亚马逊云科技

磁带网关用户指南

Amazon Storage Gateway

API 版本 2013-06-30

Amazon Storage Gateway: 磁带网关用户指南

Amazon Web Services 文档中描述的 Amazon Web Services 服务或功能可能因区域而异。要查看适用于中国区域的差异，请参阅 中国的 Amazon Web Services 服务入门 (PDF)。

Table of Contents

什么是磁带网关？ 1
磁带网关的工作原理 1
磁带网关 1
入门 Amazon Storage Gateway 5
报名参加 Amazon Storage Gateway 5
创建具有管理员权限的 IAM 用户 6
保护 IAM 用户 6
正在访问 Amazon Storage Gateway 7
Amazon Web Services 区域 支持 Storage Gateway 7
磁带网关设置要求 8
硬件和存储要求 8
的硬件要求 VMs 8
Amazon EC2 实例类型的要求 8
..... 9
存储需求 9
网络和防火墙要求 10
端口要求 11
硬件设备的网络和防火墙要求 19
允许通过防火墙和路由器进行网关访问 22
配置安全组 23
受支持的管理程序和主机要求 23
受支持的 iSCSI 启动程序 24
受支持的第三方备份应用程序 25
使用硬件设备 27
设置硬件设备 28
物理安装硬件设备 29
访问硬件设备控制台 31
配置硬件设备网络参数 32
激活硬件设备 33
在硬件设备上创建网关 34
在硬件设备上配置网关 IP 地址 35
从硬件设备中移除网关软件 37
删除硬件设备 38
创建网关 40

概述 - 网关激活 40
设置网关 40
连接到 Amazon 40
检查并激活 41
概述 - 网关配置 41
概述 - 存储资源 41
创建和激活磁带网关 41
设置磁带网关 41
将您的磁带网关连接到 Amazon 42
检查设置并激活磁带网关 43
配置磁带网关 44
创建磁带 46
WORM 磁带保护 47
手动创建磁带 47
允许自动创建磁带 49
创建自定义磁带池 51
选择类型 51
磁带保留锁定 52
创建自定义磁带池 53
连接 VTL 设备 53
连接到 Microsoft Windows 客户端 54
连接到 Linux 客户端 55
测试网关 58
Arcserve Backup 59
Bacula Enterprise 62
Commvault 65
戴尔 EMC NetWorker 70
IBM 数据保护 74
OpenText 数据保护器 77
Microsoft System Center DPM 83
NovaStor DataCenter/网络 87
Quest NetVault Back 92
Veeam Backup & Replication 95
Veritas Backup Exec 97
Veritas NetBackup 101
接下来该做什么？ 107

在 Virtual Private Cloud 中激活网关 107
为 Storage Gateway 创建 VPC 端点 108
管理磁带网关 109
编辑网关信息 109
管理自动创建磁带功能 110
存档磁带 112
将磁带移至 S3 Glacier Deep Archive 113
检索存档的磁带 113
查看磁带使用情况统计数据 115
删除磁带 115
删除自定义磁带池 116
停用磁带网关 117
理解磁带状态 117
理解 VTL 中的磁带状态信息 118
确定存档中的磁带状态 119
将数据移至新网关 120
将虚拟磁带移至新的磁带网关 120
监控 Storage Gateway 124
了解网关指标 124
Storage Gateway 指标的维度 127
监控上传缓冲区 127
监控缓存存储 129
了解 CloudWatch 警报 131
创建推荐的 CloudWatch 警报 132
创建自定义 CloudWatch 警报 133
监控磁带网关 134
获取磁带网关运行状况日志 135
使用亚马逊 CloudWatch指标 136
了解虚拟磁带指标 137
测量您的磁带网关和之间的性能 Amazon 139
维护网关 142
管理本地磁盘 142
确定本地磁盘存储量 142
添加上传缓冲区或缓存存储 145
管理带宽 146
使用 Storage Gateway 控制台更改带宽限制 147

计划带宽限制 147
使用 适用于 Java 的 Amazon SDK 148
使用 适用于 .NET 的 Amazon SDK 150
使用 Amazon Tools for Windows PowerShell 152
管理网关更新 153
更新频率和预期行为 154
开启或关闭维护更新 154
修改网关维护时段计划 155
手动应用更新 156
关闭网关虚拟机 157
启动和停止磁带网关 157
删除网关和移除资源 158
使用 Storage Gateway 控制台删除网关 158
从本地部署的网关中删除资源 159
从部署在 Amazon EC2 实例上的网关中移除资源 161
使用本地控制台执行维护任务 162
访问网关本地控制台 162
使用 Linux KVM 访问网关本地控制台 162
使用访问网关本地控制台 VMware ESXi 163
使用 Microsoft Hyper-V 访问网关本地控制台 164
在 虚拟机本地控制台上执行任务 165
登录到磁带网关本地控制台 165
为本地网关配置 SOCKS5 代理 166
配置网关网络 168
测试网关到互联网的连接性 172
在本地控制台中为本地网关运行存储网关命令 173
查看您的网关系统资源状态 175
在 EC2 本地控制台上执行任务 176
登录您的 EC2 网关本地控制台 177
配置 HTTP 代理 177
测试网关网络连接 178
查看您的网关系统资源状态 178
在本地控制台上运行 Storage Gateway 命令 179
磁带网关的性能和优化 182
磁带网关的性能指导 182
优化网关性能 184

建议的配置 184
在网关中添加资源 185
优化 iSCSI 设置 187
让磁带驱动器使用更大的数据块 187
优化虚拟磁带驱动器的性能 188
向应用程序环境添加资源 188
安全性 189
数据保护 189
数据加密 190
身份和访问管理 191
受众 192
使用身份进行身份验证 192
使用策略管理访问 195
Stor Amazon age Gateway 如何与 IAM 协作 197
基于身份的策略示例 202
故障排除 205
合规性验证 206
恢复能力 207
基础设施安全性 208
Amazon 安全最佳实践 208
日志记录和监控 209
Storage Gateway 信息位于 CloudTrail 209
了解 Storage Gateway 日志文件条目 210
排查网关问题 212
故障排除：网关离线问题 212
检查关联的防火墙或代理 213
检查是否正在对网关的流量进行 SSL 检查或深度数据包检查 213
检查虚拟机监控程序主机上是否出现停电或硬件故障 213
检查关联的缓存磁盘是否有问题 213
故障排除：网关激活问题 214
解决使用公有端点激活网关时出现的错误 214
解决使用 Amazon VPC 端点激活网关时出现的错误 217
解决使用公有端点激活网关且同一 VPC 中有 Storage Gateway VPC 端点时出现的错误 221
排查本地网关问题 221
激活 Amazon Web Services 支持 以帮助排除网关故障 224
排查 Microsoft Hyper-V 设置问题 226

Amazon EC2 网关问题疑难解答 228
过了一会儿网关并未激活 228
在实例列表中找不到 EC2 网关实例 229
无法将 Amazon EBS 卷附加到 EC2 网关实例 229
您在添加存储卷时收到一条消息，指出“无可用磁盘” 229
如何删除分配为上传缓冲区空间的磁盘，从而减少上传缓冲区空间 229
进出 EC2 网关的吞吐量降至零 229
激活 Amazon Web Services 支持 以帮助排除网关故障 230
使用串行控制台连接到您的 Amazon EC2 网关 231
排查硬件设备问题 231
如何确定服务 IP 地址 231
如何执行出厂重置 232
如何执行远程重启 232
如何获得 Dell iDRAC 支持 232
如何找到硬件设备序列号 232
如何获得硬件设备支持 232
对虚拟磁带问题进行故障排除 233
从无法恢复的网关恢复虚拟磁带 233
排查无法恢复的磁带的问题 236
高可用性运行状况通知 237
排查高可用性问题 237
运行状况通知 237
Metrics 239
最佳实践 240
最佳实践：恢复数据 240
从虚拟机意外关闭中恢复 240
从故障网关或 VM 恢复您的数据 241
从不可恢复磁带恢复数据 241
从出现故障的缓存磁盘恢复数据 241
从不可访问的数据中心恢复数据 242
清理不必要的资源 242
其他资源 244
主机设置 244
为磁带网关部署默认 Amazon EC2 主机 245
为磁带网关部署自定义 Amazon EC2 实例 247
修改 Amazon EC2 实例元数据选项 250

将 VM 时间与 Hyper-V 或 Linux KVM 主机时间同步 250
将 VM 时间与 VMware主机时间同步 251
配置半虚拟化的磁盘控制器 252
为网关配置网络适配器 253
在 Storage Gateway 中使用 VMware 高可用性 257
使用磁带网关存储资源 261
从网关中移除磁盘 262
适用于网关的 EBS EC2 卷 263
使用 VTL 设备 264
使用磁带 267
获取激活密钥 268
Linux (curl) 269
Linux (bash/zsh) 270
微软 Windows PowerShell 271
使用本地控制台 271
连接 iSCSI 启动程序 272
将 VTL 设备连接到 Windows 客户端 273
将 VTL 设备连接到 Linux 客户端 275
自定义 iSCSI 设置 276
配置 CHAP 身份验证 281
Amazon Direct Connect 与 Storage Gateway 一起使用 286
获取网关 IP 地址 286
从 Amazon EC2 主机获取 IP 地址 287
了解资源和资源 IDs 288
使用资源 IDs 288
为资源添加标签 289
使用标签 289
开源组件 290
Storage Gateway 配额 291
磁带的配额 291
为网关建议的本地磁盘大小 291
API 参考 293
必需的请求标头 293
对请求进行签名 295
实例签名计算 296
错误响应 298

异常 298
操作错误代码 300
错误响应 319
运营 321
文档历史记录 322
早期更新 334
发行说明 349
..... ccclii

什么是磁带网关？

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

你可以在本地部署 Storage Gateway 作为在 KVM 或 Microsoft Hyper-V 虚拟机管理程序上 VMware ESXi运行的虚拟机设备，也可以作为硬件设备部署，也可以作为 Amazon 亚马逊实例部署。 EC2 您可以使用托管在 EC2 实例上的网关进行灾难恢复、数据镜像以及为 Amazon EC2 上托管的应用程序提供存储。

要查看 Amazon Storage Gateway 有助于实现的各种用例，请参阅Amazon Storage Gateway。有关定价的最新信息，请参阅 详细信息页上的定价 Amazon Storage Gateway 。

Amazon Storage Gateway 提供基于文件（S3 文件网关和 FSx 文件网关）、基于卷（卷网关）和基于磁带（磁带网关）的存储解决方案。

本用户指南提供与磁带网关相关的信息。

磁带网关提供了支持云的虚拟磁带存储。通过磁带网关，可以采用经济高效且持久的方式在 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 中归档备份数据。磁带网关提供了虚拟磁带基础设施，该基础设施可根据您的业务需求以无缝方式扩展，并可消除预置、扩展和维护物理磁带基础设施的运营负担。

有关架构概述，请参阅 磁带网关的工作原理。

在本用户指南中，可以找到“入门”部分，其中涵盖了所有网关类型通用的设置信息。还可以找到磁带网关设置要求，以及描述如何部署、激活、配置和管理磁带网关的章节。

本用户指南中的过程主要侧重于使用 Amazon Web Services Management Console执行网关操作。如果要以编程方式执行这些操作，请参阅 Amazon Storage Gateway API 参考。

磁带网关的工作原理

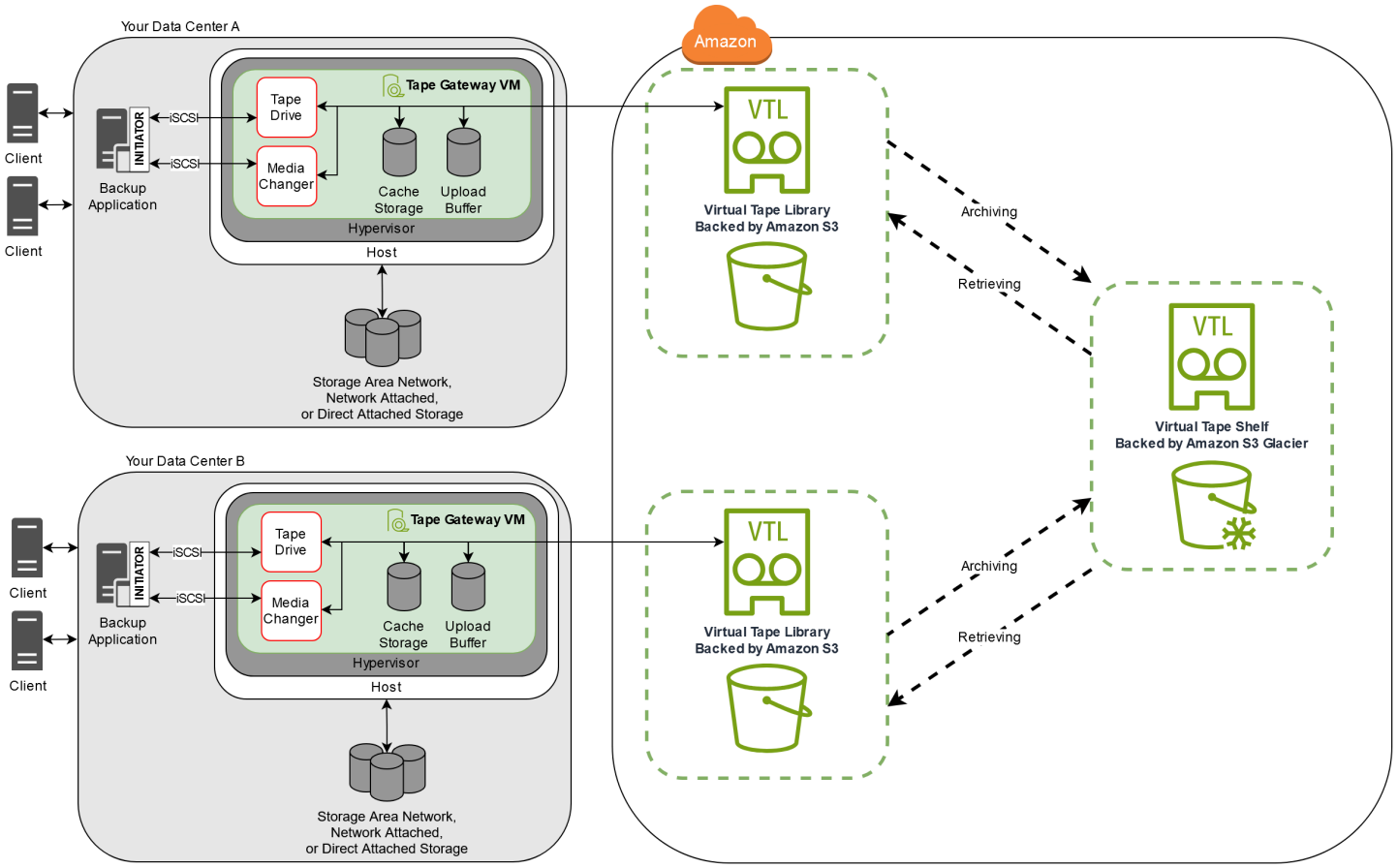
接下来，您可以找到磁带网关解决方案的架构概述。

磁带网关

磁带网关提供了一种经济高效的持久解决方案，可用于在 Amazon Web Services 云中对数据进行存档。利用虚拟磁带库 (VTL) 接口，您可以使用现有的基于磁带的备份基础设施，将数据存储到您在磁

带网关上创建的虚拟磁带盒。每个磁带网关预配置了介质更换器和磁带驱动器。这些可作为 iSCSI 设备用于您的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。

下图概述了磁带网关的部署情况。



该图标识了下列磁带网关组件：

- 虚拟磁带 - 虚拟磁带类似于物理磁带盒。但是，虚拟磁带数据存储在 Amazon Web Services 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 Storage Gateway 控制台创建虚拟磁带，也可以借助 Storage Gateway API 以编程方式创建虚拟磁带。每个网关一次可包含最多 1500 个磁带或最多 1 PiB 总磁带数据。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 15 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。您的 VTL 包括存储的虚拟磁带的集合。每个磁带网关都附带一个 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，该网关会将数据存储在本地，然后以异步方式将数据上传到 VTL 中的虚拟磁带（即 Amazon S3）中。

  - 磁带驱动器 - VTL 磁带驱动器类似于可对磁带执行 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 (10 个)，这些驱动器可作为 iSCSI 设备提供给备份应用程序。
  - 介质更换器 - VTL 介质更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械手。每个 VTL 均附带一个介质更换器，该介质更换器可作为 iSCSI 设备用于您的备份应用程序。
- 存档 - 存档类似于场外磁带容纳设备。您可以将网关 VTL 中的磁带存档到存档。如果需要，可以将存档中的磁带取回到网关的 VTL。
  - 存档磁带 - 当备份软件弹出磁带时，网关会将磁带移至存档以便长期存储。存档位于激活了网关的 Amazon 区域中。存档中的磁带存储在虚拟磁带架 (VTS) 中。VTS 使用 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 来进行备份，这是一种用于数据存档、备份和长期数据留存的低成本存储服务。
  - 取回磁带 - 您无法直接读取存档的磁带。若要读取存档的磁带，您必须先通过使用 Storage Gateway 控制台或 Storage Gateway API 将其取回到磁带网关。

> **Important**
>
> 如果您在 S3 Glacier Flexible Retrieval 中存档磁带，则通常可以在 3-5 小时内取回磁带。如果您在 S3 Glacier Deep Archive 中存档磁带，则通常可以在 12 小时内取回磁带。

在部署并激活磁带网关后，您在本地应用程序服务器上将虚拟磁带驱动器和介质更换器作为 iSCSI 设备安装。您可以根据需要创建虚拟磁带。然后您可以使用现有备份软件应用程序将数据写入虚拟磁带中。介质更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 - 缓存存储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，则网关会先检查缓存存储空间中的数据，然后再从中下载数据 Amazon。
- 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恢复点也非常重要。有关更多信息，请参阅 您需要从发生故障的磁带网关恢复虚拟磁带。

当备份应用程序将数据写入网关时，网关会将数据复制到缓存存储和上传缓冲区中。然后，它会确认已完成对备份应用程序的写入操作。

有关要为缓存存储和上传缓冲区分配的磁盘空间量的指南，请参阅确定本地磁盘存储量。

入门 Amazon Storage Gateway

本节提供入门说明 Amazon。您需要一个 Amazon 账号才能开始使用 Amazon Storage Gateway。可以使用现有 Amazon 账户，也可以注册新账户。您的 Amazon 账户中还需要一个属于群组的 IAM 用户，该用户具有执行 Storage Gateway 任务所需的管理权限。具有相应权限的用户可以访问 Storage Gateway 控制台和 Storage Gateway API，来执行网关部署、配置和维护任务。如果您是首次使用 Storage Gateway 的用户，我们建议您在使用它之前，查看 Supported Amazon regions 和 Tape Gateway setup requirements 部分。

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

主题

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

报名参加 Amazon Storage Gateway

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

如果您没有 Amazon Web Services 账户，请完成以下步骤来创建一个。

要注册 Amazon Web Services 账户

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

   在注册时，将接到电话，要求使用电话键盘输入一个验证码。

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

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

创建具有管理员权限的 IAM 用户

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

保护 IAM 用户

注册后 Amazon Web Services 账户，请开启多重身份验证 (MFA)，保护您的管理用户。有关说明，请参阅《IAM 用户指南》中的 为 IAM 用户启用虚拟 MFA 设备（控制台）。

要允许其他用户访问您的 Amazon Web Services 账户 资源，请创建 IAM 用户。为了保护您的 IAM 用户，请启用 MFA 并仅向 IAM 用户授予执行任务所需的权限。

有关创建和保护 IAM 用户的更多信息，请参阅《IAM 用户指南》中的以下主题：

- 在你的 IAM 用户中创建 Amazon Web Services 账户
- 适用于 Amazon 资源的访问权限管理
- 基于 IAM 身份的策略示例

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

正在访问 Amazon Storage Gateway

可以使用 Amazon Storage Gateway 控制台来执行各种网关配置和维护任务，包括在部署中激活或移除 Storage Gateway 硬件设备，创建、管理和删除不同类型的网关，创建、管理和删除虚拟磁带库中的磁带，以及监控 Storage Gateway 服务的各个元素的运行状况和状态。为了简单易用，本指南重点介绍使用 Storage Gateway 控制台 Web 界面来执行任务。可以通过 Web 浏览器访问 Storage Gateway 控制台，网址为：https://console.amazonaws.cn/storagegateway/home/。

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

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

有关定价的信息，请参阅 Amazon Storage Gateway 定价。

Amazon Web Services 区域 支持 Storage Gateway

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

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

设置磁带网关的要求

除非另有说明，否则所有网关配置都需要满足以下要求。

主题

- 硬件和存储要求
- 网络和防火墙要求
- 受支持的管理程序和主机要求
- 受支持的 iSCSI 启动程序
- 磁带网关支持的第三方备份应用程序

硬件和存储要求

本节介绍网关的最低硬件和设置要求，以及为所需存储分配的最小磁盘空间量。

的硬件要求 VMs

在部署网关时，您必须确保部署网关虚拟机的基础硬件能够分配以下最少资源：

- 分配给 VM 的四个虚拟处理器。
- 对于磁带网关，您的硬件应使用以下数量的 RAM：
  - 对于缓存大小不超过 16 TiB 的网关，预留 16 GiB 的 RAM
  - 对于缓存大小为 16 TiB 至 32 TiB 的网关，预留 32 GiB 的 RAM
  - 对于缓存大小为 32 TiB 至 64 TiB 的网关，预留 48 GiB 的 RAM
- 80 GiB 磁盘空间，用于安装虚拟机映像和系统数据。

有关更多信息，请参阅 优化网关性能。有关硬件如何影响网关 VM 的性能的信息，请参阅 Amazon Storage Gateway 配额。

Amazon EC2 实例类型的要求

在亚马逊弹性计算云 (Amazon EC2) 上部署网关时，实例大小必须至少为 x large 才能使网关正常运行。但是，对于计算优化型实例系列，大小必须至少为 2xlarge。

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

对于 me Gat eway 磁带网关，您的 Amazon EC2 实例应根据您计划用于网关的缓存大小分配以下数量的 RAM：

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

使用为您的网关类型推荐的以下实例类型之一。

推荐用于磁带网关

- 通用型实例系列 – m4、m5 或 m6 实例类型。
- 计算优化型实例系列 — c4、c5、c6 或 c7 实例类型。选择 2xlarge 实例大小或更大的大小，以满足所需的 RAM 要求。
- 内存优化型实例系列 — r3、r5、r6 或 r7 实例类型。
- 存储优化型实例系列 — i3、i4 或 i7 实例类型。

存储需求

除了 VM 的 80 GiB 磁盘空间外，您还需要为网关提供其他磁盘。

下表为所部署的网关推荐了本地磁盘存储的大小。

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

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

有关网关配额的信息，请参阅Amazon Storage Gateway 配额。

网络和防火墙要求

您的网关需要具有对 Internet、本地网络、域名服务 (DNS) 服务器、防火墙、路由器等的访问权。在下文中，您可以找到有关所需端口的信息，并了解如何进行设置以允许通过防火墙和路由器进行访问。

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

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

主题

- 端口要求
- Storage Gateway 硬件设备的网络和防火墙要求
- 允许通过防火墙和路由器进行 Amazon Storage Gateway 访问
- 为您的 Amazon EC2 网关实例配置安全组

端口要求

T@@ ape Gat 要求允许特定端口通过您的网络安全，才能成功部署和运行。所有网关都需要某些端口，而其他端口则仅用于特定配置，例如连接到 VPC 终端节点时。

磁带网关网关的端口要求

网络元素	From	目的	协议	端口	入站	出站	必需	备注
Web 浏览器	您的 Web 浏览器	Storage Gateway VM	TCP HTTP	80	✓	✓	✓	供本地系统用来获取 Storage Gateway 激活密钥。仅在激活 Storage Gateway 设备期间使用端口 80。Storage Gateway VM 不要求可公开访问端口 80。端口 80 所需的访问级别取决于网络配置。如

网络元素	From	目的	协议	端口	入站	出站	必需	备注
								果您从 Storage Gateway 管理控制台激活网关，则从中连接到控制台的主机必须能够访问网关的端口 80。
Web 浏览器	Storage Gateway VM	Amazon	TCP HTTPS	443	✓	✓	✓	Amazon 管理控制台（所有其他操作）
DNS	Storage Gateway VM	域名服务 (DNS) 服务器	TCP 和 UDP DNS	53	✓	✓	✓	用于 Storage Gateway 虚拟机与 DNS 服务器之间的通信，以解析 IP 名称。

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

网络元素	From	目的	协议	端口	入站	出站	必需	备注
								的网关不是必需EC2的。

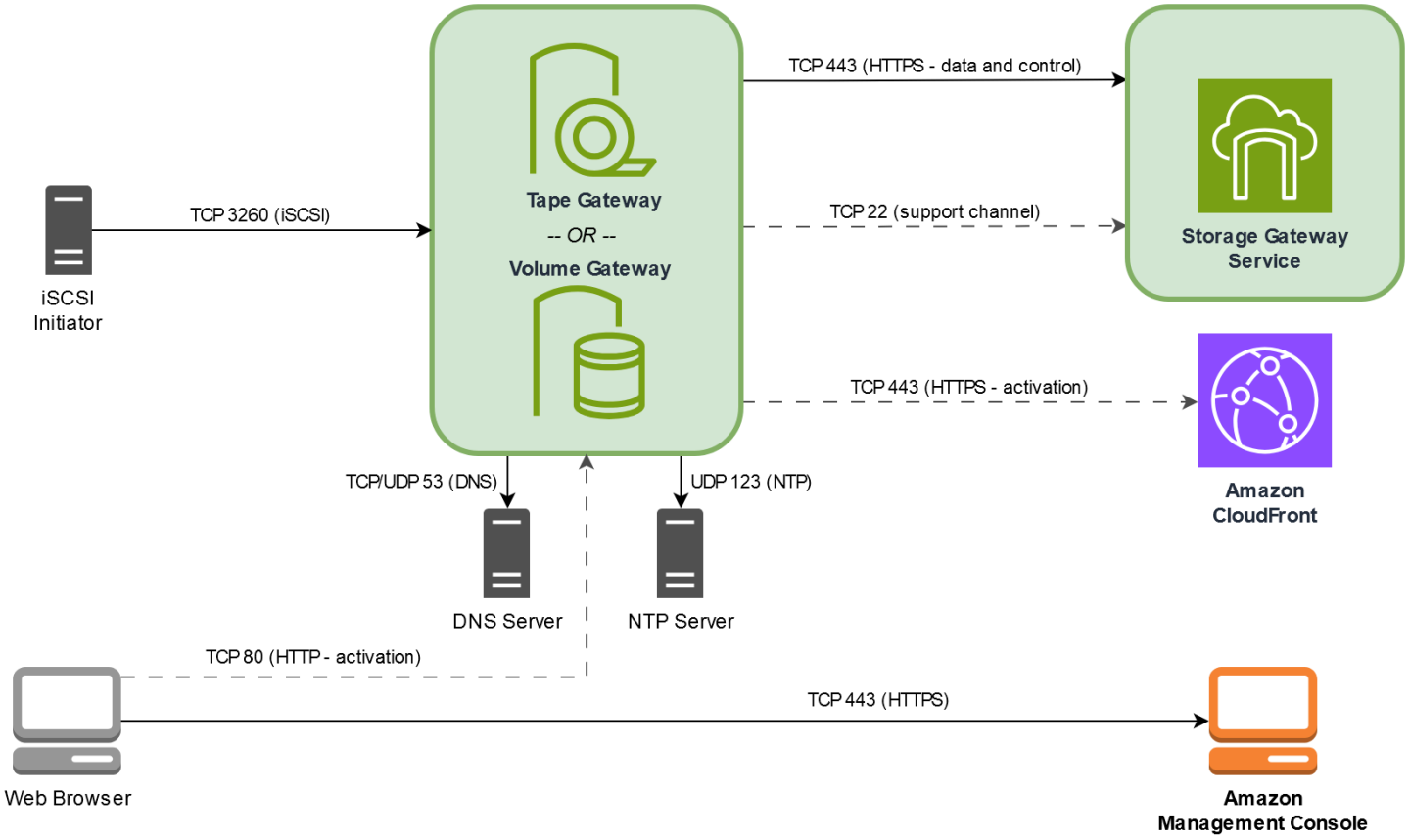
网络元素	From	目的	协议	端口	入站	出站	必需	备注
Storage Gateway	Storage Gateway VM	Amazon Web Services 支持 端点	TCP SSH	22	✓	✓	✓	Amazon Web Services 支持 允许访问您的网关以帮助您解决网关问题。您无需打开此端口即可实现网关的正常操作，但在进行问题排查时需要如此。有关支持端点的列表，请参阅Amazon Web Services 支持 端点。

网络元素	From	目的	协议	端口	入站	出站	必需	备注
Storage Gateway	Storage Gateway VM	Amazon	TCP HTTPS	443	✓	✓	✓	管理控制台
Amazon CloudFront	Storage Gateway VM	Amazon	TCP HTTPS	443	✓	✓	✓	用于激活
VPC	Storage Gateway VM	Amazon	TCP HTTPS	443	✓	✓	✓*	管理控制台 *仅在使用 VPC 终端节点时才需要
VPC	Storage Gateway VM	Amazon	TCP HTTPS	1026		✓	✓*	控制平面端点 *仅在使用 VPC 终端节点时才需要

网络元素	From	目的	协议	端口	入站	出站	必需	备注
VPC	Storage Gateway VM	Amazon	TCP HTTPS	1027		✓	✓*	匿名控制平面（用于激活） *仅在使用 VPC 终端节点时才需要
VPC	Storage Gateway VM	Amazon	TCP HTTPS	1028		✓	✓*	代理端点 *仅在使用 VPC 终端节点时才需要
VPC	Storage Gateway VM	Amazon	TCP HTTPS	1031		✓	✓*	数据层面 *仅在使用 VPC 终端节点时才需要

网络元素	From	目的	协议	端口	入站	出站	必需	备注
VPC	Storage Gateway VM	Amazon	TCP HTTPS	2222		✓	✓*	适用于 SSH Support 频道 VPCe *仅在使用 VPC 终端节点时打开支持频道时才需要
VPC	Storage Gateway VM	Amazon	TCP HTTPS	443	✓	✓	✓*	管理控制台 *仅在使用 VPC 终端节点时才需要
iSCSI 客户端	iSCSI 客户端	Storage Gateway VM	TCP	3260	✓	✓	✓	让本地系统连接到网关公开的 iSCSI 目标。

下图显示了基本的 Volume Gatewa 。



Storage Gateway 硬件设备的网络和防火墙要求

每个 Storage Gateway 硬件设备都需要以下网络服务：

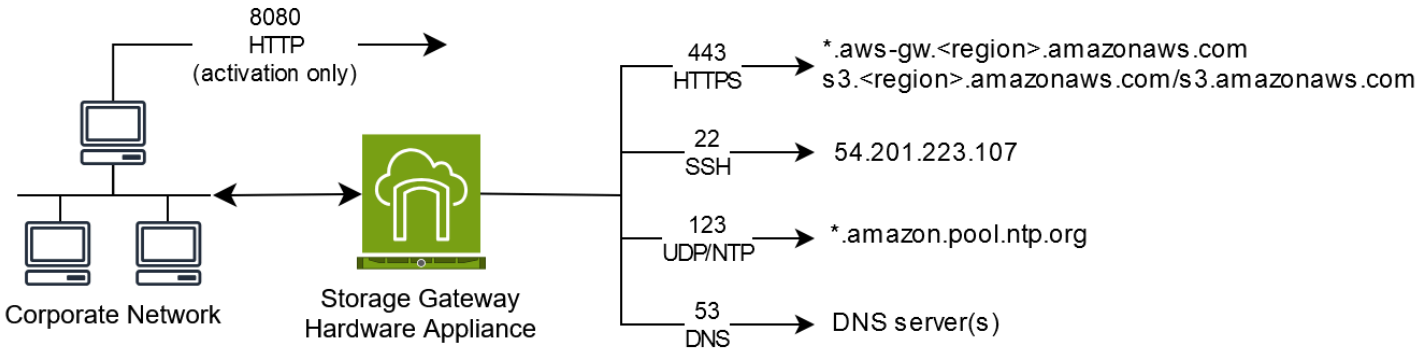
- Internet 访问 - 通过服务器上的任何网络接口实现与 Internet 的永久性网络连接。
- DNS 服务 - 用于硬件设备和 DNS 服务器之间的通信的 DNS 服务。
- 时间同步 - 必须可访问自动配置的 Amazon NTP 时间服务。
- IP 地址-分配的 DHCP IPv4 地址或静态地址。您不能分配 IPv6 地址。

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

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

5. em4

您可以使用 iDRAC 端口进行远程服务器管理。



硬件设备需要以下端口才能运行。

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

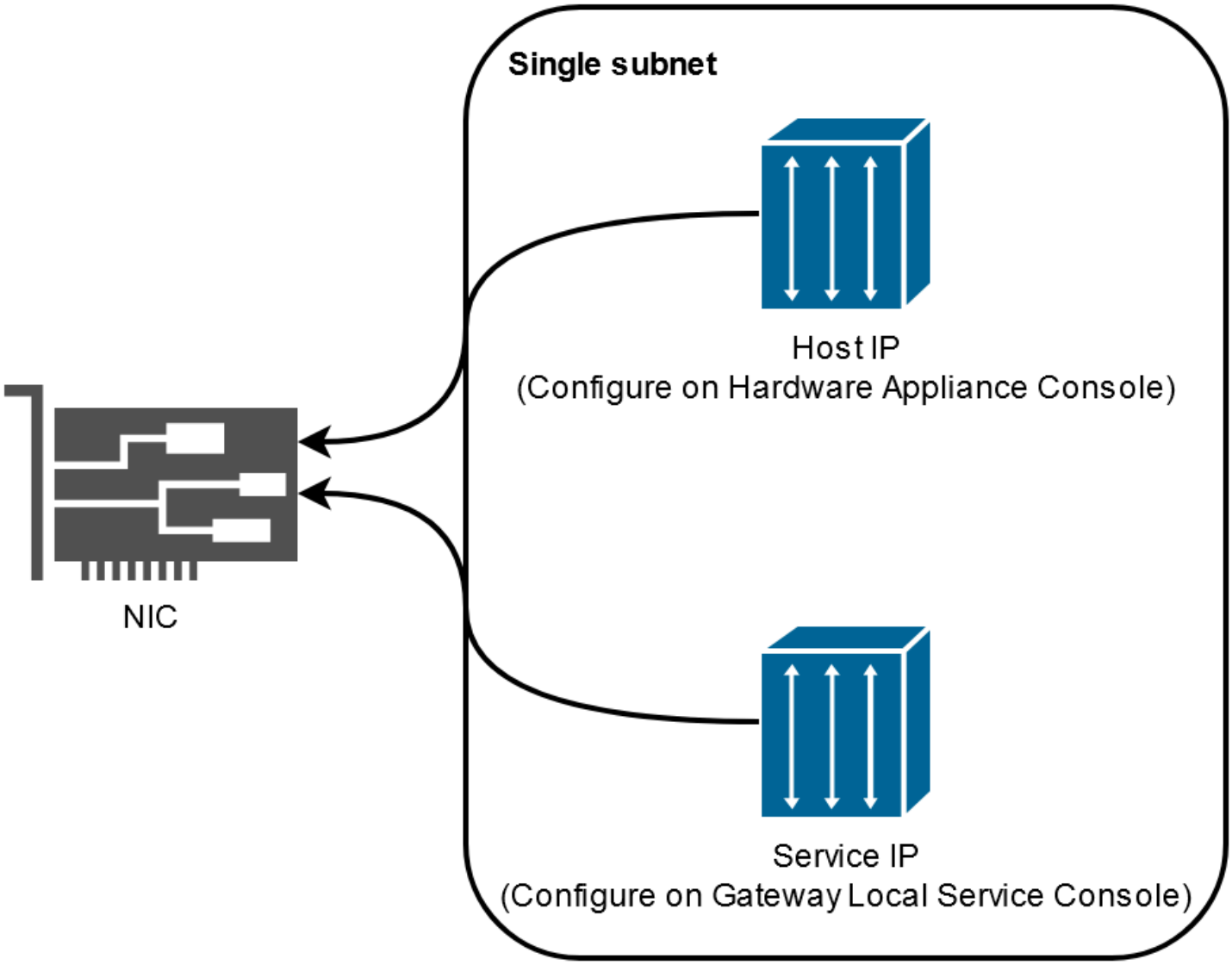
要按设计的方式运行，硬件设备需要下面所示的网络和防火墙设置：

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

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

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

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



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

允许通过防火墙和路由器进行 Amazon Storage Gateway 访问

您的网关需要访问以下服务终端节点才能与之通信 Amazon。如果使用防火墙或路由器来筛选或限制网络流量，则必须配置防火墙和路由器以允许这些服务端点与 Amazon进行出站通信。

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

> **Important**
>
> 根据网关的 Amazon 区域，在服务终端节点*region*中替换为正确的区域字符串。

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

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

调用 API 需要使用以下网关服务端点。

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

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

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

Storage Gateway VM 配置为使用以下 NTP 服务器。

```
0.amazon.pool.ntp.org
1.amazon.pool.ntp.org
2.amazon.pool.ntp.org
3.amazon.pool.ntp.org
```

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

为您的 Amazon EC2 网关实例配置安全组

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

- 安全组不应允许来自外部 Internet 的传入连接。它应仅允许网关安全组内的实例与网关进行通信。如果您需要允许实例从该安全组的外部连接到网关，我们建议您只允许端口 3260 (适用于 iSCSI 连接) 和端口 80 (适用于激活) 上的连接。
- 如果您想从网关安全组之外的 Amazon EC2 主机激活网关，请允许从该主机的 IP 地址通过端口 80 进行传入连接。如果您不能确定激活主机的 IP 地址，则可以打开端口 80、激活网关，然后在完成激活后关闭端口 80 上的访问。
- 仅当使用端口 22 Amazon Web Services 支持 进行故障排除时，才允许访问。有关更多信息，请参阅 你 Amazon Web Services 支持 想帮忙排除 EC2 网关故障。

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

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

有关要为您的网关开放的端口的信息，请参阅端口要求。

受支持的管理程序和主机要求

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

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

Storage Gateway 支持以下管理程序版本和主机：

- VMware ESXi 虚拟机管理程序（版本 7.0 或 8.0）-对于此设置，还需要一个 VMware vSphere 客户端来连接到主机。
- Microsoft Hyper-V 管理程序（版本 2012 R2、2016、2019 或 2022）- Hyper-V 的免费独立版本可从 Microsoft 下载中心获取。对于此设置，您需要 Microsoft Windows 客户端计算机上的 Microsoft Hyper-V Manager 才能连接到主机。
- 基于 Linux 内核的虚拟机 (KVM) - 免费的开源虚拟化技术。Linux 2.6.20 及更高版本中都包括了 KVM。Storage Gateway 已通过测试，并受到 CentOS/RHEL 7.7、Ubuntu 16.04 LTS 和 Ubuntu 18.04 LTS 发行版的支持。任何其他现代 Linux 发行版可能有效，但不能保证功能或性能。如果您已经启动并运行了 KVM 环境并且您已经熟悉 KVM 的工作原理，我们建议使用此选项。
- 亚马逊 EC2 实例 — Storage Gateway 提供包含网关 VM 映像的亚马逊系统映像 (AMI)。只能在 Amazon 上部署文件、缓存卷和磁带网关类型 EC2。有关如何在 Amazon 上部署网关的信息 EC2，请参阅为磁带网关部署自定义 Amazon EC2 实例。
- Storage Gateway 硬件设备 - 对于具有有限虚拟机基础架构的位置，Storage Gateway 提供了物理硬件设备来作为本地部署选项。

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

受支持的 iSCSI 启动程序

部署磁带网关时，网关会预先配置一个介质更换器和 10 个磁带驱动器。这些磁带驱动器和介质更换器可作为 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，Storage Gateway 支持以下 iSCSI 启动程序：

- 微软 Windows 服务器 2022
- Red Hat Enterprise Linux 8
- Red Hat Enterprise Linux 9
- VMware ESX Initiator，它提供了在您的客户机操作系统中使用启动器的替代方案 VMs

> **Important**
>
> Storage Gateway 不支持来自 Windows 客户端的 Microsoft Multipath I/O (MPIO)。如果主机使用 Windows Server 失效转移集群 (WSFC) 协调访问，Storage Gateway 支持将多个主机与同一个卷关联。但是，若未使用 WSFC，则不能将多个主机连接到同一个卷 (例如，共享非群集 NTFS/ext4 文件系统)。

磁带网关支持的第三方备份应用程序

使用备份应用程序通过磁带网关读取、写入和管理磁带。您选择的介质更换器的类型取决于您计划使用的备份应用程序。

Amazon 已测试下表中的第三方备份应用程序，以确保与这些 Tape Gateway 特性和功能兼容：

- 发现功能包括 iSCSI 启动器连接、介质更换器、重新扫描、自动和手动设备映射。
- 磁带功能包括创建、删除、导入、导出、清点和条形码可见性。
- 擦除磁带内容并验证后续恢复中不包含任何数据。
- 将数据备份到单个和多个磁带，验证超过磁带容量的备份作业是否会暂停以等待更多磁带。
- 从磁带恢复全部和部分数据，并验证数据完整性。
- 在备份操作期间，在网关关闭和重启事件后验证功能和数据完整性。

备份应用程序	版本	介质更换器类型	网关版本已测试
Arcserve Backup	19	AWS-Gateway-VTL	2.12.3
Bacula Enterprise	15.0.2	AWS-Gateway-VTL 或 STK-L700	2.12.3
Commvault	2024E/11.36.35	STK-L700	2.12.3
戴尔 EMC NetWorker	19.10	AWS-Gateway-VTL	2.12.3
IBM 存储保护	8.1.10	IBM-03584L32-0402	全部
Micro Focus Data Protector	24.4	AWS-Gateway-VTL	2.12.3

备份应用程序	版本	介质更换器类型	网关版本已测试
微软系统中心数据保护管理器	2025	STK-L700	2.12.3
NovaStor DataCenter	9.5.3	STK-L700	2.12.3
任务 NetVault Backup	13.3	STK-L700	2.12.3
Veeam Backup & Replication	12	AWS-Gateway-VTL	全部
Veritas Backup Exec	24	AWS-Gateway-VTL	全部
Veritas NetBackup	10.5	AWS-Gateway-VTL	2.12.3

Important

我们强烈建议您选择为备份应用程序列出的介质更换器。其他介质更换器可能无法正常工作。激活网关之后，您可以选择另一种介质更换器。有关更多信息，请参阅在网关激活后选择介质更换器。

使用 Storage Gateway 硬件设备

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

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

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

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

在以下几节中，可以找到有关如何对 Storage Gateway 硬件设备进行设置、机架安装、通电、配置、激活、启动、使用和删除的说明。

主题

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

设置 Storage Gateway 硬件设备

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

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

安装和配置硬件设备

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

   在硬件设备上设置网关的方式与在微软 Hyper-V VMware ESXi、基于 Linux 内核的虚拟机 (KVM) 或亚马逊上设置网关的方式相同。 EC2

增加可用缓存存储

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

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

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

网络接口卡选项

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

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

物理安装硬件设备

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

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

先决条件

要安装您的硬件设备，需要以下组件：

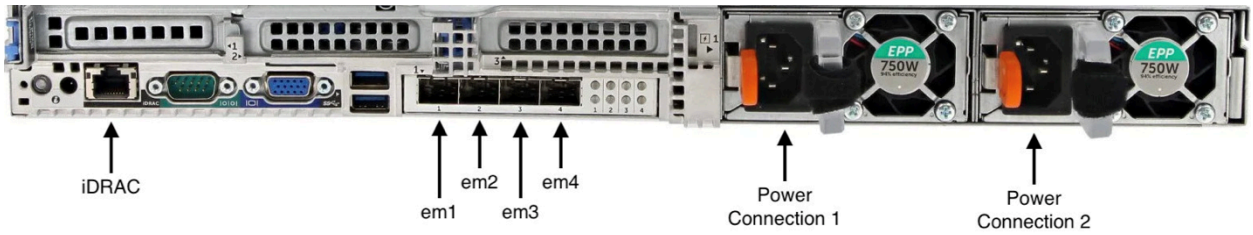
- 电源线：必需有一根，建议使用两根。
- 支持的网络布线（取决于硬件设备中包括的网络接口卡 (NIC)）。Twinax 铜质 DAC、SFP+ 光学模块（兼容英特尔）或 SFP 转 Base-T 铜质收发器。
- 键盘和显示器，或键盘、视频和鼠标 (KVM) 切换解决方案。

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

物理安装硬件设备

1. 拆开硬件设备包装，并按照箱内包含的说明操作，在机架上安装服务器。

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



   带有网络和电源连接器标签的硬件设备一背面。

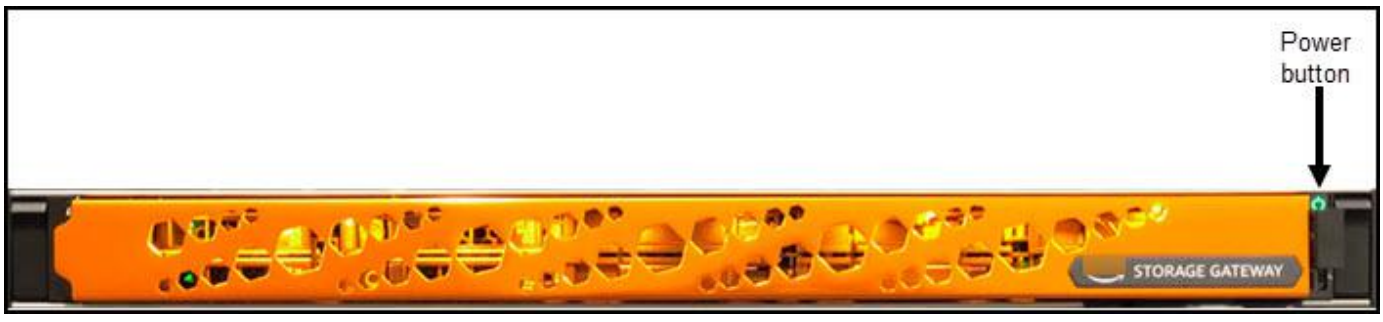
2. 插上到两个电源的电源连接。可以仅插上一个电源连接，但我们建议插上这两个电源连接来提供冗余。

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

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

4. 将键盘和显示器插入电源。

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



   带有电源按钮标签的硬件设备正面。

下一步

访问硬件设备控制台

访问硬件设备控制台

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

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

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

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

设置管理员密码

- 在请设置您的登录密码提示处，执行以下操作：

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

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

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

下一步

配置硬件设备网络参数

配置硬件设备网络参数

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

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

设置网络地址

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

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

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

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

     完成后，选择保存，然后按 Enter 来保存配置。

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

建议不要在同一个子网上配置多个网络接口，因为这有时会导致路由问题。

从硬件控制台注销

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

下一步

激活 Storage Gateway 硬件设备

激活 Storage Gateway 硬件设备

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

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

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

激活 Storage Gateway 硬件设备

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

   > **Note**
   >
   > 如果只激活，必须满足以下条件：
   >
   > - 您的浏览器必须与您的硬件设备位于同一网络上。

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

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

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

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

此时，硬件设备概览页面上会出现一个横幅，指示硬件设备已成功激活。

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

下一步

在硬件设备上创建网关

在硬件设备上创建网关

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

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

在硬件设备上创建网关

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

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

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

下一步

在硬件设备上配置网关 IP 地址

在硬件设备上配置网关 IP 地址

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

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

在设备上配置 IP 地址以使用应用程序

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

默认账户为 admin，默认密码为 password。

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

3. Amazon 设备激活 - 配置页面包括以下菜单选项：

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

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

   输入相应的数字以导航到网络配置页面。

4. 执行以下操作之一来配置网关 IP 地址：

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

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

退出网关本地控制台

- 按 Crtl+]（右方括号）按键。硬件控制台随即会出现。

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

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

从硬件设备中移除网关软件

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

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

从硬件设备中删除网关

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

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

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

删除网关不会从控制台删除硬件设备。硬件设备将保留以供将来进行网关部署。

删除 Storage Gateway 硬件设备

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

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

> **Note**
>
> 要将设备移至其他 Amazon 帐户或 Amazon Web Services 区域，必须先使用以下步骤将其删除，然后打开网关的支持渠道并联系 Amazon Web Services 支持 以执行软重置。有关更多信息，请参阅开启 Amazon Web Services 支持 访问权限以帮助对本地托管的网关进行故障排除开启 Amazon Web Services 支持 访问以帮助对本地。

删除硬件设备

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

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

创建网关

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

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

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

概述 - 网关激活

网关激活包括设置网关，将其连接到 Amazon，然后查看您的设置并激活它。

设置网关

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

连接到 Amazon

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

检查并激活

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

概述 - 网关配置

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

概述 - 存储资源

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

创建和激活磁带网关

在此部分中，您可以找到有关如何下载、部署和激活标准磁带网关的说明。

主题

- 设置磁带网关
- 将您的磁带网关连接到 Amazon
- 检查设置并激活磁带网关
- 配置磁带网关

设置磁带网关

设置新的磁带网关

1. 打开 Amazon Web Services Management Console at https://console.aws.amazon.com/storagegateway/home/，然后选择要创建网关 Amazon Web Services 区域 的位置。

2. 选择创建网关来打开设置网关页面。
3. 在网关设置部分，执行以下操作：
   a. 对于 Gateway name (网关名称)，输入网关的名称。您可以搜索此名称，以便在 Storage Gateway 控制台的列表页面上找到您的网关。
   b. 对于网关时区，选择要在其中部署网关的地区的本地时区。
4. 在网关选项部分中，对于网关类型，选择磁带网关。
5. 在平台选项部分中，执行以下操作：
   a. 对于主机平台，选择要在其中部署网关的平台，然后按照 Storage Gateway 控制台页面上显示的平台特定说明来设置主机平台。可从以下选项中进行选择：
      - VMware ESXi-使用下载、部署和配置网关虚拟机 VMware ESXi。
      - Microsoft Hyper-V - 使用 Microsoft Hyper-V 下载、部署和配置网关虚拟机。
      - Linux KVM - 使用 Linux KVM 下载、部署和配置网关虚拟机。
      - Amazon EC2-配置并启动一个用于托管您的网关的亚马逊 EC2实例。此选项不适用于存储卷网关。
      - 硬件设备-订购专用的物理硬件设备 Amazon 来托管您的网关。
   b. 对于确认设置网关，选中复选框来确认您已为所选的主机平台执行部署步骤。此步骤不适用于硬件设备主机平台。
6. 在备份应用程序设置部分，对于备份应用程序，选择要用于将磁带数据备份到与磁带网关关联的虚拟磁带的应用程序。
7. 选择下一步以继续。

现在，您的网关已设置完毕，您需要选择您想要的网关连接和通信方式 Amazon。有关说明，请参阅 Connect 您的磁带网关连接到 Amazon。

将您的磁带网关连接到 Amazon

将新的磁带网关连接到 Amazon

1. 如果您尚未完成设置磁带网关中所述的步骤，请完成这些步骤。完成后，选择下一步，在 Storage Gateway 控制台中打开连接到 Amazon 页面。
2. 在终端节点选项部分中，对于服务终端节点，选择网关将用于通信的终端节点的类型 Amazon。可从以下选项中进行选择：

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

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

- VPC 托管 - 您的网关通过与 VPC 的私有连接与 Amazon 进行通信，从而使您可以控制自己的网络设置。如果选择此选项，则必须指定现有 VPC 端点，方法是从下拉菜单中选择其 VPC 端点 ID，或者提供其 VPC 端点 DNS 名称或 IP 地址。有关更多信息，请参阅 Activating your gateway in a virtual private cloud。

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

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

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

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

4. 选择下一步以继续。

既然您已经选择了网关的连接方式 Amazon，那么您需要激活网关。有关说明，请参阅检查设置并激活磁带网关。

检查设置并激活磁带网关

激活新的磁带网关

1. 如果尚未完成以下主题中所述的程序，请先完成这些程序：

   - 设置磁带网关

- 将您的磁带网关连接到 Amazon

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

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

> **Note**
>
> 激活网关后，您无法修改网关选项或连接设置。

4. 选择激活网关以继续。

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

配置磁带网关

对新的磁带网关执行首次配置

1. 如果尚未完成以下主题中所述的程序，请先完成这些程序：

   - 设置磁带网关
   - 将您的磁带网关连接到 Amazon
   - 检查设置并激活磁带网关

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

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

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

> **Note**
>
> 要接收 Storage Gateway 运行状况日志，日志组资源策略中必须存在以下权限。将替换*highlighted section*为您部署的特定日志组 ResourceARN 信息。
>
> ```
> "Sid": "AWSLogDeliveryWrite20150319",
>       "Effect": "Allow",
>       "Principal": {
>         "Service": [
>           "delivery.logs.amazonaws.com"
>         ]
>       },
>       "Action": [
>         "logs:CreateLogStream",
>         "logs:PutLogEvents"
>       ],
>       "Resource": "arn:aws:logs:eu-west-1:1234567890:log-group:/foo/bar:log-stream:*"
> ```
>
> 只有在您想要将权限显式应用于单个日志组时，才需要使用“Resource”元素。

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

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

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

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

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

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

您已经创建了网关，现在需要创建供网关使用的虚拟磁带。有关说明，请参阅创建磁带。

为磁带网关创建新的虚拟磁带

本节介绍如何使用创建新的虚拟磁带 Amazon Storage Gateway。您可以使用 Amazon Storage Gateway 控制台或 Storage Gateway API 手动创建新的虚拟磁带。您还可以将磁带网关配置为自动创建磁带，从而有助于减少对手动磁带管理的需求、简化大型部署，并有助于扩展本地和存档存储需求。

磁带网关支持虚拟磁带上的一次写入多次读取 (WORM) 和磁带保留锁定。已激活 WORM 的虚拟磁带有助于确保无法覆盖或擦除虚拟磁带库中活动磁带上的数据。有关虚拟磁带的 WORM 保护的更多信息，请参阅以下部分，the section called “WORM 磁带保护”。

借助磁带保留锁定，您可以指定已存档虚拟磁带的保留模式和期限，从而在长达 100 年的固定时间段内防止删除这些磁带。这包括权限控制，用于控制谁可以删除磁带或修改保留设置。有关磁带保留锁定的更多信息，请参阅the section called “磁带保留锁定”。

> **Note**
>
> 您只需为写入磁带的数据量而非整个磁带容量付费。
> 您可以使用 Amazon Key Management Service (Amazon KMS) 对写入虚拟磁带的数据进行加密，这些数据存储在亚马逊简单存储服务 (Amazon S3) Simple S3 Service 中。目前，您可以使用 Amazon Storage Gateway API 或 Amazon Command Line Interface (Amazon CLI) 来执行此操作。有关更多信息，请参阅CreateTapes或创建磁带。

一次写入多次读取 (WORM) 磁带保护

您可以通过在 Amazon Storage Gateway中激活虚拟磁带的 WORM 保护来防止覆盖或擦除虚拟磁带。创建磁带时会激活虚拟磁带的 WORM 保护。

无法覆盖写入 WORM 虚拟磁带的数据。只有新数据可以追加到 WORM 虚拟磁带，无法擦除现有数据。激活虚拟磁带的 WORM 保护有助于在磁带处于使用状态时、弹出和存档之前对其进行保护。

仅在创建磁带时才可设置 WORM 配置，且在创建磁带后无法更改配置。

手动创建磁带

您可以使用 Amazon Storage Gateway 控制台或 Storage Gateway API 手动创建新的虚拟磁带。控制台提供了创建磁带的便捷界面，可以灵活地为随机生成的磁带条形码指定前缀。如果您需要完全自定义磁带条形码（例如，匹配相应物理磁带的序列号），则必须使用 API。有关使用 Storage Gateway API 创建磁带的更多信息。请参阅 Stor age Gateway API 参考CreateTapeWithBarcode中的。

使用 Storage Gateway 控制台手动创建虚拟磁带

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在导航窗格中，选择 Gateways (网关) 选项卡。
3. 选择创建磁带来打开创建磁带窗格。
4. 对于 Gateway (网关)，选择网关。将为此网关创建磁带。
5. 对于磁带类型，请选择标准来创建标准虚拟磁带。选择 WORM 来创建一次写入多次读取 (WORM) 虚拟磁带。有关更多信息，请参阅一次写入多次读取 (WORM) 磁带保护。
6. 对于 Number of tapes (磁带数)，请选择要创建的磁带数量。有关磁带配额的更多信息，请参阅Amazon Storage Gateway 配额。
7. 对于 Capacity (容量)，请输入要创建的虚拟磁带的大小。磁带必须大于 100 GiB。有关容量配额的信息，请参阅Amazon Storage Gateway 配额。
8. 对于 Barcode prefix (条码前缀)，请输入要在虚拟磁带条码前面附加的前缀。

   > **Note**
   >
   > 虚拟磁带由条码唯一标识，您可以为该条码添加前缀。您可以使用前缀来协助识别虚拟磁带。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。

9. 对于池，选择 Glacier 池、Deep Archive 池或您创建的自定义池。该池确定在备份软件弹出磁带后将磁带存储到哪个存储类。

- 如果要在 S3 Glacier Flexible Retrieval 存储类中存档磁带，请选择 Glacier 池。在备份软件弹出磁带时，将在 S3 Glacier Flexible Retrieval 中自动存档磁带。对于更多活动存档，可以使用 S3 Glacier Flexible Retrieval，这样您通常可以在 3-5 小时内取回磁带。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的用于存档对象的存储类。
- 如果要在 S3 Glacier Deep Archive 存储类中存档磁带，请选择 Deep Archive 池。在备份软件弹出磁带时，将在 S3 Glacier Deep Archive 中自动存档磁带。您可以使用 S3 Glacier Deep Archive 实现长期数据留存和数字保留，每年访问一次或两次其中的数据。您通常可以在 12 小时内取回在 S3 Glacier Deep Archive 中存档的磁带。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的用于存档对象的存储类。
- 选择自定义池（如果有）。您可以将自定义磁带池配置为使用 Deep Archive 池或 Glacier 池。当备份软件弹出磁带时，磁带将存档到配置的存储类。

如果您在 S3 Glacier Flexible Retrieval 中存档数据，以后可以将其转移到 S3 Glacier Deep Archive。有关更多信息，请参阅 将磁带移至 S3 Glacier Deep Archive 存储类。

> **Note**
>
> 对于在 2019 年 3 月 27 日之前创建的磁带，在备份软件弹出磁带时，直接在 S3 Glacier Flexible Retrieval 中存档磁带。

10. （可选）对于标签，选择添加新标签，并输入键和值来将标签添加到您的磁带。标签是帮助您管理、筛选和搜索磁带的区分大小写的键/值对。
11. 选择 Create tapes (创建磁带)。
12. 在导航窗格中，选择磁带库 > 磁带来查看您的磁带。默认情况下，此列表一次最多显示 1000 个磁带，但您执行的搜索会应用于所有磁带。您可以使用搜索栏来查找符合特定条件的磁带，也可以将列表缩减到少于 1000 个磁带。当您的列表包含 1000 个或更少磁带时，您可以按各种属性以升序或降序对磁带进行排序。

在创建虚拟磁带时，虚拟磁带的状态最初设置为 CREATING (正在创建)。创建磁带后，其状态变为 AVAILABLE (可用)。有关更多信息，请参阅 理解磁带状态。

允许自动创建磁带

磁带网关会自动创建新的虚拟磁带，从而维持您配置的最小可用磁带数。然后，它会将这些新磁带设为可由备份应用程序导入，以便备份作业可以不间断地运行。如果允许自动创建磁带，则除了无需手动创建新的虚拟磁带之外，也不需要编写自定义脚本。

当磁带网关的磁带数量少于为自动创建磁带而指定的最小可用磁带数量时，磁带网关会自动大规模生成新磁带。在以下情况下会大规模生成新磁带：

- 从导入/导出槽中导入磁带。
- 磁带已导入磁带驱动器。

网关保留最少数量的磁带，并在自动磁带创建策略中指定条形码前缀。如果磁带数量少于带条形码前缀的磁带的最小数量，则网关会自动创建足够多的新磁带，以便达到自动创建磁带策略中指定的最小磁带数量。

当您弹出磁带并将其放入import/export slot, that tape does not count toward the minimum number of tapes specified in your automatic tape creation policy. Only tapes in the import/export插槽时，会被视为 “可用”。导出磁带不会启动自动磁带创建。只有导入会影响可用磁带的数量。

将带有相同条形码前缀的磁带从import/export slot to a tape drive or storage slot reduces the number of tapes in the import/export插槽中移出。网关会创建新的磁带，从而为该条形码前缀保持最低可用磁带数量。

允许自动创建磁带

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在导航窗格中，选择 Gateways (网关) 选项卡。
3. 选择要为其自动创建磁带的网关。
4. 在 Actions (操作) 菜单上，选择 Configure tape auto-create (配置自动创建磁带)。

   此时会显示磁带自动创建页面。您可以在这里添加、更改或删除磁带自动创建选项。
5. 要允许自动创建磁带，请选择添加新项目，然后配置自动创建磁带的设置。
6. 对于磁带类型，请选择标准来创建标准虚拟磁带。选择 WORM 创建 write-once-read-many(WORM) 虚拟磁带。有关更多信息，请参阅一次写入多次读取 (WORM) 磁带保护。
7. 对于最小磁带数，请输入磁带网关上应始终可用的最小虚拟磁带数。此值的有效范围是 1 到 10。

8. 对于 Capacity (容量)，请输入虚拟磁带的容量大小（以字节为单位）。有效范围是 100 GiB 至 15 TiB。
9. 对于 Barcode prefix (条码前缀)，请输入要在虚拟磁带条码前面附加的前缀。

   > **Note**
   >
   > 虚拟磁带由条码唯一标识，您可以为该条码添加前缀。该前缀为可选，但是，可将其用于帮助识别虚拟磁带。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。

10. 对于池，选择 Glacier 池、Deep Archive 池或您创建的自定义池。该池确定在备份软件弹出磁带后将磁带存储到哪个存储类。

    - 如果要在 S3 Glacier Flexible Retrieval 存储类中存档磁带，请选择 Glacier 池。在备份软件弹出磁带时，将在 S3 Glacier Flexible Retrieval 中自动存档磁带。对于更多活动存档，可以使用 S3 Glacier Flexible Retrieval，这样您通常可以在 3-5 小时内取回磁带。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的用于存档对象的存储类。
    - 如果要在 S3 Glacier Deep Archive 存储类中存档磁带，请选择 Deep Archive 池。在备份软件弹出磁带时，将在 S3 Glacier Deep Archive 中自动存档磁带。您可以使用 S3 Glacier Deep Archive 实现长期数据留存和数字保留，每年访问一次或两次其中的数据。您通常可以在 12 小时内取回在 S3 Glacier Deep Archive 中存档的磁带。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的用于存档对象的存储类。
    - 选择自定义池（如果有）。您可以将自定义磁带池配置为使用 Deep Archive 池或 Glacier 池。当备份软件弹出磁带时，磁带将存档到配置的存储类。

    如果您在 S3 Glacier Flexible Retrieval 中存档数据，以后可以将其转移到 S3 Glacier Deep Archive。有关更多信息，请参阅 将磁带移至 S3 Glacier Deep Archive 存储类。

    > **Note**
    >
    > 对于在 2019 年 3 月 27 日之前创建的磁带，在备份软件弹出磁带时，直接在 S3 Glacier Flexible Retrieval 中存档磁带。

11. 配置完设置后，选择保存更改。
12. 在导航窗格中，选择磁带库 > 磁带来查看您的磁带。默认情况下，此列表一次最多显示 1000 个磁带，但您执行的搜索会应用于所有磁带。您可以使用搜索栏来查找符合特定条件的磁带，也可以将列表缩减到少于 1000 个磁带。当您的列表包含 1000 个或更少磁带时，您可以按各种属性以升序或降序对磁带进行排序。

在创建可用虚拟磁带时，其状态最初被设置为 CREATING (正在创建)。创建磁带后，其状态变为 AVAILABLE (可用)。有关更多信息，请参阅 理解磁带状态。

有关如何更改自动创建磁带策略或如何从磁带网关中删除自动创建磁带功能的更多信息，请参阅管理自动创建磁带功能。

下一步

使用您的磁带网关

创建自定义磁带池

本节介绍如何在 Amazon Storage Gateway中创建新的自定义磁带池。

主题

- 选择磁带池类型
- 使用磁带保留锁定
- 创建自定义磁带池

选择磁带池类型

Amazon Storage Gateway 使用磁带池来确定弹出磁带时您希望将其存档的存储类别。Storage Gateway 提供两个标准磁带池：

- Glacier 池 - 在 S3 Glacier Flexible Retrieval 存储类中存档磁带。在备份软件弹出磁带时，将在 S3 Glacier Flexible Retrieval 中自动存档磁带。对于更多活动存档，可以使用 S3 Glacier Flexible Retrieval，这样您通常可以在 3-5 小时内取回磁带。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的用于存档对象的存储类。
- Deep Archive 池 - 在 S3 Glacier Deep Archive 存储类中存档磁带。在备份软件弹出磁带时，将在 S3 Glacier Deep Archive 中自动存档磁带。您可以使用 S3 Glacier Deep Archive 实现长期数据留存和数字保留，每年访问一次或两次其中的数据。您通常可以在 12 小时内取回在 S3 Glacier Deep Archive 中存档的磁带。有关详细信息，请参阅《Amazon Simple Storage Service 用户指南》中的用于存档对象的存储类。

如果您在 S3 Glacier Flexible Retrieval 中存档数据，以后可以将其转移到 S3 Glacier Deep Archive。有关更多信息，请参阅 将磁带移至 S3 Glacier Deep Archive 存储类。

Storage Gateway 还支持创建自定义磁带池，让您可以激活磁带保留锁，从而在一定时间内（最长 100 年）防止删除存档的磁带或将其移动到另一个磁带池。这包括锁定权限控制，用于控制谁可以删除磁带或修改保留设置。

使用磁带保留锁定

借助磁带保留锁定，您可以锁定已存档的磁带。磁带保留锁定是自定义磁带池中磁带的选项。已激活磁带保留锁定的磁带在固定的时间段（最长 100 年）内无法删除或移动到另一个存储池。

您可以选择以下两种模式中的一种来配置磁带保留锁定：

- 治理模式 — 在治理模式下配置时，只有具有执行权限的 Amazon Identity and Access Management (IAM) 用户`storagegateway:BypassGovernanceRetention`才能从池中移除磁带。如果您使用 Amazon Storage Gateway API 移除磁带，则还必须将设置`BypassGovernanceRetention`为`true`。
- 合规性模式 - 在合规性模式下进行配置时，任何用户（包括 root Amazon Web Services 账户）都无法删除保护。

  在合规性模式下锁定磁带后，即无法更改其保留锁定类型，也不能缩短其保留期限。合规性模式锁定类型有助于确保在保留期限内无法覆盖或删除磁带。

> **Important**
>
> 创建自定义池后即无法更改其配置。

您可以在创建自定义磁带池时激活磁带保留锁定。附加到自定义池的任何新磁带都会继承该池的保留锁定类型、期限和存储类。

您还可以通过在默认池和您创建的自定义池之间移动磁带，来激活在此功能发布之前存档的磁带上的磁带保留锁定。如果存档磁带，则磁带保留锁定将立即生效。

> **Note**
>
> 如果您在 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 存储类之间移动存档的磁带，则需要支付移动磁带的费用。如果存储类保持不变，则将磁带从默认池移动到自定义池无需支付额外费用。

创建自定义磁带池

使用 Amazon Storage Gateway 控制台，按照以下步骤来创建自定义磁带池。

创建自定义磁带池

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在左侧导航窗格中，选择磁带库，然后选择池选项卡。
3. 选择创建池来打开创建池窗格。
4. 在名称中，输入唯一的名称来标识您的自定义磁带池。池名称必须在 2 到 100 个字符之间。
5. 对于存储类，请选择 Glacier 或 Glacier Deep Archive。
6. 对于保留锁定类型，请选择无、合规性或监管。

   > **Note**
   >
   > 如果选择合规性，则任何用户（包括 root Amazon Web Services 账户）都无法删除磁带保留锁定。

7. 如果您选择磁带保留锁定类型，请输入以天为单位的保留期。最长保留周期为 36500 天（100 年）。
8. （可选）对于标签，请选择添加新标签，将标签添加到自定义磁带池。标签是有助于管理、筛选和搜索自定义磁带池且区分大小写的键/值对。

   输入标签的键和（可选）值。您最多可以向磁带池添加 50 个标签。
9. 选择创建池来创建新的自定义磁带池。

连接 VTL 设备

在下文中，您可以找到有关如何将虚拟磁带库 (VTL) 设备连接到 Microsoft Windows 或 Red Hat Enterprise Linux (RHEL) 客户端的说明。

主题

- 连接到 Microsoft Windows 客户端
- 连接到 Linux 客户端

连接到 Microsoft Windows 客户端

以下过程显示连接到 Windows 客户端时需要遵循的步骤摘要。

将 VTL 设备连接到 Windows 客户端

1. 启动 `iscsicpl.exe`。

   > **Note**
   >
   > 必须具有客户端计算机上的管理员权限才能运行 iSCSI 启动程序。

2. 启动 Microsoft iSCSI 启动程序服务。
3. 在 iSCSI Initiator Properties (iSCSI 发起程序属性) 对话框中，选择 Discovery (发现) 选项卡，然后选择 Discover Portal (发现门户)。
4. 对于 IP 地址或 DNS 名称，提供磁带网关的 IP 地址。
5. 选择 Targets (目标) 选项卡，然后选择 Refresh (刷新)。Discovered targets (发现的目标) 框中将显示所有 10 个磁带驱动器和介质更换器。目标的状态为 Inactive (不活动)。
6. 选择第一个设备，然后连接它。一次连接一个设备。
7. 连接所有目标。

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，并在必要时更新驱动程序和提供商：

验证和更新驱动程序和提供商

1. 在 Windows 客户端上，启动“设备管理器”。
2. 展开 Tape drives (磁带驱动器)，打开磁带驱动器的上下文（右键单击）菜单，然后选择 Properties (属性)。
3. 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。
4. 如果 Driver Provider (驱动程序提供方) 不是 Microsoft，则设置如下值：

   a. 选择 Update Driver (更新驱动程序)。

   b. 在 Update Driver Software (更新驱动程序软件) 对话框中，选择 Browse my computer for driver software (浏览计算机以查找驱动程序软件)。

c. 在 Update Driver Software (更新驱动程序软件) 对话框中，选择 Let me pick from a list of device drivers on my computer (从计算机的设备驱动程序列表中选取)。

d. 选择 LTO Tape drive (LTO 磁带驱动器)，然后选择Next (下一步)。

5. 选择 Close (关闭) 以关闭 Update Driver Software (更新驱动程序软件) 窗口，然后验证 Driver Provider (驱动程序提供方) 值现在是否设置为 Microsoft。

6. 重复这些步骤以更新所有磁带驱动器的驱动程序和提供商。

连接到 Linux 客户端

以下过程显示连接到 RHEL 客户端时需要遵循的步骤摘要。

将 Linux 客户端连接到 VTL 设备

1. 安装 `iscsi-initiator-utils` RPM 软件包。

   您可以使用下面的命令来安装该包。

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

2. 确保 iSCSI 守护进程正在运行。

   对于 RHEL 8 或 9，请使用以下命令。

   ```
   sudo service iscsid status
   ```

3. 发现为网关定义的卷或 VTL 设备目标。使用以下发现命令。

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

   发现命令的输出内容类似如下示例输出内容。

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

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

4. 连接到目标。

   请务必在 connect 命令中指定正确的*[GATEWAY_IP]*和 IQN。

   使用以下命令。

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

5. 验证卷是否已附加到客户端机器 (启动程序)。为此，请使用以下命令。

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

命令的输出内容应类似如下示例输出内容。

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

对于卷网关，在设置启动程序后，我们强烈建议您按 自定义您的 Linux iSCSI 设置 中介绍的方式自定义 iSCSI 设置。

确认 VTL 设备已附加到客户端机器（启动程序）。为此，请使用以下命令。

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

命令的输出内容应类似如下示例输出内容。

```
total 0
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-mediachanger-lun-0-changer -> ../../sg20
lrwxrwxrwx 1 root root 9 Sep 8 11:19 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-01-lun-0 -> ../../st6
lrwxrwxrwx 1 root root 10 Sep 8 11:19 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-01-lun-0-nst -> ../../nst6
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-02-lun-0 -> ../../st7
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-02-lun-0-nst -> ../../nst7
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-03-lun-0 -> ../../st8
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-03-lun-0-nst -> ../../nst8
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-04-lun-0 -> ../../st9
```

```
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-04-lun-0-nst -> ../../nst9
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-05-lun-0 -> ../../st10
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-05-lun-0-nst -> ../../nst10
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-06-lun-0 -> ../../st11
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-06-lun-0-nst -> ../../nst11
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-07-lun-0 -> ../../st12
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-07-lun-0-nst -> ../../nst12
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-08-lun-0 -> ../../st13
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-08-lun-0-nst -> ../../nst13
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-09-lun-0 -> ../../st14
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-09-lun-0-nst -> ../../nst14
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-10-lun-0 -> ../../st15
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-10-lun-0-nst -> ../../nst15
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x0000000000000012-lun-0-
changer -> ../../sg6
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001c-lun-0
 -> ../../st0
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001c-
lun-0-nst -> ../../nst0
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001f-lun-0
 -> ../../st1
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001f-
lun-0-nst -> ../../nst1
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x0000000000000022-lun-0
 -> ../../st2
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.0-fc-0x0000000000000022-
lun-0-nst -> ../../nst2
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000025-lun-0
 -> ../../st5
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000025-
lun-0-nst -> ../../nst5
```

```
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000028-lun-0
 -> ../../st3
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000028-
lun-0-nst -> ../../nst3
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.1-fc-0x000000000000002b-lun-0
 -> ../../st4
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x000000000000002b-
lun-0-nst -> ../../nst4
```

下一步

使用备份软件来测试您的网关设置

使用备份软件来测试您的网关设置

您可通过使用备份应用程序执行以下任务来测试磁带网关设置：

1. 配置备份应用程序以检测您的存储设备。

> **Note**
>
> 为了提高 I/O 性能，我们建议在备份应用程序中将磁带驱动器的数据块大小设置为 1 MB。有关更多信息，请参阅让磁带驱动器使用更大的数据块。

2. 将数据备份到磁带。
3. 将磁带存档。
4. 从存档中检索磁带。
5. 从磁带还原数据。

要测试您的设置，请使用兼容的备份应用程序，如下所述。

> **Note**
>
> 除非另有说明，所有的备份应用程序都在 Microsoft Windows 上经过了检验。

有关兼容备份应用程序的更多信息，请参阅磁带网关支持的第三方备份应用程序。

主题

- 使用 Arcserve Backup 测试设置
- 使用 Bacula Enterprise 测试您的设置
- 使用 Commvault 测试您的设置
- 使用 Dell EMC 测试您的设置 NetWorker
- 使用 IBM Data Protect 测试您的设置
- 使用 D OpenText ata Protector 测试您的设置
- 使用 Microsoft System Center DPM 测试您的设置
- 使用以下方法测试您的设置 NovaStor DataCenter
- 使用 Quest B NetVault ackup 测试您的设置
- 使用 Veeam Backup and Replication 测试您的设置
- 使用 Veritas Backup Exec 测试您的设置
- 使用 Veritas 测试您的设置 NetBackup

使用 Arcserve Backup 测试设置

您可以使用 Arcserve Backup 将数据备份到虚拟磁带、存档磁带以及管理虚拟磁带库 (VTL) 设备。在本主题中，您可以找到有关使用磁带网关来配置 Arcserve Backup 并执行备份和还原操作的基本文档。有关使用 Arcserve Backup 的详细信息，请参阅 Arcserve Backup 文档。

主题

- 配置 Arcserve 以使用 VTL 设备
- 将磁带加载到介质池中
- 将数据备份到磁带
- 存档磁带
- 从磁带还原数据

配置 Arcserve 以使用 VTL 设备

在将虚拟磁带库 (VTL) 设备连接到客户端后，您可以扫描您的设备。

扫描 VTL 设备

1. 在 Arcserve Backup Manager 中，选择实用程序菜单。
2. 选择介质保障和扫描。

将磁带加载到介质池中

当 Arcserve 软件连接到网关且磁带变为可用时，Arcserve 将自动加载您的磁带。如果未在 Arcserve 软件中找到您的网关，请尝试在 Arcserve 中重新启动磁带引擎。

重新启动磁带引擎

1. 依次选择快速启动、管理 和 设备。
2. 在导航菜单中，打开网关的上下文（右键单击）菜单，然后选择导入/导出槽。
3. 选择快速导入并将磁带分配给空槽。
4. 打开网关的上下文（右键单击）菜单，然后选择清单/离线槽。
5. 选择快速清单以从数据库中检索介质信息。

如果您添加新磁带，则需要在网关中扫描新磁带以使其显示在 Arcserve 中。如果新磁带未显示，则必须导入这些磁带。

导入磁带

1. 选择快速启动菜单，然后选择备份和目标点击。
2. 选择网关，打开一个磁带的上下文（右键单击）菜单，然后选择导入/导出槽。
3. 打开每个新磁带的上下文（右键单击）菜单，然后选择清单。
4. 打开每个新磁带的上下文（右键单击）菜单，然后选择格式。

Storage Gateway 控制台中现在会显示每个磁带的条码，并且每个磁带都可供使用。

将数据备份到磁带

将磁带加载到 Arcserve 后，您可以备份数据。数据备份过程与备份物理磁带的过程相同。

将数据备份到磁带

1. 从快速启动菜单中，打开“还原备份”会话。

2. 选择源选项卡，然后选择要备份的文件系统或数据库系统。
3. 选择计划选项卡并选择要使用的重复方法。
4. 选择目标选项卡，然后选择要使用的磁带。如果正在备份的数据量大于磁带可容纳的数据量，Arcserve 将提示您装载新磁带。
5. 选择提交以备份数据。

> **Note**
>
> 如果正在执行备份任务时，磁带网关出于任何原因而重新启动，则备份任务可能会失败。要完成失败的备份任务，必须重新提交任务。

存档磁带

将磁带存档时，磁带网关将磁带从磁带库移至脱机存储。在弹出和存档磁带之前，您可能需要检查磁带上的内容。

将磁带存档

1. 从快速启动菜单中，打开“还原备份”会话。
2. 选择源选项卡，然后选择要备份的文件系统或数据库系统。
3. 选择计划选项卡并选择要使用的重复方法。
4. 选择网关，打开一个磁带的上下文（右键单击）菜单，然后选择导入/导出槽。
5. 分配邮件槽以加载磁带。Storage Gateway 控制台中的状态将更改为存档。存档过程可能需要一段时间。

存档过程可能需要一段时间才能完成。磁带的初始状态显示为正在传输到 VTS。存档开始后，状态变为正在存档。在存档完成后，磁带不再在 VTL 中列出，而是存档在 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 中。

从磁带还原数据

存档数据的还原过程包含两个步骤。

从存档磁带还原数据

1. 将存档的磁带取回到磁带网关。有关说明，请参阅 检索存档的磁带。

2. 使用 Arcserve 还原数据。此过程与从物理磁带还原数据相同。有关说明，请参阅 Arcserve Backup 文档。

要从磁带还原数据，请使用以下过程。

从磁带还原数据

1. 从快速启动菜单中，打开“还原备份”会话。
2. 选择源选项卡，然后选择要还原的文件系统或数据库系统。
3. 选择目标选项卡，并接受默认设置。
4. 选择计划选项卡，再选择要使用的重复方法，然后选择提交。

下一步

清理不必要的资源

使用 Bacula Enterprise 测试您的设置

您可以使用 Bacula Enterprise 将数据备份到虚拟磁带、存档磁带以及管理虚拟磁带库 (VTL) 设备。在本主题中，您可以找到有关如何为磁带网关配置 Bacula 版本 10 备份应用程序以及执行备份和还原操作的基本文档。有关如何使用 Bacula 的详细信息，请参阅 Bacula 系统手册和文档或联系 Bacula Systems。

> **Note**
>
> Bacula 仅在 Linux 上受支持。

设置 Bacula Enterprise

将虚拟磁带库 (VTL) 设备连接到 Linux 客户端后，配置 Bacula 软件以识别您的设备。有关如何将 VTL 设备连接到您客户端的信息，请参阅连接 VTL 设备。

设置 Bacula

1. 从 Bacula Systems 获取 Bacula Enterprise 备份软件的许可副本。
2. 在本地或云端计算机上安装 Bacula Enterprise 软件。

有关如何获取安装软件的信息，请参阅适用于 Amazon S3 和 Storage Gateway 的 Enterprise 备份。有关其他安装指南，请参阅 Bacula 白皮书在 Bacula 企业版中使用云服务和对象存储。

配置 Bacula 以使用 VTL 设备

下一步，配置 Bacula 以使用 VTL 设备。接下来，您可以找到基本配置步骤。

配置 Bacula

1. 安装 Bacula Director 和 Bacula Storage 守护程序。有关说明，请参阅 Bacula 白皮书在 Bacula 企业版中使用云服务和对象存储的第 7 章。
2. 连接到运行 Bacula Director 的系统并配置 iSCSI 启动程序。为此，请使用 Bacula 白皮书在 Bacula 企业版中使用云服务和对象存储的步骤 7.4 中提供的脚本。
3. 配置存储设备。使用前面介绍的 Bacula 白皮书中提供的脚本。
4. 配置本地 Bacula Director，添加存储目标，并为磁带定义介质池。使用前面介绍的 Bacula 白皮书中提供的脚本。

将数据备份到磁带

1. 在 Storage Gateway 控制台中创建磁带。有关如何创建磁带的信息，请参阅创建磁带。
2. 使用以下命令将磁带从 I/E 槽传输到存储槽。

   ```
   /opt/bacula/scripts/mtx-changer
   ```

   例如，以下命令将磁带从 I/E 槽 1601 传输到存储槽 1。

   ```
   /opt/bacula/scripts/mtx-changer transfer 1601 1
   ```
3. 使用以下命令启动 Bacula 控制台。

   ```
   /opt/bacula/bin/bconsole
   ```

   > **Note**
   >
   > 当您创建磁带并将其传输到 Bacula 时，请使用 Bacula 控制台 (bconsole) 命令 `update slots storage=VTL`，以便 Bacula 了解您创建的新磁带。

4. 使用以下 bconsole 命令将带有条形码的磁带标记为卷名称或标签。

```
label storage=VTL pool=pool.VTL barcodes === label the tapes with the
barcode as the volume name / label
```

5. 使用以下命令装载磁带。

```
mount storage=VTL slot=1 drive=0
```

6. 创建使用您创建的介质池的备份作业，然后将数据写入虚拟磁带，过程与使用物理磁带时的过程相同。
7. 使用以下命令从 Bacula 控制台卸载磁带。

```
umount storage=VTL slot=1 drive=0
```

> **Note**
>
> 如果正在执行备份任务时，磁带网关出于任何原因而重新启动，则备份任务会失败，并且 Bacula Enterprise 中的磁带状态将更改为已满。如果您知道磁带尚未得到充分利用，则可以手动将磁带状态更改回附加，然后使用同一个磁带继续备份任务。如果提供了其他处于附加状态的磁带，您也可以在另一个磁带上继续执行任务。

存档磁带

完成特定磁带的所有备份作业并且您可以存档磁带后，使用 mtx-changer 脚本将磁带从存储槽移动到 I/E 槽。此操作类似于其他备份应用程序中的弹出操作。

将磁带存档

1. 使用 `/opt/bacula/scripts/mtx-changer` 命令将磁带从存储槽传输到 I/E 槽。

   例如，以下命令将磁带从存储槽 1 传输到 I/E 槽 1601。

   ```
   /opt/bacula/scripts/mtx-changer transfer 1 1601
   ```

2. 确认磁带存档在脱机存储（S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）中，且磁带的状态为已存档。

从已存档并已取回的磁带还原数据

存档数据的还原过程包含两个步骤。

从存档磁带还原数据

1. 将存档磁带从存档取回到磁带网关。有关说明，请参阅 检索存档的磁带。
2. 使用 Bacula 软件还原您的数据：

   a. 使用 `/opt/bacula/scripts/mtx-changer` 命令将磁带导入存储槽，以便从 I/E 槽传输磁带。

      例如，以下命令将磁带从 I/E 槽 1601 传输到存储槽 1。

      ```
      /opt/bacula/scripts/mtx-changer transfer 1601 1
      ```

   b. 使用 Bacula 控制台更新槽，然后挂载磁带。

   c. 运行还原命令以还原数据。有关说明，请参阅 Bacula 文档。

使用 Commvault 测试您的设置

您可以使用 Commvault 将数据备份到虚拟磁带、存档磁带以及管理虚拟磁带库 (VTL) 设备。在本主题中，您可以找到有关如何为磁带网关配置 Commvault 备份应用程序、执行备份存档以及从存档的磁带中检索数据的基本文档。有关如何使用 Commvault 的详细信息，请参阅 Commvault 文档。

主题

- 配置 Commvault 以使用 VTL 设备
- 创建存储策略和子客户端
- 在 Commvault 中将数据备份到磁带
- 在 Commvault 中存档磁带
- 从磁带还原数据

配置 Commvault 以使用 VTL 设备

将 VTL 设备连接到 Windows 客户端之后，应配置 Commvault 以识别这些设备。有关如何将 VTL 设备连接到 Windows 客户端的信息，请参阅 将 VTL 设备连接到 Windows 客户端。

Commvault 备份应用程序无法自动识别 VTL 设备。您必须手动添加设备以将它们公开到 Commvault 备份应用程序，然后搜索设备。

配置 Commvault

1. 在 CommCell 控制台主菜单中，选择存储，然后选择专家存储配置以打开选择 MediaAgents对话框。
2. 选择要使用的可用介质代理，选择 Add (添加)，然后选择 OK (确定)。
3. 在 Expert Storage Configuration (专家存储配置) 对话框中，选择 Start (启动)，然后选择 Detect/Configure Devices (检测/配置设备)。
4. 将 Device Type (设备类型) 选项保持选中状态，选择 Exhaustive Detection (详尽检测)，然后选择 OK (确定)。
5. 在 Confirm Exhaustive Detection (确认详尽检测) 确认框中，选择 Yes (是)。
6. 在 Device Selection (设备选择) 对话框中，选择您的库及其所有驱动器，然后选择 OK (确定)。等待您的设备检测完成，然后选择 Close (关闭) 以关闭日志报告。
7. 右键单击您的库，选择 Configure (配置)，然后选择 Yes (是)。关闭配置对话框。
8. 在 Does this library have a barcode reader? (此库是否有条形码读取器?) 对话框中，选择 Yes (是)，然后，对于设备类型，选择 IBM ULTRIUM V5。
9. 在 CommCell 浏览器中，选择 “存储资源”，然后选择 “库” 以查看您的磁带库。
10. 要查看您的库中的磁带，请打开您的库的上下文（右键单击）菜单，然后依次选择 Discover Media (发现介质)、Media location (介质位置) 和 Media Library (介质库)。
11. 要安装您的磁带，请打开您的介质的上下文（右键单击）菜单，然后选择 Load (加载)。

创建存储策略和子客户端

每个备份和还原任务都与存储策略和子客户端策略关联。

存储策略会将数据的原始位置映射到您的媒体。

创建存储策略

1. 在 CommCell 浏览器中，选择策略。
2. 打开 Storage Policies (存储策略) 的上下文（右键单击）菜单，然后选择 New Storage Policy (新建存储策略)。
3. 在“Create Storage Policy (创建存储策略)”向导中，选择 Data Protection and Archiving (数据保护和存档)，然后选择 Next (下一步)。

4. 为 Storage Policy Name (存储策略名称) 键入一个名称，然后选择 Incremental Storage Policy (递增存储策略)。要将此存储策略与增量加载关联，请选择选项之一。否则，请将选项保持取消选中状态，然后选择 Next (下一步)。
5. 在 Do you want to Use Global Deduplication Policy? (是否要使用全局重复数据删除策略?) 对话框中，选择您的 Deduplication (重复数据删除) 首选项，然后选择 Next (下一步)。
6. 从 Library for Primary Copy (主副本库) 中，选择您的 VTL 库，然后选择 Next (下一步)。
7. 验证您的介质代理设置是否正确，然后选择 Next (下一步)。
8. 验证您的暂存池设置是否正确，然后选择 Next (下一步)。
9. 在 iData Agent Backup data (iData 代理备份数据) 中配置您的保留策略，然后选择 Next (下一步)。
10. 查看加密设置，然后选择 Next (下一步)。
11. 要查看您的存储策略，请选择 Storage Policies (存储策略)。

创建一个子客户端策略并将其与您的存储策略关联。利用子客户端策略，您可以通过中央模板配置类似的文件系统客户端，从而不必手动设置很多类似的文件系统。

创建子客户端策略

1. 在 CommCell 浏览器中，选择 “客户端计算机”，然后选择您的客户端计算机。选择 “文件系统”，然后选择defaultBackupSet。
2. 右键单击 defaultBackupSet，选择 “所有任务”，然后选择 “新建子客户端”。
3. 在 “子客户机属性” 框中，在 “名称” 中键入SubClient 名称，然后选择 “确定”。
4. 选择 Browse (浏览)，导航到要备份的文件，选择 Add (添加)，然后关闭对话框。
5. 在 Subclient (子客户端) 属性框中，选择 Storage Device (存储设备) 选项卡，从 Storage policy (存储策略) 中选择一个存储策略，然后选择 OK (确定)。
6. 在出现的 Backup Schedule (备份计划) 窗口中，将新的子客户端与备份计划关联。
7. 为一次性或按需备份选择 Do Not Schedule (不计划)，然后选择 OK (确定)。

   现在，您应该会在defaultBackupSet选项卡中看到您的子客户端。

在 Commvault 中将数据备份到磁带

创建备份任务以及将数据写入虚拟磁带的过程与使用物理磁带时的过程相同。有关更多信息，请参阅 Commvault 文档。

> **Note**
>
> 如果正在执行备份任务时，磁带网关出于任何原因而重新启动，则备份任务可能会失败。在某些情况下，您可以选择一个选项来恢复失败的任务。否则，您必须提交新任务。如果 Commvault 在任务失败后将磁带标记为不可用，则必须将磁带重新加载到驱动器中才能继续写入磁带。如果有多个磁带可用，Commvault 可能会在另一个磁带上继续执行失败的备份任务。

在 Commvault 中存档磁带

要进行存档，您首先要弹出磁带。将磁带存档时，磁带网关将磁带从磁带库移至脱机存储。在弹出和存档磁带之前，您可能需要先检查磁带上的内容。

将磁带存档

1. 在 CommCell 浏览器中，选择 “存储资源”、“库”，然后选择 “您的库”。选择 Media By Location (按位置划分介质)，然后选择 Media In Library (库中的介质)。
2. 打开要存档的磁带的上下文（右键单击）菜单，选择 All Tasks (所有任务)，选择 Export (导出)，然后选择 OK (确定)。

存档过程可能需要一段时间才能完成。磁带的初始状态显示为正在传输到 VTS。存档开始后，状态变为正在存档。存档完成后，磁带不再在 VTL 中列出。

在 Commvault 软件中，验证该磁带是否不再在存储槽中。

在 Storage Gateway 控制台的“导航”窗格中，选择磁带。验证已存档磁带的状态是否为 ARCHIVED (已存档)。

从磁带还原数据

您可以从从未存档和检索过的磁带或从已存档和检索的磁带还原数据。对于从未存档和检索过的磁带（非检索磁带），您有两个还原数据的选项：

- 通过子客户端还原
- 通过任务 ID 还原

通过子客户端从非检索磁带还原数据

1. 在 CommCell 浏览器中，选择 “客户端计算机”，然后选择您的客户端计算机。选择 “文件系统”，然后选择defaultBackupSet。
2. 打开您的子客户端的上下文（右键单击）菜单，选择 Browse and Restore (浏览和还原)，然后选择 View Content (查看内容)。
3. 选择要还原的文件，然后选择 Recover All Selected (还原所有选定内容)。
4. 选择 Home (主页)，然后选择 Job Controller (任务控制器) 以监视您的还原任务的状态。

通过任务 ID 从非检索磁带还原数据

1. 在 CommCell 浏览器中，选择 “客户端计算机”，然后选择您的客户端计算机。右键单击 File System (文件系统)，选择 View (查看)，然后选择 Backup History (备份历史记录)。
2. 在 Backup Type (备份类型) 类别中，选择所需的备份任务的类型，然后选择 OK (确定)。此时将出现包含备份任务历史记录的选项卡。
3. 查找要还原的 Job ID (任务 ID)，右键单击它，然后选择 Browse and Restore (浏览并还原)。
4. 在 Browse and Restore Options (浏览和还原选项) 对话框中，选择 View Content (查看内容)。
5. 选择要还原的文件，然后选择 Recover All Selected (还原所有选定内容)。
6. 选择 Home (主页)，然后选择 Job Controller (任务控制器) 以监视您的还原任务的状态。

从已存档和已检索的磁带还原数据

1. 在 CommCell 浏览器中，选择存储资源，选择库，然后选择您的库。选择 Media By Location (按位置划分介质)，然后选择 Media In Library (库中的介质)。
2. 右键单击已检索的磁带，选择 All Tasks (所有任务)，然后选择 Catalog (目录)。
3. 在 Catalog Media (目录介质) 对话框中，选择 Catalog only (仅目录)，然后选择 OK (确定)。
4. 选择 CommCell Home (主页)，然后选择 Job Controller (任务控制器) 以监视您的还原任务的状态。
5. 任务成功后，打开您的磁带的上下文（右键单击）菜单，选择 View (查看)，然后选择 View Catalog Contents (查看目录内容)。记下 Job ID (任务 ID) 值以供之后使用。
6. 选择 Recatalog/Merge (再录入目录/合并)。确保 Merge only (仅合并) 在 Catalog Media (目录介质) 对话框中处于选中状态。
7. 选择 Home (主页)，然后选择 Job Controller (任务控制器) 以监视您的还原任务的状态。
8. 作业成功后，选择 “CommCell 主页”，选择 “控制面板”，然后选择Browse/Search/Recovery。

9. 选择 Show aged data during browse and recovery (在浏览和恢复期间显示旧数据)，选择 OK (确定)，然后关闭 Control Panel (控制面板)。
10. 在 CommCell 浏览器中，右键单击 “客户端计算机”，然后选择您的客户端计算机。选择 View (查看)，然后选择 Job History (任务历史记录)。
11. 在 Job History Filter (任务历史记录筛选器) 对话框中，选择 Advanced (高级)。
12. 选择 Include Aged Data (包含旧数据)，然后选择 OK (确定)。
13. 在 Job History (任务历史记录) 对话框中，选择 OK (确定) 以打开 history of jobs (任务的历史记录) 选项卡。
14. 查找要还原的任务，打开它的上下文（右键单击）菜单，然后选择 Browse and Restore (浏览和还原)。
15. 在 Browse and Restore (浏览和还原) 对话框中，选择 View Content (查看内容)。
16. 选择要还原的文件，然后选择 Recover All Selected (还原所有选定内容)。
17. 选择 Home (主页)，然后选择 Job Controller (任务控制器) 以监视您的还原任务的状态。

使用 Dell EMC 测试您的设置 NetWorker

您可以使用 Dell EMC NetWorker 将数据备份到虚拟磁带、存档磁带并管理虚拟磁带库 (VTL) 设备。在本主题中，您可以找到有关如何配置 Dell EMC NetWorker 软件以与磁带网关配合使用并执行备份的基本文档，包括如何配置存储设备、将数据写入磁带、存档磁带以及如何从磁带恢复数据。

有关如何安装和使用 Dell EMC NetWorker 软件的详细信息，请参阅 NetWorker 文档。

有关兼容备份应用程序的更多信息，请参阅磁带网关支持的第三方备份应用程序。

主题

- 配置为与 VTL 设备一起使用
- 允许将 WORM 磁带导入 Dell EMC NetWorker
- 在 Dell EMC 中将数据备份到磁带 NetWorker
- 在 Dell EMC 中存档磁带 NetWorker
- 在 Dell EMC 中从存档磁带恢复数据 NetWorker

配置为与 VTL 设备一起使用

将虚拟磁带库 (VTL) 设备连接到 Microsoft Windows 客户端后，进行配置来识别您的设备。有关如何将 VTL 设备连接到 Windows 客户端的信息，请参阅 连接 VTL 设备。

Dell EMC NetWorker 不会自动识别磁带网关设备。要将您的 VTL 设备暴露给 NetWorker 软件并让软件发现它们，您需要手动配置该软件。下面我们假定您正确安装了软件，并且您熟悉管理控制台。有关管理控制台的更多信息，请参阅《Dell EMC NetWorker NetWorker 管理指南》的 “管理控制台界面” 部分。

为 VTL 设备配置 Dell EMC NetWorker 软件

1. 启动 Dell EMC NetWorker 管理控制台应用程序，从菜单中选择 “企业”，然后从左侧窗格中选择 localhost。
2. 打开 localhost 的上下文（右键单击）菜单，然后选择 Launch Application (启动应用程序)。
3. 选择 Devices (设备) 选项卡，打开 Libraries (库) 的上下文（右键单击）菜单，然后选择 Scan for Devices (扫描设备)。
4. 在“Scan for Devices (扫描设备)”向导中，选择 Start Scan (开始扫描)，然后从显示的对话框中选择 OK (确定)。
5. 展开 Libraries 文件夹树，查看您的所有库，然后按 F5 来刷新。将设备加载到库中的过程可能需要几秒钟时间。
6. 使用管理员权限打开命令窗口 (cmd.exe)，然后运行与 Dell EMC NetWorker 19.5 一起安装的`jbconfig`实用程序。
   a. 在菜单提示处，输入相应的数字来选择配置自动检测到的 SCSI 光盘机。
   b. 当系统提示您提供光盘机设备的名称时，请输入名称，例如 `AWSVTL`。
   c. 当系统提示开启 NetWorker 自动清洁功能时，请输入no。
   d. 当系统提示您绕过自动配置时，请输入 no。
   e. 当系统提示您配置其它光盘机时，请输入 no。
7. “jbconfig”完成后，返回 Networker GUI 并按 F5 来进行刷新。
8. 选择您的库，在左侧窗格中可以看到您的磁带，在右侧窗格中可以看到相应的空卷槽列表。
9. 在卷列表中，选择要激活的卷（选中的列会突出显示），打开所选列的上下文（右键单击）菜单，然后选择存放。此操作会将磁带从 I/E 槽移入卷槽。
10. 在显示的对话框中选择 Yes (是)，然后在 Load the Cartridges into (将磁带盒载入到) 对话框中选择 Yes (是)。
11. 如果没有更多磁带要存放，请选择 No (否) 或 Ignore (忽略)。否则选择 Yes (是) 存放更多磁带。

允许将 WORM 磁带导入 Dell EMC NetWorker

现在，您可以将磁带从磁带网关导入 Dell EMC NetWorker 库了。

虚拟磁带是一次写入多次读取 (WORM) 磁带，但是 Dell EMC NetWorker 期望使用非 WORM 磁带。NetWorker 要让 Dell EMC 使用您的虚拟磁带，您必须激活将磁带导入非 WORM 媒体池的功能。

允许将 WORM 磁带导入非 WORM 介质池

1. 在 NetWorker 控制台上，选择媒体，打开本地主机的上下文（右键单击）菜单，然后选择属性。
2. 在 “NetWorker 服务器属性” 窗口中，选择 “配置” 选项卡。
3. 在 Worm tape handling (WORM 磁带处理) 部分，清除 WORM tapes only in WORM pools (仅 WORM 池中的 WORM 磁带) 框，然后选择 OK (确定)。

在 Dell EMC 中将数据备份到磁带 NetWorker

将数据备份到磁带是一个两步过程。

1. 标记要将数据备份到的磁带，创建目标介质池并将磁带添加到池中。

   创建介质池和将数据写入虚拟磁带的过程与利用物理磁带时的过程相同。有关详细信息，请参阅《Dell EMC NetWorker 管理指南》的 “备份数据” 部分。

2. 将数据写入磁带。您可以使用 Dell EMC NetWorker 用户应用程序而不是 Dell EMC NetWorker 管理控制台来备份数据。Dell EMC NetWorker 用户应用程序作为安装的一部分进行 NetWorker安装。

> **Note**
>
> 您可以使用 Dell EMC NetWorker 用户应用程序执行备份，但可以在 EMC 管理控制台中查看备份和还原任务的状态。要查看状态，请选择 Devices (设备) 菜单，在 Log (日志) 窗口中查看状态。

> **Note**
>
> 如果正在执行备份任务时，磁带网关出于任何原因而重新启动，则备份任务会暂停，并且 Dell EMC Networker 中的磁带状态将更改为写保护。您可以存档磁带或继续从中读取数据。您可以在另一个磁带上恢复暂停的备份任务。

在 Dell EMC 中存档磁带 NetWorker

当您存档磁带时，Tape Gateway 会将磁带从 Dell EMC NetWorker 磁带库移动到离线存储。通过将磁带从磁带驱动器弹出至存储插槽来开始磁带存档。然后，您可以使用备份应用程序（即 Dell EMC NetWorker 软件）将磁带从插槽中提取到存档中。

使用 Dell EMC 存档磁带 NetWorker

1. 在 “ NetWorker 管理” 窗口的 “设备” 选项卡上，选择 localhost 或您的 EMC 服务器，然后选择 “库”。
2. 选择您从虚拟磁带库导入的磁带。
3. 从已写入数据的磁带的列表中，打开要存档的磁带的上下文（右键单击）菜单，然后选择 Eject/Withdraw (弹出/提取)。
4. 在显示的确认框中，选择 OK (确定)。

存档过程可能需要一段时间才能完成。磁带的初始状态显示为正在传输到 VTS。存档开始后，状态变为正在存档。存档完成后，磁带不再在 VTL 中列出。

在 Dell EMC NetWorker 软件中，确认磁带已不在存储插槽中。

在 Storage Gateway 控制台的“导航”窗格中，选择磁带。验证已存档磁带的状态是否为 ARCHIVED (已存档)。

在 Dell EMC 中从存档磁带恢复数据 NetWorker

存档数据的还原过程包含两个步骤：

1. 将存档的磁带取回到磁带网关。有关说明，请参阅 检索存档的磁带。
2. 使用 Dell EMC NetWorker 软件恢复数据。您可通过创建还原文件夹文件完成此任务，就像从物理磁带还原数据一样。有关说明，请参阅《Dell EMC NetWorker 管理指南》的 “使用 NetWorker 用户程序” 部分。

下一步

清理不必要的资源

使用 IBM Data Protect 测试您的设置

通过使用 IBM Data Protect，您可以将数据备份到虚拟磁带、存档磁带并管理虚拟磁带库 (VTL) 设备。Amazon Storage Gateway（IBM Data Protect 以前被称为 Tivoli 存储管理器。）

本主题包含有关如何为磁带网关配置 IBM Data Protect 备份软件的基本信息。它还包括有关使用 IBM Data Protect 执行备份和还原操作的基本信息。有关如何管理 IBM Data Protect 备份软件的更多信息，请参阅 IBM Data Protect 文档。

IBM Data Protec Amazon Storage Gateway t 备份软件支持以下操作系统。

- Microsoft Windows Server
- Red Hat Linux

有关支持 IBM Data Protect 的 Windows 设备的信息，请参阅适用于 AIX、HP-UX、Solaris 和 Windows 的 IBM Data Protect（前身为 Tivoli Storage Manager）支持的设备。

有关支持 IBM Data Protect 的 Linux 设备的信息，请参阅适用于 Linux 的 IBM Data Protect（前身为 Tivoli 存储管理器）支持的设备。

主题

- 设置 IBM 数据保护
- 配置 IBM Data Protect 以与 VTL 设备配合使用
- 在 IBM Data Protect 中将数据写入磁带
- 从 IBM Data Protect 中存档的磁带中恢复数据

设置 IBM 数据保护

将 VTL 设备连接到客户端后，您可以配置 IBM Data Protect 软件以识别它们。有关将 VTL 设备连接到客户端的更多信息，请参阅连接 VTL 设备。

设置 IBM Data Protect

1. 从 IBM 获取 IBM 数据保护软件的许可副本。
2. 在您的本地环境或云端 Amazon EC2 实例上安装 IBM 数据保护软件。有关更多信息，请参阅 IBM 的 IBM Data Protect 安装和升级文档。

有关配置 IBM Data Protect 软件的更多信息，请参阅为 IBM Data Protect 服务器配置 Amazon 磁带网关虚拟磁带库。

配置 IBM Data Protect 以与 VTL 设备配合使用

接下来，将 IBM Data Protect 配置为与您的 VTL 设备配合使用。你可以将 IBM Data Protect 配置为与微软 Windows Server 或 Red Hat Linux 上的 VTL 设备配合使用。

为 Windows 配置 IBM 数据保护

有关如何在 Windows 上配置 IBM Data Protect 的完整说明，请参阅联想网站上的适用于 Windows 2012 的磁带设备驱动程序-W12 6266。以下是有关该过程的基本文档。

为微软 Windows 配置 IBM 数据保护

1. 为您的介质更换器获取正确的驱动程序包。对于磁带设备驱动程序，IBM Data Protect 需要适用于 Windows 2012 的 W12 6266 版本。有关如何获取驱动程序的说明，请参阅 Lenovo 网站上的 Tape Device Driver-W12 6266 for Windows 2012。

   > **Note**
   >
   > 请确保您安装的是一组“非独占”的驱动程序。

2. 在您的计算机上，打开计算机管理，展开 Media Changer devices (介质更换器设备)，并验证介质更换器类型是否被列为 IBM 3584 Tape Library (IBM 3584 磁带库)。
3. 请确保虚拟磁带库中任何磁带的条形码不超过 8 个字符。如果您尝试为磁带分配长度超过 8 个字符的条形码，则会收到以下错误消息：`"Tape barcode is too long for media changer"`。
4. 确保所有磁带机和介质更换器都出现在 IBM Data Protect 中。为此，请使用以下命令：`\Tivoli \TSM\server>tsmdlst.exe`

为 Linux 配置 IBM 数据保护

以下是有关配置 IBM Data Protect 以在 Linux 上与 VTL 设备配合使用的基本文档。

为 Linux 配置 IBM 数据保护

1. 转到 IBM 支持网站上的 IBM Fix Central，并选择选择产品。

2. 对于 Product Group (产品组)，选择 System Storage (系统存储)。
3. 对于 Select from System Storage (从存储系统中选择)，选择 Tape systems (磁带系统)。
4. 对于 Tape systems (磁带系统)，选择 Tape drivers and software (磁带驱动程序和软件)。
5. 对于 Select from Tape drivers and software (从磁带驱动程序和软件中选择)，选择 Tape device drivers (磁带设备驱动程序)。
6. 对于 Platform (平台)，选择您的操作系统，然后选择 Continue (继续)。
7. 选择您要下载的设备驱动程序版本。然后按照 Fix Central 下载页面上的说明下载和配置 IBM Data Protect。
8. 请确保虚拟磁带库中任何磁带的条形码不超过 8 个字符。如果您尝试为磁带分配长度超过 8 个字符的条形码，则会收到以下错误消息："Tape barcode is too long for media changer"。

在 IBM Data Protect 中将数据写入磁带

利用您对物理磁带执行的同一过程和备份策略，将数据写入磁带网关虚拟磁带。为备份和还原作业创建必要的配置。有关配置 IBM Data Protect 的更多信息，请参阅 IBM Data Protect 的管理任务概述。

> **Note**
>
> 如果正在执行备份任务时，磁带网关出于任何原因而重新启动，则备份任务可能会失败。如果备份任务失败，IBM Data Protect 中的磁带状态将更改为ReadOnly。如果您知道磁带尚未得到充分利用，则可以手动将磁带状态更改回原处 ReadWrite，然后使用相同的磁带恢复或重新提交备份作业。如果其他ReadWrite处于状态的磁带可用，IBM Data Protect 可能会继续在另一个磁带上执行失败的备份作业。

从 IBM Data Protect 中存档的磁带中恢复数据

存档数据的还原过程包含两个步骤。

从存档磁带还原数据

1. 将存档磁带从存档取回到磁带网关。有关说明，请参阅 检索存档的磁带。
2. 使用 IBM Data Protect 备份软件恢复数据。您可通过创建恢复点可完成此任务，就像从物理磁带还原数据一样。有关配置 IBM Data Protect 的更多信息，请参阅 IBM Data Protect 的管理任务概述。

下一步

清理不必要的资源

使用 D OpenText ata Protector 测试您的设置

您可以使用 Data Protector 将数据备份到虚拟磁带、存档磁带以及管理虚拟磁带库 (VTL) 设备。OpenText 在本主题中，您可以找到有关如何为磁带网关配置 OpenText Data Protector 软件以及如何执行备份和恢复操作的基本文档。有关如何使用 OpenText Data Protector 软件的详细信息，请参阅 OpenText 数据保护器文档。有关兼容备份应用程序的更多信息，请参阅磁带网关支持的第三方备份应用程序。

主题

- 将 OpenText 数据保护器配置为与 VTL 设备配合使用
- 准备虚拟磁带以与数据保护器配合使用
- 将磁带加载到介质池中
- 将数据备份到磁带
- 存档磁带
- 从磁带还原数据

将 OpenText 数据保护器配置为与 VTL 设备配合使用

将虚拟磁带库 (VTL) 设备连接到客户端后，可以配置 D OpenText ata Protector 以识别您的设备。有关如何将 VTL 设备连接到客户端的信息，请参阅 连接 VTL 设备。

OpenText Data Protector 软件无法自动识别磁带网关设备。要让软件识别这些设备，请手动添加设备，然后发现 VTL 设备，如下所述。

添加 VTL 设备

1. 在 OpenText Data Protector 主窗口中，选择左上角列表中的 “设备和媒体” 功能区。

   打开 Devices (设备) 的上下文（右键单击）菜单，然后选择 Add Device (添加设备)。
2. 在 Add Device (添加设备) 选项卡上，键入 Device Name (设备名称) 的值。对于Device Type (设备类型)，选择 SCSI Library (SCSI 库)，然后选择 Next (下一步)。
3. 在下一个屏幕上执行以下操作：

a. 对于 SCSI address of the library robotic (机械手库的 SCSI 地址)，请选择您的具体地址。
b. 对于 Select what action Data Protector should take if the drive is busy (选择 Data Protector 在驱动器繁忙时应执行的操作)，请选择“Abort (中止)”或者您的首选操作。
c. 选择激活以下选项：
   - Barcode reader support (条形码读卡器支持)
   - Automatically discover changed SCSI address (自动发现已更改的 SCSI 地址)
   - SCSI Reserve/Release (robotic control) (SCSI 保留/释放(机械手控制))
d. 除非系统要求，否则将 Use barcode as medium label on initialization (在初始化时将条形码用作媒介标签) 留空（不选中）。
e. 选择下一步以继续。

4. 在下一个屏幕上，指定您希望用于 HP Data Protector 的槽。在数字之间使用连字符 (-) 来指示槽的范围，例如 1-6。指定了要使用的槽之后，选择 Next (下一步)。
5. 对于物理设备使用的标准介质类型，请选择 LTO_Ultrium，然后选择 Finish (完成) 以完成设置。

现在您的磁带库已准备好供使用。要将磁带加载到其中，请参阅下一部分。

准备虚拟磁带以与数据保护器配合使用

在将数据备份到虚拟磁带之前，您需要准备要使用的磁带。准备工作涉及以下操作：

- 将虚拟磁带加载到磁带库
- 将虚拟磁带加载到槽
- 创建介质池
- 将虚拟磁带加载到介质池中

在以下部分中，您可以找到引导您完成此过程的步骤。

将虚拟磁带加载到磁带库中

现在，您的磁带库应已在 Devices (设备) 下列出。如果您未看到，请按 F5 刷新屏幕。列出库时，您可以将虚拟磁带加载到库中。

将虚拟磁带加载到磁带库中

1. 选择您的磁带库旁边的加号可以显示机械手路径、驱动器和槽的节点。

2. 打开 Drives (驱动器) 的上下文（右键单击）菜单，选择 Add Drive (添加驱动器)，键入磁带的名称，然后选择 Next (下一步) 以继续。
3. 选择要为 SCSI address of data drive (数据驱动器的 SCSI 地址) 添加的磁带驱动器，选择 Automatically discover changed SCSI address (自动发现已更改的 SCSI 地址)，然后选择 Next (下一步)。
4. 在以下屏幕上，选择 Advanced (高级)。此时将显示 Advanced Options (高级选项) 弹出屏幕。

   a. 在 Settings (设置) 选项卡上，您应考虑以下选项：

      - CRC Check (CRC 检查)（检测意外数据更改）
      - Detect dirty drive (检测被占用的驱动器) (确保在备份之前驱动器是空的)
      - SCSI Reserve/Release(drive) (SCSI 保留/释放(驱动器))）避免磁带争用）

      出于测试目的，您可以将这些选项保持停用（未选中）。

   b. 在 Sizes (尺寸) 选项卡上，将 Block size (kB) (块尺寸(kB)) 设置为 Default (256) (默认值 (256))。
   c. 选择 OK (确定) 关闭高级选项屏幕，然后选择 Next (下一步) 以继续。
5. 在下一个屏幕的 Device Policies (驱动器策略) 下方，选择这些选项：

   - Device may be used for restore (设备可能用于还原)
   - Device may be used as source device for object copy (设备可能用作对象副本的源设备)
6. 选择 Finish (完成) 可完成将磁带驱动器添加到您的磁带库。

将虚拟磁带加载到槽中

现在，您的磁带库中已经有了一个磁带驱动器，可以将虚拟磁带加载到槽中。

将磁带加载到槽中

1. 在磁带库树节点上，打开标签为 Slots (槽) 的节点。每个槽的状态使用图标表示：

   - 绿色磁带表示磁带已经加载到槽中。
   - 灰色槽意味着槽为空。
   - 青色问号标记表示该槽中的磁带未格式化。
2. 对于空槽，请打开上下文（右键单击）菜单，然后选择 Enter (输入)。如果您已有磁带，请选择一个磁带以加载到该槽中。

创建介质池

介质池 是用于组织磁带的逻辑组。要设置磁带备份，您需要创建介质池。

创建介质池

1. 在 Devices & Media (设备和介质) 磁带架上，打开 Media (介质) 的树节点，打开 Pools (池) 节点的上下文（右键单击）菜单，然后选择 Add Media Pool (添加介质池)。
2. 对于 Pool name (池名称)，键入名称。
3. 对于 Media Type (介质类型)，选择 LTO_Ultrium，然后选择 Next (下一步)。
4. 在接下来的屏幕上，接受默认值，然后选择 Next (下一步)。
5. 选择 Finish (完成) 完成介质池创建。

将磁带加载到介质池中

在可以将数据备份到磁带之前，您必须先将磁带加载到所创建的介质池中。

将虚拟磁带加载到介质池

1. 在磁带库树节点上，选择 Slots (槽) 节点。
2. 选择已加载的磁带，即以绿色图标显示的已加载磁带。打开上下文（右键单击）菜单，选择 Format (格式)，然后选择 Next (下一步)。
3. 选择您创建的介质池，然后选择 Next (下一步)。
4. 对于 Medium Description (媒介描述)，请选择 Use barcode (使用条形码)，然后选择 Next (下一步)。
5. 对于 Options (选项)，请选择 Force Operation (强制执行操作)，然后选择 Finish (完成)。

现在您应看到选定槽的状态从未分配 (灰色) 转变为已插入磁带的状态 (绿色)。此时将显示一系列消息，确认您的介质已初始化。

此时，您应该配置好所有内容，以便开始使用带有 Data Protector 的虚拟磁带库。要认真检查确实如此，请使用以下过程。

验证您的磁带库是否已配置，可供使用

- 选择 Drives (驱动器)，然后打开驱动器的上下文（右键单击）菜单并选择 Scan (扫描)。

如果配置正确，此时将显示一条消息，确认已成功扫描您的介质。

将数据备份到磁带

将磁带加载到介质池之后，您可以在其中备份数据。

将数据备份到磁带

1. 从窗口左上角的下拉菜单中，选择备份。
2. 从左侧窗格中展开备份导航树。
3. 右键单击文件系统来打开上下文菜单，然后选择添加备份。
4. 在 Create New Backup (创建新备份) 屏幕上的 Filesystem (文件系统) 下方，选择 Blank File System Backup (空白文件系统备份)，然后选择 OK (确定)。
5. 在显示您的主机系统的树节点上，选择您要备份的一个或多个文件系统，然后选择 Next (下一步) 以继续。
6. 打开您要使用的磁带库的树节点，打开要使用的磁带驱动器的上下文（右键单击）菜单，然后选择 Properties (属性)。
7. 依次选择您的介质池、OK (确定) 和 Next (下一步)。
8. 对于接下来的三个屏幕，接受默认设置，然后选择 Next (下一步)。
9. 打开 Perform finishing steps in your backup/template design (在您的备份/模板设计中执行完成步骤) 屏幕，选择 Save as (另存为) 以保存此会话。在弹出窗口中，为备份提供名称，并将其分配到您用于保存新备份规范的组中。
10. 选择 Start Interactive Backup (开始交交互式备份)。

如果主机系统包含数据库系统，您可以将其选择作为目标备份系统。屏幕和选择内容与刚才所述的文件系统备份相似。

> **Note**
>
> 如果正在执行备份任务时，磁带网关出于任何原因而重新启动，则备份任务会失败，且 Data Protector 中的磁带设备标记为脏。Data Protector 还会将磁带质量标记为差，并阻止写入到磁带。要继续从磁带读取数据，必须清理驱动器并重新装载磁带。要完成失败的备份任务，必须在新磁带上重新提交任务。

存档磁带

将磁带存档时，磁带网关将磁带从磁带库移至脱机存储。在弹出和存档磁带之前，您可能需要检查磁带上的内容。

在存档之前检查磁带内容

1. 选择 Slots (槽)，然后选择要检查的磁带。
2. 选择 Objects (对象)，然后检查磁带上有什么内容。

选择要存档的磁带时，使用以下过程。

弹出和存档磁带

1. 打开磁带的上下文（右键单击）菜单，然后选择 Eject (弹出)。
2. 在 Storage Gateway 控制台上，选择您的网关，然后选择 VTL 磁带盒并验证所存档的虚拟磁带的状态。

在弹出磁带后，磁带将自动存档在脱机存储（S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）中。存档过程可能需要一段时间才能完成。磁带的初始状态显示为 IN TRANSIT TO VTS (正在传输到 VTS)。存档开始后，状态变为正在存档。在存档完成后，磁带不再在 VTL 中列出，而是存档在 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 中。

从磁带还原数据

存档数据的还原过程包含两个步骤。

从存档磁带还原数据

1. 将存档的磁带取回到磁带网关。有关说明，请参阅 检索存档的磁带。
2. 使用数据保护器恢复数据。此过程与从物理磁带还原数据相同。

要从磁带还原数据，请使用以下过程。

从磁带还原数据

1. 从窗口左上角的下拉菜单中，选择还原。

2. 从左侧导航树中选择要还原的文件系统或数据库系统。对于要还原的备份，请确保选中该框。选择还原。
3. 在 Start Restore Session (开始还原会话) 窗口中，选择 Needed Media (需要的介质)。选择 All media (所有介质)，然后您应看到最初用于备份的磁带。选择该磁带，然后选择 Close (关闭)。
4. 在 Start Restore Session (开始还原会话) 窗口中，接受默认设置，选择 Next (下一步)，然后选择 Finish (完成)。

下一步

清理不必要的资源

使用 Microsoft System Center DPM 测试您的设置

您可以使用 Microsoft System Center 数据保护管理器 (DPM) 将数据备份到虚拟磁带、存档磁带并管理虚拟磁带库 (VTL) 设备。在本主题中，您可以找到有关如何针对磁带网关配置 DPM 备份应用程序并执行备份和还原操作的基本文档。

有关如何使用 DPM 的详细信息，请参阅 Microsoft System Center 网站上的 DPM 文档。有关兼容备份应用程序的更多信息，请参阅磁带网关支持的第三方备份应用程序。

主题

- 配置 DPM 以识别 VTL 设备
- 将磁带导入 DPM
- 在 DPM 中将数据写入磁带
- 使用 DPM 将磁带存档
- 在 DPM 中从存档磁带还原数据

配置 DPM 以识别 VTL 设备

将虚拟磁带库 (VTL) 设备连接到 Windows 客户端后，应配置 DPM 以识别您的设备。有关如何将 VTL 设备连接到 Windows 客户端的信息，请参阅 连接 VTL 设备。

默认情况下，DPM 服务器无法识别磁带网关设备。要配置服务器以与磁带网关设备一起使用，请执行以下任务：

1. 更新 VTL 设备的设备驱动程序以使其对 DPM 服务器公开。
2. 手动将 VTL 设备映射到 DPM 磁带库。

更新 VTL 设备驱动程序

- 在设备管理器中，更新介质更换器的驱动程序。有关说明，请参阅 更新介质更换器的设备驱动程序。

您可以使用 DPMDriveMappingTool 将您的磁带驱动器映射到 DPM 磁带库。

将 磁带驱动器映射到 DPM 服务器磁带库

1. 为您的网关创建至少一个磁带。有关如何在控制台上执行此操作的信息，请参阅创建磁带。
2. 将磁带导入 DPM 库。有关如何执行此操作的信息，请参阅 将磁带导入 DPM。
3. 如果 DPMLA 服务正在运行，请打开命令终端并在命令行中键入以下命令来停止它。

   ```
   net stop DPMLA
   ```

4. 在 DPM 服务器上找到以下文件：`%ProgramFiles%\System Center\DPM\DPM\Config\DPMLA.xml`。

   > **Note**
   >
   > 目录路径可能会根据您的 System Center 或 DPM 版本而变化。
   > 如果此文件存在，则会将其 DPMDriveMappingTool 覆盖。如果您希望保留原来的文件，请创建一个备份副本。

5. 打开命令终端，将目录更改为 `%ProgramFiles%\System Center\DPM\DPM\Bin`，然后运行以下命令。

   > **Note**
   >
   > 目录路径可能会根据您的 System Center 或 DPM 版本而变化。

   ```
   C:\Microsoft System Center\DPM\DPM\bin>DPMDriveMappingTool.exe
   ```

   命令的输出如下所示。

```
Performing Device Inventory ...
Mapping Drives to Library ...
Adding Standalone Drives ...
Writing the Map File ...
Drive Mapping Completed Successfully.
```

将磁带导入 DPM

您现在已做好将磁带从磁带网关导入 DPM 备份应用程序库的准备。

将磁带导入 DPM 备份应用程序库

1. 在 DPM 服务器上，打开管理控制台，选择 Rescan (重新扫描)，然后选择 Refresh (刷新)。管理控制台显示您的介质更换器和磁带机。
2. 在 Library (库) 部分中打开介质更换器的上下文（右键单击）菜单，然后选择 Add tape (I/E port) (添加磁带(I/E 端口)) 以便将磁带添加到 Slots (槽) 列表。

   > **Note**
   >
   > 添加磁带的过程需要几分钟时间才能完成。

   磁带标签显示为 Unknown (未知)，并且磁带不可用。要使磁带可用，您必须标识它。
3. 打开您要标识的磁带的上下文（右键单击）菜单，然后选择 Identify unknown tape (标识未知磁带)。

   > **Note**
   >
   > 标识磁带的过程需要几秒或几分钟时间。
   > 如果磁带无法正确显示条形码，则需要将媒体更换器驱动程序更改为 SunStorageTek / Library。有关更多信息，请参阅 在 Microsoft System Center DPM 中显示磁带的条形码。

   标识完成后，磁带标签变为 Free (可用)。即，磁带可写入数据。

在 DPM 中将数据写入磁带

利用您对物理磁带执行的相同保护过程和策略，可以将数据写入磁带网关虚拟磁带。创建一个保护组并添加要备份的数据，然后通过创建恢复点备份这些数据。有关如何使用 DPM 的详细信息，请参阅 Microsoft System Center 网站上的 DPM 文档。

默认情况下，一个磁带的容量为 30 GB。在对大于一个磁带容量的数据进行备份时，会出现设备 I/O 错误。如果出现错误的位置大于该磁带的大小，Microsoft DPM 会将错误视为磁带结束的指示。如果出现错误的位置小于该磁带的大小，备份任务失败。要解决此问题，请更改注册表项中的 `TapeSize` 值，以匹配磁带大小。有关如何执行此操作的信息，请参阅 Microsoft System Center 处的错误 ID：30101。

> **Note**
>
> 如果正在执行备份任务时，磁带网关出于任何原因而重新启动，则备份任务会失败。要完成失败的备份任务，必须重新提交任务。

使用 DPM 将磁带存档

将磁带存档时，磁带网关将磁带从 DPM 磁带库移至脱机存储。使用备份应用程序（即 DPM）从槽中移走磁带，即可开始磁带存档。

在 DPM 中将磁带存档

1. 打开要存档的磁带的上下文（右键单击）菜单，然后选择 Remove tape (I/E port) (删除磁带(I/E 端口))。
2. 在随后显示的对话框中，选择 Yes (是)。执行此操作会从介质更换器的存储槽中弹出磁带并将磁带移至网关的 I/E 槽中。当磁带移至网关的 I/E 槽中时，它立即被发送进行存档。
3. 在 Storage Gateway 控制台上，选择您的网关，然后选择 VTL 磁带盒并验证所存档的虚拟磁带的状态。

   存档过程可能需要一段时间才能完成。磁带的初始状态显示为 IN TRANSIT TO VTS (正在传输到 VTS)。存档开始后，状态变为正在存档。存档完成后，磁带不再在 VTL 中列出。

在 DPM 中从存档磁带还原数据

存档数据的还原过程包含两个步骤。

从存档磁带还原数据

1. 将存档磁带从存档取回到磁带网关。有关说明，请参阅 检索存档的磁带。
2. 使用 DPM 备份应用程序还原数据。您可通过创建恢复点可完成此任务，就像从物理磁带还原数据一样。有关说明，请参阅 DPM 网站上的恢复客户端计算机数据。

下一步

清理不必要的资源

使用以下方法测试您的设置 NovaStor DataCenter

您可以使用 NovaStor DataCenter/Network. In this topic, you can find basic documentation on how to configure the NovaStor DataCenter/Network backup application for a Tape Gateway and perform backup and restore operations. For detailed information about how to use NovaStor DataCenter/Network, refer to the NovaStor DataCenter/Network文档将数据备份到虚拟磁带、存档磁带以及管理虚拟磁带库 (VTL) 设备。

设置 NovaStor DataCenter /网络

将虚拟磁带库 (VTL) 设备连接到 Microsoft Windows 客户端后，您可以将 NovaStor 软件配置为识别您的设备。有关如何将 VTL 设备连接到 Windows 客户端的信息，请参阅连接 VTL 设备。

NovaStor DataCenter/Network 需要驱动程序制造商提供的驱动程序。您可以使用 Windows 驱动程序，但您必须先停用其他备份应用程序。

配置 NovaStor DataCenter /Network 以使用 VTL 设备

将 VTL 设备配置为与 NovaStor DataCenter /Network 配合使用时，您可能会看到一条错误消息，上面写着：`External Program did not exit correctly`此问题需要解决方法，您需要先执行解决方法，然后再继续。

您可以在开始配置 VTL 设备之前创建解决方法来防止此问题的发生。有关如何创建解决方法的信息，请参阅解决“外部程序未正确退出”错误。

配置 NovaStor DataCenter /Network 以使用 VTL 设备

1. 在 NovaStor DataCenter /Network Admin 控制台中，选择 “媒体管理”，然后选择 “存储管理”。

2. 在 Storage Targets (存储目标) 菜单中，打开 Media Management Servers (介质管理服务器) 的上下文菜单（右键单击），选择 New (新建)，然后选择 OK (确定) 来创建并预填充 storage (存储) 节点。

   如果您看到说明 `External Program did not exit correctly` 的错误消息，请先解决此问题，然后再继续。此问题需要解决方法。有关如何解决此问题的信息，请参阅解决“外部程序未正确退出”错误。

   > **Important**
   >
   > 之所以出现此错误，是因为存储驱动器和磁带驱动器的元素分配范围超过了 NovaStor DataCenter /Network 允许的数量。 Amazon Storage Gateway

3. 打开已创建的 storage (存储) 节点的上下文（右键单击）菜单，然后选择 New Library (新库)。
4. 从列表中选择库服务器。将自动填充库列表。
5. 命名该库，然后选择 OK (确定)。
6. 选择库来显示 Storage Gateway 虚拟磁带库的所有属性。
7. 在 Storage Targets (存储目标) 菜单中，展开 Backup Servers (备份服务器)，打开服务器的上下文（右键单击）菜单，然后选择 Attach Library (附加库)。
8. 在出现的 “附加库” 对话框中，选择LTO5媒体类型，然后选择 “确定”。
9. 展开备份服务器，查看 Storage Gateway 虚拟磁带库以及库分区（显示了所有已装载的磁带驱动器）。

创建磁带池

磁带池是在 NovaStor DataCenter /Network 软件中动态创建的，因此不包含固定数量的媒体。需要磁带的磁带池从其暂存池中获取磁带。暂存池 是可供一个或多个磁带池免费使用的磁带容器。磁带池将超出保留时间且不再需要的任何介质返回到暂存池。

创建磁带池是一个分为三步的任务：

1. 创建暂存池。
2. 将磁带分配到暂存池。
3. 创建磁带池。

创建暂存池

1. 在左侧导航菜单中，选择 Scratch Pools (暂存池) 选项卡。
2. 打开 Scratch Pools (暂存池) 的上下文（右键单击）菜单，然后选择 Create Scratch Pool (创建暂存池)。
3. 在 Scratch Pools (暂存池) 对话框中，命名您的暂存池，然后选择您的介质类型。
4. 选择 Label Volume (标记卷)，然后为暂存池创建低水位。当暂存池被清空到低水位时，会出现警告。
5. 在出现的警告对话框中，选择 OK (确定) 来创建暂存池。

将磁带分配到暂存池

1. 在左侧导航菜单中，选择 Tape Library Management (磁带库管理)。
2. 选择 Library (库) 选项卡来查看您的库的清单。
3. 选择要分配到暂存池的磁带。确保磁带设置为正确的介质类型。
4. 打开库的上下文（右键单击）菜单，然后选择 Add to Scratch Pool (添加到暂存池)。

现在，您具有可用于磁带池的已填充的暂存池。

创建磁带池

1. 从左侧导航菜单中，选择 Tape Library Management (磁带库管理)。
2. 打开 Media Pools (介质池) 选项卡的上下文（右键单击）菜单，然后选择 Create Media Pool (创建介质池)。
3. 命名介质池，然后选择 Backup Server (备份服务器)。
4. 为介质池选择库分区。
5. 选择您希望该池从其中获取磁带的暂存池。
6. 对于 Schedule (计划)，选择 Not Scheduled (未计划)。

配置介质导入和导出到存档磁带

NovaStor DataCenter/Network can use import/export插槽（如果它们是媒体更换器的一部分）。

要进行导出， NovaStor DataCenter/Network 必须知道哪些磁带将从磁带库中实际取出。

对于导入， NovaStor DataCenter/Network 会识别在磁带库中导出的磁带介质，并提供从数据槽或导出插槽导入所有磁带介质。您的磁带网关将磁带存档在脱机存储（S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）中。

配置介质导入和导出

1. 导航到 Tape Library Management (磁带库管理)，为 Media Management Server (介质管理服务器) 选择一个服务器，然后选择 Library (库)。
2. 选择 Off-site Locations (场外位置) 选项卡。
3. 打开白色区域的上下文（右键单击）菜单，然后选择 Add (添加) 来打开新面板。
4. 在面板中，键入 **`S3 Glacier Flexible Retrieval`** 或 **`S3 Glacier Deep Archive`**，然后在文本框中添加可选的说明。

将数据备份到磁带

创建备份任务并将数据写入虚拟磁带的过程与利用物理磁带时的过程相同。有关如何使用该 NovaStor 软件备份数据的详细信息，请参阅文档 NovaStor DataCenter /Network。

> **Note**
>
> 如果正在执行备份任务时，磁带网关出于任何原因而重新启动，则备份任务会失败，且磁带会变得不可写入。您可以存档磁带或继续从中读取数据。要完成失败的备份任务，必须在新磁带上重新提交任务。

存档磁带

将磁带存档时，磁带网关会将磁带从磁带驱动器弹出至存储插槽。然后，它使用您的备份应用程序（即 /Network）将磁带从插槽导出到存档中。 NovaStor DataCenter

将磁带存档

1. 在左侧导航菜单中，选择 Tape Library Management (磁带库管理)。
2. 选择 Library (库) 选项卡来查看库的清单。
3. 突出显示要存档的磁带，打开磁带的上下文（右键单击）菜单，然后选择场外存档位置。

存档过程可能需要一段时间才能完成。磁带的初始状态显示为正在传输到 VTS。存档开始后，状态变为正在存档。存档完成后，磁带不再在 VTL 中列出。

在 NovaStor DataCenter /Network 中，确认磁带已不在存储插槽中。

在 Storage Gateway 控制台的“导航”窗格中，选择磁带。验证已存档磁带的状态是否为 ARCHIVED (已存档)。

从已存档并已取回的磁带还原数据

存档数据的还原过程包含两个步骤。

从存档磁带还原数据

1. 将存档磁带从存档取回到磁带网关。有关说明，请参阅 检索存档的磁带。
2. 使用 NovaStor DataCenter /Network 软件恢复数据。您可以通过刷新邮件槽并将要取回的每个磁带移动到空槽来实现此目的，就像从物理磁带还原数据一样。有关恢复数据的信息，请参阅文档 NovaStor DataCenter /网络。

编写几个同时备份到磁带驱动器的任务

在该 NovaStor 软件中，您可以使用多路复用功能同时向磁带机写入多个作业。当为介质池提供了多路复用器时，此功能可用。有关如何使用多路复用的信息，请参阅文档 NovaStor DataCenter / Network。

解决“外部程序未正确退出”错误

将 VTL 设备配置为与 NovaStor DataCenter /Network 配合使用时，您可能会看到一条错误消息，上面写着：`External Program did not exit correctly`出现此错误的原因是 Storage Gateway 中存储驱动器和磁带驱动器的元素分配范围超过了 NovaStor DataCenter /Network 允许的数量。

Storage Gateway 返回 3200 个存储空间和import/export slots, which is more than the 2400 limit that NovaStor DataCenter/Network allows. To resolve this issue, you add a configuration file that activates the NovaStor software to limit the number of storage and import/export插槽，并预配置元素分配范围。

应用“外部程序没有正确退出”错误的解决方法

1. 导航到安装 NovaStor软件的计算机上的 Tape 文件夹。
2. 在 Tape 文件夹中，创建一个文本文件并将其命名为 `hijacc.ini`。

3. 复制以下内容并将其粘贴到 hijacc.ini 文件中，然后保存该文件。

```
port:12001
san:no
define: A3B0S0L0
*DRIVES: 10
*FIRST_DRIVE: 10000
*SLOTS: 200
*FIRST_SLOT: 20000
*HANDLERS: 1
*FIRST_HANDLER: 0
*IMP-EXPS: 30
*FIRST_IMP-EXP: 30000
```

4. 添加库并将其附加到介质管理服务器。
5. 使用以下命令将磁带从导入/导出槽移动到库中。将示例库名称替换为部署中库的名称。

   C:\Program Files\NovaStor\DataCenter\Hitback\tape\ophijacc.exe -c *VTL-ec2amaz-uko8jfj-ec2amaz-uko8jfj.lcfg*
6. 将库附加到备份服务器。
7. 在 NovaStor 软件中，将导入/导出插槽中的所有磁带导入磁带库。

使用 Quest B NetVault ackup 测试您的设置

您可以使用 Quest（前身为 Dell）Backup 将数据 NetVault 备份到虚拟磁带、存档磁带以及管理虚拟磁带库 (VTL) 设备。

在本主题中，您可以找到有关如何为磁带网关配置 Quest NetVault Backup 应用程序以及如何执行备份和恢复操作的基本文档。

有关如何使用 Quest NetVault Backup 应用程序的详细信息，请参阅 Quest NetVault Backup — 管理指南。有关兼容备份应用程序的更多信息，请参阅磁带网关支持的第三方备份应用程序。

主题

- 将 Quest NetVault Backup 配置为与 VTL 设备配合使用
- 在 Quest B NetVault ackup 中将数据备份到磁带
- 使用 Quest B NetVault ackup 存档磁带
- 从 Quest B NetVault ackup 中存档的磁带中恢复数据

将 Quest NetVault Backup 配置为与 VTL 设备配合使用

将虚拟磁带库 (VTL) 设备连接到 Windows 客户端后，可以配置 Quest NetVault Backup 以识别您的设备。有关如何将 VTL 设备连接到 Windows 客户端的信息，请参阅 连接 VTL 设备。

Quest NetVault Backup 应用程序无法自动识别磁带网关设备。您必须手动添加设备才能将其公开给 Quest NetVault Backup 应用程序，然后发现这些 VTL 设备。

添加 VTL 设备

添加 VTL 设备

1. 在 Quest NetVault Backup 中，从 “配置” 选项卡中选择 “管理设备”。
2. 在“Manage Devices (管理设备)”页上，选择 Add Devices (添加设备)。
3. 在“Add Storage (添加存储)”向导中，选择 Tape library/media changer (磁带库/介质更换器)，然后选择 Next (下一步)。
4. 在下一页上，选择物理连接到库的客户端计算机，然后选择 Next (下一步) 以扫描设备。
5. 找到设备之后将显示设备。在这种情况下，您的介质更换器将显示在“Device”框中。
6. 选择您的介质更换器，然后选择 Next (下一步)。向导中显示有关设备的详细信息。
7. 在“Add Tapes to Bays (向机架中添加磁带)”页面上，选择 Scan For Devices (扫描以查找设备)，选择客户端计算机，然后选择 Next (下一步)。

   Quest B NetVault ackup 会显示您的所有硬盘，以及您可以向其中添加硬盘的 10 个托架。一次显示一个机架。
8. 选择您要添加到所显示机架的驱动器，然后选择 Next (下一步)。

   > **Important**
   >
   > 将驱动器添加到机架时，驱动器和机架数量必须匹配。例如，如果显示机架 1，则您必须添加驱动器 1。如果驱动器未连接，则将其匹配的机架留空。
9. 在出现客户端计算机时，选择该计算机，然后选择 Next (下一步)。客户端计算机可能会多次出现。
10. 在显示驱动器时，重复步骤 7 到 9，将所有驱动器添加到机架。
11. 在 Configuration (配置) 选项卡中，选择 Manage devices (管理设备)，然后在 Manage Devices (管理设备) 页面上，展开您的介质更换器以查看您添加的设备。

在 Quest B NetVault ackup 中将数据备份到磁带

创建备份任务以及将数据写入虚拟磁带的过程与利用物理磁带时的过程相同。有关如何 NetVault 备份数据的详细信息，请参阅 Quest Backup-管理指南。

> **Note**
>
> 如果正在执行备份任务时，磁带网关出于任何原因而重新启动，则备份任务会失败。要完成失败的备份任务，必须重新提交任务。

使用 Quest B NetVault ackup 存档磁带

将磁带存档时，磁带网关会将磁带从磁带驱动器弹出至存储插槽。然后，它使用您的备份应用程序（即 Quest Backup）将磁带从插槽导出到存档。 NetVault

在 Quest B NetVault ackup 中存档磁带

1. 在 Quest NetVault Backup 配置选项卡中，选择并展开介质更换器以查看您的磁带。
2. 选择槽的设置图标，以打开介质更换器的槽浏览器。
3. 在槽中，选择要归档的磁带，然后选择导出。

存档过程可能需要一段时间才能完成。磁带的初始状态显示为正在传输到 VTS。存档开始后，状态变为正在存档。存档完成后，磁带不再在 VTL 中列出。

在 Quest NetVault Backup 软件中，确认磁带已不在存储插槽中。

在 Storage Gateway 控制台的“导航”窗格中，选择磁带。验证已存档磁带的状态是否为 ARCHIVED (已存档)。

从 Quest B NetVault ackup 中存档的磁带中恢复数据

存档数据的还原过程包含两个步骤。

从存档磁带还原数据

1. 将存档磁带从存档取回到磁带网关。有关说明，请参阅 检索存档的磁带。
2. 使用 Quest NetVault Backup 应用程序恢复数据。您可通过创建还原文件夹文件完成此任务，就像从物理磁带还原数据一样。有关创建还原任务的说明，请参阅 Quest NetVault Backup-管理指南。

下一步

清理不必要的资源

使用 Veeam Backup and Replication 测试您的设置

您可以使用 Veeam Backup & Replication 将数据备份到虚拟磁带、存档磁带并管理虚拟磁带库 (VTL) 设备。在本主题中，您可以找到有关如何针对磁带网关配置 Veeam Backup & Replication 软件以及执行备份和还原操作的基本文档。有关如何使用 Veeam 软件的详细信息，请参阅 Veeam Backup & Replication 文档。有关兼容备份应用程序的更多信息，请参阅磁带网关支持的第三方备份应用程序。

主题

- 配置 Veeam 以使用 VTL 设备
- 将磁带导入 Veeam
- 在 Veeam 中将数据备份到磁带
- 使用 Veeam 将磁带存档
- 在 Veeam 中从存档磁带还原数据

配置 Veeam 以使用 VTL 设备

将您的虚拟磁带库 (VTL) 设备连接到 Windows 客户端后，应配置 Veeam Backup & Replication 以识别您的设备。有关如何将 VTL 设备连接到 Windows 客户端的信息，请参阅 连接 VTL 设备。

更新 VTL 设备驱动程序

要配置软件来与磁带网关设备一起使用，您需要更新设备驱动程序以使 VTL 设备向 Veeam 软件公开并发现 VTL 设备。在设备管理器中，更新介质更换器的驱动程序。有关说明，请参阅 更新介质更换器的设备驱动程序。

发现 VTL 设备

如果您的介质转换器未知，则必须使用本机 SCSI 命令而非 Windows 驱动程序来发现您的磁带库。有关详细说明，请参阅磁带库。

发现 VTL 设备

1. 在 Veeam 软件中，选择 Tape Infrastructur（磁带基础设施）。连接磁带网关后，虚拟磁带会在 Tape Infrastructure（磁带基础设施）选项卡中列出。

2. 展开 Tape (磁带) 树，查看您的磁带驱动器和介质更换器。
3. 展开介质更换器树。如果您的磁带驱动器映射到介质更换器，则驱动器会显示在 Drives (驱动器) 下。否则，磁带库和磁带驱动器会显示为独立设备。

   如果驱动器未自动映射，请按照 Veeam 网站上的说明映射驱动器。

将磁带导入 Veeam

您现在已做好将磁带从磁带网关导入 Veeam 备份应用程序库的准备。

将磁带导入 Veeam 库

1. 打开介质更换器的上下文（右键单击）菜单，然后选择 Import (导入) 将磁带导入到 I/E 槽。
2. 打开介质更换器的上下文（右键单击）菜单，然后选择 Inventory Library (清点库) 以标识未识别的磁带。首次将新虚拟磁带加载到磁带驱动器中时，Veeam 备份应用程序无法识别相应磁带。要标识未识别的磁带，您需要清点磁带库中的磁带。

在 Veeam 中将数据备份到磁带

将数据备份到磁带的过程包括两个步骤：

1. 创建一个介质池，将磁带添加到介质池中。
2. 将数据写入磁带。

创建介质池和将数据写入虚拟磁带的过程与利用物理磁带时的过程相同。有关如何备份数据的详细信息，请参阅 Veeam 帮助中心的开始使用磁带。

> **Note**
>
> 如果正在执行备份任务时，磁带网关出于任何原因而重新启动，则备份任务会失败。要完成失败的备份任务，必须重新提交任务。

使用 Veeam 将磁带存档

将磁带存档时，磁带网关将磁带从 Veeam 磁带库移至脱机存储。您通过以下方式开始磁带存档：将磁带从磁带驱动器弹出到存储槽，然后使用备份应用程序（即 Veeam 软件）将磁带从存储槽提取到存档。

将磁带存档到 Veeam 库中

1. 选择 Tape Infrastructure（磁带基础设施），然后选择包含要存档的磁带的介质池。
2. 打开要存档的磁带的上下文（右键单击）菜单，然后选择 Eject Tape (弹出磁带)。
3. 对于 Ejecting tape (弹出磁带)，请选择 Close (关闭)。磁带位置从磁带驱动器更改为槽。
4. 再次打开磁带的上下文（右键单击）菜单，然后选择 Export (导出)。磁带状态从 Tape drive (磁带驱动器) 更改为 Offline (脱机)。
5. 对于 Exporting tape (导出磁带)，请选择 Close (关闭)。磁带位置从 Slot (槽) 更改为 Offline (脱机)。
6. 在 Storage Gateway 控制台上，选择您的网关，然后选择 VTL 磁带盒并验证所存档的虚拟磁带的状态。

   存档过程可能需要一段时间才能完成。磁带的初始状态显示为正在传输到 VTS。存档开始后，状态变为正在存档。在存档完成后，磁带不再在 VTL 中列出，而是存档在 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 中。

在 Veeam 中从存档磁带还原数据

存档数据的还原过程包含两个步骤。

从存档磁带还原数据

1. 将存档磁带从存档取回到磁带网关。有关说明，请参阅 检索存档的磁带。
2. 使用 Veeam 软件可还原数据。您可通过创建还原文件夹文件完成此任务，就像从物理磁带还原数据一样。有关说明，请参阅 Veeam 帮助中心的从磁带还原文件。

下一步

清理不必要的资源

使用 Veritas Backup Exec 测试您的设置

通过使用 Veritas Backup Exec，可以将数据备份到虚拟磁带，对磁带进行存档和管理虚拟磁带库 (VTL) 设备。在本主题中，您可以找到使用 Backup Exec 执行备份和还原操作所需的基本文档。

有关如何使用 Backup Exec 的更多详细信息，包括如何创建安全备份、软件和硬件兼容性列表以及管理员指南，请参阅 Veritas 支持网站。

有关受支持的备份应用程序的更多信息，请参阅磁带网关支持的第三方备份应用程序。

主题

- 在 Backup Exec 中配置存储
- 在 Backup Exec 中导入磁带
- 在 Backup Exec 中将数据写入磁带
- 使用 Backup Exec 将磁带存档
- 在 Backup Exec 中从存档磁带还原数据
- 在 Backup Exec 中停用磁带驱动器

在 Backup Exec 中配置存储

将虚拟磁带库 (VTL) 设备连接到 Windows 客户端后，应配置 Backup Exec 存储以识别您的设备。有关如何将 VTL 设备连接到 Windows 客户端的信息，请参阅 连接 VTL 设备。

配置存储

1. 启动 Backup Exec 软件，然后选择工具栏左上角的黄色图标。
2. 选择配置和设置，然后选择 Backup Exec 服务以打开 Backup Exec 服务管理器。
3. 选择重新启动所有服务。Backup Exec 随后可识别 VTL 设备 (即，介质更换器和磁带驱动器)。重启过程可能需要几分钟。

> **Note**
>
> 磁带网关提供 10 个磁带驱动器。但是，您的 Backup Exec 许可协议可能要求您的备份应用程序使用少于 10 个的磁带驱动器。在这种情况下，您必须在 Backup Exec 机械手库中停用磁带驱动器，以便仅启用许可协议允许的磁带驱动器数量。有关说明，请参阅 在 Backup Exec 中停用磁带驱动器 。

4. 在重启完成之后，关闭 Backup Exec 服务管理器。

在 Backup Exec 中导入磁带

您现在已准备好将磁带从网关导入槽。

1. 选择存储选项卡，然后展开机械手库树以显示 VTL 设备。

> **Important**
>
> Veritas Backup Exec 软件需要磁带网关介质更换器类型。如果在机械手库下列出的介质更换器类型不是磁带网关，则必须先更改它，然后才能在备份应用程序中配置存储。有关如何选择不同介质更换器类型的信息，请参阅在网关激活后选择介质更换器。

2. 选择槽图标以显示所有槽。

> **Note**
>
> 将磁带导入到磁带库时，磁带存储在槽而不是磁带驱动器中。因此，磁带驱动器可能会显示消息，说明驱动器中没有介质 (No media)。当您启动备份或还原任务时，磁带将移动到磁带驱动器中。
>
> 您在网关磁带库中必须有可用磁带才能将磁带导入存储槽。有关如何创建磁带的说明，请参阅 为磁带网关创建新的虚拟磁带。

3. 打开空槽的上下文（右键单击）菜单，选择导入，然后选择立即导入介质。您可在一次导入操作中选择多个槽并导入多个磁带。
4. 在显示的介质请求窗口中，选择查看详细信息。
5. 在操作警报: 介质干预窗口中，选择响应确定以将介质插入槽。

   磁带将显示在您选择的槽中。

> **Note**
>
> 导入的磁带包括空磁带和已从存档检索到网关的磁带。

在 Backup Exec 中将数据写入磁带

利用您对物理磁带执行的同一过程和备份策略，将数据写入磁带网关虚拟磁带。有关详细信息，请参阅 Backup Exec 软件的 Backup Exec 管理指南 文档部分。

> **Note**
>
> 如果正在执行备份任务时，磁带网关出于任何原因而重新启动，则备份任务可能会失败。如果备份任务失败，Veritas Backup Exec 中的磁带状态会更改为不可附加。您可以存档磁带或继续从中读取数据。要完成失败的备份任务，必须在新磁带上重新提交任务。

使用 Backup Exec 将磁带存档

在将磁带存档时，磁带网关会将磁带从网关的虚拟磁带库 (VTL) 中移到脱机存储。您可以使用 Backup Exec 软件通过导出磁带来启动磁带存档。

对磁带进行存档

1. 选择存储菜单，选择槽，打开您要从中导出磁带的槽的上下文（右键单击）菜单，选择导出介质，然后选择立即导出介质。您可在一次导出操作中选择多个槽并导出多个磁带。
2. 在介质请求弹出窗口中，选择查看详情，然后在警报：介质干预窗口中选择响应确定。

   在 Storage Gateway 控制台中，可验证要存档的磁带的状态。将数据上传到 Amazon可能需要一段时间才能完成。在这段时间内，将在磁带网关 VTL 中列出导出的磁带，状态为正在传输到 VTS。上传完成并且存档过程开始后，状态将变为正在存档。在数据存档完成后，导出的磁带不再在 VTL 中列出，而是存档在 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 中。
3. 选择您的网关，然后选择 VTL 盒式磁带并验证您的网关中是否不再列出虚拟磁带。
4. 在 Storage Gateway 控制台的“导航”窗格中，选择磁带。确认磁带的状态为已存档。

在 Backup Exec 中从存档磁带还原数据

存档数据的还原过程包含两个步骤。

从存档磁带还原数据

1. 将存档的磁带取回到磁带网关。有关说明，请参阅 检索存档的磁带。
2. 使用 Backup Exec 还原数据。此过程与从物理磁带还原数据相同。有关说明，请参阅 Backup Exec 软件的 Backup Exec 管理指南 文档部分。

在 Backup Exec 中停用磁带驱动器

磁带网关提供了 10 个磁带驱动器，但您可以决定使用少于此数量的磁带驱动器。在这种情况下，应停用您不使用的磁带驱动器。

1. 打开 Backup Exec，并选择存储选项卡。
2. 在机械手库树中，打开要停用的磁带驱动器的上下文（右键单击）菜单，然后选择禁用。

下一步

清理不必要的资源

使用 Veritas 测试您的设置 NetBackup

您可以使用 Ver NetBackup itas 将数据备份到虚拟磁带、存档磁带并管理虚拟磁带库 (VTL) 设备。在本主题中，您可以找到有关如何为磁带网关配置 NetBackup 应用程序以及如何执行备份和恢复操作的基本文档。

有关如何使用的详细信息 NetBackup，请参阅 Veritas 网站上的 Veritas 服务和运营准备工具 (SORT) 页面。

有关兼容备份应用程序的更多信息，请参阅磁带网关支持的第三方备份应用程序。

主题

- 配置 NetBackup 存储设备
- 将数据备份到磁带
- 存档磁带
- 从磁带还原数据

配置 NetBackup 存储设备

将虚拟磁带库 (VTL) 设备连接到 Windows 客户端后，可以配置 Veritas NetBackup 存储以识别您的设备。有关如何将 VTL 设备连接到 Windows 客户端的信息，请参阅 连接 VTL 设备。

配置 NetBackup 为使用磁带网关上的存储设备

1. 以管理员身份打开 NetBackup 管理控制台。
2. 选择 Configure Storage Devices (配置存储设备) 以打开设备配置向导。

3. 选择下一步。该 NetBackup 应用程序将您的计算机检测为设备主机。
4. 在 Device Hosts (设备主机) 列中，选择您的计算机，然后选择 Next (下一步)。该 NetBackup 应用程序会扫描您的计算机中的设备并发现所有设备。
5. 在 Scanning Hosts (扫描主机) 页面上，选择 Next (下一步)，然后选择 Next (下一步)。该 NetBackup 应用程序会在您的计算机上找到所有 10 个磁带驱动器和介质更换器。
6. 在 Backup Devices (备份设备) 窗口中，选择 Next (下一步)。
7. 在 Drag and Drop Configuration (拖放配置) 窗口中，确认选择了您的介质更换器，然后选择 Next (下一步)。
8. 在随后显示的对话框中，选择 Yes (是) 以将配置保存到您的计算机上。 NetBackup 应用程序更新设备配置。
9. 更新完成后，选择 “下一步”，使设备可供 NetBackup 应用程序使用。
10. 在 Finished! (已完成!) 窗口中，选择 Finish (完成)。

在 NetBackup 应用程序中验证您的设备

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。选择 Drives (驱动器) 以显示所有磁带驱动器。
2. 在 Devices (设备) 节点中，选择 Robots (机械手) 以显示您的所有介质更换器。在 NetBackup 应用程序中，介质更换器被称为机器人。
3. 在 All Robots (所有机械手) 窗格中，打开 TLD(0)（即您的机械手）的上下文（右键单击）菜单，然后选择 Inventory Robot (清点机械手)。
4. 在机械手清点窗口中，确认从选择机械手类别下的设备主机列表中选择了主机。
5. 确认从 Robot (机械手) 列表中选择了您的机械手。
6. 在 Robot Inventory (机械手清点) 窗口中，依次选择 Update volume configuration (更新卷配置)、Preview changes (预览更改)、Empty media access port prior to update (更新前清空介质访问端口) 和 Start (启动)。

   然后，该过程会在 NetBackup 企业媒体管理 (EMM) 数据库中盘点您的介质更换器和虚拟磁带。NetBackup 在 EMM 中存储媒体信息、设备配置和磁带状态。
7. 清点完成后，在 Robot Inventory (机械手清点) 窗口中，选择 Yes (是)。在此处选择 Yes (是) 将更新配置，并将在导入/导出槽中找到的虚拟磁带移至虚拟磁带库。
8. 关闭 Robot Inventory (机械手清点) 窗口。
9. 在 Media (介质) 节点中，展开 Robots (机械手) 节点，然后选择 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**
>
> 如果您之前已将其他设备连接到 NetBackup应用程序，则可能有多个机器人。确保所选的机械手正确无误。

既然您已连接设备并使这些设备可供备份应用程序使用，现在便可以测试网关了。要测试网关，您可以将数据备份到创建的虚拟磁带并对磁带进行存档。

将数据备份到磁带

通过将数据备份到虚拟磁带上，测试磁带网关设置。

> **Note**
>
> - 对于本入门练习，只应备份少量数据，因为这会产生与存储、存档和检索数据关联的成本。有关定价信息，请参阅 Storage Gateway 详情页面上的定价。
> - 如果正在执行备份任务时，磁带网关出于任何原因而重新启动，则备份任务会暂停。当您的网关完成重启后，暂停的备份任务会自动恢复。

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 Media (介质) 节点，打开 Volume Pool (卷池) 的上下文（右键单击）菜单，然后选择 New (新建)。此时将显示 New Volume Pool (新建卷池) 对话框。
3. 对于 Name (名称)，键入卷池的名称。
4. 对于 Description (描述)，键入卷池的说明，然后选择 OK (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 Robots (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。

   如果以前已连接了机械手，则您的磁带网关机械手的名称可能不同。
2. 从虚拟磁带的列表中，打开要添加到卷池的磁带的上下文（右键单击）菜单，然后选择 Change (更改) 以打开 Change Volumes (更改卷) 对话框。
3. 对于 Volume Pool (卷池)，选择 New pool (新建池)。
4. 对于 New pool (新建池)，选择您刚刚创建的池，然后选择 OK (确定)。

   可通过展开 Media (介质) 节点并选择您的卷池，确认您的卷池包含刚刚添加的虚拟磁带。

创建备份策略

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。

1. 选择您的主服务器返回到 Veritas NetBackup 控制台。
2. 选择 Create a Policy (创建策略) 以打开 Policy Configuration Wizard (策略配置向导) 窗口。
3. 选择 File systems, databases, applications (文件系统、数据库和应用程序)，然后选择 Next (下一步)。
4. 在策略名称中，键入策略的名称并确认已从选择策略类型列表中选择 MS-Windows，然后选择下一步。
5. 在 Client List (客户端) 窗口中，选择 Add (添加)，在 Name (名称) 列中键入您的计算机的主机名，然后选择 Next (下一步)。此步骤将您定义的策略应用于 `localhost`（您的客户端计算机）。
6. 在 Files (文件) 窗口中，选择 Add (添加)，然后选择文件夹图标。
7. 在 Browse (浏览) 窗口中，浏览到要备份的文件夹或文件，选择 OK (确定)，然后选择 Next (下一步)。
8. 在 Backup Types (备份类型) 窗口中，接受默认值，然后选择 Next (下一步)。

   > **Note**
   >
   > 如果要自行开始备份，则选择 User Backup (用户备份)。

9. 在 Frequency and Retention (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，然后选择下一步。

10. 在 Start (开始时间) 窗口中，选择 Off hours (业余时间)，然后选择 Next (下一步)。此选项指定应仅在业余时间备份您的文件夹。
11. 在 Policy Configuration (策略配置) 向导中，选择 Finish (完成)。

该策略根据计划运行备份。您还可以随时执行手动备份，在下一步中我们将这样做。

执行手动备份

1. 在 NetBackup 控制台的导航窗格上，展开NetBackup 管理节点。
2. 展开 Policies (策略) 节点。
3. 打开策略的上下文（右键单击）菜单，然后选择 Manual Backup (手动备份)。
4. 在 Manual Backup (手动备份) 窗口中，选择一个计划，再选择一个客户端，然后选择 OK (确定)。
5. 在随后显示的 Manual Backup Started (手动备份已开始) 对话框中，选择 OK (确定)。
6. 在导航窗格上，选择 Activity Monitor (活动监视器) 以在 Job ID (任务 ID) 列中查看备份的状态。

要查找备份期间 NetBackup 写入文件数据的虚拟磁带的条形码，请按以下过程所述查看 Job Det ails 窗口。在下一部分中的对磁带进行存档的过程中，将需要用到此条码。

查找磁带的条码

1. 在 Activity Monitor (活动监视器) 中，打开 Job ID (任务 ID) 列中您的备份作业的标识符的上下文（右键单击）菜单，然后选择 Details (详细信息)。
2. 在 Job Details (任务详细信息) 窗口中，选择 Detailed Status (详细信息状态) 选项卡。
3. 在 Status (状态) 框中，找到介质 ID。例如，状态报告中的一个条目可能显示 `media id 87A222`。此 ID 可帮助您确定已将数据写入到哪个磁带。

您现在已成功部署了磁带网关、创建了虚拟磁带并备份了数据。接下来，可对虚拟磁带进行存档并从存档检索这些虚拟磁带。

存档磁带

对磁带进行存档时，磁带网关会将磁带从网关的虚拟磁带库 (VTL) 移至存档，这将提供脱机存储。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 “媒体和设备管理” 节点，然后展开 “媒体” 节点。
2. 展开 Robots (机械手) 并选择 TLD(0)。
3. 打开要存档的虚拟磁带的上下文（右键单击）菜单，然后选择 Eject Volume From Robot (从机械手弹出卷)。
4. 在 Eject Volumes (弹出卷) 窗口中，确保 Media ID (介质 ID) 与要弹出的虚拟磁带相符，然后选择 Eject (弹出)。
5. 在此对话框中，选择 Yes (是)。

   弹出过程完毕后，Eject Volumes (弹出卷) 对话框中磁带的状态指示弹出已成功。
6. 选择 Close (关闭) 以关闭 Eject Volumes (弹出卷) 窗口。
7. 在 Storage Gateway 控制台中，验证您在网关 VTL 中存档的磁带的状态。将数据上传到 Amazon 需要一段时间才能完成。在这段时间内，将在网关 VTL 中列出弹出的磁带，状态为 IN TRANSIT TO VTS (正在传输到 VTS)。在存档开始时，状态为 ARCHIVING (正在存档)。在数据上传完成后，弹出的磁带不再在 VTL 中列出，而是存档在 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 中。
8. 要验证您的网关中是否不再列出虚拟磁带，请选择您的网关，然后选择 VTL Tape Cartridges (VTL 盒式磁带)。
9. 在 Storage Gateway 控制台的“导航”窗格中，选择磁带。验证已存档磁带的状态是否为 ARCHIVED (已存档)。

从磁带还原数据

存档数据的还原过程包含两个步骤。

从存档磁带还原数据

1. 将存档的磁带取回到磁带网关。有关说明，请参阅 检索存档的磁带。
2. 使用与 Veritas NetBackup 应用程序一起安装的 Backup、存档和恢复软件。此过程与从物理磁带还原数据相同。有关说明，请参阅 Veritas 网站上的 Veritas Services and Operations Readiness Tools (SORT)。

下一步

清理不必要的资源

接下来该做什么？

在磁带网关投入使用之后，您可以执行一些维护任务，例如添加和移除磁带、监控和优化网关性能以及进行故障排除。有关这些管理任务的一般信息，请参阅 管理磁带网关。

您可以在上执行一些 Tape Gateway 维护任务 Amazon Web Services Management Console，例如配置网关的带宽速率限制和管理网关软件更新。如果您的磁带网关部署在本地，您可在网关的本地控制台上执行一些维护任务。其中包括通过代理来路由磁带网关以及将网关配置为使用静态 IP 地址。如果您将网关作为亚马逊 EC2 实例运行，则可以在亚马逊 EC2 控制台上执行特定的维护任务，例如添加和移除 Amazon EBS 卷。有关维护磁带网关的更多信息，请参阅管理磁带网关。

如果您计划将您的网关部署在生产环境中，则在确定磁盘大小时应考虑实际工作负载。有关如何确定实际磁盘大小的信息，请参阅 管理 Storage Gateway 的本地磁盘。此外，如果您不打算继续使用您的磁带网关，请考虑将其清除。清除可让您避免产生费用。有关清除的信息，请参阅 清理不必要的资源。

在 Virtual Private Cloud 中激活网关

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

要在 VPC 中激活您的网关，请使用 Amazon VPC 控制台为 Storage Gateway 创建 VPC 端点并获取 VPC 端点 ID，然后在创建和激活网关时指定此 VPC 端点 ID。有关更多信息，请参阅 Connect 您的磁带网关以 Amazon。

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

主题

- 为 Storage Gateway 创建 VPC 端点

为 Storage Gateway 创建 VPC 端点

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

为 Storage Gateway 创建 VPC 端点

1. 登录 Amazon Web Services Management Console 并打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Endpoints (终端节点)，然后选择 Create Endpoint (创建终端节点)。
3. 在创建端点页面上，为服务类别选择 Amazon 服务。
4. 对于 Service Name (服务名称)，选择 `com.amazonaws.region.storagegateway`。例如 `com.amazonaws.us-east-2.storagegateway`。
5. 对于 VPC，选择您的 VPC 并记录其可用区和子网。
6. 确认未选中 Enable Private DNS Name (启用私有 DNS 名称)。
7. 对于 Security group (安全组)，选择您要用于 VPC 的安全组。您可以接受默认安全组。验证在您的安全组中已经允许了以下所有的 TCP 端口：

   - TCP 443
   - TCP 1026
   - TCP 1027
   - TCP 1028
   - TCP 1031
   - TCP 2222
8. 选择创建端点。终端节点的初始状态为 pending (待处理)。创建终端节点时，记下您刚创建的 VPC 终端节点的 ID。
9. 在创建终端节点时，选择 Endpoints (终端节点)，然后选择新的 VPC 终端节点。
10. 在所选存储网关端点的详细信息选项卡中，在 DNS 名称下，使用第一个未指定可用区的 DNS 名称。您的 DNS 名称类似这样：`vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

现在，您有了 VPC 终端节点，可以创建您的网关。有关更多信息，请参阅创建网关。

管理磁带网关

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

接下来，您可以找到有关如何管理磁带网关资源的信息。

主题

- 编辑基本网关信息-了解如何使用 Storage Gateway 控制台编辑现有网关的基本信息，包括网关名称、时区和 CloudWatch 日志组。
- 管理自动创建磁带功能：了解如何配置磁带网关来自动创建新的虚拟磁带，从而保持指定的最小可用磁带数。
- 将虚拟磁带存档：了解如何在创建新磁带时，将磁带归档配置为 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类。
- 将磁带移至 S3 Glacier Deep Archive 存储类：了解如何将磁带从 S3 Glacier Flexible Retrieval 移到 S3 Glacier Deep Archive，从而以非常低的成本提供长期数据留存和数字保留。
- 检索存档的磁带：了解如何通过首先将磁带检索到磁带网关，来访问存储在归档虚拟磁带上的数据。
- 查看磁带使用情况统计数据：了解如何使用 Storage Gateway 控制台来查看磁带上存储的数据量。
- 从磁带网关中删除虚拟磁带：了解如何使用 Storage Gateway 控制台来从磁带网关中删除虚拟磁带。
- 删除自定义磁带池：了解如何使用 Storage Gateway 控制台来删除自定义磁带池。
- 停用磁带网关：了解在磁带网关出现故障，而您想要将磁带从出现故障的网关恢复到另一个网关时，如何停用该网关。
- 理解磁带状态：了解 Storage Gateway 报告的各种磁带状态值，以协助确定磁带是否运行正常，或者是否存在可能需要您采取措施的问题。
- 将数据移至新网关：了解随着数据和性能需求的增长，或者如果收到迁移网关的 Amazon 通知，如何在网关之间移动数据。

编辑基本网关信息

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

编辑现有网关的基本信息

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

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

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

管理自动创建磁带功能

磁带网关会自动创建新的虚拟磁带，来维持您配置的最小可用磁带数。然后，它会将这些新磁带设为可由备份应用程序导入，以便备份作业可以不间断地运行。自动创建磁带功能除了无需手动创建新的虚拟磁带之外，还不需要自定义脚本。

删除自动磁带创建策略

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在导航窗格中，选择 Gateways (网关) 选项卡。
3. 选择要为其管理自动磁带创建功能的网关。
4. 在 Actions (操作) 菜单上，选择 Configure tape auto-create (配置自动创建磁带)。

5. 要删除网关上的自动磁带创建策略，请选择要删除的策略右侧的删除。

   要停止网关上的自动磁带创建功能，请删除该网关的所有自动磁带创建策略。

   选择保存更改，确认删除所选磁带网关的磁带自动创建策略。

   > **Note**
   >
   > 删除网关中的自动创建磁带策略的操作无法撤消。

更改磁带网关的自动磁带创建策略

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在导航窗格中，选择 Gateways (网关) 选项卡。
3. 选择要为其管理自动磁带创建功能的网关。
4. 在操作菜单中，选择配置磁带自动创建，然后在显示的页面上更改设置。
5. 对于最小磁带数，请输入磁带网关上应始终可用的最小虚拟磁带数。此值的有效范围是 1 到 10。
6. 对于 Capacity (容量)，请输入虚拟磁带的容量大小（以字节为单位）。此值的有效范围是 100 GiB 至 15 TiB。
7. 对于 Barcode prefix (条码前缀)，请输入要在虚拟磁带条码前面附加的前缀。

   > **Note**
   >
   > 虚拟磁带由条码唯一标识，您可以为该条码添加前缀。该前缀为可选，但是，可将其用于帮助识别虚拟磁带。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。

8. 对于 Pool (池)，请选择 Glacier Pool (Glacier 池) 或 Deep Archive Pool (Deep Archive 池)。该池代表磁带在被备份软件弹出后将存储到的存储类。

   - 如果要在 S3 Glacier Flexible Retrieval 存储类中存档磁带，请选择 Glacier 池。在备份软件弹出磁带时，将在 S3 Glacier Flexible Retrieval 中自动存档磁带。对于更多活动存档，可以使用 S3 Glacier Flexible Retrieval，这样您通常可以在 3-5 小时内取回磁带。有关详细信息，请参阅《Amazon Simple Storage Service 用户指南》中的用于存档对象的存储类。
   - 如果要在 S3 Glacier Deep Archive 中存档磁带，请选择 Deep Archive 池。在备份软件弹出磁带时，将在 S3 Glacier Deep Archive 中自动存档磁带。您可以使用 S3 Glacier Deep Archive 实现长期数据留存和数字保留，每年访问一次或两次其中的数据。您通常可以在 12 小时内取回

在 S3 Glacier Deep Archive 中存档的磁带。有关详细信息，请参阅《Amazon Simple Storage Service 用户指南》中的用于存档对象的存储类。

如果您在 S3 Glacier Flexible Retrieval 中存档磁带，以后可以将其转移到 S3 Glacier Deep Archive。有关更多信息，请参阅 将磁带移至 S3 Glacier Deep Archive 存储类。

9. 您可以在磁带概述页面上找到有关磁带的信息。默认情况下，此列表一次最多显示 1000 个磁带，但您执行的搜索会应用于所有磁带。您可以使用搜索栏来查找符合特定条件的磁带，也可以将列表缩减到少于 1000 个磁带。当您的列表包含 1000 个或更少磁带时，您可以按各种属性以升序或降序对磁带进行排序。

   在创建可用虚拟磁带时，其状态最初被设置为 CREATING (正在创建)。创建磁带后，其状态变为 AVAILABLE (可用)。有关更多信息，请参阅 理解磁带状态。

   有关启用自动磁带创建功能的更多信息，请参阅自动创建磁带。

将虚拟磁带存档

您可以将磁带存档到 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive。在创建磁带时，您可以选择要用于存档磁带的存档池。

如果要在 S3 Glacier Flexible Retrieval 中存档磁带，请选择 Glacier 池。在备份软件弹出磁带时，将在 S3 Glacier Flexible Retrieval 中自动存档磁带。如果定期检索数据并需要在几分钟内完成，您可以使用 S3 Glacier Flexible Retrieval 存储更多活动存档。有关详细信息，请参阅用于存档对象的存储类。

如果要在 S3 Glacier Deep Archive 存档磁带，请选择 Deep Archive 池。在备份软件弹出磁带时，将在 S3 Glacier Deep Archive 中自动存档磁带。您可以使用 S3 Glacier Deep Archive 以极低的成本提供长期数据留存和数字保留。系统不会经常检索或很少检索 S3 Glacier Deep Archive 中的数据。有关详细信息，请参阅用于存档对象的存储类。

> **Note**
>
> 对于在 2019 年 3 月 27 日之前创建的任何磁带，在备份软件弹出磁带时，将直接在 S3 Glacier Flexible Retrieval 中存档磁带。

在备份软件弹出磁带时，自动在您创建磁带时选择的池中存档磁带。根据备份软件，弹出磁带的过程将会有所不同。某些备份软件要求您在弹出磁带后将其导出，然后才能开始存档。有关受支持备份软件的信息，请参阅使用备份软件来测试您的网关设置。

将磁带移至 S3 Glacier Deep Archive 存储类

将磁带从 S3 Glacier Flexible Retrieval 移动到 S3 Glacier Deep Archive，以极低的成本提供长期数据留存和数字保留。您可以使用 S3 Glacier Deep Archive 实现长期数据留存和数字保留，每年访问一次或两次其中的数据。有关详细信息，请参阅用于存档对象的存储类。

将磁带从 S3 Glacier Flexible Retrieval 移动到 S3 Glacier Deep Archive

1. 在导航窗格中，选择磁带库 > 磁带来查看您的磁带。默认情况下，此列表一次最多显示 1000 个磁带，但您执行的搜索会应用于所有磁带。您可以使用搜索栏来查找符合特定条件的磁带，也可以将列表缩减到少于 1000 个磁带。当您的列表包含 1000 个或更少磁带时，您可以按各种属性以升序或降序对磁带进行排序。
2. 选中要移到 S3 Glacier Deep Archive 的磁带的复选框。您可以在池列中看到与每个磁带关联的池。
3. 选择分配到池。
4. 在“将磁带分配到池”对话框中，验证您正在移动的磁带的条码并选择分配。

> **Note**
>
> 如果磁带已由备份应用程序弹出并在 S3 Glacier Deep Archive 中存档，则无法将其移回 S3 Glacier Flexible Retrieval。将磁带从 S3 Glacier Flexible Retrieval 移动到 S3 Glacier Deep Archive 会产生费用。此外，如果您在 90 天之前将磁带从 S3 Glacier Flexible Retrieval 移至 S3 Glacier Deep Archive，则会产生 S3 Glacier Flexible Retrieval 的提前删除费用。

5. 移动磁带后，您可以在磁带概述页面的池列中看到更新的状态。

检索存档的磁带

要访问存储在存档虚拟磁带上的数据，必须先将所需的磁带取回到磁带网关。您的磁带网关为每个网关提供一个虚拟磁带库 (VTL)。

如果您在中有多个磁带网关 Amazon Web Services 区域，则只能将磁带检索到一个网关。

已检索的磁带被写保护，您只能读取磁带上的数据。

> **Important**
>
> 如果您在 S3 Glacier Flexible Retrieval 中存档磁带，则通常可以在 3-5 小时内取回磁带。如果您在 S3 Glacier Deep Archive 中存档磁带，则通常可以在 12 小时内取回磁带。

> **Note**
>
> 从存档检索磁带需要收费。有关详细定价信息，请参阅 Storage Gateway 定价。

将存档的磁带取回到网关中

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在导航窗格中，选择磁带库 > 磁带来查看您的磁带。默认情况下，此列表一次最多显示 1000 个磁带，但您执行的搜索会应用于所有磁带。您可以使用搜索栏来查找符合特定条件的磁带，也可以将列表缩减到少于 1000 个磁带。当您的列表包含 1000 个或更少磁带时，您可以按各种属性以升序或降序对磁带进行排序。
3. 从虚拟磁带架选项卡中选择要取回的虚拟磁带，然后选择取回磁带。

   > **Note**
   >
   > 要取回的虚拟磁带的状态必须为 ARCHIVED (已存档)。

4. 在 Retrieve tape 对话框中，对于 Barcode，确认条码标识要检索的虚拟磁带。
5. 对于网关，选择要将存档的磁带取回到其中的网关，然后选择取回磁带。

磁带的状态从“ARCHIVED”(已存档) 变为“RETRIEVING”(正在检索)。此时，您的数据将从虚拟磁带架（使用 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）移动到虚拟磁带库（由 Amazon S3 支持）。在移动所有数据后，存档中的虚拟磁带状态将变为 RETRIEVED (已检索)。

> **Note**
>
> 取回的虚拟磁带为只读。

查看磁带使用情况统计数据

当您将数据写入磁带时，可以在 Storage Gateway 控制台中查看磁带上存储的数据量。每个磁带的 Details 选项卡显示磁带使用率信息。

查看磁带上存储的数据量

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在导航窗格中，选择磁带库 > 磁带来查看您的磁带。默认情况下，此列表一次最多显示 1000 个磁带，但您执行的搜索会应用于所有磁带。您可以使用搜索栏来查找符合特定条件的磁带，也可以将列表缩减到少于 1000 个磁带。当您的列表包含 1000 个或更少磁带时，您可以按各种属性以升序或降序对磁带进行排序。
3. 选择您感兴趣的磁带。
4. 显示的页面提供了有关磁带的各种详细信息，包括：
   - 大小：所选磁带的总容量。
   - 已使用：您的备份应用程序写入磁带的数据的大小。

   > **Note**
   >
   > 该值不适用于在 2015 年 5 月 13 日之前创建的磁带。

从磁带网关中删除虚拟磁带

可使用 Storage Gateway 控制台从磁带网关中删除虚拟磁带。

> **Note**
>
> 如果要从磁带网关中删除状态为“已取回”的磁带，则必须先使用备份应用程序弹出磁带，然后再删除该磁带。有关如何使用 Symantec NetBackup 软件弹出磁带的说明，请参阅存档磁带。弹出磁带后，磁带状态变回“已存档”。然后，您可以删除磁带。

在删除磁带之前，请先备份数据。删除的磁带将无法恢复。

删除虚拟磁带

> **Warning**
>
> 此过程将永久删除所选的虚拟磁带。

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在导航窗格中，选择磁带库 > 磁带来查看您的磁带。默认情况下，此列表一次最多显示 1000 个磁带，但您执行的搜索会应用于所有磁带。您可以使用搜索栏来查找符合特定条件的磁带，也可以将列表缩减到少于 1000 个磁带。当您的列表包含 1000 个或更少磁带时，您可以按各种属性以升序或降序对磁带进行排序。
3. 选择一个或多个要删除的磁带。
4. 在操作中，选择删除。此时会显示确认对话框。
5. 确认要删除指定的磁带，然后在确认框中键入单词 delete 并选择删除。

删除磁带后，该磁带将从磁带网关中消失。

删除自定义磁带池

以下过程说明如何使用 Storage Gateway 控制台删除自定义磁带池。要使用 API 以编程方式执行此操作，请参阅 Storage Gateway API 参考DeleteTapePool中的。

只有在自定义磁带池中没有已存档的磁带，且池没有附加自动磁带创建策略时，才能删除该池。如果您需要从磁带池中删除自动磁带创建策略，请参阅 Managing Automatic Tape Creation。

使用 Storage Gateway 控制台删除自定义磁带池

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在导航窗格中，选择池来查看可用池。
3. 选择一个或多个要删除的磁带池。

   如果您要删除的磁带池的磁带计数为 0，且没有引用该自定义磁带池的自动磁带创建策略，则可以删除这些池。
4. 选择删除。此时会显示确认对话框。
5. 确认要删除指定的磁带池，然后在确认框中键入单词 delete 并选择删除。

> **Warning**
>
> 使用此程序会永久删除选定的磁带池，且无法撤销。

删除磁带池后，它们会从磁带库中消失。

停用磁带网关

如果一个磁带网关出现故障且您想要将磁带从出现故障的网关恢复到另一个网关，则应停用此磁带网关。

要恢复磁带，您必须先停用出现故障的网关。停用磁带网关会锁定该网关中的虚拟磁带。也就是说，在停用网关之后，不会将您可能写入这些磁带的任何数据发送到 Amazon。您只能在网关不再连接到 Amazon时在 Storage Gateway 控制台上停用网关。如果网关已连接到 Amazon，则无法停用磁带网关。

您可以在数据恢复过程中停用磁带网关。有关恢复磁带的更多信息，请参阅 您需要从发生故障的磁带网关恢复虚拟磁带。

激活网关

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在导航窗格中，选择网关，然后选择失效的网关。
3. 选择网关的详细信息选项卡来显示停用网关消息。
4. 选择 Create recovery tapes。
5. 选择 Disable gateway。

理解磁带状态

每个磁带都有关联的状态，让您一目了然地了解磁带的运行状态。状态大多数时候会显示磁带运行正常，无需您采取任何行动。有些情况下，状态指示磁带有问题，可能需要您执行相关操作。您可以找到以下信息以帮助您决定何时需要采取行动。

主题

- 理解 VTL 中的磁带状态信息

- 确定存档中的磁带状态

理解 VTL 中的磁带状态信息

磁带的状态必须为 AVAILABLE (可用)，您才能对磁带进行读取或写入操作。下表列出并介绍可能存在的状态值。

状态	描述	磁带数据的存储位置
CREATING	正在创建虚拟磁带。由于正在创建磁带，所以无法将其载入磁带驱动器。	—
AVAILABLE	已创建虚拟磁带，并准备好将其载入磁带驱动器。	Amazon S3
IN TRANSIT TO VTS	虚拟磁带已弹出并将上传到存档。此时，您的磁带网关正在将数据上传到 Amazon。如果要上传的数据量较小，则可能不会显示此状态。上传完成后，状态将变为“ARCHIVING (正在存档)”。	Amazon S3
ARCHIVING	磁带网关正在将虚拟磁带转移到使用 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 的存档。此过程发生在数据上传到 Amazon 完成之后。	正在将数据从 Amazon S3 转移到 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive。
DELETING	正在删除虚拟磁带。	正在从 Amazon S3 中删除数据
DELETED	已成功删除虚拟磁带。	—
RETRIEVING	正在将虚拟磁带从存档取回到磁带网关。 **Note** 虚拟磁带只能取回到磁带网关。	正在将数据从 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 移动到 Amazon S3。
RETRIEVED	正在从存档中检索虚拟磁带。已取回的磁带具有写保护。	Amazon S3
RECOVERED	虚拟磁带已恢复并为只读。	Amazon S3

状态	描述	磁带数据的存储位置
	因任何原因而无法访问磁带网关时，可将与该磁带网关关联的虚拟磁带恢复到另一个磁带网关。必须先停用无法访问的磁带网关，然后才能恢复虚拟磁带。	
IRRECOVERABLE	无法从虚拟磁带读取或向其中写入。此状态指示磁带网关中存在错误。	Amazon S3

确定存档中的磁带状态

您可以使用以下过程来确定存档中的虚拟磁带状态。

确定虚拟磁带的状态

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在导航窗格中，选择 Tapes。
3. 在磁带库网格的 Status 列中，查看磁带的状态。

   磁带状态还会显示在每个虚拟磁带的 Details (详细信息) 选项卡中。

在下文中，您可以找到有关可能的状态值的说明。

状态	描述
ARCHIVED	虚拟磁带已弹出并将上传到存档。
RETRIEVING	正在从存档中检索虚拟磁带。 **Note** 虚拟磁带只能取回到磁带网关。
RETRIEVED	已从存档中检索虚拟磁带。已取回的磁带是只读的。

有关如何使用磁带和 VTL 设备的更多信息，请参阅 管理虚拟磁带库中的磁带。

将数据移至新网关

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

- 将您的数据转移到更好的主机平台或更新的 Amazon EC2 实例。
- 刷新服务器的底层硬件。

将数据移至新网关所遵循的步骤取决于您的网关类型。

> **Note**
>
> 数据只能在相同类型的的网关之间移动。

将虚拟磁带移至新的磁带网关

将虚拟磁带移至新的磁带网关

1. 使用备份应用程序将所有数据备份到虚拟磁带上。等待备份成功完成。
2. 使用备份应用程序来弹出磁带。磁带将存储到其中一个 Amazon S3 存储类中。弹出的磁带存档在 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 中，且为只读。

   在继续操作之前，请确认弹出的磁带已存档：

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

   b. 在导航窗格中，选择磁带库 > 磁带来查看您的磁带。默认情况下，此列表一次最多显示 1000 个磁带，但您执行的搜索会应用于所有磁带。您可以使用搜索栏来查找符合特定条件的磁带，也可以将列表缩减到少于 1000 个磁带。当您的列表包含 1000 个或更少磁带时，您可以按各种属性以升序或降序对磁带进行排序。

   c. 在列表的状态列中，查看磁带的状态。

      磁带状态还会显示在每个虚拟磁带的 Details (详细信息) 选项卡中。

      有关确定存档中磁带状态的更多信息，请参阅确定存档中的磁带状态。

3. 使用您的备份应用程序，确认在停止现有磁带网关之前，没有活动备份任务正在进入现有磁带网关。如果有任何处于活动状态的备份任务，请等待它们完成并弹出磁带（参见前面的步骤），然后再停止网关。
4. 按照以下步骤来停止现有磁带网关：

   a. 在导航窗格中，选择网关，然后选择要停止的旧磁带网关。网关处于 Running 状态。

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

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

   有关停止网关的更多信息，请参阅启动和停止磁带网关。
5. 创建新的磁带网关。有关详细说明，请参阅创建网关。
6. 按照以下步骤来创建新磁带：

   a. 在导航窗格中，选择 Gateways (网关) 选项卡。

   b. 选择创建磁带来打开创建磁带对话框。

   c. 对于 Gateway (网关)，选择网关。将为此网关创建磁带。

   d. 对于 Number of tapes (磁带数)，请选择要创建的磁带数量。有关磁带限制的更多信息，请参阅Amazon Storage Gateway 配额。

      此时您还可以设置自动磁带创建。有关更多信息，请参阅自动创建磁带。

   e. 对于 Capacity (容量)，请输入要创建的虚拟磁带的大小。磁带必须大于 100 GiB。有关容量限制的信息，请参阅 Amazon Storage Gateway 配额。

   f. 对于 Barcode prefix (条码前缀)，请输入要在虚拟磁带条码前面附加的前缀。

      > **Note**
      >
      > 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，可将其用于帮助识别虚拟磁带。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。

   g. 对于 Pool (池)，请选择 Glacier Pool (Glacier 池) 或 Deep Archive Pool (Deep Archive 池)。该池表示存储类，在备份软件弹出磁带时，将在其中存储磁带。

如果要在 S3 Glacier Flexible Retrieval 中存档磁带，请选择 Glacier 池。在备份软件弹出磁带时，将在 S3 Glacier Flexible Retrieval 中自动存档磁带。对于更多活动存档，可以使用 S3 Glacier Flexible Retrieval，这样您通常可以在 3-5 小时内取回磁带。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的用于存档对象的存储类。

如果要在 S3 Glacier Deep Archive 中存档磁带，请选择 Deep Archive 池。在备份软件弹出磁带时，将在 S3 Glacier Deep Archive 中自动存档磁带。您可以使用 S3 Glacier Deep Archive 实现长期数据留存和数字保留，每年访问一次或两次其中的数据。您通常可以在 12 小时内取回在 S3 Glacier Deep Archive 中存档的磁带。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的用于存档对象的存储类。

如果您在 S3 Glacier Flexible Retrieval 中存档数据，以后可以将其转移到 S3 Glacier Deep Archive。有关更多信息，请参阅 将磁带移至 S3 Glacier Deep Archive 存储类。

> **Note**
>
> 对于在 2019 年 3 月 27 日之前创建的磁带，在备份软件弹出磁带时，直接在 S3 Glacier Flexible Retrieval 中存档磁带。

h. （可选）对于 Tags (标签)，输入键和值以将标签添加到您的磁带。标签是帮助您管理、筛选和搜索磁带的区分大小写的键/值对。

i. 选择 Create tapes (创建磁带)。

7. 使用备份应用程序来启动备份任务，并将数据备份到新磁带。

8. （可选）如果磁带已存档且需要从中还原数据，请将其取回到新的磁带网关。磁带将处于只读模式。有关取回已存档磁带的更多信息，请参阅检索存档的磁带。

> **Note**
>
> 可能需要支付出站数据费用。

a. 在导航窗格中，选择磁带库 > 磁带来查看您的磁带。默认情况下，此列表一次最多显示 1000 个磁带，但您执行的搜索会应用于所有磁带。您可以使用搜索栏来查找符合特定条件的磁带，也可以将列表缩减到少于 1000 个磁带。当您的列表包含 1000 个或更少磁带时，您可以按各种属性以升序或降序对磁带进行排序。

b. 选择要取回的虚拟磁带。在操作中选择取回磁带。

> **Note**
>
> 要取回的虚拟磁带的状态必须为 ARCHIVED。

c. 在 Retrieve tape 对话框中，对于 Barcode，确认条码标识要检索的虚拟磁带。

d. 对于网关，选择要将存档的磁带取回到其中的磁带网关，然后选择取回磁带。

确认新的磁带网关运行正常后，可以删除旧的磁带网关。

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

9. 按照以下步骤来删除旧的磁带网关：

> **Warning**
>
> 删除网关后便无法恢复。

a. 在导航窗格中，选择网关，然后选择要删除的网关。

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

在出现的确认对话框中，确保列出的网关 ID 指定了要删除的旧磁带网关，在确认字段中输入 **`delete`**，然后选择删除。

c. 删除 VM。有关删除 VM 的更多信息，请参阅管理程序的文档。

监控 Storage Gateway

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

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

有关特定于监控磁带网关及其关联资源的信息，请参阅 Monitoring your Tape Gateway。

主题

- 了解网关指标
- 监控上传缓冲区
- 监控缓存存储
- 了解 CloudWatch 警报
- 为您的网关创建推荐的 CloudWatch 警报
- 为您的网关创建自定义 CloudWatch 警报
- 监控磁带网关

了解网关指标

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

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

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

指标	描述
AvailabilityNotifications	网关生成的与可用性相关的运行状况通知数。 将此指标与 Sum 统计数据结合使用可观察网关是否遇到了任何与可用性相关的事件。有关事件的详细信息，请查看您配置的 CloudWatch 日志组。 单位：数字
CacheHitPercent	缓存传送的应用程序读取率。样本在报告周期结束时采用。 单位：百分比
CachePercentDirty	网关缓存中尚未持久化的总体百分比。 Amazon样本在报告周期结束时采用。 将此指标与Sum统计数据结合使用。 理想情况下，该指标应保持在较低水平。 单位：百分比
CacheUsed	网关的缓存存储中正在使用的字节总数。样本在报告周期结束时采用。

指标	描述
	单位：字节
IoWaitPercent	网关等待本地磁盘响应的时间百分比。 单位：百分比
MemTotalBytes	为网关 VM 预配置的 RAM 量，以字节为单位。 单位：字节
MemUsedBytes	网关 VM 当前正在使用的 RAM 量，以字节为单位。 单位：字节
QueuedWrites	等待写入的字节数 Amazon，在报告周期结束时对网关中所有卷进行采样。这些字节保存在网关的工作存储空间中。 单位：字节
TotalCacheSize	以字节为单位的缓存总大小。样本在报告周期结束时采用。 单位：字节
UploadBufferPercentUsed	网关上传缓冲区的使用率。样本在报告周期结束时采用。 单位：百分比
UploadBufferUsed	网关的上传缓冲区正在使用的总字节数。样本在报告周期结束时采用。 单位：字节

指标	描述	
UserCpuPercent	网关处理所花 CPU 时间的百分比，在所有核心上平均计算。 单位：百分比	

Storage Gateway 指标的维度

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

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

监控上传缓冲区

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

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

> **Note**
>
> 在 Storage Gateway 中的缓存卷功能发布前，WorkingStoragePercentUsed、WorkingStorageUsed 和 WorkingStorageFree 指标仅适用于存储卷的上传缓冲区。现在，请使用等效上传缓冲区指标

UploadBufferPercentUsed、UploadBufferUsed 和 UploadBufferFree。这些指标适用于两种网关架构。

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

测量使用的上传缓冲区的百分比

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

得出的按时间排序的数据点集包含上传缓冲区的使用率。

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

如需为网关的上传缓冲区设置上阈值警报

1. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 选择 Create Alarm (创建警报) 可启动“Create Alarm (创建警报)”向导。
3. 为您的警报指定指标：
   a. 在 “创建警报” 向导的 “选择指标” 页面上 GatewayId，选择Amazon/StorageGateway:，GatewayName维度，然后找到要使用的网关。
   b. 选择 UploadBufferPercentUsed 指标。使用 Average 统计数据和 5 分钟的周期。
   c. 选择继续。

4. 定义警报名称、描述和阈值：

   a. 在“Create Alarm (创建警报)”向导的 Define Alarm (定义警报) 页面上，通过分别在 Name (名称) 和 Description (描述) 框中为您的警报提供名称和说明来标识警报。

   b. 定义警报阈值。

   c. 选择继续。

5. 针对该警报配置电子邮件操作：

   a. 在“创建警报”向导的配置操作页面上，为警报状态选择警报。

   b. 为主题选择选择或创建电子邮件。

      创建电子邮件主题意味着设置 Amazon SNS 主题。有关亚马逊 SNS 的更多信息，请参阅亚马逊用户指南中的设置亚马逊 SNS。 CloudWatch

   c. 对于 Topic (主题)，请为主题输入一个描述性名称。

   d. 选择 Add Action。

   e. 选择继续。

6. 检查警报设置，然后创建警报：

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

   b. 检查警报摘要后，选择 Save Alarm。

7. 确认您对警报主题的订阅：

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

   b. 单击电子邮件中的链接，确认您的订阅。

      将显示订阅确认。

监控缓存存储

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

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

关注项	如何测量
缓存总使用率	将 CachePercentUsed 和 TotalCacheSize 指标结合 Average 统计数据使用。例如，将 CachePercentUsed 与 Average 统计数据结合使用，以分析一段时间内的缓存使用率。 TotalCacheSize 指标仅在您向网关添加缓存时变化。
从缓存中提供的读取请求的百分比	将 CacheHitPercent 指标与 Average 统计数据结合使用。 通常，您希望 CacheHitPercent 保持较高。
缓存中肮脏的百分比，也就是说，它包含尚未上传到的内容 Amazon	将 CachePercentDirty 指标与 Average 统计数据结合使用。 一般而言，您希望 CachePercentDirty 保持较低。

测量网关及其所有卷的缓存废数据百分比

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

得出的按时间排序的数据点集包含 5 分钟以上的时间内的缓存废数据率。

测量卷的缓存废数据百分比

1. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 选择 StorageGateway：交易量指标维度，然后找到您要使用的交易量。
3. 选择 CachePercentDirty 指标。
4. 对于 Time Range，请选择一个值。
5. 选择 Average 统计数据。

6. 对于 Period，请选择值 5 分钟以匹配默认报告时间。

得出的按时间排序的数据点集包含 5 分钟以上的时间内的缓存废数据率。

了解 CloudWatch 警报

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

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

对于每个激活的网关，我们建议您创建以下 CloudWatch 警报：

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

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

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

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

下表描述了警报的状态。

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

为您的网关创建推荐的 CloudWatch 警报

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

为现有网关添加或更新推荐的 CloudWatch 警报

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

1. 在家中打开 Storage Gateway 控制台 https://console.aws.amazon.com/storagegateway//。
2. 在导航窗格中，选择 Gateways，然后选择要为其创建推荐 CloudWatch 警报的网关。

3. 在网关详细信息页面上，选择监控选项卡。
4. 在警报下，选择创建推荐警报。自动创建推荐的警报。

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

为您的网关创建自定义 CloudWatch 警报

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

在 Storage Gateway 控制台中创建 CloudWatch 警报

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

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

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

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

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

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

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

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

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

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

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

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

监控磁带网关

本节中的主题描述了有关如何监控磁带网关的过程和概念性信息。可以监控与磁带网关关联的虚拟磁带、缓存存储和上传缓冲区。您可以使用 Amazon Web Services Management Console 来查看您的磁带网关的指标。借助指标，您可以跟踪磁带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。

您可以使用 Amaz CloudWatch on Logs 来获取有关磁带网关和相关资源运行状况的信息。您可以使用日志来监控网关遇到的错误。此外，您还可以使用 Amazon CloudWatch 订阅筛选器实时自动处理日志信息。

Storage Gateway 免费提供 CloudWatch 指标。记录为期两周的 Storage Gateway 指标。通过使用这些指标，您可以访问历史信息并更好地了解您的磁带网关和虚拟磁带的性能。有关详细信息 CloudWatch，请参阅 Amazon CloudWatch 用户指南。

可以通过数据吞吐量、数据延迟和每秒操作数这三个衡量指标，来了解存储应用程序在使用磁带网关时的性能。当您使用正确的聚合统计数据时，可使用提供给您的 Storage Gateway 指标来衡量这些值。

主题

- 使用 CloudWatch 日志组获取磁带网关运行状况日志
- 使用亚马逊 CloudWatch指标
- 了解虚拟磁带指标
- 测量您的磁带网关和之间的性能 Amazon

使用 CloudWatch 日志组获取磁带网关运行状况日志

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

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

有关如何排查和修复此类错误的信息，请参阅对虚拟磁带问题进行故障排除。

以下过程说明如何在激活网关后配置 CloudWatch 日志组。

将 CloudWatch 日志组配置为与您的文件网关配合使用

1. 登录 Amazon Web Services Management Console 并在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在导航窗格中，选择 Gateways，然后选择要为其配置 CloudWatch 日志组的网关。
3. 在 “操作” 中，选择 “编辑网关信息”，或者在 “详细信息” 选项卡上的 “健康日志” 和 “未启用” 下，选择 “配置日志组” 以打开 CustomerGatewayName“编辑” 对话框。
4. 对于网关运行状况日志组，请选择以下选项之一：

- 如果您不想使用@@ 日志组监控网关，请禁用 CloudWatch 日志记录。
- 创建新的日志组以创建新的 CloudWatch 日志组。
- 使用现有日志组使用已存在的 CloudWatch 日志组。

  从现有日志组列表中选择一个日志组。

5. 选择 Save changes（保存更改）。
6. 要查看网关的运行状况日志，请执行以下操作：

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

以下是发送到的磁带网关事件消息的示例 CloudWatch。此示例显示了一条 `TapeStatusTransition` 消息。

```
{
"severity": "INFO",
"source": "FZTT16FCF5",
"type": "TapeStatusTransition",
"gateway": "sgw-C51DFEAC",
"timestamp": "1581553463831",
"newStatus": "RETRIEVED"
}
```

使用亚马逊 CloudWatch指标

您可以使用 Amazon Web Services Management Console 或 CloudWatch API 获取磁带网关的监控数据。控制台将根据来自 CloudWatch API 的原始数据显示一系列图表。该 CloudWatch API 也可以通过亚马逊 Amazon 软件开发套件 (SDKs) 或亚马逊 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：

- 要使用的指标维度。维度 是帮助您对某指标进行唯一标识的名称/值对。Storage Gateway 的维度为 `GatewayId` 和 `GatewayName`。在 CloudWatch 控制台中，您可以使用 `Gateway Metrics` 视图

来轻松选择特定于网关和特定于磁带的维度。有关尺寸的更多信息，请参阅 Amazon CloudWatch 用户指南中的尺寸。

- 指标名称，如 `ReadBytes`。

下表总结了可供您使用的 Storage Gateway 指标数据的类型。

Amazon CloudWatch 命名空间	维度	描述
`AWS/StorageGateway`	`GatewayId`，`GatewayName`	这些维度筛选描述磁带网关各个方面的指标数据。您可以通过指定 `GatewayId` 和 `GatewayName` 维度来标识要使用的磁带网关。 磁带网关的吞吐量和延迟数据基于磁带网关中的所有虚拟磁带。 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。您可以在下面所列的 CloudWatch 文档中找到一个有关某些最常见的指标任务的讨论：

- 查看可用指标
- 获取指标的数据
- 创建 CloudWatch 警报

了解虚拟磁带指标

您可以在下面找到有关包含虚拟磁带的 Storage Gateway 指标的信息。每个磁带均有与其关联的一组指标。

某些特定于磁带的指标可能与某些特定于网关的指标同名。这些指标代表同类度量，但其范围限于磁带，而非网关。在开始工作之前，请指定要使用网关指标还是磁带指标。在使用磁带指标时，请为要查看其指标的磁带指定磁带 ID。有关更多信息，请参阅 使用亚马逊 CloudWatch指标。

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

下表描述了可用来获取磁带相关信息的 Storage Gateway 指标。

指标	描述
CachePercentDirty	磁带在未传送到 Amazon的网关缓存的总体比例中的占比。样本在报告周期结束时采用。 使用网关的 CachePercentDirty 指标来查看未传送到 Amazon的网关缓存总体比例。有关更多信息，请参阅 了解网关指标。 单位：百分比
CloudTraffic	上传的字节数以及从云下载到磁带的字节数。 单位：字节
IoWaitPercent	磁带当前使用的已分配 IoWait 单元的百分比。 单位：百分比
HealthNotification	由磁带发送的运行状况通知的数量。 单位：计数
MemUsedBytes	磁带当前所使用的已分配内存的百分比。 单位：字节
MemTotalBytes	磁带当前所用的总内存的百分比。 单位：字节
ReadBytes	文件共享的报告周期内从本地应用程序读取的总字节数。

指标	描述
	将此指标与 Sum 统计数据结合使用可测量吞吐量，将其与 Samples 统计数据结合使用可测量 IOPS。 单位：字节
UserCpuPercent	磁带当前所使用的为用户分配的 CPU 计算单位的百分比。 单位：百分比
WriteBytes	报告周期内写入到场内应用程序的总字节数。 将此指标与 Sum 统计数据结合使用可测量吞吐量，将其与 Samples 统计数据结合使用可测量 IOPS。 单位：字节

测量您的磁带网关和之间的性能 Amazon

您可以通过数据吞吐量、数据延迟和每秒操作数这三个衡量指标来了解使用磁带网关的应用程序存储的性能状况。当您使用正确的聚合统计数据时，可使用提供给您的 Storage Gateway 指标来衡量这些值。

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

下表总结了用来测量磁带网关与 Amazon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	如何测量
延迟	将 ReadTime 和 WriteTime 指标结合 Average CloudWatch 统计数据使用。例如，Average 指标的 ReadTime 值为您提供采样周期内的每个操作的延迟时间。

关注项	如何测量
吞吐量到 Amazon	在Sum CloudWatch 统计数据中使用CloudBytesDownloaded 和CloudBytesUploaded 指标。例如，5 分钟采样周期内的CloudBytesDownloaded 指标Sum值除以 300 秒，得出从磁带网关到磁带网关的吞吐量， Amazon 以每秒字节为单位。
数据延迟到 Amazon	将 CloudDownloadLatency 指标与 Average 统计数据结合使用。例如，Average 指标的 CloudDownloadLatency 统计数据为您提供每操作延迟。

测量从磁带网关到的上传数据吞吐量 Amazon

1. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 请选择 Metrics（指标）选项卡。
3. 选择 StorageGateway：网关指标维度，然后找到要使用的磁带网关。
4. 选择 CloudBytesUploaded 指标。
5. 对于 Time Range，请选择一个值。
6. 选择 Sum 统计数据。
7. 对于 Period，请选择值 5 分钟或更长的时间。
8. 在得出的按时间排序的数据点集中，将各个数据点除以周期 (以秒为单位) 获得该样本周期当时的吞吐量。例如，如果给定数据点从磁带网关到的吞吐量 Amazon 为 555,544,576 字节，周期为 300 秒，则近似吞吐量为每秒 1.85 兆字节。

测量从磁带网关到的数据延迟 Amazon

1. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 请选择 Metrics（指标）选项卡。
3. 选择StorageGateway: GatewayMetrics维度，然后找到要使用的磁带网关。
4. 选择 CloudDownloadLatency 指标。
5. 对于 Time Range，请选择一个值。
6. 选择 Average 统计数据。
7. 对于 Period，请选择值 5 分钟以匹配默认报告时间。

得出的按时间排序的数据点集包含以秒为单位的延迟。

将磁带网关吞吐量的上限阈值警报设置为 Amazon

1. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 选择 Create Alarm (创建警报) 可启动“Create Alarm (创建警报)”向导。
3. 选择 StorageGateway：网关指标维度，然后找到要使用的磁带网关。
4. 选择 `CloudBytesUploaded` 指标。
5. 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，可定义 `CloudBytesUploaded` 指标在 60 分钟内大于 10MB 时的警报状态。
6. 针对该警报状态配置要采取的行动。例如，可获得向您发送的电子邮件通知。
7. 选择创建警报。

为读取数据设置上限阈值警报 Amazon

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

维护网关

维护磁带网关包括如下任务：为缓存存储和上传缓冲区空间调整本地磁盘大小和配置本地磁盘、管理更新和设置更新计划、管理带宽使用，以及在必要时关闭或删除网关和关联的资源等。这些任务是所有网关类型的常见任务。如果您尚未创建网关，请参阅创建网关。

主题

- 管理 Storage Gateway 的本地磁盘：了解如何评测磁盘大小要求、添加缓存容量以及管理分配给磁带网关用于缓冲和存储的本地磁盘。
- 管理磁带网关卷网关的带宽-了解如何将网关的上传吞吐量限制 Amazon 为以控制网关使用的网络带宽量。
- 管理网关更新：了解如何开启或关闭维护更新，以及修改磁带网关的维护时段计划。
- 关闭网关虚拟机：了解在需要关闭或重启网关虚拟机来进行维护时该怎么做，例如在为虚拟机监控程序应用补丁时。
- 删除网关和移除关联的资源-了解如何使用 Amazon Storage Gateway 控制台删除网关并清理相关资源，以免因继续使用这些资源而被收费。

管理 Storage Gateway 的本地磁盘

网关虚拟机 (VM) 使用您在本地分配的本地磁盘进行缓冲和存储。在 Amazon EC2 实例上创建的网关使用 Amazon EBS 卷作为本地磁盘。

主题

- 确定本地磁盘存储量
- 配置额外的上传缓冲区和缓存存储

确定本地磁盘存储量

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

- 磁带网关至少需要两个磁盘。一个用作缓存，另一个用作上传缓冲区。

下表为所部署的网关推荐了本地磁盘存储的大小。在设置网关后以及工作负载需求增大时，您可以添加更多本地存储。

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

> **Note**
>
> 预置磁盘时，强烈建议您不要将本地磁盘预置为使用相同物理存储资源（同一磁盘）的上传缓冲区和缓存存储空间。底层物理存储资源在中表示为数据存储 VMware。部署网关 VM 时，您可选择用来存储 VM 文件的数据存储。预配置本地磁盘 (例如，用作缓存存储空间或上传缓冲区) 时，您可以选择将虚拟磁盘存储在与 VM 相同的数据存储中，也可以选择将其存储在其他数据存储中。
>
> 如果您有多个数据存储，强烈建议为缓存存储空间选择一个数据存储，为上传缓冲区选择另一个数据存储。仅由一个底层物理磁盘支持的数据存储在用于同时支持缓存存储空间和上传缓冲区的某些情况下可能导致性能不佳。如果备份是性能较低的 RAID 配置（例如），也是如此。RAID1

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

确定要分配的上传缓冲区的大小

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

> **Note**
>
> 对于磁带网关，当上传缓冲区达到其容量后，您的应用程序可继续在存储卷中读写数据。但是，在 Storage Gateway 将本地存储的数据与存储在中的数据副本同步 Amazon 之前，磁带网关不会将您的任何卷数据写入其上传缓冲区，也不会将任何此类数据上传到。 Amazon此同步将在卷处于 BOOTSTRAPPING 状态时发生。

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

传入数据的速率

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

传出数据的速率

此速率指网络吞吐量，亦即您的网关将数据上传到 Amazon时可达到的速率。此速率取决于您的网络速度、使用率以及您是否激活了带宽限制。该速率应该针对压缩率进行调整。将数据上传到时 Amazon，网关会尽可能应用数据压缩。例如，如果您的应用程序数据为纯文本，您可以获得约 2:1 的有效压缩率。不过，如果您正在写入视频，网关可能无法实现任何数据压缩，并且可能需要更多的网关上传缓冲区。

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

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

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

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

Example

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

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

确定要分配的缓存存储的大小

您的网关使用其缓存存储来提供对最近访问数据的低延迟访问。缓存存储空间用作等待从上传缓冲区上传到 Amazon S3 的数据的本地持久存储。一般而言，将缓存存储空间的大小配置为上传缓冲区大小的 1.1 倍。有关如何估算缓存存储大小的更多信息，请参阅 确定要分配的上传缓冲区的大小。

您可以将此近似值用来初步为缓存存储空间预配置磁盘。然后，您可以使用 Amazon CloudWatch 运营指标监控缓存存储空间使用情况，并使用控制台根据需要配置更多存储空间。有关使用指标和设置警报的信息，请参阅 监控缓存存储。

配置额外的上传缓冲区和缓存存储

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

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

为网关配置额外的上传缓冲区或缓存存储

1. 在您的网关主机虚拟机管理程序或 Ama EC2 zon 实例上配置一个或多个新磁盘。有关如何在管理程序中预配置磁盘的信息，请参阅管理程序的文档。有关为亚马逊实例配置亚马逊 EBS 卷的信息，请参阅适用于 Linux EC2 实例的亚马逊弹性计算云用户指南中的亚马逊 EBS 卷。在以下步骤中，将此磁盘配置为上传缓冲区或缓存存储。

2. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
3. 在导航窗格中，选择网关。
4. 搜索您的网关并从列表中选择它。
5. 从操作菜单中选择配置存储。
6. 在配置存储部分，确定您预配置的磁盘。如果您未看到您的磁盘，请选择刷新图标来刷新列表。对于每个磁盘，从已分配给下拉菜单中选择上传缓冲区或缓存存储。
7. 选择保存更改来保存您的配置设置。

管理磁带网关卷网关的带宽

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

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

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

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

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

主题

- 使用 Storage Gateway 控制台更改带宽限制
- 使用 Storage Gateway 控制台实施基于计划的带宽限制
- 使用更新网关带宽速率限制 适用于 Java 的 Amazon SDK
- 使用更新网关带宽速率限制 适用于 .NET 的 Amazon SDK

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

使用 Storage Gateway 控制台更改带宽限制

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

如需使用控制台更改网关的带宽限制

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在左侧导航窗格中，选择网关，然后选择要管理的网关。
3. 对于操作，选择编辑带宽速率限制。
4. 在编辑速率限制对话框中，输入新的限制值，然后选择保存。您的更改将显示在网关的 Details 选项卡中。

使用 Storage Gateway 控制台实施基于计划的带宽限制

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

添加或修改网关带宽限制计划

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

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

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

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

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

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

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

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

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

完成更改后，选择保存。

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

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

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

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

使用更新网关带宽速率限制 适用于 Java 的 Amazon SDK

通过以编程方式更新带宽速率限制，您可以在一段时间内自动调整限制（例如，使用计划任务进行调整）。以下示例展示了如何使用 适用于 Java 的 Amazon 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，请参阅《适用于 Java 的 Amazon SDK 开发人员指南》中的入门。

Example : 使用更新网关带宽速率限制 适用于 Java 的 Amazon SDK

以下 Java 代码示例更新网关的带宽速率限制。要使用此示例代码，您必须提供服务端点、网关的 Amazon 资源名称 (ARN) 以及上传和下载限制。有关可以与 Storage Gateway 配合使用的 Amazon 服务终端节点列表，请参阅中的Amazon Storage Gateway 终端节点和配额Amazon Web Services 一般参考。

```
import java.io.IOException;

import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.PropertiesCredentials;
import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitRequest;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitResult;


public class UpdateBandwidthExample {

    public static AWSStorageGatewayClient sgClient;

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

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

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

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

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

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

        UpdateBandwidth(gatewayARN, uploadRate, downloadRate);
```

```
    }

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

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

使用更新网关带宽速率限制 适用于 .NET 的 Amazon SDK

通过以编程方式更新带宽速率限制，您可以在一段时间内自动调整限制（例如，使用计划任务进行调整）。以下示例展示了如何使用 适用于 .NET 的 Amazon 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，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的入门。

Example ：使用更新网关带宽速率限制 适用于 .NET 的 Amazon SDK

以下 C# 代码示例更新网关的带宽速率限制。要使用此示例代码，您必须提供服务端点、网关的 Amazon 资源名称 (ARN) 以及上传和下载限制。有关可以与 Storage Gateway 配合使用的 Amazon 服务终端节点列表，请参阅中的Amazon Storage Gateway 终端节点和配额Amazon Web Services 一般参考。

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

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

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

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

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

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

            UpdateBandwidth(gatewayARN, uploadRate, downloadRate);

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

        public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
 downloadRate)
        {
            try
            {
                UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
```

```
                    new UpdateBandwidthRateLimitRequest()
                    .WithGatewayARN(gatewayARN)
                    .WithAverageDownloadRateLimitInBitsPerSec(downloadRate)
                    .WithAverageUploadRateLimitInBitsPerSec(uploadRate);

                UpdateBandwidthRateLimitResponse updateBandwidthRateLimitResponse =
 sgClient.UpdateBandwidthRateLimit(updateBandwidthRateLimitRequest);
                String returnGatewayARN =
 updateBandwidthRateLimitResponse.UpdateBandwidthRateLimitResult.GatewayARN;
                Console.WriteLine("Updated the bandwidth rate limits of " +
 returnGatewayARN);
                Console.WriteLine("Upload bandwidth limit = " + uploadRate + " bits per
 second");
                Console.WriteLine("Download bandwidth limit = " + downloadRate + " bits
 per second");
            }
            catch (AmazonStorageGatewayException ex)
            {
                Console.WriteLine("Error updating gateway bandwith.\n" +
 ex.ToString());
            }
        }
    }
}
```

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

通过以编程方式更新带宽速率限制，您可以在一段时间内自动调整限制（例如，使用计划任务进行调整）。以下示例展示了如何使用 Amazon Tools for Windows PowerShell更新网关的带宽速率限制。要使用示例代码，您应该熟悉如何运行 PowerShell脚本。有关更多信息，请参阅《Amazon Tools for Windows PowerShell 用户指南》中的入门。

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

以下 PowerShell 脚本示例更新了网关的带宽速率限制。要使用此示例脚本，您必须提供网关的 Amazon 资源名称 (ARN) 以及上传和下载限制。

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

.NOTES
```

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


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

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

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

$limits =  Get-SGBandwidthRateLimit -GatewayARN $gatewayARN

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

管理网关更新

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

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

更新频率和预期行为

Amazon 根据需要更新云服务组件，而不会对已部署的网关造成中断。已部署的网关设备每月都会收到维护更新。每月维护更新可能包括操作系统和软件升级、用于解决稳定性、性能和安全性的修复程序以及对新功能的访问。所有更新均为累积更新，应用后会将网关升级到当前版本。有关每个更新中包含的具体更改的信息，请参阅 Release Notes for Tape Gateway Appliance Software。

每月维护更新可能会导致服务短暂中断。网关的 VM 主机在更新期间无需重启，但在网关设备更新和重新启动期间，网关将在短时间内不可用。您可以通过增大 iSCSI 启动程序的超时值将由网关重新启动导致的应用程序的任何中断几率降到最低。有关针对 Windows 和 Linux 增大 iSCSI 启动程序超时值的更多信息，请参阅 自定义您的 Windows iSCSI 设置 和 自定义您的 Linux iSCSI 设置。

部署并激活网关后，将设置默认的每周维护时段计划。可以随时修改维护时段计划。也可以关闭每月维护更新，但我们建议将其保持为开启状态。

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

在将任何更新应用于您的网关之前， Amazon 会在 Storage Gateway 控制台上发送一条消息通知您，然后您的 Amazon Health Dashboard。有关更多信息，请参阅 Amazon Health Dashboard。要修改发送软件更新通知的电子邮件地址，请参阅《账户管理参考指南》中的 “更新 Amazon Amazon 账户的备用联系人”。

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

开启或关闭维护更新

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

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

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

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

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

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

修改网关维护时段计划

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

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

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

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

   a. 对于计划，选择每周或每月以设置维护时段节奏。

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

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

      > **Note**
      >
      > 可以为月份中的某一天设置的最大值为 28。无法将维护计划设置为从日期 29 至日期 31 开始。

如果您在配置此设置时收到错误，则可能意味着网关软件已过期。考虑先手动更新网关，然后尝试再次配置维护时段计划。

5. 完成后，选择保存更改。

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

手动应用更新

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

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

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

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

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

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

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

关闭网关虚拟机

您可能需要关闭或重新启动虚拟机进行维护，例如在向虚拟机管理程序应用补丁时。关闭虚拟机之前，您必须先停止网关。尽管本节的内容重点说明了使用 Storage Gateway 管理控制台启动和停止网关，但您也可以使用 VM 本地控制台或 Storage Gateway API 启动和停止网关。当您开启虚拟机时，请记住重新启动网关。

Important

如果您停止并启动使用临时存储的 Amazon EC2 网关，则该网关将永久处于离线状态。发生这种情况的原因是替换了物理存储磁盘。此问题没有解决方法。唯一的解决方法是删除网关并在新 EC2 实例上激活一个新网关。

Note

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

- 网关 VM 本地控制台 - 请参阅登录到磁带网关本地控制台。
- Storage Gateway API — 参见 ShutdownGateway

启动和停止磁带网关

停止磁带网关

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

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

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

启动磁带网关

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

删除网关和移除关联的资源

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

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

> **Note**
>
> 删除磁带网关时，当前处于 AVAILABLE 状态的所有磁带也会被删除，并且这些磁带上的任何数据都将丢失。如果您想要保留您要删除的网关正在使用的磁带中的数据，则必须在删除网关之前对磁带进行归档。有关更多信息，请参阅存档虚拟磁带。

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

主题

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

使用 Storage Gateway 控制台删除网关

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

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

删除网关

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

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

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

> **Important**
>
> 删除网关后，您无需再支付软件费用，但虚拟磁带、Amazon Elastic Block Store (Amazon EBS) 快照和亚马逊 EC2 实例等资源仍然存在。您将继续为这些资源付费。您可以通过取消亚马逊订阅来选择移除亚马逊 EC2 实例和亚马逊 EBS 快照。 EC2 如果您想保留您的亚马逊 EC2 订阅，则可以使用亚马逊 EC2控制台删除您的亚马逊 EBS 快照。

从本地部署的网关中删除资源

您可按照下面的说明从本地部署的网关中移除资源。

从部署在 VM 上的磁带网关中移除资源

当您删除网关虚拟磁带库 (VTL) 时，请在删除网关前后执行额外的清除步骤。这些额外的步骤可帮助您移除不需要的资源，使您不用继续为它们付费。

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

> **Important**
>
> 在删除磁带网关前，您必须取消所有磁带取回操作并弹出所有已取回的磁带。
> 在删除磁带网关之后，您必须移除与磁带网关相关的所有不需要的资源，以避免这些资源产生费用。

在删除磁带网关时，您可能会遇到以下两种情况之一。

- 磁带网关已连接到 Amazon — 如果磁带网关已连接 Amazon 并且您删除了该网关，则与该网关关联的 iSCSI 目标（即虚拟磁带机和介质更换器）将不再可用。
- 磁带网关未连接到 Amazon — 如果磁带网关未连接到 Amazon，例如，如果底层虚拟机已关闭或网络已关闭，则无法删除该网关。如果您尝试这样做，则在备份并运行环境后，您可能拥有包含可用 iSCSI 目标并在本地运行的磁带网关。但是，不会将任何磁带网关数据上传到或从中下载 Amazon。

如果要删除的磁带网关无法正常工作，则必须先停用该网关，然后才能将其删除，如下所述：

- 要从库中删除处于 RETRIEVED 状态的磁带，请使用备份软件弹出磁带。有关说明，请参阅存档磁带。

停用磁带网关并删除磁带后，您可以删除磁带网关。有关如何删除网关的说明，请参阅使用 Storage Gateway 控制台删除网关。

如果已对磁带进行存档，则会保留这些磁带，并且您需要继续为存储付费，直至您删除它们。有关如何从存档中删除磁带的说明，请参阅从磁带网关中删除虚拟磁带。

> **Important**
>
> 对于存档中的虚拟磁带，您至少需要支付 90 天的存储费用。如果您取回的虚拟磁带在存档中存储的时间不到 90 天，仍需支付 90 天的存储费用。

从部署在 Amazon EC2 实例上的网关中移除资源

如果您想删除在 Amazon EC2 实例上部署的网关，我们建议您清理用于该网关的 Amazon 资源，特别是亚马逊 EC2 实例、所有 Amazon EBS 卷以及磁带（如果您部署了磁带网关）。完成此操作有助于避免产生非故意的使用费用。

从部署在 Amazon 上的磁带网关中移除资源 EC2

如果您部署了磁带网关，我们建议您执行以下操作来删除网关并清除其资源：

1. 删除所有已取回到磁带网关的虚拟磁带。有关更多信息，请参阅 从磁带网关中删除虚拟磁带。
2. 从磁带库中删除所有虚拟磁带。有关更多信息，请参阅 从磁带网关中删除虚拟磁带。
3. 删除磁带网关。有关更多信息，请参阅 使用 Storage Gateway 控制台删除网关。
4. 终止所有亚马逊 EC2 实例，并删除所有亚马逊 EBS 卷。有关更多信息，请参阅 Amazon EC2 用户指南中的清理实例和卷。
5. 删除所有存档的虚拟磁带。有关更多信息，请参阅 从磁带网关中删除虚拟磁带。

> **Important**
>
> 对于存档中的虚拟磁带，您至少需要支付 90 天的存储费用。如果您取回的虚拟磁带在存档中存储的时间不到 90 天，仍需支付 90 天的存储费用。

使用本地控制台执行维护任务

本节包含以下主题，这些主题提供有关如何使用网关设备本地控制台来执行维护任务的信息。本地控制台直接在托管网关设备的虚拟化主机平台上运行。对于本地网关，您可以 VMware通过 Hyper-V 或 Linux KVM 虚拟化主机访问本地控制台。对于 Amazon EC2 网关，您可以使用 SSH 连接到亚马逊 EC2实例来访问控制台。大多数任务对不同的主机平台来说具有共性，但也存在一些差异。

主题

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

访问网关本地控制台

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

主题

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

使用 Linux KVM 访问网关本地控制台

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

使用 KVM 访问网关的本地控制台

1. 使用以下命令列出 KVM 中当前可用的内容。 VMs

```
# virsh list
```

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

2. 使用以下命令访问本地控制台。

```
# virsh console Id
```

*Id*替换为您在上一步中记下的虚拟机的 ID。

Amazon 设备网关本地控制台会提示您登录以更改网络配置和其他设置。

3. 输入您的用户名和密码以登录网关本地控制台。有关更多信息，请参阅 Logging in to the Tape Gateway local console。

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

使用访问网关本地控制台 VMware ESXi

要使用访问网关的本地控制台 VMware ESXi

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

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

3. 在应用程序窗口右侧的主信息面板中选择控制台选项卡。

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

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

4. 输入您的用户名和密码以登录网关本地控制台。有关更多信息，请参阅 Logging in to the Tape Gateway local console。

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

使用 Microsoft Hyper-V 访问网关本地控制台

访问网关的本地控制台 (Microsoft Hyper-V)

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

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

3. 从操作面板中选择连接。

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

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

4. 输入您的用户名和密码以登录网关本地控制台。有关更多信息，请参阅 Logging in to the Tape Gateway local console。

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

在 虚拟机本地控制台上执行任务

对于您在本地部署的磁带网关，可以使用从虚拟机主机平台访问的网关本地控制台来执行以下维护任务。这些任务是微软 Hyper-V 和基于 Linux 内核的虚拟机 (KVM) 虚拟机管理程序的常见任务。VMware

主题

- 登录到磁带网关本地控制台：了解如何登录到网关本地控制台，可以在此控制台中配置网关网络设置和更改默认密码。
- 为本地网关配置 SOCKS5 代理-了解如何将 Storage Gateway 配置为通过 Socket Secure 版本 5 (SOCKS5) 代理服务器路由所有 Amazon 端点流量。
- 配置网关网络：了解如何将网关配置为使用 DHCP 或分配静态 IP 地址。
- 测试网关到互联网的连接：了解如何使用网关本地控制台来测试网关和互联网之间的连接。
- 在本地控制台中为本地网关运行存储网关命令-了解如何运行本地控制台命令，这些命令允许您执行其他任务，例如保存路由表、连接路由表等。 Amazon Web Services 支持
- 查看您的网关系统资源状态：了解如何检查可用于网关设备的虚拟 CPU 内核、根卷大小和 RAM。

登录到磁带网关本地控制台

在 VM 做好登录准备时，登录屏幕将显示。如果这是您首次登录本地控制台，请使用默认登录凭证来登录。您可以使用这些默认登录凭证来访问一些菜单，这些菜单可用来配置网关网络设置和从本地控制台更改密码。Storage Gateway 允许您从 Amazon Storage Gateway 控制台设置自己的密码，而不必从本地控制台更改密码。您无需知道默认密码就可以设置新密码。有关更多信息，请参阅 从 Storage Gateway 控制台设置本地控制台密码。

登录网关的本地控制台

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

  否则，请使用您的凭证登录。

  > **Note**
  >
  > 我们建议更改默认密码，方法是在 Amazon 设备激活 - 配置主菜单中为网关控制台输入相应的数字，然后运行 `passwd` 命令。有关如何运行该命令的信息，请参阅在本地控制台中

为本地网关运行存储网关命令。您也可以通过 Amazon Storage Gateway 控制台设置自己的密码。有关更多信息，请参阅 从 Storage Gateway 控制台设置本地控制台密码。

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

从 Storage Gateway 控制台设置本地控制台密码

当您首次登录本地控制台时，使用默认凭证（用户名为 `admin`，密码为 `password`）登录 VM。我们建议您总是在创建新网关后立即设置新密码。如果愿意，您可以从 Amazon Storage Gateway 控制台而不是本地控制台设置此密码。您无需知道默认密码就可以设置新密码。

在 Storage Gateway 控制台上设置本地控制台密码

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在导航栏中，选择 Gateways，然后选择要为其设置新密码的网关。
3. 对于 Actions (操作)，选择 Set Local Console Password (设置本地控制台密码)。
4. 在 Set Local Console Password 对话框中，键入新密码，确认该密码，然后选择 Save。您的新密码会替换默认密码。Storage Gateway 不会保存密码，而是将其安全地传输到 VM。

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

为本地网关配置 SOCKS5 代理

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

> **Note**
>
> 唯一支持的代理配置是 SOCKS5。

如果网关必须使用代理服务器与 Internet 进行通信，则需要为网关配置 SOCKS 代理设置。为此，您可以为运行代理的主机指定 IP 地址和端口号。完成此操作后，Storage Gateway 通过您的代理服务器路由所有流量。有关网关的网络要求的信息，请参阅网络和防火墙要求。

以下过程显示如何为卷网关和磁带网关配置 SOCKS 代理。

为卷和磁带网关配置 SOCKS5 代理

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

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

4. 重新启动 VM 来应用 HTTP 配置。

配置网关网络

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

如需将您的网关配置为使用静态 IP 地址。

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

执行此任务	请执行此操作
描述网络适配器	输入相应的数字来选择描述适配器。 此时会显示适配器名称的列表，并且系统会提示您输入适配器名称，例如 **`eth0`**。如果您指定的适配器正在使用中，有关该适配器的下列信息就会显示： • 媒体访问控制 (MAC) 地址 • IP 地址 • 网络掩码 • 网关 IP 地址 • DHCP 激活状态 配置静态 IP 地址或设置网关的默认适配器时，使用此处列出的适配器名称。

执行此任务	请执行此操作
配置 DHCP	输入相应的数字来选择配置 DHCP。 系统将提示您将网络接口配置为使用 DHCP。

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

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

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

测试网关到互联网的连接

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

测试网关到 Internet 的连接

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

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

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

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

在本地控制台中为本地网关运行存储网关命令

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

运行配置或诊断命令

1. 登录到网关的本地控制台：
   - 有关登录 VMware ESXi 本地控制台的更多信息，请参阅使用访问网关本地控制台 VMware ESXi。
   - 有关登录到 Microsoft Hyper-V 本地控制台的更多信息，请参阅使用 Microsoft Hyper-V 访问网关本地控制台。
   - 有关登录到 KVM 本地控制台的更多信息，请参阅使用 Linux KVM 访问网关本地控制台。
2. 在 Amazon 设备激活 - 配置主菜单中，输入相应的数字来选择网关控制台。
3. 在网关控制台命令提示符处输入 **h**。

   控制台会显示可用命令菜单，其中列出了可用的命令：

命令	函数
dig	从 dig 收集输出来进行 DNS 故障排除。
exit	返回到“配置”菜单。
h	显示可用的命令列表。
ifconfig	查看或配置网络接口。

命令	函数
	Note 我们建议使用 Storage Gateway 控制台或专用的本地控制台菜单选项来配置网络或 IP 设置。有关说明，请参阅配置网关网络。
ip	显示/操作路由、设备和隧道。 **Note** 我们建议使用 Storage Gateway 控制台或专用的本地控制台菜单选项来配置网络或 IP 设置。有关说明，请参阅配置网关网络。
iptables	用于 IPv4 数据包过滤和 NAT 的管理工具。
ncport	测试与网络上特定 TCP 端口的连接。
nping	从 nping 收集输出来进行网络故障排除。
open-support-channel	Connect to S Amazon upport。
passwd	更新身份验证令牌。
save-iptables	保留 IP 表。
save-routing-table	保存新添加的路由表条目。

命令	函数
sslcheck	返回证书颁发者的输出 **Note** Storage Gateway 使用证书颁发者验证，而不支持 ssl 检查。如果此命令返回 aws-appliance@amazon.com 以外的颁发者，则很可能是应用程序在执行 ssl 检查。在这种情况下，我们建议绕过 Storage Gateway 设备的 ssl 检查。
tcptraceroute	收集有关流向目的地的 TCP 流量的 traceroute 输出。

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

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

查看您的网关系统资源状态

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

查看系统资源检查的状态

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

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

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

控制台还会在资源检查菜单选项旁边显示错误和警告的数量。

在 Amazon EC2 本地控制台上执行任务

某些 Storage Gateway 维护任务要求您登录已在 Amazon EC2 实例上部署的网关的本地控制台。您可以使用安全外壳 (SSH) 客户端访问您的 Amazon EC2 实例上的网关本地控制台。本节中的主题描述了如何登录网关本地控制台并执行维护任务。

主题

- 登录您的 Amazon EC2 Gateway 本地控制台-了解如何使用安全外壳 (SSH) 客户端连接和登录 Amazon EC2 实例的网关本地控制台。
- EC2 通过 HTTP 代理路由部署在上的网关-了解如何配置 Storage Gateway，使其通过 Sock Amazon et Secure 版本 5 (SOCKS5) 代理服务器将所有端点流量路由到您的 Amazon EC2 网关实例。
- 测试网关网络连接：了解如何使用网关本地控制台来测试网关与各种网络资源之间的网络连接。
- 查看您的网关系统资源状态：了解如何使用网关本地控制台来检查可用于网关设备的虚拟 CPU 内核、根卷大小和 RAM。
- 在本地控制台上运行 Storage Gateway 命令-了解如何运行本地控制台命令，这些命令允许您执行其他任务，例如保存路由表、连接路由表等。 Amazon Web Services 支持

登录您的 Amazon EC2 Gateway 本地控制台

您可以使用安全外壳 (SSH) 客户端连接到您的 Amazon EC2 实例。有关详细信息，请参阅 Amazon EC2 用户指南中的 Connect to Your Instance。要以这种方式连接，您需要在启动实例时指定的 SSH 密钥对。有关亚马逊 EC2 密钥对的信息，请参阅亚马逊 EC2 用户指南中的亚马逊 EC2 密钥对。

登录网关本地控制台

1. 登录到本地控制台。如果您是从 Windows 计算机连接到您的 EC2 实例，请以管理员身份登录。
2. 登录后，您将看到 Amazon Storage Gateway - 配置主菜单，您可以通过这个菜单执行各种任务。

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

要关闭网关，请输入 **0**。

要退出配置会话，请输入 **x**。

EC2 通过 HTTP 代理路由部署在上的网关

Storage Gateway 支持在部署在亚马逊上的网关 EC2 和之间配置套接字安全版本 5 (SOCKS5) 代理 Amazon。

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

通过本地代理服务器路由网关 Internet 流量

1. 登录到网关的本地控制台。有关说明，请参阅 登录您的 Amazon EC2 Gateway 本地控制台。
2. 在 Amazon 设备激活 - 配置主菜单中，输入相应的数字来选择配置 HTTP 代理。
3. 在 Amazon 设备激活 HTTP 代理配置菜单中，输入与要执行的任务对应的数字：

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

测试网关网络连接

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

测试网关的连接

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

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

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

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

查看您的网关系统资源状态

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

查看系统资源检查的状态

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

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

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

   控制台还会在资源检查菜单选项旁边显示错误和警告的数量。

在本地控制台上运行 Storage Gateway 命令

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

运行配置或诊断命令

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

   控制台会显示可用命令菜单，其中列出了可用的命令：

命令	函数
dig	从 dig 收集输出来进行 DNS 故障排除。

命令	函数
exit	返回到“配置”菜单。
h	显示可用的命令列表。
ifconfig	查看或配置网络接口。 **Note** 我们建议使用 Storage Gateway 控制台或专用的本地控制台菜单选项来配置网络或 IP 设置。
ip	显示/操作路由、设备和隧道。 **Note** 我们建议使用 Storage Gateway 控制台或专用的本地控制台菜单选项来配置网络或 IP 设置。
iptables	用于 IPv4 数据包过滤和 NAT 的管理工具。
ncport	测试与网络上特定 TCP 端口的连接。
nping	从 nping 收集输出来进行网络故障排除。
open-support-channel	Connect to S Amazon upport。
save-iptables	保留 IP 表。
save-routing-table	保存新添加的路由表条目。
sslcheck	检查 SSL 有效性以排除网络故障。
tcptraceroute	收集有关流向目的地的 TCP 流量的 traceroute 输出。

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

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

磁带网关的性能和优化

本节介绍了 Storage Gateway 性能。

主题

- 磁带网关的性能指导
- 优化网关性能

磁带网关的性能指导

在本部分中，您可以找到为磁带网关 VM 预配置硬件的配置指南。表中列出的 Amazon EC2 实例大小和类型仅为示例，仅供参考。

配置	写入吞吐量 Gbps	从缓存读取的吞吐量 Gbps	从 Amazon Web Services 云读取的吞吐量 Gbps
主机平台：亚马逊 EC2 实例 — c5.4xlarge CPU：16 个 vCPU | RAM：32 GB 根磁盘：80 GB，io1 SSD，4000 IOPS 缓存磁盘：条带 RAID（2 x 500 GB，io1 EBS 固态硬盘，25000）IOPs 上传缓冲磁盘：450 GB、io1 固态硬盘、2000 IOPs 到云的网络带宽：10 Gbps	2.3	4.0	2.2
主机平台：存储网关硬件设备 缓存磁盘：2.5 TB	2.3	8.8	3.8

配置	写入吞吐量 Gbps	从缓存读取的吞吐量 Gbps	从 Amazon Web Services 云读取的吞吐量 Gbps
上传缓冲区磁盘：2 TB 到云的网络带宽：10 Gbps			
主机平台：亚马逊 EC2instance — c5d.9xlarge CPU：36 个 vCPU | RAM：72 GB 根磁盘：80 GB，io1 SSD，4000 IOPS 缓存磁盘：900 GB NVMe 磁盘 上传缓冲区磁盘：900 GB NVMe 磁盘 到云的网络带宽：10 Gbps	5.2	11.6	5.2
主机平台：亚马逊 EC2instance — c5d.metal CPU：96 个 vCPU | RAM：192 GB 根磁盘：80 GB，io1 SSD，4000 IOPS 缓存磁盘：条带化 RAID（2 x 900 GB NVMe 磁盘） 上传缓冲区磁盘：900 GB NVMe 磁盘 到云的网络带宽：10 Gbps	5.2	11.6	7.2

> **Note**
>
> 此性能是通过同时使用 1 MB 块大小和十个磁带驱动器来实现的。
> 上表中的 EC2 配置仅用于代表您在拥有类似资源的物理服务器上可能获得的性能。例如，使用条带化 RAID 的 EC2 配置是通过一种特殊机制完成的，而我们的网关通常不支持这种机制 EC2。要实现类似的性能，您应该改用连接到运行网关的本地服务器的硬件 RAID 控制器。
> 您的性能可能因主机平台配置和网络带宽而异。

要提高磁带网关的读写吞吐量性能，请参阅优化 iSCSI 设置、让磁带驱动器使用更大的数据块和在备份软件中优化虚拟磁带驱动器的性能。

优化网关性能

推荐的网关服务器配置

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

- 至少 64 个专用的物理 CPU 核心
- 对于磁带网关，您的硬件应使用以下数量的 RAM：
  - 对于缓存大小不超过 16 TiB 的网关，至少预留 16 GiB 的 RAM
  - 对于缓存大小为 16 TiB 至 32 TiB 的网关，至少预留 32 GiB 的 RAM
  - 对于缓存大小为 32 TiB 至 64 TiB 的网关，至少预留 48 GiB 的 RAM

> **Note**
>
> 要获得最佳网关性能，您必须预配置至少 32 GiB 的 RAM。

- 磁盘 1，用作网关缓存，如下所示：
  - 条带 RAID（独立磁盘冗余阵列）包括 NVMe SSDs。
- 磁盘 2，用作网关上传缓冲区，如下所示：
  - 条带 RAID 包括 NVMe SSDs。
- 磁盘 3，用作网关上传缓冲区，如下所示：
  - 条带 RAID 包括 NVMe SSDs。
- 在虚拟机网络 1 上配置网络适配器 1：

  - 使用虚拟机网络 1 并添加 VMXnet3 (10 Gbps) 以用于摄取。
- 在虚拟机网络 2 上配置网络适配器 2：
  - 使用虚拟机网络 2 并添加 VMXnet3 (10 Gbps) 以用于连接。 Amazon

在网关中添加资源

以下瓶颈可能会使磁带网关卷网关 Amazon 云的带宽）以下：

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

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

您可以使用以下一种或多种方法在网关中添加资源以优化网关性能。

使用更高性能的磁盘

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

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

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

- 使用直接连接的高性能磁盘

  要优化网关性能，您可以添加高性能磁盘，例如固态硬盘 (SSDs) 和控制器。 NVMe 您还可以直接从存储区域网络 (SAN) 而不是 Microsoft Hyper-V NTFS 将虚拟磁盘连接到 VM。更高的磁盘性能通常可带来更大的吞吐量和更多的每秒输入/输出操作 (IOPS) 次数。

要衡量吞吐量，请将ReadBytes和WriteBytes指标与 Samples Amazon CloudWatch 统计数据结合使用。例如，5 分钟的采样周期内的 Samples 指标的 ReadBytes 统计数据除以 300 秒可以得出 IOPS。一般来说，查看网关的这些指标时，应注意低吞吐量和低 IOPS 趋势，以便显示与磁盘相关的瓶颈。有关网关指标的更多信息，请参阅测量您的磁带网关和之间的性能 Amazon。

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

添加更多上传缓冲区磁盘

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

使用独立物理磁盘支持网关虚拟磁盘

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

如果您有多个数据存储，则强烈建议为要创建的每个类型的本地存储选择一个数据存储。仅由一个底层物理磁盘支持的数据存储可能会导致性能下降。例如，在使用此类磁盘同时支持网关设置中的缓存存储和上传缓冲区时。同样，采用性能不太高的 RAID 配置（如 RAID 1 或 RAID 6）的数据存储可能会导致性能下降。

添加 CPU 资源到您的网关主机

网关主机服务器的最低要求是四个虚拟服务器。要优化网关性能，请确认分配给网关 VM 的每个虚拟处理器均采用一个专用的 CPU 内核。此外，请确认您没有超额订阅主机 CPUs 服务器的。

CPUs 向网关主机服务器添加其他内容时，可以提高网关的处理能力。通过执行该操作，您的网关可以并行处理将应用程序中的数据存储到本地存储以及将该数据上传到 Amazon S3 的过程。其他 CPUs 功能还有助于确保您的网关在与其他主机共享主机时获得足够的 CPU 资源 VMs。提供足够的 CPU 资源通常能取得增加吞吐量的效果。

增加网关和 Amazon 云之间的带宽

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

往返网络带宽 Amazon 定义了持续工作负载期间磁带网关的理论最大平均性能。

- 在长时间间隔内，向磁带网关写入数据的平均速率不会超过向 Amazon上传数据的上传带宽。
- 长时间间隔内从磁带网关读取数据的平均速率不会超过您的下载带宽 Amazon。

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

优化 iSCSI 设置

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

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

让磁带驱动器使用更大的数据块

对于磁带网关，磁带驱动器的默认块大小为 64 KB。但是，您可以将块大小增加到最多 1 MB 以提高 I/O 性能。

您选择的块大小取决于备份软件支持的最大块大小。我们建议您在备份软件中将磁带驱动器的块大小尽可能设置为较大的值。但是，该块大小不能大于网关支持的最大大小 (1 MB)。

磁带网关协商虚拟磁带驱动器的块大小，以便自动与备份软件中设置的值相匹配。在备份软件中增加块大小时，我们建议您还要检查这些设置，以确保主机启动程序支持新的块大小。有关更多信息，请参阅备份软件的文档。有关特定网关性能指南的更多信息，请参阅磁带网关的性能和优化。

在备份软件中优化虚拟磁带驱动器的性能

您的备份软件可以同时备份磁带网关上的最多 10 个虚拟磁带驱动器上的数据。我们建议您在备份软件中配置备份任务，从而在磁带网关上同时使用至少 4 个虚拟磁带驱动器。在备份软件同时将数据备份到多个虚拟磁带时，您可以实现更高的写入吞吐量。

通常，您可以通过同时对更多虚拟磁带进行操作（读取或写入）来实现更高的最大吞吐量。通过使用更多的磁带驱动器，可以让您的网关同时处理更多请求，从而有可能提高性能。

向应用程序环境添加资源

提高应用程序服务器和网关之间的带宽

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

- 升级网络电缆，使启动程序和网关之间具有更高的带宽。
- 同时使用尽可能多的磁带驱动器。iSCSI 不支持为同一个目标排队多个请求，这意味着您使用的磁带驱动器越多，网关可以同时处理的请求就越多。这将使您能够更充分地利用网关和启动程序之间的带宽，从而提高网关的表观吞吐量。

要优化网关性能，请确保应用程序和网关之间的网络带宽可满足您的应用程序需求。您可以使用网关的 `ReadBytes` 和 `WriteBytes` 指标来测量总数据吞吐量。)。有关这些指标的更多信息，请参阅测量您的磁带网关和之间的性能 Amazon。

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

向应用程序环境添加 CPU 资源

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

Amazon Storage Gateway 中的安全

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

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

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

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

主题

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

Amazon Storage Gateway 中的数据保护

Amazon 分适用于 Amazon Storage Gateway 中的数据保护。如本模型所述 Amazon ，负责保护运行所有内容的全球基础架构 Amazon Web Services 云。您负责维护对托管在此基础结构上的内容的控制。您还负责您所使用的 Amazon Web Services 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。

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

- 对每个账户使用多重身份验证（MFA）。
- 使用 SSL/TLS 与资源通信。 Amazon 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 Amazon CloudTrail。有关使用 CloudTrail 跟踪捕获 Amazon 活动的信息，请参阅《Amazon CloudTrail 用户指南》中的使用跟 CloudTrail 踪。
- 使用 Amazon 加密解决方案以及其中的所有默认安全控件 Amazon Web Services 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 Amazon 通过命令行界面或 API 进行访问时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-3 版》。

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

使用数据加密 Amazon KMS

Storage Gateway 使用 Layer Security（SSL/TLS (Secure Socket Layers/Transport层安全）来加密在网关设备和 Amazon 存储设备之间传输的数据。默认情况下，Storage Gateway 使用 Amazon S3 托管的加密密钥 (SSE-S3) 对其存储在 Amazon S3 中的所有数据进行服务器端加密。您可以选择使用 Storage Gateway API 将网关配置为使用服务器端加密和 Amazon Key Management Service (SSE-KMS) 密钥对存储在云中的数据进行加密。

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

加密文件共享

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

加密卷

对于缓存和存储的卷，您可以使用 Storage Gateway API 将网关配置为使用 Amazon KMS托管密钥加密存储在云中的卷数据。您可以将其中一个托管密钥指定为 KMS 密钥。创建卷后，即无法更改用于加密卷的密钥。有关使用 Storage Gateway API 加密写入缓存或存储卷的数据的信息，请参阅 Amazon Storage Gateway API 参考CreateStorediSCSIVolume中的CreateCachediSCSIVolume或。

加密磁带

对于虚拟磁带，您可以使用 Storage Gateway API 将网关配置为使用 Amazon KMS托管密钥加密存储在云中的磁带数据。您可以将其中一个托管密钥指定为 KMS 密钥。创建磁带后，即无法更改用于加密磁带数据的密钥。有关使用 Storage Gateway API 加密写入虚拟磁带的数据的信息，请参阅 Amazon Storage Gateway API 参考CreateTapes中的。

使用 Amazon KMS 加密数据时，请记住以下几点：

- 您的数据在云中进行静态加密。也就是说，在 Amazon S3 中对数据进行加密。
- IAM 用户必须具有调用 Amazon KMS API 操作所需的权限。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的将 IAM 策略与 Amazon KMS结合使用。
- 如果您删除或停用 Amazon Amazon KMS 密钥或撤消授权令牌，则无法访问卷或磁带上的数据。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的删除 KMS 密钥。
- 如果从采用 KMS 加密的卷中创建快照，则将加密快照。快照将继承卷的 KMS 密钥。
- 如果从采用 KMS 加密的快照中创建新卷，则将加密卷。可以为新卷指定不同的 KMS 密钥。

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

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

Amazon Storage Gateway 的身份和访问管理

Amazon Identity and Access Management (IAM) Amazon Web Services 服务 可帮助管理员安全地控制对 Amazon 资源的访问权限。IAM 管理员控制谁可以进行身份验证（登录）和授权（有权限）使用 Amazon SGW 资源。您可以使用 IAM Amazon Web Services 服务 ，无需支付额外费用。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- Stor Amazon age Gateway 如何与 IAM 协作
- 适用于 Storage Gateway 的基于身份的策略示例
- Amazon Storage Gateway 身份和访问疑难解答

受众

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

服务用户-如果您使用 Amazon SGW 服务完成工作，则您的管理员会为您提供所需的凭证和权限。当你使用更多的 Amazon SGW 功能来完成工作时，你可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 Amazon SGW 中的功能，请参阅Amazon Storage Gateway 身份和访问疑难解答。

服务管理员 — 如果您负责公司的 Amazon SGW 资源，则可能拥有对 Amazon SGW 的完全访问权限。您的工作是确定您的服务用户应访问哪些 Amazon SGW 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要详细了解贵公司如何在 Amazon SGW 中使用 IAM，请参阅Stor Amazon age Gateway 如何与 IAM 协作。

IAM 管理员 — 如果您是 IAM 管理员，则可能需要详细了解如何编写策略来管理 Amazon SGW 的访问权限。要查看您可以在 IAM 中使用的 Amazon SGW 基于身份的策略示例，请参阅。适用于 Storage Gateway 的基于身份的策略示例

使用身份进行身份验证

身份验证是您 Amazon 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 Amazon Web Services 账户根用户任 IAM 角色进行身份验证（登录 Amazon）。

如果您 Amazon 以编程方式访问，则会 Amazon 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 Amazon 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅《IAM 用户指南》中的用于签署 API 请求的Amazon 签名版本 4。

无论使用何种身份验证方法，您都可能需要提供其他安全信息。例如， Amazon 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《IAM 用户指南》中的 IAM 中的Amazon 多重身份验证。

Amazon Web Services 账户 root 用户

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

联合身份

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

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

IAM 用户和群组

I AM 用户是您 Amazon Web Services 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的用例，应在需要时更新访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可以拥有一个名为的群组，IAMAdmins并向该群组授予管理 IAM 资源的权限。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM 用户指南》中的 IAM 用户的使用案例。

IAM 角色

I AM 角色是您内部具有特定权限 Amazon Web Services 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。要在中临时担任 IAM 角色 Amazon Web Services Management Console，您可以从用户切换到 IAM 角色（控制台）。您可以通过调用 Amazon CLI 或 Amazon API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的代入角色的方法。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问：要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关用于联合身份验证的角色的信息，请参阅《IAM 用户指南》中的针对第三方身份提供商创建角色（联合身份验证）。
- 临时 IAM 用户权限：IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取：您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 Amazon Web Services 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅 IAM 用户指南中的 IAM 中的跨账户资源访问。
- 跨服务访问 — 有些 Amazon Web Services 服务 使用其他 Amazon Web Services 服务服务中的功能。例如，当您在服务中拨打电话时，该服务通常会在 Amazon 中运行应用程序 EC2 或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 Amazon，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 Amazon Web Services 服务 向下游服务发出请求的请求。 Amazon Web Services 服务只有当服务收到需要与其他 Amazon Web Services 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
  - 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 Amazon Web Services 服务委派权限的角色。
  - 服务相关角色-服务相关角色是一种链接到的服务角色。 Amazon Web Services 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 Amazon Web Services 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 A@@ mazon 上运行的应用程序 EC2 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 Amazon CLI 或 Amazon API 请求的应用程序的临时证书。这比在 EC2 实例中存储访问密钥更可取。要为 EC2 实例分配 Amazon 角色并使其可供其所有应用程序使用，您需要创建一个附加到该实

例的实例配置文件。实例配置文件包含角色并允许在 EC2 实例上运行的程序获得临时证书。有关更多信息，请参阅 IAM 用户指南中的使用 IAM 角色向在 A mazon EC2 实例上运行的应用程序授予权限。

使用策略管理访问

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

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

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

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

基于身份的策略

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

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

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么

条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 Amazon Web Services 服务。

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

访问控制列表 (ACLs)

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

Amazon S3 和 Amazon VPC 就是支持的服务示例 ACLs。 Amazon WAF要了解更多信息 ACLs，请参阅《亚马逊简单存储服务开发者指南》中的访问控制列表 (ACL) 概述。

其他策略类型

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

- 权限边界：权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅IAM 用户指南中的 IAM 实体的权限边界。
- 服务控制策略 (SCPs) — SCPs 是 JSON 策略，用于指定中组织或组织单位 (OU) 的最大权限 Amazon Organizations。 Amazon Organizations 是一项用于对您的企业拥有的多 Amazon Web Services 账户 项进行分组和集中管理的服务。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有帐户。SCP 限制成员账户中的实体（包括每个 Amazon Web Services 账户根用户实体）的权限。有关 Organization SCPs s 和的更多信息，请参阅《Amazon Organizations 用户指南》中的服务控制策略。
- 资源控制策略 (RCPs) — RCPs 是 JSON 策略，您可以使用它来设置账户中资源的最大可用权限，而无需更新附加到您拥有的每个资源的 IAM 策略。RCP 限制成员账户中资源的权限，并可能影响身份（包括身份）的有效权限 Amazon Web Services 账户根用户，无论这些身份是否属于您的组织。有关 Organizations 的更多信息 RCPs，包括 Amazon Web Services 服务 该支持的列表 RCPs，请参阅《Amazon Organizations 用户指南》中的资源控制策略 (RCPs)。
- 会话策略：会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的会话策略。

多个策略类型

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

Stor Amazon age Gateway 如何与 IAM 协作

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

你可以在 Amazon Storage Gateway 中使用的 IAM 功能

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

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

SGW 基于身份的策略 Amazon

支持基于身份的策略：是

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

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

SGW 基于身份的策略示例 Amazon

要查看 Amazon SGW 基于身份的策略示例，请参阅。适用于 Storage Gateway 的基于身份的策略示例

SGW 内部 Amazon 基于资源的政策

支持基于资源的策略：否

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

要启用跨账户访问，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 Amazon Web Services 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

Amazon SGW 的政策行动

支持策略操作：是

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

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

在策略中包含操作以授予执行关联操作的权限。

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

Amazon SGW 中的策略操作在操作前使用以下前缀：

```
sgw
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

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

要查看 Amazon SGW 基于身份的策略示例，请参阅。适用于 Storage Gateway 的基于身份的策略示例

Amazon SGW 的政策资源

支持策略资源：是

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

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符（*）指示语句应用于所有资源。

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

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

要查看 Amazon SGW 基于身份的策略示例，请参阅。适用于 Storage Gateway 的基于身份的策略示例

Amazon SGW 的策略条件密钥

支持特定于服务的策略条件键：是

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

在 `Condition` 元素（或 `Condition` 块）中，可以指定语句生效的条件。`Condition` 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 `Condition` 元素，或在单个 `Condition` 元素中指定多个键，则 Amazon 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 Amazon 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM 策略元素：变量和标签。

Amazon 支持全局条件密钥和特定于服务的条件键。要查看所有 Amazon 全局条件键，请参阅 IAM 用户指南中的Amazon 全局条件上下文密钥。

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

要查看 Amazon SGW 基于身份的策略示例，请参阅。适用于 Storage Gateway 的基于身份的策略示例

ACLs 在 Amazon SGW

支持 ACLs：否

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

带有 SGW 的 ABA Amazon C

支持 ABAC（策略中的标签）：部分支持

基于属性的访问控制（ABAC）是一种授权策略，该策略基于属性来定义权限。在中 Amazon，这些属性称为标签。您可以向 IAM 实体（用户或角色）和许多 Amazon 资源附加标签。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

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

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

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

在 Amazon SGW 中使用临时证书

支持临时凭证：是

当你使用临时证书登录时，有些 Amazon Web Services 服务 不起作用。有关更多信息，包括哪些 Amazon Web Services 服务 适用于临时证书，请参阅 IAM 用户指南中的Amazon Web Services 服务与 IA M 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 Amazon Web Services Management Console 使用的是临时证书。例如，当您 Amazon 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的从用户切换到 IAM 角色（控制台）。

您可以使用 Amazon CLI 或 Amazon API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 Amazon。 Amazon 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

转发 Amazon SGW 的访问会话

支持转发访问会话（FAS）：是

当您使用 IAM 用户或角色在中执行操作时 Amazon，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 Amazon Web Services 服务 向下游服务发出请求的请求。 Amazon Web Services 服务只有当服务收到需要与其他 Amazon Web Services 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

Amazon SGW 的服务角色

支持服务角色：是

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

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

SGW 的 Amazon 服务相关角色

支持服务相关角色：是

服务相关角色是一种链接到的服务角色。 Amazon Web Services 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 Amazon Web Services 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

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

适用于 Storage Gateway 的基于身份的策略示例

默认情况下，用户和角色无权创建或修改 Amazon SGW 资源。他们也无法使用 Amazon Web Services Management Console、 Amazon Command Line Interface (Amazon CLI) 或 Amazon API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

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

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

主题

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

策略最佳实践

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

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

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

使用 Amazon SGW 控制台

要访问 Amazon Storage Gateway 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您 Amazon Web Services 账户的 Amazon SGW 资源的详细信息。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 Amazon CLI 或 Amazon API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色仍然可以使用 Amazon SGW 控制台，还要将 Amazon SGW *ConsoleAccess* 或*ReadOnly* Amazon 托管策略附加到实体。有关更多信息，请参阅《IAM 用户指南》中的为用户添加权限。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 Amazon CLI 或 Amazon API 以编程方式完成此操作的权限。

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

```
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon Storage Gateway 身份和访问疑难解答

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

主题

- 我无权在 Amazon SGW 中执行操作
- 我无权执行 iam：PassRole
- 我想允许我以外的人 Amazon Web Services 账户 访问我的 Amazon SGW 资源

我无权在 Amazon SGW 中执行操作

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

当 `mateojackson` IAM 用户尝试使用控制台查看有关虚构 *`my-example-widget`* 资源的详细信息，但不拥有虚构 `sgw:`*`GetWidget`* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 sgw:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 `mateojackson` 用户的策略，以允许使用 `sgw:`*`GetWidget`* 操作访问 *`my-example-widget`* 资源。

如果您需要帮助，请联系您的 Amazon 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam：PassRole

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

有些 Amazon Web Services 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 marymajor 的 IAM 用户尝试使用控制台在 Amazon SGW 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 Amazon 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人 Amazon Web Services 账户 访问我的 Amazon SGW 资源

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

要了解更多信息，请参阅以下内容：

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

Amazon Storage Gateway 的合规性验证

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

有关特定合规计划范围内的 Amazon 服务列表，请参阅按合规计划划分的划分的范围内的服务。有关一般信息，请参阅合规计划。

您可以使用下载第三方审计报告 Amazon Artifact。有关更多信息，请参阅中的 “下载报告” Amazon Artifact。

您在使用 Storage Gateway 时的合规性责任由您的数据的敏感性、您公司的合规性目标以及适用的法律法规决定。 Amazon 提供以下资源来帮助满足合规性要求：

- 安全与合规性快速入门指南安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了在上部署以安全性和合规性为重点的基准环境的步骤。 Amazon
- HIPAA 安全与合规架构白皮书 — 本白皮书描述了公司如何使用来 Amazon 创建符合 HIPAA 标准的应用程序。
- 合规资源 — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- 使用Amazon Config 开发人员指南中的规则评估资源 — 该 Amazon Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- Amazon Security Hub— 此 Amazon 服务可全面了解您的安全状态 Amazon ，帮助您检查是否符合安全行业标准和最佳实践。

Amazon Storage Gateway 中的弹性

Amazon 全球基础设施是围绕 Amazon Web Services 区域 可用区构建的。

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

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

有关 Amazon Web Services 区域 和可用区的更多信息，请参阅Amazon 全球基础设施。

除了 Amazon 全球基础架构外，Storage Gateway 还提供多项功能来帮助支持您的数据弹性和备份需求：

- 使用 VMware vSphere 高可用性 (VMware HA) 帮助保护存储工作负载免受硬件、虚拟机管理程序或网络故障的影响。有关更多信息，请参阅 将 VMware vSphere 高可用性与 Storage Gateway 配合使用。
- 将虚拟磁带存档在 S3 Glacier Flexible Retrieval 中。有关更多信息，请参阅 将虚拟磁带存档。

Amazon Storage Gateway 中的基础设施安全

作为一项托管服务， Amazon Storage Gateway 受亚马逊网络服务：安全流程概述白皮书中描述的 Amazon 全球网络安全程序的保护。

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

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

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

Amazon 安全最佳实践

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

登录和监控 Amazon Storage Gateway

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

要了解更多信息 CloudTrail，请参阅Amazon CloudTrail 用户指南。

Storage Gateway 信息位于 CloudTrail

CloudTrail 在您创建账户时，将在您的亚马逊 Web Services 账户上激活。当 Storage Gateway 中发生活动时，该活动会与其他 Amazon 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在 Amazon Web Services 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录 Amazon Web Services 账户中的事件（包括 Storage Gateway 的事件），请创建跟踪记录。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。默认情况下，当您在控制台中创建跟踪时，该跟踪将应用于所有 Amazon 区域。此跟踪记录在 Amazon 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Simple Storage Service（Amazon S3）存储桶。此外，您可以配置其他 Amazon 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

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

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

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

- 请求是使用根证书还是 Amazon Identity and Access Management (IAM) 用户凭证发出。

- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 Amazon 服务发出。

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

了解 Storage Gateway 日志文件条目

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

以下示例显示了演示该操作的 CloudTrail 日志条目。

```
{ "Records": [{
                "eventVersion": "1.02",
                "userIdentity": {
                "type": "IAMUser",
                "principalId": "AIDAII5AUEPBH2M7JTNVC",
                "arn": "arn:aws:iam::111122223333:user/StorageGateway-team/JohnDoe",
                "accountId": "111122223333",
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                 "userName": "JohnDoe"
               },
                  "eventTime": "2014-12-04T16:19:00Z",
                  "eventSource": "storagegateway.amazonaws.com",
                  "eventName": "ActivateGateway",
                  "awsRegion": "us-east-2",
                  "sourceIPAddress": "192.0.2.0",
                  "userAgent": "aws-cli/1.6.2 Python/2.7.6 Linux/2.6.18-164.el5",
                   "requestParameters": {
                                          "gatewayTimezone": "GMT-5:00",
                                          "gatewayName": "cloudtrailgatewayvtl",
                                          "gatewayRegion": "us-east-2",
                                          "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
                                          "gatewayType": "VTL"
                                               },
                                               "responseElements": {
                                                                      "gatewayARN":
 "arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayvtl"
                                               },
```

```
                                                    "requestID":
 "54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
                                                    "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
                                                    "eventType": "AwsApiCall",
                                                    "apiVersion": "20130630",
                                                    "recipientAccountId": "444455556666"
             }]
}
```

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

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

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

排查网关问题

接下来，可以查找有关与网关、主机平台、虚拟磁带、高可用性、数据恢复和安全性相关的最佳实践以及问题故障排除的信息。本地网关故障排除信息涵盖部署在支持的虚拟化平台上的网关。高可用性问题的故障排除信息涵盖在 VMware vSphere 高可用性 (HA) 平台上运行的网关。

主题

- 故障排除：网关离线问题：了解如何诊断可能导致网关在 Storage Gateway 控制台中显示为离线的问题。
- 故障排除：网关激活期间的内部错误：了解在尝试激活 Storage Gateway 时收到内部错误消息的情况下该怎么做。
- 排查本地网关问题-了解在使用本地网关时可能遇到的典型问题，以及如何允许 Amazon Web Services 支持 连接到网关以帮助进行故障排除。
- 排查 Microsoft Hyper-V 设置：了解您在 Microsoft Hyper-V 平台上部署 Storage Gateway 时可能遇到的典型问题。
- Amazon EC2 网关问题疑难解答-查找有关您在使用部署在 Amazon 上的网关时可能遇到的典型问题的信息 EC2。
- 排查硬件设备问题：了解如何解决您可能遇到的有关 Storage Gateway 硬件设备的问题。
- 对虚拟磁带问题进行故障排除：了解在虚拟磁带出现意外问题时可以采取的措施。
- 排查高可用性问题-了解在 VMware HA 环境中部署的网关遇到问题时该怎么做。

故障排除：网关离线问题

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

网关可能由于以下一个或多个原因而显示为离线：

- 网关无法到达 Storage Gateway 服务端点。
- 网关意外关闭。
- 与网关关联的缓存磁盘已断开连接或经过修改，或者出现故障。

要使网关恢复在线，请确定并解决导致网关离线的问题。

检查关联的防火墙或代理

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

检查是否正在对网关的流量进行 SSL 检查或深度数据包检查

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

检查虚拟机监控程序主机上是否出现停电或硬件故障

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

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

检查关联的缓存磁盘是否有问题

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

如果从虚拟机监控程序主机上移除了正常工作的缓存磁盘：

1. 关闭网关。
2. 重新添加该磁盘。

> **Note**
>
> 确保将磁盘添加到同一个磁盘节点。

3. 重新启动网关。

如果缓存磁盘损坏、被更换或调整大小：

1. 关闭网关。
2. 重置缓存磁盘。

3. 重新配置磁盘以进行缓存存储。
4. 重新启动网关。

有关对磁带网关的已损坏缓存磁盘进行故障排除的更多信息，请参阅 You need to recover a virtual tape from a malfunctioning cache disk。

故障排除：网关激活期间的内部错误

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

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

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

解决使用公有端点激活网关时出现的错误

要解决使用公有端点激活网关时的激活错误，请执行以下检查和配置。

检查所需的端口

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

```
telnet d4kdq0yaxexbo.cloudfront.net 443
telnet storagegateway.region.amazonaws.com 443
```

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

要确认网关本身是否可以到达端点，请访问网关的本地 VM 控制台（适用于本地部署的网关）。或者，您可以通过 SSH 连接到网关的实例（适用于部署在 Amazon 上的网关 EC2）。然后，运行网络连接测试。确认测试返回 [PASSED]。有关更多信息，请参阅 Testing Your Gateway Connection to the Internet。

> **Note**
>
> 网关控制台的默认登录用户名为 admin，默认密码为 password。

确保防火墙安全性不会修改从网关发送到公有端点的数据包

SSL 检查、深度数据包检查或其它形式的防火墙安全性可能会干扰从网关发送的数据包。如果 SSL 证书的修改结果与激活端点所预期的情况不同，则 SSL 握手失败。要确认没有正在进行的 SSL 检查，请在端口 443 上的主激活端点 (anon-cp.storagegateway.region.amazonaws.com) 上运行 OpenSSL 命令。必须从与网关位于同一子网中的计算机上运行此命令：

```
$ openssl s_client -connect  anon-cp.storagegateway.region.amazonaws.com:443 -
servername anon-cp.storagegateway.region.amazonaws.com
```

> **Note**
>
> 替换*region*为你的 Amazon Web Services 区域。

如果没有正在进行的 SSL 检查，则该命令将返回类似于以下内容的响应：

```
$ openssl s_client -connect anon-cp.storagegateway.us-east-2.amazonaws.com:443 -
servername anon-cp.storagegateway.us-east-2.amazonaws.com
CONNECTED(00000003)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-2.amazonaws.com
```

```
verify return:1
---
Certificate chain
 0 s:/CN=anon-cp.storagegateway.us-east-2.amazonaws.com
   i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
 1 s:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
   i:/C=US/O=Amazon/CN=Amazon Root CA 1
 2 s:/C=US/O=Amazon/CN=Amazon Root CA 1
   i:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
 3 s:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
   i:/C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority
---
```

如果正在进行 SSL 检查，则响应将显示更改的证书链，类似于以下内容：

```
$ openssl s_client -connect  anon-cp.storagegateway.ap-southeast-1.amazonaws.com:443 -
servername anon-cp.storagegateway.ap-southeast-1.amazonaws.com
CONNECTED(00000003)
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.ap-southeast-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

激活端点仅在识别 SSL 证书时才接受 SSL 握手。这意味着，网关到端点的出站流量必须免受网络中防火墙执行的检查。这些检查可能是 SSL 检查或深度数据包检查。

检查网关时间同步

时间偏差过大可能会导致 SSL 握手错误。对于本地网关，可以使用网关的本地 VM 控制台来检查网关的时间同步。时间偏差应不大于 60 秒。有关更多信息，请参阅 Synchronizing Your Gateway VM Time。

系统时间管理选项在托管在 Amazon EC2 实例上的网关上不可用。为确保 Amazon EC2 网关能够正确同步时间，请确认 Amazon EC2 实例可以通过端口 UDP 和 TCP 123 连接到以下 NTP 服务器池列表：

- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org
- 2.amazon.pool.ntp.org
- 3.amazon.pool.ntp.org

解决使用 Amazon VPC 端点激活网关时出现的错误

要解决使用 Amazon Virtual Private Cloud（Amazon VPC）端点激活网关时出现的激活错误，请执行以下检查和配置。

检查所需的端口

确保本地防火墙（对于本地部署的网关）或安全组（对于部署在 Amazon 中的网关 EC2）中的所需端口已打开。将网关连接到 Storage Gateway VPC 端点所需的端口与将网关连接到公有端点时所需的端口不同。连接到 Storage Gateway VPC 端点需要以下端口：

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

有关更多信息，请参阅 Creating a VPC endpoint for Storage Gateway。

此外，请检查连接到 Storage Gateway VPC 端点的安全组。连接到端点的默认安全组可能不支持所需的端口。创建一个新的安全组，让来自网关 IP 地址范围的流量通过所需端口。然后，将该安全组连接到 VPC 端点。

> **Note**
>
> 使用 Amazon VPC 控制台来验证连接到 VPC 端点的安全组。从控制台查看 Storage Gateway VPC 端点，然后选择安全组选项卡。

要确认所需端口处于打开状态，可以在 Storage Gateway VPC 端点上运行 telnet 命令。必须从与网关位于同一子网中的服务器上运行这些命令。可以对第一个未指定可用区的 DNS 名称运行测试。例如，以下 telnet 命令使用 DNS 名称 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 测试所需的端口连接：

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 443
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1026
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1027
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1028
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1031
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 2222
```

确保防火墙安全性不会修改从网关发送到 Storage Gateway Amazon VPC 端点的数据包

SSL 检查、深度数据包检查或其它形式的防火墙安全性可能会干扰从网关发送的数据包。如果 SSL 证书的修改结果与激活端点所预期的情况不同，则 SSL 握手失败。要确认没有正在进行的 SSL 检查，请在 Storage Gateway VPC 端点上运行 OpenSSL 命令。必须从与网关位于同一子网中的计算机上运行此命令。针对每个必需的端口运行命令：

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:443 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1026 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1028 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1031 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:2222 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

如果没有正在进行的 SSL 检查，则该命令将返回类似于以下内容的响应：

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-1.amazonaws.com
verify return:1
---
Certificate chain
 0 s:CN = anon-cp.storagegateway.us-east-1.amazonaws.com
   i:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
 1 s:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
   i:C = US, O = Amazon, CN = Amazon Root CA 1
 2 s:C = US, O = Amazon, CN = Amazon Root CA 1
   i:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
 3 s:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
   i:C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification
 Authority
---
```

如果正在进行 SSL 检查，则响应将显示更改的证书链，类似于以下内容：

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
```

```
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.us-
east-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.us-east-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

激活端点仅在识别 SSL 证书时才接受 SSL 握手。这意味着，网关通过所需端口到 VPC 端点的出站流量免受由网络防火墙执行的检查。这些检查可能是 SSL 检查或深度数据包检查。

检查网关时间同步

时间偏差过大可能会导致 SSL 握手错误。对于本地网关，可以使用网关的本地 VM 控制台来检查网关的时间同步。时间偏差应不大于 60 秒。有关更多信息，请参阅 Synchronizing Your Gateway VM Time。

系统时间管理选项在托管在 Amazon EC2 实例上的网关上不可用。为确保 Amazon EC2 网关能够正确同步时间，请确认 Amazon EC2 实例可以通过端口 UDP 和 TCP 123 连接到以下 NTP 服务器池列表：

- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org
- 2.amazon.pool.ntp.org
- 3.amazon.pool.ntp.org

检查 HTTP 代理并确认关联的安全组设置

在激活之前，请检查您是否在本地网关虚拟机上 EC2 将 Amazon 上的 HTTP 代理配置为端口 3128 上的 Squid 代理。在此情况下，确认以下事项：

- 附加到 Amazon 上 HTTP 代理的安全组 EC2 必须具有入站规则。此入站规则必须在端口 3128 上支持来自网关 VM 的 IP 地址的 Squid 代理流量。
- 连接到 Amazon EC2 VPC 终端节点的安全组必须具有入站规则。这些入站规则必须允许来自亚马逊 HTTP 代理 IP 地址的端口 1026-1028、1031、2222 和 443 上的流量。 EC2

解决使用公有端点激活网关且同一 VPC 中有 Storage Gateway VPC 端点时出现的错误

要解决在同一 VPC 中有 Amazon Virtual Private Cloud（Amazon VPC）端点的情况下使用公有端点激活网关时出现的错误，请执行以下检查和配置。

确认 Storage Gateway VPC 端点上启用私有 DNS 名称设置未处于启用状态

如果启用私有 DNS 名称处于启用状态，则无法激活从该 VPC 到公有端点的任何网关。

要禁用 DNS 名称选项，请执行以下操作：

1. 打开 Amazon VPC 控制台。
2. 在导航窗格中，选择端点。
3. 选择 Storage Gateway VPC 端点。
4. 选择操作。
5. 选择管理私有 DNS 名称。
6. 对于启用私有 DNS 名称，清除为此端点启用。
7. 选择修改私有 DNS 名称来保存设置。

排查本地网关问题

您可以在下面找到有关在使用本地网关时可能遇到的典型问题以及如何激活 Amazon Web Services 支持 以帮助排除网关故障的信息。

下表列出了您在使用场内网关时可能遇到的典型问题。

事务	要采取的操作
您找不到网关的 IP 地址。	请使用管理程序客户端连接主机，以便查找网关 IP 地址。 • 对于 VMware ESXi，虚拟机的 IP 地址可以在 vSphere 客户端的“摘要”选项卡上找到。 • 对于 Microsoft Hyper-V，可登录本地控制台查找 VM 的 IP 地址。 如果您仍然难以找到网关 IP 地址：

事务	要采取的操作
	• 检查 VM 是否已开启。仅在 VM 已开启的情况下，IP 地址才会分配给您的网关。 • 等待 VM 完成启动。如果您刚刚打开 VM，那么网关可能需要一些时间才能完成启动序列。
您遇到了网络或防火墙问题。	• 允许适用于网关的端口。 • SSL 证书validation/inspection should not be activated. Storage Gateway utilizes mutual TLS authentication which would fail if any 3rd party application tries to intercept/sign任一证书。 • 如果使用防火墙或路由器来筛选或限制网络流量，则必须配置防火墙和路由器以允许这些服务端点与 Amazon进行出站通信。有关网络和防火墙要求的更多信息，请参阅网络和防火墙要求。
当您单击 Storage Gateway 管理控制台中的继续激活按钮时，网关的激活过程会失败。	• 检查网关 VM 是否可通过从客户端 ping 通。 • 检查您的 VM 是否已与 Internet 建立网络连接。否则，您需要配置 SOCKS 代理。有关执行此操作的更多信息，请参阅 为本地网关配置 SOCKS5 代理。 • 检查主机的时间是否准确，主机是否已配置为与网络时间协议 (NTP) 服务器自动同步，以及网关 VM 的时间是否准确。有关同步虚拟机管理程序主机的时间和 VMs的信息，请参见。将 VM 时间与 Hyper-V 或 Linux KVM 主机时间同步 • 执行这些步骤后，您可以使用 Storage Gateway 控制台和设置并激活网关向导重新尝试网关部署。 • SSL 证书validation/inspection should not be activated. Storage Gateway utilizes mutual TLS authentication which would fail if any 3rd party application tries to intercept/sign任一证书。 • 检查您的 VM 至少有 7.5 GB 的 RAM。如果 RAM 少于 7.5 GB，网关分配就会失效。有关更多信息，请参阅 设置磁带网关的要求。

事务	要采取的操作
您需要移除分配为上传缓冲区空间的磁盘。例如，您可能希望减少网关的上传缓冲区空间大小，或者可能需要替换已发生故障的用作上传缓冲区的磁盘。	有关移除分配为上传缓冲区的磁盘的说明，请参阅从网关中移除磁盘
您需要提高网关和 Amazon 之间的带宽。	您可以将互联网连接设置为与连接应用程序和网关 VM Amazon 的网卡 (NIC) 分开的网络适配器 (NIC)，从而 Amazon 改善从网关到网关的带宽。如果您有高带宽连接， Amazon 并且想要避免带宽争用，尤其是在快照还原期间，则采用这种方法很有用。对于高吞吐量工作负载需求，您可以使用 Amazon Direct Connect 在本地网关和 Amazon间建立专用网络连接。要测量从您的网关到的连接带宽 Amazon，请使用网关的`CloudBytesDownloaded` 和`CloudBytesUploaded` 指标。有关本主题的更多信息，请参阅 测量您的磁带网关和之间的性能 Amazon。提高 Internet 连接性能有助于确保您的上传缓冲区不被填满。

事务	要采取的操作

往返您网关的吞吐量将为零。	• 在 Storage Gateway 控制台的网关选项卡上，验证网关虚拟机的 IP 地址是否与使用虚拟机管理程序客户端软件（即 VMware vSphere 客户端或 Microsoft Hyper-V Manager）看到的 IP 地址相同。如果发现 IP 地址不一致，请从 Storage Gateway 控制台重启网关，如关闭网关虚拟机中所述。重启后，Storage Gateway 控制台的网关选项卡中 IP 地址列表中的地址应与您从管理程序客户端确定的网关 IP 地址相匹配。
	  • 对于 VMware ESXi，虚拟机的 IP 地址可以在 vSphere 客户端的 “摘要” 选项卡上找到。
	  • 对于 Microsoft Hyper-V，可登录本地控制台查找 VM 的 IP 地址。
	• 检查您的网关与的连接， Amazon 如中所述测试网关到互联网的连接。
	• 检查网关的网络适配器配置，确保要激活的所有网关接口均已激活。若要查看网关的网络适配器配置，请遵循 配置网关网络 中的说明并选择能够查看网关网络配置的选项。
	
	您可以从 Amazon CloudWatch 控制台查看进出网关的吞吐量。有关测量进出网关的吞吐量的更多信息 Amazon，请参阅测量您的磁带网关和之间的性能 Amazon。

在 Microsoft Hyper-V 中导入（部署）Storage Gateway 时遇到问题。	请参阅 排查 Microsoft Hyper-V 设置，其中对您在 Microsoft Hyper-V 上部署网关时遇到的部分常见问题进行了说明。
您收到一条消息，指出“已写入网关卷中的数据未安全存储在 Amazon中”。	如果您的网关虚拟机是从另一个网关虚拟机的克隆或快照创建的，则您会收到此消息。如果不是这种情况，请联系 Amazon Web Services 支持。

允许帮助 Amazon Web Services 支持 对本地托管的网关进行故障排除

Storage Gateway 提供了一个本地控制台，您可以使用它来执行多项维护任务，包括激活 Amazon Web Services 支持 以访问网关以帮助您解决网关问题。默认情况下，对您的网关的 Amazon Web

Services 支持 访问处于停用状态。您可通过主机的本地控制台来实现此访问。要 Amazon Web Services 支持 访问您的网关，请先登录主机的本地控制台，导航到 Storage Gateway 的控制台，然后连接到支持服务器。

允许 Amazon Web Services 支持 访问您的网关

1. 登录到主机的本地控制台。
   - VMware ESXi — 有关更多信息，请参阅使用访问网关本地控制台 VMware ESXi。
   - Microsoft Hyper-V - 有关更多信息，请参阅使用 Microsoft Hyper-V 访问网关本地控制台。
2. 在提示符处输入相应的数字来选择网关控制台。
3. 输入 **h** 打开可用命令的列表。
4. 请执行以下操作之一：
   - 如果网关使用的是公有端点，请在可用命令窗口中，输入 **`open-support-channel`** 来连接到 Storage Gateway 的客户支持。允许 TCP 端口 22，以便您可以打开 Amazon的支持通道。在连接到客户支持时，Storage Gateway 将为您分配支持编号。请记下您的支持编号。
   - 如果网关使用的是 VPC 端点，请在 AVAILABLE COMMANDS 窗口中，输入 **`open-support-channel`**。如果未激活网关，请提供要连接到 Storage Gateway 客户支持的 VPC 端点或 IP 地址。允许 TCP 端口 22，以便您可以打开 Amazon的支持通道。在连接到客户支持时，Storage Gateway 将为您分配支持编号。请记下您的支持编号。

   > **Note**
   >
   > 信道号不是（传输控制Protocol/User Datagram Protocol (TCP/UDP）端口号。相反，网关会与 Storage Gateway 服务器建立 Secure Shell (SSH) (TCP 22) 连接，并提供用于连接的支持通道。

5. 建立支持渠道后，请向提供您的支持服务号码， Amazon Web Services 支持 Amazon Web Services 支持 以便提供故障排除帮助。
6. 在支持会话完成后，输入 **q** 以将其结束。在 Amazon Web Services Support 通知您支持会话完成之前，请勿关闭该会话。
7. 输入**`exit`**以注销网关控制台。
8. 按照提示操作退出本地控制台。

排查 Microsoft Hyper-V 设置

下表列出了您在 Microsoft Hyper-V 平台上部署 Storage Gateway 时可能遇到的典型问题。

事务	要采取的操作
您尝试导入网关并收到以下错误消息： “尝试导入虚拟机时发生服务器错误。导入失败。在位置 [...] 下找不到虚拟机导入文件。仅当使用 Hyper-V 创建和导出虚拟机时，才能导入虚拟机。”	出现此错误的原因如下： • 如果您没有指向解压缩网关源文件的根目录。您在导入虚拟机对话框中所指定位置的最后一部分应该是 `AWS-Storage-Gateway` 。例如： `C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\` . • 如果您已经部署了网关，但没有在导入虚拟机对话框中选择复制虚拟机选项和复制所有文件选项，则在解压缩的网关文件所在位置创建 VM，并且您无法再从这个位置导入。为了修复此问题，请获取最新的解压缩网关源文件副本，并将其复制到新的位置。将新的位置用作导入源目录。 如果您计划从一个已解压缩的源文件位置创建多个网关，则必须选择复制虚拟机，然后在导入虚拟机对话框中选中复制所有文件框。
您尝试导入网关并收到以下错误消息： “尝试导入虚拟机时发生服务器错误。导入失败。导入任务无法从 [...] 复制文件：文件存在。（0x80070050）”	如果您已经部署网关且试图重新使用存储了虚拟硬盘文件和虚拟机配置文件的默认文件夹，那么会出现此错误。要修复此问题，请在 Hyper-V 设置对话框左侧面板的服务器下方指定新位置。
您尝试导入网关并收到以下错误消息： “尝试导入虚拟机时发生服务器错误。导入失败。Import failed because the virtual machine must	导入网关时，请确保在导入虚拟机对话框中选择复制虚拟机选项并选中复制所有文件框，来为 VM 创建新的唯一 ID。

事务	要采取的操作
have a new identifie r。Select a new identifier and try the import again.”	
您尝试启动网关 VM 并收到以下错误消息： “尝试启动选定的虚拟机时出错。子分区处理器设置与父分区不兼容。‘AWS-Storage-Gateway’无法初始化。（虚拟机 ID [...]）”	此错误可能是由于网关所需的 CPU 与主机 CPUs 上可用 CPUs 的 CPU 差异造成的。确保 VM 的 CPU 个数获得了底层管理程序的支持。 有关 Storage Gateway 要求的更多信息，请参阅设置磁带网关的要求。
您尝试启动网关 VM 并收到以下错误消息： “尝试启动选定的虚拟机时出错。‘AWS-Storage-Gateway’无法初始化。（虚拟机 ID [...]）无法创建分区：系统资源不足，无法完成所请求的服务。（0x800705AA）”	此错误很可能是该网关所需的 RAM 和主机上可用的 RAM 之间的差异导致的。 有关 Storage Gateway 要求的更多信息，请参阅设置磁带网关的要求。
您的快照和网关软件更新的出现时间会与预计的稍有不同。	网关 VM 的时钟可能会偏离实际的时间，这称为时钟漂移。使用本地网关控制台的时间同步选项，校验和纠正 VM 的时间。有关更多信息，请参阅 将 VM 时间与 Hyper-V 或 Linux KVM 主机时间同步。
您需要将解压缩的 Microsoft Hyper-V Storage Gateway 文件放入主机文件系统中。	按照访问典型 Microsoft Windows 服务器的方式访问主机。例如，如果虚拟机监控程序主机名为 `hyperv-server` ，则可使用以下 UNC 路径 `\\hyperv-server\c$` ，其中假定可解析名称 `hyperv-server` ，或在本地 hosts 文件中定义了该名称。
在连接管理程序时，系统会提示您输入证书。	以本地管理员的身份使用 Sconfig.cmd 工具给管理程序主机添加用户证书。

事务	要采取的操作
如果对使用 Broadcom 网络适配器的 Hyper-V 主机开启虚拟机队列（VMQ），则可能会注意到网络性能不佳。	有关解决方法的信息，请参阅 Microsoft 文档：Poor network performance on virtual machines on a Windows Server 2012 Hyper-V host if VMQ is turned on。

Amazon EC2 网关问题疑难解答

在以下各节中，您可以找到在使用部署在 Amazon 上的网关时可能遇到的典型问题 EC2。有关本地网关和部署在 Amazon 中的网关之间的区别的更多信息 EC2，请参阅为磁带网关部署自定义 Amazon EC2 实例。

主题

- 过了一会儿您的网关并未激活
- 您在实例列表中找不到您的 EC2 网关实例
- 您创建了 Amazon EBS 卷，但无法将其连接到您的 EC2 网关实例
- 您在尝试添加存储卷时收到一条消息称“无可用磁盘”
- 您希望删除一个分配为上传缓冲区空间的磁盘来减少上传缓冲区空间
- 进出 EC2 网关的吞吐量降至零
- 你 Amazon Web Services 支持 想帮忙排除 EC2 网关故障
- 您想使用 Amazon EC2 串行控制台连接到您的网关实例

过了一会儿您的网关并未激活

在 Amazon EC2 控制台中检查以下内容：

- 已在与实例关联的安全组中激活端口 80。有关添加安全组规则的更多信息，请参阅 Amazon EC2 用户指南中的添加安全组规则。
- 网关实例会标记为“running”。在 Amazon EC2 控制台中，实例的状态值应为 RUNNING。
- 确保您的 Amazon EC2 实例类型符合最低要求，如中所述存储需求。

纠正该问题后，请尝试重新激活网关。为此，请打开 Storage Gatew ay 控制台，选择在亚马逊上部署新网关 EC2，然后重新输入实例的 IP 地址。

您在实例列表中找不到您的 EC2 网关实例

如果您没有为您的实例赋予资源标签，并且有很多实例在运行，则很难分辨哪个实例是您启动的。在这种情况下，可执行以下操作来查找网关实例：

- 检查实例说明选项卡上的 Amazon 系统映像 (AMI) 名称。基于 Storage Gateway AMI 的实例应以 **`aws-storage-gateway-ami`** 文本开头。
- 如果您有几个实例基于 Storage Gateway AMI，请查看实例启动时间来找到正确的实例。

您创建了 Amazon EBS 卷，但无法将其连接到您的 EC2 网关实例

检查讨论中的 Amazon EBS 卷是否与网关实例在同一可用区中。如果在不同的可用区，请在您的实例所在的可用区中创建一个新的 Amazon EBS 卷。

您在尝试添加存储卷时收到一条消息称“无可用磁盘”

没有为新激活的网关定义卷存储。在定义卷存储之前，必须将本地磁盘分配给网关，以便用作上传缓冲区和缓冲存储空间。对于部署到亚马逊的网关 EC2，本地磁盘是连接到该实例的 Amazon EBS 卷。出现这个错误消息很可能是因为没有为实例定义 Amazon EBS 卷。

查看为运行网关的实例所定义的块储存设备。如果只存在两个数据块储存设备 (AMI 附带的默认设备)，那么应该增加存储。有关执行此操作的更多信息，请参阅 为磁带网关部署自定义 Amazon EC2 实例。在附加两个或两个以上的 Amazon EBS 卷后，尝试在网关上创建卷存储。

您希望删除一个分配为上传缓冲区空间的磁盘来减少上传缓冲区空间

按照确定要分配的上传缓冲区的大小中的步骤操作。

进出 EC2 网关的吞吐量降至零

验证网关实例是否在运行。例如，如果实例因系统重启而处于启动过程中，请等待该实例完成重启。

另外，验证网关 IP 是否改变。如果实例已停止，然后重新启动，那么实例的 IP 地址可能会发生更改。在这种情况下，您必须激活新的网关。

您可以从 Amazon CloudWatch 控制台查看进出网关的吞吐量。有关测量进出网关的吞吐量的更多信息 Amazon，请参阅测量您的磁带网关和之间的性能 Amazon。

你 Amazon Web Services 支持 想帮忙排除 EC2 网关故障

Storage Gateway 提供了一个本地控制台，您可以使用它来执行多项维护任务，包括激活 Amazon Web Services 支持 以访问网关以帮助您解决网关问题。默认情况下，对您的网关的 Amazon Web Services 支持 访问处于停用状态。您可以通过 Amazon EC2 本地控制台提供此访问权限。您通过安全外壳 (SSH) 登录到 Amazon EC2 本地控制台。要通过 SSH 成功登录，您的实例的安全组必须具有开放 TCP 端口 22 的规则。

> **Note**
>
> 如果将新规则添加到现有安全组，则新规则适用于使用该安全组的所有实例。有关安全组以及如何添加安全组规则的更多信息，请参阅《亚马逊 EC2 用户指南》中的 Amazon EC2 安全组。

要 Amazon Web Services 支持 连接您的网关，您需要先登录 Amazon EC2 实例的本地控制台，导航到存储网关的控制台，然后提供访问权限。

激活对部署在 Amazon EC2 实例上的网关的 Amazon Web Services 支持 访问权限

1. 登录您的 Amazon EC2 实例的本地控制台。有关说明，请转至 Amazon EC2 用户指南中的 Connect 到您的实例。

   您可以使用以下命令登录 EC2 实例的本地控制台。

   ```
   ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
   ```

   > **Note**
   >
   > *PRIVATE-KEY*是包含您用于启动 Amazon EC2 实例的 EC2 密钥对的私有证书的 .pem文件。有关更多信息，请参阅《亚马逊 EC2 用户指南》中的检索密钥对的公钥。*INSTANCE-PUBLIC-DNS-NAME*是运行网关的 Amazon EC2 实例的公有域名系统 (DNS) 名称。您可以通过在 EC2 控制台中选择 Amazon EC2 实例并单击 “描述” 选项卡来获取此公有 DNS 名称。

2. 在提示符处，输入 **6 - Command Prompt** 来打开 Amazon Web Services 支持 通道控制台。
3. 输入 **h** 以打开 AVAILABLE COMMANDS 窗口。
4. 请执行以下操作之一：

- 如果网关使用的是公有端点，请在可用命令窗口中，输入 **`open-support-channel`** 来连接到 Storage Gateway 的客户支持。允许 TCP 端口 22，以便您可以打开 Amazon的支持通道。在连接到客户支持时，Storage Gateway 将为您分配支持编号。请记下您的支持编号。
- 如果网关使用的是 VPC 端点，请在 AVAILABLE COMMANDS 窗口中，输入 **`open-support-channel`**。如果未激活网关，请提供要连接到 Storage Gateway 客户支持的 VPC 端点或 IP 地址。允许 TCP 端口 22，以便您可以打开 Amazon的支持通道。在连接到客户支持时，Storage Gateway 将为您分配支持编号。请记下您的支持编号。

> **Note**
>
> 信道号不是（传输控制Protocol/User Datagram Protocol (TCP/UDP）端口号。相反，网关会与 Storage Gateway 服务器建立 Secure Shell (SSH) (TCP 22) 连接，并提供用于连接的支持通道。

5. 建立支持渠道后，请向提供您的支持服务号码， Amazon Web Services 支持 Amazon Web Services 支持 以便提供故障排除帮助。
6. 在支持会话完成后，输入 **`q`** 以将其结束。在 Amazon Web Services 支持 通知您支持会话已完成之前，请勿关闭会话。
7. 输入 **`exit`** 来退出 Storage Gateway 控制台。
8. 通过控制台菜单操作来注销 Storage Gateway 实例。

您想使用 Amazon EC2 串行控制台连接到您的网关实例

您可以使用 Amazon EC2 串行控制台对启动、网络配置和其他问题进行故障排除。有关说明和故障排除提示，请参阅《亚马逊弹性计算云用户指南》中的 Amazon EC2 串行控制台。

排查硬件设备问题

以下主题介绍了您可能遇到的 Storage Gateway 硬件设备问题以及排查这些问题的建议。

您无法确定服务 IP 地址

当尝试连接到您的服务时，请确保您使用的是该服务的 IP 地址，而不是主机的 IP 地址。在服务控制台中配置服务 IP 地址，并在硬件控制台中配置主机 IP 地址。您将在启动硬件设备时看到硬件控制台。要从硬件控制台转到服务控制台，请选择 Open Service Console (打开服务控制台)。

如何执行出厂重置？

如果您需要在设备上执行出厂重置，请联系 Storage Gateway 硬件设备团队来获得支持，如后面的“支持”部分中所述。

如何执行远程重启？

如果您需要远程重启设备，可以使用 Dell iDRAC 管理界面执行此操作。有关更多信息，请参阅 Dell Technologies InfoHub 网站上的 i DRAC9 虚拟电源循环：远程重启 Dell EMC PowerEdge 服务器。

您在何处获得 Dell iDRAC 支持？

戴尔 PowerEdge 服务器配有戴尔iDRAC管理接口。我们建议执行下列操作：

- 如果您使用 iDRAC 管理界面，则应更改默认密码。有关iDRAC凭证的更多信息，请参阅 PowerEdge 戴尔——iDRAC的默认登录凭据是什么？ 。
- 确保固件是 up-to-date为了防止安全漏洞。
- 将 iDRAC 网络接口移动到正常的 (em) 端口可能会导致性能问题或阻止设备正常运行。

您找不到硬件设备序列号

可以使用 Storage Gateway 控制台查找 Storage Gateway 硬件设备的序列号。

查找硬件设备序列号：

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 从页面左侧的导航菜单中选择硬件。
3. 从列表中选择硬件设备。
4. 在设备的详细信息选项卡上找到序列号字段。

在何处获得硬件设备支持

Amazon 要联系您的硬件设备的技术支持，请参阅Amazon Web Services 支持。

该 Amazon Web Services 支持 团队可能会要求您激活支持渠道，以远程解决您的网关问题。您无需打开此端口即可实现网关的正常操作，但在进行问题排查时需要打开。您可以从硬件控制台激活支持通道，如下面的过程所示。

要打开支持渠道 Amazon

1. 打开硬件控制台。
2. 选择硬件控制台主页底部的打开支持渠道，然后按 Enter。

   如果没有网络连接或防火墙问题，分配的端口号应该在 30 秒内出现。例如：

   状态：在端口 19599 上打开
3. 记下端口号并将其提供给 Amazon Web Services 支持。

对虚拟磁带问题进行故障排除

您可以在下面找到有关您遇到虚拟磁带意外问题时要采取的措施的信息。

主题

- 从无法恢复的网关恢复虚拟磁带
- 排查无法恢复的磁带的问题
- 高可用性运行状况通知

从无法恢复的网关恢复虚拟磁带

虽然很少发生，但您的磁带网关仍可能会遇到不可恢复的故障。此类故障可能发生在管理程序主机、网关本身或缓存磁盘上。如果发生故障，您可以遵照本节中的故障排除说明来恢复磁带。

主题

- 您需要从发生故障的磁带网关恢复虚拟磁带
- 您需要从发生故障的缓存磁盘恢复虚拟磁带

您需要从发生故障的磁带网关恢复虚拟磁带

如果您的磁带网关或虚拟机管理程序主机遇到无法恢复的故障，则可以恢复已上传 Amazon 到另一个磁带网关的任何数据。

注意，写入到磁带的数据可能不会全部上传，直到该磁带成功存档到 VTS。以这种方式恢复到另一个网关的磁带数据可能不完整或空白。我们建议在所有恢复的磁带上建立清单，确保它们包含所需的内容。

将磁带恢复到另一个磁带网关

1. 指定一个正常运行的现有磁带网关来充当您的恢复目标网关。如果您没有可将磁带恢复到的磁带网关，请创建新的磁带网关。有关如何创建网关的信息，请参阅创建网关。
2. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
3. 在导航窗格中，选择网关，然后选择您要从中恢复磁带的磁带网关。
4. 选择详细信息选项卡。此时选项卡上将显示磁带恢复消息。
5. 选择创建恢复磁带来停用网关。
6. 在显示的对话框中，选择 Disable gateway。

   这个过程会永久终止磁带网关的正常功能，并公开所有可用的恢复点。有关说明，请参阅停用磁带网关。
7. 从已停用网关显示的磁带中，选择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。
8. 要开始将所需的任何磁带恢复到目标磁带网关，请选择创建恢复磁带。
9. 在 Create recovery tape 对话框中，验证要恢复的虚拟磁带的条码。
10. 对于网关，选择要将虚拟磁带恢复到的磁带网关。
11. 选择 Create recovery tape。
12. 删除发生故障的磁带网关，以免向您收费。有关说明，请参阅 删除网关和移除关联的资源。

Storage Gateway 将磁带从出现故障的磁带网关移动到您指定的磁带网关。磁带网关将磁带状态标记为“已恢复”。

您需要从发生故障的缓存磁盘恢复虚拟磁带

如果您的缓存磁盘遇到错误，则该网关会阻止对其中的虚拟磁带执行读写操作。例如，当磁盘损坏或从网关中移除时，可能发生错误。Storage Gateway 控制台将显示有关该错误的消息。

在该错误消息中，Storage Gateway 会提示您执行可以恢复磁带的两种操作之一：

- 关闭并重新添加磁盘 - 如果磁盘的数据未变但已移除磁盘，则采用此方法。例如，如果由于意外从主机移除了磁盘而导致发生错误，但磁盘和数据未变，则您可以重新添加该磁盘。要执行此操作，请参阅本主题后文中的过程。
- 重置缓存磁盘 - 如果缓存磁盘损坏或无法访问，则采用此方法。如果因磁盘错误导致缓存磁盘不可访问、无法使用或损坏，您可重置该磁盘。如果重置缓存磁盘，则您可以继续使用包含干净数据的磁带（即其缓存磁盘中的数据和 Amazon S3 中的数据已同步的磁带）。但是，其中包含的数据未与

Amazon S3 同步的磁带将自动恢复。这些磁带的状态将设置为 RECOVERED，但磁带将为只读。有关如何从主机中移除磁盘的信息，请参阅确定要分配的上传缓冲区的大小。

> **Important**
>
> 如果您要重置的缓存磁盘包含还未上传到 Amazon S3 的数据，则这些数据可能丢失。重置缓存磁盘以后，网关中将不再有已配置的缓存磁盘，因此，为了让网关能够正常工作，您必须至少配置一个新的缓存磁盘。

要重置缓存磁盘，请参阅本主题下文中的过程。

关闭再重新添加磁盘

1. 关闭网关。有关如何关闭网关的信息，请参阅关闭网关虚拟机。
2. 将磁盘重新添加到主机，并确保磁盘的磁盘节点号未发生改变。有关如何添加磁盘的信息，请参阅确定要分配的上传缓冲区的大小。
3. 重新启动网关。有关如何重新启动网关的信息，请参阅关闭网关虚拟机。

网关重新启动以后，您可验证缓存磁盘的状态。磁盘可能处于以下状态之一：

- 存在 - 磁盘可供使用。
- 缺失 - 磁盘不再与网关相连接。
- 不匹配 - 磁盘节点被包含不正确元数据的磁盘占用，或磁盘内容已损坏。

重置和重新配置缓存磁盘

1. 在前面阐明的 A disk error has occurred 错误消息中，选择 Reset Cache Disk。
2. 在配置网关页面中，为缓存存储配置磁盘。有关如何配置的信息，请参阅配置磁带网关。
3. 配置缓存存储后，关闭并重启网关，如上一过程所述。

网关重新启动后应该就会恢复。然后，您可以验证缓存磁盘的状态。

验证缓存磁盘的状态

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

2. 在导航窗格中，选择 Gateways，然后选择您的网关。
3. 对于 Actions (操作)，选择 Configure Local Storage (配置本地存储) 以显示 Configure Local Storage (配置本地存储) 对话框。此对话框将显示网关中的所有本地磁盘。

缓存磁盘节点状态显示在磁盘旁边。

> **Note**
>
> 如果您没有完成恢复过程，则网关会显示一个横幅，提示您配置本地存储。

排查无法恢复的磁带的问题

如果您的虚拟磁带出现意外故障，Storage Gateway 会将出现故障的虚拟磁带的状态设为“不可恢复”。要采取的操作视情况而定。您可以在下面找到有关您可能会发现的一些问题以及如何对这些问题进行故障排除的信息。

您需要从无法恢复的磁带恢复数据

如果您的虚拟磁带状态为 IRRECOVERABLE 且您需要使用该磁带，请尝试以下操作之一：

- 如果还没有激活磁带网关，请激活一个新的磁带网关。有关更多信息，请参阅创建网关。
- 停用包含不可恢复磁带的磁带网关，将磁带从恢复点恢复到新的磁带网关。有关更多信息，请参阅您需要从发生故障的磁带网关恢复虚拟磁带。

> **Note**
>
> 您必须重新配置 iSCSI 启动程序和备份应用程序才能使用新的磁带网关。有关更多信息，请参阅 连接 VTL 设备。

您不需要未存档的状态为 IRRECOVERABLE 的磁带

如果您有一个状态为 IRRECOVERABLE 的虚拟磁带，您不需要该磁带，且该磁带从未进行存档，则您应删除该磁带。有关更多信息，请参阅 从磁带网关中删除虚拟磁带。

您网关中的一个缓存磁盘遇到了故障

如果网关中的一个或多个缓存磁盘出现故障，则该网关会阻止对虚拟磁带执行读写操作。要恢复正常功能，请按如下所述重新配置网关：

- 如果缓存磁盘无法访问或不可用，请从网关配置中删除该磁盘。
- 如果缓存磁盘仍然可以访问和使用，请将其重新连接到您的网关。

> **Note**
>
> 如果删除缓存磁盘，则当网关恢复正常功能时，拥有干净数据的磁带或卷（即其缓存磁盘中的数据和 Amazon S3 中的数据已同步）将继续可用。例如，如果您的网关有三个缓存磁盘，而您删除了两个缓存磁盘，则干净的磁带或卷将处于“可用”状态。其他磁带和卷将处于“不可恢复”状态。
>
> 如果您使用临时磁盘作为网关的缓存磁盘或将缓存磁盘装载到临时驱动器，则关闭网关时缓存磁盘将丢失。在缓存磁盘和 Amazon S3 未同步时关闭网关会导致数据丢失。因此，我们不建议使用临时驱动器或磁盘。

高可用性运行状况通知

在 VMware vSphere 高可用性 (HA) 平台上运行网关时，您可能会收到运行状况通知。有关运行状况通知的更多信息，请参阅排查高可用性问题。

排查高可用性问题

如果您遇到可用性问题，则可在下面查找有关要采取的操作的信息。

主题

- 运行状况通知
- Metrics

运行状况通知

当您在 VMware vSphere HA 上运行网关时，所有网关都会向您配置的 Amazon CloudWatch 日志组生成以下运行状况通知。这些通知将转至名为 `AvailabilityMonitor` 的日志流中。

主题

- 通知：重启
- 通知： HardReboot
- 通知： HealthCheckFailure
- 通知： AvailabilityMonitorTest

通知：重启

在重新启动网关 VM 时，您会收到重启通知。您可以使用 VM 管理程序管理控制台或 Storage Gateway 控制台重新启动网关 VM。您也可以在网关维护周期内使用网关软件来重新启动。

措施

如果重启时间在网关的已配置维护开始时间的 10 分钟内，则此情况可能是正常的，并不指示任何问题。如果重启发生在维护时段之外，请检查是否已手动重新启动网关。

通知： HardReboot

当网关 VM 意外重启时，您会收到 `HardReboot` 通知。此类重启可能是因断电、硬件故障或其他事件导致的。对于 VMware 网关，vSphere 高可用性应用程序监控的重置可以启动此事件。

措施

当您的网关在这样的环境中运行时，请检查`HealthCheckFailure`通知是否存在，并查阅虚拟机 VMware 的事件日志。

通知： HealthCheckFailure

对于 VMware vSphere HA 上的网关，当运行状况检查失败并请求重启虚拟机时，您可以收到`HealthCheckFailure`通知。此事件也会在测试期间发生来监控可用性（由 `AvailabilityMonitorTest` 通知指示）。在此情况下，应会有 `HealthCheckFailure` 通知。

> **Note**
>
> 此通知仅适用于 VMware 网关。

措施

如果此事件重复发生，但没有 AvailabilityMonitorTest 通知，请检查您的 VM 基础设施是否存在问题（存储、内存等）。如果您需要其他帮助，请联系 Amazon Web Services 支持。

通知： AvailabilityMonitorTest

对于 VMware vSphere HA 上的网关，当您在中运行可用性和应用程序监控系统测试时，您会AvailabilityMonitorTest收到通知。 VMware

Metrics

AvailabilityNotifications 指标适用于所有网关。此指标是网关生成的与可用性相关的运行状况通知数。使用 Sum 统计数据可观察网关是否遇到了任何与可用性相关的事件。有关事件的详细信息，请咨询您配置的 CloudWatch 日志组。

磁带网关的最佳实践

本节包含以下主题，这些主题提供有关使用网关、本地磁盘、快照和数据的最佳实践的信息。我们建议您自行熟悉本节中概述的信息，并尝试遵循这些指南，以避免 Amazon Storage Gateway出现问题。有关诊断和解决您在部署中可能遇到的常见问题的更多指导，请参阅排查网关问题。

主题

- 最佳实践：恢复数据
- 清理不必要的资源

最佳实践：恢复数据

虽然很少发生，但您的网关仍可能会遇到不可恢复的故障。这种故障可能在您的虚拟机 (VM)、网关本身、本地存储或其他位置发生。如果出现故障，我们建议您按照以下相应部分中的说明恢复您的数据。

> **Important**
>
> Storage Gateway 不支持从您的虚拟机管理程序创建的快照或 EC2 亚马逊系统映像 (AMI) 中恢复网关虚拟机。如果您的网关 VM 出现故障，则激活新网关，然后根据以下说明将您的数据恢复到该网关。

主题

- 从虚拟机意外关闭中恢复
- 从故障网关或 VM 恢复您的数据
- 从不可恢复磁带恢复您的数据
- 从出现故障的缓存磁盘恢复您的数据
- 从不可访问的数据中心恢复您的数据

从虚拟机意外关闭中恢复

如果您的 VM 意外关闭，例如在停电期间，您的网关会变得不可访问。当电力和网络连接恢复后，您的网关会变得能够访问并开始正常运行。下面是此时您能够采取的有助于恢复数据的一些步骤：

- 如果断电导致网络连接问题，您可以进行对此问题进行排查。有关如何测试网络连接的信息，请参阅测试网关到互联网的连接。
- 对于磁带设置，当您的网关可供访问时，您的磁带会进入“正在引导”状态。此功能可确保您本地存储的数据继续与同步 Amazon。有关此状态的更多信息，请参阅理解磁带状态。
- 如果您的网关发生故障并且您的卷或磁带因意外关闭而出现问题，您可以恢复您的数据。有关如何恢复数据的信息，请参阅以下适用于您的情况的内容。

从故障网关或 VM 恢复您的数据

如果您的磁带网关或管理程序主机遇到无法恢复的故障，您可以使用以下步骤将磁带从出现故障的磁带网关恢复到另一磁带网关：

1. 确定要用作恢复目标的磁带网关，您也可以新建一个磁带网关。
2. 停用出现故障的网关。
3. 为您要恢复的每个磁带创建恢复磁带，并且指定目标磁带网关。
4. 删除出现故障的磁带网关。

有关如何将磁带从出现故障的磁带网关恢复到另一个磁带网关的详细信息，请参阅您需要从发生故障的磁带网关恢复虚拟磁带。

从不可恢复磁带恢复您的数据

如果磁带出现故障，并且磁带的状态为 IRRECOVERABLE，我们建议您根据具体情况使用以下选项之一恢复数据或解决故障：

- 如果您需要不可恢复磁带上的数据，您可以将该磁带恢复到新网关。
- 如果您不需要该磁带上的数据，且从未对该磁带进行存档，则您可以从磁带网关中删除该磁带。

  有关在磁带状态为 IRRECOVERABLE 时如何恢复数据或解决故障的详细信息，请参阅排查无法恢复的磁带的问题。

从出现故障的缓存磁盘恢复您的数据

如果缓存磁盘出现故障，我们建议您根据具体情况采用以下步骤恢复数据：

- 如果故障是因将缓存磁盘从您的主机中移除导致的，则关闭网关，重新添加该磁盘，然后重新启动网关。
- 如果缓存磁盘受损或无法访问，则关闭网关，重置缓存磁盘，重新为缓存存储配置磁盘，然后重新启动网关。

有关详细信息，请参阅 您需要从发生故障的缓存磁盘恢复虚拟磁带。

从不可访问的数据中心恢复您的数据

如果您的网关或数据中心由于某种原因无法访问，您可以将数据恢复到其他数据中心的另一个网关，或者恢复到托管在 Amazon EC2 实例上的网关。如果您无法访问其他数据中心，我们建议您在 Amazon EC2 实例上创建网关。您要执行的步骤取决于您要从中恢复数据的网关类型。

从不可访问的数据中心内的磁带网关恢复数据

1. 在 Amazon EC2 主机上创建并激活新的磁带网关。有关更多信息，请参阅 为磁带网关部署自定义 Amazon EC2 实例。
2. 将磁带从数据中心的源网关恢复到您在 Amazon 上创建的新网关。 EC2 有关更多信息，请参阅从无法恢复的网关恢复虚拟磁带。

   您的磁带应覆盖到新的 Amazon EC2 网关。

清理不必要的资源

如果您创建了网关作为示例练习或测试，请考虑清除以避免导致意外或不必要的费用。

如果您计划继续使用您的磁带网关，请参阅接下来该做什么？中的其他信息

清除不需要的资源

1. 从网关的虚拟磁带库 (VTL) 和存档中删除磁带。有关更多信息，请参阅 删除网关和移除关联的资源。

   a. 在您的网关的 VTL 中将任何处于 RETRIEVED (已检索) 状态的磁带存档。有关说明，请参阅存档磁带。
   b. 从网关的 VTL 中删除任何剩余的磁带。有关说明，请参阅 从磁带网关中删除虚拟磁带。
   c. 删除您在存档中拥有的任何磁带。有关说明，请参阅 从磁带网关中删除虚拟磁带。
2. 除非您计划继续使用磁带网关，否则请删除它：有关说明，请参阅删除网关和移除关联的资源。

3. 从本地主机中删除 Storage Gateway VM。如果您在 Amazon EC2 实例上创建了网关，请终止该实例。

其他 Storage Gateway 资源

本节介绍 Amazon 可帮助您设置或管理网关的第三方软件、工具和资源，以及 Storage Gateway 配额。

主题

- 部署和配置网关 VM 主机：了解如何为网关部署和配置虚拟机主机。
- 使用磁带网关存储资源：了解与磁带网关存储资源相关的过程，例如移除本地磁盘、管理 Amazon EBS 卷、使用虚拟磁带库设备以及管理虚拟磁带库中的磁带。
- 获取网关的激活密钥：了解部署新网关时可以在哪里找到您需要提供的激活密钥。
- 连接 iSCSI 启动程序：了解如何使用作为互联网小型计算机系统接口（iSCSI）目标公开的卷或虚拟磁带库（VTL）设备。
- Amazon Direct Connect 与 Storage Gateway 一起使用：了解如何在本地网关与 Amazon 云之间创建专用网络连接。
- 获取网关设备的 IP 地址：了解在哪里可以找到网关的虚拟机主机 IP 地址，部署新网关时需要提供该地址。
- 了解 Storage Gateway 资源和资源 IDs-了解如何 Amazon 识别 Storage Gateway 创建的资源和子资源。
- 标记 Storage Gateway 资源：了解如何使用元数据标签来对资源进行分类并使其更易于管理。
- 使用 Storage Gateway 的开源组件：了解用于提供 Storage Gateway 功能的第三方工具和许可证。
- Amazon Storage Gateway 配额：了解磁带网关的限制和配额，包括磁带大小和数量的最大限制，以及本地磁盘大小建议。

部署和配置网关 VM 主机

本节中的主题介绍如何为您的 Storage Gateway 设备设置和管理虚拟机主机，包括在 Hyper-V 或 Linux KVM 上 VMware运行的本地设备以及在云中亚马逊 EC2 实例上运行的设备。 Amazon

主题

- 为磁带网关部署默认 Amazon EC2 主机-了解如何使用默认规格在亚马逊弹性计算云 (Amazon EC2) 实例上部署和激活磁带。
- 为磁带网关部署自定义 Amazon EC2 实例-了解如何使用自定义设置在亚马逊弹性计算云 (Amazon EC2) 实例上部署和激活磁带。

- 修改 Amazon EC2 实例元数据选项-了解如何配置您的 Amazon EC2 网关实例，使其接受使用 IMDS 版本 1 (IMDSv1) 或要求所有元数据请求都使用 IMDS 版本 2 (IMDSv2) 的传入元数据请求。
- 将 VM 时间与 Hyper-V 或 Linux KVM 主机时间同步：了解如何查看本地 Hyper-V 或 Linux KVM 网关虚拟机的时间，并将其同步到网络时间协议（NTP）服务器。
- 将 VM 时间与 VMware主机时间同步-了解如何检查 VMware 网关虚拟机的主机时间，并在需要时设置时间并将主机配置为自动将其时间与网络时间协议 (NTP) 服务器同步。
- 在主机上配置半虚拟化 VMware -了解如何将 Storage Gateway 设备 VMware 的主机平台配置为使用半虚拟化互联网小型计算机系统接口协议 (iSCSI) 控制器。
- 为网关配置网络适配器-了解如何重新配置网关以使用 VMXNET3 (10 GbE) 网络适配器，或使用多个网络适配器，以便可以从多个 IP 地址访问网关。
- 将 VMware vSphere 高可用性与 Storage Gateway 配合使用-了解如何通过配置 Storage Gateway 使其与 VMware vSphere 高可用性配合使用，保护存储工作负载免受硬件、虚拟机管理程序或网络故障的影响。

为磁带网关部署默认 Amazon EC2 主机

本主题列出了使用默认规范部署 Amazon EC2 主机的步骤。

您可以在亚马逊弹性计算云 (Amazon EC2) 实例上部署和激活磁带网关。 Amazon Storage Gateway Amazon 系统映像 (AMI) 以社区 AMI 形式提供。

> **Note**
>
> Storage Gateway 社区 AMIs 由发布并完全支持 Amazon。你可以看到发布者是一个 Amazon 经过验证的提供商。

1. 要设置亚马逊 EC2instance，请在工作流程的平台选项部分选择亚马逊 EC2作为托管平台。有关配置 Amazon EC2 实例的说明，请参阅部署亚马逊 EC2实例来托管您的磁带网关。
2. 选择启动实例，在亚马逊 EC2 控制台中打开 Amazon Storage Gateway AMI 模板并自定义其他设置，例如实例类型、网络设置和配置存储。
3. 或者，您可以在 Storage Gateway 控制台中选择使用默认设置来部署具有默认配置的 Amazon EC2 实例。

   使用默认设置创建的 Amazon EC2 实例具有以下默认规格：

   - 实例类型 - m5.xlarge

- 网络设置
  - 对于 VPC，请选择您希望您的 EC2 实例在其中运行的 VPC。
  - 对于子网，请指定您的 EC2实例应在哪个子网中启动。

> **Note**
>
> 只有在 VPC 管理控制台中激活了自动分配公共 IPv4 地址设置后，VPC 子网才会出现在下拉列表中。

  - 自动分配公有 IP – 已激活

已创建 EC2 安全组并将其与 EC2 实例关联。安全组具有以下入站端口规则：

> **Note**
>
> 在网关激活期间，您需要打开端口 80。在激活后立即关闭该端口。此后，只能通过所选 VPC 的其他端口访问您的 EC2 实例。
> 只能通过与网关位于同一 VPC 中的主机来访问网关上的 iSCSI 目标。如果需要从 VPC 之外的主机访问 iSCSI 目标，则应更新相应的安全组规则。
> 您可以随时编辑安全组，方法是导航到 Amazon EC2 实例详情页面，选择安全，导航到安全组详情，然后选择安全组 ID。

端口	协议	文件系统协议				
80	TCP	用于激活的 HTTP 访问权限				
3260	TCP	iSCSI				

- 配置存储

默认设置	AMI 根卷	卷 2 缓存	卷 3 缓存			
设备名称		'/dev/sdb'	'/dev/sdc'			

默认设置	AMI 根卷	卷 2 缓存	卷 3 缓存			
大小	80 GiB	165 GiB	150 GiB			
卷类型	gp3	gp3	gp3			
IOPS	3000	3000	3000			
终止时删除	支持	是	是			
已加密	否	否	否			
吞吐量	125	125	125			

为磁带网关部署自定义 Amazon EC2 实例

您可以在亚马逊弹性计算云 (Amazon EC2) 实例上部署和激活磁带网关。 Amazon Storage Gateway Amazon 系统映像 (AMI) 以社区 AMI 形式提供。

> **Note**
>
> Storage Gateway 社区 AMIs 由发布并完全支持 Amazon。你可以看到发布者是一个 Amazon 经过验证的提供商。
> 磁带网关 AMIs 使用以下命名约定。AMI 名称中附加的版本号会随着每个版本的发布而变化。
> `aws-storage-gateway-CLASSIC-2.9.0`

部署 Amazon EC2 实例来托管您的磁带网关

1. 开始使用 Storage Gateway 控制台来设置新的网关。有关说明，请参阅设置磁带网关。当您进入平台选项部分时，选择 Amazon EC2 作为主机平台，然后按照以下步骤启动将托管您的磁带网关网关的 Amazon EC2 实例。
2. 选择启动实例，在亚马逊 EC2 控制台中打开 Amazon Storage Gateway AMI 模板，您可以在其中配置其他设置。

   使用快速启动启动具有默认设置的 Amazon EC2 实例。有关 Amazon EC2 Quicklaunch 默认规格的更多信息，请参阅亚马逊快速启动配置规范。 EC2

3. 在“名称”中，输入 Amazon EC2 实例的名称。部署实例后，您可以搜索此名称以在 Amazon EC2 控制台的列表页面上找到您的实例。
4. 在实例类型部分的实例类型列表中，为您的实例选择硬件配置。硬件配置必须满足某些最低要求才能支持您的网关。我们建议您首先使用 m5.xlarge 实例类型，它满足网关正常运行所需的最低硬件要求。有关更多信息，请参阅 Amazon EC2 实例类型的要求。

   如果需要，您可以在启动后调整实例的大小。有关更多信息，请参阅 Amazon EC2 用户指南中的调整实例大小。

   > **Note**
   >
   > 某些实例类型，特别是 i3 EC2，使用 NVMe SSD 磁盘。这可能会在您启动或停止磁带网关时导致出现问题；例如，您可能会丢失缓存中的数据。监控 `CachePercentDirty` Amazon CloudWatch 指标，只有在该参数为时才启动或停止系统`0`。要了解有关网关监控指标的更多信息，请参阅 CloudWatch 文档中的 Storage Gateway 指标和维度。

5. 在密钥对(登录) 部分的密钥对名称 -必需中，选择要用于安全连接到实例的密钥对。如有必要，您可以创建新的密钥对。有关更多信息，请参阅《适用于 Linux 实例的 Amazon Elastic Compute Cloud 用户指南》中的创建密钥对。
6. 在网络设置部分，检查预配置的设置并选择编辑来更改以下字段：

   a. 对于 VPC（必填），请选择要在其中启动 Amazon EC2 实例的 VPC。有关 Amazon VPC 的更多信息，请参阅《Amazon Virtual Private Cloud 用户指南》中的 Amazon VPC 的工作原理。

   b. （可选）对于子网，选择您要在其中启动 Amazon EC2 实例的子网。

   c. 对于自动分配公有 IP，选择启用。
7. 在防火墙（安全组）子部分中，查看预配置的设置。如果您愿意，可以更改要为您的 Amazon EC2 实例创建的新安全组的默认名称和描述，也可以选择应用现有安全组中的防火墙规则。
8. 在入站安全组规则子部分中，添加防火墙规则来打开客户端用于连接实例的端口。有关磁带网关所需端口的更多信息，请参阅端口要求。有关添加防火墙规则的更多信息，请参阅《适用于 Linux 实例的 Amazon Elastic Compute Cloud 用户指南》中的安全组规则。

   > **Note**
   >
   > 磁带网关要求在网关激活期间为入站流量和一次性 HTTP 访问打开 TCP 端口 80。激活后，您可以关闭此端口。

此外，您必须打开 TCP 端口 3260 才能访问 iSCSI。

9. 在高级网络配置子部分中，检查预配置的设置，必要时进行更改。
10. 在配置存储部分，选择添加新卷，将存储添加到网关实例。

> **Important**
>
> 除了预配置的根卷外，您还必须至少添加一个容量至少为 165 GiB 的 Amazon EBS 卷作为缓存存储，并至少添加一个容量至少为 150 GiB 的 Amazon EBS 卷作为上传缓冲区。为了提高性能，我们建议分配多个 EBS 卷作为缓存存储，每个卷至少为 150 GiB。

11. 在高级详细信息部分，检查预配置的设置，必要时进行更改。
12. 选择启动实例，使用配置的设置启动您的新 Amazon EC2 网关实例。
13. 要验证您的新实例是否成功启动，请导航至 Amazon EC2 控制台中的实例页面，然后按名称搜索您的新实例。确保实例状态显示为正在运行且带有绿色复选标记，并确保状态检查已完成且显示绿色复选标记。
14. 从详细信息页面中选择您的实例。从 “实例摘要” 部分复制公共 IPv4地址，然后返回 Storage Gateway 控制台中的设置网关页面，继续设置您的磁带网关。

您可以使用 Storage Gateway 控制台或查询 Amazon Systems Manager 参数存储来确定用于启动磁带网关网关的 AMI ID。

要确定 AMI ID，请执行以下任一操作：

- 开始使用 Storage Gateway 控制台来设置新的网关。有关说明，请参阅设置磁带网关。当您进入平台选项部分时，选择亚马逊 EC2作为主机平台，然后选择启动实例以在亚马逊 EC2控制台中打开 Amazon Storage Gateway AMI 模板。

  您将被重定向到 EC2 社区 AMI 页面，您可以在网址中看到您所在 Amazon 地区的 AMI ID。
- 查询 Systems Manager 参数存储。你可以使用 Amazon CLI 或 Storage Gateway API 查询命名空间下的 Systems Manager 公共参数`/aws/service/storagegateway/ami/VTL/latest`。例如，使用以下 CLI 命令返回 Amazon Web Services 区域 您指定的当前 AMI 的 ID。

```
aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/VTL/
latest
```

该 CLI 命令会返回类似以下内容的输出：

```
{
    "Parameter": {
        "Type": "String",
        "LastModifiedDate": 1561054105.083,
        "Version": 4,
        "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/VTL/
latest",
        "Name": "/aws/service/storagegateway/ami/VTL/latest",
        "Value": "ami-123c45dd67d891000"
    }
}
```

修改 Amazon EC2 实例元数据选项

实例元数据服务 (IMDS) 是一个实例组件，可提供对 Amazon EC2 实例元数据的安全访问。可以将实例配置为接受使用 IMDS 版本 1 (IMDSv1) 或要求所有元数据请求都使用 IMDS 版本 2 (IMDSv2) 的传入元数据请求。 IMDSv2 使用面向会话的请求并缓解了几种可用于尝试访问 IMDS 的漏洞。有关信息 IMDSv2，请参阅 Amazon Elastic Compute Cloud 用户指南中的实例元数据服务版本 2 的工作原理。

我们建议您要求 IMDSv2 所有托管 Storage Gateway 的亚马逊 EC2 实例。 IMDSv2 默认情况下，所有新启动的网关实例都是必需的。如果您的现有实例仍配置为接受 IMDSv1 元数据请求，请参阅 Amazon Elastic Compute Cloud 用户指南 IMDSv2中的要求使用，了解如何修改您的实例元数据选项以要求使用 IMDSv2。应用此更改不需要重启实例。

将 VM 时间与 Hyper-V 或 Linux KVM 主机时间同步

对于部署在上的网关 VMware ESXi，设置虚拟机管理程序主机时间并将虚拟机时间同步到主机就足以避免时间偏差。有关更多信息，请参阅 将 VM 时间与 VMware主机时间同步。对于在 Microsoft Hyper-V 或 Linux KVM 上部署的网关，我们建议您使用下面介绍的过程来定期检查虚拟机时间。

查看虚拟机监控程序网关虚拟机的时间并将其同步到网络时间协议（NTP）服务器

1. 登录到网关的本地控制台：

   - 有关登录到 Microsoft Hyper-V 本地控制台的更多信息，请参阅使用 Microsoft Hyper-V 访问网关本地控制台。
   - 有关登录到基于 Linux 内核的虚拟机（KVM）的本地控制台的更多信息，请参阅使用 Linux KVM 访问网关本地控制台。

2. 在 Storage Gateway 配置主菜单屏幕上，输入相应的数字以选择系统时间管理。
3. 在系统时间管理菜单屏幕上，输入相应的数字以选择查看和同步系统时间。

   网关本地控制台显示当前系统时间，并将其与 NTP 服务器报告的时间进行比较，然后以秒为单位报告两个时间之间的确切差异。
4. 如果时间差异大于 60 秒，请输入 **y** 来将系统时间与 NTP 时间同步。否则，请输入 **n**。

   时间同步可能需要一些时间。

将 VM 时间与 VMware主机时间同步

若要成功激活网关，您必须确保 VM 时间与主机时间同步，并且主机时间设置正确。在本节中，您首先要将 VM 时间与主机时间同步。然后，您将检查主机时间，如果需要，您应设置主机时间并将主机配置为自动与网络时间协议 (NTP) 服务器同步。

> **Important**
>
> 要成功激活网关，就需要同步 VM 时间和主机时间。

如需将 VM 时间与主机时间同步

1. 配置您的 VM 时间。

   a. 在 vSphere 客户端中，在应用程序窗口左侧的面板中，右键单击网关 VM 的名称以打开虚拟机的快捷菜单，然后选择编辑设置。

      “Virtual Machine Properties”对话框打开。

   b. 选择 “选项” 选项卡，然后从选项列表中选择 “VMware 工具”。

   c. 选中虚拟机属性对话框右侧高级部分中的与主机同步访客时间选项，然后选择确定。

      VM 时间与主机进行同步。
2. 配置主机时间。

   请注意，确保您设置了正确的主机时间。如果您尚未配置主机时间，请执行下列步骤进行设置并将其与 NTP 服务器同步。

   a. 在 VMware vSphere 客户端中，在左侧面板中选择 vSphere 主机节点，然后选择配置选项卡。

b. 在软件面板中选择时间配置，然后选择属性链接。

“Time Configuration”对话框显示。

c. 在日期和时间下，设置 vSphere 主机的日期和时间。

d. 将主机配置为自动将其时间与 NTP 服务器同步。

i. 在时间配置对话框中选择选项，然后在 NTP 进程守护程序（ntpd）选项对话框中，选择左侧面板中的 NTP 设置。

ii. 选择 Add 以添加新 NTP 服务器。

iii. 在 Add NTP Server 对话框中，键入 NTP 服务器的 IP 地址或完全限定域名，然后选择 OK。

可以将 `pool.ntp.org` 用作域名。

iv. 在 NTP 进程守护程序（ntpd）选项对话框中，选择左侧面板中的常规。

v. 在服务命令下，选择启动来启动服务。

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

e. 选择 OK 以关闭 NTP Daemon (ntpd) Options 对话框。

f. 选择 OK 以关闭 Time Configuration 对话框。

在主机上配置半虚拟化 VMware

以下过程介绍如何将 Storage Gateway 设备 VMware 的主机平台配置为使用半虚拟化互联网小型计算机系统接口协议 (iSCSI) 控制器。半虚拟化 iSCSI 控制器是高性能存储控制器，可以导致吞吐量提高和 CPU 使用量降低。这些控制器最适合高性能存储环境。以这种方式配置 iSCSI 控制器时，Storage Gateway 虚拟机将与主机操作系统配合使用，可让网关控制台识别您添加到虚拟机的虚拟磁盘。

> **Note**
>
> 您需要完成此步骤，才能避免在网关控制台中配置这些磁盘时出现磁盘标识问题。

将 VMware 主机平台配置为使用半虚拟化控制器

1. 在 VMware vSphere 客户端中，在应用程序窗口左侧的导航窗格中右键单击网关虚拟机的名称以打开快捷菜单，然后选择编辑设置。

2. 在虚拟机属性对话框中，选择硬件选项卡。
3. 在硬件选项卡上，选择 SCSI 控制器 0，然后选择更改类型。
4. 在 “更改 SCSI 控制器类型” 对话框中，选择 P VMware aravirtual SCSI 控制器类型，然后选择 “确定” 以保存配置。

为网关配置网络适配器

默认情况下，Storage Gateway 配置为使用 E1000 网络适配器类型，但您可以将网关重新配置为使用 VMXNET3 (10 GbE) 网络适配器。还可以将 Storage Gateway 配置为能够通过多个 IP 地址来访问。为此，您可以将网关配置为使用多个网络适配器。

主题

- 将网关配置为使用 VMXNET3网络适配器
- 为多个网关配置网关 NICs

将网关配置为使用 VMXNET3网络适配器

Storage Gateway 在两者中都 VMware ESXi 支持 E1000 网络适配器类型，也支持 Microsoft Hyper-V 虚拟机管理程序主机。但是，只有 VMware ESXi 虚拟机管理程序支持 VMXNET3 (10 GbE) 网络适配器类型。如果您的网关托管在 VMware ESXi 虚拟机管理程序上，则可以将网关重新配置为使用 (VMXNET3 10 GbE) 适配器类型。有关这些适配器的更多信息，请参阅 Broadcom (VMware) 网站上为您的虚拟机选择网络适配器。

> **Important**
>
> 要进行选择 VMXNET3，您的客户机操作系统类型必须是 “其他 Linux 64”。

以下是将网关配置为使用 VMXNET3适配器所采取的步骤：

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

下面是有关如何执行每个步骤的详细信息。

移除默认 E1000 适配器并将网关配置为使用该VMXNET3 适配器

1. 在中 VMware，打开网关的上下文（右键单击）菜单，然后选择编辑设置。
2. 在虚拟机属性窗口中，选择硬件选项卡。
3. 对于 Hardware，选择 Network adapter。请注意，在适配器类型部分，当前适配器为 E1000。您将用适配器替换此 VMXNET3 适配器。
4. 选择 E1000 网络适配器，然后选择 Remove。在本示例中，E1000 网络适配器是网络适配器 1。

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

5. 选择添加来打开“添加硬件”向导。
6. 选择 Ethernet Adapter，然后选择 Next。
7. 在“网络类型”向导中，为适配器类型选择 **VMXNET3**，然后选择下一步。
8. 在 “虚拟机属性” 向导中，在 “适配器类型” 部分中验证 “当前适配器” 已设置为 VMXNET3，然后选择 “确定”。
9. 在 VMware VSphere 客户端中，关闭您的网关。
10. 在 VMware VSphere 客户端中，重新启动您的网关。

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

为网络配置适配器

1. 在 VSphere 客户端中，选择控制台选项卡以启动本地控制台。在本配置任务中，使用默认登录凭证登录网关的本地控制台。有关如何使用默认凭证登录的信息，请参阅使用默认凭证登录本地控制台。
2. 在提示符处输入相应的数字来选择网络配置。
3. 在提示符处，输入相应的数字来选择全部重置为 DHCP，然后在命令提示符处输入 **y**（表示“是”）以将所有适配器设置为使用动态主机配置协议 (DHCP)。所有可用适配器均设置为使用 DHCP。

   如果网关已激活，则必须从 Storage Gateway 管理控制台将其关闭并重新启动。在网关重新启动后，必须测试 Internet 网络连接。有关如何测试网络连接的信息，请参阅测试网关与 Internet 的连接。

为多个网关配置网关 NICs

如果将网关配置为使用多个网络适配器 (NICs)，则可以由多个 IP 地址访问网关。您可能希望在以下情况下执行此操作：

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

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

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

- 在一台 VMware ESXi 主机上配置多个网络适配器
- 在 Microsoft Hyper-V 主机上配置多个网络适配器

在一台 VMware ESXi 主机上配置多个网络适配器

以下过程假设您的网关 VM 已经定义了一个网络适配器，并描述了如何在上面添加适配器 VMwareESXi。

将网关配置为在VMware ESXi 主机中使用其他网络适配器

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

   VM 在此过程中可能保持开启状态。
3. 在客户端中，打开网关 VM 的上下文（右键单击）菜单，然后选择 Edit Settings (编辑设置)。
4. 在虚拟机属性对话框的硬件选项卡上，选择添加来添加设备。
5. 按 Add Hardware (添加硬件) 向导添加网络适配器。

a. 在 Device Type (设备类型) 窗格中，选择 Ethernet Adapter (以太网适配器) 以添加适配器，然后选择 Next (下一步)。
b. 在网络类型窗格中，确保为类型选择开机时连接，然后选择下一步。

   我们建议您将 VMXNET3 网络适配器与 Storage Gateway 配合使用。有关适配器列表中可能出现的适配器类型的更多信息，请参阅ESXi 和 vCenter Server 文档中的网络适配器类型。
c. 在 Ready to Complete (已准备好完成) 窗格中，查看信息，然后选择 Finish (完成)。

6. 选择 VM 的摘要选项卡，然后选择 IP 地址 框旁边的查看全部。虚拟机 IP 地址窗口显示您可以用来访问网关的全部 IP 地址。确认第二个 IP 地址已针对该网关列出。

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

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

有关 Hyper-V 和 KVM 主机常见的本地控制台任务的信息，请参阅 VMware 在 虚拟机本地控制台上执行任务

在 Microsoft Hyper-V 主机上配置多个网络适配器

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。此过程演示如何为 Microsoft Hyper-V 主机添加适配器。

将网关配置为使用 Microsoft Hyper-V 主机中的另一个网络适配器

1. 在 Storage Gateway 控制台中，关闭网关。
2. 在 Microsoft Hyper-V Manager 中，从虚拟机面板中选择网关 VM。
3. 如果网关 VM 尚未关闭，请右键单击 VM 名称以打开上下文菜单，然后选择关闭。
4. 右键单击网关 VM 名称以打开上下文菜单，然后选择设置。
5. 在设置对话框中的硬件下，选择添加硬件。
6. 在设置对话框右侧的添加硬件面板中，选择网络适配器，然后选择添加来添加设备。
7. 配置网络适配器，然后选择 Apply (应用) 以应用设置。
8. 在设置对话框的硬件下，确认新的网络适配器已添加到硬件列表中，然后选择确定。

9. 使用 Storage Gateway 控制台开启网关。
10. 在 Storage Gateway 控制台的导航面板中，选择网关，然后选择向其中添加了适配器的网关。确认详细信息选项卡中列出了第二个 IP 地址。

有关 Hyper-V 和 KVM 主机常见的本地控制台任务的信息，请参阅 VMware 在 虚拟机本地控制台上执行任务

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

Storage Gateway VMware 通过一组与 VMware vSphere 高可用性 (HA) 集成的应用程序级运行状况检查提供高可用性。VMware 此方法有助于保护存储工作负载免受硬件、管理程序或网络故障的影响。它还有助于防止软件错误，例如连接超时和文件共享或卷不可用。

vSphere HA 的工作原理是将虚拟机及其所在的主机汇集到一个集群中以实现冗余。集群中的主机将受到监控，如果出现故障，故障主机上的虚拟机将在备用主机上重新启动。通常，这种恢复会快速发生，而不会丢失数据。有关 vSphere HA 的更多信息，请参阅文档中的 vSphere HA 的工作原理。 VMware

> **Note**
>
> 重新启动出现故障的虚拟机并在新主机上重新建立 iSCSI 连接所需的时间取决于诸多因素，例如主机操作系统和资源负载、磁盘速度、网络连接以及 SAN/存储基础设施。为最大限度地减少失效转移停机时间，请实施 Optimizing Gateway Performance 中概述的建议。
> 要将 Storage Gateway 与 VMware HA 配合使用，我们建议您执行以下操作：
>
> - 仅在 VMware 集群中的一台主机上部署包含 Storage Gateway 虚拟机的 ESX `.ova` 可下载软件包。
> - 在部署 `.ova` 程序包时，选择一个不在主机本地的数据存储。而是使用一个可供群集的所有主机访问的数据存储。如果您选择的是主机本地数据存储，而主机发生了故障，则群集中的其他主机可能无法访问该数据源，并且可能无法成功地故障转移到另一台主机。
> - 要防止启动程序在故障转移期间与存储卷目标断开连接，请遵循针对您的操作系统建议的 iSCSI 设置。在故障转移事件中，网关 VM 在故障转移群集中的新主机中启动时，需要花费几秒钟到几分钟的时间。Windows 和 Linux 客户端的建议 iSCSI 超时超过了完成故障转移通常所需的时间。有关自定义 Windows 客户端的超时设置的更多信息，请参阅 自定义您的 Windows iSCSI 设置。有关自定义 Linux 客户端的超时设置的更多信息，请参阅 自定义您的 Linux iSCSI 设置。
> - 利用群集化，如果您将 `.ova` 程序包部署到群集，请在系统提示您这样做时选择一台主机。或者您也可以直接部署到群集中的主机里。

以下主题介绍如何在 VMware HA 集群中部署 Storage Gateway：

主题

- 配置您的 vSphere VMware 高可用集群
- 从 Storage Gateway 控制台下载 .ova 映像
- 部署网关
- （可选）为集群 VMs 上的其他人添加覆盖选项
- 激活网关
- 测试您的 VMware 高可用性配置

配置您的 vSphere VMware 高可用集群

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

接下来，将您的 VMware 集群配置为与 Storage Gateway 配合使用。

配置您的 VMware 集群

1. 在 VMware vSphere 的 “编辑集群设置” 页面上，确保为虚拟机和应用程序监控配置了虚拟机监控。为此，请为每个选项设置以下值：

   - 主机故障响应：重新启动 VMs
   - 主机隔离的响应：关闭并重启 VMs
   - Datastore with PDL (具有 PDL 的数据存储)：Disabled (已禁用)
   - Datastore with APD (具有 APD 的数据存储)：Disabled (已禁用)
   - VM Monitoring (VM 监控)：VM and Application Monitoring (VM 和应用程序监控)
2. 通过调整以下值来微调集群的敏感度：

   - 故障间隔 - 在此间隔之后，如果未收到 VM 检测信号，则将重新启动 VM。
   - 最短正常运行时间 - 在 VM 开始监控 VM 工具的检测信号之后，集群等待的时间。
   - 每个 VM 的最大重置次数 - 集群在最大重置时段内重启 VM 的最大次数。
   - 最大重置次数的时段 - 计算每个 VM 的最大重置次数的时段。

   如果您不确定要设置的值，请使用以下示例设置：

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

如果您在集群上 VMs 运行其他值，则可能需要专门为虚拟机设置这些值。在从 .ova 部署 VM 之前，无法执行此操作。有关设置这些值的更多信息，请参阅 （可选）为集群 VMs 上的其他人添加覆盖选项。

从 Storage Gateway 控制台下载 .ova 映像

下载适用于您的网关的 .ova 映像

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

部署网关

在已配置的集群中，将 .ova 映像部署到集群的主机之一。

部署网关 .ova 映像

1. 将 .ova 映像部署到集群中的主机之一。
2. 确保为根磁盘和缓存选择的数据存储对集群中的所有主机可用。在 VMware 或本地环境中部署 Storage Gateway .ova 文件时，这些磁盘被描述为半虚拟化 SCSI 磁盘。半虚拟化 是一种模式，在此模式下，网关 VM 使用主机操作系统来让控制台标识您添加到 VM 的虚拟磁盘。

   如需将 VM 配置为使用半虚拟化的控制器

   1. 在 VMware vSphere 客户端中，打开网关 VM 的上下文（右键单击）菜单，然后选择编辑设置。
   2. 在 Virtual Machine Properties 对话框中，选择 Hardware 选项卡，再选择 SCSI controller 0，然后选择 Change Type。
   3. 在 “更改 SCSI 控制器类型” 对话框中，选择 “VMware 半虚拟 SCSI 控制器类型”，然后选择 “确定”。

（可选）为集群 VMs 上的其他人添加覆盖选项

如果您的集群上 VMs 正在运行其他虚拟机，则可能需要专门为每个 VM 设置集群值。有关说明，请参阅 VMware vSphere 在线文档中的自定义单个虚拟机。

为集群 VMs 上的其他人添加覆盖选项

1. 在 VMware vSphere 的 “摘要” 页面上，选择您的集群以打开集群页面，然后选择配置。
2. 选择 Configuration (配置) 选项卡，然后选择 VM Overrides (VM 覆盖)。
3. 添加新的 VM 覆盖选项来更改每个值。

   为 vSphere HA - VM 监控下的每个选项设置以下值：

   - VM 监控：已启用覆盖 - VM 和应用程序监控
   - VM 监控灵敏度：已启用覆盖 - VM 和应用程序监控
   - VM 监控：自定义
   - 故障间隔：**30** 秒
   - 最短正常运行时间：**120** 秒
   - Maximum per-VM resets (每个 VM 的最大重置次数)：**5**
   - 最大重置时段：**1** 小时内

激活网关

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

激活网关

- 请按照以下主题概述的步骤操作：

  a. 将您的磁带网关连接到 Amazon

  b. 检查设置并激活磁带网关

  c. 配置磁带网关

测试您的 VMware 高可用性配置

激活网关后，请测试您的配置。

测试您的 VMware HA 配置

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在导航窗格上，选择 Gateways，然后选择要测试 VMware HA 的网关。
3. 在 “操作” 中，选择 “验证 VMware HA”。
4. 在出现的 “验证 VMware 高可用性配置” 框中，选择 “确定”。

> **Note**
>
> 测试 VMware HA 配置会重新启动网关 VM 并中断与网关的连接。该测试可能需要几分钟才能完成。

   如果测试成功，则控制台中网关的详细信息选项卡中将显示 Verified (已验证) 状态。
5. 请选择 Exit（退出）。

您可以在 Amazon CloudWatch 日志组中找到有关 VMware HA 事件的信息。有关更多信息，请参阅使用日志组获取 Tape Gateway Health CloudWatch 日志使用日志组。 CloudWatch

使用磁带网关存储资源

本节中的主题介绍如何管理与您的磁带网关相关的存储资源，例如连接到网关虚拟主机平台的物理磁盘、连接到网关的 Amazon EC2 实例的 Amazon EBS 卷、介质更换器等虚拟磁带库设备以及虚拟磁带库中的磁带。

主题

- 从网关中移除磁盘：了解如果需要从网关的虚拟主机平台中移除磁盘（例如，如果磁盘发生故障），该怎么做。
- 在亚马逊网关上管理 Amaz EC2 on EBS 卷-了解如何增加或减少分配给托管在 Amazon 实例上的网关的上传缓冲区或缓存存储空间的 Ama EC2 zon EBS 卷的数量。
- 使用 VTL 设备：了解如何管理虚拟磁带库设备，包括如何为磁带网关选择介质更换器、如何更新介质更换器的设备驱动程序，以及如何在 Microsoft System Center Data Protection Manager 中显示磁带的条形码。
- 管理虚拟磁带库中的磁带：了解如何管理与磁带网关关联的磁带和虚拟磁带库，包括如何手动归档磁带和取消正在进行的磁带归档。

从网关中移除磁盘

尽管我们不建议您从网关中移除底层磁盘，但您可能希望从网关中移除磁盘，例如，当您有发生故障的磁盘时。

从托管于的网关中移除磁盘 VMware ESXi

您可以使用以下步骤从 VMware 虚拟机管理程序上托管的网关中移除磁盘。

移除分配给上传缓冲区的磁盘 (VMware ESXi)

1. 在 vSphere 客户端中，打开上下文 (右键单击) 菜单，选择网关 VM 的名称，然后选择 Edit Settings。
2. 在虚拟机属性对话框的硬件选项卡上，选择分配为上传缓冲区空间的磁盘，然后选择移除。

   确认虚拟机属性对话框中的虚拟设备节点值与之前记下的值相同。这样做可帮助确保移除正确的磁盘。
3. 在 Removal Options 面板中选择一个选项，然后选择 OK 以完成移除磁盘的过程。

从托管于 Microsoft Hyper-V 上的网关中移除磁盘

利用以下过程，您可以从托管于 Microsoft Hyper-V 管理程序上的网关中移除磁盘。

移除为上传缓冲区分配的底层磁盘 (Microsoft Hyper-V)

1. 在 Microsoft Hyper-V Manager 中，打开上下文 (右键单击) 菜单，选择网关 VM 的名称，然后选择 Settings。
2. 在设置对话框的硬件列表中，选择要移除的磁盘，然后选择移除。

   添加到网关的磁盘显示在硬件列表的 SCSI 控制器条目下面。确认 Controller (控制器) 和 Location (位置) 值与之前记录的值相同。这样做可帮助确保移除正确的磁盘。

   在 Microsoft Hyper-V Manager 中显示的第一个 SCSI Controller 是控制器 0。
3. 选择 OK 以应用更改。

从托管于 Linux KVM 上的网关中移除磁盘

要将磁盘从基于 Linux 内核的虚拟机 (KVM) 管理程序上托管的网关分离，可以使用类似于以下命令的 `virsh` 命令。

```
$ virsh detach-disk domain_name /device/path
```

有关管理 KVM 磁盘的更多详细信息，请参阅 Linux 发行版的文档。

在亚马逊网关上管理 Amaz EC2 on EBS 卷

当您最初将网关配置为作为 Amazon EC2 实例运行时，您分配了 Amazon EBS 卷用作上传缓冲区和缓存存储空间。由于应用程序需求会随着时间发生变化，因此可分配额外的 Amazon EBS 卷来达到此目的。还可通过删除以前分配的 Amazon EBS 卷来减少已分配的存储。有关亚马逊 EBS 的更多信息，请参阅亚马逊用户指南中的亚马逊 Elastic Block Store (Amazon EBS)。 EC2

在向网关添加更多存储之前，应检查如何根据网关的应用程序需求调整上传缓冲区和缓存存储的大小。为此，请参阅确定要分配的上传缓冲区的大小和确定要分配的缓存存储的大小。

可分配为上传缓冲区和缓存存储的最大存储存在配额。可向实例附加所需数量的 Amazon EBS 卷，但是，将这些卷配置为上传缓冲区和缓存存储空间时必须遵守这些存储配额。有关更多信息，请参阅 Amazon Storage Gateway 配额。

添加 Amazon EBS 卷并为网关配置该卷

1. 创建 Amazon EBS 卷。有关说明，请参阅亚马逊 EC2 用户指南中的创建或恢复 Amaz on EBS 卷。
2. 将 Amazon EBS 卷附加到您的亚马逊 EC2 实例。有关说明，请参阅亚马逊 EC2 用户指南中的将 Amazon EBS 卷附加到实例。
3. 将添加的 Amazon EBS 卷配置为上传缓冲区或缓存存储。有关说明，请参阅 管理 Storage Gateway 的本地磁盘。

有时，可能会发现为上传缓冲区分配的存储量大于需要的存储量。

删除 Amazon EBS 卷

> **Warning**
>
> 这些步骤仅适用于分配为上传缓冲区空间的 Amazon EBS 卷，不适用于分配为缓存的卷。如果从磁带网关中移除分配为缓存存储的 Amazon EBS 卷，则该网关上的虚拟磁带的状态将为“无法恢复”，并且您将面临数据丢失的风险。有关“无法恢复”状态的更多信息，请参阅理解 VTL 中的磁带状态信息。

1. 通过按照关闭网关虚拟机一节中介绍的方法操作，关闭网关。
2. 将 Amazon EBS 卷与您的亚马逊 EC2 实例分离。有关说明，请参阅亚马逊 EC2 用户指南中的将 Amazon EBS 卷与实例分离。
3. 删除 Amazon EBS 卷。有关说明，请参阅亚马逊 EC2 用户指南中的删除 Amazon EBS 卷。
4. 通过按照关闭网关虚拟机一节中介绍的方法操作，启动网关。

使用 VTL 设备

激活 Tape Gateway 时，您可以从列表中选择备份应用程序并使用相应的介质更换器。如果您的备份应用程序未列出，您可以选择 Other，然后选择与备份应用程序结合使用的介质更换器。有关支持的备份应用程序推荐的介质更换器列表，请参见https://docs.amazonaws.cn/storagegateway/latest/tgw/Requirements.html#requirements-backup-sw-for-vtl。

您的磁带网关设置提供以下 iSCSI 设备，您可以在激活网关时选择这些设备。

介质更换器：

- Amazon-Gateway-VTL - 此设备是网关附带的。
- STK-L700 - 此设备模拟是网关附带的。

磁带驱动器：

- IBM-ULT358 0-TD5 —此设备仿真与网关一起提供。

主题

- 在网关激活后选择介质更换器
- 更新介质更换器的设备驱动程序
- 在 Microsoft System Center DPM 中显示磁带的条形码

在网关激活后选择介质更换器

激活网关之后，您可以选择其他介质更换器类型。

在网关激活后选择其他介质更换器类型

1. 停止您的备份软件中运行的任何相关任务。

2. 在 Windows 服务器上，打开 iSCSI 启动程序属性窗口。
3. 选择 Targets 选项卡以显示发现的目标。
4. 在“Discovered targets”窗格中，依次选择要更改的介质更换器、Disconnect 和 OK。
5. 在 Storage Gateway 控制台上，从导航窗格中选择网关，然后选择其介质更换器需要更改的网关。
6. 选择 VTL Devices (VTL 设备) 选项卡，再选择要更改的介质更换器，然后选择 Change Media Changer (更改介质更换器)。
7. 在显示的“Change Media Changer Type”对话框中，从下拉列表框中选择所需的介质更换器，然后选择 Save。

更新介质更换器的设备驱动程序

1. 在您的 Windows 服务器上打开设备管理器，展开 Medium Changer devices (介质更换器设备) 树。
2. 打开 Unknown Medium Changer 的上下文 (右键单击) 菜单，然后选择 Update Driver Software 以打开 Update Driver Software-unknown Medium Changer 窗口。
3. 在 How do you want to search for driver software? (您希望如何搜索驱动程序软件?) 部分中，选择 Browse my computer for driver software (浏览计算机以查找驱动程序软件)。
4. 选择 Let me pick from a list of device drivers on my computer。

> **Note**
>
> 我们建议对 Veeam Backup & Replication 11A 和 Microsoft System Center Data Protection Manager 备份软件使用 Sony TSL-A500C Autoloader 驱动程序。此 Sony 驱动程序已在 Windows Server 2019 及之前版本中针对这些类型的备份软件进行了测试。

5. 在选择要为此硬件安装的设备驱动程序部分中，清除显示兼容的硬件复选框，在制造商列表中选择 Sony，在型号列表中选择 Sony-TSL-A500C Autoloader，然后选择下一步。
6. 在随后显示的警告对话框中，选择 Yes。驱动程序安装成功后，关闭 Update drive software (更新驱动器软件) 窗口。

在 Microsoft System Center DPM 中显示磁带的条形码

如果您使用 Sony TSL-A500C Autoloader 的介质更换器驱动程序，Microsoft System Center Data Protection Manager 不会自动显示在 Storage Gateway 中为虚拟磁带创建的条形码。要正确显示磁带的条形码，请将媒体更换器驱动程序更改为 SunStorageTek /Library。

显示条形码

1. 请确保所有备份作业都已完成，并且没有待处理或正在进行的作业。
2. 弹出磁带并将其转移到脱机存储（S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）中，然后退出 DPM Administrator 控制台。有关如何在 DPM 中弹出磁带的信息，请参阅使用 DPM 将磁带存档。
3. 在管理工具中，选择服务，在详细信息窗格中打开 DPM 服务的上下文（右键单击）菜单，然后选择属性。
4. 在常规选项卡上，确保启动类型设置为自动，选择停止以停止 DPM 服务。
5. 从微软网站上的微软更新目录中获取 StorageTek 驱动程序。

   > **Note**
   >
   > 记下不同大小的不同驱动程序。

   对于 Size (大小) 18K，选择 x86 drivers (x86 驱动程序)。

   对于 Size (大小) 19K，选择 x64 drivers (x64 驱动程序)。
6. 在您的 Windows 服务器上，打开设备管理器，展开介质更换器设备树。
7. 打开 Unknown Medium Changer 的上下文 (右键单击) 菜单，然后选择 Update Driver Software 以打开 Update Driver Software-unknown Medium Changer 窗口。
8. 浏览到新驱动程序位置的路径并安装。驱动程序显示为 Sun/ Libr StorageTek ary。磁带机仍作为 IBM ULT358 0-TD5 SCSI 顺序设备。
9. 重启 DPM 服务器。
10. 在 Storage Gateway 控制台中，创建新磁带。
11. 打开 DPM 管理员控制台，选择 Management (管理)，然后选择 Rescan for new tape libraries (重新扫描新磁带库)。你应该看看 S un/ StorageTek 图书馆。
12. 选择该库，然后选择 Inventory (清单)。

13. 选择 Add Tapes (添加磁带) 以向 DPM 中添加新磁带。新磁带现在应该显示自己的条形码。

管理虚拟磁带库中的磁带

Storage Gateway 为您激活的每个磁带网关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。应用程序可对磁带网关上提供的任何磁带执行读取和写入操作。磁带的状态必须为 AVAILABLE (可用)，您才能对该磁带进行写入操作。这些磁带依赖 Amazon Simple Storage Service (Amazon S3)，也就是说，当您写入这些磁带时，磁带网关会将数据存储在 Amazon S3 中。有关更多信息，请参阅 理解 VTL 中的磁带状态信息。

主题

- 存档磁带
- 取消磁带存档

磁带库显示磁带网关中的磁带。此库显示磁带条码、状态和大小、已使用的磁带大小以及与磁带关联的网关。

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，可按状态和网关进行筛选。

按条码、状态和网关进行搜索

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在导航窗格中，选择 Tapes，然后在搜索框中键入一个值。该值可以是条码、状态或网关。默认情况下，Storage Gateway 会搜索所有虚拟磁带。但是，也可以按状态筛选搜索。

   如果按状态筛选，则 Storage Gateway 控制台中的库中会显示符合条件的磁带。

   如果按网关筛选，则 Storage Gateway 控制台中的库中会显示与该网关关联的磁带。

   > **Note**
   >
   > 默认情况下，Storage Gateway 会显示所有磁带，无论其状态是什么。

存档磁带

您可以将磁带网关中的虚拟磁带存档。将磁带存档时，Storage Gateway 会将磁带移至存档。

要将磁带存档，请使用备份软件。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传输到 VTS、正在存档和已存档：

- 要存档磁带，请使用备份应用程序提供的命令。当存档过程开始时，磁带状态变为正在传输到 VTS，并且备份应用程序无法再访问磁带。在此阶段，您的磁带网关正在将数据上传到 Amazon。如果需要，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。

  > **Note**
  >
  > 磁带存档步骤取决于您的备份应用程序。有关详细说明，请参阅备份应用程序的文档。

- 数据上传 Amazon 完成后，磁带状态更改为存档，Storage Gateway 开始将磁带移至存档。此时无法取消存档过程。
- 将磁带移至存档后，其状态变为已存档，您可以将磁带取回到您的任意网关。有关磁带检索的详细信息，请参阅检索存档的磁带。

磁带存档涉及的步骤取决于您的备份软件。有关如何使用 Symantec NetBackup 软件存档磁带的说明，请参阅存档磁带。

取消磁带存档

开始对磁带进行存档后，您可能会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。正在存档的磁带将经历三种状态，如下所示：

- 正在传输到 VTS：磁带网关正在将数据上传到 Amazon。
- 正在存档：数据上传完毕，磁带网关正在将磁带移至存档。
- 已存档：已移动磁带，且存档可供检索。

仅在磁带的状态为“正在传输到 VTS”时可取消存档。根据上传带宽和所上传的数据量等因素，在 Storage Gateway 控制台中可能看到或看不到此状态。要取消磁带存档，请使用 API 参考中的CancelRetrieval操作。

获取网关的激活密钥

要接收网关的激活密钥，请向网关虚拟机 (VM) 发出 Web 请求。VM 返回包含激活密钥的重定向，激活密钥作为 `ActivateGateway` API 操作的参数之一传递，用于指定网关的配置。有关更多信息，请参阅 Storage Gateway API 参考ActivateGateway中的。

> **Note**
>
> 如果未使用，网关激活密钥将在 30 分钟后过期。

您向网关 VM 发出的请求包括激活发生的 Amazon 区域。响应中重定向返回的 URL 包含称为 `activationkey` 的查询字符串参数。此查询字符串参数是您的激活密钥。此查询字符串的格式如下所示：`http://`*`gateway_ip_address`*`/?activationRegion=`*`activation_region`*。此查询的输出会返回激活区域和密钥。

URL 还包括 `vpcEndpoint`，即使用 VPC 端点类型连接的网关的 VPC 端点 ID。

> **Note**
>
> Storage Gateway 硬件设备、虚拟机映像模板和 EC2 亚马逊系统映像 (AMI) 已预先配置了接收和响应本页所述网络请求所需的 HTTP 服务。不要求也不建议在网关上安装任何其他服务。

主题

- Linux (curl)
- Linux (bash/zsh)
- 微软 Windows PowerShell
- 使用本地控制台

Linux (curl)

以下示例向您显示如何使用 Linux (curl) 获取激活密钥。

> **Note**
>
> 将突出显示的变量替换为您的网关的实际值。可接受的值如下所示：
>
> - *`gateway_ip_address`*-您的网关 IPv4 地址，例如 `172.31.29.201`
> - *`gateway_type`*-您要激活的网关类型，例如`STOREDCACHED`、`VTL`、`FILE_S3`、或`FILE_FSX_SMB`。

- *region_code*-您要激活网关的区域。请参阅《Amazon 一般参考指南》中的区域端点。如果未指定此参数，或者提供的值拼写错误或与有效区域不匹配，则该命令将默认为 us-east-1 区域。
- *vpc_endpoint*-例如，您的网关的 VPC 终端节点名称vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com。

要获取公有端点的激活密钥，请执行以下操作：

```
curl "http://gateway_ip_address/?activationRegion=region_code&no_redirect"
```

要获取 VPC 端点的激活密钥，请执行以下操作：

```
curl "http://gateway_ip_address/?
activationRegion=region_code&vpcEndpoint=vpc_endpoint&no_redirect"
```

Linux (bash/zsh)

以下示例显示如何使用 Linux (bash/zsh) 获取 HTTP 响应、分析 HTTP 标头以及获取激活密钥。

```
function get-activation-key() {
  local ip_address=$1
  local activation_region=$2
  if [[ -z "$ip_address" || -z "$activation_region" || -z "$gateway_type" ]]; then
    echo "Usage: get-activation-key ip_address activation_region gateway_type"
    return 1
  fi

  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region&gatewayType=$gateway_type"); then
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
    echo "$activation_key_param" | cut -f2 -d=
  else
    return 1
  fi
}
```

微软 Windows PowerShell

以下示例向您展示了如何使用 Microsoft Windows PowerShell 获取 HTTP 响应、解析 HTTP 标头和获取激活密钥。

```
function Get-ActivationKey {
  [CmdletBinding()]
  Param(
    [parameter(Mandatory=$true)][string]$IpAddress,
    [parameter(Mandatory=$true)][string]$ActivationRegion,
    [parameter(Mandatory=$true)][string]$GatewayType
  )
  PROCESS {
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion&gatewayType=$GatewayType" -MaximumRedirection 0 -
ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

使用本地控制台

以下示例显示了如何使用本地控制台来生成和显示激活密钥。

从本地控制台获取网关的激活密钥

1. 登录到本地控制台。如果您是从 Windows 计算机连接到您的亚马逊 EC2 实例，请以管理员身份登录。
2. 登录并查看 Amazon 设备激活 - 配置主菜单后，选择 0 来选择获取激活密钥。
3. 选择 Storage Gateway 作为网关系列选项。
4. 出现提示时，输入要激活网关的 Amazon 区域。
5. 对于公有端点，输入 1，或对于 VPC 端点，输入 2 作为网络类型。
6. 对于标准端点，输入 1，或对于美国联邦信息处理标准 (FIPS) 端点，输入 2 作为端点类型。

连接 iSCSI 启动程序

在管理网关时，您将使用作为 Internet 小型计算机系统接口 (iSCSI) 目标公开的卷或虚拟磁带库 (VTL) 设备。对于卷网关，iSCSI 目标是卷。对于磁带网关，目标为 VTL 设备。作为此工作的一部分，您将执行以下任务：连接到这些目标、自定义 iSCSI 设置、从 Red Hat Linux 客户端进行连接以及配置质询握手身份验证协议 (CHAP)。

主题

- 将 VTL 设备连接到 Windows 客户端
- 将 VTL 设备连接到 Linux 客户端
- 自定义 iSCSI 设置
- 为 iSCSI 目标配置 CHAP 身份验证

iSCSI 标准是一种基于互联网协议 (IP) 的存储网络标准，该标准用于启动和管理基于 IP 的存储设备与客户端之间的连接。以下列表定义了用来描述 iSCSI 连接和相关组件的一些术语。

iSCSI 启动程序

iSCSI 网络的客户端组件。启动程序向 iSCSI 目标发送请求。可以在软件或硬件中实施启动程序。Storage Gateway 仅支持软件启动程序。

iSCSI 目标

iSCSI 网络的服务器组件，接收并响应来自启动程序的请求。每个卷均作为一个 iSCSI 目标公开。仅对每个 iSCSI 目标连接一个 iSCSI 启动程序。

Microsoft iSCSI 启动程序

Microsoft Windows 计算机上的软件程序，让您可以将客户端计算机（即运行您希望将其数据写入网关的应用程序的计算机）连接到基于 iSCSI 的外部阵列（即网关）。使用主机的以太网网络适配卡建立此连接。微软 iSCSI 启动器已在 Windows Server 2022 上通过 Storage Gateway 进行验证。启动器内置在操作系统中。

Red Hat iSCSI 启动程序

`iscsi-initiator-utils` 资源包管理器 (RPM) 程序包为您提供了在适用于 Red Hat Linux 的软件中实施的 iSCSI 启动程序。该包含有用于 iSCSI 协议的服务器守护进程。

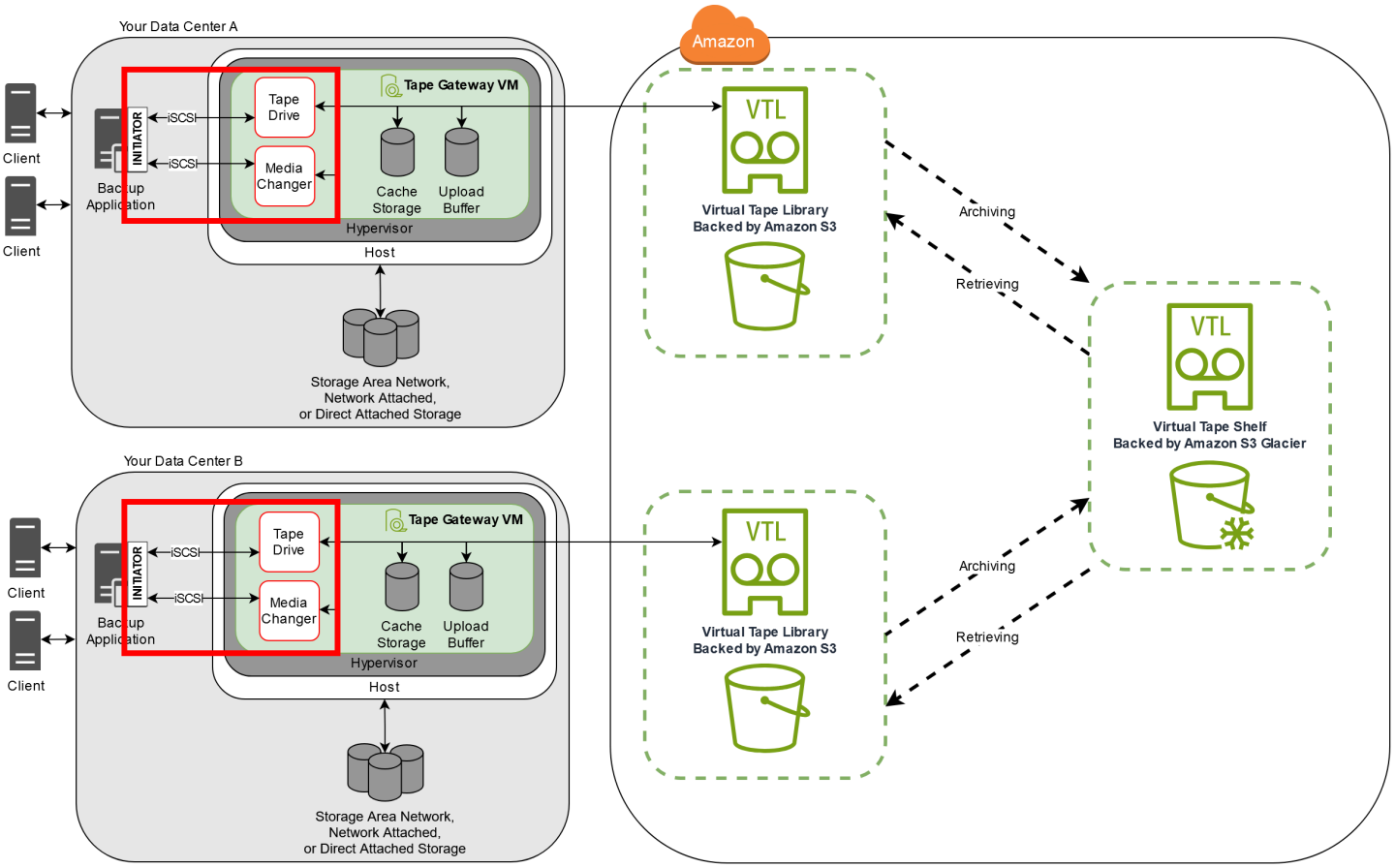
每种类型的网关都可以连接到 iSCSI 设备，而您可以自定义这些连接，如下所述。

将 VTL 设备连接到 Windows 客户端

磁带网关将若干磁带驱动器和一个介质更换器（统称为 VTL 设备）作为 iSCSI 目标公开。有关更多信息，请参阅 设置磁带网关的要求。

> **Note**
>
> 您向每个 iSCSI 目标仅连接一个应用程序。

下图在 Storage Gateway 架构的大图中突出显示了 iSCSI 目标。有关 Storage Gateway 架构的更多信息，请参阅磁带网关的工作原理（架构）。



将 Windows 客户端连接到 VTL 设备

1. 在 Windows 客户端计算机的开始菜单上，在搜索程序和文件框中输入 **`iscsicpl.exe`**，找到 iSCSI 启动程序，然后运行它。

> **Note**
>
> 必须具有客户端计算机上的管理员权限才能运行 iSCSI 启动程序。

2. 如果出现提示，则单击 Yes 以启动 Microsoft iSCSI 启动程序服务。
3. 在 iSCSI Initiator Properties (iSCSI 发起程序属性) 对话框中，选择 Discovery (发现) 选项卡，然后选择 Discover Portal (发现门户)。
4. 在发现目标门户对话框的 IP 地址或 DNS 名称中输入磁带网关的 IP 地址，然后选择确定。要获取网关的 IP 地址，请查看 Storage Gateway 控制台上的网关选项卡。如果您在亚马逊 EC2 实例上部署了网关，则可以在亚马逊 EC2 控制台的描述选项卡中找到公有 IP 或 DNS 地址。

> **Warning**
>
> 对于部署在 Amazon EC2 实例上的网关，不支持通过公共互联网连接访问网关。Amazon EC2 实例的弹性 IP 地址不能用作目标地址。

5. 选择 Targets (目标) 选项卡，然后选择 Refresh (刷新)。发现的目标框中会显示所有 10 个磁带驱动器和介质更换器。目标的状态为 Inactive (不活动)。
6. 选择第一个设备，然后选择 Connect。一次连接一个设备。
7. 在 Connect to Target 对话框中，选择 OK。
8. 对每台设备重复步骤 6 和 7 来连接所有设备，然后在 iSCSI 启动程序属性对话框中选择确定。

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，并在必要时更新驱动程序和提供商。

验证驱动程序提供商并在必要时更新 Windows 客户端上的提供程序和驱动程序

1. 在 Windows 客户端上，启动“设备管理器”。
2. 展开 Tape drives，选择磁带驱动器的上下文 (右键单击) 菜单，然后选择 Properties。
3. 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。
4. 如果驱动程序提供商不是 Microsoft，则按如下方式设置值：
   a. 选择 Update Driver (更新驱动程序)。
   b. 在 Update Driver Software (更新驱动程序软件) 对话框中，选择 Browse my computer for driver software (浏览计算机以查找驱动程序软件)。

c. 在 Update Driver Software (更新驱动程序软件) 对话框中，选择 Let me pick from a list of device drivers on my computer (从计算机的设备驱动程序列表中选取)。

d. 选择 LTO Tape drive，然后选择 Next。

e. 选择关闭来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置为 Microsoft。

5. 重复步骤 4.1 到 4.5 以更新所有磁带驱动器。

将 VTL 设备连接到 Linux 客户端

使用 Red Hat Enterprise Linux (RHEL) 时，应使用 `iscsi-initiator-utils` RPM 程序包连接到网关 iSCSI 目标（卷或 VTL 设备）。

将 Linux 客户端连接到 iSCSI 目标

1. 如果尚未在您的客户端上安装 `iscsi-initiator-utils` RPM 程序包，请安装程序包。

   您可以使用下面的命令来安装该包。

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

2. 确保 iSCSI 守护进程正在运行。

   a. 使用下以下命令之一验证 iSCSI 守护进程是否正在运行。

      对于 RHEL 8 或 9，请使用以下命令。

      ```
      sudo service iscsid status
      ```

   b. 如果 status 命令未返回 running 状态，则使用以下命令之一启动守护程序。

      对于 RHEL 8 或 9，请使用以下命令。您通常不需要显式启动该`iscsid`服务。

      ```
      sudo service iscsid start
      ```

3. 要发现为网关定义的卷目标或 VTL 设备目标，请使用以下发现命令。

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

   用网关的 IP 地址代替前面命令中的*[GATEWAY_IP]*变量。您可以在 Storage Gateway 控制台上某个卷的 iSCSI 目标信息属性中找到网关 IP。

发现命令的输出内容类似如下示例输出内容。

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

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

您的 iSCSI 限定名称 (IQN) 与以上所示不同，因为每个组织的 IQN 值不同。目标名称是您创建卷时指定的名称。在 Storage Gateway 控制台上选择某个卷时，也可以在 iSCSI 目标信息属性窗格中找到此目标名称。

4. 要连接到目标，请使用以下命令。

请注意，您需要在 connect 命令中指定正确的*[GATEWAY_IP]*和 IQN。

> **Warning**
>
> 对于部署在 Amazon EC2 实例上的网关，不支持通过公共互联网连接访问网关。Amazon EC2 实例的弹性 IP 地址不能用作目标地址。

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

5. 要确认卷已附加到客户端 (启动程序)，请使用以下命令。

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

命令的输出如下面的示例输出所示。

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

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

自定义 iSCSI 设置

我们强烈建议您在设置启动程序后，自定义 iSCSI 设置以防止启动程序从目标断开。

通过增大下列步骤中所示的 iSCSI 超时值，您可以提高应用程序对需要较长时间的写入操作以及网络中断等其他瞬态问题的处理能力。

> **Note**
>
> 修改注册表前，您应该制作一份该注册表的备份副本。有关制作备份副本的信息以及使用注册表时应遵循的其他最佳做法，请参阅 Microsoft TechNet 库中的注册表最佳做法。

主题

- 自定义您的 Windows iSCSI 设置
- 自定义您的 Linux iSCSI 设置

自定义您的 Windows iSCSI 设置

对于磁带网关设置，使用 Microsoft iSCSI 启动程序连接 VTL 设备是一个两步过程：

1. 将您的磁带网关设备连接到 Windows 客户端。
2. 如果要使用备份应用程序，则将该应用程序配置为使用这些设备。

本入门示例设置提供对这两个步骤的说明。它使用赛门铁克 NetBackup 备份应用程序。有关更多信息，请参阅连接 VTL 设备 和配置 NetBackup 存储设备。

如需自定义您的 Windows iSCSI 设置

1. 提高请求排队的最长时间。

   a. 启动注册表编辑器 (`Regedit.exe`)。

   b. 导航到设备类别的全局唯一标识符 (GUID) 密钥，其中包含 iSCSI 控制器设置，如下所示。

> **Warning**
>
> 确保您使用的是CurrentControlSet子键而不是其他控件集，例如 00 ControlSet1 或 ControlSet00 2。

```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}
```

c. 找到微软 iSCSI 启动器的子密钥，如下所示。*[<Instance Number]*

该项由四位数字表示，如 `0000`。

```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\[<Instance Number]
```

根据计算机上安装的内容，Microsoft iSCSI 启动程序可能不是子项 `0000`。可以通过验证字符串 `DriverDesc` 是否具有 `Microsoft iSCSI Initiator` 值来确保选择了正确的子项。

d. 要显示 iSCSI 设置，请选择 Parameters (参数) 子项。

e. 打开 MaxRequestHoldTimeDWORD（32 位）值的上下文（右键单击）菜单，选择“修改”，然后将该值更改为。**`600`**

MaxRequestHoldTime指定在通知上层事件之前，Microsoft iSCSI 启动器应保留多长时间并重试未完成的命令。`Device Removal`该值表示 600 秒的保持时间。

2. 通过修改以下参数，可以提高可在 iSCSI 数据包中发送的最大数据量：

- FirstBurstLength控制在未经请求的写入请求中可以传输的最大数据量。将此值设置为 **`262144`** 或 Windows 操作系统的默认值，以较高者为准。
- MaxBurstLength类似于 FirstBurstLength，但它设置了在请求的写入序列中可以传输的最大数据量。将此值设置为 **`1048576`** 或 Windows 操作系统的默认值，以较高者为准。
- MaxRecvDataSegmentLength控制与单个协议数据单元 (PDU) 关联的最大数据段大小。将此值设置为 **`262144`** 或 Windows 操作系统的默认值，以较高者为准。

> **Note**
>
> 不同的备份软件可使用不同的 iSCSI 设置进行优化来达到最佳效果。要确认如何设置这些参数的值才能提供最佳性能，请参阅备份软件的文档。

3. 增大磁盘超时值，如下所示：

a. 如果您尚未启动注册表编辑器 (`Regedit.exe`)，请将其启动。

b. 导航到“服务”子项中的“磁盘”子项 CurrentControlSet，如下所示。

```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Services\Disk
```

c. 打开 TimeOutValueDWORD（32 位）值的上下文（右键单击）菜单，选择 “修改”，然后将该值更改为。**600**

TimeOutValue指定 iSCSI 启动器在尝试通过断开并重新建立连接来恢复会话之前，将等待目标的响应多少秒。该值表示 600 秒的超时期间。

4. 要确保新配置的值生效，请重新启动系统。

重新启动之前，必须确保刷新了对卷进行的所有写入操作的结果。要这样做，请在重启前将任何映射的存储卷磁盘脱机。

自定义您的 Linux iSCSI 设置

为网关设置启动程序后，我们强烈建议您自定义 iSCSI 设置以防止启动程序从目标断开。通过增大下面所示的 iSCSI 超时值，您可以提高应用程序对需要较长时间的写入操作以及网络中断等其他瞬态问题的处理能力。

> **Note**
>
> 命令可能与 Linux 的其他命令类型略有不同。以下示例基于 Red Hat Linux。

如需自定义您的 Linux iSCSI 设置

1. 提高请求排队的最长时间。

a. 打开 `/etc/iscsi/iscsid.conf` 文件，然后找到以下各行。

```
node.session.timeo.replacement_timeout = [replacement_timeout_value]
node.conn[0].timeo.noop_out_interval = [noop_out_interval_value]
node.conn[0].timeo.noop_out_timeout = [noop_out_timeout_value]
```

b. 将该*[replacement_timeout_value]*值设置为**600**。

将该*[noop_out_interval_value]*值设置为**60**。

将该*[noop_out_timeout_value]*值设置为**600**。

这三种值的单位均为秒。

> **Note**
>
> 必须在发现网关之前进行 iscsid.conf 设置。如果已发现网关和/或已登录到目标，则可使用以下命令从发现数据库中删除该项。然后可以重新发现或登录，从而使新设置生效。
>
> ```
> iscsiadm -m discoverydb -t sendtargets -p [GATEWAY_IP]:3260 -o delete
> ```

2. 提高可在每个响应中传输的最大数据量。

   a. 打开 /etc/iscsi/iscsid.conf 文件，然后找到以下各行。

   ```
   node.session.iscsi.FirstBurstLength = [replacement_first_burst_length_value]
   node.session.iscsi.MaxBurstLength = [replacement_max_burst_length_value]
   node.conn[0].iscsi.MaxRecvDataSegmentLength
    = [replacement_segment_length_value]
   ```

   b. 我们建议使用以下值，以实现更佳性能。您的备份软件可以使用不同的值进行优化，因此请参阅备份软件文档了解最佳效果。

   将该*[replacement_first_burst_length_value]*值设置为**262144**或 Linux 操作系统的默认值，以较高者为准。

   将该*[replacement_max_burst_length_value]*值设置为**1048576**或 Linux 操作系统的默认值，以较高者为准。

   将该*[replacement_segment_length_value]*值设置为**262144**或 Linux 操作系统的默认值，以较高者为准。

   > **Note**
   >
   > 不同的备份软件可使用不同的 iSCSI 设置进行优化来达到最佳效果。要确认如何设置这些参数的值才能提供最佳性能，请参阅备份软件的文档。

3. 重启系统以确保新配置的值生效。

重新启动之前，确保刷新了对卷进行的所有写入操作的结果。为此，请在重新启动之前卸载磁带。

为 iSCSI 目标配置 CHAP 身份验证

Storage Gateway 支持使用质询握手身份验证协议 (CHAP) 在网关和 iSCSI 启动程序之间进行身份验证。CHAP 通过定期验证 iSCSI 启动程序的身份是否具有访问卷目标和 VTL 设备目标的权限来预防反演攻击。

> **Note**
>
> CHAP 配置是可选的，但强烈推荐进行此配置。

要设置 CHAP，必须在 Storage Gateway 控制台和用于连接目标的 iSCSI 启动程序软件中对其进行配置。Storage Gateway 使用双方 CHAP，即启动程序对目标进行身份验证，目标对启动程序进行身份验证。

为目标设置双向 CHAP

1. 在 Storage Gateway 控制台上配置 CHAP，如 在 Storage Gateway 控制台上为 VTL 设备目标配置 CHAP 中所述。
2. 在客户端启动程序软件中，完成 CHAP 配置：
   - 要在 Windows 客户端上配置双向 CHAP，请参阅 在 Windows 客户端上配置双向 CHAP。。
   - 要在 Red Hat Linux 客户端上配置双向 CHAP，请参阅 如需在 Red Hat Linux 客户端上配置双向 CHAP。

在 Storage Gateway 控制台上为 VTL 设备目标配置 CHAP

在本步骤中，您指定两个用来读取和写入虚拟磁带的私有密钥。这两个密钥也用来在本步骤中配置客户端启动程序。

1. 在导航窗格中，选择网关。
2. 选择您的网关，然后选择 VTL Devices 选项卡以显示您的所有 VTL 设备。
3. 选择要为其配置 CHAP 的设备。
4. 在配置 CHAP 身份验证对话框中提供要求的信息。

a. 对于启动程序名称，请输入 iSCSI 启动程序的名称。此名称是 Amazon iSCSI 限定名称 (IQN)，前面加上 `iqn.1997-05.com.amazon:`，后跟目标名称。示例如下：

   `iqn.1997-05.com.amazon:`*`your-tape-device-name`*

   您可以使用 iSCSI 启动程序软件找到启动程序名称。例如，对于 Windows 客户端，该名称为 iSCSI 启动程序的 Configuration (配置) 选项卡上的值。有关更多信息，请参阅 在 Windows 客户端上配置双向 CHAP。。

   > **Note**
   >
   > 如需更改启动程序名称，您必须先停用 CHAP，在 iSCSI 启动程序软件中更改启动程序名称，然后使用新名称激活 CHAP。

b. 对于用于对启动程序进行身份验证的密钥，输入要求的密钥。

   此私有密钥的长度最少为 12 个字符，最多为 16 个字符。此值是私有密钥，启动程序 (即 Windows 客户端) 必须知道该私有密钥才能参与到与目标的 CHAP 中。

c. 对于用于对目标进行身份验证的密钥（双向 CHAP），输入要求的密钥。

   此私有密钥的长度最少为 12 个字符，最多为 16 个字符。目标必须知道此值才能参与到与启动程序的 CHAP 中。

   > **Note**
   >
   > 用来验证目标身份的私有密钥必须不同于用来验证启动程序的私有密钥。

d. 选择保存。

5. 在 VTL Devices 选项卡上，确认 iSCSI CHAP 身份验证字段设置为 true。

在 Windows 客户端上配置双向 CHAP。

在此过程中，您使用在控制台中为卷配置 CHAP 所用的同一密钥在 Microsoft iSCSI 启动程序中配置 CHAP。

1. 如果 iSCSI 启动程序尚未启动，请在 Windows 客户端计算机的开始菜单上，选择运行，输入 **`iscsicpl.exe`**，然后选择确定来运行该程序。
2. 为启动程序 (即 Windows 客户端) 配置双向 CHAP 配置：

a. 选择配置选项卡。

> **Note**
>
> Initiator Name 值对于您的启动程序和公司是唯一的。前面显示的名称是您在 Storage Gateway 控制台的配置 CHAP 身份验证对话框中使用的值。
> 示例图像中所示名称仅作示范用途。

b. 选择 CHAP。

c. 在 iSCSI 启动程序双向 CHAP 密钥对话框中，输入双向 CHAP 密钥值。

在此对话框中，输入启动程序 (Windows 客户端) 用来对目标 (存储卷) 进行身份验证的私有密钥。该私有密钥允许目标读取并写入启动程序。此密钥与在配置 CHAP 身份验证对话框的用于对目标进行身份验证的密钥（双向 CHAP）框中输入的密钥相同。有关更多信息，请参阅为 iSCSI 目标配置 CHAP 身份验证。

d. 如果您输入的密钥少于 12 个字符或多于 16 个字符，则会显示启动程序 CHAP 密钥错误对话框。

选择确定，然后重新输入密钥。

3. 使用启动程序的密钥进行配置，完成双向 CHAP 配置。

a. 选择目标选项卡。

b. 如果当前连接了要为 CHAP 配置的目标，则通过选择该目标并选择 Disconnect 来断开该目标。

c. 选择要为 CHAP 配置的目标，然后选择 Connect。

d. 在 Connect to Target 对话框中，选择 Advanced。

e. 在“Advanced Settings”对话框中，配置 CHAP。

i. 选择激活 CHAP 登录。

ii. 输入验证启动程序所需的密钥。此密钥与在配置 CHAP 身份验证对话框的用于对启动程序进行身份验证的密钥框中输入的密钥相同。有关更多信息，请参阅为 iSCSI 目标配置 CHAP 身份验证。

iii. 选择“Perform mutual authentication”。

iv. 要应用更改，请选择 OK。

f. 在 Connect to Target 对话框中，选择 OK。

4. 如果提供的私有密钥正确无误，则目标将显示 Connected (已连接) 状态。

如需在 Red Hat Linux 客户端上配置双向 CHAP

在此过程中，您使用在 Storage Gateway 控制台中为卷配置 CHAP 所用的同一密钥在 Linux iSCSI 启动程序中配置 CHAP。

1. 确保 iSCSI 守护进程正在运行并且您已连接到目标。如果您尚未完成这两项任务，请参阅连接到 Linux 客户端。
2. 断开并移除您即将为其配置 CHAP 的目标的任何现有配置。

   a. 要查找目标名称并确保其为定义的配置，请使用以下命令列出保存的配置。

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

   b. 从目标断开。

   以下命令从 Amazon iSCSI 限定名称 (IQN) 中定义的名为 **myvolume** 的目标断开连接。按您的需求情况更改目标名称和 IQN。

   ```
   sudo /sbin/iscsiadm --mode node --logout GATEWAY_IP:3260,1
    iqn.1997-05.com.amazon:myvolume
   ```

   c. 移除目标的配置。

   下面的命令移除 **myvolume** 目标的配置。

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

3. 编辑 iSCSI 配置文件来激活 CHAP。

   a. 获取启动程序 (即您正在使用的客户端) 的名称。

   以下命令从文件 `/etc/iscsi/initiatorname.iscsi` 获取发起程序名称。

   ```
   sudo cat /etc/iscsi/initiatorname.iscsi
   ```

   该命令的输出内容类似于以下内容：

```
InitiatorName=iqn.1994-05.com.redhat:8e89b27b5b8
```

b. 打开 /etc/iscsi/iscsid.conf文件。

c. 取消文件中以下各行的注释，并为*username*、*passwordusername_in*、和*password_in*指定正确的值。

```
node.session.auth.authmethod = CHAP
node.session.auth.username = username
node.session.auth.password = password
node.session.auth.username_in = username_in
node.session.auth.password_in = password_in
```

有关要指定的值的指南，请参阅下表。

配置设置	值
username	您在此过程中的上一步中找到的启动程序名称。该值以 iqn 开头。例如，**iqn.1994-05.com.redhat:8e89b27b5b8** 是一个有效*username*值。
password	用于在启动程序 (您正在使用的客户端) 与卷通信时对启动程序进行身份验证的私有密钥。
username_in	目标卷的 IQN。该值以 iqn 开头，以目标名称结尾。例如，**iqn.1997-05.com.amazon:myvolume** 是一个有效*username_in* 值。
password_in	用于在目标 (卷) 与启动程序通信时对目标进行身份验证的私有密钥。

d. 保存配置文件中的更改，然后关闭该文件。

4. 发现并登录到目标。为此，请按照连接到 Linux 客户端中的步骤进行操作。

Amazon Direct Connect 与 Storage Gateway 一起使用

Amazon Direct Connect 将您的内部网络链接到亚马逊 Web Services 云。通过 Amazon Direct Connect 与 Storage Gateway 配合使用，您可以创建满足高吞吐量工作负载需求的连接，从而在本地网关和 Amazon之间提供专用的网络连接。

Storage Gateway 使用公有端点。 Amazon Direct Connect 建立连接后，您可以创建一个公共虚拟接口，以允许将流量路由到 Storage Gateway 端点。该公共虚拟接口将绕过您的网络路径中的 Internet 服务提供商。Storage Gateway 服务的公共终端节点可以与该 Amazon Direct Connect 位置位于同一个 Amazon 区域，也可以位于不同的 Amazon 区域。

下图显示了如何 Amazon Direct Connect 使用 Storage Gateway 的示例。
网络架构显示 Storage Gateway 使用 Amazon 直接连接连接到云端。

以下过程假定您已创建正常运行的网关。

Amazon Direct Connect 与 Storage Gateway 配合使用

1. 在您的本地数据中心和 Storage Gateway 终端节点之间创建并建立 Amazon Direct Connect 连接。有关如何创建连接的更多信息，请参阅《Amazon Direct Connect 用户指南》中的 Amazon Direct Connect入门。
2. 将您的本地 Storage Gateway 设备连接到 Amazon Direct Connect 路由器。
3. 创建一个公共虚拟接口，然后相应地配置您的本地路由器。即使使用 Direct Connect，也必须使用创建 VPC 终端节点 HAProxy。有关更多信息，请参阅《Amazon Direct Connect 用户指南》中的创建虚拟接口。

有关的详细信息 Amazon Direct Connect，请参阅什么是 Amazon Direct Connect？ 在《Amazon Direct Connect 用户指南》中。

获取网关设备的 IP 地址

在选择主机并部署网关 VM 后，您可以连接并激活网关。为此，需要使用网关 VM 的 IP 地址。您可以从网关的本地控制台获取 IP 地址。您可以登录到本地控制台并从控制台页面顶部获取 IP 地址。

对于本地部署的网关，您也可以从管理程序获取 IP 地址。对于亚马逊 EC2 网关，您还可以从亚马逊 EC2管理控制台获取您的亚马逊 EC2 实例的 IP 地址。要了解如何获取网关的 IP 地址，请参阅以下内容之一：

- VMware 主持人：使用访问网关本地控制台 VMware ESXi
- HyperV 主机：使用 Microsoft Hyper-V 访问网关本地控制台
- 基于 Linux 内核的虚拟机 (KVM) 主机：使用 Linux KVM 访问网关本地控制台
- EC2 主持人：从 Amazon EC2 主机获取 IP 地址

找到 IP 地址之后，请记下它。然后返回到 Storage Gateway 控制台并在控制台中键入该 IP 地址。

从 Amazon EC2 主机获取 IP 地址

要获取部署网关的 Amazon EC2 实例的 IP 地址，请登录该 EC2 实例的本地控制台。然后从控制台页面顶部获取 IP 地址。有关说明，请参阅 登录您的 Amazon EC2 Gateway 本地控制台。

您也可以从亚马逊 EC2 管理控制台获取 IP 地址。我们建议使用公有 IP 地址进行激活。要获取公有 IP 地址，请使用程序 1。如果您选择使用弹性 IP 地址，请参阅程序 2。

程序 1：使用公有 IP 地址连接到网关

1. 打开亚马逊 EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例，然后选择部署网关的 EC2 实例。
3. 选择底部的 Description (描述) 选项卡，然后记下公有 IP 地址。您可以使用此 IP 地址连接到网关。返回到 Storage Gateway 控制台并键入该 IP 地址。

如果您想使用弹性 IP 地址进行激活，可使用以下程序。

程序 2：使用弹性 IP 地址连接到网关

1. 打开亚马逊 EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例，然后选择部署网关的 EC2 实例。
3. 选择底部的 Description (描述) 选项卡，然后记下 Elastic IP (弹性 IP) 值。您可以使用此弹性 IP 地址连接到网关。返回到 Storage Gateway 控制台并键入弹性 IP 地址。
4. 激活网关之后，选择刚刚激活的网关，然后选择底部面板中的 VTL devices (VTL 设备) 选项卡。
5. 获取您的所有 VTL 设备的名称。
6. 对于每个目标，运行以下命令以配置目标。

```
iscsiadm -m node -o new -T [$TARGET_NAME] -p [$Elastic_IP]:3260
```

7. 对于每个目标，运行以下命令以登录。

```
iscsiadm -m node -p [$ELASTIC_IP]:3260 --login
```

现在，您的网关已使用 EC2实例的弹性 IP 地址进行连接。

了解 Storage Gateway 资源和资源 IDs

在 Storage Gateway 中，主要资源是网关，而其他资源类型包括：卷、虚拟磁带、iSCSI 目标和 vtl 设备。这些称为子资源，除非它们与网关关联，否则视为不存在。

这些资源和子资源具有与之关联的唯一 Amazon 资源名称 (ARNs)，如下表所示。

资源类型	ARN 格式
网关 ARN	arn:aws:storagegateway: *region*:*account-id* :gateway/ *gateway-id*
磁带 ARN	arn:aws:storagegateway: *region*:*account-id* :tape/*tapebarcode*
目标 ARN (iSCSI 目标)	arn:aws:storagegateway: *region*:*account-id* :gateway/ *gateway-id* /target/*iSCSItarget*
VTL 设备 ARN	arn:aws:storagegateway: *region*:*account-id* :gateway/ *gateway-id* /device/*vtldevice*

Storage Gateway 还支持使用 EC2 实例、EBS 卷和快照。这些资源是在 Storage Gateway 中使用的亚马逊 EC2 资源。

使用资源 IDs

在您创建某个资源时，Storage Gateway 会为该资源分配一个唯一资源 ID。此资源 ID 是资源 ARN 的一部分。资源 ID 采用以下格式：资源标识符后跟连字符，然后是 8 个字母与数字的唯一组合。例如，网关 ID 的格式为 `sgw-12A3456B`，其中 `sgw` 是网关的资源标识符。卷 ID 的格式为 `vol-3344CCDD`，其中 `vol` 是卷的资源标识符。

对于虚拟磁带，可以为条码 ID 追加最多 4 字符前缀，以帮助您整理磁带。

Storage Gateway 资源 IDs 使用大写字母。但是，当您将这些资源 IDs 与 Amazon EC2 API 一起使用时，亚马逊 EC2 需要使用小写 IDs 的资源。您必须将资源 ID 更改为小写才能在 EC2 API 中使用。例

如，在 Storage Gateway 中，卷的 ID 可能为 `vol-1122AABB`。在 EC2 API 中使用此 ID 时，必须将其更改为`vol-1122aabb`。否则， EC2 API 可能无法按预期运行。

标记 Storage Gateway 资源

在 Storage Gateway 中，您可以使用标签来管理资源。利用标签，您可以向资源添加元数据和对资源分类，以便更轻松地管理它们。每个标签都包含您定义的一个键-值对。您可以向网关、卷和虚拟磁带添加标签。您可以根据添加的标签搜索和筛选这些资源。

例如，您可以使用这些标签标识组织中的每个部门使用的 Storage Gateway 资源。您可能为会计部使用的网关和卷添加类似于下面的标签： (`key=department` 和 `value=accounting`)。然后，您可以使用此标签进行筛选，以便标识会计部使用的所有网关和卷并使用此信息确定成本。有关更多信息，请参阅使用成本分配标签和使用标签编辑器。

如果您存档了一个已标记的虚拟磁带，则该磁带将在存档中保留其标签。同样，如果您将磁带从存档取回到另一网关，则该标记将保留在新网关中。

标签没有任何语义意义，应作为字符串进行解析。

以下限制适用于标签：

- 标签键和值区分大小写。
- 每个资源的最大标签数是 50。
- 标签键不能以 `aws:` 开头。此前缀是专为 Amazon 使用而预留。
- 键属性的有效字符包括 UTF-8 字母和数字、空格以及特殊字符 +、-、=、.、_、:、/ 和 @。

使用标签

您可以使用 Storage Gateway 控制台、Storage Gateway API 或 Storage Gateway 命令行界面 (CLI) 处理标签。下面的过程介绍如何在控制台上添加、编辑和删除标签。

添加标签

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 在导航窗格中，选择要标记的资源。

   例如，要标记网关，请选择 Gateways，然后从网关列表中选择要标记的网关。
3. 选择 Tags，然后选择 Add/edit tags。

4. 在 Add/edit tags 对话框中，选择 Create tag。
5. 为 Key 键入密钥，为 Value 键入值。例如，您可以键入 **`Department`** 作为密钥，并键入 **`Accounting`** 作为值。

   > **Note**
   >
   > 您可以将 Value 框留空。

6. 选择 Create Tag 以添加更多标签。您可以向资源添加多个标签。
7. 添加完标签后，选择 Save。

编辑标签

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 选择要编辑其标签的资源。
3. 选择 Tags 以打开 Add/edit tags 对话框。
4. 选择要编辑的标签旁的铅笔图标，然后编辑该标签。
5. 编辑完标签后，选择 Save。

删除标签

1. 在https://console.aws.amazon.com/storagegateway/家中打开 Storage Gateway 控制台。
2. 选择要删除其标签的资源。
3. 选择 Tags，然后选择 Add/edit tags 以打开 Add/edit tags 对话框。
4. 选择要删除的标签旁边的 X 图标，然后选择 Save。

使用 Storage Gateway 的开源组件

本节介绍我们在提供 Storage Gateway 功能时所依赖的第三方工具和许可证。

可在以下网址下载 Amazon Storage Gateway 软件附带的某些开源软件组件的源代码：

- 对于部署在上的网关 VMware ESXi，请下载 sources.tar
- 对在 Microsoft Hyper-V 上部署的网关，请下载 sources_hyperv.tar
- 对在基于 Linux 内核的虚拟机 (KVM) 上部署的网关，请下载 sources_KVM.tar

该产品包括 OpenSSL Project 为在 OpenSSL Toolkit 中使用而开发的软件 (http://www.openssl.org/)。有关所有依赖的第三方工具的相关许可证，请参阅第三方许可证。

Amazon Storage Gateway 配额

在本主题中，您可找到有关 Storage Gateway 的卷和磁带配额、配置和性能限制的信息。

主题

- 磁带的配额
- 为网关建议的本地磁盘大小

磁带的配额

下表列出了磁带的配额。

描述	磁带网关
虚拟磁带的最小大小	100GiB
虚拟磁带的最大大小	15 TiB
分配给网关的虚拟磁带的最大数量	1500
分配给网关的所有磁带的总大小	1 PiB
存档中虚拟磁带的最大数量	无限制
存档中所有磁带的总大小	无限制

为网关建议的本地磁盘大小

下表为所部署的网关推荐了本地磁盘存储的大小。

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

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

Storage Gateway 的 API 参考

除了使用控制台外，您还可以使用 Amazon Storage Gateway API 以编程方式配置和管理您的网关。本节介绍 Amazon Storage Gateway 操作、身份验证请求签名和错误处理。有关 Storage Gateway 可用的区域和端点的信息，请参阅《Amazon Web Services 一般参考》中的 Amazon Storage Gateway 端点和配额。

> **Note**
>
> 在开发应用程序 Amazon SDKs 时，也可以使用 Amazon Storage Gateway。 Amazon SDKs 适用于 Java、.NET 和 PHP 的 API 封装了底层 Amazon Storage Gateway API，从而简化了您的编程任务。有关下载开发工具包库的信息，请参阅示例代码库。

主题

- Storage Gateway 必需的请求标头
- 对请求进行签名
- 错误响应
- 操作

Storage Gateway 必需的请求标头

本部分描述您每次向 Storage Gateway 发送 POST 请求时必须使用的标头。您将 HTTP 标头包含在内以识别有关请求的密钥信息，包括您希望调用的操作、请求的日期以及表示您拥有请求发送者授权的信息。标头区分大小写，其次序不重要。

以下示例显示了ActivateGateway操作中使用的标头。

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120425/us-east-2/
storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target,
 Signature=9cd5a3584d1d67d57e61f120f35102d6b3649066abdd4bf4bbcf05bd9f2f8fe2
```

```
x-amz-date: 20120912T120000Z
x-amz-target: StorageGateway_20120630.ActivateGateway
```

以下是必须包含在向 Storage Gateway 发送的 POST 请求中的标头。下面显示的以 “x-amz” 开头的标题是 Amazon特定标题。列出的其他所有标头均为 HTTP 事务中使用的普通标头。

标题	描述
`Authorization`	授权标头包含有关请求的数种信息，这些信息可以让 Storage Gateway 确定请求是否为请求者的有效操作。该标头的格式如下所示 (为便于阅读，添加了换行符)： `Authorization: AWS4-HMAC_SHA456 Credentials= YourAccessKey /yyymmdd/region/storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature= CalculatedSignature` 在前面的语法中，您可以指定YourAccessKey年、月和日 (yyyymmdd)、区域和。CalculatedSignature授权标头的格式由 Amazon V4 签名过程的要求决定。签名的详细信息在主题 对请求进行签名 中进行讨论。
`Content-Type`	将 `application/x-amz-json-1.1` 用作所有发往 Storage Gateway 的请求的内容类型。 `Content-Type: application/x-amz-json-1.1`
`Host`	使用主机标头指定向其发送请求的 Storage Gateway 网关端点。例如，`storagegateway.us-east-2.amazonaws.com` 是美国东部（俄亥俄州）区域的端点。有关 Storage Gateway 可用的端点的更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon Storage Gateway 端点和配额。 `Host: storagegateway. region.amazonaws.com`

标题	描述
x-amz-date	您必须在 HTTP Date 标头或标头中 Amazon x-amz-date 提供时间戳。(部分 HTTP 客户端库文件不允许您设置Date标头。) 当存在 x-amz-date 标头时，Storage Gateway 会在请求验证期间忽略任何 Date 标头。x-amz-date 格式必须是 YYYYMMDD'T'HHMMS'Z' 格式的 ISO8601 Basic。如果同时使用Date和x-amz-date 标题，则日期标题的格式不必为 ISO86 01。 `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
x-amz-target	该标头指定 API 的版本以及您要请求的操作。目标标头值通过结合 API 版本和 API 名称而形成，其格式如下。 `x-amz-target: StorageGateway_ APIversion .operationName` 操作名称值（例如 ActivateGateway “”）可以从 API 列表中找到。Storage Gateway 的 API 参考

对请求进行签名

Storage Gateway 要求通过对请求进行签名，验证所发送的每个请求的身份。您使用加密哈希函数计算数字签名，从而对请求签名。加密哈西是根据输入内容返回唯一哈希值的函数。对哈希函数的输入内容包括您的请求文本和秘密访问密钥。哈希函数返回哈希值，您将该值包含在请求中，作为签名。该签名是您的请求的 Authorization 标头的一部分。

在收到您的请求后，Storage Gateway 将使用您用于对该请求进行签名的同一哈希函数和输入重新计算签名。如果所得签名与该请求中的签名相匹配，则 Storage Gateway 处理该请求。否则，请求将被拒绝。

Storage Gateway 支持使用 Amazon 签名版本 4 进行身份验证。计算签名的过程可分为三个任务：

- 任务 1：创建规范请求

将您的 HTTP 请求重新排列为规范格式。必须使用规范格式，因为 Storage Gateway 在重新计算签名以与您发送的签名进行比较时使用同一规范格式。

- 任务 2：创建待签字符串

  创建一个字符串，将该字符串用作您的加密哈希函数输入值中的一项。该字符串称为待签字符串，是哈希算法名称、请求日期、凭证范围字符串以及来自上一任务的规范化请求的结合。凭证范围字符串本身是日期、区域和服务信息的结合。

- 任务 3：创建签名

  使用加密哈希函数为您的请求创建签名，该函数接受两种输入字符串：待签字符串和派生密钥。派生密钥的计算方法是从您的私有访问密钥开始，然后使用凭证范围字符串创建一系列基于哈希的消息身份验证码 () HMACs。

实例签名计算

以下示例引导您了解为 ListGateways 创建签名的详细信息。该示例可用作核查您的签名计算方法的参考。其他参考计算方法包含在 Amazon Web Services 词汇表的签名版本 4 测试套件中。

示例假定以下各项：

- 请求的时间戳为“Mon, 10 Sep 2012 00:00:00”GMT。
- 端点是美国东部（俄亥俄州）区域。

通用请求语法 (包括 JSON 正文) 为：

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
x-amz-Date: 20120910T000000Z
Authorization: SignatureToBeCalculated
Content-type: application/x-amz-json-1.1
x-amz-target: StorageGateway_20120630.ListGateways
{}
```

为任务 1：创建规范请求计算的请求规范格式为：

```
POST
/
```

```
content-type:application/x-amz-json-1.1
host:storagegateway.us-east-2.amazonaws.com
x-amz-date:20120910T000000Z
x-amz-target:StorageGateway_20120630.ListGateways

content-type;host;x-amz-date;x-amz-target
44136fa355b3678a1146ad16f7e8649e94fb4fc21fe77e8310c060f61caaff8a
```

规范请求的最后一行是请求正文的哈希值。另外，请注意规范请求的第三行是空的。这是因为此 API（或任何 Storage Gateway APIs）没有查询参数。

任务 2：创建待签字符串 的待签字符串是：

```
AWS4-HMAC-SHA256
20120910T000000Z
20120910/us-east-2/storagegateway/aws4_request
92c0effa6f9224ac752ca179a04cecbede3038b0959666a8160ab452c9e51b3e
```

用来签名的请求的第一行是算法，第二行是时间戳，第三行是证书范围，最后一行是任务 1 中规范请求的哈希值。

对于 任务 3：创建签名，派生密钥可表示为：

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey,"20120910"),"us-
east-2"),"storagegateway"),"aws4_request")
```

如果是私有访问密钥，wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY使用，则计算出的签名为：

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

最终步骤是构造 Authorization 标头。对于演示访问密钥 AKIAIOSFODNN7EXAMPLE，标题（为了便于阅读，添加了换行符）是：

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120910/us-east-2/
storagegateway/aws4_request,
```

```
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

错误响应

主题

- 异常
- 操作错误代码
- 错误响应

本节提供有关 Amazon Storage Gateway 错误的参考信息。这些错误以错误例外和操作错误代码表示。例如，如果请求签名存在问题，那么会由任何 API 响应返回错误例外 `InvalidSignatureException`。但是，`ActivationKeyInvalid`仅返回 ActivateGatewayAPI 的操作错误代码。

根据错误类型的情况，Storage Gateway 可能只返回例外，或者可能同时返回例外和操作错误代码。错误响应 中显示了误差响应示例。

异常

下表列出了 Amazon Storage Gateway API 异常。当 Amazon Storage Gateway 操作返回错误响应时，响应正文包含其中一个异常。`InternalServerError` 和 `InvalidGatewayRequestException` 返回操作错误代码 (提供特定的操作错误代码的 操作错误代码 消息代码) 之一。

例外	消息	HTTP 状态代码
`IncompleteSignatureException`	指定的签名不完全。	400 错误请求
`InternalFailure`	由于某些未知错误、异常或故障导致请求处理失败。	500 内部服务器错误
`InternalServerError`	一个操作错误代码消息操作错误代码。	500 内部服务器错误
`InvalidAction`	请求的操作无效。	400 错误请求

例外	消息	HTTP 状态代码
InvalidClientTokenId	我们的记录中不存在提供的 X.509 证书或 Amazon 访问密钥 ID。	403 禁止访问
InvalidGatewayRequestException	操作错误代码 中的操作错误代码消息之一。	400 错误请求
InvalidSignatureException	我们计算出的请求签名与您提供的签名不匹配。检查您的 Amazon 访问密钥和签名方法。	400 错误请求
MissingAction	请求中遗漏了一个操作或运行参数。	400 错误请求
MissingAuthenticationToken	请求必须包含有效（已注册的）Amazon 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	Amazon 访问密钥 ID 需要订阅该服务。	400 错误请求
ThrottlingException	费率已超。	400 错误请求
TooManyRequests	过多请求。	429 请求过多
UnknownOperationException	指定了未知操作。Storage Gateway 中的操作 中列出了有效操作。	400 错误请求
UnrecognizedClientException	请求中包含的安全令牌无效。	400 错误请求

例外	消息	HTTP 状态代码
ValidationException	输入参数的值不正确或者超出范围。	400 错误请求

操作错误代码

下表显示了 Amazon Storage Gateway 操作错误代码和可以返回代码 APIs 的错误代码之间的映射。返回所有操作错误代码，包含异常中所述的两个一般异常（InternalServerError 和 InvalidGatewayRequestException）之一。

操作错误代码	消息	返回此错误代码的操作
ActivationKeyExpired	指定的激活密钥已过期。	ActivateGateway
ActivationKeyInvalid	指定的激活密钥无效。	ActivateGateway
ActivationKeyNotFound	找不到指定的激活密钥。	ActivateGateway
BandwidthThrottleScheduleNotFound	找不到指定的带宽限制。	DeleteBandwidthRateLimit
CannotExportSnapshot	无法导出指定的快照。	CreateCachediSCSIVolume CreateStorediSCSIVolume
InitiatorNotFound	找不到指定的启动程序。	DeleteChapCredentials
DiskAlreadyAllocated	指定的磁盘已分配。	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
DiskDoesNotExist	指定的磁盘不存在。	AddCache

操作错误代码	消息	返回此错误代码的操作
		AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
DiskSizeNotGigAligned	指定的磁盘没有以 GB 为整单位。	CreateStorediSCSIVolume
DiskSizeGreaterThanVolumeMaxSize	指定的磁盘大小超过最高卷大小。	CreateStorediSCSIVolume
DiskSizeLessThanVolumeSize	指定的磁盘大小低于最高卷大小。	CreateStorediSCSIVolume
DuplicateCertificateInfo	指定的证书信息是副本。	ActivateGateway

操作错误代码	消息	返回此错误代码的操作
GatewayInternalError	出现网关内部错误。	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

操作错误代码	消息	返回此错误代码的操作
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

操作错误代码	消息	返回此错误代码的操作
GatewayNotConnected	没有连接指定的网关。	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

操作错误代码	消息	返回此错误代码的操作
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

操作错误代码	消息	返回此错误代码的操作
GatewayNotFound	找不到指定的网关。	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage

操作错误代码	消息	返回此错误代码的操作
		ListLocalDisks ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

操作错误代码	消息	返回此错误代码的操作
GatewayProxyNetworkConnectionBusy	指定的网关代理网络连接忙。	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

操作错误代码	消息	返回此错误代码的操作
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

操作错误代码	消息	返回此错误代码的操作
InternalError	出现内部错误。	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

操作错误代码	消息	返回此错误代码的操作
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule

操作错误代码	消息	返回此错误代码的操作
InvalidParameters	指定的请求中包含错误参数。	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

操作错误代码	消息	返回此错误代码的操作
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
LocalStorageLimitExceeded	已超过本地存储限制。	AddCache AddUploadBuffer AddWorkingStorage
LunInvalid	指定的 LUN 错误。	CreateStorediSCSIVolume
MaximumVolumeCountExceeded	已超过最大卷计数。	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes

操作错误代码	消息	返回此错误代码的操作
NetworkConfigurationChanged	已更改网关网络配置。	CreateCachediSCSIVolume CreateStorediSCSIVolume

操作错误代码	消息	返回此错误代码的操作
NotSupported	不支持指定的操作。	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

操作错误代码	消息	返回此错误代码的操作
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
OutdatedGateway	指定的网关已过时。	ActivateGateway
SnapshotInProgressException	指定的快照在进行中。	DeleteVolume
SnapshotIdInvalid	指定的快照无效。	CreateCachediSCSIVolume CreateStorediSCSIVolume
StagingAreaFull	暂存区域已满。	CreateCachediSCSIVolume CreateStorediSCSIVolume

操作错误代码	消息	返回此错误代码的操作
TargetAlreadyExists	已存在指定的目标。	CreateCachediSCSIVolume CreateStorediSCSIVolume
TargetInvalid	指定的目标无效。	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials UpdateChapCredentials
TargetNotFound	找不到指定的目标。	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials DeleteVolume UpdateChapCredentials

操作错误代码	消息	返回此错误代码的操作
UnsupportedOperationForGatewayType	对于这类网关，指定的操作无效。	AddCache AddWorkingStorage CreateCachediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteSnapshotSchedule DescribeCache DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
VolumeAlreadyExists	已存在指定的卷。	CreateCachediSCSIVolume CreateStorediSCSIVolume
VolumeIdInvalid	指定的卷无效。	DeleteVolume
VolumeInUse	指定的卷已在使用中。	DeleteVolume

操作错误代码	消息	返回此错误代码的操作
VolumeNotFound	找不到指定的卷。	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint DeleteVolume DescribeCachediSCSIVolumes DescribeSnapshotSchedule DescribeStorediSCSIVolumes UpdateSnapshotSchedule
VolumeNotReady	指定的卷没有准备好。	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

错误响应

当存在错误时，响应头信息会包含：

- 内容类型：应用程序/ -1.1 x-amz-json
- 适当的 4xx 或 5xx HTTP 状态码

错误响应的正文会包含有关错误出现的信息。下列错误响应示例显示的是所有错误响应中常见的响应元素的输出语法。

```
{
    "__type": "String",
    "message": "String",
    "error":
        { "errorCode": "String",
          "errorDetails": "String"
        }
```

```
}
```

下表介绍了前一语法中显示的 JSON 错误响应字段。

__type

异常 中的例外之一。

类型：字符串

error

包含特定于 API 的错误详细信息。在常规的 (即不特定于任何 API 的) 错误中，不显示这个误差信息。

类型：集合

errorCode

其中一个操作错误代码。

类型：字符串

errorDetails

此字段不在 API 的当前版本中使用。

类型：字符串

message

一个操作错误代码消息。

类型：字符串

错误响应示例

如果您使用 DescribeStoredi SCSIVolumes API 并指定了不存在的网关 ARN 请求输入，则会返回以下 JSON 正文。

```
{
  "__type": "InvalidGatewayRequestException",
  "message": "The specified volume was not found.",
  "error": {
```

```
    "errorCode": "VolumeNotFound"
  }
}
```

如果 Storage Gateway 计算的签名不符合通过请求发送的签名，那么会返回如下 JSON 正文。

```
{
  "__type": "InvalidSignatureException",
  "message": "The request signature we calculated does not match the signature you
 provided."
}
```

Storage Gateway 中的操作

有关 Storage Gateway 操作的列表，请参阅《Amazon Storage Gateway API 参考》中的操作。

《磁带网关用户指南》的文档历史记录

- API 版本：2013-06-30
- 文档最近更新时间：2020 年 11 月 24 日

下表描述了在 2018 年 4 月后每次发布《Amazon Storage Gateway 用户指南》时进行的重要更改。要获得本文档的更新通知，您可以订阅 RSS 源。

变更	说明	日期
FSx 文件网关可用性变更通知	Amazon FSx 文件网关不再向新客户开放。 FSx File Gateway 的现有客户可以继续正常使用该服务。有关与 FSx 文件网关类似的功能，请访问此博客文章。	2024 年 10 月 28 日
FSx 文件网关可用性变更通知	Amazon Storage Gateway 从 24 年 10 月 28 日起，新客户将不再使用的 FSx File Gateway。要使用该服务，必须在该日期之前注册。 FSx File Gateway 的现有客户可以继续正常使用该服务。有关与 FSx 文件网关类似的功能，请访问此博客文章。	2024 年 9 月 26 日
添加了开启或关闭维护更新的选项	Storage Gateway 会定期收到维护更新，其中可能包括操作系统和软件升级、用于解决稳定性、性能和安全性的修复程序以及对新功能的访问。现在，可以配置一项设置，来为部署中的每个单独网关开启或关闭这些更新。有关更多信息，请参阅使用控制台管理网	2024 年 6 月 6 日

	关更新使用 Amazon Storage Gateway 控制台。 Amazon Storage Gateway	
Snowball Edge 上对磁带网关的支持已弃用	不再能够在 Snowball Edge 设备上托管磁带网关。	2024 年 3 月 14 日
更新了使用第三方应用程序测试网关设置的说明	现在，使用第三方应用程序测试网关设置的说明描述了在执行备份任务期间网关重新启动时的预期行为。有关更多信息，请参阅使用备份软件来测试您的网关设置。	2023 年 10 月 24 日
更新了推荐的 CloudWatch 警报	该 CloudWatch `HealthNotifications` 警报现在适用于所有网关类型和主机平台，并建议该警报适用于所有网关类型和主机平台。`HealthNotifications` 和 `AvailabilityNotifications` 的建议配置设置也已更新。有关更多信息，请参阅了解 CloudWatch 警报。	2023 年 10 月 2 日
将磁带网关的最大磁带大小增加到 15 TiB	对于磁带网关，虚拟磁带的最大大小现在从 5 TiB 增加到 15 TiB。有关更多信息，请参阅《Storage Gateway 用户指南》中的磁带配额。	2022 年 10 月 4 日

单独的磁带网关和卷网关用户指南	《Storage Gateway 用户指南》以前包含有关磁带网关和卷网关类型的信息，现已分为《磁带网关用户指南》和《卷网关用户指南》，每份指南仅包含有关一种网关类型的信息。有关更多信息，请参阅磁带网关用户指南和卷网关用户指南。	2022 年 3 月 23 日
更新了网关创建程序	使用 Storage Gateway 控制台创建所有网关类型的过程均已更新。有关更多信息，请参阅创建网关。	2022 年 1 月 18 日
新的磁带接口	Amazon Storage Gateway 控制台中的磁带概述页面已更新，增加了新的搜索和筛选功能。为了描述新功能，本指南中的所有相关程序均已更新。有关更多信息，请参阅管理您的磁带网关。	2021 年 9 月 23 日
支持适用于磁带网关的 Quest NetVault Backup 13	磁带网关现在支持在微软 Windows Server 2012 R2 或微软 Windows Server 2016 上运行的 Quest B NetVault ackup 13。有关更多信息，请参阅 “使用 Quest NetVault Backup 测试您的设置”。	2021 年 8 月 22 日
S3 文件网关主题已从磁带网关和卷网关指南中删除	为了使设置各自网关类型的客户更容易遵循磁带网关和卷网关的用户指南，删除了一些不必要的主题。	2021 年 7 月 21 日

为磁带网关支持 Windows 和 Linux 上的 IBM Spectrum Protect 8.1.10	磁带网关现在支持在 Microsoft Windows Server 和 Linux 上运行的 IBM Spectrum Protect 8.1.10。有关更多信息，请参阅使用 IBM Spectrum Protect 测试您的设置。	2020 年 11 月 24 日
FedRAMP 合规性	Storage Gateway 现已符合 FedRAMP 标准。有关更多信息，请参阅 Storage Gateway 的合规性验证。	2020 年 11 月 24 日
基于计划的带宽限制	Storage Gateway 现在支持对磁带网关和卷网关进行基于计划的带宽限制。有关更多信息，请参阅使用 Storage Gateway 控制台调度带宽限制。	2020 年 11 月 9 日
缓存卷和磁带网关本地缓存存储增加 4 倍	Storage Gateway 现在为缓存卷和磁带网关支持高达 64 TB 的本地缓存，通过提供对更大工作数据集的低延迟访问来提高本地应用程序的性能。有关更多信息，请参阅为网关推荐的本地磁盘大小。	2020 年 11 月 9 日
网关迁移	Storage Gateway 现在支持将缓存的卷网关迁移到新的虚拟机。有关更多信息，请参阅将缓存卷移至新的缓存卷网关虚拟机。	2020 年 9 月 10 日

支持磁带保留锁和 write-once-read-many (WORM) 磁带保护	Storage Gateway 支持虚拟磁带上的磁带保留锁定和一次写入多次读取 (WORM)。磁带保留锁定让您可以指定已存档虚拟磁带的保留模式和期限，从而在长达 100 年的固定时间段内防止删除这些磁带。这包括权限控制，用于控制谁可以删除磁带或修改保留设置。有关更多信息，请参阅使用磁带保留锁定。已激活 WORM 的虚拟磁带有助于确保无法覆盖或擦除虚拟磁带库中活动磁带上的数据。有关更多信息，请参阅一次写入多次读取 (WORM) 磁带保护。	2020 年 8 月 19 日
通过控制台订购硬件设备	现在，您可以通过 Amazon Storage Gateway 控制台订购硬件设备。有关更多信息，请参阅使用 Storage Gateway 硬件设备。	2020 年 8 月 12 日
在新的 Amazon 区域支持美国联邦信息处理标准 (FIPS) 端点	现在您可以在美国东部（俄亥俄州）、美国东部（弗吉尼亚州北部）、美国西部（北加利福尼亚）、美国西部（俄勒冈州）和加拿大（中部）区域通过 FIPS 端点激活网关。有关更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon Storage Gateway 端点和配额。	2020 年 7 月 31 日

网关迁移	Storage Gateway 现在支持将磁带和存储的卷网关迁移到新的虚拟机。有关更多信息，请参阅将数据移到新网关。	2020 年 7 月 31 日
在 Storage Gateway 控制台中查看亚马逊 CloudWatch 警报	现在，您可以在 Storage Gateway 控制台中查看 CloudWatch 警报。有关更多信息，请参阅了解 CloudWatch 警报。	2020 年 5 月 29 日
支持美国联邦信息处理标准 (FIPS) 端点	现在，您可以在 Amazon GovCloud (US) 区域中通过 FIPS 终端节点激活网关。要为卷网关选择 FIPS 端点，请参阅选择服务端点。要为磁带网关选择 FIPS 端点，请参阅将磁带网关连接到 Amazon。	2020 年 5 月 22 日
新 Amazon 区域	Storage Gateway 现已在非洲（开普敦）和欧洲（米兰）区域推出。有关更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon Storage Gateway 端点和配额。	2020 年 5 月 7 日
支持 S3 Intelligent-Tiering 存储类	Storage Gateway 现在支持 S3 Intelligent-Tiering 存储类。S3 智能分层存储类可以通过自动将数据移至最具成本效益的存储访问层来优化存储成本，而不会影响性能或产生运营开销。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的可自动优化经常访问和不常访问对象的存储类。	2020 年 4 月 30 日

磁带网关的读写性能提升了两倍	Storage Gateway 将读写磁带网关上的虚拟磁带的性能提高了两倍，从而使您能够比之前更快地执行备份和还原。有关更多信息，请参阅《Storage Gateway 用户指南》中的磁带网关性能指导。	2020 年 4 月 23 日
支持自动磁带创建	Storage Gateway 现在可以自动创建新的虚拟磁带。磁带网关可以自动创建新的虚拟磁带，从而维持您配置的最小可用磁带数，然后将这些新磁带设为可由备份应用程序导入，从而使备份任务能够不间断地运行。有关更多信息，请参阅《Storage Gateway 用户指南》中的自动创建磁带。	2020 年 4 月 23 日
新 Amazon 区域	Storage Gateway 现已在 Amazon GovCloud（美国东部）地区推出。有关更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon Storage Gateway 端点和配额。	2020 年 3 月 12 日
支持基于 Linux 内核的虚拟机 (KVM) 管理程序	Storage Gateway 现在可将本地网关部署在 KVM 虚拟化平台上。KVM 上部署的网关与现有本地网关具有相同的功能和功能。有关更多信息，请参阅《Storage Gateway 用户指南》中的支持的虚拟机管理程序和主机要求。	2020 年 2 月 4 日

支持 VMware vSphere 高可用性	Storage Gateway 现在支持高可用性 VMware ，以帮助保护存储工作负载免受硬件、虚拟机管理程序或网络故障的影响。有关更多信息，请参阅《Storage G ateway 用户指南》中的 “将 VMware vSphere 高可用性与存储网关配合使用”。此版本还包含性能改进。有关更多信息，请参阅《Storage Gateway 用户指南》中的性能。	2019 年 11 月 20 日
磁带网关的新 Amazon 区域	磁带网关现已在南美洲（圣保罗）区域推出。有关更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon Storage Gateway 端点和配额。	2019 年 9 月 24 日
在 Linux 上支持 IBM Spectrum Protect 7.1.9，对于磁带网关，最大磁带大小增加到 5 TiB	除了在 Microsoft Windows 上运行之外，磁带网关现在还支持在 Linux 上运行的 IBM Spectrum Protect (Tivoli Storage Manager) 7.1.9。有关更多信息，请参阅《Storage Gateway 用户指南》中的使用 IBM Spectrum Protect 测试您的设置。此外，对于磁带网关，虚拟磁带的最大大小现在从 2.5 TiB 增加到 5 TiB。有关更多信息，请参阅《Storage Gateway 用户指南》中的磁带配额。	2019 年 9 月 10 日

支持 Amazon CloudWatch 日志	现在，您可以使用 Amazon CloudWatch 日志组配置文件网关，以获得有关错误以及网关及其资源的运行状况的通知。有关更多信息，请参阅 Storage Gateway 用户指南中的获取有关网关运行状况和亚马逊 CloudWatch 日志组错误的通知。	2019 年 9 月 4 日
新 Amazon 区域	Storage Gateway 现已在亚太地区（香港）区域推出。有关更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon Storage Gateway 端点和配额。	2019 年 8 月 14 日
新 Amazon 区域	Storage Gateway 现已在中东（巴林）区域推出。有关更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon Storage Gateway 端点和配额。	2019 年 7 月 29 日
支持在 Virtual Private Cloud (VPC) 中激活网关	现在，您可以在 VPC 中激活网关。您可以在本地软件设备和基于云的存储基础设施之间创建私有连接。有关更多信息，请参阅在 Virtual Private Cloud 中激活网关。	2019 年 6 月 20 日

支持将虚拟磁带从 S3 Glacier Flexible Retrieval 移动到 S3 Glacier Deep Archive	您现在可以将在 S3 Glacier Flexible Retrieval 存储类中存档的虚拟磁带转移到 S3 Glacier Deep Archive 存储类，从而实现经济高效且长期的数据留存。有关更多信息，请参阅将磁带从 S3 Glacier Flexible Retrieval 转移到 S3 Glacier Deep Archive。	2019 年 5 月 28 日
支持微软 Windows 的 SMB 文件共享 ACLs	对于文件网关，你现在可以使用 Microsoft Windows 访问控制列表 (ACLs) 来控制对服务器消息块 (SMB) 文件共享的访问。有关更多信息，请参阅使用 Microsoft Windows ACLs 控制对 SMB 文件共享的访问权限。	2019 年 5 月 8 日
与 S3 Glacier Deep Archive 集成	磁带网关与 S3 Glacier Deep Archive 集成在一起。现在，您可以在 S3 Glacier Deep Archive 中存档虚拟磁带来实现长期数据留存。有关更多信息，请参阅存档虚拟磁带。	2019 年 3 月 27 日

Storage Gateway 硬件设备在欧洲推出	Storage Gateway 硬件设备现已在欧洲推出。有关更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon Storage Gateway 硬件设备区域。此外，您现在还可以将 Storage Gateway 硬件设备上的可用存储从 5 TB 增加到 12 TB，并将安装的铜质网卡更换为 10 Gb 以太网光纤网卡。有关更多信息，请参阅设置您的硬件设备。	2019 年 2 月 25 日
与集成 Amazon Backup	Storage Gateway 与集成 Amazon Backup。现在，您可以使用备份使用 Amazon Backup Storage Gateway 卷进行云支持的存储的本地业务应用程序。有关更多信息，请参阅备份您的卷。	2019 年 1 月 16 日
支持 Bacula Enterprise 和 IBM Spectrum Protect	磁带网关现在支持 Bacula Enterprise 和 IBM Spectrum Protect。Storage Gateway 现在还支持更新版本的 Veritas NetBackup、Veritas Backup Exec 和 Quest 备份。NetVault 现在，您可以使用这些备份应用程序将数据备份到 Amazon S3 并直接存档到脱机存储（S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）中。有关更多信息，请参阅使用备份软件来测试您的网关设置。	2018 年 11 月 13 日

支持 Storage Gateway 硬件设备	Storage Gateway 硬件设备包括在第三方服务器上预安装的 Storage Gateway 软件。您可以从 Amazon Web Services Management Console管理设备。该设备可以承载文件、磁带和卷网关。有关更多信息，请参阅使用 Storage Gateway 硬件设备。	2018 年 9 月 18 日
与 Microsoft System Center 2016 Data Protection Manager (DPM) 的兼容性	磁带网关现在与 Microsoft System Center 2016 Data Protection Manager (DPM) 兼容。现在，您可以使用 Microsoft DPM 将数据备份到 Amazon S3 并直接存档到脱机存储（S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）中。有关更多信息，请参阅使用 Microsoft System Center Data Protection Manager 测试您的设置。	2018 年 7 月 18 日
支持服务器消息块 (SMB) 协议	文件网关向文件共享添加了对服务器消息块 (SMB) 协议的支持。有关更多信息，请参阅创建文件共享。	2018 年 6 月 20 日
支持文件共享、缓存卷和虚拟磁带加密	现在，您可以使用 Amazon Key Management Service (Amazon KMS) 对写入文件共享、缓存卷或虚拟磁带的数据进行加密。目前，您可以使用 Amazon Storage Gateway API 执行此操作。有关更多信息，请参阅使用 Amazon KMS进行数据加密。	2018 年 6 月 12 日

对 NovaStor DataCenter / Network 的支持	磁带网关现在支持 6.4 或 7.1 NovaStor DataCenter/Network . You can now use NovaStor DataCenter/Network 版，可将您的数据备份到 Amazon S3 并直接存档到离线存储（S3 Glacier 灵活检索或 S3 Glacier Deep Archive）。有关更多信息，请参阅使用 NovaStor DataCenter /Network 测试您的设置。	2018 年 5 月 24 日

早期更新

下表描述了 2018 年 5 月之前的每个 Amazon Storage Gateway 用户指南发行版中的重要更改。

更改	描述	更改日期
支持 S3 One Zone_IA 存储类别	对于文件网关，您现在可以选择 S3 One Zone_IA 作为文件共享的默认存储类。使用此存储类，您可以在 Amazon S3 内的单个可用区中存储对象数据。有关更多信息，请参阅创建文件共享。	2018 年 4 月 4 日
新的 区域	磁带网关现已在亚太地区（新加坡）区域推出。有关详细信息，请参阅 Amazon Web Services 区域 支持 Storage Gateway。	2018 年 4 月 3 日
支持 Amazon S3 存储桶刷新缓存通知、申请者付款和预ACLs 设。	使用文件网关，您现在可以在网关完成为 Amazon S3 存储桶刷新缓存后获得通知。有关更多信息，请参阅 Storage Gateway API 参考中的 RefreshCache.html。 借助文件网关，申请方或读取者（而不是存储桶拥有者）现在能够支付访问费用。 借助文件网关，您现在能够向映射到 NFS 文件共享的 S3 存储桶的所有者授予完全控制权限。	2018 年 3 月 1 日

更改	描述	更改日期
	有关更多信息，请参阅创建文件共享。	
支持 Dell EMC NetWorker v9.x	磁带网关现在支持 Dell EMC NetWorker v9.x。现在，您可以使用 Dell EMC NetWorker v9.x 将数据备份到 Amazon S3，然后直接存档到离线存储（S3 Glacier 灵活检索或 S3 Glacier Deep Archive）。有关更多信息，请参阅使用 Dell EMC 测试您的设置 NetWorker。	2018 年 2 月 27 日
新的 区域	Storage Gateway 现已在欧洲（巴黎）区域推出。有关详细信息，请参阅 Amazon Web Services 区域 支持 Storage Gateway。	2017 年 12 月 18 日
支持文件上传通知和 MIME 类型猜测	现在，写入 NFS 文件共享的所有文件均已上传至 Amazon S3 后，文件网关会向您发送通知。有关更多信息，请参阅 Storage Gateway API 参考NotifyWhenUploaded中的。 文件网关现在可根据文件扩展名猜测已上传对象的 MIME 类型。有关更多信息，请参阅创建文件共享。	2017 年 11 月 21 日
Support 支持 VMware ESXi Hypervisor 版本 6.5	Amazon Storage Gateway 现在支持 VMware ESXi 虚拟机管理程序版本 6.5。这是对版本 4.1、5.0、5.1、5.5 和 6.0 支持提供的补充。有关更多信息，请参阅 受支持的管理程序和主机要求。	2017 年 9 月 13 日
与 Commvault 11 兼容	磁带网关现在与 Commvault 11 兼容。现在，您可以使用 Commvault 将数据备份到 Amazon S3 并直接存档到脱机存储（S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）中。有关更多信息，请参阅使用 Commvault 测试您的设置。	2017 年 9 月 12 日
文件网关支持 Microsoft Hyper-V 管理程序	现在您可以在 Microsoft Hyper-V 管理程序上部署文件网关。有关信息，请参阅受支持的管理程序和主机要求。	2017 年 6 月 22 日

更改	描述	更改日期
支持在三至五个小时内从存档中检索磁带	对于磁带网关，您现在可以在三至五个小时内从存档中取回磁带。您还可以确定从备份应用程序或虚拟磁带库 (VTL) 写入到磁带中的数据量。有关更多信息，请参阅查看磁带使用情况。	2017 年 5 月 23 日
新的 区域	Storage Gateway 现已在亚太地区（孟买）区域推出。有关详细信息，请参阅 Amazon Web Services 区域 支持 Storage Gateway。	2017 年 5 月 02 日
对文件共享设置的更新 对文件共享的缓存刷新的支持	文件网关现在将挂载选项添加到文件共享设置。您现在可以为文件共享设置 squash 和只读选项。有关更多信息，请参阅创建文件共享。 文件网关现在可以在 Amazon S3 存储桶中查找自网关上次列出存储桶内容并缓存结果后添加或删除的对象。有关更多信息，请参阅 API 参考RefreshCache中的。	2017 年 3 月 28 日
对克隆卷的支持	对于缓存卷网关， Amazon Storage Gateway 现在支持从现有卷克隆卷的功能。有关克隆卷的更多信息，请参阅克隆卷。	2017 年 3 月 16 日
Amazon 上对文件网关的支持 EC2	Amazon Storage Gateway 现在提供了在 Amazon 中部署文件网关的功能 EC2。您可以使用现已作为社区 AM EC2 I 提供的 Storage Gateway Amazon 系统映像 (AMI) 在亚马逊启动文件网关。有关如何创建文件网关并将其部署到 EC2 实例上的信息，请参阅创建和激活 Amazon S3 文件网关或创建并激活 Amazon FSx 文件网关。有关如何启动文件网关 AMI 的信息，请参阅在 Amazon EC2 主机上部署 S3 文件网关或在 Amaz on EC2 主机上部署 FSx 文件网关。	2017 年 2 月 8 日
与 Arcserve 17 的兼容性	磁带网关现在与 Arcserve 17 兼容。您现在可使用 Arcserve 将数据备份到 Amazon S3 并直接存档到 S3 Glacier Flexible Retrieval。有关更多信息，请参阅使用 Arcserve Backup r17.0 测试您的设置。	2017 年 1 月 17 日

更改	描述	更改日期
新的 区域	Storage Gateway 现已在欧洲（伦敦）区域推出。有关详细信息，请参阅 Amazon Web Services 区域 支持 Storage Gateway。	2016 年 12 月 13 日
新的 区域	Storage Gateway 现已在加拿大（中部）区域推出。有关详细信息，请参阅 Amazon Web Services 区域 支持 Storage Gateway。	2016 年 12 月 8 日
支持文件网关	除了卷网关和磁带网关外，Storage Gateway 现在还提供文件网关。文件网关将服务和虚拟软件设备组合在一起，使您能够使用行业标准文件协议（例如，网络文件系统 (NFS)）在 Amazon S3 中存储和检索对象。利用网关，可以将 Amazon S3 中的对象作为 NFS 装载点上的文件进行访问。	2016 年 11 月 29 日
Backup Exec 16	磁带网关现与 Backup Exec 16 兼容。现在，您可以使用 Backup Exec 16 将数据备份到 Amazon S3 并直接存档到脱机存储（S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）中。有关更多信息，请参阅使用 Veritas Backup Exec 测试您的设置。	2016 年 11 月 7 日
与 Micro Focus (HPE) Data Protector 9.x 兼容	磁带网关现在与 Micro Focus (HPE) Data Protector 9.x 兼容。您现在可以使用 HPE Data Protector 将数据备份到 Amazon S3 并直接存档到 S3 Glacier Flexible Retrieva。有关更多信息，请参阅使用 Micro Focus (HPE) Data Protector 测试您的设置。	2016 年 11 月 2 日
新的 区域	Storage Gateway 现已在美国东部（俄亥俄州）区域推出。有关详细信息，请参阅 Amazon Web Services 区域 支持 Storage Gateway。	2016 年 10 月 17 日

更改	描述	更改日期
Storage Gateway 控制台重新设计	Storage Gateway 管理控制台经过了重新设计，您可以更加轻松地配置、管理和监控您的网关、卷和虚拟磁带。用户界面现在提供可筛选的视图，并提供指向集成 Amazon 服务（例如 CloudWatch 和 Amazon EBS）的直接链接。有关更多信息，请参阅 报名参加 Amazon Storage Gateway。	2016 年 8 月 30 日
与 Veeam Backup & Replication V9 Update 2 或更高版本的兼容性	磁带网关现在与 Veeam Backup & Replication V9 Update 2 或更高版本（即 9.0.0.1715 或更高版本）兼容。现在，您可以使用 Veeam Backup Replication V9 Update 2 或更高版本将数据备份到 Amazon S3 并直接存档到脱机存储（S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）中。有关更多信息，请参阅使用 Veeam Backup & Replication 测试您的设置。	2016 年 8 月 15 日
更长的卷和快照 IDs	Storage Gateway IDs 为卷和快照引入了更长的使用时间。您可以为卷、快照和其他支持的 Amazon 资源激活加长 ID 格式。有关更多信息，请参阅 了解 Storage Gateway 资源和资源 IDs。	2016 年 4 月 25 日
新的 区域 支持存储最大 512 TiB 的存储卷 对 Storage Gateway 本地控制台的其他网关更新和增强	磁带网关现已在亚太（首尔）区域推出。有关更多信息，请参阅 Amazon Web Services 区域 支持 Storage Gateway。 对于存储卷，您现在最多可以创建 32 个存储卷，每个存储卷最大为 16 TiB，最大存储量为 512 TiB。有关更多信息，请参阅存储卷架构和Amazon Storage Gateway 配额。 一个虚拟磁带库中所有磁带的总大小增加到 1 PiB。有关更多信息，请参阅 Amazon Storage Gateway 配额。 您现在可以在 Storage Gateway 控制台上设置您的 VM 本地控制台的密码。有关信息，请参阅从 Storage Gateway 控制台设置本地控制台密码。	2016 年 3 月 21 日

更改	描述	更改日期
与 Dell EMC NetWorker 8.x 的兼容性	磁带网关现在与 Dell EMC NetWorker 8.x 兼容。现在，您可以使用 Dell EMC NetWorker 将数据备份到 Amazon S3，然后直接存档到离线存储（S3 Glacier 灵活检索或 S3 Glacier Deep Archive Deep Archive）。有关更多信息，请参阅使用 Dell EMC 测试您的设置 NetWorker。	2016 年 2 月 29 日
支持 6.0 版 VMware ESXi 虚拟机管理程序和红帽企业 Linux 7 iSCSI 启动器	Amazon Storage Gateway 现在支持 VMware ESXi 虚拟机管理程序 6.0 版和红帽企业 Linux 7 iSCSI 启动器。有关更多信息，请参阅受支持的管理程序和主机要求 和受支持的 iSCSI 启动程序。	2015 年 10 月 20 日
调整内容	此版本包含以下改进：该文档现在包含结合了所有网关解决方案的常见管理任务的“管理已激活的网关”部分。在下文中，您可以找到有关如何在部署并激活网关后管理网关的说明。有关更多信息，请参阅 管理磁带网关。	
支持存储最大 1024 TiB 的缓存卷 支持 VMwareESXi 虚拟机管理程序中的 VMXNET3 (10 GbE) 网络适配器类型 性能增强 对 Storage Gateway 本地控制台的多项改进和更新	对于缓存卷，您现在最多可以创建 32 个存储卷，每个存储卷最大为 32 TiB，最大总存储为 1024 TiB。有关更多信息，请参阅缓存卷架构和Amazon Storage Gateway 配额。 如果您的网关托管在 VMware ESXi 虚拟机管理程序上，则可以将网关重新配置为使用适配器类型。VMXNET3 有关更多信息，请参阅 为网关配置网络适配器。 Storage Gateway 的最高上传速率提高到了每秒 120 MB，最高下载速率提高到了每秒 20 MB。 Storage Gateway 本地控制台已更新并通过额外功能进行增强，从而有助于执行维护任务。有关更多信息，请参阅 配置网关网络。	2015 年 9 月 16 日

更改	描述	更改日期
对标签的支持	Storage Gateway 现在支持资源标记。现在，您可以为网关、卷和虚拟磁带添加标签，以便更轻松地管理它们。有关更多信息，请参阅 标记 Storage Gateway 资源。	2015 年 9 月 2 日
与 Quest（前身为戴尔）NetVault Backup 10.0 的兼容性	磁带网关现在与 Quest NetVault Backup 10.0 兼容。现在，你可以使用 Quest NetVault Backup 10.0 将数据备份到 Amazon S3，然后直接存档到离线存储（S3 Glacier 灵活检索或 S3 Glacier Deep Archive）。有关更多信息，请参阅使用 Quest NetVault Backup 测试您的设置。	2015 年 6 月 22 日

更改	描述	更改日期
支持将 16 TiB 存储卷用于存储卷网关设置	Storage Gateway 现在支持将 16 TiB 存储卷用于存储卷网关设置。您现在最多可以创建 12 个 16 TiB 存储卷，最大存储空间为 192 TiB。有关更多信息，请参阅存储卷架构。	2015 年 6 月 3 日
支持 Storage Gateway 本地控制台上的系统资源检查	现在，您可以确定系统资源（虚拟 CPU 核心、根卷大小和 RAM）是否足够让网关正常运行。有关更多信息，请参阅 查看您的网关系统资源状态或 查看您的网关系统资源状态。	
支持 Red Hat Enterprise Linux 6 iSCSI 启动程序	Storage Gateway 现在支持 Red Hat Enterprise Linux 6 iSCSI 启动程序。有关更多信息，请参阅 设置磁带网关的要求。 此版本包括以下 Storage Gateway 改进和更新： • 在 Storage Gateway 控制台中，您现在可以查看上次成功将软件更新应用到网关的日期和时间。有关更多信息，请参阅 管理网关更新。 • Storage Gateway 现在提供了 API，您可以使用该 API 来列出连接到存储卷的 iSCSI 启动程序。有关更多信息，请参阅《API 参考》中的 ListVolumeInitiators。	
支持 Microsoft Hyper-V 管理程序版本 2012 和 2012 R2	Storage Gateway 现在支持 Microsoft Hyper-V 管理程序版本 2012 和 2012 R2。这是对 Microsoft Hyper-V 管理程序版本 2008 R2 支持提供的补充。有关更多信息，请参阅 受支持的管理程序和主机要求。	2015 年 4 月 30 日

更改	描述	更改日期
与 Symantec Backup Exec 15 的兼容性	磁带网关现在与 Symantec Backup Exec 15 兼容。现在，您可以使用 Symantec Backup Exec 15 将数据备份到 Amazon S3 并直接存档到脱机存储（S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）中。有关更多信息，请参阅使用 Veritas Backup Exec 测试您的设置。	2015 年 4 月 6 日
存储卷的 CHAP 身份验证支持	Storage Gateway 现在支持为存储卷配置 CHAP 身份验证。有关更多信息，请参阅为卷配置 CHAP 身份验证。	2015 年 4 月 2 日
Support 支持 5.1 和 5. VMware ESXi 5 版虚拟机管理程序	Storage Gateway 现在支持 VMware ESXi 虚拟机管理程序版本 5.1 和 5.5。除此之外，还支持 VMware ESXi 虚拟机管理程序版本 4.1 和 5.0。有关更多信息，请参阅 受支持的管理程序和主机要求。	2015 年 3 月 30 日
支持 Windows CHKDSK 实用工具	Storage Gateway 现在支持 Windows CHKDSK 实用工具。您可以使用此实用工具来验证卷的完整性并修复卷上的错误。有关更多信息，请参阅排查卷问题。	2015 年 3 月 04 日

更改	描述	更改日期
与集成 Amazon CloudTrail 以捕获 API 调用	Storage Gateway 现已与集成 Amazon CloudTrail。Amazon CloudTrail 捕获您的 Amazon Web Services 账户中由 Storage Gateway 或代表 Storage Gateway 发出的 API 调用，并将日志文件传输到您指定的亚马逊 S3 存储桶。有关更多信息，请参阅 登录和监控 Amazon Storage Gateway。 此版本包括以下 Storage Gateway 改进和更新： • 现在，当网关缓存的驱动器发生更改时，将恢复在缓存存储中包含废数据（即包含尚未上传到 Amazon的内容）的虚拟磁带。有关更多信息，请参阅从无法恢复的网关恢复虚拟磁带。	2014 年 12 月 16 日

更改	描述	更改日期
与更多备份软件和介质更换器的兼容性	磁带网关现在与以下备份软件兼容： • Symantec Backup Exec 2014 • Microsoft System Center 2012 R2 Data Protection Manager • Veeam Backup & Replication V7 • Veeam Backup & Replication V8 现在，您可以使用这四种备份软件产品和 Storage Gateway 虚拟磁带库 (VTL) 将数据备份到 Amazon S3 并直接存档到脱机存储（S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）中。有关更多信息，请参阅使用备份软件来测试您的网关设置。 Storage Gateway 现在提供了另一种可用于新备份软件的介质更换器。 此版本包括其他 Amazon Storage Gateway 改进和更新。	2014 年 11 月 3 日
欧洲地区（法兰克福）区域	Storage Gateway 现已在欧洲（法兰克福）区域推出。有关详细信息，请参阅 Amazon Web Services 区域 支持 Storage Gateway。	2014 年 10 月 23 日
调整内容	已创建对所有网关解决方案通用的“入门”章节。在下文中，您可以找到有关下载、部署和激活网关的说明。在部署和激活网关后，您可以继续参考特定于存储卷、缓存卷和磁带网关设置的进一步说明。有关更多信息，请参阅创建磁带网关。	2014 年 5 月 19 日

更改	描述	更改日期
与 Symantec Backup Exec 2012 兼容	磁带网关现在与 Symantec Backup Exec 2012 兼容。现在，您可以使用 Symantec Backup Exec 2012 将数据备份到 Amazon S3 并直接存档到脱机存储（S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）中。有关更多信息，请参阅使用 Veritas Backup Exec 测试您的设置。	2014 年 4 月 28 日
对 Windows Server 故障转移集群的支持 Support 对 VMware ESX 启动器 支持在 Storage Gateway 本地控制台上执行配置任务	• 如果主机使用 Windows Server 失效转移集群 (WSFC) 协调访问，Storage Gateway 现在支持将多个主机与同一个卷关联。但是，若未使用 WSFC，则不能将多个主机与同一个卷关联。 • Storage Gateway 现在使您可以直接通过 ESX 主机管理存储连接。这为使用驻留在您的VMs客户机操作系统中的启动程序提供了一种替代方案。 • Storage Gateway 现在支持在 Storage Gateway 本地控制台中执行配置任务。有关在本地部署的网关上执行配置任务的信息，请参阅 在 虚拟机本地控制台上执行任务 或 在 虚拟机本地控制台上执行任务。有关在 EC2 实例上部署的网关上执行配置任务的信息，请参阅在 Amazon EC2 本地控制台上执行任务或在 Amazon EC2 本地控制台上执行任务。	2014 年 1 月 31 日

更改	描述	更改日期
支持虚拟磁带库 (VTL) 并引入 API 版本 2013-06-30	Storage Gateway 将本地软件设备与基于云的存储连接起来，将您的本地 IT 环境与 Amazon 存储基础架构集成。除了卷网关（缓存卷和存储卷）外，Storage Gateway 现在还支持网关虚拟磁带库 (VTL)。对于每个网关，最多可为磁带网关配置 10 个虚拟磁带驱动器。每个虚拟磁带驱动器均可响应 SCSI 命令集，因此现有的本地备份应用程序无需修改即可工作。有关更多信息，请参阅《Amazon Storage Gateway 用户指南》中的以下主题。 • 有关架构概述，请参阅磁带网关的工作原理（架构）。 • 要开始使用磁带网关，请参阅创建磁带网关。	2013 年 11 月 5 日
支持 Microsoft Hyper-V	Storage Gateway 现在可将本地网关部署在 Microsoft Hyper-V 虚拟化平台上。在 Microsoft Hyper-V 上部署的网关拥有的功能与现有的本地 Storage Gateway 完全相同。要开始用 Microsoft Hyper-V 部署网关，请参阅受支持的管理程序和主机要求。	2013 年 4 月 10 日
支持在 Amazon 上部署网关 EC2	Storage Gateway 现在能够在亚马逊弹性计算云 (亚马逊 EC2) 中部署网关。您可以使用中提供的 Storag EC2 e Gateway AMI 在亚马逊中启动网关实例Amazon Web Services Marketplace。要开始使用 Storage Gateway AMI 部署网关，请参阅 为磁带网关部署自定义 Amazon EC2 实例。	2013 年 1 月 15 日

更改	描述	更改日期
支持缓存卷并推出了 API 版本 2012-06-30	在此版本中，Storage Gateway 引入了对缓存卷的支持。缓存卷可尽量避免扩展本地存储基础设施，还能为您的应用程序提供对其活动数据的低延迟访问。您可以创建容量高达 32 TiB 的存储卷，并从本地应用程序服务器将其安装为 iSCSI 设备。向缓存卷写入的数据将存储在 Amazon Simple Storage Service (Amazon S3) 中，而只有近期写入和读取的数据的缓存才会存储在本地存储硬件中。借助缓存卷，您可以对接受较高检索延迟的数据（例如不常访问的早期数据）使用 Amazon S3，同时为要求低延迟访问的数据在本地保留存储。 在此版本中，Storage Gateway 还引入了一个新的 API 版本，该版本除了支持当前的操作之外，还提供新操作来支持缓存卷。 有关两种 Storage Gateway 解决方案的更多信息，请参阅 磁带网关的工作原理。 您也可以尝试测试设置。有关说明，请参阅创建磁带网关。	2012 年 10 月 29 日

更改	描述	更改日期
API 和 IAM 支持	在此版本中，Storage Gateway 引入了 API 支持以及对 Amazon Identity and Access Management(IAM) 的支持。 • API 支持 - 您现在可以以编程方式配置和管理 Storage Gateway 资源。有关 API 的更多信息，请参阅《Amazon Storage Gateway 用户指南》中的 Storage Gateway 的 API 参考。 • IAM 支持 - 利用 Amazon Identity and Access Management (IAM)，您可以创建用户并通过 IAM 策略来管理用户对您的 Storage Gateway 资源的访问权限。有关 IAM 策略的示例，请参阅 Amazon Storage Gateway 的身份和访问管理。有关 IAM 的更多信息，请参阅 Amazon Identity and Access Management (IAM) 详情页面。	2012 年 5 月 9 日
支持静态 IP	您现在可以为本地网关指定静态 IP。有关更多信息，请参阅 配置网关网络。	2012 年 3 月 5 日
新指南	这是 Amazon Storage Gateway 用户指南的首个版本。	2012 年 1 月 24 日

磁带网关设备软件的发布说明

这些发布说明描述了磁带网关设备的每个版本中包含的新增功能和更新的功能、改进和修复。每个软件版本都由其发布日期和唯一版本号标识。

您可以通过在 Storage Gateway 控制台中查看网关的详细信息页面来确定网关的软件版本号，或者使用类似于以下内容的 Amazon CLI 命令调用 DescribeGatewayInformationAPI 操作：

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

版本号将在 API 响应的 `SoftwareVersion` 字段中返回。

> **Note**
>
> 在以下情况下，网关不会报告软件版本信息：
>
> - 网关处于离线状态。
> - 网关正在运行不支持版本报告的旧软件。
> - 网关类型为 FSx 文件网关。

有关 T ape G ateway V ateway 更新的更多信息，包括如何修改网关的默认自动维护和更新计划，请参阅使用 Storage Gateway 控制台管理网关更新使用 Amazon Storag 。 Amazon

发行日期	软件版本	发布说明
2025-05-01	2.12.8	• 更新了操作系统和软件元素，以提高新网关和现有网关的安全性和性能
2025-04-01	2.12.7	• 更新了操作系统和软件元素，以提高新网关和现有网关的安全性和性能
2025-03-04	2.12.6	• 更新了操作系统和软件元素，以提高新网关和现有网关的安全性和性能

发行日期	软件版本	发布说明
2025-02-04	2.12.5	• 更新了操作系统和软件元素，以提高新网关和现有网关的安全性和性能 • 解决了软件更新后网关可能卡在关闭状态的问题
2025-01-07	2.12.3	• 更新了操作系统和软件元素，以提高新网关和现有网关的安全性和性能
2024-12-06	2.12.2	• 更新了操作系统和软件元素，以提高新网关和现有网关的安全性和性能
2024-11-06	2.12.1	• 更新了操作系统和软件元素，以提高新网关和现有网关的安全性和性能
2024-10-03	2.12.0	• 更新了操作系统和软件元素，以提高新网关和现有网关的安全性和性能
2024-08-30	2.11.0	• 更新了操作系统和软件元素，以提高新网关和现有网关的安全性和性能
2024-07-29	2.10.0	• 更新了操作系统和软件元素，以提高新网关和现有网关的安全性和性能 • 其它错误修复和增强功能
2024-06-17	2.9.2	• 更新了操作系统和软件元素，以提高新网关和现有网关的安全性和性能

发行日期	软件版本	发布说明
2024-05-28	2.9.0	• 缩短了软件更新期间的网关重启时间 • 减少了用于估算网络带宽的数据传输量
2024-05-08	2.8.3	• 解决了使用 SOCKS5 代理服务器时的云连接问题 • 解决了在某些条件下（例如大量磁带擦除操作）上传性能降级的问题
2024-04-10	2.8.1	• 解决了 2.8.0 中引入的内存使用问题 • 安全补丁更新 • 改进了软件更新流程 • 修复了新网关缺少网络时间协议（NTP）组件的问题
2024-03-06	2.8.0	• 更新了操作系统和软件元素，以提高新网关的安全性和性能 • 安全补丁更新 • 提高了并发备份和还原工作负载的性能
2023-12-19	2.7.0	• 更新了操作系统和软件元素，以提高新网关的安全性和性能
2023-12-14	2.6.6	• 修复了大于 5 TiB 的磁带上的相对定位问题
2023-10-19	2.6.5	• 增加了保护措施，防止网关重启后客户端覆盖磁带

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