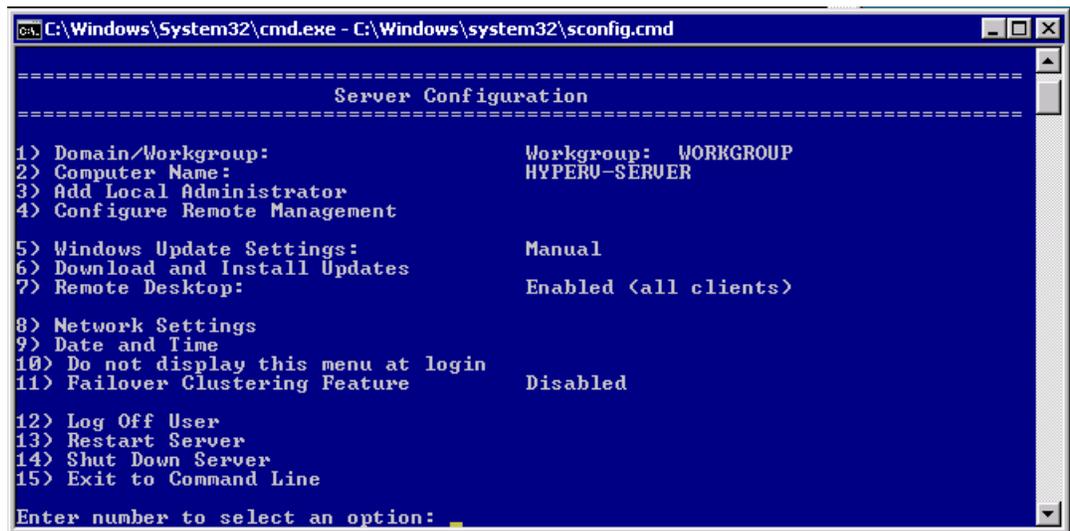
此项操作会擦除磁盘上的任何现有内容，并且安装管理程序。

在成功安装 Hyper-V 管理程序主机后，系统会提示您创建管理员账户密码。创建此账户后，显示器将显示服务器配置菜单，从中将进一步配置主机。

4. 在服务器配置菜单中，配置主机。我们建议执行下列操作：

如需...	请执行此操作...
配置远程管理。	选择选项 4，然后启用下列： <ul style="list-style-type: none"> <li>• 选项 1，允许 MMC 远程管理</li> <li>• 选项 2，启用 Windows PowerShell</li> <li>• 选项 3，允许服务器管理器远程管理</li> </ul>
查找主机的网络地址。	选择选项 8，并按照提示操作。记录 IP 地址，供稍后使用。
设置日期和时间。	选择选项 9，并按照提示操作。
( 可选 ) 更改计算机名称。	选择选项 2，并按照提示操作。因为这需要重新启动，所以，您需要最后再进行此配置更改。
( 可选 ) 添加本地管理员。	选择选项 3，并按照提示操作。
( 可选 ) 启用远程桌面。	选择选项 7，并按照提示操作。

下列介绍"Server Configuration"菜单。



5. ( 可选 ) 您可能必须将管理程序的 IP 地址放入已连接到管理程序主机的客户端计算机的主机文件中。

例如，在 Windows 7 和 8 中，可以在在这一位置找到主机文件：

```
%SystemRoot%\system32\drivers\etc\hosts
```

## 连接 Microsoft Hyper-V 主机

Hyper-V Manager 在您的客户端计算机上运行，并连接到管理程序主机。使用 Microsoft Hyper-V 管理器导入、配置和启动 AWS Storage Gateway VM。

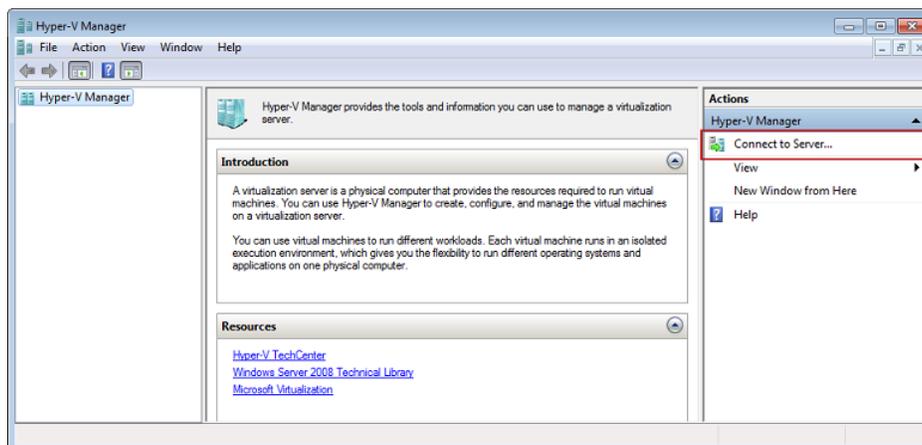
如需连接到管理程序主机

1. 启动 Microsoft Hyper-V Manager (virtmgmt.msc)。



### Note

您可以为客户端计算机启用 Hyper-V Manager 功能。有关启用该功能的详细信息，请转到[安装和配置 Hyper-V 工具用于远程管理](#)。



2. 在操作窗格中，选择连接到服务器...。
3. 在选择计算机对话框中，选择另一台计算机，键入虚拟机监控程序主机的 IP 地址或主机名，然后单击确定。



### Note

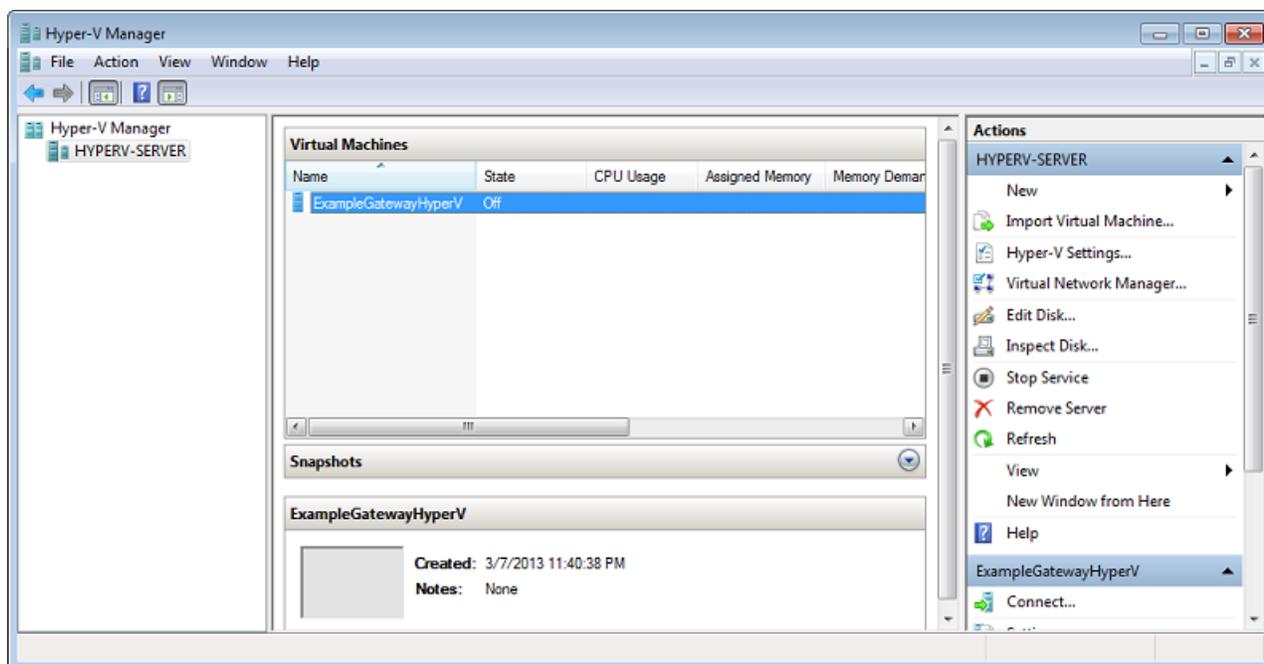
要使用主机名连接到虚拟机监控程序主机，可能需要在 hosts 文件中输入一个条目，以使主机名可映射到正确的 IP 地址。



### Note

如果您没有被添加到管理程序主机的本地管理员中，那么，系统可能会提示您输入证书。

下例展示 Hyper-V 管理器连接到名为 HYPERV-SERVER 的虚拟机监控程序主机，该主机有一个网关 VM。

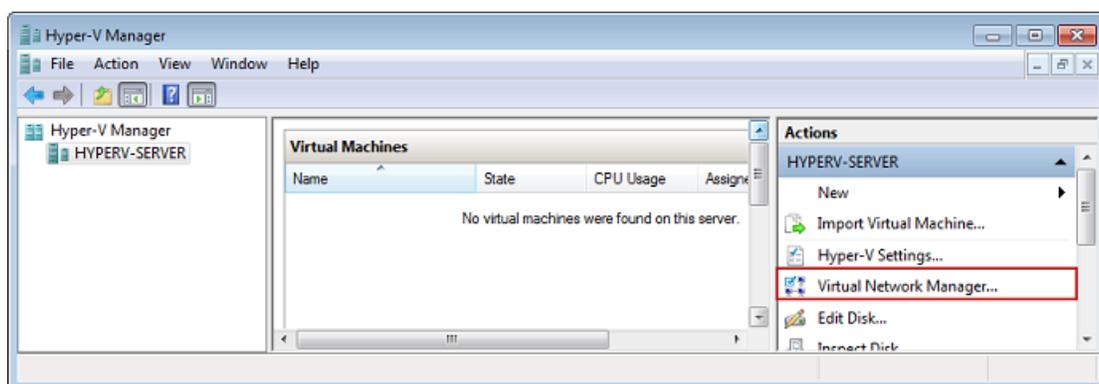


## 配置虚拟网络设置

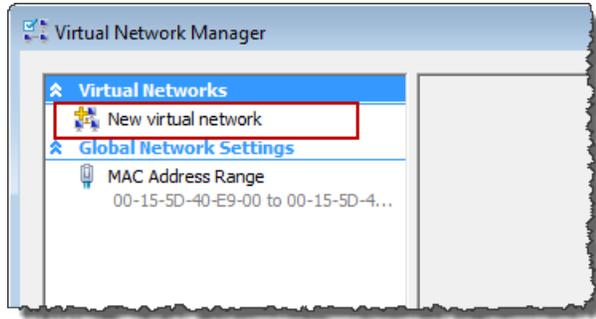
在安装和配置 Microsoft Hyper-V 主机后，我们建议您创建新的虚拟网络和将其关联到主机的网络接口，从而设置虚拟网络。稍后，当您配置网关 VM 时，您必须将其与一个或多个虚拟网络关联，以便 VM 获得连接性。

### 配置您的 Hyper-V 主机的虚拟网络设置

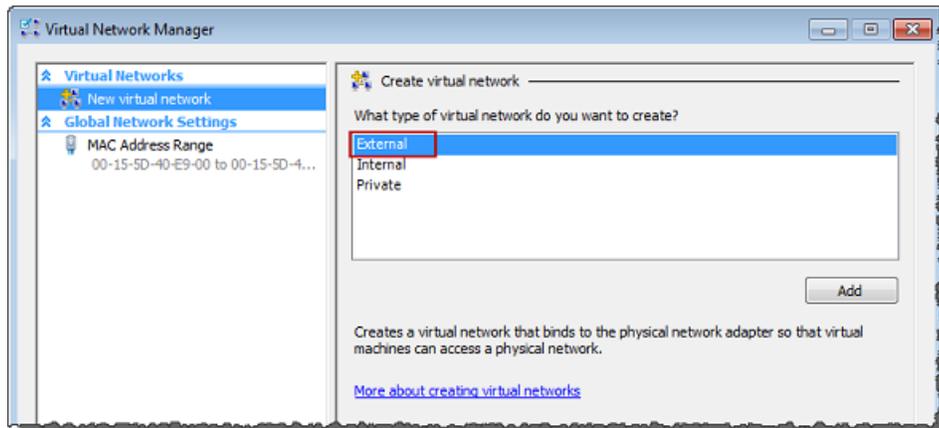
1. 启动 Microsoft Hyper-V Manager (virtmgmt.msc)。
2. 在左边窗格的管理程序主机列表中，选择您的管理程序。
3. 在操作菜单中的虚拟机监控程序主机名（例如，HYPERV-SERVER）下，单击虚拟网络管理器。



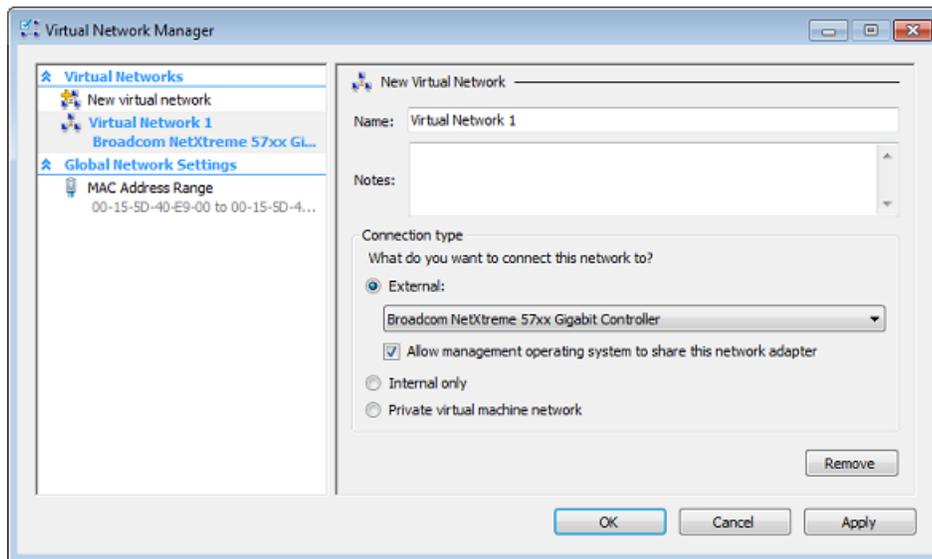
4. 在虚拟网络管理器对话框中，选择新建虚拟网络。



5. 选择外部作为虚拟网络类型，然后单击添加。



6. 为该网络提供一个名称，然后单击确定。



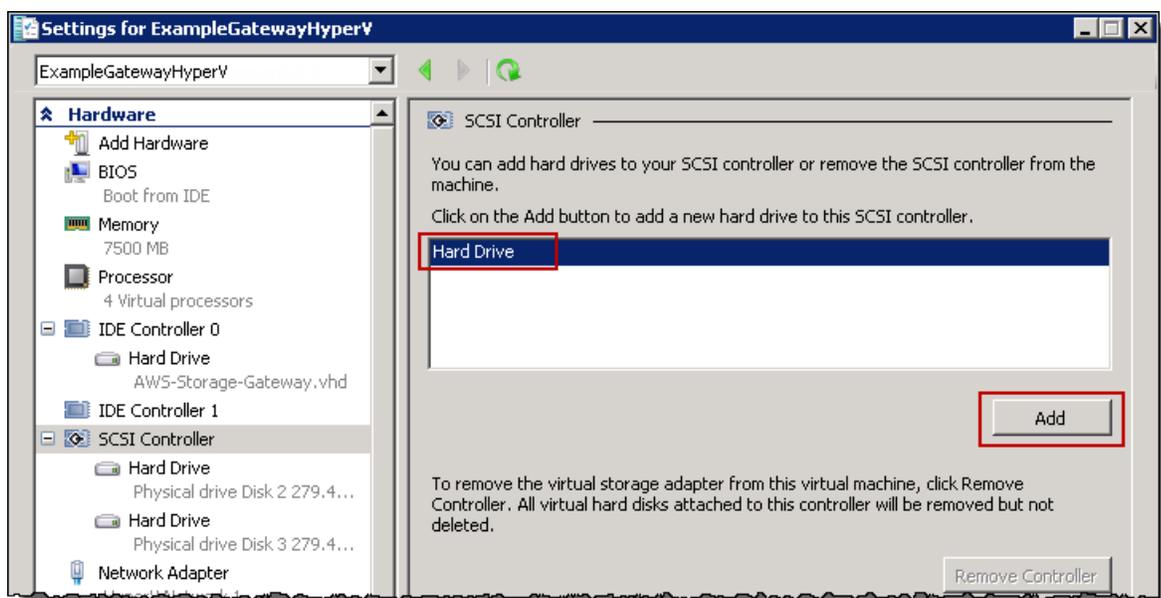
当配置网关虚拟机时，您可以使用此虚拟网络。

## 添加通过硬盘支持的虚拟磁盘

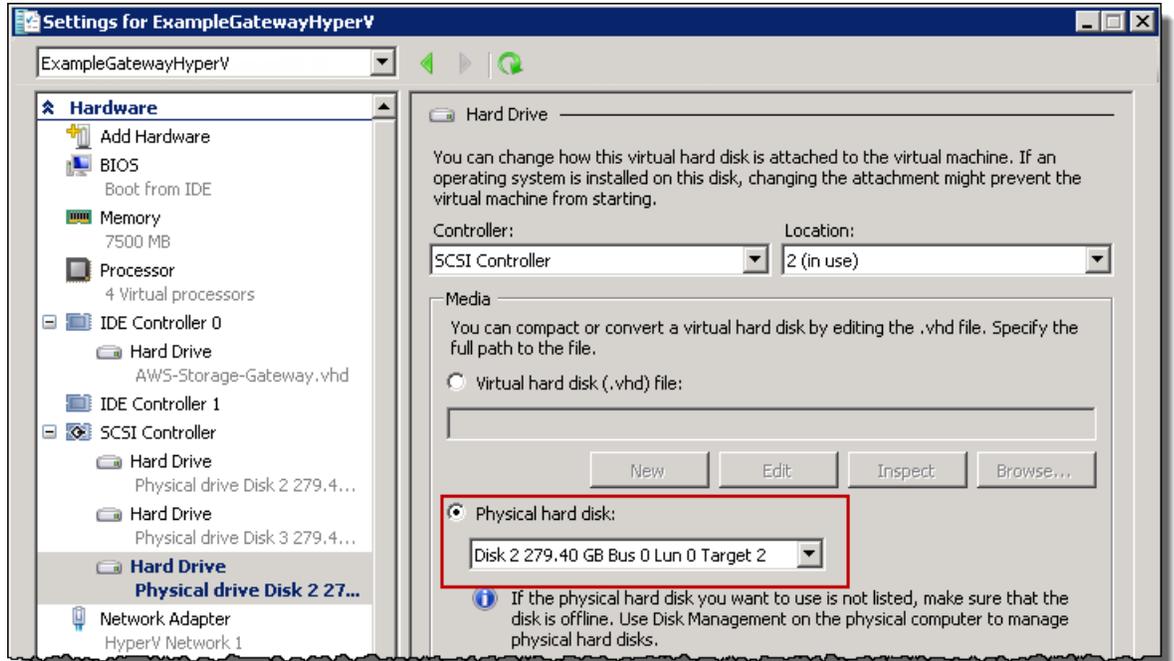
在前一部分中，您预配置了带有 Hyper-V 管理程序的主机。管理程序了解主计算机配置，例如可用处理器、内存和本地硬盘。主机向 AWS Storage Gateway 提供这些资源。您可以通过添加更多存储空间，例如直接连接的磁盘或 SAN 磁盘，有选择地配置该主机。在本部分中，我们介绍如何添加通过直接附加磁盘支持的虚拟磁盘。

### 添加通过物理硬盘支持的虚拟磁盘

1. 启动 Microsoft Hyper-V Manager (virtmgmt.msc)。
2. 选择 VM。
3. 在 VM 的操作列表中，单击设置...。
4. 在硬件列表中，单击 SCSI 控制器。
5. 在 SCSI 控制器窗格中选择硬盘驱动器，然后单击添加。



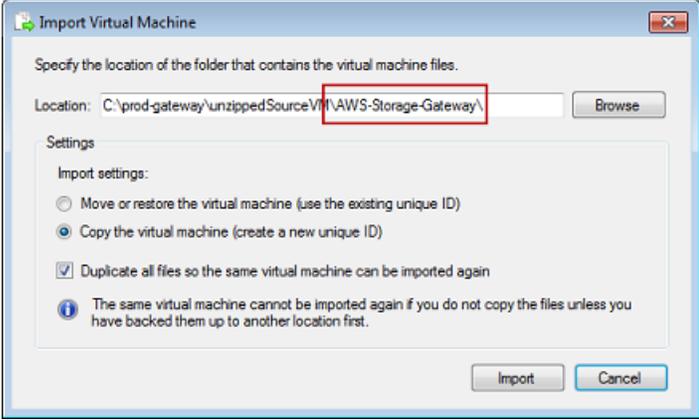
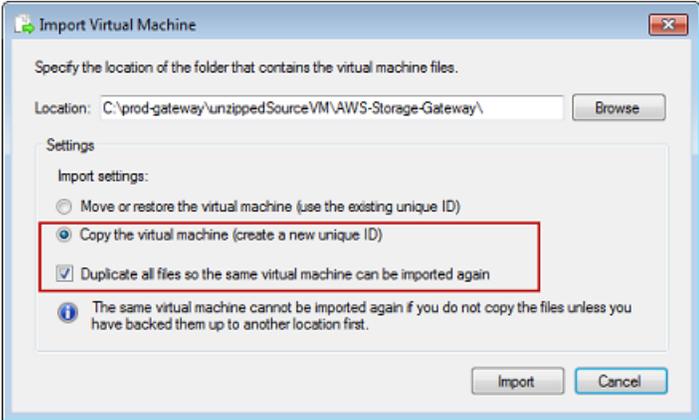
6. 在硬盘驱动器窗格中，选择物理硬盘。



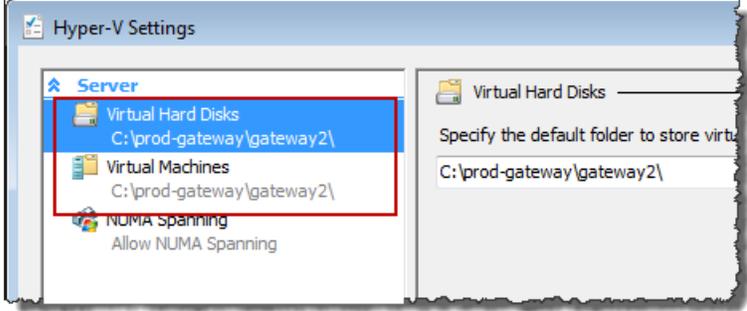
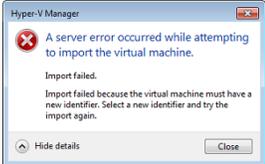
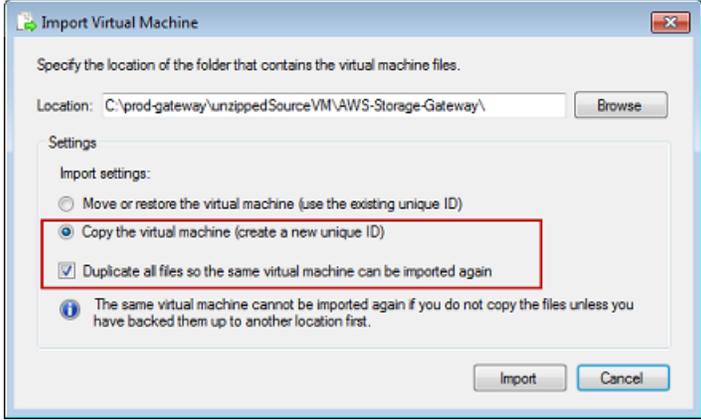
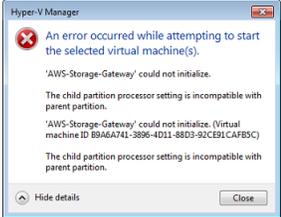
7. 单击确定。

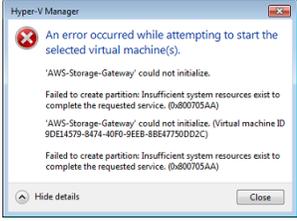
## 故障诊断 Microsoft Hyper-V 设置

下表列出了您在 Microsoft Hyper-V 平台上部署 AWS Storage Gateway 时可能遇到的典型问题。

问题	措施
<p>尝试导入网关时显示错误消息：“导入失败。此处找不到虚拟机导入文件...”。</p> 	<p>出现此错误的原因如下：</p> <ul style="list-style-type: none"><li>• 如果您没有指向解压缩网关源文件的根目录。在导入虚拟机对话框中指定的位置的最后一部分应为 <code>AWS-Storage-Gateway\</code>，如下例所示：</li></ul>  <ul style="list-style-type: none"><li>• 如果已部署网关，但未选择复制虚拟机选项，也未选中导入虚拟机对话框中的复制所有文件... 选项，则在解压缩网关文件的位置创建该 VM，并且无法再次从此位置进行导入。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。</li></ul> 

有关部署网关的详细信息，请参阅 Microsoft Hyper-V 入门练习中的 [下载 AWS Storage Gateway VM 并将其部署在您的主机上 \(p. 35\)](#)。

问题	措施
<p>尝试导入网关时显示错误消息：“导入失败。Import task failed to copy file.”</p> 	<p>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。要解决此问题，请在 Hyper-V 设置对话框中指定新位置。</p>  <p>有关部署网关的详细信息，请参阅 Microsoft Hyper-V 练习中的<a href="#">导入该 VM (p. 39)</a>。</p>
<p>尝试导入网关时显示错误消息：“导入失败。Import failed because the virtual machine must have a new identifier. Select a new identifier and try the import again.”</p> 	<p>在导入网关时，确保选中导入虚拟机对话框中的复制虚拟机选项和复制所有文件... 选项，为该 VM 新建一个独一无二的 ID。下例展示导入虚拟机对话框中应使用的选项。</p>  <p>有关导入网关的详细信息，请参阅 Microsoft Hyper-V 练习中的<a href="#">导入该 VM (p. 39)</a>。</p>
<p>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.”</p> 	<p>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 AWS Storage Gateway 的要求的详细信息，请参阅<a href="#">要求 (p. 7)</a>。</p>

问题	措施
<p>尝试启动网关 VM 时显示错误消息“无法创建分区:系统资源不足,无法完成请求的服务。”</p> 	<p>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。</p> <p>有关 AWS Storage Gateway 的要求的详细信息,请参阅<a href="#">要求 (p. 7)</a>。</p>
<p>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。</p>	<p>网关 VM 的时钟可能会偏离实际的时间,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<a href="#">同步您的网关 VM 时间 (p. 227)</a>。</p>
<p>您必须将解压缩的 Microsoft Hyper-V AWS Storage Gateway 文件放入主机文件系统中。</p>	<p>按照典型 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 <code>hyperv-server</code>,则可使用以下 UNC 路径 <code>\\hyperv-server\c\$</code>,其中假定可解析名称 <code>hyperv-server</code>,或在本地 <code>hosts</code> 文件中定义了该名称。</p>
<p>在连接管理程序时,系统会提示您输入证书。</p> 	<p>以本地管理员的身份使用 <code>Sconfig.cmd</code> 工具给管理程序主机添加用户证书。有关更多信息,请参阅<a href="#">设置和配置 Microsoft Hyper-V 主机 (p. 447)</a>。</p>

## 附录 E : AWS Storage Gateway 资源

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 :

- <https://s3.amazonaws.com/aws-storage-gateway-terms/sources.tar> ( 对于在 VMware ESXi 上部署的网关 )
- [https://s3.amazonaws.com/aws-storage-gateway-terms/sources\\_hyperv.tar](https://s3.amazonaws.com/aws-storage-gateway-terms/sources_hyperv.tar) ( 对于在 Microsoft Hyper-V 上部署的网关 )

本产品包括 OpenSSL Project 开发的用于 OpenSSL Toolkit 中的软件 (<http://www.openssl.org/>)。

组成 AWS Storage Gateway VM 的软件包受到跟踪和监控以发现安全漏洞。发布更新后,将其应用于每个网关,并且更新后的软件包将提高其版本号,但 Linux 发行版的主版本号可能不提高。有关管理更新的详细信息,请参阅[使用 AWS Storage Gateway 控制台管理网关更新 \(p. 212\)](#)。

## 附录 F : AWS Storage Gateway 限制

下表列出 AWS Storage Gateway 中卷、虚拟磁带、上传和下载速率的限制。

	网关缓存卷	网关存储卷	虚拟网关磁带库
卷的最大大小	32 TiB	1 TiB	—
网关中所有卷的总最大大小	150 TiB	12 TiB	—
缓存存储磁盘的最大大小	16 TiB	—	16 TiB
网关中所有缓存磁盘的总最大大小	16 TiB	—	16 TiB
上传缓冲区磁盘的最大大小	2 TiB	2 TiB	2 TiB
网关的所有上传缓冲区磁盘的总最大大小	2 TiB	2 TiB	2 TiB
最低下载速率	51200 bps	51200 bps	—
最低上传速率	102400 bps	102400 bps	—
虚拟磁带的最大大小	—	—	2.5 TiB
虚拟磁带的最小大小	—	—	100 GiB
网关中所有磁带的总大小	—	—	150 TiB
网关的最大卷数	20	12	—
网关中虚拟磁带的最大数量	—	—	1500