《磁帶閘道使用者指南》

AWS Storage Gateway

API 版本 2013-06-30

AWS Storage Gateway: 《磁帶閘道使用者指南》

Table of Contents

什麼是磁帶閘道？

AWS Storage Gateway 將內部部署軟體設備與雲端儲存連線，以便在內部部署 IT 環境和 AWS 儲存基礎設施之間提供與資料安全功能的無縫整合。您可以使用此服務將資料存放至 Amazon Web Services 雲端，以獲得可擴展且具有成本效益的儲存，協助維護資料安全。

您可以將 Storage Gateway 部署為內部部署，做為在 VMware ESXi、 KVM或 Microsoft Hyper-V Hypervisor 上執行的 VM 設備、硬體設備，或 AWS 部署為 Amazon EC2執行個體。您可以使用託管在EC2執行個體上的閘道進行災難復原、資料鏡像，並為託管在 Amazon 上的應用程式提供儲存空間 EC2。

若要查看 AWS Storage Gateway 有助於實現實現的廣泛使用案例，請參閱 AWS Storage Gateway。如需目前定價資訊，請參閱 詳細資訊頁面上的定價 AWS Storage Gateway 。

AWS Storage Gateway 提供檔案型 （ S3 File Gateway 和 FSx File Gateway ）、磁碟區型 （ 磁碟區閘道 ） 和磁帶型 （ 磁帶閘道 ） 儲存解決方案。

本使用者指南提供與磁帶閘道相關的資訊。

Tape Gateway 提供雲端支援的虛擬磁帶儲存。使用磁帶閘道，您可以在 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 中以符合成本效益且持久地封存備份資料。Tape Gateway 提供虛擬磁帶基礎設施，可根據您的業務需求無縫擴展，並消除佈建、擴展和維護實體磁帶基礎設施的操作負擔。

如需架構概觀，請參閱 磁帶閘道的運作方式。

在本使用者指南中，您可以找到入門區段，其中涵蓋所有閘道類型常見的設定資訊。您也可以找到磁帶閘道設定需求，以及描述如何部署、啟用、設定和管理磁帶閘道的章節。

本使用者指南中的程序主要著重於使用 執行閘道操作 AWS Management Console。如果您想要以程式設計方式執行這些操作，請參閱AWS Storage Gateway API參考 。

磁帶閘道的運作方式

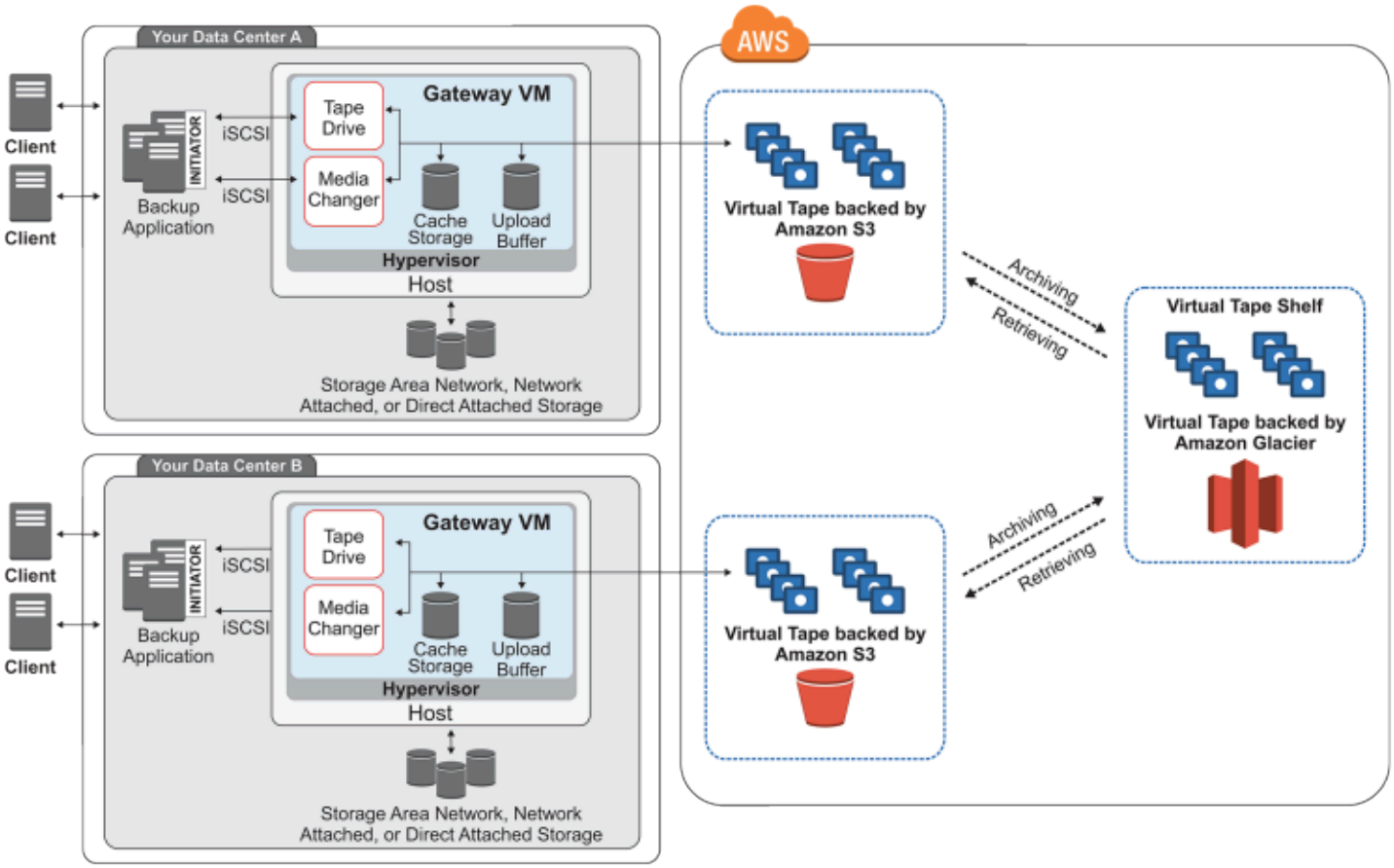
接下來，您可以尋找磁帶閘道解決方案的架構概觀。

磁帶閘道

磁帶閘道提供耐久且具有成本效益的解決方案，以將資料存檔至 Amazon Web Services 雲端。透過其虛擬磁帶程式庫 （ VTL ） 介面，您可以使用現有的磁帶型備份基礎設施，將資料存放在您在磁帶閘道

上建立的虛擬磁帶卡匣上。每個磁帶閘道都已預先設定媒體更換器和磁帶機。這些可作為 iSCSI 裝置的現有用戶端備份應用程式使用。在您需要存檔資料時，可以新增磁帶匣。

下圖概述磁帶閘道部署。



此圖表識別下列磁帶閘道元件：

- 虛擬磁帶 – 虛擬磁帶就像實體磁帶匣。不過，虛擬磁帶資料存放至 Amazon Web Services 雲端。就像實體磁帶，虛擬磁帶可以空白，也可以在其上寫入資料。您可以使用 Storage Gateway 主控台建立虛擬磁帶，或使用 Storage Gateway 以程式設計方式建立虛擬磁帶API。每個閘道一次最多可以包含 1,500 個磁帶或 1 PiB 的總磁帶資料。您在建立磁帶時可設定的每個虛擬磁帶大小介於 100 GiB 與 15 TiB 之間。
- 虛擬磁帶程式庫 （ VTL ） – VTL就像現場提供的實體磁帶程式庫，具有機器人機臂和磁帶機。您的VTL包含儲存的虛擬磁帶集合。每個磁帶閘道都隨附一個 VTL。

  您建立的虛擬磁帶會顯示在閘道的 中VTL。中的磁帶由 Amazon S3 VTL 備份。當備份軟體將資料寫入閘道時，閘道會在本機儲存資料，然後非同步地將其上傳至 中的虛擬磁帶VTL，也就是 Amazon S3。

  - 磁帶機 – VTL磁帶機類似於可以執行 I/O 並在磁帶上尋找操作的實體磁帶機。每個 VTL 都隨附一組 10 個磁帶機，可供備份應用程式作為 iSCSI 裝置使用。
  - 媒體變更器 – VTL 媒體變更器類似於機器人，在實體磁帶庫的儲存插槽和磁帶機中移動磁帶。每個 VTL 都隨附一個媒體變更器，可供您的備份應用程式作為 iSCSI 裝置使用。
- 存檔 – 存檔類似離站磁帶存放設施。您可以將磁帶從閘道封存VTL到封存。如有需要，您可以將磁帶從封存擷取回閘道的 VTL。
  - 存檔磁帶 – 當您的備份軟體退出磁帶時，閘道會將磁帶移至存檔以供長期儲存。存檔位於您已啟用閘道的 AWS 區域。封存中的磁帶會存放在虛擬磁帶架（）中VTS。由 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive VTS提供支援，提供低成本儲存服務，用於資料封存、備份和長期資料保留。
  - 擷取磁帶 – 您無法直接讀取存檔磁帶。若要讀取封存磁帶，您必須先使用 Storage Gateway 主控台或 Storage Gateway ，將其擷取至磁帶閘道API。

    > **Important**
    >
    > 若您在 S3 Glacier Flexible Retrieval 中存檔磁帶，您通常可以在 3 到 5 小時內擷取磁帶。如果您在 S3 Glacier Deep Archive 中存檔磁帶，通常可以在 12 小時內擷取它。

在部署和啟用磁帶閘道之後，您將虛擬磁帶機和媒體更換器作為 iSCSI 裝置掛載到內部部署應用程式伺服器上。您可以視需要建立虛擬磁帶。然後，您可以使用現有備份軟體應用程式，將資料寫入至虛擬磁帶。媒體更換器會將虛擬磁帶載入和卸載至虛擬磁帶機，以執行讀取和寫入操作。

配置閘道 VM 的本機磁碟

您的閘道 VM 需要基於下列目的而配置的本機磁碟：

- 快取儲存：快取儲存做為耐久存放區來存放等待從上傳緩衝區上傳至 Amazon S3 的資料。

  如果您的應用程式讀取虛擬磁帶中的資料，則閘道會將資料儲存至快取儲存。閘道會將最近存取的資料存放至快取儲存，以供低延遲存取。如果您的應用程式請求磁帶資料，閘道會先檢查資料的快取儲存體，然後再從 下載資料 AWS。
- 上傳緩衝區：上傳緩衝區會先提供閘道的暫存區域，再將資料上傳至虛擬磁帶。上傳緩衝區對於建立您可用來復原磁帶之意外故障的復原點也很重要。如需詳細資訊，請參閱您需要從故障的磁帶閘道復原虛擬磁帶。

您的備份應用程式將資料寫入至閘道時，閘道會將資料複製至快取儲存和上傳緩衝區。它接著會確認完成備份應用程式的寫入操作。

如需配置給快取儲存和上傳緩衝區之磁碟空間量的準則，請參閱決定本機磁碟儲存體的數量。

入門 AWS Storage Gateway

本節提供開始使用 的指示 AWS。您需要一個 AWS 帳戶，才能開始使用 AWS Storage Gateway。您可以使用現有 AWS 帳戶，或註冊新帳戶。您也需要 AWS 帳戶中屬於具有執行 Storage Gateway 任務必要管理許可之群組IAM的使用者。具有適當權限的使用者可以存取 Storage Gateway 主控台和 Storage GatewayAPI，以執行閘道部署、組態和維護任務。如果您是第一次使用 ，建議您在使用 Storage Gateway 之前，先檢閱支援的 AWS 區域和磁帶閘道設定需求區段。

本節包含下列主題，提供開始使用 的額外資訊 AWS Storage Gateway：

主題

- 註冊 AWS Storage Gateway - 了解如何註冊 AWS 和建立 AWS 帳戶。
- 建立具有管理員權限IAM的使用者 - 了解如何為 AWS 您的帳戶建立具有管理權限IAM的使用者。
- 存取 AWS Storage Gateway - 了解如何 AWS Storage Gateway 透過 Storage Gateway 主控台或以程式設計方式使用 進行 AWS 存取SDKs。
- AWS 區域 支援 Storage Gateway - 了解當您在 Storage Gateway 中啟用閘道時，可以使用哪些 AWS 區域來儲存資料。

註冊 AWS Storage Gateway

AWS 帳戶 是存取 AWS 服務的基本要求。您的 AWS 帳戶 是作為 AWS 使用者建立的所有 AWS 資源的基本容器。您的 AWS 帳戶 也是 資源 AWS 的基本安全界限。您在帳戶中建立的任何資源，都可供擁有帳戶憑證的使用者使用。您必須先註冊 AWS Storage Gateway，才能開始使用 AWS 帳戶。

如果您沒有 AWS 帳戶，請完成下列步驟以建立 。

若要註冊 AWS 帳戶

1. 開啟https://portal.aws.amazon.com/billing/註冊 。
2. 請遵循線上指示進行。

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   當您註冊 時 AWS 帳戶，AWS 帳戶根使用者會建立 。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

我們也建議您要求使用者在存取 時使用臨時憑證 AWS。若要提供臨時憑證，您可以使用聯合和身分提供者，例如 AWS IAM身分中心。如果您的公司已使用身分提供者，您可以搭配聯合使用，以簡化您提供 AWS 帳戶資源存取權的方式。

建立具有管理員權限IAM的使用者

建立 AWS 帳戶後，請使用下列步驟為自己建立 AWS Identity and Access Management （ IAM ） 使用者，然後將該使用者新增至具有管理許可的群組。如需使用 AWS Identity and Access Management 服務控制 Storage Gateway 資源存取權的詳細資訊，請參閱 Identity and Access Management for AWS Storage Gateway。

若要建立管理員使用者，請選擇下列其中一個選項。

選擇一種管理管理員的方式	到	By	您也可以
在IAM身分中心 (建議)	使用短期憑證存取 AWS。 這與安全性最佳實務一致。如需最佳實務的相關資訊，請參閱 IAM 使用者指南 中的安全最佳實務IAM。	請遵循 AWS IAM Identity Center 使用者指南的入門中的說明。	透過在 AWS Command Line Interface 使用者指南 中設定AWS CLI 要使用的 來設定 AWS IAM Identity Center程式設計存取。
在 中 IAM (不建議使用)	使用長期憑證存取 AWS。	遵循 IAM 使用者指南 IAM 中建立第一個管理員使用者和使用者群組的指示。	在 IAM 使用者指南 中管理IAM 使用者的存取金鑰，以設定程式設計存取。

> **Warning**
>
> IAM 使用者有長期憑證，這會造成安全風險。為了協助降低此風險，建議您只為這些使用者提供執行任務所需的許可，並在不再需要這些使用者時將其移除。

存取 AWS Storage Gateway

您可以使用 AWS Storage Gateway 主控台來執行各種閘道組態和維護任務，包括從部署中啟動或移除 Storage Gateway 硬體設備、建立、管理及刪除不同類型的閘道、在虛擬磁帶庫儲存磁碟區中，以及監控 Storage Gateway 服務各種元素的運作狀態和狀態。為了簡單易用，本指南著重於使用 Storage Gateway 主控台 Web 介面執行任務。您可以透過網頁瀏覽器存取 Storage Gateway 主控台，網址為：https://console.aws.amazon.com/storagegateway/home/。

如果您偏好程式設計方法，則可以使用 AWS Storage Gateway 應用程式介面（API）或命令列介面（CLI）來設定和管理 Storage Gateway 部署中的資源。如需 Storage Gateway 的動作、資料類型和所需語法的詳細資訊API，請參閱 Storage Gateway API參考 。如需 Storage Gateway 的詳細資訊CLI，請參閱 AWS CLI 命令參考 。

您也可以使用 AWS SDKs來開發與 Storage Gateway 互動的應用程式。 AWS SDKs 適用於 Java、.NET和 PHP 包裝基礎 Storage GatewayAPI，以簡化您的程式設計任務。如需下載SDK程式庫的相關資訊，請參閱 AWS Developer Center 。

如需定價的詳細資訊，請參閱 AWS Storage Gateway 定價。

AWS 區域 支援 Storage Gateway

AWS 區域 是世界上 AWS 具有多個可用區域的實體位置。可用區域由一或多個離散 AWS 資料中心組成，每個資料中心都具有備援電源、聯網和連線能力，並存放在個別設施中。這表示每個 AWS 區域 都已實際隔離，且獨立於其他 區域。區域提供容錯能力、穩定性和恢復能力，也可降低延遲。除非您明確使用 AWS 服務提供的複寫功能，否則您在一個區域中建立的資源不存在於任何其他區域中。例如，Amazon S3 和 Amazon EC2支援跨區域複寫。有些服務，例如 AWS Identity and Access Management，沒有區域資源。您可以在符合您業務需求的位置啟動 AWS 資源。例如，您可能想要啟動 Amazon EC2執行個體，以 AWS 區域 在歐洲的 中託管您的 AWS Storage Gateway 設備，以便更接近您的歐洲使用者，或滿足法律要求。您的 會 AWS 帳戶 決定特定服務支援的 區域，供您使用。

- Storage Gateway — 如需支援 AWS 的區域和服務 AWS 端點清單 Storage Gateway ，請參閱 中的AWS Storage Gateway 端點和配額AWS 一般參考。
- Storage Gateway 硬體設備 — 如需可與硬體設備搭配使用的支援 AWS 區域，請參閱 中的AWS Storage Gateway 硬體設備區域AWS 一般參考。

設定磁帶閘道的需求

除非另有說明，否則以下需求皆為所有閘道組態的常見需求。

主題

硬體及儲存體需求

本節描述您閘道之最低硬體及設定的相關資訊，以及配置必要儲存體所需的最小磁碟空間。

的硬體需求 VMs

在部署您的閘道時，您必須確保要部署閘道 VM 的基礎硬體可專用於下列基本資源：

- 指派給 VM 的四個虛擬處理器。
- 對於磁帶閘道 ，您的硬體應專用以下金額的 RAM：
  - RAM 為快取大小高達 16 GiB的閘道預留 16 GiB TiB
  - 為快取大小RAM為 16 TiB GiB的閘道預留 32 TiB
  - 為快取大小RAM為 32 TiB GiBTiB
- 安裝 VM 映像和系統資料的 80 GiB 磁碟空間。

如需詳細資訊，請參閱最佳化閘道效能。如需您硬體影響閘道 VM 效能之方式的資訊，請參閱 AWS Storage Gateway 配額。

Amazon EC2執行個體類型的需求

在 Amazon Elastic Compute Cloud （Amazon EC2） 上部署閘道時，執行個體大小必須至少為 xlarge，閘道才能運作。但是，針對運算最佳化的執行個體系列，大小必須至少為 2xlarge。

> **Note**
>
> Storage Gateway AMI僅與使用 Intel 或AMD處理器的 x86 型執行個體相容。ARM不支援使用 Graviton 處理器的 型執行個體。

對於磁帶閘道 ，您的 Amazon EC2執行個體應根據您計劃用於閘道RAM的快取大小，指定下列數量的 ：

- RAM 為快取大小高達 16 GiB的閘道預留 16 GiB TiB
- 為快取大小RAM為 16 TiB GiB的閘道預留 32 TiB
- 為快取大小RAM為 32 TiB GiBTiB

請針對您的閘道類型，使用下列其中一個建議的執行個體類型。

快取磁碟區及磁帶閘道類型的建議項目

- 一般用途執行個體系列：m4、m5 或 m6 執行個體類型。

  > **Note**
  >
  > 我們不建議使用 m4.16xlarge 執行個體類型。

- 運算最佳化執行個體系列：c4、c5 或 c6 執行個體類型。選擇 2xlarge 或更高的執行個體大小，以符合必要的RAM需求。
- 記憶體最佳化執行個體系列：r3、r5 或 r6 執行個體類型。
- 儲存體最佳化執行個體系列：i3 或 i4 執行個體類型。

儲存需求

除了 VM 的 80 GiB 磁碟空間之外，您的閘道也需要額外的磁碟。

下表針對您所部署的閘道建議本機磁碟儲存體大小。

閘道類型	快取 (最小值)	快取 (最大值)	上傳緩衝區 (最小值)	上傳緩衝區 (最大值)	其他必要的本機磁碟
磁帶閘道	150 GiB	64 TiB	150 GiB	2 TiB	—

> **Note**
>
> 您可以為快取和上傳緩衝區設定一個或多個本機磁碟機，上限為最大容量。
> 在將快取或上傳緩衝區新增至現有閘道時，請務必在主機（Hypervisor 或 Amazon EC2執行個體）中建立新的磁碟。如果先前已將磁碟配置為快取或上傳緩衝區，請勿變更現有磁碟的大小。

如需閘道配額的詳細資訊，請參閱 AWS Storage Gateway 配額。

網路與防火牆需求

您的閘道需要存取網際網路、本機網路、網域名稱服務（DNS）伺服器、防火牆、路由器等。您可以在以下內容找到必要連接埠及如何允許透過防火牆及路由器進行存取的相關資訊。

> **Note**
>
> 在某些情況下，您可以在 Amazon 上部署 Storage Gateway，EC2或使用其他類型的部署（包括內部部署）搭配限制 AWS IP 地址範圍的網路安全政策。在這些情況下，當 AWS IP 範圍值變更時，您的閘道可能會遇到服務連線問題。您需要使用的 AWS IP 地址範圍值位於您啟用閘道之 AWS 區域的 Amazon 服務子集中。如需有關目前 IP 範圍值的資訊，請參閱 AWS 一般參考 中的 AWS IP 地址範圍。

> **Note**
>
> 網路頻寬要求會根據閘道上傳及下載的資料數量而有所不同。至少需要 100Mbps 才能成功下載、啟用和更新閘道。您的資料傳輸模式將決定支援工作負載所需的頻寬。在某些情況下，您可以在 Amazon 上部署 Storage Gateway EC2或使用其他類型的部署

主題

- 連接埠需求
- Storage Gateway 硬體設備的網路與防火牆要求
- 允許透過防火牆和路由器 AWS Storage Gateway 存取
- 為您的 Amazon EC2閘道執行個體設定安全群組

連接埠需求

Storage Gateway 的操作需要允許特定的連接埠。下圖顯示您必須為每一種類型的閘道允許的必要連接埠。有些連接埠為所有閘道類型的必要連接埠，其他的則為特定閘道類型的必要連接埠。如需連接埠需求的詳細資訊，請參閱Tape Gateway 的連接埠需求。

所有閘道類型的常見連接埠

以下為所有閘道類型常見的連接埠，所有閘道磁帶均需使用到。

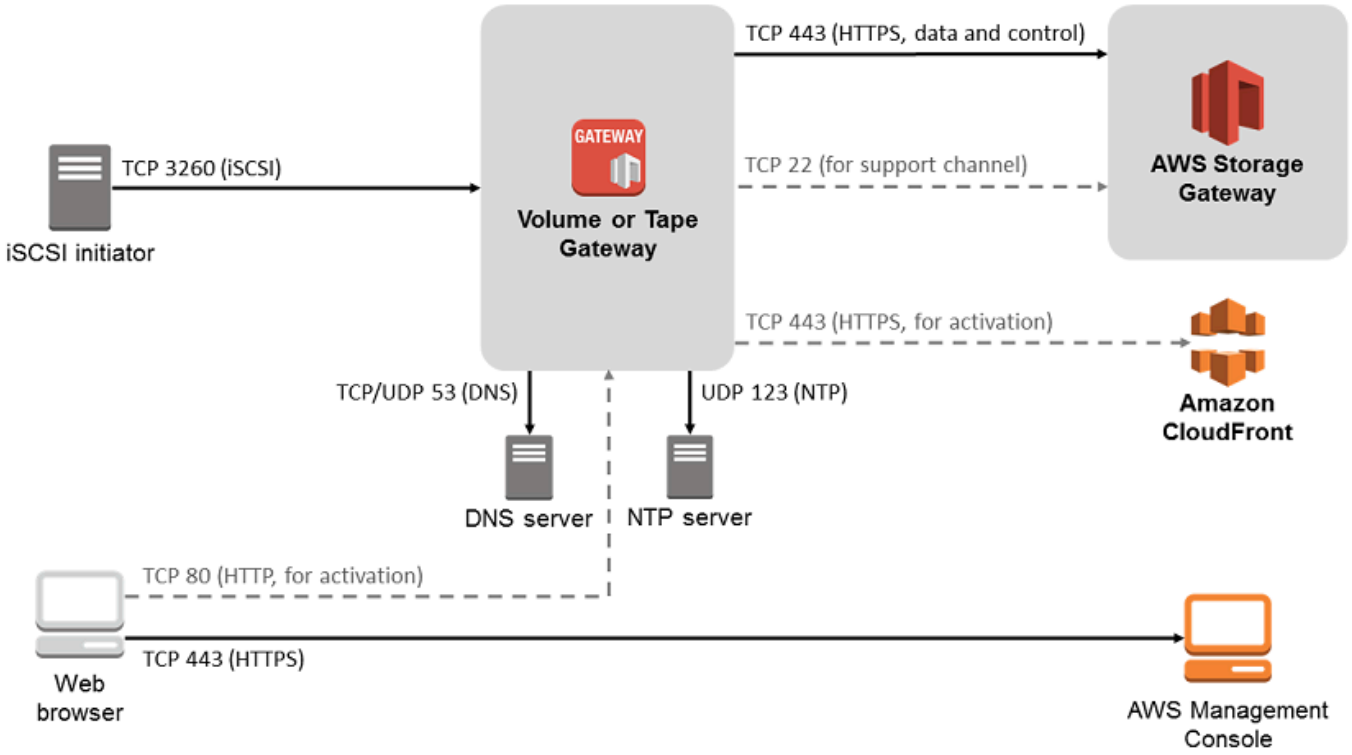
通訊協定	連線埠	Direction	來源	目的地	使用方式
TCP	443（HTTPS）	傳出	Storage Gateway	AWS	用於從 Storage Gateway 到 AWS 服務端點的通訊。如需服務端點的資訊，請參閱允許透過防火牆和路由器 AWS Storage Gateway 存取。
TCP	80（HTTP）	傳入	您從中連線至 AWS 管理主控台的主機。	Storage Gateway	由本機系統取得 Storage Gateway 啟用金鑰。僅有在啟用 Storage

通訊協定	連線埠	Direction	來源	目的地	使用方式
					Gateway 裝置時，才會使用連接埠 80。 Storage Gateway 不需要可公開存取連接埠 80。連接埠 80 所需的存取權限級別取決於您的網路設定。若您是以 Storage Gateway 管理主控台啟動您的閘道，則您連線至主控台的主機必須擁有閘道連接埠 80 的存取權限。
TCP/UDP	53 （DNS）	傳出	Storage Gateway	網域名稱服務（DNS） 伺服器	用於 Storage Gateway 與 DNS伺服器之間的通訊。

通訊協定	連線埠	Direction	來源	目的地	使用方式
TCP	22 (支援通道)	傳出	Storage Gateway	AWS Support	允許 AWS Support 存取您的閘道，以協助您疑難排解閘道問題。不需要將此埠開放給閘道的正常操作使用，但進行疑難排解時需要用到。
UDP	123 （NTP）	傳出	NTP 用戶端	NTP 伺服器	本機系統用來將 VM 的時間與主機時間同步。

磁碟區及磁帶閘道的連接埠

下圖顯示要為磁帶閘道開啟的連接埠。



除了常用的連接埠之外，磁帶閘道還需要下列連接埠。

通訊協定	連線埠	Direction	來源	目的地	使用方式
TCP	3260 （iSCSI）	傳入	iSCSI 啟動器	Storage Gateway	由本機系統連線到閘道公開的 iSCSI 目標。

如需連接埠要求的詳細資訊，請參閱其他 Storage Gateway 資源區段中的 Tape Gateway 的連接埠需求。

Storage Gateway 硬體設備的網路與防火牆要求

每個 Storage Gateway 硬體設備都需要下列網路服務：

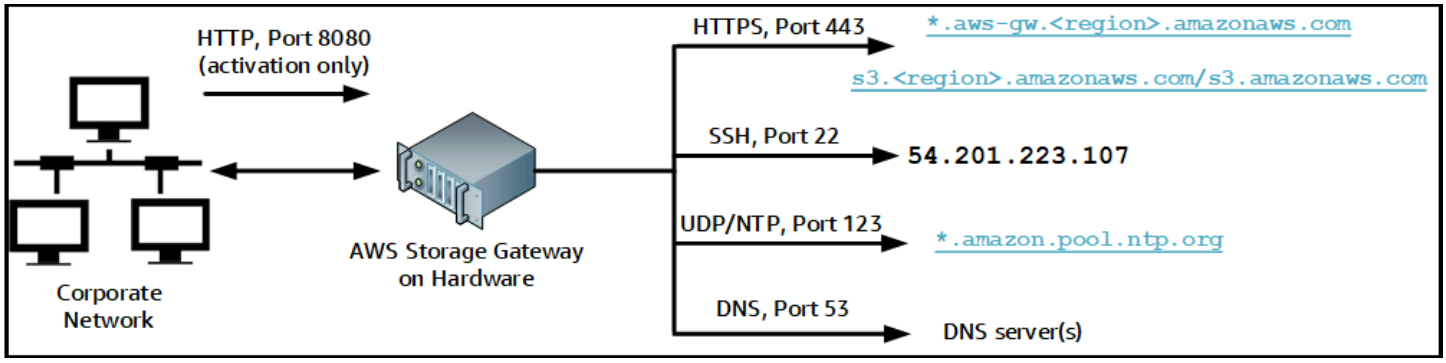
- 網際網路存取：透過任何伺服器上的網路介面，全年無休的連線到網際網路。
- DNS 服務 – 硬體設備與DNS伺服器之間的通訊DNS服務。
- 時間同步 – 必須能夠連線自動設定的 Amazon NTP時間服務。

- IP 地址 – 指派的 DHCP或 靜態IPv4地址。您無法指派IPv6地址。

Dell PowerEdge R640 伺服器後方有五個實體網路連接埠。從左到右 (面向伺服器的背面)，這些連接埠如下所示：

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

您可以使用 iDRAC 連接埠進行遠端伺服器管理。



硬體設備需要以下連接埠才能運作。

通訊協定	連線埠	Direction	來源	目的地	使用方式
SSH	22	傳出	硬體設備	54.201.223.107	支援通道
DNS	53	傳出	硬體設備	DNS 伺服器	名稱解析
UDP/NTP	123	傳出	硬體設備	*.amazon.pool.ntp.org	時間同步
HTTPS	443	傳出	硬體設備	*.amazonaws.com	資料傳輸

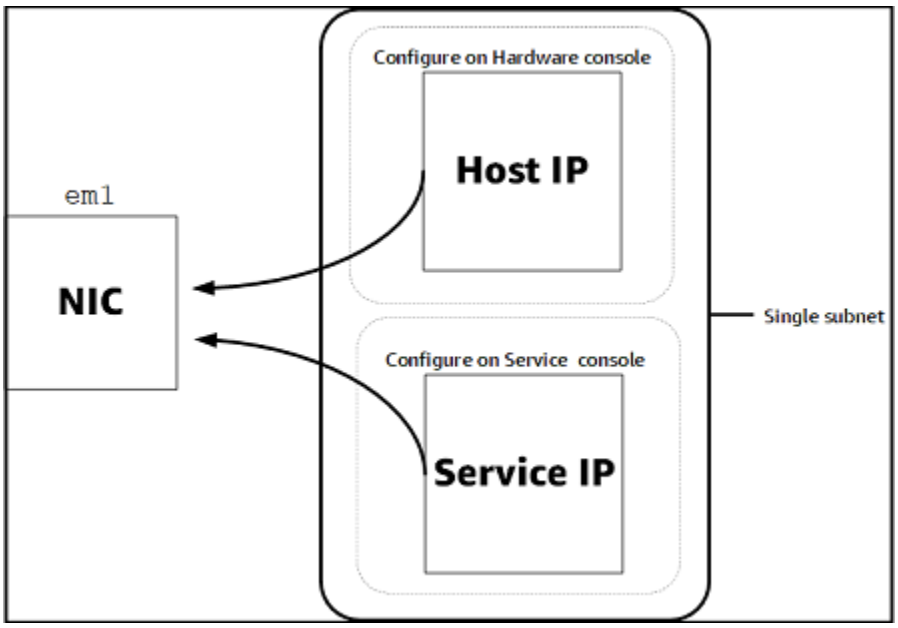
通訊協定	連線埠	Direction	來源	目的地	使用方式
HTTP	8080	傳入	AWS	硬體設備	啟用 (只需短暫時間)

若要依設計方式執行，硬體設備需要如下所示的網路和防火牆設定：

- 在硬體主控台設定所有連接的網路介面。
- 確保每個網路介面位於唯一的子網路。
- 提供所有連接網路介面可以對外存取前面的圖表中所列的端點。
- 至少設定一個網路介面來支援硬體設備。如需詳細資訊，請參閱設定硬體設備網路參數。

> **Note**
>
> 若要查看顯示伺服器背面及其連接埠的插圖，請參閱實際安裝您的硬體設備

相同網路介面 （NIC） 上的所有 IP 地址，無論是閘道或主機，都必須位於相同的子網路上。下圖顯示了定址配置。



如需啟動和設定硬體設備的詳細資訊，請參閱使用 Storage Gateway 硬體設備。

允許透過防火牆和路由器 AWS Storage Gateway 存取

您的閘道需要存取下列服務端點，才能與 通訊 AWS。若您使用防火牆或路由器來篩選或限制網路流量，則必須設定防火牆和路由器，以允許這些服務端點可與 AWS進行傳出通訊。

> **Note**
>
> 如果您將 Storage Gateway 的私有VPC端點設定為用於 的連線和往返 的資料傳輸 AWS，則閘道不需要存取公有網際網路。如需詳細資訊，請參閱在虛擬私有雲端中啟用閘道。

> **Important**
>
> 根據閘道 AWS 的區域，取代 *region* 在具有正確區域字串的服務端點中。

所有閘道都需要下列服務端點，才能進行頭部儲存貯體的操作。

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

下列服務端點為所有閘道的必要項目，用於控制路徑 (anon-cp、client-cp、proxy-app) 及資料路徑 (dp-1) 操作。

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

需要下列閘道服務端點才能API撥打電話。

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

下列範例是美國西部 (奧勒岡) 區域 (us-west-2) 中的閘道服務端點。

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

以下顯示的 Amazon S3 服務端點僅由檔案閘道使用。檔案閘道需要此端點來存取檔案共享映射的 S3 儲存貯體。

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

下列範例是美國東部 (俄亥俄) 區域 (us-east-2) 中的 S3 服務端點。

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

> **Note**
>
> 如果您的閘道無法判斷 S3 儲存貯體所在的 AWS 區域，此服務端點會預設為 s3.us-east-1.amazonaws.com。建議您除了您的閘道啟用所在、以及 S3 儲存貯體所在的 AWS 區域之外，也允許存取美國東部 (維吉尼亞北部) 區域 (us-east-1)。

下列是 AWS GovCloud (US) 區域的 S3 服務端點。

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

下列範例是 AWS GovCloud （美國西部） 區域中 S3 儲存貯體FIPS的服務端點。

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

Storage Gateway VM 設定為使用下列NTP伺服器。

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

- Storage Gateway — 如需支援 AWS 的區域和服務 AWS 端點清單 Storage Gateway ，請參閱 中的AWS Storage Gateway 端點和配額AWS 一般參考。
- Storage Gateway 硬體設備 — 如需可與硬體設備搭配使用的支援 AWS 區域，請參閱 中的 Storage Gateway 硬體設備區域AWS 一般參考。

為您的 Amazon EC2閘道執行個體設定安全群組

安全群組會控制 Amazon EC2閘道執行個體的流量。當您設定安全群組時，建議使用下列各項：

- 安全群組不應該允許來自外部網際網路的傳入連線。它只應該允許閘道安全群組內的執行個體與閘道通訊。如果您需要允許執行個體從安全群組外部連線至閘道，建議您僅允許連接埠 3260（iSCSI 連線）和 80（啟用）上的連線。
- 如果您想要從閘道安全群組外部的 Amazon EC2 主機啟用閘道，請允許連接埠 80 上來自該主機 IP 地址的傳入連線。如果您無法判斷啟用主機的 IP 地址，則可以開啟連接埠 80，並啟用閘道，然後在完成啟用後關閉連接埠 80 上的存取。
- 只有在您使用 AWS Support 進行疑難排解時，才允許連接埠 22 存取。如需詳細資訊，請參閱您想 AWS Support 要協助疑難排解EC2閘道。

在某些情況下，您可能會使用 Amazon EC2執行個體作為啟動器（亦即，連線到您在 Amazon 上部署的閘道上的 iSCSI 目標EC2。在這種情況下，建議使用兩個步驟的方法：

1. 您應該啟動與閘道相同之安全群組中的啟動器執行個體。
2. 您應該設定存取權，讓啟動器可以與您的閘道通訊。

如需要針對閘道所開啟之連接埠的資訊，請參閱Tape Gateway 的連接埠需求。

支援的 Hypervisor 與主機需求

您可以將 Storage Gateway 內部部署作為虛擬機器（VM）設備、實體硬體設備，或 AWS 作為 Amazon EC2執行個體在 中執行。

> **Note**
>
> 當製造商結束對 Hypervisor 版本的一般支援時，Storage Gateway 也將結束對該 Hypervisor 版本的支援。如需有關特定 Hypervisor 版本支援的詳細資訊，請參閱製造商的說明文件。

Storage Gateway 支援下列 Hypervisor 版本與主機：

- VMware ESXi Hypervisor（7.0 或 8.0 版）– 在此設定中，您也需要VMware vSphere 用戶端來連線至主機。

- Microsoft Hyper-V Hypervisor (2012 R2、2016、2019 或 2022 版本)：Hyper-V 的免費、獨立版本可從 Microsoft 下載中心取得。針對此設定，您需要 Microsoft Windows 用戶端電腦上的 Microsoft Hyper-V 管理員以連線到主機。
- Linux 核心型虛擬機器 （KVM） – 免費開放原始碼虛擬化技術。KVM 包含在 Linux 2.6.20 版及更新版本的所有版本中。Storage Gateway 已針對 CentOS /RHEL 7.7、Ubuntu 16.04 LTS和 Ubuntu 18.04 LTS分佈進行測試和支援。任何其他現代 Linux 發行版都可以運作，但不保證功能或性能。如果您已經啟動並執行KVM環境，而且已經熟悉KVM運作方式，建議您使用此選項。
- Amazon EC2執行個體 – Storage Gateway 提供包含閘道 VM 映像的 Amazon Machine Image （AMI）。只有檔案、快取磁碟區和磁帶閘道類型可以部署在 Amazon 上EC2。如需有關如何在 Amazon 上部署閘道的資訊EC2，請參閱 部署適用於磁帶閘道的自訂 Amazon EC2執行個體。
- Storage Gateway 硬體設備：Storage Gateway 以內部部署選項形式，為具有有限虛擬機器基礎設施的位置提供實體硬體設備。

> **Note**
>
> Storage Gateway 不支援從從其他閘道 VM 的快照或複製建立的 VM 或從 Amazon EC2 復原閘道AMI。若您的閘道 VM 發生問題，請啟用新的閘道並將您的資料復原至該閘道。如需詳細資訊，請參閱從非預期的虛擬機器關機復原。
> Storage Gateway 不支援動態記憶體和虛擬記憶體佔用。

支援的 iSCSI 啟動器

部署磁帶閘道時，會使用一個媒體變更器和 10 個磁帶機預先設定閘道。這些磁帶機和媒體變更器可作為 iSCSI 裝置提供給現有的用戶端備份應用程式。

若要連線至這些 iSCSI 裝置，Storage Gateway 支援下列 iSCSI 啟動器：

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows 10
- Windows 8.1
- Red Hat Enterprise Linux 5
- Red Hat Enterprise Linux 6

- Red Hat Enterprise Linux 7
- VMware ESX Initiator，提供在 的訪客作業系統中使用 Initiator 的替代方案 VMs

> **Important**
>
> Storage Gateway 不支援來自 Windows 用戶端的 Microsoft Multipath I/O （MPIO）。如果主機使用 Windows Server 容錯移轉叢集 （ ） 協調存取，則 Storage Gateway 支援將多個主機連接到相同的磁碟區WSFC。但是，如果不使用 ，則無法將多個主機連接到相同的磁碟區 （例如共用非叢集 NTFS/ext4 檔案系統）WSFC。

磁帶閘道支援的第三方備份應用程式

您可以與磁帶閘道使用備份應用程式讀取、寫入和管理磁帶。下列支援的第三方備份應用程式可與磁帶閘道使用。

您選擇的媒體變更器類型取決於您計劃使用的備份應用程式。下表列出了已通過測試且發現與磁帶閘道相容的第三方備份應用程式。此表格包含建議用於每個備份應用程式的媒體變更器類型。

備份應用程式	媒體變更器類型
Arcserve Backup	`AWS-Gateway-VTL`
Bacula Enterprise V10.x	`AWS-Gateway-VTL` 或 `STK-L700`
Commvault V11	`STK-L700`
Dell EMC NetWorker 19.5	`AWS-Gateway-VTL`
IBM Spectrum Protect v8.1.10	`IBM-03584L32-0402`
Micro Focus （HPE） Data Protector 9 或 11.x	`AWS-Gateway-VTL`
Microsoft System Center 2012 R2 或 2016 Data Protection Manager	`STK-L700`
NovaStor DataCenter/Network 6.4 或 7.1	`STK-L700`
Quest NetVault Backup 12.4 或 13.x	`STK-L700`

備份應用程式	媒體變更器類型
Veeam Backup & Replication 11A	`AWS-Gateway-VTL`
Veritas Backup Exec 2014 或 15 或 16 或 20 或 22.x	`AWS-Gateway-VTL`
Veritas Backup Exec 2012 **Note** Veritas 已終止對 Backup Exec 2012 的支援。	`STK-L700`
Veritas 7.x 版或 8.x NetBackup 版	`AWS-Gateway-VTL`

Important

我們強烈建議您選擇為備份應用程式列出的媒體變更器。其他媒體變更器可能無法正常運作。啟用閘道之後，您可以選擇不同的媒體變更器類型。如需詳細資訊，請查閱在啟用閘道後選取媒體變更器。

使用 Storage Gateway 硬體設備

Storage Gateway 硬體設備是一種實體硬體設備，其 Storage Gateway 軟體已預先安裝在經過驗證的伺服器組態上。您可以從 AWS Storage Gateway 主控台的硬體設備概觀頁面管理部署中的硬體設備。

每個硬體設備都是高效能的 1U 伺服器，您可以部署在您的資料中心內或內部部署在公司防火牆內。當您購買並啟用硬體設備時，啟用程序會將硬體設備與您的 建立關聯 AWS 帳戶。啟用之後，您的硬體設備會出現在主控台中，做為硬體設備概觀頁面上的閘道。您可以將硬體設備設定為 S3 File Gateway、FSxFile Gateway、磁帶閘道或磁碟區閘道類型。您用來在硬體設備上部署和啟用這些閘道類型的程序，與在虛擬平台上相同。

如需 AWS 區域 Storage Gateway 硬體設備可供啟用和使用的支援清單，請參閱 中的 Storage Gateway 硬體設備區域AWS 一般參考。

在下列各節中，您可以找到如何設定、機架掛載、電源、設定、啟用、啟動、使用和刪除 Storage Gateway 硬體設備的指示。

主題

設定 Storage Gateway 硬體設備

收到 Storage Gateway 硬體設備後，您可以使用硬體設備主控台來設定聯網，以提供與設備永遠連線 AWS 並啟用設備。啟用會將您的設備與啟用程序期間使用的 AWS 帳戶建立關聯。啟用裝置之後，您可以在 Storage Gateway 主控台中啟動檔案、磁碟區或磁帶閘道。

若要安裝並設定硬體設備，請執行下列步驟：

1. 將裝置掛載到機架上，並插上電源和網路連線。如需詳細資訊，請參閱實際安裝您的硬體設備。
2. 設定硬體設備（主機IPv4）和 Storage Gateway（服務）的網際網路通訊協定第 4 版（）地址。如需詳細資訊，請參閱設定硬體設備網路參數。
3. 在您選擇的 AWS 區域中的主控台硬體設備概觀頁面上啟用硬體設備。如需詳細資訊，請參閱啟用 Storage Gateway 硬體設備。
4. 在您的硬體設備上安裝 Storage Gateway。如需詳細資訊，請參閱建立和啟用磁帶閘道。

   您可以在硬體設備上設定閘道，方法與在 VMware ESXi、Microsoft Hyper-V、Linux Kernel 型虛擬機器（KVM）或 Amazon 上設定閘道相同EC2。

增加可使用的快取儲存體

您可以將硬體設備上的可用儲存體從 5 TB 增加至 12 TB。這樣做可提供更大的快取，以低延遲存取 中的資料 AWS。如果您訂購 5 TB 模型，您可以購買五個 1.92 TB SSDs（固態磁碟機），將可用儲存體增加到 12 TB。

然後，您可以將它們加入到硬體設備後再啟用它。如果您已經啟動硬體設備，並想要將裝置上的可用儲存體增加至 12 TB，請執行下列操作：

1. 將硬體設備重設為出廠設定。如需如何執行此操作的指示，請聯絡 AWS 支援。
2. 將五個 1.92 TB SSDs 新增至設備。

NIC 選項

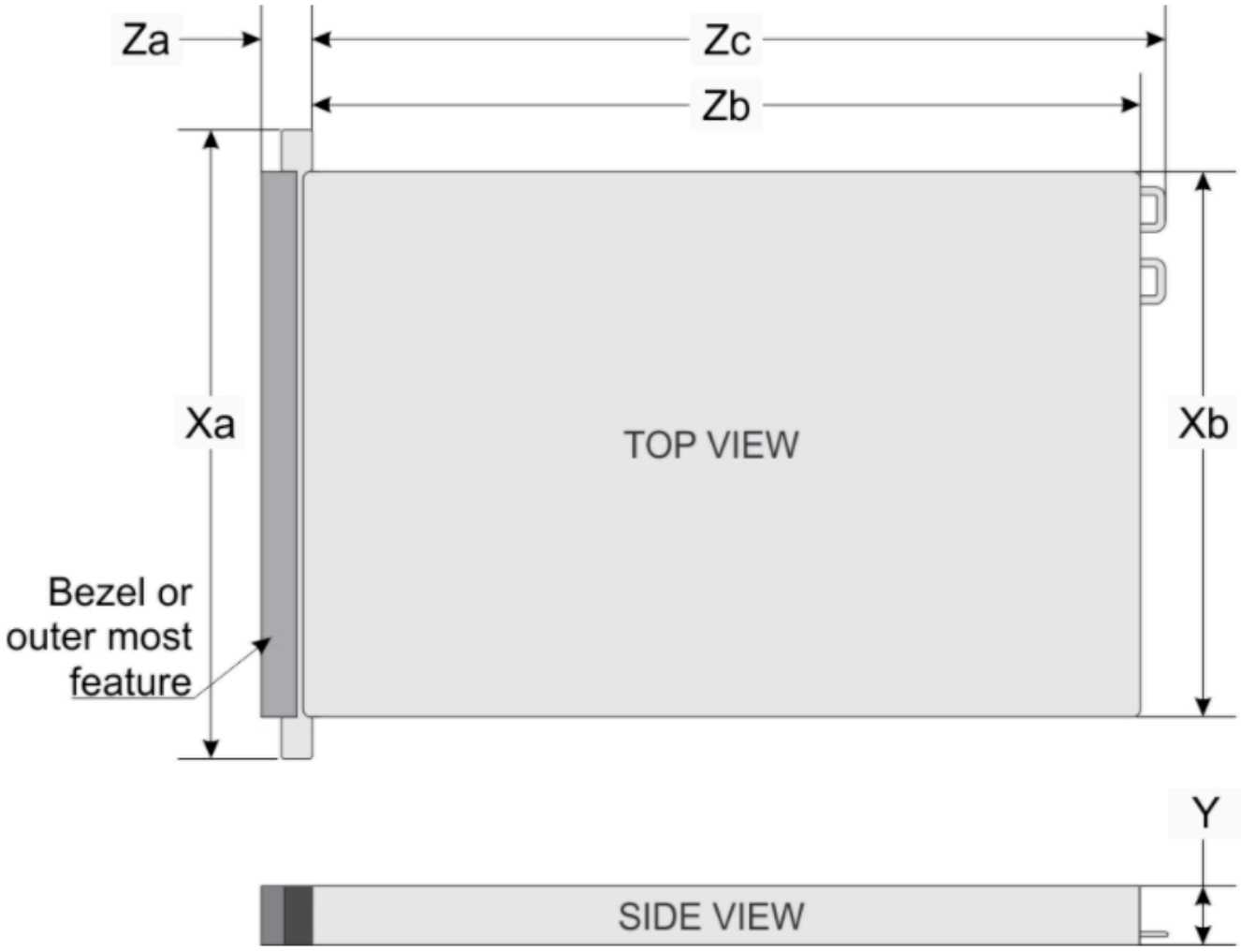
根據您訂購的設備型號，它可能隨附 10G-Base-T 銅纜網路卡或 10G DA/SFP+ 網路卡。

- 10G-Base-T NIC組態：
  - 針對 10G 使用CAT6纜線，或針對 1G 使用 CAT5（e）1G
- 10G DA/SFP+ NIC組態：
  - 使用長達 5 公尺的雙軸銅直接連接纜線
  - Dell/Intel 相容 SFP+ 光學模組（SR 或 LR）
  - SFP適用於 1G-Base-T 或 10G-Base-T 的 /SFP+ 銅收發器

實際安裝您的硬體設備

您的設備具有 1U 外形規格，並適用於標準國際電工委員會 （IEC） 相容 19 英吋機架。下圖顯示硬體設備的維度：

硬體設備尺寸，包括安裝支架和擋板。



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

硬體設備尺寸，包括安裝支架和擋板。

先決條件

若要安裝硬體設備，您需要下列元件：

- 電源線：一條為必要、建議兩條。
- 支援的網路佈線（取決於硬體設備中包含的網路介面卡（NIC））。Twinax Copper DAC、SFP+ 光學模組（Intel 相容）或 SFP Base-T 銅收發器。
- 鍵盤和監視器，或鍵盤、影片和滑鼠（KVM）切換解決方案。

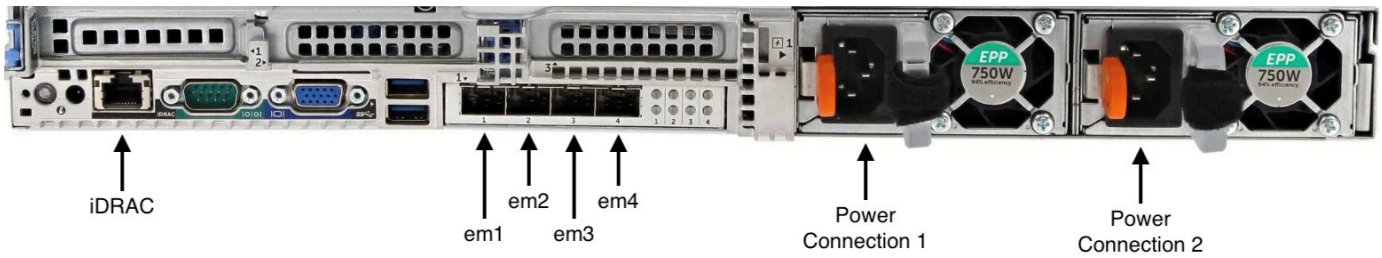
> **Note**
>
> 執行下列程序之前，請確定您符合 Storage Gateway 硬體設備的網路與防火牆要求 中所述的所有 Storage Gateway 硬體設備要求。

實際安裝您的硬體設備

1. 解除硬體設備的封裝，並遵循 方塊中的指示以機架掛載伺服器。

   下圖顯示硬體設備的背面，其中包含用於連接電源、乙太網路、USB、監視器、鍵盤和 i 的連接埠 DRAC。

   背面有網路和電源連接器標籤的硬體設備。

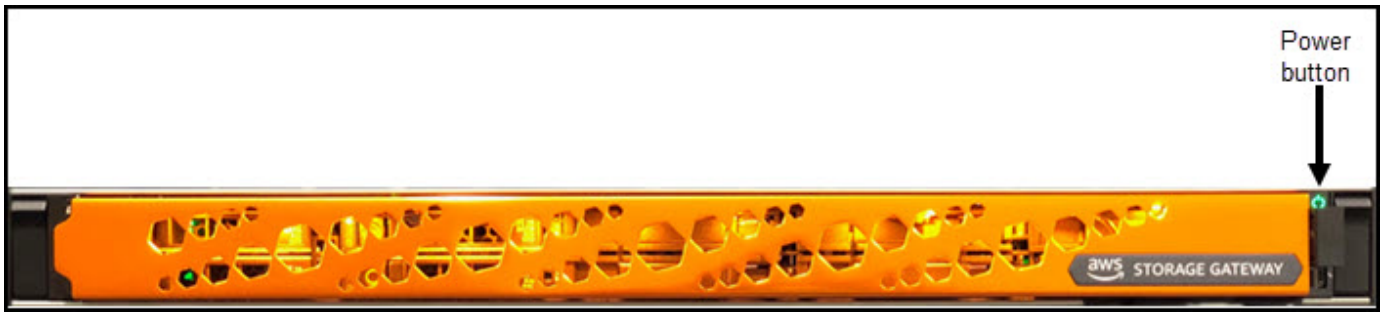


   背面有網路和電源連接器標籤的硬體設備。

2. 將電源線插入兩個電源供應器。可以只插入一個電源，但建議兩個電源供應器都插上。
3. 將乙太網路纜線插入 em1 連接埠，以提供全年無休的網際網路連線。em1 連接埠是背面四個實體網路連接埠 (從左到右) 中的第一個。

> **Note**
>
> 硬體設備不支援VLAN中繼。將要將硬體設備連接到的交換器連接埠設定為非截斷VLAN連接埠。

4. 插入鍵盤和顯示器。
5. 按前面板的 Power (電源) 按鈕 (如下圖所示)，開啟伺服器電源。
   硬件裝置正面帶有電源按鈕標籤。



硬件裝置正面帶有電源按鈕標籤。

下一步驟

[存取硬體設備主控台]

存取硬體設備主控台

當您開啟硬體設備電源時，硬體設備主控台會顯示在監視器上。硬體設備主控台會呈現特定使用者介面，您可以使用 AWS 該介面來設定管理員密碼、設定初始網路參數，以及開啟支援通道以 AWS。

若要使用硬體設備主控台，請從鍵盤輸入文字，並使用 Up、Right、 Down和 Left Arrow鍵在指定方向的畫面上移動。使用按 Tab 鍵以依序向前選擇畫面上的項目。在某些設定上，您可使用 Shift +Tab 鍵依序向後移動。使用 Enter 鍵可儲存選項，或是在螢幕上選擇按鈕。

第一次出現硬體設備主控台時，會顯示歡迎頁面，並提示您設定管理員使用者帳戶的密碼，然後才能存取主控台。

設定管理員密碼

- 在請設定您的登入密碼提示中，執行下列動作：
  a. 在 設定密碼 中，輸入密碼然後按 Down arrow。
  b. 在 確認 中，再次輸入您的密碼，然後選擇 儲存密碼。

設定密碼後，會顯示硬體主控台首頁。首頁會顯示 em1、em2、em3 和 em4 網路介面的網路資訊，並具有下列功能表選項：

- 設定網路
- 開啟訪客主控台
- 變更密碼
- 登出
- 開啟支援主控台

下一步驟

設定硬體設備網路參數

設定硬體設備網路參數

在硬體設備啟動並在硬體主控台中設定管理員使用者密碼後存取硬體設備主控台，請使用下列程序來設定網路參數，以便您的硬體設備可以連線至 AWS。

若要設定網路地址

1. 在首頁中，選擇設定網路，然後按 Enter。隨即顯示設定網路頁面。設定網路頁面顯示硬體設備上 4 個網路介面的 IP 和DNS資訊，並包含每個介面的設定DHCP或靜態地址的功能表選項。
2. 針對 em1 介面，執行下列其中一項操作：

   - 選擇 DHCP，然後按 Enter 使用動態主機組態通訊協定 （DHCP） 伺服器指派給實體網路連接埠IPv4的地址。

     請注意此地址，以便稍後在啟用步驟中使用。
   - 選擇靜態，然後按 Enter設定靜態IPv4地址。

     輸入 em1 網路介面的有效 IP 地址 、子網路遮罩 、閘道 和DNS伺服器地址。

     完成後，選擇儲存，然後按 Enter 儲存組態。

> **Note**
>
> 除了 em1 備援之外，您可以使用此程序來設定其他網路介面。如果您設定其他介面，則必須提供與 需求中列出的端點相同的永遠連線 AWS 。
> 硬體設備或 Storage Gateway 不支援網路聯結和連結彙總控制通訊協定 （LACP）。
> 我們不建議在子網路上設定多個網路介面，因為這有時可能會導致路由問題。

若要登出硬體主控台

1. 選擇返回，然後按 Enter 返回首頁。
2. 選擇登出，然後按 Enter 返回歡迎頁面。

下一步驟

啟用 Storage Gateway 硬體設備

啟用 Storage Gateway 硬體設備

設定 IP 地址後，您可以在 AWS Storage Gateway 主控台的硬體頁面上輸入此 IP 地址，以啟用您的硬體設備。啟用程序會驗證您的硬體設備擁有適當的安全登入資料，並將設備註冊到您的 AWS 帳戶。

您可以選擇在任何支援的 中啟用您的硬體設備 AWS 區域。如需支援的 清單 AWS 區域，請參閱 中的 Storage Gateway 硬體設備區域AWS 一般參考。

如要啟用您的儲存閘道硬體設備。

1. 開啟 AWS Storage Gateway 管理主控台，並用您想要啟用硬體的帳戶憑證登入。

   > **Note**
   >
   > 僅限啟用，必須符合下列條件：
   >
   > - 您的瀏覽器必須位於硬體設備的同一個網路上。
   > - 您的防火牆必須允許傳入流量在連接埠 8080 上HTTP存取設備。

2. 在頁面左側的導覽窗格選擇硬體。
3. 選擇啟用設備。
4. 針對 IP 地址，輸入您為硬體應用裝置設定的 IP 地址，然後選擇連接。

   如需有關設定 IP 地址的詳細資訊，請參閱設定網路參數來。
5. 為硬體設備輸入名稱。名稱最多可包含 255 個字元，不可包含斜線字元。
6. 針對硬體應用裝置時區，輸入要產生閘道大部分工作負載的本機時區。然後選擇下一步。

   時區控制何時進行硬體更新，以上午 2 點做為預設更新時間。理想情況下，如果時區設定正確，則依預設，更新將在當地工作日時段外進行。

7. 檢閱硬體應用裝置詳細資料區段中的啟用參數。如有必要，您可以選擇上一步返回並進行變更。否則，請選擇啟動以完成啟用。

硬體設備概況頁面會顯示橫幅，指出硬體設備已成功啟用。

此時，裝置已與您的帳戶關聯。下一步是在新設備上設定和啟動 S3 檔案閘道、FSx檔案閘道、磁帶閘道或磁碟區閘道。

下一步驟

在硬體設備上建立閘道

在硬體設備上建立閘道

您可以安裝閘道設備軟體，在部署中的任何 Storage Gateway 硬體設備上建立 S3 File Gateway、FSxFile Gateway、磁帶閘道或磁碟區閘道。

若要在硬體設備上建立閘道

1. 登入 AWS Management Console 並開啟位於 首頁的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/
2. 從主控台頁面左側的導覽窗格中，選擇硬體 。
3. 從硬體設備清單中，選取要建立閘道的已啟用硬體設備，然後選擇建立閘道 。
4. 請遵循建立閘道中所述的程序，以設定您要部署的 Storage Gateway 類型。

在 Storage Gateway 主控台中完成建立閘道後，Storage Gateway 軟體會自動開始在硬體設備上進行安裝。如果您使用動態主機組態通訊協定 （DHCP），閘道在主控台中顯示為線上可能需要 5 到 10 分鐘。若要將靜態 IP 地址指派給已安裝的閘道，請參閱為閘道設定 IP 地址為。

若要將靜態 IP 地址指派給已安裝閘道，接下來請設定閘道的網路界面，讓您的應用程式可以使用它。

下一步驟

在硬體設備上設定閘道 IP 地址

在硬體設備上設定閘道 IP 地址

在啟動硬體設備之前，您已為其實體網路介面指派 IP 地址。現在您已啟動裝置並在其上啟動 Storage Gateway，您需要將另一個 IP 地址指派給在硬體設備上執行的 Storage Gateway VM。若要將靜態 IP

地址指派給硬體設備上安裝的閘道，請從該閘道的本機主控台設定 IP 地址。您的應用程式（例如您的 NFS或 SMB 用戶端）會連線至此 IP 地址。您可以從硬體設備主控台存取閘道本機主控台。

若要在裝置上設定 IP 地址以使用應用程式

1. 在硬體主控台上，選擇開啟服務主控台，然後按 Enter 開啟閘道本機主控台的登入頁面。
2. AWS Storage Gateway 本機主控台登入頁面會提示您登入以變更網路組態和其他設定。

   針對 localhost 登入 ，輸入帳戶名稱，然後按 Enter。然後，輸入密碼，然後按 Enter。

   預設帳戶是 admin，預設密碼是 password。

   > **Note**
   >
   > 建議您從 AWS 設備啟用 - 組態主功能表中輸入閘道主控台的對應數字，然後執行 passwd 指令，以變更預設密碼。如需如何執行命令的資訊，請參閱 在本機主控台中執行內部部署閘道的儲存閘道命令。您也可以從 Storage Gateway 主控台設定密碼。如需詳細資訊，請參閱從 Storage Gateway 主控台設定本機主控台密碼。

3. AWS Appliance Activation - Configuration 頁面包含下列選單選項：

   - HTTP/SOCKS Proxy 組態
   - 網路組態
   - 測試網路連線
   - 檢視系統資源檢查
   - 系統時間管理
   - 授權資訊
   - 命令提示
   - 取得啟用金鑰

   > **Note**
   >
   > 某些選項僅針對特定閘道類型或主機平台顯示。

   輸入對應的數字以導覽至網路組態頁面。

4. 執行下列其中一個動作來設定閘道 IP 地址：

   - 若要使用動態主機組態通訊協定（DHCP）伺服器指派的 IP 地址，請輸入設定 DHCP的對應數字，然後在下頁輸入有效的DHCP組態資訊。
   - 若要指派靜態 IP 地址，請輸入設定靜態 IP 的對應數字，然後在下頁輸入有效的 IP 地址和DNS資訊。

   > **Note**
   >
   > 您在此指定的 IP 地址必須與硬體設備啟用期間使用的 IP 地址位於相同的子網路上。

結束閘道本機主控台

- 按 `Crtl+]` (右括號) 按鍵。硬體主控台會顯示。

> **Note**
>
> 前述按鍵是結束閘道本機主控台的唯一方式。

啟用並設定硬體設備後，您的裝置會顯示在主控台中。現在您可以在 Storage Gateway 主控台中繼續閘道的設定和組態程序。如需說明，請參閱「」。

從硬體設備移除閘道軟體

如果您不再需要已部署在硬體設備上的特定 Storage Gateway，您可以從硬體設備中移除閘道軟體。移除閘道軟體後，您可以選擇部署新的閘道，或從 Storage Gateway 主控台刪除硬體設備本身。若要從硬體設備移除閘道軟體，請使用下列步驟。

若要從硬體設備移除閘道

1. 開啟位於首頁 的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/
2. 從主控台頁面左側的導覽窗格中選擇硬體，然後選擇您要從中移除閘道軟體之設備的硬體設備名稱。
3. 從動作下拉式選單中，選擇移除閘道 。

   出現確認對話方塊。

4. 確認您要從指定的硬體設備中移除閘道軟體，然後在`remove`確認方塊中輸入該字詞。
5. 選擇移除以永久移除閘道軟體。

> **Note**
>
> 移除閘道軟體後，就無法復原動作。對於特定的閘道類型，刪除後可能會遺失資料，特別是快取的資料。如需刪除閘道的詳細資訊，請參閱 刪除閘道並移除相關資源。

移除閘道並不會從主控台刪除硬體設備。硬體設備會保留以供日後閘道部署。

刪除 Storage Gateway 硬體設備

如果您不再需要已啟動的 Storage Gateway 硬體設備，您可以從 AWS 您的帳戶完全刪除設備。

> **Note**
>
> 若要將設備移至不同的 AWS 帳戶或 AWS 區域，您必須先使用下列程序將其刪除，然後開啟閘道的支援管道並聯絡 AWS Support 以執行軟重設。如需詳細資訊，請參閱開啟 AWS Support 存取權，以協助故障診斷內部部署託管的閘道。

刪除您的硬體設備

1. 如果您已在硬體設備上安裝閘道，您必須先移除該閘道，之後才能刪除裝置。如需如何從您的硬體設備移除閘道的詳細資訊，請參閱 從硬體設備移除閘道軟體。
2. 在 Storage Gateway 主控台的硬體頁面上，選擇要刪除的硬體裝置。
3. 在 Actions (動作) 中選擇 Delete Appliance (刪除裝置)。出現確認對話方塊。
4. 確認您要刪除指定的硬體設備，然後在確認方塊中輸入刪除文字，然後選擇刪除。

   刪除硬體設備時，也會刪除裝置上安裝且與閘道相關聯的所有資源，但不會刪除硬體設備本身上的資料。

建立閘道

此頁面的概觀區段提供 Storage Gateway 建立程序運作方式的高階摘要。如需使用 Storage Gateway 主控台建立特定類型閘道 step-by-step 的程序，請參閱下列主題：

- 建立和啟用 Amazon S3 File Gateway
- 建立和啟用 Amazon FSx File Gateway
- 建立和啟用磁帶閘道
- 建立和啟用磁碟區閘道

> **Important**
>
> AWS Storage Gateway的 FSx File Gateway 在 10/28/24 之後將不再提供給新客戶。若要使用服務，您必須在該日期之前註冊。FSx File Gateway 的現有客戶可以繼續正常使用服務。如需類似 FSx File Gateway 的功能，請造訪此部落格文章 。

概觀：閘道啟動

閘道啟用涉及設定閘道、將其連線至 AWS，然後檢閱您的設定並啟用。

設定閘道

若要設定 Storage Gateway，請先選擇要建立的閘道類型，以及要在其上執行閘道虛擬設備的主機平台。然後，您可以下載所選平台的閘道虛擬裝置範本，並將其部署到您的內部部署環境中。您也可以將 Storage Gateway 部署為向偏好的經銷商訂購的實體硬體設備，或部署為 AWS 雲端環境中的 Amazon EC2執行個體。部署閘道設備時，您可以在虛擬化主機上配置本機實體磁碟空間。

連線至 AWS

下一步是將您的閘道連接至 AWS。若要這麼做，請先選擇您要用於雲端中閘道虛擬設備 AWS 與服務之間通訊的服務端點類型。此端點可以從公有網際網路存取，也可以從 Amazon 內存取VPC，您可以在其中完全控制網路安全組態。然後，您可以指定閘道的 IP 地址或其啟用金鑰，透過連線至閘道設備上的本機主控台來取得該 IP 地址或啟用金鑰。

檢閱並啟用

此時，您將有機會檢閱您選擇的閘道和連線選項，並在必要時進行變更。設定好所要的所有設定好後，您可以啟用閘道。您必須先設定一些其他設定並建立儲存資源，才能開始使用已啟動的閘道。

概觀：閘道組態

啟用 Storage Gateway 後，您必須執行一些額外的設定。在此步驟中，您可以配置在閘道主機平台上佈建的實體儲存區，以供閘道設備用作快取或上傳緩衝區。然後，您可以設定 設定以協助使用 Amazon CloudWatch Logs 和 CloudWatch 警示監控閘道的運作狀態，並視需要新增標籤以協助識別閘道。您必須先建立儲存資源，才能開始使用已啟動和設定的閘道。

概觀：儲存資源

啟用並設定 Storage Gateway 後，您需要建立供其使用的雲端儲存資源。根據您建立的閘道類型，您將使用 Storage Gateway 主控台來建立磁碟區、磁帶或 Amazon S3 或 Amazon FSx 檔案共用，以與其建立關聯。每種閘道類型都會使用其各自的資源來模擬相關類型的網路儲存基礎結構，並將您寫入的資料傳輸到 AWS 雲端。

建立和啟用磁帶閘道

在本節中，您可以找到如何下載、部署及啟用磁帶閘道的說明。

主題

設定磁帶閘道

設定新的磁帶閘道

1. 開啟 AWS Management Console at https://console.aws.amazon.com/storagegateway/home/，然後選擇您要建立閘道 AWS 區域 的 。

2. 選擇建立閘道以開啟設定閘道頁面。
3. 在閘道設定區段中，執行下列操作：
   a. 為 Gateway name (閘道名稱) 輸入閘道的名稱。您可以搜尋此名稱，在 Storage Gateway 主控台的清單頁面上尋找閘道。
   b. 針對閘道時區，請選擇您要部署閘道的全球當地時區。
4. 在閘道選項區段中，針對閘道類型選擇磁帶閘道。
5. 在平台選項區段中，執行下列操作：
   a. 對於主機平台，請選擇要在其上部署閘道的平台，然後依照 Storage Gateway 主控台頁面上顯示的平台特定指示來設定主機平台。您可以從下列選項來選擇：
      - VMware ESXi - 使用 下載、部署和設定閘道虛擬機器VMwareESXi。
      - Microsoft Hyper-V：使用 Microsoft Hyper-V 下載、部署和配置閘道虛擬機。
      - Linux KVM - 使用 Linux 下載、部署和設定閘道虛擬機器KVM。
      - Amazon EC2 - 設定並啟動 Amazon EC2執行個體來託管您的閘道。此選項不適用於儲存磁碟區閘道。
      - 硬體設備 - 從 訂購專用實體硬體設備 AWS 以託管您的閘道。
   b. 在確認設定閘道中，選取核取方塊以確認您已針對所選主機平台執行部署步驟。此步驟不適用於硬體設備主機平台。
6. 在備份應用程式設定值區段中，針對備份應用程式，選擇要用來將磁帶資料備份到與磁帶閘道關聯之虛擬磁帶的應用程式。
7. 選擇下一步繼續進行。

現在您的閘道已設定完成，您需要選擇想要它與 連線和通訊的方式 AWS。如需指示，請參閱將磁帶閘道連線至 AWS。

將您的磁帶閘道連接至 AWS

將新的磁帶閘道連接至 AWS

1. 如果您尚未完成設定磁帶閘道中所述的程序，請完成該程序。完成時，請選擇下一步，在 Storage Gateway 主控台中開啟連接到 AWS 頁面。
2. 在端點選項區段中，針對服務端點 ，選擇閘道用來與 通訊的端點類型 AWS。您可以從下列選項來選擇：

- 可公開存取 - 您的閘道 AWS 會透過公有網際網路與 通訊。如果您選取此選項，請使用FIPS啟用的端點核取方塊來指定連線是否應符合聯邦資訊處理標準 （FIPS）。

  > **Note**
  >
  > 如果您在 AWS 透過命令列介面或 FIPS 存取 時需要 140-2 個經過驗證的密碼編譯模組API，請使用 FIPS合規的端點。如需詳細資訊，請參閱聯邦資訊處理標準 （FIPS） 140-2。
  >
  > FIPS 服務端點僅適用於某些 AWS 區域。如需詳細資訊，請參閱 AWS 一般參考 中的 Storage Gateway 端點和配額。

- VPC 託管 - 閘道 AWS 透過與 的私有連線與 通訊VPC，可讓您控制網路設定。如果您選取此選項，則必須從下拉式功能表VPC中選擇其VPC端點 ID，或提供其端點DNS名稱或 IP 地址，以指定現有的VPC端點。如需詳細資訊，請參閱在虛擬私有雲端中啟用閘道。

3. 在閘道連線選項區段中，針對連線選項，選擇如何識別連線至 AWS的閘道。您可以從下列選項來選擇：

   - IP 地址：在對應欄位中提供閘道的 IP 地址。此 IP 地址必須是公開的，或可從您目前的網路存取，而且您必須能夠從 Web 瀏覽器連線到該 IP 地址。

     您可以從 Hypervisor 用戶端登入閘道的本機主控台，或從 Amazon EC2執行個體詳細資訊頁面複製閘道 IP 地址，以取得閘道 IP 地址。

   - 啟用金鑰：在對應欄位中提供閘道的啟用金鑰。您可以使用閘道的本機主控台產生啟用金鑰。如果閘道的 IP 地址無法使用，請選擇此選項。

4. 選擇下一步繼續進行。

現在您已選擇閘道連線到 的方式 AWS，您需要啟用閘道。如需指示，請參閱檢閱設定並啟用磁帶閘道。

檢閱設定並啟動磁帶閘道

啟動新的磁帶閘道

1. 如果您尚未這麼做，請完成下列主題中所述的程序：

   - 設定磁帶閘道
   - 將您的磁帶閘道連接至 AWS

完成時，請選擇下一步，在 Storage Gateway 主控台中開啟檢閱並啟用頁面。

2. 檢閱頁面上每個區段的初始閘道詳細資訊。
3. 如果區段包含錯誤，請選擇編輯以傳回對應的設定頁面並進行變更。

> **Note**
>
> 啟動閘道後，您無法修改閘道選項或連線設定。

4. 選擇啟動閘道以繼續。

現在您已啟動閘道，您必須執行第一次設定，以配置本機儲存磁碟並設定記錄。如需指示，請參閱設定磁帶閘道。

設定您的磁帶閘道

在新磁帶閘道上執行第一次設定

1. 如果您尚未這麼做，請完成下列主題中所述的程序：
   - 設定磁帶閘道
   - 將您的磁帶閘道連接至 AWS
   - 檢閱設定並啟動磁帶閘道

   完成時，請選擇下一步，在 Storage Gateway 主控台中開啟設定閘道頁面。
2. 在設定儲存區段中，使用下拉式功能表為 配置至少一個具有至少 165 GiB 容量的磁碟，以及為 CACHE STORAGE配置至少一個具有至少 150 GiB UPLOAD BUFFER容量的磁碟。本節中列出的本機磁碟對應於您在主機平台上佈建的實體儲存體。
3. 在CloudWatch 日誌群組區段中，選擇如何設定 Amazon CloudWatch Logs 來監控閘道的運作狀態。您可以從下列選項來選擇：
   - 建立新的日誌群組：設定新的日誌群組以監控閘道。
   - 使用現有的日誌群組：從對應的下拉式功能表中選擇現有的日誌群組。
   - 停用記錄 - 請勿使用 Amazon CloudWatch Logs 監控您的閘道。

> **Note**
>
> 若要接收 Storage Gateway 運作狀態日誌，您的日誌群組資源政策中必須存在下列許可。取代 *highlighted section* 部署的特定日誌群組 resourceArn 資訊。
>
> ```
> "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:*"
> ```
>
> 只有在您希望許可明確套用至個別日誌群組時，才需要「資源」元素。

4. 在CloudWatch 警示區段中，選擇如何設定 Amazon CloudWatch 警示，以便在閘道指標偏離定義的限制時通知您。您可以從下列選項來選擇：

   - 建立 Storage Gateway 的建議警示 – 在建立閘道時自動建立所有建議 CloudWatch 警示。如需建議警示的詳細資訊，請參閱了解 CloudWatch 警示。

     > **Note**
     >
     > 此功能需要 CloudWatch 政策許可，該許可不會自動授予為預先設定的 Storage Gateway 完整存取政策的一部分。在嘗試建立建議的 CloudWatch 警示之前，請確定您的安全政策授予下列許可：
     >
     > - `cloudwatch:PutMetricAlarm`：建立警示
     > - `cloudwatch:DisableAlarmActions`：關閉警示動作
     > - `cloudwatch:EnableAlarmActions`：開啟警示動作
     > - `cloudwatch:DeleteAlarms`：刪除警示

- 建立自訂警示 – 設定新 CloudWatch 警示，以通知您閘道的指標。選擇建立警示以定義指標，並在 Amazon CloudWatch 主控台中指定警示動作。如需指示，請參閱 Amazon 使用者指南 中的使用 Amazon CloudWatch 警示。 CloudWatch
- 無警示 – 不會收到 CloudWatch閘道指標的通知。

5. (選用) 在標籤區段中，選擇新增標籤，然後輸入區分大小寫的鍵值對，以協助您在 Storage Gateway 主控台的清單頁面上搜尋及篩選閘道。重複此步驟，視需要新增任意數量的標籤。
6. 選擇設定以完成建立閘道。

   若要檢查新閘道的狀態，請在 Storage Gateway 的閘道概觀頁面上進行搜尋。

現在您已經建立閘道，您必須建立要使用的虛擬磁帶。如需說明，請參閱建立磁帶。

為磁帶閘道建立新的虛擬磁帶

本節說明如何使用 建立新的虛擬磁帶 AWS Storage Gateway。您可以使用 AWS Storage Gateway 主控台或 Storage Gateway 手動建立新的虛擬磁帶API。您也可以將磁帶閘道設定為自動建立磁帶，這有助於減少手動磁帶管理的需求、簡化大型部署作業，並協助擴展內部部署和封存儲存需求。

Tape Gateway 支援一次寫入、讀取許多（WORM）和虛擬磁帶上的磁帶保留鎖定。WORM啟用的虛擬磁帶有助於確保虛擬磁帶程式庫中作用中磁帶上的資料無法覆寫或清除。如需虛擬磁帶WORM保護的詳細資訊，請參閱以下章節：the section called “WORM 磁帶保護”。

透過磁帶保留鎖定，您可以指定封存虛擬磁帶上的保留模式和期間，防止它們遭到刪除，最長可達 100 年的固定時間。其中包括誰可以刪除磁帶或修改保留設定的權限控制。如需磁帶擷取的詳細資訊，請參閱 the section called “磁帶保留鎖定”。

> **Note**
>
> 只會向您收取您寫入至磁帶之資料量的費用，而非磁帶容量。
> 您可以使用 AWS Key Management Service（AWS KMS）加密寫入 Amazon Simple Storage Service（Amazon S3）中儲存的虛擬磁帶的資料。目前，您可以使用 AWS Storage Gateway API或 AWS Command Line Interface（ ）來執行此操作AWS CLI。如需詳細資訊，請參閱 CreateTapes或 create-tapes 。

寫入一次，讀取許多（WORM）磁帶保護

您可以在 中啟用虛擬磁帶的WORM保護，以防止虛擬磁帶遭到覆寫或清除 AWS Storage Gateway。WORM 虛擬磁帶的保護會在建立磁帶時啟用。

寫入WORM虛擬磁帶的資料無法覆寫。只有新資料可以附加到WORM虛擬磁帶，且現有資料無法清除。啟用虛擬磁帶的WORM保護有助於在磁帶處於作用中狀態時，在彈出和封存磁帶之前保護這些磁帶。

WORM 只有在建立磁帶時才能設定組態，而且在建立磁帶後無法變更組態。

手動建立磁帶

您可以使用 AWS Storage Gateway 主控台或 Storage Gateway 手動建立新的虛擬磁帶API。此主控台提供方便的磁帶建立介面，可靈活地為隨機產生的磁帶條碼指定前置詞。如果您需要完全自訂磁帶條碼（例如，為了符合對應實體磁帶的序號），您必須使用 API。如需使用 Storage Gateway 建立磁帶的詳細資訊API，請參閱 Storage Gateway 參考 CreateTapeWithBarcode中的 。 Storage Gateway API

使用 Storage Gateway 主控台手動建立虛擬磁帶

1. 開啟位於首頁 的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/
2. 在導覽窗格中，選擇 Gateways (閘道) 標籤。
3. 選擇建立磁帶以開啟建立磁帶窗格。
4. 針對 Gateway (閘道)，選擇閘道。磁帶是針對此閘道所建立。
5. 針對磁帶類型，選擇標準建立標準虛擬磁帶。選擇WORM在讀取多個（）虛擬磁帶後建立寫入。WORM如需詳細資訊，請參閱寫入一次、讀取許多（WORM）磁帶保護。
6. 針對 Number of tapes (磁帶數目)，選擇您要建立的磁帶數目。如需磁帶配額的詳細資訊，請參閱AWS Storage Gateway 配額。
7. 針對 Capacity (容量)，輸入您要建立之虛擬磁帶的大小。磁帶必須大於 100 GiB。如需容量配額的詳細資訊，請參閱AWS Storage Gateway 配額。
8. 針對 Barcode prefix (條碼字首)，輸入您要加到虛擬磁帶條碼前面的字首。

> **Note**
>
> 虛擬磁帶都有獨特可辨識的條碼，您可為條碼新增字首。您可以使用字首來協助識別虛擬磁帶。字首必須為大寫字母 (A–Z)，而且長度必須為一到四個字元。

9. 在集區中，選擇 Glacier 集區、Deep Archive 集區或您已建立的自訂集區。此集區確定了備份軟體退出您的磁帶時，您的磁帶存放之處的儲存類別。

   - 如果您想要將磁帶存檔到 S3 Glacier Flexible Retrieval 儲存類別中，請選擇 Glacier 集區。當您的備份軟體退出磁帶時，它會自動存檔在 S3 Glacier Flexible Retrieval 中。您可以將 S3 Glacier Flexible Retrieval 用於多個作用中存檔，在其中，您通常可以於 3 到 5 小時內擷取磁帶。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的存檔物件的儲存類別。
   - 如果您想要將磁帶存檔在 S3 Glacier Deep Archive 儲存類別中，請選擇 Deep Archive 集區。當您的備份軟體退出磁帶時，磁帶會自動存檔在 S3 Glacier Deep Archive 中。您可以將 S3 Glacier Deep Archive 用於長期資料保留和數位保存，其中的資料一年存取一次或兩次。您通常可以在 12 小時內擷取 S3 Glacier Deep Archive 中的磁帶存檔。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的存檔物件的儲存類別。
   - 選擇自訂集區 (如有)。您可以將自訂磁帶集區設定為使用 Deep Archive 集區或 Glacier 集區。當您的備份軟體彈出磁帶時，磁帶會封存至已設定的儲存類別。

   如果您將磁帶存檔在 S3 Glacier Flexible Retrieval 中，您可以稍後將其移到 S3 Glacier Deep Archive。如需詳細資訊，請參閱將磁帶移至 S3 Glacier Deep Archive 儲存類別。

   > **Note**
   >
   > 在 2019 年 3 月 27 日之前建立的磁帶，會於您的備份軟體將它退出時，直接存檔在 S3 Glacier Flexible Retrieval 中。

10. (選用) 針對 標籤，請選擇新增標籤，然後您磁帶的輸入標籤金鑰和標籤值。標籤為區分大小寫的索引鍵值組，可協助您管理、篩選和搜尋磁帶。
11. 選擇 Create tapes (建立磁帶)。
12. 在導覽窗格中選擇磁帶館 > 磁帶標籤以查看您的磁帶。根據預設，此清單一次最多可顯示 1,000 個磁帶，但您執行的搜尋會套用至所有磁帶。您可以使用搜尋列尋找符合特定準則的磁帶，或將清單減少到 1,000 個以下的磁帶。當您的清單包含 1,000 個或更少的磁帶時，您可以依各種屬性，以遞增或遞減順序來排序磁帶。

虛擬磁帶的狀態最初會在建立虛擬磁帶CREATING時設定為 。建立磁帶後，其狀態會變更為 AVAILABLE。如需詳細資訊，請參閱了解磁帶狀態。

允許自動建立磁帶

磁帶閘道會自動建立新的虛擬磁帶，以維持您設定的可用磁帶數目下限。然後，這些新磁帶可供備份應用程式進行匯入，讓您執行備份任務時無須中斷。自動磁帶建立除了不再需要手動建立新的虛擬磁帶，更免去對自訂程式碼編寫的需求。

當磁帶閘道的磁帶數量少於自動建立磁帶所指定的可用磁帶數目下限時，會自動產生新磁帶。在以下情況下產生新的磁帶：

- 磁帶是從匯入/匯出槽匯入的。
- 磁帶會匯入至磁帶機。

閘道會使用自動磁帶建立原則中指定的條碼前置詞，維護最少數量的磁帶。如果磁帶數量少於具有條碼前置詞的最小磁帶數量，閘道會自動建立足夠的新磁帶，使其與自動磁帶建立原則中指定的最小磁帶數量相等。

當您退出磁帶並進入匯入/匯出插槽時，該磁帶不會計入自動磁帶建立原則中指定的最小磁帶數目。只有匯入/匯出插槽中的磁帶才會被視為「可用」。匯出磁帶不會起始自動建立磁帶。只有匯入會影響可用磁帶的數量。

將磁帶從匯入/匯出槽移至磁帶機或儲存槽，可減少匯入/匯出插槽中具有相同條碼字首的磁帶數量。閘道會建立新的磁帶，以維持該條碼前置詞的最小可用磁帶數量。

允許自動建立磁帶

1. 開啟位於首頁 的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/
2. 在導覽窗格中，選擇 Gateways (閘道) 標籤。
3. 選擇您要自動建立磁帶的閘道。
4. 在 Actions (動作) 選單，選擇 Configure tape auto-create (設定磁帶自動建立)。

   便會顯示磁帶自動建立頁面。您可在此新增、變更或刪除磁帶自動建立選項。
5. 若要允許自動建立磁帶，請選擇新增項目，然後設定自動建立磁帶的設定。
6. 針對磁帶類型，選擇標準建立標準虛擬磁帶。選擇WORM建立 write-once-read-many（WORM）虛擬磁帶。如需詳細資訊，請參閱寫入一次、讀取許多（WORM）磁帶保護。
7. 針對磁帶數目下限，請輸入磁帶閘道隨時應有的可用虛擬磁帶最低數量。此值有效範圍最小為 1，最大為 10。

8. 針對 Capacity (容量)，輸入虛擬磁帶容量的大小 (位元組)。有效範圍最小為 100 Gib，最大為 15 TiB。
9. 針對 Barcode prefix (條碼字首)，輸入您要加到虛擬磁帶條碼前面的字首。

> **Note**
>
> 虛擬磁帶都有獨特可辨識的條碼，您可為條碼新增字首。字首是選用性的，但您可以使用它來協助識別虛擬磁帶。字首必須為大寫字母 (A–Z)，而且長度必須為一到四個字元。

10. 在集區中，選擇 Glacier 集區、Deep Archive 集區或您已建立的自訂集區。此集區確定了備份軟體退出您的磁帶時，您的磁帶存放之處的儲存類別。

    - 如果您想要將磁帶存檔到 S3 Glacier Flexible Retrieval 儲存類別中，請選擇 Glacier 集區。當您的備份軟體退出磁帶時，它會自動存檔在 S3 Glacier Flexible Retrieval 中。您可以將 S3 Glacier Flexible Retrieval 用於多個作用中存檔，在其中，您通常可以於 3 到 5 小時內擷取磁帶。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的存檔物件的儲存類別。
    - 如果您想要將磁帶存檔在 S3 Glacier Deep Archive 儲存類別中，請選擇 Deep Archive 集區。當您的備份軟體退出磁帶時，磁帶會自動存檔在 S3 Glacier Deep Archive 中。您可以將 S3 Glacier Deep Archive 用於長期資料保留和數位保存，其中的資料一年存取一次或兩次。您通常可以在 12 小時內擷取 S3 Glacier Deep Archive 中的磁帶存檔。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的存檔物件的儲存類別。
    - 選擇自訂集區 (如有)。您可以將自訂磁帶集區設定為使用 Deep Archive 集區或 Glacier 集區。當您的備份軟體彈出磁帶時，磁帶會封存至已設定的儲存類別。

    如果您將磁帶存檔在 S3 Glacier Flexible Retrieval 中，您可以稍後將其移到 S3 Glacier Deep Archive。如需詳細資訊，請參閱將磁帶移至 S3 Glacier Deep Archive 儲存類別。

> **Note**
>
> 在 2019 年 3 月 27 日之前建立的磁帶，會於您的備份軟體將它退出時，直接存檔在 S3 Glacier Flexible Retrieval 中。

11. 完成設定後，選擇儲存變更。
12. 在導覽窗格中選擇磁帶館 > 磁帶標籤以查看您的磁帶。根據預設，此清單一次最多可顯示 1,000 個磁帶，但您執行的搜尋會套用至所有磁帶。您可以使用搜尋列尋找符合特定準則的磁帶，或將清

單減少到 1,000 個以下的磁帶。當您的清單包含 1,000 個或更少的磁帶時，您可以依各種屬性，以遞增或遞減順序來排序磁帶。

建立磁帶CREATING時，可用虛擬磁帶的狀態一開始會設為 。建立磁帶後，其狀態會變更為AVAILABLE。如需詳細資訊，請參閱了解磁帶狀態。

如需變更自動磁帶建立政策或刪除磁帶閘道的自動建立磁帶的詳細資訊，請參閱 管理自動磁帶建立。

後續步驟

使用磁帶閘道

建立自訂磁帶集區

本節描述了如何在 AWS Storage Gateway中建立新的自訂磁帶集區。

主題

- 選擇磁帶集區類型
- 使用磁帶保留鎖定
- 建立自訂磁帶集區

選擇磁帶集區類型

AWS Storage Gateway 使用磁帶集區來決定您希望磁帶在退出時封存的儲存類別。Storage Gateway 提供兩個標準磁帶集區：

- Glacier 集區：將磁帶存放在 S3 Glacier Flexible Retrieval 儲存類別中。當您的備份軟體退出磁帶時，它會自動存檔在 S3 Glacier Flexible Retrieval 中。您可以將 S3 Glacier Flexible Retrieval 用於多個作用中存檔，您通常可以於 3 到 5 小時內從其中擷取磁帶。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的存檔物件的儲存類別。
- Deep Archive：S3 Glacier Deep Archive 儲存體類別中的磁帶。當您的備份軟體退出磁帶時，磁帶會自動存檔在 S3 Glacier Deep Archive 中。您可以將 S3 Glacier Deep Archive 用於長期資料保留和數位保存，其中的資料一年存取一次或兩次。您通常可以於 12 個小時內擷取存檔在 S3 Glacier Deep Archive 中的磁帶。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的存檔物件的儲存類別。

如果您將磁帶存檔在 S3 Glacier Flexible Retrieval 中，您可以稍後將其移到 S3 Glacier Deep Archive。如需詳細資訊，請參閱將磁帶移至 S3 Glacier Deep Archive 儲存類別。

Storage Gateway 也支援建立自訂磁帶集區，讓您可以啟動磁帶保留鎖定，以防止封存的磁帶在固定時間遭到刪除或移動到另一個集區，磁帶保留鎖定最長可達 100 年。這包括鎖定權限控制誰可以刪除磁帶或修改保留設定。

使用磁帶保留鎖定

使用磁帶保留鎖定，您可以鎖定封存的磁帶。磁帶保留鎖定是自訂磁帶集區中磁帶的選項。已啟用磁帶保留鎖定的磁帶在固定時間內，無法刪除或移動至其他集區，最長可達 100 年。

您可以使用下列兩種模式之一來設定磁帶保留鎖定：

- 治理模式 – 在治理模式下設定時，只有 AWS Identity and Access Management （ IAM ） 具有執行許可的使用者`storagegateway:BypassGovernanceRetention`才能從集區中移除磁帶。如果您使用 AWS Storage Gateway API來移除磁帶，也必須將 `BypassGovernanceRetention`設定為 `true`。
- 合規模式：在合規模式下配置時，任何使用者 (包括 root AWS 帳戶) 都無法移除保護。

  當磁帶在合規模式中受到鎖定時，您無法變更物件的保留模式，亦無法縮短它的保留期。合規模式可協助確保磁帶在保留期間均不會受到覆寫或刪除。

> **Important**
>
> 自訂集區的組態在建立之後無法變更。

您可以在建立自訂磁帶集區時啟用磁帶保留鎖定。連接至自訂集區的任何新磁帶都會繼承該集區的保留鎖定類型、期間和儲存類別。

您也可以在預設集區和您建立的自訂集區之間移動磁帶，在此功能發行前封存的磁帶上啟動磁帶保留鎖定。如果磁帶已封存，磁帶保留鎖會立即生效。

> **Note**
>
> 如果您要在 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 儲存類別之間移動封存磁帶，則需支付移動磁帶的費用。如果儲存類別保持不變，則無需額外付費即可將磁帶從預設集區移至自訂集區。

建立自訂磁帶集區

使用下列步驟可使用 AWS Storage Gateway 主控台建立自訂磁帶集區。

建立自訂磁帶集區

1. 開啟位於首頁 的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/
2. 在導覽窗格中選擇磁帶櫃，然後選擇集區標籤。
3. 選擇建立集區以開啟建立集區窗格。
4. 在名稱中，輸入唯一的名稱以識別您的自訂磁帶集區。集區名稱長度必須介於 2 到 100 個字元之間。
5. 對於儲存類別，請選擇 Glacier 或 Glacier Deep Archive。
6. 對於保留鎖定類型，請選擇無、合規或控管。

   > **Note**
   >
   > 如果您選擇合規，包括根 AWS 帳戶在內的任何使用者都無法移除磁帶保留鎖定。

7. 如果您選擇磁帶保留鎖定類型，請輸入保留期間 (以天為單位)。最長保留期為 36,500 天 (100 年)。
8. (選用) 對於標籤，請選擇新增標籤，將標籤新增至您的自訂磁帶集區。標籤為區分大小寫的索引鍵值組，可協助您管理、篩選和搜尋自訂磁帶集區。

   輸入一個金鑰，並選用地輸入標籤的值。您最多可以為磁帶集區新增 50 個標籤。
9. 選擇建立集區以建立新的自訂磁帶集區。

連接VTL您的裝置

以下說明如何將虛擬磁帶程式庫 （ VTL ） 裝置連接至 Microsoft Windows 或 Red Hat Enterprise Linux （ RHEL ） 用戶端。

主題

- 連線至 Microsoft Windows 用戶端
- 連線到 Linux 用戶端

連線至 Microsoft Windows 用戶端

下列程序概略說明您連線至 Windows 用戶端所遵循的步驟。

將VTL裝置連線至 Windows 用戶端

1. 啟動 `iscsicpl.exe`。

   > **Note**
   >
   > 您必須在用戶端電腦上具有管理員權限，才能執行 iSCSI 啟動器。

2. 啟動 Microsoft iSCSI 啟動器服務。
3. 在 iSCSI Initiator Properties 對話方塊中，選擇探索索引標籤，然後選擇探索入口網站 。
4. 提供磁帶閘道的 IP 地址，做為 IP 地址或DNS名稱 。
5. 選擇 Targets (目標) 標籤，然後選擇 Refresh (重新整理)。所有 10 個磁帶硬碟和媒體變更器都會出現在 Discovered targets (已搜索到的目標) 方塊中。目標的狀態為 Inactive (非使用中)。
6. 選擇第一個裝置並與之連線。您一次可以連線一個裝置。
7. 連線所有目標。

在 Windows 用戶端上，磁帶硬碟的驅動程式提供者必須是 Microsoft。使用下列程序來驗證驅動程式提供者，並在需要時更新驅動程式和提供者：

驗證及更新驅動程式及提供者

1. 在 Windows 用戶端上，啟動 [裝置管理員]。
2. 展開 Tape drives (磁帶硬碟)，開啟磁帶硬碟的內容 (按右鍵) 選單，然後選擇 Properties (屬性)。
3. 在 Device Properties (裝置屬性) 對話方塊的 Driver (驅動程式) 標籤中，確認 Driver Provider (驅動程式提供者) 為 Microsoft。
4. 若驅動程式提供者並非 Microsoft，請將值設定如下：

   a. 選擇 Update Driver (更新驅動程式)。

   b. 在 Update Driver Software (更新驅動程式軟體) 對話方塊中，選擇 Browse my computer for driver software (瀏覽我的電腦以搜尋驅動程式軟體)。

   c. 在 Update Driver Software (更新驅動程式軟體) 對話方塊中，選擇 Let me pick from a list of device drivers on my computer (讓我從電腦上的裝置驅動程式清單中挑選)。

d. 選擇LTO磁帶機，然後選擇下一步 。

5. 選擇關閉以關閉更新驅動程式軟體視窗，然後確認驅動程式提供者的值已設為 Microsoft。
6. 重複這些步驟來更新所有磁帶硬碟的驅動程式及提供者。

連線到 Linux 用戶端

下列程序顯示您連接至RHEL用戶端所遵循的步驟摘要。

將 Linux 用戶端連線至VTL裝置

1. 安裝`iscsi-initiator-utils`RPM套件。

   您可以使用下列命令來安裝套件。

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

2. 確定 iSCSI 常駐程式正在執行。

   對於 RHEL 5 或 6，請使用下列命令。

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

   對於 RHEL 7，請使用下列命令。

   ```
   sudo service iscsid status
   ```

3. 探索為閘道定義的磁碟區或VTL裝置目標。請使用下列搜索命令。

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

   搜索命令的輸出看起來會類似下列範例輸出。

   若為磁碟區閘道：`[GATEWAY_IP]:3260, 1 iqn.1997-05.com.amazon:myvolume`

   若為磁帶閘道，請參閱：`iqn.1997-05.com.amazon:[GATEWAY_IP]-tapedrive-01`。

4. 連線至目標

   請務必指定正確的 *[GATEWAY_IP]* 和 IQN 。

使用下列 命令。

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

5. 確認磁碟區已連接至用戶端機器 (啟動器)。為此，請使用下列命令。

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

命令的輸出看起來應該像下列範例輸出。

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

對於磁碟區閘道，強烈建議您在設定啟動器之後，如 中所述自訂您的 iSCSI 設定[自訂 Linux iSCSI 設定]。

確認VTL裝置已連接至用戶端機器 （ 啟動器 ）。為此，請使用下列命令。

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

命令的輸出看起來應該像下列範例輸出。

```
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
```

後續步驟

使用您的備份軟體來測試您的閘道設定

使用備份軟體測試閘道設定

您可以透過使用您的備份應用程式，執行下列任務來測試您的磁帶閘道設定：

1. 設定備份應用程式以偵測您的儲存裝置。

> **Note**
>
> 為改善 I/O 效能，我們建議將您備份應用程式內的磁帶硬碟區塊大小設為 1 MB。如需詳細資訊，請參閱 針對磁帶硬碟使用較大的區塊大小。

2. 將資料備份至磁帶。
3. 存檔磁帶。
4. 從存檔擷取磁帶。
5. 從磁帶還原資料。

為了測試您的設定，請使用相容的備份應用程式，如下所說明。

> **Note**
>
> 除非另有說明，所有備份應用程式都可在 Microsoft Windows 使用。

如需相容備份應用程式的詳細資訊，請參閱 磁帶閘道支援的第三方備份應用程式。

主題

使用 Arcserve Backup 測試您的設定

您可以使用 Arcserve Backup r17.0 將資料備份至虛擬磁帶、封存磁帶，以及管理虛擬磁帶程式庫（VTL）裝置。在本主題中，您可以找到如何使用磁帶閘道設定 Arcserve Backup 以及執行備份和還原操作的基本文件。如需使用 Arcserve Backup r17.0 的詳細資訊，請參閱《Arcserve 管理指南》https://documentation.arcserve.com/Arcserve-Backup/Available/R17/ENU/Bookshelf_Files/HTML/admingde/index.htm中的 Arcserve Backup r17 文件。

主題

將 Arcserve 設定為使用 VTL 裝置

將虛擬磁帶程式庫 （ VTL ） 裝置連接至用戶端後，您會掃描裝置。

掃描VTL裝置

1. 在 Arcserve Backup Manager 中，選擇 Utilities (公用程式) 選單。
2. 選擇 Media Assure and Scan (媒體確保和掃描)。

將磁帶載入至媒體集區

Arcserve 軟體連線至閘道而且磁帶變成可用時，Arcserve 會自動載入磁帶。如果在 Arcserve 軟體中找不到您的閘道，請試著在 Arcserve 中重新啟動磁帶引擎。

重新啟動磁帶引擎

1. 選擇 Quick Start (快速入門)，並選擇 Administration (管理)，然後選擇 Device (裝置)。
2. 在導覽選單上，開啟閘道的內容 (按右鍵) 選單，然後選擇匯入/匯出插槽。
3. 選擇 Quick Import (快速匯入)，並將磁帶指派給空的插槽。
4. 開啟閘道的內容 (按右鍵) 選單，然後選擇 Inventory/Offline Slots (清查/離線插槽)。
5. 選擇 Quick Inventory (快速清查)，以從資料庫擷取媒體資訊。

如果您新增新的磁帶，則需要掃描閘道中是否有新磁帶，以讓它出現在 Arcserve 中。如果新的磁帶未出現，則您必須匯入磁帶。

匯入磁帶

1. 選擇 Quick Start (快速入門) 選單，並選擇 Back up (備份)，然後選擇 Destination tape (目標磁帶)。
2. 選擇閘道，並開啟某個磁帶的內容 (按右鍵) 選單，然後選擇 Import/Export Slot (匯入/匯出插槽)。
3. 開啟每個新磁帶的內容 (按右鍵) 選單，然後選擇 Inventory (清查)。
4. 開啟每個新磁帶的內容 (按右鍵) 選單，然後選擇 Format (格式化)。

每個磁帶的條碼現在都會出現在 Storage Gateway 主控台中，而且每個磁帶都已可供使用。

將資料備份至磁帶

已將您的磁帶載入至 Arcserve 時，即可備份資料。備份程序與備份實體磁帶相同。

將資料備份至磁帶

1. 從 Quick Start (快速入門) 選單，開啟還原備份工作階段。
2. 選擇 Source (來源) 標籤，然後選擇您要備份的檔案系統或資料庫系統。
3. 選擇 Schedule (排程) 標籤，然後選擇您要使用的重複方法。
4. 選擇 Destination (目標) 標籤，然後選擇您要使用的磁帶。如果您所備份的資料大於磁帶可保留的資料，則 Arcserve 會提示您掛載新的磁帶。
5. 選擇 Submit (提交) 以備份資料。

> **Note**
>
> 如果磁帶閘道在進行中的備份工作期間因任何原因重新啟動，備份工作可能會失敗。若要完成失敗的備份工作，您必須重新提交備份工作。

存檔磁帶

當您存檔磁帶時，磁帶閘道會將磁帶從磁帶館移至離線儲存體。退出和存檔磁帶之前，建議您先檢查其上的內容。

存檔磁帶

1. 從 Quick Start (快速入門) 選單，開啟還原備份工作階段。
2. 選擇 Source (來源) 標籤，然後選擇您要備份的檔案系統或資料庫系統。
3. 選擇 Schedule (排程) 標籤，然後選擇您要使用的重複方法。
4. 選擇閘道，並開啟某個磁帶的內容 (按右鍵) 選單，然後選擇 Import/Export Slot (匯入/匯出插槽)。
5. 指派郵件插槽，以載入磁帶。Storage Gateway 主控台中的狀態會變更為存檔。存檔程序可能需要一些時間。

存檔程序可能需要一些時間才能完成。磁帶的初始狀態顯示為 IN TRANSIT TO VTS。封存開始時，狀態會變更為 ARCHIVING。封存完成時，磁帶不再列在 中，VTL而是封存在 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 中。

從磁帶還原資料

還原您已存檔資料的程序包含兩個步驟。

從存檔磁帶還原資料

1. 將存檔磁帶擷取至磁帶閘道。如需說明，請參閱 擷取已存檔的磁帶。
2. 使用 Arcserve 還原資料。此程序與從實體磁帶還原資料相同。如需說明，請參閱 Arcserve Backup r17 文件。

若要從磁帶還原資料，請使用下列程序。

從磁帶還原資料

1. 從 Quick Start (快速入門) 選單，開啟還原某個還原工作階段。
2. 選擇 Source (來源) 標籤，然後選擇您要還原的檔案系統或資料庫系統。
3. 選擇 Destination (目標) 標籤，並接受預設設定。
4. 選擇 Schedule (排程) 標籤，並選擇您要使用的重複方法，然後選擇 Submit (提交)。

後續步驟

清除不必要的資源

使用 Bacula Enterprise 測試設定

您可以使用 Bacula Enterprise 版本 10 將資料備份到虛擬磁帶、封存磁帶，以及管理您的虛擬磁帶櫃 (VTL) 裝置。在本主題中，您可以找到如何為磁帶閘道設定 Bacula 第 10 版備份應用程式以及執行備份和還原操作的基本文件。如需有關如何使用 Bacula 第 10 版的資訊，請參閱 Bacula Systems 手冊和文件或聯絡 Bacula Systems。

> **Note**
>
> Bacula 僅支援 Linux。

設定 Bacula Enterprise

將虛擬磁帶櫃 (VTL) 裝置連接到 Linux 用戶端後，您可以設定 Bacula 軟體以辨識您的裝置。如需如何將VTL裝置連線至用戶端的相關資訊，請參閱連接VTL您的裝置。

設定 Bacula

1. 從 Bacula Systems 取得經授權的 Bacula Enterprise 備份軟體。
2. 將 Bacula Enterprise 軟體安裝在您的內部部署環境或雲端電腦。

   有關如何取得安裝軟體的詳細資訊，請參閱 Enterprise Backup for Amazon S3 and Storage Gateway。如需更多安裝指引，請參閱 Bacula 白皮書 Using Cloud Services and Object Storage with Bacula Enterprise Edition。

配置真菌與設備一起使用 VTL

接下來，配置 Bacula 與您的設VTL備一起使用。以下為基本設定步驟。

設定 Bacula

1. 安裝 Bacula Director 和 Bacula Storage 協助程式。如需說明，請參閱 Bacula 白皮書 Using Cloud Services and Object Storage with Bacula Enterprise Edition 第 7 章。
2. Connect 到正在運行 Bacula 導演的系統並配置 i SCSI 啟動器。若要這麼做，請使用 Bacula 白皮書 Using Cloud Services and Object Storage with Bacula Enterprise Edition 步驟 7.4 提供的指令碼。
3. 設定儲存裝置。使用先前提到，Bacula 白皮書提供的指令碼。
4. 設定本機 Bacula Director、新增儲存目標，然後定義您磁帶的媒體集區。使用先前提到，Bacula 白皮書提供的指令碼。

將資料備份至磁帶

1. 在 Storage Gateway 主控台中建立磁帶。如需如何建立磁帶的資訊，請參閱建立磁帶。
2. 使用下列命令，將磁帶從 I/E 插槽移到儲存插槽。

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

   例如，下列命令將磁帶從 I/E 插槽 1601 移到儲存插槽 1。

   ```
   /opt/bacula/scripts/mtx-changer transfer 1601 1
   ```
3. 使用下列命令，啟動 Bacula 主控台。

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

> **Note**
>
> 建立和傳輸磁帶到 Bacula 時，請使用 Bacula 主控台 (bconsole) 命令 `update slots storage=VTL`，讓 Bacula 知道您建立的新磁帶。

4. 將磁帶以條碼標示為磁碟區名稱，或使用下列 bconsole 命令標示。

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

5. 使用下列命令掛載磁帶。

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

6. 建立使用您所建立之媒體集區的備份任務，然後使用與操作實體磁帶相同的順序，將資料寫入虛擬磁帶。
7. 使用下列命令，將磁帶從 Bacula 主控台卸載。

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

> **Note**
>
> 如果您的磁帶閘道在進行中的備份工作期間基於任何原因重新啟動，備份工作將會失敗，且 Bacula Enterprise 中的磁帶狀態將變更為FULL。如果您知道磁帶尚未完全使用，可以手動將磁帶狀態變更回，APPEND然後使用相同的磁帶繼續備份工作。如果有其他APPEND狀態的磁帶可用，您也可以在不同的磁帶上繼續工作。

存檔磁帶

特定磁帶的所有備份任務完成後，您可以將磁帶存檔，使用 mtx-changer 指令碼將磁帶從儲存插槽移至 I/E 插槽。這個動作類似其他備份應用程式的退出動作。

存檔磁帶

1. 使用 `/opt/bacula/scripts/mtx-changer` 命令，將磁帶從儲存插槽移到 I/E 插槽。

   例如，下列命令將磁帶從儲存插槽 1 移到 I/E 插槽 1601。

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

2. 確認磁帶是存檔在離線儲存體 (S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive)，且磁帶的狀態為已存檔。

從存檔和擷取磁帶還原資料

還原您已存檔資料的程序包含兩個步驟。

從存檔磁帶還原資料

1. 將存檔磁帶從存檔擷取至磁帶閘道。如需說明，請參閱 擷取已存檔的磁帶。
2. 使用 Bacula 軟體還原資料：

   a. 使用 `/opt/bacula/scripts/mtx-changer` 命令，將磁帶匯入儲存插槽，將磁帶從儲存插槽移到 I/E 插槽。

      例如，下列命令將磁帶從 I/E 插槽 1601 移到儲存插槽 1。

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

   b. 使用 Bacula 主控台更新插槽，然後掛載磁帶。

   c. 執行還原命令來還原您的資料。如需說明，請參閱 Bacula 文件。

使用 Commvault 測試設定

您可以使用 Commvault 第 11 版將資料備份至虛擬磁帶、封存磁帶，以及管理虛擬磁帶程式庫（VTL）裝置。在本主題中，您可以找到如何設定磁帶閘道之 Commvault 備份應用程式、執行備份存檔以及從存檔磁帶擷取資料的基本文件。如需如何使用 Commvault 的詳細資訊，請參閱 Commvault 網站上的 Commvault 快速入門指南。

主題

- 設定 Commvault 以使用 VTL 裝置
- 建立儲存政策和子用戶端
- 在 Commvault 中將資料備份至磁帶
- 在 Commvault 中存檔磁帶
- 從磁帶還原資料

設定 Commvault 以使用 VTL 裝置

將VTL裝置連接至 Windows 用戶端後，您可以將 Commvault 設定為識別它們。如需有關如何將VTL裝置連線至 Windows 用戶端的資訊，請參閱 將VTL裝置連線至 Windows 用戶端。

Commvault 備份應用程式不會自動識別VTL裝置。您必須手動新增裝置以向 Commvault 備份應用程式公開裝置，才能探索裝置。

設定 Commvault

1. 在 CommCell 主控台主功能表中，選擇 Storage ，然後選擇專家 Storage Configuration 以開啟選取 MediaAgents對話方塊。
2. 選擇您要使用的可用媒體代理程式，並選擇新增，然後選擇確定。
3. 在 Expert Storage Configuration (專家儲存組態) 對話方塊中，選擇 Start (啟動)，然後選擇 Detect/Configure Devices (偵測/設定裝置)。
4. 保持選取裝置類型 選項，並選擇詳盡偵測，然後選擇確定。
5. 在 Confirm Exhaustive Detection (確認詳盡偵測) 確認方塊中，選擇 Yes (是)。
6. 在 Device Selection (選取裝置) 對話方塊中，選擇媒體庫和其所有磁碟機，然後選擇 OK (確定)。請等待偵測到裝置，然後選擇關閉以關閉日誌報告。
7. 以滑鼠右鍵按一下媒體庫，並選擇設定，然後選擇是。關閉組態對話方塊。
8. 在 此程式庫是否有條碼讀取器？對話方塊中，選擇是 ，然後針對裝置類型選擇 IBM ULTRIUM V5。
9. 在 CommCell 瀏覽器中，選擇 Storage Resources ，然後選擇 Libraries 來查看您的磁帶程式庫。
10. 若要查看媒體庫中的磁帶，請開啟媒體庫的內容 (按右鍵) 選單，然後選擇 探索媒體、媒體位置、媒體庫。
11. 若要掛載磁帶，請開啟媒體的內容 (按右鍵) 選單，然後選擇載入。

建立儲存政策和子用戶端

每個備份和還原任務都會與一個儲存政策和一個子用戶端政策建立關聯。

儲存政策會將資料的原始位置映射到您的媒體。

建立儲存政策

1. 在 CommCell 瀏覽器中，選擇政策 。

2. 開啟儲存政策的內容 (按右鍵) 選單，然後選擇新增儲存政策。
3. 在建立儲存政策精靈中，選擇資料保護和存檔，然後選擇下一步。
4. 針對儲存政策名稱輸入名稱，然後選擇增量儲存政策。若要將此儲存政策與增量載入建立關聯，請選擇其中一個選項。否則，請保留未核取選項，然後選擇下一步。
5. 在 Do you want to Use Global Deduplication Policy? (您想要使用全域重複資料刪除政策嗎？) 對話方塊中，選擇您的 Deduplication (重複資料刪除) 偏好設定，然後選擇 Next (下一步)。
6. 從主要副本的 Library 中，選擇您的VTL程式庫，然後選擇下一個 。
7. 確認媒體代理程式設定正確，然後選擇下一步。
8. 確認臨時集區設定正確，然後選擇下一步。
9. 在iData 客服人員備份資料 中設定您的保留政策，然後選擇下一步 。
10. 檢閱加密設定，然後選擇下一步。
11. 若要查看儲存政策，請選擇儲存政策。

您建立子用戶端政策，並將它與儲存政策建立關聯。子用戶端政策可讓您從中央範本設定類似的檔案系統用戶端，因此您不需要手動設定許多類似的檔案系統。

建立子用戶端政策

1. 在 CommCell 瀏覽器中，選擇用戶端電腦 ，然後選擇您的用戶端電腦。選擇 File System ，然後選擇 defaultBackupSet。
2. 按一下滑鼠右鍵defaultBackupSet，選擇所有任務 ，然後選擇新增子用戶端 。
3. 在子用戶端屬性方塊中，在名稱 SubClient 中輸入名稱，然後選擇確定 。
4. 選擇 Browse (瀏覽)，並導覽至您要備份的檔案，然後選擇 Add (新增)，再關閉對話方塊。
5. 在 Subclient (子用戶端) 屬性方塊中，選擇 Storage Device (儲存裝置) 標籤，並從 Storage policy (儲存政策) 選擇儲存政策，然後選擇 OK (確定)。
6. 在出現的備份排程 視窗中，建立新子用戶端與備份排程的關聯。
7. 針對一次性或根據需求備份，選擇不排定，然後選擇確定。

   您現在應該會在 defaultBackupSet索引標籤中看到您的子用戶端。

在 Commvault 中將資料備份至磁帶

您會使用與您在使用實體磁帶時相同的程序，來建立備份任務並將資料寫入虛擬磁帶。如需詳細資訊，請參閱 Commvault 文件。

> **Note**
>
> 如果磁帶閘道在進行中的備份工作期間因任何原因重新啟動，備份工作可能會失敗。在某些情況下，您可以選取繼續失敗的備份工作的選項。否則您必須提交新的備份工作。如果 Commvault 在工作失敗後將磁帶標示為無法使用，您必須將磁帶重新載入磁帶機，才能繼續寫入磁帶。如果有多個磁帶可用，Commvault 可能會在不同的磁帶上繼續執行故障的備份工作。

在 Commvault 中存檔磁帶

您退出磁帶來開始存檔程序。當您存檔磁帶時，磁帶閘道會將磁帶從磁帶館移至離線儲存體。退出和存檔磁帶之前，建議您先檢查磁帶上的內容。

存檔磁帶

1. 在 CommCell 瀏覽器中，選擇 Storage Resources 、 Library ，然後選擇您的 Library 。選擇依位置的媒體，然後選擇媒體庫中的媒體。
2. 開啟您要存檔之磁帶的內容 (按右鍵) 選單，選擇所有任務、匯出，然後選擇確定。

存檔程序可能需要一些時間才能完成。磁帶的初始狀態顯示為 IN TRANSIT TO VTS。封存開始時，狀態會變更為 ARCHIVING。封存完成時，磁帶不再列於 中VTL。

在 Commvault 軟體中，確定磁帶已不再位於儲存體插槽中。

在 Storage Gateway 主控台的導覽窗格上，選擇磁帶。確認封存磁帶的狀態為 ARCHIVED。

從磁帶還原資料

您可以從未曾存檔和擷取過的磁帶還原資料，或從已存檔和擷取的磁帶還原資料。針對未曾存檔和擷取過的磁帶 (未擷取磁帶)，您有兩個選項來還原資料：

- 依子用戶端還原
- 依任務 ID 還原

依子用戶端還原未擷取磁帶中的資料

1. 在 CommCell 瀏覽器中，選擇用戶端電腦 ，然後選擇用戶端電腦。選擇 File System ，然後選擇 defaultBackupSet。

2. 開啟子用戶端的內容 (按右鍵) 選單，並選擇瀏覽和還原，然後選擇檢視內容。
3. 選擇您要還原的檔案，然後選擇復原所有選取項目。
4. 選擇首頁，然後選擇任務控制器以監控還原任務的狀態。

依任務 ID 還原未擷取磁帶中的資料

1. 在 CommCell 瀏覽器中，選擇用戶端電腦 ，然後選擇您的用戶端電腦。以滑鼠右鍵按一下檔案系統，並選擇檢視，然後選擇備份歷史記錄。
2. 在備份類型 類別中，選擇您要的備份任務類型，然後選擇確定。具有備份任務歷史記錄的標籤即會出現。
3. 尋找您要還原的任務 ID，並以滑鼠右鍵按一下它，然後選擇瀏覽和還原。
4. 在 Browse and Restore Options (瀏覽和還原選項) 對話方塊中，選擇 View Content (檢視內容)。
5. 選擇您要還原的檔案，然後選擇復原所有選取項目。
6. 選擇首頁，然後選擇任務控制器以監控還原任務的狀態。

從存檔和擷取磁帶還原資料

1. 在 CommCell 瀏覽器中，選擇 Storage Resources ，選擇 Library ，然後選擇您的 Library 。選擇依位置的媒體，然後選擇媒體庫中的媒體。
2. 以滑鼠右鍵按一下擷取磁帶，並選擇所有任務，然後選擇類別。
3. 在 Catalog Media (類別媒體) 對話方塊中，選擇 Catalog only (僅限類別)，然後選擇 OK (確定)。
4. 選擇 CommCell 首頁 ，然後選擇 任務控制器 來監控還原任務的狀態。
5. 任務成功之後，請開啟磁帶的內容 (按右鍵) 選單，並選擇檢視，然後選擇檢視類別內容。請記下任務 ID 值以供稍後使用。
6. 選擇重新分類/合併。請確定已在 Catalog Media (類別媒體) 對話方塊中選擇 Merge only (僅限合併)。
7. 選擇首頁，然後選擇任務控制器以監控還原任務的狀態。
8. 任務成功後，選擇CommCell 首頁 ，選擇控制面板 ，然後選擇瀏覽/搜尋/復原 。
9. 選擇在瀏覽和復原期間顯示過時資料、確定，然後選擇控制面板。
10. 在 CommCell 瀏覽器中，用滑鼠右鍵按一下用戶端電腦 ，然後選擇您的用戶端電腦。選擇檢視，然後選擇任務歷史記錄。
11. 在 Job History Filter (任務歷史記錄篩選條件) 對話方塊中，選擇 Advanced (進階)。
12. 選擇包含過時資料，然後選擇確定。

13. 在 Job History (任務歷史記錄) 對話方塊中，選擇 OK (確定) 以開啟 history of jobs (任務歷史記錄) 標籤。
14. 尋找您要還原的任務，並開啟其內容 (按右鍵) 選單，然後選擇瀏覽和還原。
15. 在 Browse and Restore (瀏覽和還原) 對話方塊中，選擇 View Content (檢視內容)。
16. 選擇您要還原的檔案，然後選擇復原所有選取項目。
17. 選擇首頁，然後選擇任務控制器以監控還原任務的狀態。

使用 Dell 測試您的設定 EMC NetWorker

您可以使用 Dell EMC NetWorker 19.5 將資料備份到虛擬磁帶、封存磁帶並管理您的虛擬磁帶程式庫（VTL）裝置。在本主題中，您可以找到有關如何設定 Dell EMC NetWorker 軟體與磁帶閘道搭配使用和執行備份的基本文件，包括如何設定儲存裝置、將資料寫入磁帶、封存磁帶，以及從磁帶還原資料。

如需如何安裝和使用 Dell EMC NetWorker 軟體的詳細資訊，請參閱 管理指南 。

如需相容備份應用程式的詳細資訊，請參閱 磁帶閘道支援的第三方備份應用程式。

主題

- 設定 以使用 VTL 裝置
- 允許將WORM磁帶匯入 Dell EMC NetWorker
- 將資料備份到 Dell 中的磁帶 EMC NetWorker
- 在 Dell 中封存磁帶 EMC NetWorker
- 從 Dell 中的封存磁帶還原資料 EMC NetWorker

設定 以使用 VTL 裝置

將虛擬磁帶程式庫 （VTL） 裝置連接至 Microsoft Windows 用戶端後，您可以設定 來識別您的裝置。如需有關如何將VTL裝置連線至 Windows 用戶端的資訊，請參閱 連接VTL您的裝置。

不會自動識別磁帶閘道裝置。若要讓VTL裝置暴露在 NetWorker 軟體中並取得軟體以進行探索，您可以手動設定軟體。以下內容假設您已正確安裝軟體，並且假設您對管理主控台相當熟悉。如需管理主控台的詳細資訊，請參閱 Dell EMC NetWorker 管理指南 中的 NetWorker 管理主控台介面一節。

設定VTL裝置的 Dell EMC NetWorker 軟體

1. 啟動 Dell EMC NetWorker Management Console 應用程式，從選單中選擇企業，然後從左側窗格中選擇 localhost。

2. 開啟 localhost 的內容 (按右鍵) 選單，然後選擇 Launch Application (啟動應用程式)。
3. 選擇 Devices (裝置) 標籤，開啟 Libraries (媒體櫃) 的內容 (按右鍵) 選單，然後選擇 Scan for Devices (掃描裝置)。
4. 在掃描裝置精靈中，選擇 Start Scan (開始掃描)，然後在出現的對話方塊中選擇 OK (確定)。
5. 展開媒體櫃資料夾以查看您所有的媒體櫃，並點擊 F5 刷新。此程序可能需要數秒鐘的時間才能將裝置載入媒體櫃。
6. 使用管理員權限開啟命令視窗 （cmd.exe），並執行與 Dell EMC NetWorker 19.5 一起安裝的`jbconfig`公用程式。

    a. 在選單提示中，輸入對應的數字，以選取設定自動偵測的SCSI點唱機 。
    b. 提示提供點唱機裝置的名稱時，請輸入名稱，例如 `AWSVTL`。
    c. 提示開啟 NetWorker 自動清理時，輸入 no。
    d. 出現略過自動設定的提示時，輸入 no。
    e. 當系統提示您設定另一個點唱機時，輸入 no。
7. 當 "jbconfig" 完成時，返回 Networker GUI並按 F5 重新整理。
8. 選擇您的媒體櫃以在左側裝格中查看您的磁帶，並在右側窗格中查看對應的空白磁碟區插槽清單。
9. 在磁碟區清單中，選取您希望啟用的磁碟區 (選取的磁碟區會以反白顯示)，開啟選取磁碟區的內容 (按右鍵) 選單，然後選擇 儲放。此動作會將磁帶從 I/E 插槽移動到磁碟區插槽。
10. 在出現的對話方塊中，選擇 Yes (是)，然後在 Load the Cartridges into (載入卡匣至) 對話方塊中，選擇 Yes (是)。
11. 若您沒有其他要儲放的磁帶，請選擇 No (否) 或 Ignore (略過)。否則，請選擇 Yes (是) 以儲放其他磁帶。

允許將WORM磁帶匯入 Dell EMC NetWorker

您現在可以將磁帶從磁帶閘道匯入 Dell EMC NetWorker程式庫。

虛擬磁帶會在讀取許多 （WORM） 磁帶時寫入，但 Dell EMC NetWorker預期不會WORM寫入磁帶。若要EMC NetWorker 讓 Dell 使用虛擬磁帶，您必須啟用將磁帶匯入非WORM媒體集區。

允許將WORM磁帶匯入非WORM媒體集區

1. 在 NetWorker 主控台上，選擇媒體 ，開啟 localhost 的內容 （按一下滑鼠右鍵） 選單，然後選擇屬性 。
2. 在NetWorker 嚴重屬性視窗中，選擇組態索引標籤。

3. 在蠕蟲磁帶處理區段WORM中，僅清除WORM集區方塊中的磁帶，然後選擇確定。

將資料備份到 Dell 中的磁帶 EMC NetWorker

將資料備份到磁帶的程序包含兩個步驟。

1. 標籤您希望備份資料的目標磁帶、建立目標媒體集區，然後將磁帶新增至集區。

   您會使用與操作實體磁帶相同的程序，來建立媒體集區並將資料寫入虛擬磁帶。如需詳細資訊，請參閱 Dell EMC NetWorker 管理指南 中的備份資料一節。
2. 將資料寫入磁帶。您可以使用 Dell EMC NetWorker User 應用程式而不是 Dell EMC NetWorker Management Console 備份資料。Dell EMC NetWorker User 應用程式會安裝 作為安裝的一部分 NetWorker。

> **Note**
>
> 您可以使用 Dell EMC NetWorker User 應用程式來執行備份，但您可以在 EMC 管理主控台中檢視備份和還原任務的狀態。若要檢視狀態，請選擇 Devices (裝置) 選單，然後在 Log (日誌) 視窗中檢視狀態。

> **Note**
>
> 如果您在進行中的備份任務期間，磁帶閘道因任何原因重新啟動，備份任務將暫停，且 Dell EMC Networker 中的磁帶狀態將變更為寫入保護 。您可以封存磁帶或繼續讀取磁帶中的資料。您可以在不同的磁帶上繼續暫停的備份工作。

在 Dell 中封存磁帶 EMC NetWorker

當您封存磁帶時，磁帶閘道會將磁帶從 Dell EMC NetWorker 磁帶程式庫移至離線儲存。您可以透過將磁帶從磁帶磁碟區退出至儲存體插槽，來開始存檔磁帶。然後，您可以使用備份應用程式，也就是 Dell EMC NetWorker 軟體，從插槽將磁帶撤回至封存。

使用 Dell 封存磁帶 EMC NetWorker

1. 在 NetWorker 管理視窗中的裝置索引標籤上，選擇 localhost 或您的EMC伺服器，然後選擇程式庫 。

2. 選擇您從虛擬磁帶媒體櫃中匯入的媒體櫃。
3. 從您已將資料寫入的磁帶清單中，開啟您希望存檔之磁帶的內容 (按右鍵) 選單，然後選擇 Eject/Withdraw (退出/撤銷)。
4. 在出現的確認方塊中，選擇 OK (確定)。

存檔程序可能需要一些時間才能完成。磁帶的初始狀態顯示為 IN TRANSIT TO VTS。封存開始時，狀態會變更為 ARCHIVING。封存完成時，磁帶不再列於 中VTL。

在 Dell EMC NetWorker 軟體中，確認磁帶不再位於儲存插槽中。

在 Storage Gateway 主控台的導覽窗格上，選擇磁帶。確認封存磁帶的狀態為 ARCHIVED。

從 Dell 中的封存磁帶還原資料 EMC NetWorker

還原您已存檔資料的程序包含兩個步驟：

1. 擷取已存檔磁帶的磁帶閘道。如需說明，請參閱 擷取已存檔的磁帶。
2. 使用 Dell EMC NetWorker 軟體還原資料。您可以透過建立一個還原資料夾檔案 (如同您從實體磁帶還原資料時) 以執行此作業。如需指示，請參閱 Dell EMC NetWorker 管理指南 中的使用 NetWorker 使用者程式一節。

後續步驟

清除不必要的資源

使用IBM頻譜保護來測試您的設定

您可以使用 IBM Spectrum Protect 與來將資料備份到虛擬磁帶、封存磁帶，以及管理虛擬磁帶櫃 (VTL) 裝置 AWS Storage Gateway。（ IBM頻譜保護以前稱為 Tivoli 存儲管理器。 ）

本主題包含如何為磁帶閘道設定IBM頻譜保護 8.1.10 版備份軟體的基本資訊。同時也包含使用IBM頻譜保護執行備份和還原作業的基本資訊。如需有關如何管理IBM頻譜保護備份軟體的詳細資訊，請參閱IBMIBM頻譜保護的管理工作概觀。

IBM頻譜保護備份軟體支援 AWS Storage Gateway 下列作業系統。

- Microsoft Windows Server
- Red Hat Linux

如需有關 Windows 的IBM頻譜保護支援的裝置的詳細資訊，請參閱IBM頻譜保護 (以前稱為 Tivoli 儲存管理員) 支援的裝置AIX，適用於 HP-UX、Solaris 和 Windows。

如需有關 Linux 的IBM頻譜保護支援的裝置的資訊，請參閱IBM頻譜保護 (以前稱為 Tivoli 儲存管理員) 支援的 Linux 裝置。

主題

- 設定IBM頻譜保護
- 設定IBM頻譜保護以與VTL裝置搭配使用
- 將資料寫入IBM頻譜中的磁帶保護
- 從存檔在IBM頻譜保護中的磁帶還原資料

設定IBM頻譜保護

將設VTL備連接到客戶端後，您可以配置IBM頻譜保護版本 8.1.10 軟件以識別它們。如需將VTL裝置連線到用戶端的詳細資訊，請參閱連接VTL您的裝置。

若要設定IBM頻譜保護

1. 從中獲取IBM頻譜保護版本 8.1.10 軟件的許可副本。IBM
2. 在您的現場部署環境或雲端 Amazon EC2 執行個體上安裝IBM頻譜保護軟體。如需詳細資訊，請參閱IBM頻譜保護IBM的安裝和升級文件。

   如需有關設定IBM頻譜保護軟體的詳細資訊，請參閱設定IBM頻譜保護伺服器的磁 AWS 帶閘道虛擬磁帶庫。

設定IBM頻譜保護以與VTL裝置搭配使用

接下來，配置IBM頻譜保護以與您的設VTL備一起使用。您可以設定IBM頻譜保護來搭配 Microsoft 視窗伺服器或 RHEL 上的VTL裝置使用。

設定視窗的IBM頻譜保護

有關如何在 Windows 上配置IBM頻譜保護的完整說明，請參閱聯想網站上的磁帶設備驅動程序 W126266。以下是此程序的基本文件。

為 Microsoft 視窗設定IBM頻譜保護

1. 取得正確的媒體變更器驅動程式套件。對於磁帶裝置驅動程式，IBM頻譜保護需要適用於 Windows 2012 的版本 W12 6266。如需如何取得驅動程式的詳細資訊，請參閱 Lenovo 網站上的 Tape Device Driver-W12 6266 for Windows 2012。

   > **Note**
   >
   > 請務必安裝「非專屬」的驅動程式。

2. 在您的電腦上，開啟 [電腦管理]，展開 [媒體轉換器裝置]，然後確認媒體轉換器類型是否列為 IBM3584 磁帶櫃。
3. 確認虛擬磁帶館裡的磁帶條碼都在八個字元以下。如果您嘗試分配的磁帶條碼超過 8 個字元，會出現此錯誤訊息："Tape barcode is too long for media changer"。
4. 確保您的所有磁帶機和媒體更換器都出現在 IBM Spectrum Protect 中。為此，請使用下列命令：`\Tivoli\TSM\server>tsmdlst.exe`

設定適用於 Linux 的IBM頻譜保護

以下是關於配置IBM頻譜與 Linux 上的設VTL備一起工作的基本文檔。

若要設定適用於 Linux 的IBM頻譜保護

1. 前往 Sup IBM port 網站上的「IBM修正中心」，然後選擇 「選取產品」。
2. 針對 Product Group (產品群組) 選擇 System Storage (系統儲存裝置)。
3. 針對 Select from System Storage (從系統儲存裝置中選取) 選擇 Tape systems (磁帶系統)。
4. 針對 Tape systems (磁帶系統) 選擇 Tape drivers and software (磁帶驅動程式和軟體)。
5. 針對 Select from Tape drivers and software (從磁帶驅動程式和軟體選取) 選擇 Tape device drivers (磁帶裝置驅動程式)。
6. 針對 Platform (平台) 選擇您的作業系統，然後選擇 Continue (繼續)。
7. 選擇您要下載的裝置驅動程式版本。然後依照「修正中心」下載頁面上的指示，下載並設定IBM頻譜保護。
8. 確認虛擬磁帶館裡的磁帶條碼都在八個字元以下。如果您嘗試分配的磁帶條碼超過 8 個字元，會出現此錯誤訊息："Tape barcode is too long for media changer"。

將資料寫入IBM頻譜中的磁帶保護

請使用與您在操作實體磁帶時相同的程序和備份政策，將資料寫入磁帶閘道虛擬磁帶。建立必要的備份和還原任務組態。如需有關設定IBM頻譜保護的詳細資訊，請參閱IBM頻譜保護的管理工作概觀。

> **Note**
>
> 如果磁帶閘道在進行中的備份工作期間因任何原因重新啟動，備份工作可能會失敗。如果備份工作失敗，IBM頻譜保護中的磁帶狀態會變更為ReadOnly。如果您知道磁帶尚未完全使用，可以手動將磁帶狀態變更回 ReadWrite，然後使用相同的磁帶繼續或重新提交備份工作。IBM如果其他處於ReadWrite狀態的磁帶可用，Spectrum Protect 可能會繼續在不同磁帶上執行故障的備份工作。

從存檔在IBM頻譜保護中的磁帶還原資料

還原您已存檔資料的程序包含兩個步驟。

從存檔磁帶還原資料

1. 將存檔磁帶從存檔擷取至磁帶閘道。如需說明，請參閱 擷取已存檔的磁帶。
2. 使用IBM頻譜保護備份軟體還原資料。您可以建立復原點來執行此作業，就像您從實體磁帶還原資料一樣。如需有關設定IBM頻譜保護的詳細資訊，請參閱IBM頻譜保護的管理工作概觀。

後續步驟

清除不必要的資源

使用 Micro Focus Data Protector 測試您的設定

您可以使用 Micro Focus （ VTL ） Data Protector v9.x 將資料備份到虛擬磁帶、封存磁帶，以及管理虛擬磁帶程式庫 （ HPE ） 裝置。在本主題中，您可以找到有關如何為磁帶閘道設定 Micro Focus （ HPE ） Data Protector 軟體，以及執行備份和還原操作的基本文件。如需如何使用 Micro Focus （ HPE ） Data Protector 軟體的詳細資訊，請參閱 Hewlett Packard 文件。如需相容備份應用程式的詳細資訊，請參閱 磁帶閘道支援的第三方備份應用程式。

主題

- 設定 Micro Focus （ HPE ） Data Protector 以使用 VTL 裝置
- 準備虛擬磁帶以搭配 HPE Data Protector 使用

- 將磁帶載入至媒體集區
- 將資料備份至磁帶
- 存檔磁帶
- 從磁帶還原資料

設定 Micro Focus （HPE） Data Protector 以使用 VTL 裝置

將虛擬磁帶程式庫 （VTL） 裝置連接至用戶端後，您可以設定 Micro Focus （HPE） Data Protector 來識別您的裝置。如需有關如何將VTL裝置連線至用戶端的資訊，請參閱 連接VTL您的裝置。

Micro Focus （HPE） Data Protector 軟體不會自動識別磁帶閘道裝置。若要讓軟體識別這些裝置，請手動新增裝置，然後探索VTL裝置，如下所述。

若要新增VTL裝置

1. 在 Micro Focus （HPE） Data Protector 主視窗中，選擇左上角清單中的裝置和媒體架。

   開啟 Devices (裝置) 的內容 (按右鍵) 選單，然後選擇 Add Device (新增裝置)。
2. 在 Add Device (新增裝置) 標籤上，輸入 Device Name (裝置名稱) 的值。針對裝置類型 ，選擇 SCSI Library ，然後選擇 Next 。
3. 在下個畫面上，執行下列作業：

   a. 如需SCSI程式庫機器人 的地址，請選取您的特定地址。

   b. 針對 Select what action Data Protector should take if the drive is busy (選取裝置忙碌時 Data Protector 應採取的動作)，選擇 Abort (中止) 或您慣用的動作。

   c. 選擇啟用這些選項：

      - 條碼讀取器支援
      - 自動探索變更SCSI的地址
      - SCSI Reserve/Release （聲控）

   d. 保持不選取 (未勾選) Use barcode as medium label on initialization (使用條碼做為初始化媒體標籤)，除非您的系統需要它。

   e. 選擇 Next (下一步) 繼續。
4. 在下個畫面上，指定您想要使用 HP Data Protector 的插槽。數字之間使用連字號 ("-")，以指出插槽範圍，例如 1–6。指定要使用的插槽後，請選擇 Next (下一步)。
5. 對於實體裝置使用的標準媒體類型，請選擇 LTO_Ultrium ，然後選擇完成以完成設定。

您的磁帶館現在已可使用。若要載入磁帶，請參閱下一節。

準備虛擬磁帶以搭配 HPE Data Protector 使用

您需要先準備要使用的磁帶，才能將資料備份到虛擬磁帶。執行此作業包括下列動作：

- 將虛擬磁帶載入到磁帶館
- 將虛擬磁帶載入到插槽
- 建立媒體集區
- 將虛擬磁帶載入到媒體集區

在下列各節中，您可以找到引導您完成此程序的步驟。

將虛擬磁帶載入到磁帶館

您的磁帶館現在應該會列於 Devices (裝置) 下。如果您沒有看見它，請按 F5 重新整理畫面。當您的程式庫列出後，您就可以將虛擬磁帶載入到程式庫。

將虛擬磁帶載入到您的磁帶館

1. 選擇磁帶館旁的加號顯示機器人路徑、磁碟機和插槽的節點。
2. 開啟 Drives (磁碟機) 的內容 (按右鍵) 選單，選擇 Add Drive (新增磁碟機)，輸入磁帶名稱，然後選擇 Next (下一步) 繼續。
3. 選擇您要為SCSI資料磁碟機地址新增的磁帶機，選擇自動探索變更SCSI的地址 ，然後選擇下一步。
4. 在下列畫面上，選擇 Advanced (進階)。Advanced Options (進階選項) 彈出式畫面隨即出現。

    a. 在 Settings (設定) 標籤上，您應考慮下列選項：

        - CRC 檢查 （偵測意外資料變更）
        - Detect dirty drive (偵測已變更磁碟機) (備份前請務必清理磁碟機)
        - SCSI Reserve/Release（drive）（避免磁帶爭用）

        針對測試用途，您可以保持停用這些選項 (取消核取)。

    b. 在 Sizes (大小) 標籤上，將 Block size (kB) (區塊大小 (kB)) 設定為 Default (256) (預設值 (256))。

    c. 選擇 OK (確定) 關閉進階選項畫面，然後選擇 Next (下一步) 繼續。

5. 在下個畫面上，選擇 Device Policies (裝置政策) 下的這些選項：
   - Device may be used for restore (可用於還原的裝置)
   - Device may be used as source device for object copy (可做為物件副本來源裝置的裝置)
6. 選擇 Finish (完成) 完成將磁帶機新增到磁帶館。

將虛擬磁帶載入到插槽

現在您的磁帶館中已有磁帶機，您可以將虛擬磁帶載入到插槽。

將虛擬磁帶載入到插槽

1. 在磁帶館樹節點中，開啟標籤為 Slots (插槽) 的節點。每個插槽都有以圖示表示的狀態：
   - 綠色磁帶表示磁帶已載入到插槽。
   - 灰色插槽表示插槽是空的。
   - 青色問號表示該插槽的磁帶未格式化。
2. 針對空插槽請開啟內容 (按右鍵) 選單，然後選擇 Enter。如有現成的磁帶，請選擇其中一個來載入到該插槽。

建立媒體集區

媒體集區是用來整理您磁帶的邏輯群組。您建立媒體集區以設定磁帶備份。

建立媒體集區

1. 在 Devices & Media (裝置和媒體) 欄中，開啟 Media (媒體) 樹節點，再開啟 Pools (集區) 節點的內容 (按右鍵) 選單，然後選擇 Add Media Pool (新增媒體集區)。
2. 針對 Pool name (集區名稱)，輸入名稱。
3. 對於媒體類型 ，選擇 LTO_Ultrium ，然後選擇下一步 。
4. 在下列畫面上，接受預設值，然後選擇 Next (下一步)。
5. 選擇 Finish (完成) 完成建立媒體集區。

將磁帶載入至媒體集區

您必須先將磁帶載入到您所建立的媒體集區，才能將資料備份到您的磁帶。

將虛擬磁帶載入到媒體集區

1. 在您的磁帶館樹節點上，選擇 Slots (插槽) 節點。
2. 選擇已載入的磁帶，有綠色圖示顯示該磁帶已載入。開啟內容 (按右鍵) 選單，然後選擇 Format (格式化) 及 Next (下一步)。
3. 選擇您建立的媒體集區，然後選擇 Next (下一步)。
4. 針對 Medium Description (媒體描述)，選擇 Use barcode (使用條碼)，然後選擇 Next (下一步)。
5. 針對 Options (選項)，選擇 Force Operation (強制操作)，然後選擇 Finish (完成)。

您現在應該會看到您所選擇的插槽已從未指派 (灰色) 狀態變更成插入磁帶 (綠色) 狀態。會顯示一系列訊息確認您的媒體已初始化。

此時，您應該已設定所有設定，以開始將虛擬磁帶程式庫與 HPE Data Protector 搭配使用。請使用下列程序再次確認一切正確。

驗證您的磁帶櫃是否設定好可供使用

- 選擇 Drives (磁碟機)，然後開啟您磁碟機的內容 (按右鍵) 選單並選擇 Scan (掃描)。

如果您的組態正確，訊息就會確認已成功掃描您的媒體。

將資料備份至磁帶

當您的磁帶已載入至媒體集區時，您就可以將資料備份到磁帶。

將資料備份至磁帶

1. 從視窗左上角的下拉式功能表中選擇備份。
2. 從左側窗格展開備份導覽樹狀目錄。
3. 在 Filesystem 上按一下滑鼠右鍵以開啟內容選單，然後選擇新增備份 。
4. 在 Create New Backup (建立新備份) 畫面的 Filesystem (檔案系統) 下，選擇 Blank File System Backup (空白檔案系統備份)，然後選擇 OK (確定)。
5. 在顯示主機系統的樹節點上，選取檔案系統或您要備份的檔案系統，然後選擇 Next (下一步) 繼續。
6. 開啟您要使用的磁帶館樹節點及您要使用的磁帶機內容 (按右鍵) 選單，然後選擇 Properties (屬性)。
7. 選擇您的媒體集區，然後選擇 OK (確定) 及 Next (下一步)。

8. 在接下來的三個畫面中，接受預設設定，然後選擇 Next (下一步)。
9. 在 Perform finishing steps in your backup/template design (執行備份/範本設計的完成步驟) 畫面上，選擇 Save as (另存新檔) 儲存此工作階段。在彈出式視窗中，命名備份，並將它指派給您想要儲存新備份規格的群組。
10. 選擇 Start Interactive Backup (開始互動式備份)。

如果主機系統包含資料庫系統，您可以選擇它做為您的目標備份系統。這些畫面和選項類似前述的檔案系統備份。

> **Note**
>
> 如果您的磁帶閘道在進行中的備份工作期間因任何原因重新啟動，備份工作將會失敗，而且 Data Protector 中的磁帶機會標示為已修改。Data Protector 也會將磁帶品質標籤為差，並防止寫入磁帶。若要繼續從磁帶讀取資料，您必須清理磁碟機並重新掛載磁帶。若要完成失敗的備份工作，您必須在新磁帶上重新提交備份工作。

存檔磁帶

當您存檔磁帶時，磁帶閘道會將磁帶從磁帶館移至離線儲存。退出和存檔磁帶之前，建議您先檢查其上的內容。

磁帶存檔前先檢查內容

1. 選擇 Slots (插槽)，然後選擇您要檢查的磁帶。
2. 選擇 Objects (物件) 然後檢查磁帶的內容。

如已選擇存檔磁帶，請使用下列程序。

退出和存檔磁帶

1. 開啟該磁帶的內容 (按右鍵) 選單，然後選擇 Eject (退出)。
2. 在 Storage Gateway 主控台上，選擇閘道，然後選擇VTL磁帶磁帶磁帶磁帶匣，然後驗證您正在封存的虛擬磁帶的狀態。

退出磁帶之後，它會自動存檔在離線儲存 (S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive)。存檔程序可能需要一些時間才能完成。磁帶的初始狀態顯示為 IN TRANSIT TO VTS。封

存開始時，狀態會變更為 ARCHIVING。封存完成時，磁帶不再列在 中，VTL而是封存在 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 中。

從磁帶還原資料

還原您已存檔資料的程序包含兩個步驟。

從存檔磁帶還原資料

1. 將存檔磁帶擷取至磁帶閘道。如需說明，請參閱 擷取已存檔的磁帶。
2. 使用 HPE Data Protector 還原資料。此程序與從實體磁帶還原資料相同。

若要從磁帶還原資料，請使用下列程序。

從磁帶還原資料

1. 從視窗左上角的下拉式功能表中選擇還原。
2. 選擇您要從左側導覽樹狀結構還原的檔案系統或資料庫系統。確定已選取您想要還原的備份。選擇 Restore (還原)。
3. 在 Start Restore Session (開始還原工作階段) 視窗中，選擇 Needed Media (需要的媒體)。選擇 All media (全部媒體)，您應該會看到備份原來使用的磁帶。選擇該磁帶，然後選擇 Close (關閉)。
4. 在 Start Restore Session (開始還原工作階段) 視窗中，接受預設設定，選擇 Next (下一步) 及 Finish (完成)。

後續步驟

清除不必要的資源

使用 Microsoft System Center 測試您的設定 DPM

您可以使用 Microsoft System Center 2012 R2 或 2016 Data Protection Manager （ VTL ），將資料備份至虛擬磁帶、封存磁帶和管理虛擬磁帶程式庫 （ ） 裝置DPM。在本主題中，您可以找到有關如何設定磁帶閘道DPM備份應用程式，以及執行備份和還原操作的基本文件。

如需如何使用 的詳細資訊DPM，請參閱 Microsoft System Center 網站上的DPM文件。如需相容備份應用程式的詳細資訊，請參閱 磁帶閘道支援的第三方備份應用程式。

主題

- 設定 DPM以識別VTL裝置
- 將磁帶匯入 DPM
- 在 中將資料寫入磁帶 DPM
- 使用 封存磁帶 DPM
- 從 中封存的磁帶還原資料 DPM

設定 DPM以識別VTL裝置

將虛擬磁帶程式庫 （ VTL ） 裝置連接至 Windows 用戶端後，您可以設定 DPM 來識別您的裝置。如需有關如何將VTL裝置連線至 Windows 用戶端的資訊，請參閱 連接VTL您的裝置。

根據預設，DPM伺服器無法辨識磁帶閘道裝置。若要設定伺服器使用磁帶閘道裝置，您可以執行下列任務：

1. 更新VTL裝置的裝置驅動程式，以將其公開至DPM伺服器。
2. 手動將VTL裝置映射至DPM磁帶程式庫。

更新VTL裝置驅動程式

- 在裝置管理員中，更新媒體變更器的驅動程式。如需說明，請參閱 更新媒體變更器的裝置驅動程式。

您可以使用 DPMDriveMappingTool將磁帶機映射至DPM磁帶程式庫。

將磁帶機映射至DPM伺服器磁帶程式庫

1. 為您的閘道建立至少一個磁帶。如需如何在主控台上執行此作業的資訊，請參閱建立磁帶。
2. 將磁帶匯入DPM程式庫。如需如何執行此作業的資訊，請參閱 將磁帶匯入 DPM。
3. 如果DPMLA服務正在執行，請開啟命令終端機並在命令列中輸入下列項目來停止服務。

   ```
   net stop DPMLA
   ```

4. 在DPM伺服器上找到下列檔案：`%ProgramFiles%\System Center 2016 R2\DPM\DPM\Config\DPMLA.xml`。

> **Note**
>
> 如果存在此檔案， 會DPMDriveMappingTool覆寫它。如果您要保留原始檔案，請建立備份複本。

5. 開啟命令終端機，並將目錄切換至 `%ProgramFiles%\System Center 2016 R2\DPM\DPM\Bin`，然後執行下列命令。

```
C:\Microsoft System Center 2016 R2\DPM\DPM\bin>DPMDriveMappingTool.exe
```

此命令的輸出如下。

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

將磁帶匯入 DPM

您現在可以將磁帶從磁帶閘道匯入DPM備份應用程式程式庫。

將磁帶匯入DPM備份應用程式程式庫

1. 在DPM伺服器上，開啟管理主控台，選擇重新掃描 ，然後選擇重新整理 。管理主控台會顯示您的媒體變更器和磁帶機。
2. 在 Library (磁帶館) 區段中開啟媒體變更器的內容 (按右鍵) 選單，然後選擇 Add tape (I/E port) (新增磁帶 (I/E 連接埠)) 將磁帶新增至 Slots (插槽) 清單。

> **Note**
>
> 新增磁帶的程序需要幾分鐘的時間才能完成。

磁帶標籤會顯示為 Unknown (不明)，而且無法使用磁帶。若要讓磁帶可供使用，您必須識別它。

3. 開啟您要識別之磁帶的內容 (按右鍵) 選單，然後選擇 Identify unknown tape (識別不明磁帶)。

> **Note**
>
> 識別磁帶的程序可能需要幾秒鐘或幾分鐘的時間。
> 如果磁帶未正確顯示條碼，您需要將媒體變更器驅動程式變更為 Sun/StorageTek Library。如需詳細資訊，請參閱在 Microsoft System Center 中顯示磁帶的條碼 DPM。

識別完成時，磁帶標籤會變更為 Free (可用)。也就是說，可將資料寫入磁帶。

在 中將資料寫入磁帶 DPM

您可以使用與您在操作實體磁帶時相同的保護程序和政策，將資料寫入磁帶閘道虛擬磁帶。您可以建立保護群組，並新增您要備份的資料，然後建立復原點來備份資料。如需如何使用 的詳細資訊DPM，請參閱 Microsoft System Center 網站上的DPM文件。

根據預設，磁帶的容量為 30GB。所備份的資料大於磁帶的容量時，會發生磁帶 I/O 錯誤。如果錯誤發生的位置大於磁帶的大小，Microsoft DPM 會將錯誤視為磁帶結束的指示。如果發生錯誤的位置小於磁帶的大小，則備份任務會失敗。若要解決此問題，請變更登錄項目中的 `TapeSize` 值，以符合磁帶的大小。如需如何執行此作業的資訊，請參閱 Microsoft System Center 上的錯誤 ID：30101。

> **Note**
>
> 如果您的磁帶閘道在進行中的備份工作期間因任何原因重新啟動，備份工作將會失敗。若要完成失敗的備份工作，您必須重新提交備份工作。

使用 封存磁帶 DPM

當您封存磁帶時，磁帶閘道會將磁帶從DPM磁帶程式庫移至離線儲存。您可以使用備份應用程式從插槽移除磁帶，即 開始磁帶封存DPM。

在 中封存磁帶 DPM

1. 開啟您要存檔之磁帶的內容 (按右鍵) 選單，然後選擇 Remove tape (I/E port) (移除磁帶 (I/E 連接埠))。
2. 在出現的對話方塊中，選擇 Yes (是)。這樣做會從媒體變更器的儲存插槽退出磁帶，並將磁帶移至其中一個閘道的 I/E 插槽。將磁帶移至閘道的 I/E 插槽時，即會立即傳送它以供存檔。
3. 在 Storage Gateway 主控台上，選擇您的閘道，然後選擇VTL磁帶磁帶磁帶匣，然後驗證您正在封存的虛擬磁帶的狀態。

   存檔程序可能需要一些時間才能完成。磁帶的初始狀態顯示為 IN TRANSIT TO VTS。封存開始時，狀態會變更為 ARCHIVING。封存完成時，磁帶不再列於 中VTL。

從 中封存的磁帶還原資料 DPM

還原您已存檔資料的程序包含兩個步驟。

從存檔磁帶還原資料

1. 將存檔磁帶從存檔擷取至磁帶閘道。如需說明，請參閱 擷取已存檔的磁帶。
2. 使用DPM備份應用程式還原資料。您可以建立復原點來執行此作業，就像您從實體磁帶還原資料一樣。如需指示，請參閱 DPM 網站上的復原用戶端電腦資料。

後續步驟

清除不必要的資源

使用 測試您的設定 NovaStor DataCenter

您可以使用 NovaStor DataCenter/Network 6.4 或 7.1 版，將資料備份至虛擬磁帶、封存磁帶，以及管理虛擬磁帶程式庫 （ VTL ） 裝置。在本主題中，您可以找到如何為磁帶閘道設定 NovaStor DataCenter/Network 7.1 版備份應用程式，以及執行備份和還原操作的基本文件。如需如何使用 NovaStor DataCenter/Network 7.1 版的詳細資訊，請參閱 文件 NovaStor DataCenter/Network 。

設定 NovaStor DataCenter/Network

將虛擬磁帶程式庫 （ VTL ） 裝置連接至 Microsoft Windows 用戶端後，您可以將 NovaStor 軟體設定為識別您的裝置。如需有關如何將VTL裝置連線至 Windows 用戶端的資訊，請參閱 連接VTL您的裝置。

NovaStor DataCenter/Network 需要驅動程式製造商的驅動程式。您可以使用 Windows 驅動程式，但必須先停用其他備份應用程式。

設定 NovaStor DataCenter/Network 以使用 VTL 裝置

將VTL裝置設定為使用 NovaStor DataCenter/Network 6.4 或 7.1 版時，您可能會看到錯誤訊息，其中顯示 `External Program did not exit correctly`。此問題需要您在繼續之前所需執行的解決方法。

您可以在開始設定VTL裝置之前建立解決方法，以防止問題發生。如需如何建立解決方法的資訊，請參閱解決 "External Program Did Not Exit Correctly" 錯誤。

若要設定 NovaStor DataCenter/Network 以使用 VTL 裝置

1. 在 NovaStor DataCenter/Network Admin 主控台中，選擇 Media Management ，然後選擇 Storage Management 。
2. 在 Storage Targets (儲存目標) 選單中，開啟 Media Management Servers (媒體管理伺服器) 的內容 (按右鍵) 選單，並選擇 New (新增)，然後選擇 OK (確定) 以建立並預先填入 storage (儲存) 節點。

   如果您看到的錯誤訊息指出 `External Program did not exit correctly`，則請先解決問題，再繼續。此問題需要解決方法。如需解決此問題的詳細資訊，請參閱 解決 "External Program Did Not Exit Correctly" 錯誤。

   > **Important**
   >
   > 發生此錯誤是因為儲存磁碟機和磁帶機的 AWS Storage Gateway 元素指派範圍超過 DataCenter/Network 允許的數量 NovaStor。

3. 開啟所建立 storage (儲存) 節點的內容 (按右鍵) 選單，然後選擇 New Library (新增磁帶館)。
4. 從清單選擇磁帶館伺服器。即會自動填入磁帶館清單。
5. 指定磁帶館名稱，然後選擇 OK (確定)。

6. 選擇磁帶館，以顯示 Storage Gateway 虛擬磁帶館的所有屬性。
7. 在 Storage Targets (儲存目標) 選單中，展開 Backup Servers (備份伺服器)，並開啟伺服器的內容 (按右鍵) 選單，然後選擇 Attach Library (連接磁帶館)。
8. 在出現的連接程式庫對話方塊中，選擇LTO5媒體類型，然後選擇確定 。
9. 展開備份伺服器，以查看 Storage Gateway 虛擬磁帶館以及顯示所有掛載磁帶機的磁帶館分割區。

建立磁帶集區

在 NovaStor DataCenter/Network 軟體中動態建立磁帶集區，因此不包含固定數量的媒體。需要磁帶的磁帶集區會從其臨時集區中取得。臨時集區是可供一或多個磁帶集區自由使用的磁帶蓄水池。磁帶集區會將超過其保留時間且不再需要的任何媒體傳回給臨時集區。

建立磁帶集區是一種三步驟的任務：

1. 您建立臨時集區。
2. 您將磁帶指派給臨時集區。
3. 您建立磁帶集區。

建立臨時集區

1. 在左導覽選單中，選擇 Scratch Pools (臨時集區) 標籤。
2. 開啟 Scratch Pools (臨時集區) 的內容 (按右鍵) 選單，然後選擇 Create Scratch Pool (建立臨時集區)。
3. 在 Scratch Pools (臨時集區) 對話方塊中，指定臨時集區的名稱，然後選擇媒體類型。
4. 選擇 Label Volume (將磁碟區加上標籤)，然後建立臨時集區的低水位。將臨時集區清空至低水位時，會出現警告。
5. 在出現的警告對話方塊中，選擇 OK (確定) 以建立臨時集區。

將磁帶指派給臨時集區

1. 在左導覽選單中，選擇 Tape Library Management (磁帶館管理)。
2. 選擇 Library (磁帶館) 標籤，以查看磁帶館清查。
3. 選擇要指派給臨時集區的磁帶。請確定磁帶設定為正確的媒體類型。

4. 開啟磁帶館的內容 (按右鍵) 選單，然後選擇 Add to Scratch Pool (新增至臨時集區)。

您現在有可用於磁帶集區的實心臨時集區。

建立磁帶集區

1. 從左導覽選單，選擇 Tape Library Management (磁帶館管理)。
2. 開啟 Media Pools (媒體集區) 標籤的內容 (按右鍵) 選單，然後選擇 Create Media Pool (建立媒體集區)。
3. 指定媒體集區的名稱，然後選擇 Backup Server (備份伺服器)。
4. 選擇媒體集區的磁帶館分割區。
5. 選擇臨時集區，讓集區從中取得磁帶。
6. 針對 Schedule (排程)，選擇 Not Scheduled (未排定)。

設定媒體匯入和匯出以存檔磁帶

NovaStor DataCenter如果 /Network 是媒體變更器的一部分，則可以使用匯入/匯出插槽。

對於匯出， NovaStor DataCenter/網路必須知道要從程式庫實際取出哪些磁帶。

對於匯入， NovaStor DataCenter/Network 會識別在磁帶程式庫中匯出的磁帶媒體，並提供從資料插槽或匯出插槽匯入所有磁帶媒體。您的磁帶閘道會將磁帶存檔在離線儲存體 (S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive)。

設定媒體匯入和匯出

1. 導覽至 Tape Library Management (磁帶館管理)，並選擇 Media Management Server (媒體管理伺服器) 的伺服器，然後選擇 Library (磁帶館)。
2. 選擇 Off-site Locations (離站位置) 標籤。
3. 開啟白色區域的內容 (按右鍵) 選單，然後選擇 Add (新增) 以開啟新的面板。
4. 在面板中，輸入 **`S3 Glacier Flexible Retrieval`** 或 **`S3 Glacier Deep Archive`**，並在文字方塊中新增選用描述。

將資料備份至磁帶

您會使用與您在操作實體磁帶時相同的程序，來建立備份任務並將資料寫入虛擬磁帶。如需如何使用 NovaStor 軟體備份資料的詳細資訊，請參閱 文件 NovaStor DataCenter/網路 。

> **Note**
>
> 如果您的磁帶閘道在進行中的備份工作期間基於任何原因重新啟動，備份工作將會失敗，且磁帶將變為無法寫入。您可以封存磁帶或繼續讀取磁帶中的資料。若要完成失敗的備份工作，您必須在新磁帶上重新提交備份工作。

存檔磁帶

當您存檔磁帶時，磁帶閘道會將磁帶從磁帶機退出至儲存插槽。然後，它會使用您的備份應用程式，即 NovaStor DataCenter網路，將磁帶從插槽匯出至封存。

存檔磁帶

1. 在左導覽選單中，選擇 Tape Library Management (磁帶館管理)。
2. 選擇 Library (磁帶館) 標籤，以查看磁帶館清查。
3. 反白您要存檔的磁帶，並開啟磁帶的內容 (按右鍵) 功能表，然後選擇離站存檔位置。

存檔程序可能需要一些時間才能完成。磁帶的初始狀態顯示為 IN TRANSIT TO VTS。封存開始時，狀態會變更為 ARCHIVING。封存完成時，磁帶不再列於 中VTL。

在 NovaStor DataCenter/Network 中，確認磁帶已不在儲存槽中。

在 Storage Gateway 主控台的導覽窗格上，選擇磁帶。確認封存磁帶的狀態為 ARCHIVED。

從存檔和擷取磁帶還原資料

還原您已存檔資料的程序包含兩個步驟。

從存檔磁帶還原資料

1. 將存檔磁帶從存檔擷取至磁帶閘道。如需說明，請參閱 擷取已存檔的磁帶。
2. 使用 NovaStor DataCenter/Network 軟體還原資料。做法是重新整理郵件插槽，並將您要擷取的每個磁帶移至空的插槽，就像從實體磁帶還原資料時一樣。如需還原資料的相關資訊，請參閱 文件 NovaStor DataCenter/網路 。

同時將數個備份任務寫入至磁帶硬碟

在 NovaStor 軟體中，您可以使用多工功能同時將數個任務寫入磁帶機。多工器適用於媒體集區時，可以使用此功能。如需如何使用多工的詳細資訊，請參閱 文件 NovaStor DataCenter/網路 。

解決 "External Program Did Not Exit Correctly" 錯誤

將VTL裝置設定為使用 NovaStor DataCenter/Network 6.4 或 7.1 版時，您可能會看到錯誤訊息，其中顯示 `External Program did not exit correctly`。發生此錯誤是因為儲存磁碟機和磁帶機的 Storage Gateway 的元素指派範圍超過 DataCenter/Network NovaStor允許的數字。

Storage Gateway 會傳回 3200 個儲存和匯入/匯出插槽，這超過 NovaStor DataCenter/Network 允許的 2400 個限制。若要解決此問題，請新增組態檔案，以啟用 NovaStor 軟體來限制儲存體和匯入/匯出插槽的數量，並預先設定元素指派範圍。

套用 "external program did not exit correctly" 錯誤的解決方案

1. 導覽至電腦上安裝軟體的 NovaStor磁帶資料夾。
2. 在磁帶資料夾中，建立文字檔案，並將它命名為 `hijacc.ini`。
3. 複製下列內容，並將其貼入 `hijacc.ini` 檔案，然後儲存檔案。

```
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. 將磁帶館新增並連接至媒體管理伺服器。
5. 使用下列命令，將磁帶從匯入/匯出插槽移至程式庫。將範例程式庫名稱取代為您部署中的程式庫名稱。

   ```
   C:\Program Files\NovaStor\DataCenter\Hitback\tape\ophijacc.exe -c VTL-ec2amaz-uko8jfj-ec2amaz-uko8jfj.lcfg
   ```

6. 將磁帶館連接至備份伺服器。
7. 在 NovaStor 軟體中，從匯入/匯出插槽將所有磁帶匯入程式庫。

使用 Quest NetVault Backup 測試您的設定

您可以使用下列 Quest （ 先前為 DellVTL ） NetVault 備份版本，將資料備份至虛擬磁帶、封存磁帶，以及管理虛擬磁帶程式庫 （ ） 裝置：

- Quest NetVault Backup 12.4
- Quest NetVault Backup 13.x

在本主題中，您可以找到有關如何為磁帶閘道設定 Quest NetVault Backup 應用程式，以及執行備份和還原操作的基本文件。

如需如何使用 Quest NetVault Backup 應用程式的詳細資訊，請參閱 Quest NetVault Backup – 管理指南。如需相容備份應用程式的詳細資訊，請參閱 磁帶閘道支援的第三方備份應用程式。

主題

設定 Quest NetVault Backup 以使用 VTL 裝置

將虛擬磁帶程式庫 （ VTL ） 裝置連接至 Windows 用戶端後，您可以設定 Quest NetVault Backup 來識別您的裝置。如需有關如何將VTL裝置連線至 Windows 用戶端的資訊，請參閱 連接VTL您的裝置。

Quest NetVault Backup 應用程式不會自動識別磁帶閘道裝置。您必須手動新增裝置，以將其公開至 Quest NetVault Backup 應用程式，然後探索VTL裝置。

新增VTL裝置

若要新增VTL裝置

1. 在 Quest NetVault Backup 中，選擇組態索引標籤中的管理裝置。
2. 在管理裝置頁面上，選擇 Add Devices (新增裝置)。
3. 在新增儲存體精靈中，選擇 Tape library / media changer (磁帶媒體櫃 / 媒體變更器)，然後選擇 Next (下一步)。
4. 在下一頁上，選擇實體連接到媒體櫃的用戶端機器，然後選擇 Next (下一步) 以掃描裝置。

5. 若找到裝置，便會顯示。在這種情形下，您的媒體變更器會在裝置方塊中顯示。
6. 選擇您的媒體變更器，然後選擇 Next (下一步)。精靈中會顯示裝置的詳細資訊。
7. 在 Add Tapes to Bays (新增磁帶至插槽) 頁面上，選擇 Scan For Devices (掃描裝置)，選擇您的用戶端機器，然後選擇 Next (下一步)。

   Quest NetVault Backup 會顯示所有磁碟機，以及您可以新增磁碟機的 10 個磁碟槽。插槽會一次顯示一個。
8. 選擇您希望新增至剛才顯示之插槽的磁碟，然後選擇 Next (下一步)。

   > **Important**
   >
   > 當您將磁碟新增至插槽時，磁碟和插槽號碼必須相符。例如若顯示插槽 1，您必須新增磁碟 1。若磁碟尚未連線，請將其相符的插槽保留空白。
9. 當您的用戶端機器出現時，請選擇它，然後選擇 Next (下一步)。用戶端機器可顯示多次。
10. 在顯示磁碟時，請重複步驟 7 到 9 來將所有磁碟新增至插槽。
11. 在 Configuration (組態) 標籤中，選擇 Manage devices (管理裝置)，然後在 Manage Devices (管理裝置) 頁面上，展開您的媒體變更器，以查看您新增的裝置。

在 Quest NetVault Backup 中將資料備份至磁帶

您會使用與操作實體磁帶相同的程序，來建立備份任務並將資料寫入虛擬磁帶。如需如何備份資料的詳細資訊，請參閱 Quest NetVault Backup - 管理指南 。

> **Note**
>
> 如果您的磁帶閘道在進行中的備份工作期間因任何原因重新啟動，備份工作將會失敗。若要完成失敗的備份工作，您必須重新提交備份工作。

使用 Quest NetVault Backup 封存磁帶

當您存檔磁帶時，磁帶閘道會將磁帶從磁帶機退出至儲存插槽。然後，它會使用您的備份應用程式將磁帶從插槽匯出到封存，也就是 Quest NetVault Backup。

在 Quest NetVault Backup 中封存磁帶

1. 在 Quest NetVault Backup Configuration 索引標籤中，選擇並展開媒體變更器，以查看磁帶。

2. 選擇插槽的設定圖示，以開啟媒體變更器的插槽瀏覽器。
3. 在插槽中，選擇要封存的磁帶，然後選擇匯出 。

存檔程序可能需要一些時間才能完成。磁帶的初始狀態顯示為 IN TRANSIT TO VTS。封存開始時，狀態會變更為 ARCHIVING。封存完成時，磁帶不再列於 中VTL。

在 Quest NetVault Backup 軟體中，確認磁帶已不在儲存槽中。

在 Storage Gateway 主控台的導覽窗格上，選擇磁帶。確認封存磁帶的狀態為 ARCHIVED。

從 Quest NetVault Backup 中封存的磁帶還原資料

還原您已存檔資料的程序包含兩個步驟。

從存檔磁帶還原資料

1. 將存檔磁帶從存檔擷取至磁帶閘道。如需說明，請參閱 擷取已存檔的磁帶。
2. 使用 Quest NetVault Backup 應用程式還原資料。您可以透過建立一個還原資料夾檔案 (如同您從實體磁帶還原資料時) 以執行此作業。如需建立還原任務的指示，請參閱 Quest NetVault Backup - 管理指南 。

後續步驟

清除不必要的資源

使用 Veeam Backup and Replication 測試您的設定

您可以使用 Veeam Backup & Replication 11A 將資料備份至虛擬磁帶、封存磁帶，以及管理虛擬磁帶程式庫 （ VTL ） 裝置。在本主題中，您可以找到如何設定磁帶閘道之 Veeam Backup & Replication 軟體以及執行備份和還原操作的基本文件。如需如何使用 Veeam 軟體的詳細資訊，請參閱 Veeam 說明中心內的關於 Veeam Backup & Replication。如需相容備份應用程式的詳細資訊，請參閱 磁帶閘道支援的第三方備份應用程式。

主題

- 將 Veeam 設定為使用 VTL 裝置
- 將磁帶匯入至 Veeam
- 在 Veeam 中將資料備份至磁帶

- 使用 Veeam 存檔磁帶
- 在 Veeam 中從存檔的磁帶還原資料

將 Veeam 設定為使用 VTL 裝置

將虛擬磁帶程式庫 （ VTL ） 裝置連接至 Windows 用戶端後，您可以設定 Veeam Backup & Replication 來識別您的裝置。如需有關如何將VTL裝置連線至 Windows 用戶端的資訊，請參閱 連接VTL您的裝置。

更新VTL裝置驅動程式

若要將軟體設定為與磁帶閘道裝置搭配使用，請更新VTL裝置的裝置驅動程式，以將其公開至 Veeam 軟體，然後探索VTL裝置。在裝置管理員中，更新媒體變更器的驅動程式。如需說明，請參閱 更新媒體變更器的裝置驅動程式。

探索VTL裝置

如果您的媒體變更器未知，您必須使用原生SCSI命令而非 Windows 驅動程式來探索磁帶程式庫。如需詳細說明，請參閱磁帶館。

若要探索VTL裝置

1. 在 Veeam 軟體中，選擇 磁帶基礎設施。連線磁帶閘道時，虛擬磁帶會列在磁帶基礎設施標籤中。
2. 展開 Tape (磁帶) 樹狀目錄，以查看磁帶機和媒體變更器。
3. 展開媒體變更器樹狀目錄。如果您的磁帶機映射至媒體變更器，則磁帶機會出現在 Drives (磁碟機) 下。否則，磁帶館和磁帶機會顯示為不同的裝置。

   如果未自動映射磁碟機，請遵循 Veeam 網站上的說明來映射磁碟機。

將磁帶匯入至 Veeam

您現在已準備好將磁帶從您的磁帶閘道匯入至 Veeam 備份應用程式庫。

將磁帶匯入至 Veeam 媒體庫

1. 開啟媒體變更器的內容 (按右鍵) 選單，然後選擇 Import (匯入) 以將磁帶匯入至 I/E 插槽。
2. 開啟媒體充電器的內容 (按右鍵) 選單，然後選擇 Inventory Library (清查媒體庫) 以識別無法辨識的磁帶。第一次將新的虛擬磁帶載入至磁帶機時，Veeam 備份應用程式無法辨識該磁帶。為了識別無法辨識的磁帶，您可以清查磁帶館中的磁帶。

在 Veeam 中將資料備份至磁帶

將資料備份至磁帶是包含兩個步驟的程序：

1. 建立媒體集區，並將磁帶新增至媒體集區。
2. 將資料寫入至磁帶。

您會使用與操作實體磁帶相同的程序，來建立媒體集區並將資料寫入虛擬磁帶。如需如何備份資料的詳細資訊，請參閱 Veeam 說明中心內的磁帶入門。

> **Note**
>
> 如果您的磁帶閘道在進行中的備份工作期間因任何原因重新啟動，備份工作將會失敗。若要完成失敗的備份工作，您必須重新提交備份工作。

使用 Veeam 存檔磁帶

當您存檔磁帶時，磁帶閘道會將磁帶從 Veeam 磁帶館移至離線儲存體。您可以從磁帶機退出到儲存插槽，然後使用備份應用程式 (即 Veeam 軟體) 將磁帶從插槽匯出至存檔，來開始磁帶存檔。

將磁帶存檔至 Veeam 媒體庫

1. 選擇磁帶基礎設施，然後選擇包含您要存檔之磁帶的媒體集區。
2. 開啟您要存檔之磁帶的內容 (按右鍵) 選單，然後選擇 Eject Tape (退出磁帶)。
3. 針對 Ejecting tape (退出磁帶)，選擇 Close (關閉)。磁帶的位置會從磁帶機變更為插槽。
4. 重新開啟該磁帶的內容 (按右鍵) 選單，然後選擇 Export (匯出)。磁帶的狀態會從 Tape drive (磁帶機) 變更為 Offline (離線)。
5. 針對 Exporting tape (匯出磁帶)，選擇 Close (關閉)。磁帶的位置會從 Slot (插槽) 變更為 Offline (離線)。
6. 在 Storage Gateway 主控台上，選擇閘道，然後選擇VTL磁帶磁帶磁帶磁帶匣，然後驗證您正在封存的虛擬磁帶狀態。

   存檔程序可能需要一些時間才能完成。磁帶的初始狀態顯示為 IN TRANSIT TO VTS。封存開始時，狀態會變更為 ARCHIVING。封存完成時，磁帶不再列在 中，VTL而是封存在 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 中。

在 Veeam 中從存檔的磁帶還原資料

還原您已存檔資料的程序包含兩個步驟。

從存檔磁帶還原資料

1. 將存檔磁帶從存檔擷取至磁帶閘道。如需說明，請參閱 擷取已存檔的磁帶。
2. 使用 Veeam 軟體還原資料。您可以透過建立一個還原資料夾檔案 (如同您從實體磁帶還原資料時) 以執行此作業。如需說明，請參閱 Veeam 說明中心內的從磁帶還原檔案。

後續步驟

清除不必要的資源

使用 Veritas Backup Exec 測試設定

您可以使用 Veritas Backup Exec 將資料備份至虛擬磁帶、封存磁帶，以及管理虛擬磁帶程式庫（VTL）裝置。在本主題中，您可以找到使用下列 Backup Exec 版本執行備份和還原操作所需的基本文件：

- Veritas Backup Exec 2014
- Veritas Backup Exec 15
- Veritas Backup Exec 16
- Veritas Backup Exec 20.x
- Veritas Backup Exec 22.x

搭配使用這些 Backup Exec 版本與磁帶閘道的程序相同。請參閱 Veritas 支援網站 ，以取得有關如何使用 Backup Exec 的詳細資訊，包括如何使用 Backup Exec 建立安全備份、軟體與硬體相容性清單，以及Backup Exec 的系統管理員指南。

如需所支援備份應用程式的詳細資訊，請參閱磁帶閘道支援的第三方備份應用程式。

主題

- 在 Backup Exec 中設定儲存
- 在 Backup Exec 中匯入磁帶
- 在 Backup Exec 中將資料寫入至磁帶
- 使用 Backup Exec 存檔磁帶

- 在 Backup Exec 中從存檔的磁帶還原資料
- 在 Backup Exec 中停用磁帶硬碟

在 Backup Exec 中設定儲存

將虛擬磁帶程式庫（VTL）裝置連接至 Windows 用戶端後，您可以設定 Backup Exec 儲存體來識別您的裝置。如需有關如何將VTL裝置連線至 Windows 用戶端的資訊，請參閱 連接VTL您的裝置。

設定儲存

1. 啟動 Backup Exec 軟體，然後選擇工具列左上角的黃色圖示。
2. 選擇 Configuration and Settings (組態和設定)，然後選擇 Backup Exec Services (Backup Exec 服務) 以開啟 Backup Exec Service Manager。
3. 選擇 Restart All Services (重新啟動所有服務)。然後， Backup Exec 會識別VTL裝置（即媒體變更器和磁帶機）。重新啟動程序可能需要幾分鐘的時間。

   > **Note**
   >
   > 磁帶閘道提供 10 個磁帶硬碟。不過，Backup Exec 授權合約可能需要備份應用程式使用 10 個以下的磁帶硬碟。在該情況下，您必須停用 Backup Exec 機器庫中的磁帶硬碟，只保持啟用授權合約所允許的磁帶硬碟數目。如需說明，請參閱 在 Backup Exec 中停用磁帶硬碟 。

4. 重新啟動完成之後，請關閉 Backup Exec Service Manager。

在 Backup Exec 中匯入磁帶

您現在已可以將磁帶從閘道匯入至插槽。

1. 選擇儲存索引標籤，然後展開機器人程式庫樹狀結構以顯示VTL裝置。

   > **Important**
   >
   > Veritas Backup Exec 軟體需要磁帶閘道媒體變更器類型。如果 機器庫 下方所列的媒體變更器類型不是磁帶閘道，則您必須先變更它，再設定備份應用程式中的儲存。如需如何選取不同媒體變更器類型的資訊，請參閱在啟用閘道後選取媒體變更器。

2. 選擇 Slots (插槽) 圖示以顯示所有插槽。

> **Note**
>
> 當您將磁帶匯入至機器庫時，會將磁帶存放至插槽，而非磁帶硬碟。因此，磁帶硬碟可能會有訊息，指出硬碟中沒有媒體 (無媒體)。當您初始化備份或還原任務時，會將磁帶移至磁帶硬碟。
>
> 您必須要有閘道磁帶館中可用的磁帶，以將磁帶匯入至儲存插槽。如需如何建立磁帶的說明，請參閱為磁帶閘道建立新的虛擬磁帶。

3. 開啟空插槽的內容 (按右鍵) 選單，並選擇 Import (匯入)，然後選擇 Import media now (立即匯入媒體)。您可以使用單一匯入操作選取多個插槽並匯入多個磁帶。
4. 在出現的 Media Request (媒體請求) 視窗中，選擇 View details (檢視詳細資訊)。
5. 在 Action Alert: Media Intervention (動作提醒：媒體介入) 視窗中，選擇 Respond OK (回應正常) 以將媒體插入至插槽。

   磁帶會出現在您選取的插槽中。

> **Note**
>
> 所匯入的磁帶包含空的磁帶以及已從存檔擷取至閘道的磁帶。

在 Backup Exec 中將資料寫入至磁帶

您可以使用與您在操作實體磁帶時相同的程序和備份政策，將資料寫入磁帶閘道虛擬磁帶。如需詳細資訊，請參閱 Backup Exec 軟體之文件小節中的 Backup Exec 管理指南。

> **Note**
>
> 如果磁帶閘道在進行中的備份工作期間因任何原因重新啟動，備份工作可能會失敗。如果備份工作失敗，Veritas Backup Exec 中的磁帶狀態會變更為無法附加。您可以封存磁帶或繼續讀取磁帶中的資料。若要完成失敗的備份工作，您必須在新磁帶上重新提交備份工作。

使用 Backup Exec 存檔磁帶

當您封存磁帶時，磁帶閘道會將磁帶從閘道的虛擬磁帶程式庫 （VTL） 移至離線儲存。您可以使用 Backup Exec 軟體匯出磁帶，以開始磁帶存檔。

存檔磁帶

1. 選擇 Storage (儲存) 選單，並選擇 Slots (插槽)，再開啟您要從中匯出磁帶之插槽的內容 (按右鍵) 選單，選擇 Export media (匯出媒體)，然後選擇 Export media now (立即匯出媒體)。您可以使用單一匯出操作選取多個插槽並匯出多個磁帶。
2. 在 Media Request (媒體請求) 彈出式視窗中，選擇 View details (檢視詳細資訊)，然後選擇 Alert: Media Intervention (提醒：媒體介入) 視窗中的 Respond OK (回應正常)。

   在 Storage Gateway 主控台中，您可以確認所存檔磁帶的狀態。這可能需要一些時間，才能完成將資料上傳至 AWS。在此期間，匯出的磁帶會列在磁帶閘道中VTL，狀態為 IN TRANSIT TO VTS。當上傳完成且封存程序開始時，狀態會變更為 ARCHIVING。資料封存完成時，匯出的磁帶不再列在 中，VTL而是封存在 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 中。
3. 選擇您的閘道，然後選擇VTL磁帶磁帶磁帶匣，並確認虛擬磁帶不再列在您的閘道中。
4. 在 Storage Gateway 主控台的導覽窗格上，選擇磁帶。確認您的磁帶狀態為 ARCHIVED。

在 Backup Exec 中從存檔的磁帶還原資料

還原您已存檔資料的程序包含兩個步驟。

從存檔磁帶還原資料

1. 將存檔磁帶擷取至磁帶閘道。如需說明，請參閱 擷取已存檔的磁帶。
2. 使用 Backup Exec 還原資料。此程序與從實體磁帶還原資料相同。如需說明，請參閱 Backup Exec 軟體之文件小節中的 Backup Exec 管理指南。

在 Backup Exec 中停用磁帶硬碟

磁帶閘道提供 10 個磁帶硬碟，但您可能決定使用較少的磁帶硬碟。在該情況下，您可以停用未使用的磁帶硬碟。

1. 開啟 Backup Exec，然後選擇 儲存 標籤。
2. 在機器庫樹狀目錄中，開啟您要停用之磁帶硬碟的內容 (按右鍵) 選單，然後選擇停用。

後續步驟

清除不必要的資源

使用 Veritas 測試您的設定 NetBackup

您可以使用 Veritas 將資料備份到虛擬磁帶、封存磁帶，以及管理您的虛擬磁帶程式庫 （VTL） 裝置 NetBackup。在本主題中，您可以找到有關如何設定磁帶閘道 NetBackup 應用程式，以及執行備份和還原操作的基本文件。若要這麼做，您可以使用下列版本的 NetBackup：

- Veritas NetBackup 7.x
- Veritas NetBackup 8.x

搭配使用這些 Backup Exec 版本與磁帶閘道的程序相同。如需如何使用 的詳細資訊 NetBackup，請參閱 Veritas 網站上的 Veritas 服務和操作就緒工具 （SORT）。如需 Veritas 硬體相容性的支援資訊，請參閱 Veritas 網站上的 NetBackup 7.0 - 7.6.x 硬體相容性清單、NetBackup 8.0 - 8.1.x 硬體相容性清單 或 NetBackup 8.2 - 8.x.x 硬體相容性清單。

如需相容備份應用程式的詳細資訊，請參閱 磁帶閘道支援的第三方備份應用程式。

主題

設定 NetBackup 儲存裝置

將虛擬磁帶程式庫 （VTL） 裝置連接至 Windows 用戶端後，您可以設定 Veritas NetBackup 儲存體來識別您的裝置。如需有關如何將VTL裝置連線至 Windows 用戶端的資訊，請參閱 連接VTL您的裝置。

若要設定 NetBackup 以在磁帶閘道上使用儲存裝置

1. 以管理員身分開啟 NetBackup 管理主控台。
2. 選擇 Configure Storage Devices (設定儲存裝置) 以開啟 Device Configuration (裝置組態) 精靈。
3. 選擇 Next (下一步)。 NetBackup 應用程式會將您的電腦偵測為裝置主機。
4. 在 Device Hosts (裝置主機) 欄中，選取您的電腦，然後選擇 Next (下一步)。 NetBackup 應用程式會掃描您的電腦尋找裝置，並探索所有裝置。
5. 在 Scanning Hosts (掃描主機) 頁面中，選擇 Next (下一步)，然後選擇 Next (下一步)。 NetBackup 應用程式會在電腦上找到所有 10 個磁帶機和媒體更換器。

6. 在 Backup Devices (備份裝置) 視窗中，選擇 Next (下一步)。
7. 在 Drag and Drop Configuration (拖放組態) 視窗中，確認已選取您的媒體變更器，然後選擇 Next (下一步)。
8. 在出現的對話方塊中，選擇 Yes (是) 儲存您電腦上的組態。 NetBackup 應用程式會更新裝置組態。
9. 更新完成時，請選擇下一步，讓裝置可供 NetBackup 應用程式使用。
10. 在 Finished! (已完成！) 視窗中，選擇 Finish (完成)。

在 NetBackup 應用程式中驗證您的裝置

1. 在 NetBackup 管理主控台中，展開媒體和裝置管理節點，然後展開裝置節點。選擇 Drives (磁碟機) 顯示所有磁帶機。
2. 在 Devices (裝置) 節點中，選擇 Robots (機器人) 顯示所有媒體變更器。在 NetBackup 應用程式中，媒體變更器稱為機器人 。
3. 在所有機器人窗格中，開啟 （ TLD0 ） （ 即您的機器人 ） 的內容 （ 按一下滑鼠右鍵 ） 選單，然後選擇庫存機器人 。
4. 在 Robot Inventory (機器人清查) 視窗中，確認從 Select robot (選取機器人) 類別的 Device-Host (裝置-主機) 清單選取您的主機。
5. 確認已從 Robot (機器人) 清單選取您的機器人。
6. 在 Robot Inventory (機器人清查) 視窗中，選取 Update volume configuration (更新磁碟區組態)、Preview changes (預覽變更)、Empty media access port prior to update (先清空媒體存取連接埠，再更新)，然後選擇 Start (開始)。

   程序接著會在 NetBackup Enterprise Media Management （ EMM ） 資料庫中清查媒體變更器和虛擬磁帶。 會將媒體資訊、裝置組態和磁帶狀態 NetBackup 儲存在 中EMM。
7. 在 Robot Inventory (機器人清查) 視窗中，於在清查完成之後選擇 Yes (是)。在這裡選擇 Yes (是) 會更新組態，以及將匯入/匯出插槽中找到的虛擬磁帶移至虛擬磁帶館。
8. 關閉 Robot Inventory (機器人清查) 視窗。
9. 在媒體節點中，展開機器人節點，然後選擇 TLD （ 0 ） 以顯示機器人可用的所有虛擬磁帶 （ 中繼換片機 ）。

> **Note**
>
> 如果您先前已將其他裝置連接至 NetBackup應用程式，則可能有多個機器人。請確定您選取正確的機器人。

既然您已連線裝置並讓它們可供備份應用程式使用，就已經準備好測試閘道。若要測試您的閘道，請將資料備份至您建立的虛擬磁帶，並存檔磁帶。

將資料備份至磁帶

您可以將資料備份至虛擬磁帶，以測試磁帶閘道設定。

> **Note**
>
> - 在本入門練習中，您應該只備份少量資料，因為有許多與存放、存檔和擷取資料相關的成本。如需定價的詳細資訊，請參閱詳細資訊頁面的定價。
> - 如果您的磁帶閘道在進行中的備份工作期間因任何原因重新啟動，備份工作將會暫停。閘道完成重新啟動後，暫停的備份工作將自動繼續。

建立磁碟區集區

磁碟區集區是用於備份的虛擬磁帶集合。

1. 啟動 NetBackup 管理主控台。
2. 展開 Media (媒體) 節點，並開啟 Volume Pool (磁碟區集區) 的內容 (按右鍵) 選單，然後選擇 New (新建)。New Volume Pool (新增磁碟區集區) 對話方塊隨即顯示。
3. 針對 Name (名稱)，輸入您磁碟區集區的名稱。
4. 針對 Description (描述)，輸入磁碟區集區的描述，然後選擇 OK (確定)。您剛建立的磁碟區集區會新增至磁碟區集區清單。

   下列螢幕擷取畫面顯示磁碟區集區的清單。

將虛擬磁帶新增至磁碟區集區

1. 展開機器人節點，然後選擇 TLD（0）機器人以顯示此機器人已知的虛擬磁帶。

   如果您之前已連線機器人，則磁帶閘道機器人的名稱可能會不同。
2. 從虛擬磁帶清單，開啟您要新增至磁碟區集區之磁帶的內容 (按右鍵) 選單，然後選擇 Change (變更) 以開啟 Change Volumes (變更磁碟區) 對話方塊。
3. 針對 Volume Pool (磁碟區集區)，選擇 New pool (新增集區)。
4. 針對 New pool (新增集區)，選取您剛建立的集區，然後選擇 OK (確定)。

   您可以展開 Media (媒體) 節點，並選擇磁碟區集區，確認磁碟區集區包含您剛新增的虛擬磁帶。

建立備份政策

備份政策指定要備份的資料、備份的時間，以及要使用的磁碟區集區。

1. 選擇主伺服器以返回 Veritas NetBackup 主控台。
2. 選擇 Create a Policy (建立政策) 以開啟 Policy Configuration Wizard (政策組態精靈) 視窗。
3. 選取 File systems, databases, applications (檔案系統、資料庫、應用程式)，然後選擇 Next (下一步)。
4. 針對 Policy Name (政策名稱)，輸入您政策的名稱，並確認已從 Select the policy type (選取政策類型) 清單選取 MS-Windows，然後選擇 Next (下一步)。
5. 在 Client List (用戶端清單) 視窗中，選擇 Add (新增)，並在 Name (名稱) 欄中輸入您電腦的主機名稱，然後選擇 Next (下一步)。此步驟會將您要定義的政策套用至 `localhost` (您的用戶端電腦)。
6. 在 Files (檔案) 視窗中，選擇 Add (新增)，然後選擇資料夾圖示。
7. 在 Browse (瀏覽) 視窗中，瀏覽至您要備份的資料夾或檔案，並選擇 OK (確定)，然後選擇 Next (下一步)。
8. 在 Backup Types (備份類型) 視窗中，接受預設值，然後選擇 Next (下一步)。

   > **Note**
   >
   > 如果您要自行初始化備份，請選取 User Backup (使用者備份)。

9. 在 Frequency and Retention (頻率和保留) 視窗中，選取您要套用至備份的頻率和保留政策。在此練習中，您可以接受所有預設值，然後選擇下一步。

10. 在 Start (開始) 視窗中，選取 Off hours (下班時間)，然後選擇 Next (下一步)。此選擇指定只應該在下班時間備份資料夾。
11. 在 Policy Configuration (政策組態) 精靈中，選擇 Finish (完成)。

政策會根據排程來執行備份。您也可以隨時執行手動備份，這是在下一個步驟中執行。

執行手動備份

1. 在 NetBackup 主控台的導覽窗格中，展開NetBackup 管理節點。
2. 展開 Policies (政策) 節點。
3. 開啟政策的內容 (按右鍵) 選單，然後選擇 Manual Backup (手動備份)。
4. 在 Manual Backup (手動備份) 視窗中，選取排程，並選取用戶端，然後選擇 OK (確定)。
5. 在出現的 Manual Backup Started (已開始手動備份) 對話方塊中，選擇 OK (確定)。
6. 在導覽窗格上，選擇 Activity Monitor (活動監控)，以在 Job ID (任務 ID) 欄中檢視您備份的狀態。

若要尋找在備份期間 NetBackup 寫入檔案資料的虛擬磁帶條碼，請參閱下列程序所述的任務詳細資訊視窗。在存檔磁帶之下節的程序中，您需要此條碼。

尋找磁帶的條碼

1. 在 Activity Monitor (活動監控) 中，於 Job ID (任務 ID) 欄中開啟備份任務識別符的內容 (按右鍵) 選單，然後選擇 Details (詳細資訊)。
2. 在 Job Details (任務詳細資訊) 視窗中，選擇 Detailed Status (詳細狀態) 標籤。
3. 在 Status (狀態) 方塊中，找到媒體 ID。例如，狀態報告中的項目可能會讀取 `media id 87A222`。此 ID 可協助您判斷您已寫入資料的磁帶。

您現在已成功部署磁帶閘道、建立虛擬磁帶，以及備份資料。您接著可以存檔虛擬磁帶，以及從存檔擷取虛擬磁帶。

存檔磁帶

當您封存磁帶時，磁帶閘道會將磁帶從閘道的虛擬磁帶程式庫 （VTL） 移至提供離線儲存的封存。您可以使用備份應用程式來退出磁帶，以初始化磁帶存檔。

存檔虛擬磁帶

1. 在 NetBackup 管理主控台中，展開媒體和裝置管理節點，然後展開媒體節點。

2. 展開機器人並選擇 TLD（0）。
3. 開啟您要存檔之虛擬磁帶的內容 (按右鍵) 選單，然後選擇 Eject Volume From Robot (從機器人退出磁碟區)。
4. 在 Eject Volumes (退出磁碟區) 視窗中，確定 Media ID (媒體 ID) 符合您要退出的虛擬磁帶，然後選擇 Eject (退出)。
5. 在對話方塊中，選擇 Yes (是)。

   退出程序完成後，Eject Volumes (退出磁碟區) 對話方塊的磁帶狀態指出退出已成功。
6. 選擇 Close (關閉) 以關閉 Eject Volumes (退出磁碟區) 視窗。
7. 在 Storage Gateway 主控台中，驗證您要在閘道的 中封存的磁帶狀態VTL。這可能需要一些時間才能將資料上傳至 AWS。在此期間，退出的磁帶會列在閘道的 中VTL，狀態為 IN TRANSIT TO VTS。封存開始時，狀態為 ARCHIVING。資料上傳完成後，彈出的磁帶將不再列在 中，VTL而是封存在 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 中。
8. 若要確認虛擬磁帶不再列在您的閘道中，請選擇閘道，然後選擇VTL磁帶磁帶磁帶匣 。
9. 在 Storage Gateway 主控台的導覽窗格上，選擇磁帶。確認封存磁帶的狀態為 ARCHIVED。

從磁帶還原資料

還原您已存檔資料的程序包含兩個步驟。

從存檔磁帶還原資料

1. 將存檔磁帶擷取至磁帶閘道。如需說明，請參閱 擷取已存檔的磁帶。
2. 使用與 Veritas NetBackup 應用程式一起安裝的 Backup、 Archive 和 Restore 軟體。此程序與從實體磁帶還原資料相同。如需指示，請參閱 Veritas 網站上的 Veritas 服務和操作就緒工具（SORT）。

後續步驟

清除不必要的資源

接下來做些什麼？

在您的磁帶閘道進入生產環境之後，您可以執行幾項維護任務，例如：新增和移除磁帶、監控及最佳化閘道效能，以及疑難排解。如需這些管理任務的一般資訊，請參閱管理您的磁帶閘道。

您可以在 上執行一些磁帶閘道維護任務 AWS Management Console，例如設定閘道的頻寬速率限制和管理閘道軟體更新。若您的磁帶閘道是在內部部署，您可以在閘道的本機主控台上執行一些維護任務。這包含將您的磁帶閘道透過代理路由，以及設定您的閘道使用靜態 IP 地址。如果您以 Amazon EC2執行個體執行閘道，您可以在 Amazon EC2主控台上執行特定維護任務，例如新增和移除 Amazon EBS 磁碟區。如需維護您磁帶閘道的詳細資訊，請參閱管理您的磁帶閘道。

若您計劃將您的閘道部署於生產環境，建議您在決定磁碟大小時將實際工作負載納入考量。如需如何判斷實際磁碟大小的資訊，請參閱管理 Storage Gateway 的本機磁碟。此外，若您不打算繼續使用磁帶閘道，請考慮加以清理。清理有助於避免產生費用。如需清理的資訊，請參閱清除不必要的資源。

在 VPC 中啟用閘道

您可以在內部部署閘道裝置以及雲端儲存基礎設施之間建立私有連線。您可以使用此連線來啟動閘道，並允許其將資料傳輸至 AWS 儲存服務，而無需透過公用網際網路進行通訊。使用 Amazon VPC 服務，您可以在自訂虛擬私有雲 (VPC) 中啟動 AWS 資源，包括私有網路界面端點。A 可VPC讓您控制網路設定，例如 IP 位址範圍、子網路、路由表和網路閘道。如需詳細資訊VPCs，請參閱什麼是AmazonVPC？ 在 Amazon 用VPC戶指南。

若要在中啟用閘道VPC，請使用 Amazon VPC 主控台為 Storage Gateway 建立VPC端點並取得VPC端點 ID，然後在建立和啟用閘道時指定此VPC端點 ID。如需詳細資訊，請參閱 Connect 磁帶閘道以AWS。

> **Note**
>
> 您必須在為 Storage Gateway 建立VPC端點的相同區域啟動閘道

主題

- 建立 Storage Gateway 的VPC端點

建立 Storage Gateway 的VPC端點

請依照下列指示建立VPC端點。如果您已經有 Storage Gateway 的VPC端點，您可以使用它來啟動閘道。

建立 Storage Gateway 的VPC端點

1. 登錄 AWS Management Console 並在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇端點，然後選擇建立端點。
3. 在建立端點頁面上，針對服務類別選擇 AWS 服務。
4. 在 Service Name (服務名稱) 中，選擇 `com.amazonaws.region.storagegateway`。例如 `com.amazonaws.us-east-2.storagegateway`。
5. 對於 VPC，請選擇您的VPC並記下其可用區域和子網路。
6. 確認未選取 「啟用私人DNS名稱」。
7. 在「安全性」群組中，選擇您要用於您的安全性群組VPC。您可以接受預設的安全群組。確認您的安全性群組允許下列所有TCP連接埠：

   - TCP443
   - TCP1026
   - TCP1027
   - TCP1028
   - TCP1031
   - TCP2222
8. 選擇建立端點。端點的最初狀態是 pending (擱置中)。建立端點時，請記下您剛建立之VPC端點的ID。
9. 建立端點後，選擇「端點」，然後選擇新VPC端點。
10. 在所選儲存區閘道端點的 [詳細資料] 索引標籤的 [DNS名DNS稱] 下，使用未指定可用區域的名字。你的DNS名字看起來像這樣：`vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

現在您已經有了VPC端點，就可以建立閘道了。如需詳細資訊，請參閱建立閘道。

管理您的磁帶閘道

管理閘道包括設定快取儲存體和上傳緩衝區空間、使用虛擬磁帶，以及執行一般維護等任務。若您尚未建立閘道，請參閱入門 AWS Storage Gateway。

接下來，您可以找到如何管理磁帶閘道資源的相關資訊。

主題

- 編輯基本閘道資訊 - 了解如何使用 Storage Gateway 主控台編輯現有閘道的基本資訊，包括閘道名稱、時區和 CloudWatch 日誌群組。
- 管理自動磁帶建立 - 了解如何設定磁帶閘道自動建立新的虛擬磁帶，以維持您指定的可用磁帶數量下限。
- 存檔虛擬磁帶 - 了解如何在建立新磁帶時，將磁帶封存設定為 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 儲存類別。
- 將磁帶移至 S3 Glacier Deep Archive 儲存類別 - 了解如何將磁帶從 S3 Glacier Flexible Retrieval 移至 S3 Glacier Deep Archive，以極低的成本進行長期資料保留和數位保存。
- 擷取已存檔的磁帶 - 了解如何先將磁帶擷取至磁帶閘道，以存取儲存在封存虛擬磁帶上的資料。
- 檢視磁帶用量統計資料 - 了解如何使用 Storage Gateway 主控台檢視儲存在磁帶上的資料量。
- 從磁帶閘道刪除虛擬磁帶 - 了解如何使用 Storage Gateway 主控台從磁帶閘道刪除虛擬磁帶。
- 刪除自訂磁帶集區 - 了解如何使用 Storage Gateway 主控台刪除自訂磁帶集區。
- 停用磁帶閘道 - 了解如何在閘道失敗，且您想要將磁帶從失敗的閘道復原至另一個閘道時停用磁帶閘道。
- 了解磁帶狀態 - 了解 Storage Gateway 報告的各種磁帶狀態值，以協助判斷磁帶是否正常運作，或是否有可能需要您採取行動的問題。
- 將資料移至新閘道 - 了解如何在資料和效能需求增加時，或在您收到遷移閘道的 AWS 通知時，在閘道之間移動資料。

編輯基本閘道資訊

您可以使用 Storage Gateway 主控台來編輯現有閘道的基本資訊，包括閘道名稱、時區和 CloudWatch 日誌群組。

編輯現有閘道的基本資訊

1. 開啟位於首頁 的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/
2. 選擇閘道，然後選擇您要編輯基本資訊的閘道。
3. 從動作下拉式功能表中選擇編輯閘道資訊。
4. 為 Gateway name (閘道名稱) 輸入閘道的名稱。您可以搜尋此名稱，在 Storage Gateway 主控台的清單頁面上尋找閘道。

   > **Note**
   >
   > 閘道名稱必須介於 2 到 255 個字元之間，且不能包含斜線 （ \ 或 / ）。
   > 變更閘道的名稱將中斷任何設定以監控閘道的 CloudWatch 警示。若要重新連接警示，GatewayName請更新 CloudWatch 主控台中每個警示的 。

5. 針對閘道時區，請選擇您要部署閘道的全球當地時區。
6. 針對選擇如何設定日誌群組 ，選擇如何設定 Amazon CloudWatch Logs 來監控閘道的運作狀態。您可以從下列選項來選擇：

   - 建立新的日誌群組 – 設定新的日誌群組以監控您的閘道。
   - 使用現有日誌群組 – 從對應的下拉式清單中選擇現有日誌群組。
   - 停用記錄 – 請勿使用 Amazon CloudWatch Logs 監控您的閘道。

7. 當您完成修改要變更的設定時，請選擇儲存變更 。

管理自動磁帶建立

磁帶閘道會自動建立新的虛擬磁帶，以維持您設定的可用磁帶數目下限。然後，這些新磁帶可供備份應用程式進行匯入，讓您執行備份任務時無須中斷。自動磁帶建立除了不再需要手動建立新的虛擬磁帶，更免去對自訂程式碼編寫的需求。

刪除自動磁帶建立政策

1. 開啟位於首頁 的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/
2. 在導覽窗格中，選擇 Gateways (閘道) 標籤。
3. 選擇您要管理自動磁帶建立的閘道。
4. 在 Actions (動作) 選單，選擇 Configure tape auto-create (設定磁帶自動建立)。
5. 若要刪除閘道上的自動磁帶建立政策，請在您要刪除的政策右方選擇移除。

若要停止閘道上的自動磁帶建立，請刪除該閘道所有自動磁帶建立政策。

選擇儲存變更，確認刪除所選磁帶閘道的磁帶自動建立政策。

> **Note**
>
> 閘道刪除磁帶自動建立政策後無法復原。

變更磁帶閘道的自動磁帶建立原則

1. 開啟位於首頁 的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/
2. 在導覽窗格中，選擇 Gateways (閘道) 標籤。
3. 選擇您要管理自動磁帶建立的閘道。
4. 在動作功能表中，選擇設定磁帶自動建立，然後在顯示的頁面上變更設定。
5. 針對磁帶數目下限，請輸入磁帶閘道隨時應有的可用虛擬磁帶最低數量。此值有效範圍最小為 1，最大為 10。
6. 針對 Capacity (容量)，輸入虛擬磁帶容量的大小 (位元組)。此值有效範圍最小為 100 GiB，最大為 15 TiB。
7. 針對 Barcode prefix (條碼字首)，輸入您要加到虛擬磁帶條碼前面的字首。

> **Note**
>
> 虛擬磁帶都有獨特可辨識的條碼，您可為條碼新增字首。字首是選用性的，但您可以使用它來協助識別虛擬磁帶。字首必須為大寫字母 (A–Z)，而且長度必須為一到四個字元。

8. 對於 Pool (集區)，選擇 Glacier Pool (Glacier 集區) 或 Deep Archive Pool (Deep Archive 集區)。此集區代表備份軟體退出您的磁帶時，您的磁帶存放之處的儲存體方案。

   - 如果您想要將磁帶存檔在 S3 Glacier Flexible Retrieval 儲存類別中，請選擇 Glacier 集區。當您的備份軟體退出磁帶，將會自動存檔在 S3 Glacier Flexible Retrieval 中。您可以將 S3 Glacier Flexible Retrieval 用於多個作用中存檔，在其中，您通常可以於 3 到 5 小時內擷取磁帶。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的存檔物件的儲存類別。
   - 如果您想要將磁帶存檔在 S3 Glacier Deep Archive 中，請選擇 Deep Archive 集區。當您的備份軟體退出磁帶時，磁帶會自動存檔在 S3 Glacier Deep Archive 中。您可以將 S3 Glacier Deep Archive 用於長期資料保留和數位保存，其中的資料一年存取一次或兩次。您通常可以

在 12 小時內擷取 S3 Glacier Deep Archive 中的磁帶存檔。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的存檔物件的儲存類別。

如果您將磁帶存檔在 S3 Glacier Flexible Retrieval 中，您可以稍後將其移到 S3 Glacier Deep Archive。如需詳細資訊，請參閱將磁帶移至 S3 Glacier Deep Archive 儲存類別。

9. 您可以在磁帶概觀頁面上找到磁帶的相關資訊。根據預設，此清單一次最多可顯示 1,000 個磁帶，但您執行的搜尋會套用至所有磁帶。您可以使用搜尋列尋找符合特定準則的磁帶，或將清單減少到 1,000 個以下的磁帶。當您的清單包含 1,000 個或更少的磁帶時，您可以依各種屬性，以遞增或遞減順序來排序磁帶。

   建立磁帶CREATING時，可用虛擬磁帶的狀態一開始會設為 。建立磁帶後，其狀態會變更為AVAILABLE。如需詳細資訊，請參閱了解磁帶狀態。

   如需啟用自動磁帶建立的詳細資訊，請參閱自動磁帶建立。

存檔虛擬磁帶

您可以將磁帶封存至 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive。建立磁帶時，您可以選擇您希望用於存檔磁帶的存檔集區。

如果您想要將磁帶存檔在 S3 Glacier Flexible Retrieval 中，請選擇 Glacier 集區。當您的備份軟體退出磁帶時，它會自動存檔在 S3 Glacier Flexible Retrieval 中。對於會定期擷取資料並在幾分鐘內便需要資料的多個作用中存檔，您可以使用 S3 Glacier Flexible Retrieval。如需詳細資訊，請參閱存檔物件的儲存類別。

如果您想要將磁帶存檔在 S3 Glacier Deep Archive 中，請選擇 Deep Archive 集區。當您的備份軟體退出磁帶時，磁帶會自動存檔在 S3 Glacier Deep Archive 中。您可以用非常低的成本將 S3 Glacier Deep Archive 用於長期資料保留和數位保存。S3 Glacier Deep Archive中的資料不會經常擷取或很少擷取。如需詳細資訊，請參閱存檔物件的儲存體方案。

> **Note**
>
> 在 2019 年 3 月 27 日之前建立的任何磁帶，會於您的備份軟體將它退出時，直接存檔在 S3 Glacier Flexible Retrieval 中。

於您的備份軟體將磁帶退出時，會將它自動存檔在建立磁帶時選擇的集區。退出磁帶的程序因您的備份軟體而有所不同。某些備份軟體會要求您在退出磁帶後將其匯出，然後才能開始進行封存。如需詳細資訊，請參閱使用您的備份軟體來測試您的閘道設定。

將磁帶移至 S3 Glacier Deep Archive 儲存類別

將磁帶從 S3 Glacier Flexible Retrieval 移到 S3 Glacier Deep Archive，可以極低成本獲得長期資料保留和數位保存。您可以將 S3 Glacier Deep Archive 用於長期資料保留和數位保存，其中的資料一年存取一次或兩次。如需詳細資訊，請參閱存檔物件的儲存體方案。

將磁帶從 S3 Glacier Flexible Retrieval 遷移至 S3 Glacier Deep Archive

1. 在導覽窗格中選擇磁帶館 > 磁帶標籤以查看您的磁帶。根據預設，此清單一次最多可顯示 1,000 個磁帶，但您執行的搜尋會套用至所有磁帶。您可以使用搜尋列尋找符合特定準則的磁帶，或將清單減少到 1,000 個以下的磁帶。當您的清單包含 1,000 個或更少的磁帶時，您可以依各種屬性，以遞增或遞減順序來排序磁帶。
2. 請選取您要遷移至 S3 Glacier Deep Archive 的磁帶的核取方塊。您可以在集區欄查看每個磁帶相關聯的集區。
3. 選擇指派給集區。
4. 在指派磁帶到集區對話方塊中，驗證您要移動的磁帶條碼，然後選擇指派。

   > **Note**
   >
   > 如果磁帶已被備份應用程式退出並存檔在 S3 Glacier Deep Archive 中，您無法將它移回至 S3 Glacier Flexible Retrieval。將磁帶從 S3 Glacier Flexible Retrieval 遷移至 S3 Glacier Deep Archive 需收取費用。此外，如果您在 90 天之前將磁帶從 S3 Glacier Flexible Retrieval 遷移至 S3 Glacier Deep Archive，須收取 S3 Glacier Flexible Retrieval 的提早刪除費。

5. 移動磁帶之後，您可以在磁帶總覽頁面的集區欄中看到更新的狀態。

擷取已存檔的磁帶

若要存取存放在已存檔虛擬磁帶上的資料，您必須先將您要的磁帶擷取至您的磁帶閘道。您的磁帶閘道為每個閘道提供一個虛擬磁帶程式庫（VTL）。

如果您在 中有多個磁帶閘道 AWS 區域，則只能將磁帶擷取至一個閘道。

擷取的磁帶具有防寫保護。您只能讀取磁帶上的資料。

> **Important**
>
> 若您在 S3 Glacier Flexible Retrieval 中存檔磁帶，您通常可以在 3 到 5 小時內擷取磁帶。如果您在 S3 Glacier Deep Archive 中存檔磁帶，通常可以在 12 小時內擷取它。

> **Note**
>
> 從存檔擷取磁帶必須支付費用。如需定價的詳細資訊，請參閱 Storage Gateway 定價。

將已存檔磁帶擷取至您的閘道

1. 開啟位於首頁 的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/
2. 在導覽窗格中選擇磁帶館 > 磁帶標籤以查看您的磁帶。根據預設，此清單一次最多可顯示 1,000 個磁帶，但您執行的搜尋會套用至所有磁帶。您可以使用搜尋列尋找符合特定準則的磁帶，或將清單減少到 1,000 個以下的磁帶。當您的清單包含 1,000 個或更少的磁帶時，您可以依各種屬性，以遞增或遞減順序來排序磁帶。
3. 從虛擬磁帶架標籤選擇要擷取的虛擬磁帶，然後選擇擷取磁帶。

   > **Note**
   >
   > 您要擷取的虛擬磁帶狀態必須為 ARCHIVED。

4. 在 Retrieve tape (擷取磁帶) 對話方塊中，針對 Barcode (條碼)，請確認條碼可識別您希望擷取的虛擬磁帶。
5. 針對 Gateway (閘道)，請選擇您要擷取已存檔磁帶的目標閘道，然後選擇 Retrieve tape (擷取磁帶)。

磁帶的狀態會從 變更為 ARCHIVED RETRIEVING。此時，您的資料會從虛擬磁帶櫃 (後端為 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive) 遷移至虛擬磁帶媒體櫃 (後端為 Amazon S3)。移動所有資料後，封存中虛擬磁帶的狀態會變更為 RETRIEVED。

> **Note**
>
> 擷取的虛擬磁帶為唯讀。

檢視磁帶用量統計資料

當您將資料寫入磁帶時，您可以在 Storage Gateway 主控台中檢視存放在磁帶上的資料量。每個磁帶的 Details (詳細資訊) 標籤會顯示磁帶的用量資訊。

檢視存放在磁帶上的資料量

1. 開啟位於首頁 的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/
2. 在導覽窗格中選擇磁帶館 > 磁帶標籤以查看您的磁帶。根據預設，此清單一次最多可顯示 1,000 個磁帶，但您執行的搜尋會套用至所有磁帶。您可以使用搜尋列尋找符合特定準則的磁帶，或將清單減少到 1,000 個以下的磁帶。當您的清單包含 1,000 個或更少的磁帶時，您可以依各種屬性，以遞增或遞減順序來排序磁帶。
3. 選擇您感興趣的磁帶。
4. 隨即顯示的頁面提供關於磁帶的各種詳細資訊和資訊，包括下列各項：

   - Size: (大小：) 選取之磁帶的總容量。
   - Used: (已使用：) 由您的備份應用程式寫入磁帶的資料大小。

   > **Note**
   >
   > 這個值不可用於在 2015 年 5 月 13 日之前建立的磁帶。

從磁帶閘道刪除虛擬磁帶

您可以使用 Storage Gateway 主控台，從您的磁帶閘道刪除虛擬磁帶。

> **Note**
>
> 如果您要從磁帶閘道中刪除的磁帶狀態為 RETRIEVED，您必須先使用備份應用程式退出磁帶，然後再刪除磁帶。如需如何使用 Symantec NetBackup 軟體退出磁帶的說明，請參閱封存磁帶 。磁帶退出後，磁帶狀態會變回 ARCHIVED。然後，您便可以刪除磁帶。

請在您刪除磁帶之前複製您的資料。在您刪除磁帶之後，便無法復原。

刪除虛擬磁帶

> **Warning**
>
> 此程序會永久刪除選取的虛擬磁帶。

1. 開啟位於首頁 的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/
2. 在導覽窗格中選擇磁帶館 > 磁帶標籤以查看您的磁帶。根據預設，此清單一次最多可顯示 1,000 個磁帶，但您執行的搜尋會套用至所有磁帶。您可以使用搜尋列尋找符合特定準則的磁帶，或將清單減少到 1,000 個以下的磁帶。當您的清單包含 1,000 個或更少的磁帶時，您可以依各種屬性，以遞增或遞減順序來排序磁帶。
3. 選取一個或多個要刪除的磁帶。
4. 針對動作，選擇刪除磁帶。出現確認對話方塊。
5. 確認您要刪除指定的磁帶，然後在確認方塊中輸入刪除一詞，然後選擇刪除。

在刪除磁帶之後，磁帶便會從磁帶閘道中消失。

刪除自訂磁帶集區

下列程序說明如何使用 Storage Gateway 主控台刪除自訂磁帶集區。若要使用 以程式設計方式執行此動作API，請參閱 Storage Gateway 參考 DeleteTapePool中的 。 Storage Gateway API

只有在集區中沒有封存的磁帶，且集區沒有附加自動磁帶建立政策時，才能刪除自訂磁帶集區。如果您需要從磁帶集區刪除自動磁帶建立政策，請參閱管理自動磁帶建立。

使用 Storage Gateway 主控台刪除自訂磁帶集區

1. 開啟位於首頁 的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/
2. 在導覽窗格中選擇集區以查看可用的集區。
3. 選取要刪除的一個或多個磁帶集區。

   如果您要刪除之磁帶集區的磁帶計數為 0，而且沒有參照自訂磁帶集區的自動磁帶建立政策，您可以刪除集區。
4. 選擇 刪除 。出現確認對話方塊。

5. 確認您要刪除指定的磁帶集區，然後在確認方塊中輸入刪除一詞，然後選擇刪除。

> **Warning**
>
> 此程序會永久刪除選取的磁帶集區且無法復原。

刪除磁帶集區之後，它們會從磁帶館中消失。

停用磁帶閘道

您可以在磁帶閘道失敗，並且您希望將磁帶從失敗的閘道復原至另一個閘道時停用磁帶閘道。

若要復原磁帶，您必須先停用失敗的閘道。停用磁帶閘道會鎖定該閘道中的虛擬磁帶。這表示任何可能在停用閘道之後寫入這些磁帶的資料都不會傳送到 AWS。您只能在閘道不再連線到 AWS時，於 Storage Gateway 主控台上停用閘道。如果閘道已連線至 AWS，則您無法停用磁帶閘道。

您會停用磁帶閘道，做為資料復原的一部分。如需復原磁帶的詳細資訊，請參閱 [您需要從故障的磁帶閘道復原虛擬磁帶]。

停用閘道

1. 開啟位於首頁 的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/
2. 在導覽窗格中，選擇 Gateways (閘道)，然後選擇失敗的閘道。
3. 選擇閘道的詳細資訊標籤，以顯示停用閘道訊息。
4. 選擇 Create recovery tapes (建立復原磁帶)。
5. 選擇 Disable gateway (停用閘道)。

了解磁帶狀態

每個磁帶都有一個相關聯的狀態，可讓您一眼得知磁帶的運作狀態。大多數時間，該狀態指出磁帶正常運作，而且您不需要採取任何動作。在某些情況下，該狀態指出磁帶發生可能需要您採取動作的問題。您可以找到下列資訊，協助您決定何時需要採取操作。

主題

- [了解 中的磁帶狀態資訊 VTL]
- [判斷存檔中的磁帶狀態]

了解 中的磁帶狀態資訊 VTL

磁帶的狀態必須AVAILABLE可讓您讀取或寫入磁帶。下表列出並說明可能的狀態值。

狀態	描述	磁帶資料存放位置
CREATING	正在建立虛擬磁帶。因為正在建立磁帶，所以無法將磁帶載入至磁帶硬碟。	—
AVAILABLE	虛擬磁帶已建立並準備好載入至磁帶硬碟。	Amazon S3
在 TRANSIT 到 中 VTS	虛擬磁帶已退出並且正在上傳以供存檔。此時，您的磁帶閘道正在將資料上傳至 AWS。如果所上傳的資料量很小，則此狀態可能不會出現。上傳完成時，狀態會變更為 ARCHIVING。	Amazon S3
ARCHIVING	磁帶閘道正在將虛擬磁帶移至 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 所支援的存檔。此程序會在資料上傳至 AWS 完成後進行。	資料正從 Amazon S3 移至 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive。
DELETING	正在刪除虛擬磁帶。	正在從 Amazon S3 刪除資料
DELETED	已成功刪除虛擬磁帶。	—
RETRIEVING	正在將虛擬磁帶從存檔擷取至磁帶閘道。 **Note** 虛擬磁帶只能擷取至磁帶閘道。	資料正從 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 移至 Amazon S3
RETRIEVED	從存檔擷取虛擬磁帶。擷取的磁帶具有防寫保護。	Amazon S3
RECOVERED	虛擬磁帶已復原且為唯讀。 當您因任何原因而無法存取磁帶閘道時，可以將與該磁帶閘道建立關聯的虛擬磁帶復原到另一個磁帶閘道。若要復原虛擬磁帶，請先停用無法存取的磁帶閘道。	Amazon S3

狀態	描述	磁帶資料存放位置
IRRECOVERABLE	無法讀取或寫入至虛擬磁帶。此狀態指出磁帶閘道發生錯誤。	Amazon S3

判斷存檔中的磁帶狀態

您可以使用下列程序，判斷虛擬磁帶在存檔中的狀態。

判斷虛擬磁帶的狀態

1. 開啟位於首頁 的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/
2. 在導覽窗格中，選擇 Tapes (磁帶)。
3. 在磁帶館網格的 Status (狀態) 欄中，檢查磁帶的狀態。

   磁帶狀態也會出現在每個虛擬磁帶的 Details (詳細資訊) 標籤中。

您可以在以下找到可能狀態值的描述。

狀態	描述
ARCHIVED	虛擬磁帶已退出並上傳至存檔。
RETRIEVING	正在從存檔擷取虛擬磁帶。 **Note** 虛擬磁帶只能擷取至磁帶閘道。
RETRIEVED	已從存檔擷取虛擬磁帶。擷取的磁帶為唯讀。

如需如何使用磁帶和VTL裝置的詳細資訊，請參閱 管理虛擬磁帶程式庫中的磁帶。

將資料移至新閘道

您可以隨著資料和效能需求的增長，或者您收到遷移閘道的 AWS 通知，在閘道之間移動資料。以下是執行此操作的一些原因：

- 將資料移至更好的主機平台或更新的 Amazon EC2執行個體。
- 重新整理您伺服器的底層硬體。

將資料移至新閘道所遵循的步驟取決於您擁有的閘道類型。

> **Note**
>
> 資料只能在相同的閘道類型之間移動。

將虛擬磁帶移至新的磁帶閘道

要將虛擬磁帶移至新的磁帶閘道

1. 使用備份應用程式將所有資料備份到虛擬磁帶上。等待備份成功完成。
2. 使用備份應用程式退出磁帶。磁帶將存放在其中一個 Amazon S3 儲存類別上。退出的磁帶存放在 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 中，並且是唯讀模式。

   在繼續之前，請確認退出的磁帶已存檔：

   a. 開啟位於首頁 的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/

   b. 在導覽窗格中選擇磁帶館 > 磁帶標籤以查看您的磁帶。根據預設，此清單一次最多可顯示 1,000 個磁帶，但您執行的搜尋會套用至所有磁帶。您可以使用搜尋列尋找符合特定準則的磁帶，或將清單減少到 1,000 個以下的磁帶。當您的清單包含 1,000 個或更少的磁帶時，您可以依各種屬性，以遞增或遞減順序來排序磁帶。

   c. 在清單的狀態欄中，檢查磁帶的狀態。

      磁帶狀態也會出現在每個虛擬磁帶的 Details (詳細資訊) 標籤中。

      如需有關確定存檔中磁帶狀態的詳細資訊，請參閱 判斷存檔中的磁帶狀態。

3. 使用您的備份應用程式，確認現有磁帶閘道沒有作用中的備份任務，然後再停止它。如果有任何作用中的備份任務，請等待它們完成並退出磁帶 (請參閱上一步)，然後再停止閘道。
4. 請使用下列步驟來停止現有磁帶閘道：

   a. 在導覽窗格中，選擇閘道，然後選擇您要停止的舊磁帶閘道。閘道的狀態為 Running (正在執行)。

   b. 對於動作，選擇停止閘道。從對話方塊確認閘道 ID，然後選擇停止閘道。

      舊磁帶閘道停止時，您可能會看到指出閘道狀態的訊息。閘道關閉時，訊息和啟動閘道按鈕會出現在詳細資訊標籤中。

   如需如何關閉閘道的詳細資訊，請參閱 啟動和停止磁帶閘道。
5. 建立新的磁帶閘道。如需詳細說明，請參閱建立閘道。
6. 使用下列步驟來建立新磁帶。

   a. 在導覽窗格中，選擇 Gateways (閘道) 標籤。

   b. 選擇建立磁帶以開啟建立磁帶對話方塊。

   c. 針對 Gateway (閘道)，選擇閘道。磁帶是針對此閘道所建立。

   d. 針對 Number of tapes (磁帶數目)，選擇您要建立的磁帶數目。如需磁帶限制的詳細資訊，請參閱 AWS Storage Gateway 配額。

      您也可以在此時設定自動建立磁帶。如需詳細資訊，請參閱自動建立磁帶。

   e. 針對 Capacity (容量)，輸入您要建立之虛擬磁帶的大小。磁帶必須大於 100 GiB。如需容量限制的資訊，請參閱 AWS Storage Gateway 配額。

   f. 針對 Barcode prefix (條碼字首)，輸入您要加到虛擬磁帶條碼前面的字首。

      > **Note**
      >
      > 虛擬磁帶可透過條碼唯一識別。您可以新增條碼的字首。字首是選用性的，但您可以使用它來協助識別虛擬磁帶。字首必須為大寫字母 (A–Z)，而且長度必須為一到四個字元。

   g. 對於 Pool (集區)，選擇 Glacier Pool (Glacier 集區) 或 Deep Archive Pool (Deep Archive 集區)。此集區代表備份軟體退出您的磁帶時，將存放您的磁帶所在的儲存體方案。

如果您想要將磁帶存檔在 S3 Glacier Flexible Retrieval 中，請選擇 Glacier 集區。當您的備份軟體退出磁帶時，它會自動存檔在 S3 Glacier Flexible Retrieval 中。您可以將 S3 Glacier Flexible Retrieval 用於多個作用中存檔，在其中，您通常可以於 3 到 5 小時內擷取磁帶。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的存檔物件的儲存類別。

如果您想要將磁帶存檔在 S3 Glacier Deep Archive 中，可以選擇 Deep Archive 集區。當您的備份軟體退出磁帶時，磁帶會自動存檔在 S3 Glacier Deep Archive 中。您可以將 S3 Glacier Deep Archive 用於長期資料保留和數位保存，其中的資料一年存取一次或兩次。您通常可以在 12 小時內擷取 S3 Glacier Deep Archive 中的磁帶存檔。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的存檔物件的儲存類別。

如果您將磁帶存檔在 S3 Glacier Flexible Retrieval 中，您可以稍後將其移到 S3 Glacier Deep Archive。如需詳細資訊，請參閱將磁帶移至 S3 Glacier Deep Archive 儲存類別。

> **Note**
>
> 在 2019 年 3 月 27 日之前建立的磁帶，會於您的備份軟體將它退出時，直接存檔在 S3 Glacier Flexible Retrieval 中。

h. (選用) 針對 Tags (標籤)，輸入索引鍵和值以將標籤新增至磁帶。標籤為區分大小寫的索引鍵值組，可協助您管理、篩選和搜尋磁帶。

i. 選擇 Create tapes (建立磁帶)。

7. 使用備份應用程式開始備份工作，並將資料備份到新磁帶。

8. (選用) 如果您的磁帶已存檔，而您需要從該磁帶還原資料，請將其擷取至新的磁帶閘道。磁帶將處於唯讀模式。如需更多有關擷取存檔磁帶的詳細資訊，請參閱 擷取已存檔的磁帶。

> **Note**
>
> 可能需要支付出站資料費用。

a. 在導覽窗格中選擇磁帶館 > 磁帶標籤以查看您的磁帶。根據預設，此清單一次最多可顯示 1,000 個磁帶，但您執行的搜尋會套用至所有磁帶。您可以使用搜尋列尋找符合特定準則的磁帶，或將清單減少到 1,000 個以下的磁帶。當您的清單包含 1,000 個或更少的磁帶時，您可以依各種屬性，以遞增或遞減順序來排序磁帶。

b. 選擇您要擷取的虛擬磁帶。對於動作，選擇擷取磁帶。

> **Note**
>
> 您希望擷取之虛擬磁帶的狀態必須為 ARCHIVED。

c. 在 Retrieve tape (擷取磁帶) 對話方塊中，針對 Barcode (條碼)，請確認條碼可識別您希望擷取的虛擬磁帶。

d. 針對閘道，請選擇您要將已存檔磁帶擷取到的新磁帶閘道，然後選擇擷取磁帶。

當您確認新的磁帶閘道正常運作時，您可以刪除舊磁帶閘道。

> **Important**
>
> 在刪除閘道之前，請確定目前沒有應用程式寫入至閘道的磁碟區。如果您刪除使用中的閘道，則資料可能會遺失。

9. 請使用下列步驟來刪除舊磁帶閘道：

> **Warning**
>
> 閘道一旦刪除，就無法還原。

a. 在導覽窗格中，選擇閘道，然後選擇您要刪除的閘道。

b. 針對 Actions (動作)，選擇 Delete gateway (刪除閘道)。

在出現的確認對話方塊中，確定列出的閘道 ID 指定了您要刪除的舊磁帶閘道，在確認欄位中輸入 **`delete`**，然後選擇刪除。

c. 刪除 VM。如需有關刪除 VM 的詳細資訊，請參閱 Hypervisor 文件。

監控 Storage Gateway

本節說明如何使用 Amazon 監控 Storage Gateway ，包括監控與閘道相關聯的資源 CloudWatch。您可以監控閘道的上傳緩衝區和快取儲存。您可以使用 Storage Gateway 主控台檢視閘道的指標和警示。例如，您可以檢視用於讀取和寫入操作的位元組數目、讀取和寫入操作所花的時間，以及從 Amazon Web Services 雲端擷取資料所花的時間。使用指標，您可以追蹤閘道的運作狀態，並設定警示，在一或多個指標落在定義閾值以外時通知您。

Storage Gateway 免費提供 CloudWatch 指標。會記錄兩週期間的 Storage Gateway 指標。透過使用這些指標，您可以存取歷史資訊，並更加了解閘道和磁碟區的執行狀況。Storage Gateway 也免費提供高解析度 CloudWatch 警示以外的警示。如需 CloudWatch 定價的詳細資訊，請參閱 Amazon CloudWatch 定價。 如需 的詳細資訊 CloudWatch，請參閱 Amazon CloudWatch 使用者指南 。

如需監控磁帶閘道及其相關資源的特定資訊，請參閱監控磁帶閘道 。

主題

了解閘道指標

在本主題的討論中，將閘道指標定義為範圍設為閘道的指標；也就是說，它們測量閘道的某個項目。因為閘道包含一或多個磁碟區，所以閘道專屬指標代表閘道上的所有磁碟區。例如，`CloudBytesUploaded` 指標是閘道在報告期間傳送至雲端的位元組總數。此指標包含閘道上所有磁碟區的活動。

使用閘道指標資料時，請指定您要檢視其指標之閘道的唯一識別碼。若要執行此作業，請指定 `GatewayId` 和 `GatewayName` 值。當您想要使用閘道的指標時，請在指標命名空間中指定閘道維度，以區分閘道專屬指標與磁碟區專屬指標。如需詳細資訊，請參閱使用 Amazon CloudWatch 指標。

> **Note**
>
> 某些指標只有在最近的監視期間產生新資料時，才會傳回資料點。

指標	描述
AvailabilityNotifications	閘道產生的可用相關運作狀態通知數目。 使用此指標搭配 Sum 統計資料，即可觀察閘道是否發生任何可用性相關事件。如需事件的詳細資訊，請檢查您設定的 CloudWatch 日誌群組。 單位：數字
CacheHitPercent	從快取服務的應用程式讀取百分比。報告期間結束時會取樣。 單位：百分比
CacheUsed	閘道快取儲存體中已使用的位元組總數。報告期間結束時會取樣。 單位：位元組
IoWaitPercent	閘道等候本機磁碟回應的時間百分比。 單位：百分比
MemTotalBytes	RAM 佈建至閘道 VM 的金額，以位元組為單位。 單位：位元組

指標	描述	
MemUsedBytes	閘道 VM RAM目前使用的位元組數。 單位：位元組	
QueuedWrites	等待寫入 的位元組數 AWS，在閘道中所有磁碟區的報告期間結束時取樣。這些位元組會保留在您閘道工作儲存體中。 單位：位元組	
TotalCacheSize	快取大小總計 (位元組)。報告期間結束時會取樣。 單位：位元組	
UploadBufferPercentUsed	閘道上傳緩衝區的使用百分比。報告期間結束時會取樣。 單位：百分比	
UploadBufferUsed	閘道上傳緩衝區中已使用的位元組總數。報告期間結束時會取樣。 單位：位元組	
UserCpuPercent	閘道處理所花費CPU的時間百分比，在所有核心之間進行平均。 單位：百分比	

Storage Gateway 指標的維度

Storage Gateway 服務的 CloudWatch 命名空間為 AWS/StorageGateway。每隔 5 分鐘免費自動提供資料。

維度	描述
GatewayId ，GatewayName	這些維度可篩選您向閘道特定指標請求的資料。您可以根據 GatewayId 或 GatewayName 的值來識別要運作的閘道。如果閘道名稱在您有興趣檢視指標的時間範圍內呈現不同的名稱，則請使用 GatewayId 。 閘道的傳輸量與延遲資料以該閘道的所有磁碟區為基準。如需有關使用閘道指標的詳細資訊，請參閱測量您閘道與 AWS之間的效能。

監控上傳緩衝區

您可以在以下找到如何監控閘道上傳緩衝區的相關資訊，以及如何建立警示，讓您在緩衝區超過指定閾值時收到通知。使用此方法，即可在完全填入緩衝區儲存之前將緩衝區儲存新增至閘道，而儲存應用程式會停止備份至 AWS。

上傳緩衝區的監控方式與快取磁碟區和磁帶閘道架構相同。如需詳細資訊，請參閱磁帶閘道的運作方式。

> **Note**
>
> 在 Storage Gateway 中發行快取磁碟區功能之前，WorkingStoragePercentUsed、WorkingStorageUsed 和 WorkingStorageFree 指標僅代表存放磁碟區的上傳緩衝區。現在，請使用對等的上傳緩衝區指標 UploadBufferPercentUsed、UploadBufferUsed 和 UploadBufferFree。這些指標套用至兩種閘道架構。

感興趣的項目	測量方式
上傳緩衝區用量	搭配使用 UploadBufferPercentUsed 、UploadBufferUsed 和 UploadBufferFree 指標與 Average 統計資料。例如，搭配使用 UploadBufferUsed 與 Average 統計資料，以分析一段時間的儲存用量。

測量已使用的上傳緩衝區百分比

1. 在 開啟 CloudWatch 主控台https://console.aws.amazon.com/cloudwatch/。
2. 選擇 StorageGateway： Gateway Metrics 維度，然後尋找您要使用的閘道。
3. 選擇 UploadBufferPercentUsed 指標。
4. 針對 Time Range (時間範圍)，選擇一個值。
5. 選擇 Average 統計資料。
6. 針對 Period (期間)，選擇 5 分鐘的值以符合預設報告時間。

其結果之依照時間排序的資料點集合包含上傳緩衝區使用百分比。

您可以使用下列程序，使用 CloudWatch 主控台建立警示。若要進一步了解警示和閾值，請參閱 Amazon CloudWatch 使用者指南 中的建立 CloudWatch 警示。

設定閘道上傳緩衝區的閾值警示上限

1. 在 開啟 CloudWatch 主控台https://console.aws.amazon.com/cloudwatch/。
2. 選擇 Create Alarm (建立警示) 以啟動 [Create Alarm] (建立警示) 精靈。
3. 指定警示的指標：
   a. 在建立警示精靈的選取指標頁面上，選擇 AWS/StorageGateway：GatewayId、GatewayName維度，然後尋找您要使用的閘道。
   b. 選擇 UploadBufferPercentUsed 指標。使用 Average 統計資料和 5 分鐘的期間。
   c. 選擇繼續。
4. 定義警示名稱、描述和閾值：
   a. 在 [Create Alarm] (建立警示) 精靈的 Define Alarm (定義警示) 頁面上，透過在 Name (名稱) 和 Description (描述) 方塊中提供警示的名稱和描述來識別警示。

b. 定義警示閾值。

c. 選擇繼續。

5. 設定警示的電子郵件動作：

a. 在建立警示精靈的設定動作頁面中，針對警示狀態選擇警示。

b. 針對 Topic (主題)，選擇 Choose or create email topic (選擇或建立主題)。

若要建立電子郵件主題，表示您設定了 Amazon SNS主題。如需 Amazon 的詳細資訊SNS，請參閱 Amazon 使用者指南中的設定 SNS Amazon。 CloudWatch

c. 針對 Topic (主題)，輸入主題的描述性名稱。

d. 選擇 Add Action (新增動作)。

e. 選擇繼續。

6. 檢閱警示設定，然後建立警示：

a. 在 [Create Alarm] (建立警示) 精靈的 Review (檢閱) 頁面上，檢閱警示定義、指標和要採取的相關聯動作 (例如傳送電子郵件通知)。

b. 在檢閱警示摘要之後，請選擇 Save Alarm (儲存警示)。

7. 確認警示主題的訂閱：

a. 開啟SNS您在建立主題時指定的電子郵件地址所傳送的 Amazon 電子郵件。

b. 按一下電子郵件中的連結，以確認訂閱。

訂閱確認隨即出現。

監控快取儲存

您可以在以下找到如何監控閘道快取儲存的相關資訊，以及如何建立警示，讓您在快取的參數超過指定閾值時收到通知。使用此警示，即可知道何時將快取儲存新增至閘道。

您只能監控快取磁碟區架構的快取儲存。如需詳細資訊，請參閱磁帶閘道的運作方式。

感興趣的項目	測量方式
總快取用量	搭配使用 `CachePercentUsed` 和 `TotalCacheSize` 指標與 `Average` 統計資料。例如，搭配使用 `CachePercentUsed` 與 `Average` 統計資料，以分析一段時間的快取用量。

感興趣的項目	測量方式
	只有在您將快取新增至閘道時，TotalCacheSize 指標才會變更。
由快取提供服務的讀取請求百分比	搭配 CacheHitPercent 統計資料使用 Average 指標。 一般而言，您想要將 CacheHitPercent 保留為高。
快取中髒污的百分比，也就是包含尚未上傳至 的內容 AWS	搭配使用 CachePercentDirty 指標與 Average 統計資料。 一般而言，您想要將 CachePercentDirty 保留為低。

測量閘道及其所有磁碟區的快取已變更百分比

1. 在 開啟 CloudWatch 主控台https://console.aws.amazon.com/cloudwatch/。
2. 選擇 StorageGateway： Gateway Metrics 維度，然後尋找您要使用的閘道。
3. 選擇 CachePercentDirty 指標。
4. 針對 Time Range (時間範圍)，選擇一個值。
5. 選擇 Average 統計資料。
6. 針對 Period (期間)，選擇 5 分鐘的值以符合預設報告時間。

其結果之依照時間排序的資料點集合包含超過 5 分鐘的快取已變更百分比。

測量磁碟區的快取已變更百分比

1. 在 開啟 CloudWatch 主控台https://console.aws.amazon.com/cloudwatch/。
2. 選擇 StorageGateway： 磁碟區指標維度，然後尋找您要使用的磁碟區。
3. 選擇 CachePercentDirty 指標。
4. 針對 Time Range (時間範圍)，選擇一個值。
5. 選擇 Average 統計資料。
6. 針對 Period (期間)，選擇 5 分鐘的值以符合預設報告時間。

其結果之依照時間排序的資料點集合包含超過 5 分鐘的快取已變更百分比。

了解 CloudWatch 警示

CloudWatch 警示會根據指標和表達式監控閘道的相關資訊。您可以在 Storage Gateway 主控台中新增閘道的 CloudWatch 警示，並檢視其狀態。如需用來監督磁帶閘道之測量結果的相關資訊，請參閱了解閘道指標和了解虛擬磁帶指標。對於每個警示，您指定將啟動其ALARM狀態的條件。Storage Gateway 主控台中的警示狀態指示燈會在處於 ALARM 狀態時變成紅色，讓您更輕鬆地主動監控狀態。您可以將警示設定為根據持續的狀態變更自動調用動作。如需 CloudWatch 警示的詳細資訊，請參閱 Amazon CloudWatch 使用者指南 中的使用 Amazon 警示。 CloudWatch

> **Note**
>
> 如果您沒有檢視 的許可 CloudWatch，則無法檢視警示。

針對每個啟用的閘道，建議您建立下列 CloudWatch警示：

- 高 IO 等候：`IoWaitpercent` >= 20，15 分鐘內 3 個資料點
- 快取變更百分比：`CachePercentDirty` > 80，20 分鐘內 4 個資料點
- 健康狀況通知：`HealthNotifications` >= 1，5 分鐘內 1 個資料點。設定此警示時，請將遺失資料處理設定為 notBreaching。

> **Note**
>
> 只有在閘道在 中有先前的運作狀態通知時，您才能設定運作狀態通知警示 CloudWatch。

對於啟用 HA 模式的VMware主機平台上的閘道，我們也建議使用此額外 CloudWatch 警示：

- 可用性通知：`AvailabilityNotifications` >= 1，5 分鐘內 1 個資料點。設定此警示時，請將遺失資料處理設定為 notBreaching。

下表說明警示的狀態。

州	描述
OK (確定)	指標或表達式在定義的閾值內。

州	描述
警示	指標或表達式在定義的閾值外。
資料不足	警示剛啟動，無法使用指標；或資料不足，無法讓指標判斷警示狀態。
無	未對閘道建立任何警示。若要建立新警示，請參閱為您的閘道建立自訂 CloudWatch 警示。
Unavailable	警示的狀態不明。選擇 Unavailable (無法使用)，可檢視 Monitoring (監控) 標籤中的錯誤資訊。

為您的閘道建立建議的 CloudWatch 警示

當您使用 Storage Gateway 主控台建立新的閘道時，您可以選擇自動建立所有建議的 CloudWatch 警示，做為初始設定程序的一部分。如需詳細資訊，請參閱設定磁帶閘道。如果您想要新增或更新現有閘道的建議 CloudWatch 警示，請使用下列程序。

新增或更新現有閘道的建議 CloudWatch 警示

> **Note**
>
> 此功能需要 CloudWatch 政策許可，該許可不會自動授予為預先設定的 Storage Gateway 完整存取政策的一部分。在嘗試建立建議的 CloudWatch 警示之前，請確定您的安全政策授予下列許可：
>
> - `cloudwatch:PutMetricAlarm`：建立警示
> - `cloudwatch:DisableAlarmActions`：關閉警示動作
> - `cloudwatch:EnableAlarmActions`：開啟警示動作
> - `cloudwatch:DeleteAlarms`：刪除警示

1. 開啟位於 https://console.aws.amazon.com/storagegateway/Home/ 的 Storage Gateway 主控台。
2. 在導覽窗格中，選擇閘道 ，然後選擇您要為其建立建議 CloudWatch 警示的閘道。
3. 在閘道詳細資訊頁面上，選擇監控標籤。
4. 在警示下，選擇建議的警示。建議的警示會自動建立。

警示區段列出特定閘道的所有 CloudWatch 警示。您可以在此處選擇和刪除一或多個鬧鐘、開啟或關閉鬧鐘動作，以及建立新鬧鐘。

為您的閘道建立自訂 CloudWatch 警示

CloudWatch 使用 Amazon Simple Notification Service （Amazon SNS） 在警示變更狀態時傳送警示通知。警示會監看指定時段內的單一指標，並根據與多個時段內指定閾值相對的指標值來執行一或多個動作。動作是傳送至 Amazon SNS主題的通知。您可以在建立 CloudWatch 警示時建立 Amazon SNS 主題。如需 Amazon 的詳細資訊SNS，請參閱 Amazon Simple Notification Service 開發人員指南 SNS 中的什麼是 Amazon？。

在 Storage Gateway 主控台中建立 CloudWatch 警示

1. 開啟位於 https://console.aws.amazon.com/storagegateway/Home/ 的 Storage Gateway 主控台。
2. 在導覽窗格中，選擇閘道，然後選擇您要管理的閘道。
3. 在閘道詳細資訊頁面上，選擇監控標籤。
4. 在警示 下，選擇建立警示以開啟 CloudWatch 主控台。
5. 使用 CloudWatch 主控台建立您想要的警示類型。您可以建立以下類型的警示：

   - 靜態閾值警示：根據所選指標之設定閾值的警示。當指標違反指定數量的評估期間閾值時，警示會進入 ALARM 狀態。

     若要建立靜態閾值警示，請參閱 Amazon CloudWatch 使用者指南 中的根據靜態閾值建立 CloudWatch 警示。
   - 異常偵測警示：異常偵測會探勘過去的指標資料，並建立預期值的模型。您可以設定異常偵測閾值的值，並將此閾值與模型 CloudWatch 搭配使用，以判斷指標的值的「正常」範圍。較高的臨界值會產生較厚的「正常」值範圍。您可以選擇警示觸發時機是在指標值超過預期值範圍、低於範圍，或者兩者擇一。

     若要建立異常偵測警示，請參閱 Amazon CloudWatch 使用者指南 中的根據異常偵測建立 CloudWatch 警示。
   - 指標數學運算式警示：以數學運算式中使用的一或多個指標為基礎的警示。您要指定表達式、閾值和評估期間。

     若要建立指標數學表達式警示，請參閱 Amazon CloudWatch 使用者指南 中的根據指標數學表達式建立 CloudWatch 警示。

- 複合警示：一種警示，可透過監看其他警示的警示狀態來決定警示狀態。複合警示可協助您減少警示噪音。

  若要建立複合警示，請參閱 Amazon CloudWatch 使用者指南 中的建立複合警示。

6. 在 CloudWatch 主控台中建立警示之後，請返回 Storage Gateway 主控台。您可以執行下列其中一個操作來檢視警示：

   - 在導覽窗格中，選擇閘道，然後選擇您要檢視的閘道。在詳細資訊索引標籤的警示 下，選擇CloudWatch 警示 。
   - 在瀏覽窗格中，選擇閘道，選擇要檢視警示的閘道，然後選擇監控標籤頁。

     警示區段列出特定閘道的所有 CloudWatch 警示。您可以在此處選擇和刪除一或多個鬧鐘、開啟或關閉鬧鐘動作，以及建立新鬧鐘。
   - 在導覽窗格中，選擇閘道，然後選擇您要檢視其警示之閘道的警示狀態。

如需有關如何編輯或刪除警示的資訊，請參閱編輯或刪除 CloudWatch 警示 。

> **Note**
>
> 當您使用 Storage Gateway 主控台刪除閘道時，與閘道相關聯的所有 CloudWatch 警示也會自動刪除。

監控磁帶閘道

本節中的主題描述如何監控磁帶閘道的程序和概念資訊。您可以監控與磁帶閘道相關聯的虛擬磁帶、快取儲存體和上傳緩衝區。您可以使用 AWS Management Console 來檢視磁帶閘道的指標。使用指標，您可以追蹤您磁帶閘道的運作狀況，並設定警示，在一或多個指標超出定義的閾值時通知您。

您可以使用 Amazon CloudWatch Logs 取得有關磁帶閘道和相關資源運作狀態的資訊。您可以使用日誌來監控閘道遇到的錯誤。此外，您可以使用 Amazon CloudWatch 訂閱篩選條件，即時自動處理日誌資訊。

Storage Gateway 免費提供 CloudWatch 指標。會記錄兩週期間的 Storage Gateway 指標。透過使用這些指標，您可以存取歷史資訊，並更加了解磁帶閘道及虛擬磁帶的執行狀況。如需 的詳細資訊 CloudWatch，請參閱 Amazon CloudWatch 使用者指南。

資料輸送量、資料延遲和每秒操作數是您可以用來了解儲存應用程式如何透過磁帶閘道執行的指標。當您使用正確的彙整統計資料時，便可做為您提供的 Storage Gateway 指標測量這些值。

主題

使用日誌群組取得磁帶閘道運作狀態 CloudWatch 日誌

您可以使用 Amazon CloudWatch Logs 取得有關磁帶閘道和相關資源運作狀態的資訊。您可以使用日誌來監控閘道遇到的錯誤。此外，您可以使用 Amazon CloudWatch 訂閱篩選條件，即時自動處理日誌資訊。如需詳細資訊，請參閱 Amazon 使用者指南中的使用訂閱即時處理日誌資料。 CloudWatch

例如，假設閘道部署在啟用 VMware HA 的叢集中，而且您需要了解任何錯誤。您可以設定 CloudWatch 日誌群組來監控閘道，並在閘道遇到錯誤時收到通知。您可以在啟用閘道時或在啟用並啟動及執行閘道之後，設定群組。如需在啟用閘道時如何設定 CloudWatch 日誌群組的詳細資訊，請參閱設定磁帶閘道 。如需 CloudWatch 日誌群組的一般資訊，請參閱 Amazon 使用者指南中的使用日誌群組和日誌串流。 CloudWatch

如需有關如何疑難排解和修正這些類型錯誤的詳細資訊，請參閱為虛擬磁帶問題進行故障診斷。

下列程序說明如何在閘道啟用後設定 CloudWatch 日誌群組。

若要設定 CloudWatch 日誌群組以搭配您的檔案閘道使用

1. 登入 AWS Management Console 並開啟位於 首頁的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/
2. 在導覽窗格中，選擇閘道 ，然後選擇您要設定 CloudWatch 日誌群組的閘道。
3. 對於動作 ，選擇編輯閘道資訊或在詳細資訊索引標籤上，在運作狀態日誌 和 未啟用 下，選擇設定日誌群組以開啟編輯CustomerGatewayName對話方塊。
4. 針對閘道運作狀態日誌群組，選擇下列其中一項：
   - 如果您不想使用日誌群組監控閘道，請停用 CloudWatch 日誌。
   - 建立新的日誌群組以建立新的 CloudWatch 日誌群組。

- 使用現有的日誌群組來使用已存在的 CloudWatch 日誌群組。

  從現有的日誌群組清單中選擇日誌群組。

5. 選擇 Save changes (儲存變更)。
6. 若要查看閘道的運作狀態日誌，請依下列步驟執行：

   1. 在導覽窗格中，選擇閘道 ，然後選擇您設定 CloudWatch 日誌群組的閘道。
   2. 選擇詳細資訊索引標籤，然後在運作狀態日誌 下，選擇CloudWatch 日誌 。日誌群組詳細資訊頁面會在 CloudWatch主控台中開啟。

以下是傳送至 的磁帶閘道事件訊息範例 CloudWatch。此範例顯示 `TapeStatusTransition` 訊息。

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

使用 Amazon CloudWatch 指標

您可以使用 或 取得磁帶閘道 AWS Management Console 的監控資料 CloudWatch API。主控台會根據來自 的原始資料顯示一系列圖形 CloudWatch API。也可以透過其中一個 Amazon 軟體開發套件 CloudWatch API ( ) 或 Amazon CloudWatch API 工具使用 。 AWS SDKs根據您的需求，您可能偏好使用主控台中顯示的圖形或從 擷取的圖形API。

無論您選擇使用指標的方法為何，您都必須指定下列資訊：

- 要使用的指標維度。維度是一組用來單獨辨識指標的名稱值組。Storage Gateway 的維度為 `GatewayId` 和 `GatewayName`。在 CloudWatch 主控台中，您可以使用 `Gateway Metrics` 檢視輕鬆選取閘道特定和磁帶特定維度。如需維度的詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的維度。
- 指標名稱，例如 `ReadBytes`。

下表摘要說明可供您使用之 Storage Gateway 指標資料的類型。

Amazon CloudWatch 命名空間	維度	描述
`AWS/StorageGateway`	`GatewayId`，`GatewayName`	這些維度會篩選描述磁帶閘道各層面的指標資料。您可以透過同時指定 `GatewayId` 和 `GatewayName` 維度，來識別要使用的磁帶閘道。 磁帶閘道的輸送量與延遲資料基於該磁帶閘道中的所有虛擬磁帶。 每隔 5 分鐘免費自動提供資料。

閘道和磁帶指標的使用類似其他服務指標的使用。您可以在下列文件中找到一些最常見的指標任務CloudWatch的討論：

- 檢視可用的指標
- 取得指標的統計資料
- 建立 CloudWatch警示

了解虛擬磁帶指標

您可以在以下找到涵蓋虛擬磁帶之 Storage Gateway 指標的相關資訊。每個磁帶都有一組相關聯的指標。

有些磁帶專屬指標可能與特定閘道專屬指標的名稱相同。這些指標代表相同類型的測量，但其範圍為磁帶而非閘道。開始工作前，請指定您要使用閘道指標還是磁帶指標。使用磁帶指標時，請指定您要檢視指標之磁帶的磁帶 ID。如需詳細資訊，請參閱使用 Amazon CloudWatch 指標。

> **Note**
>
> 某些指標只有在最近的監視期間產生新資料時，才會傳回資料點。

下表說明 Storage Gateway 指標，您可以用於取得磁帶的相關資訊。

指標	描述
CachePercentDirty	未保存到 AWS的閘道快取整體百分比中磁帶的比重。報告期間結束時會取樣。 使用閘道的 CachePercentDirty 指標可檢視未保存到 AWS的閘道快取整體百分比。如需詳細資訊，請參閱了解閘道指標。 單位：百分比
CloudTraffic	已上傳以及已從雲端下載到磁帶的位元組數量。 單位：位元組
IoWaitPercent	磁帶目前使用的已配置 IoWait 單位百分比。 單位：百分比
HealthNotification	磁帶已傳送的運作狀態通知數目。 單位：計數
MemUsedBytes	磁帶目前使用的已配置記憶體百分比。 單位：位元組
MemTotalBytes	磁帶目前使用的總記憶體百分比。 單位：位元組
ReadBytes	檔案共享報告期間從您內部部署應用程式讀取的位元組總數。 使用此指標搭配Sum統計資料來測量輸送量，並搭配Samples統計資料來測量 IOPS。 單位：位元組
UserCpuPercent	磁帶目前使用的使用者配置的CPU運算單位百分比。

指標	描述
	單位：百分比
WriteBytes	報告期間寫入至您內部部署應用程式的位元組總數。 使用此指標搭配Sum統計資料來測量輸送量，並搭配Samples統計資料來測量 IOPS。 單位：位元組

測量磁帶閘道與 之間的效能 AWS

資料輸送量、資料延遲和每秒操作數這三個測量，可讓您了解使用您磁帶閘道之應用程式儲存體的執行狀況。當您使用正確的彙整統計資料時，便可做為您提供的 Storage Gateway 指標測量這些值。

「統計資料」是在一段指定期間內的指標彙整。當您在 中檢視指標的值時 CloudWatch，請使用資料延遲Average的統計資料 （毫秒），並使用每秒輸入/輸出操作的統計資料 Samples （IOPS）。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南 中的統計資料。

下表摘要說明指標和對應的統計資料，您可以用來測量輸送量、延遲，以及磁帶閘道與 IOPS之間的傳輸量、延遲 AWS。

感興趣的項目	測量方式
Latency (延遲)	將 ReadTime和 WriteTime 指標與 Average CloudWatch 統計資料搭配使用。例如，Average 指標的 ReadTime 值可讓您了解在範例期間內每個操作的延遲。
對 的輸送量 AWS	將 CloudBytesDownloaded 和 Sum CloudBytesUploaded 指標與 CloudWatch 統計資料搭配使用。例如，在 5 分鐘的取樣期間，CloudBytesDownloaded 指標Sum的值除以 300 秒，可讓您以每秒位元組為單位的速率，從 AWS 到磁帶閘道的輸送量。
資料的延遲 AWS	搭配 CloudDownloadLatency 統計資料使用 Average 指標。例如，Average 指標的 CloudDownloadLatency 統計資料可讓您了解在範例期間內每個操作的延遲。

測量從磁帶閘道到 的上傳資料輸送量 AWS

1. 在 開啟 CloudWatch 主控台https://console.aws.amazon.com/cloudwatch/。
2. 選擇指標標籤。
3. 選擇 StorageGateway： Gateway Metrics 維度，然後尋找您要使用的磁帶閘道。
4. 選擇 `CloudBytesUploaded` 指標。
5. 針對 Time Range (時間範圍)，選擇一個值。
6. 選擇 Sum 統計資料。
7. 針對 Period (期間)，選擇 5 分鐘或更高的值。
8. 在結果依照時間排序的資料點集合中，將每個資料點除以期間 (單位為秒)，便可取得範例期間的輸送量。例如，如果指定資料點從磁帶閘道到 的輸送量 AWS 為 555，544，576 位元組，且期間為 300 秒，則大約輸送量為每秒 1.85 MB。

測量從磁帶閘道到 的資料延遲 AWS

1. 在 開啟 CloudWatch 主控台https://console.aws.amazon.com/cloudwatch/。
2. 選擇指標標籤。
3. 選擇 StorageGateway： GatewayMetrics 維度，然後尋找您要使用的磁帶閘道。
4. 選擇 `CloudDownloadLatency` 指標。
5. 針對 Time Range (時間範圍)，選擇一個值。
6. 選擇 `Average` 統計資料。
7. 針對 Period (期間)，選擇 5 分鐘的值以符合預設報告時間。

其結果之依照時間排序的資料點集合便包含延遲 (單位為毫秒)。

將磁帶閘道輸送量的閾值上限警示設定為 AWS

1. 在 開啟 CloudWatch 主控台https://console.aws.amazon.com/cloudwatch/。
2. 選擇 Create Alarm (建立警示) 以啟動 [Create Alarm] (建立警示) 精靈。
3. 選擇 StorageGateway： Gateway Metrics 維度，然後尋找您要使用的磁帶閘道。
4. 選擇 `CloudBytesUploaded` 指標。
5. 定義當 `CloudBytesUploaded` 指標大於等於指定值且持續指定時間之後的警示狀態，來定義警示。例如，您可以定義當 `CloudBytesUploaded` 指標大於 10 MB 長達 60 分鐘時的警示狀態。

6. 設定要針對警示狀態採取的動作。例如，您可以設定要傳送一封電子郵件通知給您。
7. 選擇建立警示 。

設定從 讀取資料的閾值上限警示 AWS

1. 在 開啟 CloudWatch 主控台https://console.aws.amazon.com/cloudwatch/。
2. 選擇 Create Alarm (建立警示) 以啟動 [Create Alarm] (建立警示) 精靈。
3. 選擇 StorageGateway： Gateway Metrics 維度，然後尋找您要使用的磁帶閘道。
4. 選擇 `CloudDownloadLatency` 指標。
5. 定義當 `CloudDownloadLatency` 指標大於等於指定值且持續指定時間之後的警示狀態，來定義警示。例如，您可以定義當 `CloudDownloadLatency` 指標大於 60,000 毫秒且長達 2 小時的情形下之警示狀態。
6. 設定要針對警示狀態採取的動作。例如，您可以設定要傳送一封電子郵件通知給您。
7. 選擇建立警示。

維護您的閘道

維護您的磁帶閘道包含各種任務，例如為快取儲存體調整大小和設定本機磁碟，以及上傳緩衝空間、管理更新和設定更新排程、管理頻寬用量，以及在必要時關閉或刪除閘道和相關資源。這些任務對於所有閘道類型而言非常常見。若您尚未建立閘道，請參閱建立閘道。

主題

- 管理 Storage Gateway 的本機磁碟 - 了解如何評估磁碟大小需求、新增快取容量，以及管理您配置到磁帶閘道以進行緩衝和儲存的本機磁碟。
- 管理磁帶閘道的頻寬 - 了解如何將閘道的上傳輸送量限制為 AWS ，以控制閘道使用的網路頻寬量。
- 管理閘道更新 - 了解如何開啟或關閉維護更新，並修改磁帶閘道的維護時段排程。
- 關閉閘道 VM - 了解如果您需要關閉或重新啟動閘道虛擬機器以進行維護時該怎麼做，例如將修補程式套用至 Hypervisor 時。
- 刪除閘道並移除相關資源 - 了解如何使用 AWS Storage Gateway 主控台刪除閘道，並清除相關聯的資源，以避免因繼續使用而被收取費用。

管理 Storage Gateway 的本機磁碟

閘道虛擬機器 (VM) 使用您內部部署的本機磁碟來進行緩衝及儲存。在 Amazon EC2執行個體上建立的閘道會使用 Amazon EBS磁碟區作為本機磁碟。

主題

- 決定本機磁碟儲存體的數量
- 設定額外的上傳緩衝和快取儲存體

決定本機磁碟儲存體的數量

您希望為閘道配置的磁碟數目及大小皆由您決定。根據您部署的儲存解決方案，閘道需要額外的儲存：

- 磁帶閘道需要至少兩個磁碟。一個做為快取使用，另一個則做為上傳緩衝使用。

下表針對您所部署的閘道建議本機磁碟儲存體大小。您可以在設定閘道之後以及工作負載需求增加時，新增更多本機儲存體。

本機儲存體	描述
上傳緩衝	上傳緩衝可在閘道將資料上傳至 Amazon S3 前，提供資料的預備區域。您的閘道會透過加密的安全通訊端層 （SSL） 連線將此緩衝區資料上傳至 AWS。
快取儲存體	快取儲存體做為內部部署耐久存放區，存放等待從上傳緩衝上傳至 Amazon S3 的資料。當您的應用程式在磁碟區或磁帶上執行 I/O 時，閘道會將資料儲存到快取儲存體，以提供低延遲存取。當您的應用程式從磁碟區或磁帶請求資料時，閘道會先檢查快取儲存體是否有資料，之後才會從 AWS下載資料。

> **Note**
>
> 當您佈建磁碟時，若上傳緩衝和快取儲存體使用相同的實體資源 (相同的磁碟)，強烈建議您不要為上傳緩衝及快取儲存體佈建本機磁碟。基礎實體儲存資源在 中表示為資料存放區 VMware。當您部署閘道 VM 時，您會選擇要存放 VM 檔案的資料存放區。當您佈建本機磁碟 (例如：做為快取儲存體或上傳緩衝使用) 時，您選用擇將虛擬磁碟存放在與 VM 相同的資料存放區中，或是其他資料存放區中。
>
> 若您有超過一個資料存放區，我們強烈建議您為快取儲存體選擇一個資料存放區，並為上傳緩衝選擇另外一個資料存放區。後端僅為一個基礎實體磁碟的資料存放區，在用以同時做為快取儲存體和上傳緩衝的後端時，可能會在某些情況下導致效能不佳。如果備份是效能較差的RAID組態，例如 ，也是如此RAID1。

在您閘道的初始設定和部署完成後，您可以透過新增或移除上傳緩衝的磁碟來調整本機儲存體。您也可以新增快取儲存體的磁碟。

判斷要配置的上傳緩衝大小

您可以透過使用上傳緩衝公式，來判斷要配置的上傳緩衝大小。我們強烈建議您為上傳緩衝配置至少 150 GiB。若公式傳回的值小於 150 GiB，請使用 150 GiB 做為您為上傳緩衝配置的數量。您可以為每個閘道設定最多 2 TiB 的上傳緩衝容量。

> **Note**
>
> 針對磁帶閘道，當上傳緩衝到達其容量時，您的應用程式可繼續從您的儲存體磁碟區讀取及寫入資料。不過，磁帶閘道不會將任何磁碟區資料寫入其上傳緩衝區，也不會將任何這些資料上傳到 ， AWS 直到 Storage Gateway 將本機儲存的資料與存放在 中的資料副本同步為止 AWS。當磁碟區處於 BOOTSTRAPPING 狀態時，會發生此同步。

若要估計需配置的上傳緩衝數量，您可以判斷預期的傳入及傳出資料速率，並帶入下列公式。

傳入資料的速率

此速率指的是應用程式輸送量，即您的內部部署應用程式於一段時間內，將資料寫入您閘道的速率。

傳出資料的速率

此速率指的是網路輸送量，即您的閘道可將資料上傳至 AWS的速率。此速率取決於您的網路速度、使用率，以及您是否啟用頻寬限流。此速率應針對壓縮進行調整。將資料上傳至 時 AWS，閘道會盡可能套用資料壓縮。例如，若您的應用程式資料為純文字，您可能取得 2:1 的有效壓縮比。但是，若您是要寫入影片，則閘道可能會無法達到任何資料壓縮比，並且可能會需要更多的閘道上傳緩衝。

若為下列任一情形，強烈建議您配置至少 150 GiB 的上傳緩衝區空間：

- 您的傳入率高於傳出率。
- 該公式傳回小於 150 GiB 的值。

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

例如，假設您的商業應用程式將文字資料寫入您閘道的速率為每秒 40 MB，每天 12 小時，則您的網路輸送量為每秒 12 MB。假設文字資料的壓縮因數為 2:1，則您應為上傳緩衝配置約 690 GiB 的空間。

Example

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

您可以先使用概略值來判斷您希望配置給閘道做為上傳緩衝空間的磁碟大小。視需要使用 Storage Gateway 主控台新增更多上傳緩衝空間。此外，您可以使用 Amazon CloudWatch 操作指標來監控上傳緩衝區用量，並判斷其他儲存需求。如需指標和設定警示的資訊，請參閱監控上傳緩衝區。

判斷要配置的快取儲存體大小

您的閘道會使用其快取儲存體來提供您最近存取之資料的低延遲存取。快取儲存體做為內部部署耐久存放區，存放等待從上傳緩衝上傳至 Amazon S3 的資料。一般而言，您會將快取儲存體的大小設為上傳緩衝大小的 1.1 倍。如需如何估計您快取儲存體大小的詳細資訊，請參閱判斷要配置的上傳緩衝大小。

您可以先使用概略值來佈建快取儲存體的磁碟。然後，您可以使用 Amazon CloudWatch 操作指標來監控快取儲存用量，並根據需要使用主控台佈建更多儲存。如需使用指標和設定警示的資訊，請參閱監控快取儲存。

設定額外的上傳緩衝和快取儲存體

隨著您應用程式的需求變更，您可以增加閘道的上傳緩衝或快取儲存體容量。您可以為閘道增加儲存容量，而不會中斷功能或造成停機。在您新增更多儲存空間時，您的閘道 VM 會同時維持開啟狀態。

> **Important**
>
> 新增快取或上傳緩衝至現有閘道時，您必須在閘道主機 Hypervisor 或 Amazon EC2執行個體上建立新的磁碟。請勿移除或變更已配置為快取或上傳緩衝的現有磁碟大小。

為您的閘道設定額外的上傳緩衝或快取儲存體

1. 在閘道主機 Hypervisor 或 Amazon EC2執行個體上佈建一或多個新磁碟。如需如何在 Hypervisor 中佈建磁碟的資訊，請參閱 Hypervisor 文件。如需為 Amazon EC2執行個體佈建 Amazon EBS 磁碟區的相關資訊，請參閱 Amazon Elastic Compute Cloud 使用者指南中的 Linux 執行個體 Amazon EBS磁碟區。在以下步驟中，您將設定此磁碟為上傳緩衝或快取儲存體。

2. 開啟位於首頁 的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/
3. 在導覽窗格中，選擇 Gateways (網際網路閘道)。
4. 從清單中搜尋您的閘道，並選取它。
5. 從動作功能表中，選擇設定儲存體。
6. 在設定儲存體區段中，識別您佈建的磁碟。如果您沒有看到您的磁碟，請選擇重新整理圖示重新整理清單。針對每個磁碟，CACHESTORAGE從配置到下拉式功能表中選擇UPLOADBUFFER或 。
7. 選擇儲存變更以儲存您的組態設定。

管理磁帶閘道的頻寬

您可以限制 (或限制) 從閘道到閘道的上傳輸量， AWS 或限制從 AWS 閘道下載輸送量。使用頻寬調節可協助您控制閘道所用的網路頻寬。根據預設，啟用的閘道在上傳或下載都沒有速率限制。

您可以使用 AWS Management Console，或以程式設計方式使用 Storage Gateway API (請參閱 UpdateBandwidthRateLimit) 或 AWS 軟體開發套件 (SDK) 來指定速率限制。透過編寫程式的方式進行頻寬限流，您可以全天候自動變更限制，例如，排程變更頻寬的任務。

您也可以為閘道定義以排程為基礎的頻寬限流。您可以透過定義一或多 bandwidth-rate-limit 個間隔來排程頻寬節流。如需詳細資訊，請參閱使用 Storage Gateway 主控台進行排程的頻寬限流。

設定頻寬節流的單一設定與定義排程的功能相當於定義排程，其中的 [開始時 bandwidth-rate-limit 間] `00:00` 和 [結束時間] 為 [每天] 設定的單一間隔。`23:59`

> **Note**
>
> 本節中的資訊僅適用於磁帶和磁碟區閘道。若要管理 Amazon S3 檔案閘道的頻寬，請參閱管理 Amazon S3 檔案閘道的頻寬。Amazon FSx 檔案閘道目前不支援頻寬速率限制。

主題

- 使用 Storage Gateway 主控台變更頻寬限流
- 使用 Storage Gateway 主控台進行排程的頻寬限流
- 使用更新閘道頻寬速率限制 AWS SDK for Java
- 使用更新閘道頻寬速率限制 AWS SDK for .NET

- 使用更新閘道頻寬速率限制 AWS Tools for Windows PowerShell

使用 Storage Gateway 主控台變更頻寬限流

下列程序說明如何從 Storage Gateway 主控台變更閘道的頻寬限流。

使用主控台變更閘道的頻寬調節

1. 在https://console.aws.amazon.com/storagegateway/首頁開啟 Storage Gateway 主控台。
2. 在導覽窗格中，選擇閘道，然後選擇您要管理的閘道。
3. 在動作中，選擇編輯頻寬限制。
4. 在編輯速率限制對話方塊中，輸入新的限制值，然後選擇儲存。您的變更會出現在閘道的 Details (詳細資訊) 標籤中。

使用 Storage Gateway 主控台進行排程的頻寬限流

下列程序說明如何從 Storage Gateway 主控台變更閘道的頻寬限流排程。

新增或修改閘道頻寬限流的排程

1. 在https://console.aws.amazon.com/storagegateway/首頁開啟 Storage Gateway 主控台。
2. 在導覽窗格中，選擇閘道，然後選擇您要管理的閘道。
3. 在動作中，選擇編輯頻寬速率限制排程。

   設備的 bandwidth-rate-limit 排程會顯示在 [編輯頻寬速率限制排程] 對話方塊中。根據預設，新的閘道 bandwidth-rate-limit 排程為空白。
4. 在 [編輯頻寬速率限制排程] 對話方塊中，選擇 [新增項目] 以新增 bandwidth-rate-limit間隔。為每個 bandwidth-rate-limit間隔輸入下列資訊：

   - 星期幾 — 您可以為工作日 (星期一至星期五)、週末 (星期六和星期日)、一週中的每一天或一週中的一或多個特定日期建立 bandwidth-rate-limit 間隔。
   - 開始時間：輸入閘道本機時區中頻寬間隔的開始時間 (使用 HH: MM 格式)。

   > **Note**
   >
   > 您的 bandwidth-rate-limit 間隔會從您在此處指定的分鐘開始開始。

- 結束時間 — 以 HH: MM 格式輸入閘道本地時區 bandwidth-rate-limit 間隔的結束時間。

  > **Important**
  >
  > 間 bandwidth-rate-limit 隔在此處指定的分鐘結束時結束。若要排定在小時結束時結束的間隔，請輸入 **59**。
  > 若要排程不間斷的連續間隔，在小時開始時轉換且間隔之間沒有中斷，請輸入 **59** 作為第一個間隔的結束分鐘。針對後續間隔的開始分鐘，輸入 **00**。

- 下載速率：輸入下載速率限制 (以每秒 KB (Kbps) 為單位，或選取無限制停用下載的頻寬限流。下載速率的最小值為 100 Kbps。
- 上傳速率：輸入上傳速率限制 (以 Kbps 為單位)，或選取無限制停用上傳的頻寬限流。上傳速率為 50 Kbps。

若要修改間 bandwidth-rate-limit 隔，您可以輸入間隔參數的修訂值。

要刪除間 bandwidth-rate-limit 隔，您可以選擇要刪除的間隔右側的「刪除」。

完成變更後，選擇儲存。

5. 選擇 [新增項目]，然後輸入日 bandwidth-rate-limit 期、開始和結束時間以及下載和上傳速率限制，以繼續新增間隔。

   > **Important**
   >
   > B andwidth-rate-limit 間隔不能重疊。間隔的開始時間必須在前一個間隔的結束時間之後，以及在下列間隔的開始時間之前發生。

6. 輸入所有 bandwidth-rate-limit 間隔後，選擇 [儲存變更] 以儲存 bandwidth-rate-limit 排程。

成功更新 bandwidth-rate-limit 排程後，您可以在閘道的「詳細資料」面板中查看目前的下載和上傳速率限制。

使用更新閘道頻寬速率限制 AWS SDK for Java

透過編寫程式的方式更新頻寬速率限制，您可以自動調整一段時間內的限制，例如使用排程的任務。下列範例示範如何使用 AWS SDK for Java更新閘道的頻寬速率限制。若要使用範例程式碼，您應該熟悉

如何執行 Java 主控台應用程式。如需詳細資訊，請參閱《AWS SDK for Java 開發人員指南》中的入門。

Example ：使用更新閘道頻寬速率限制 AWS SDK for Java

下列 Java 程式碼範例會更新閘道的頻寬速率限制。若要使用此範例程式碼，您必須提供服務端點、閘道 Amazon 資源名稱 (ARN) 以及上傳和下載限制。如需可與 Storage Gateway 搭配使用的 AWS 服務 AWS Storage Gateway 端點清單，請參閱 AWS 一般參考.

```
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());
        }
    }
}
```

使用更新閘道頻寬速率限制 AWS SDK for .NET

透過編寫程式的方式更新頻寬速率限制，您可以自動調整一段時間內的限制，例如使用排程的任務。下列範例示範如何使用 AWS SDK for .NET更新閘道的頻寬速率限制。若要使用範例程式碼，您應該熟悉執行. NET控制台應用程序 如需詳細資訊，請參閱《AWS SDK for .NET 開發人員指南》中的入門。

Example ：使用更新閘道頻寬速率限制 AWS SDK for .NET

下列 C# 程式碼範例會更新閘道的頻寬速率限制。若要使用此範例程式碼，您必須提供服務端點、閘道 Amazon 資源名稱 (ARN) 以及上傳和下載限制。如需可與 Storage Gateway 搭配使用的 AWS 服務 AWS Storage Gateway 端點清單，請參閱 AWS 一般參考.

```
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());
            }
        }
    }
}
```

使用更新閘道頻寬速率限制 AWS Tools for Windows PowerShell

透過編寫程式的方式更新頻寬速率限制，您可以自動調整一段時間內的限制，例如使用排程的任務。下列範例示範如何使用 AWS Tools for Windows PowerShell更新閘道的頻寬速率限制。若要使用範例程式碼，您應該熟悉執行指 PowerShell令碼。如需詳細資訊，請參閱 AWS Tools for Windows PowerShell 使用者指南中的入門。

Example ：使用更新閘道頻寬速率限制 AWS Tools for Windows PowerShell

下列 PowerShell 指令碼範例會更新閘道的頻寬速率限制。若要使用此範例指令碼，您必須提供閘道 Amazon 資源名稱 (ARN) 以及上傳和下載限制。

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

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

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

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

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

$limits =  Get-SGBandwidthRateLimit -GatewayARN $gatewayARN

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

管理閘道更新

Storage Gateway 由受管雲端服務元件和閘道設備元件組成，您可以在內部部署或在 AWS 雲端的 Amazon EC2執行個體上部署。這兩個元件都會定期收到更新。本節中的主題描述這些更新的節奏、如何套用更新，以及如何在部署中的閘道上設定更新相關設定。

> **Important**
>
> 您應該將 Storage Gateway 裝置視為受管理的虛擬機器，且不應嘗試以任何方式存取或修改其安裝。嘗試使用一般 AWS 閘道更新機制（例如， 或 Hypervisor 工具）以外的方法安裝SSM 或更新任何軟體套件，可能會導致閘道故障。

更新頻率和預期行為

AWS 會視需要更新雲端服務元件，而不會造成部署的閘道中斷。您部署的閘道設備會收到每月維護更新。每月維護更新可能包括作業系統和軟體升級、解決穩定性、效能和安全性的修正，以及對新功能的

存取。所有更新都是累積的，並在套用時升級閘道至目前版本。如需有關每次更新中包含的特定變更的資訊，請參閱適用於磁帶閘道裝置版本的備註適用於

每月維護更新可能會導致服務短暫中斷。閘道的 VM 主機不需要在更新期間重新啟動，但閘道會在閘道設備更新和重新啟動時暫時無法使用。您可以透過增加 iSCSI 啟動器的逾時，將因閘道重新啟動而導致應用程式中斷的可能性降至最低。如需為 Windows 和 Linux 增加 iSCSI 啟動器逾時的詳細資訊，請參閱 自訂 Windows iSCSI 設定和 自訂 Linux iSCSI 設定。

部署和啟用閘道時，會設定預設的每週維護時段排程。您可以隨時修改維護時段排程。您也可以關閉每月維護更新，但我們建議您將其保持開啟狀態。

> **Note**
>
> 即使定期維護更新已關閉，緊急更新有時也會根據維護時段排程套用。

在將任何更新套用至閘道之前， 會在 Storage Gateway 主控台和您的 上 AWS 通知您訊息 AWS Health Dashboard。如需詳細資訊，請參閱AWS Health Dashboard。若要修改傳送軟體更新通知的電子郵件地址，請參閱 AWS 帳戶管理參考指南 中的更新帳戶的替代聯絡人。 AWS

更新可用時，閘道詳細資訊索引標籤會顯示維護訊息。您也可以在詳細資訊索引標籤上查看上次成功更新的日期和時間。

開啟或關閉維護更新

開啟維護更新時，閘道會根據設定的維護時段排程自動套用這些更新。如需詳細資訊，請參閱 。

如果維護更新已關閉，閘道不會自動套用這些更新，但您可以隨時使用 Storage Gateway 主控台、API或 手動套用這些更新CLI。無論此設定為何，緊急更新有時會在您設定的維護時段期間套用。

> **Note**
>
> 下列程序說明如何使用 Storage Gateway 主控台開啟或關閉閘道更新。若要使用 以程式設計方式變更此設定API，請參閱 Storage Gateway 參考 UpdateMaintenanceStartTime中的 。Storage Gateway API

若要使用 Storage Gateway 主控台開啟或關閉維護更新：

1. 開啟位於首頁 的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/

2. 在導覽窗格中，選擇閘道 ，然後選擇您要設定維護更新的閘道。
3. 選擇動作 ，然後選擇編輯維護設定 。
4. 針對維護更新 ，選取開啟或關閉 。
5. 完成後選擇儲存變更。

您可以在 Storage Gateway 主控台中驗證所選閘道的詳細資訊索引標籤上的更新設定。

修改閘道維護時段排程

如果開啟維護更新，閘道會根據維護時段排程自動套用這些更新。無論您的維護更新設定為何，緊急更新有時都會在您設定的維護時段期間套用。

> **Note**
>
> 下列程序說明如何使用 Storage Gateway 主控台修改維護時段排程。若要使用 以程式設計方式變更此設定API，請參閱 Storage Gateway 參考 UpdateMaintenanceStartTime中的 。Storage Gateway API

若要使用 Storage Gateway 主控台修改維護時段排程：

1. 開啟位於首頁 的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/
2. 在導覽窗格中，選擇閘道 ，然後選擇您要設定維護更新的閘道。
3. 選擇動作 ，然後選擇編輯維護設定 。
4. 在維護時段開始時間 下，執行下列動作：

    a. 針對排程 ，選擇每週或每月以設定維護時段節奏。

    b. 如果您選擇每週 ，請修改星期幾和時間的值，以在每週開始維護時段期間設定特定點。

    如果您選擇每月 ，請修改當月日期的值和時間，以設定每個月開始維護時段的特定點。

    > **Note**
    >
    > 可以為月份中的日期設定的最大值為 28。無法將維護排程設定為從第 29 天到第 31 天開始。
    > 如果您在設定此設定時收到錯誤，可能表示閘道軟體已過時。考慮先手動更新閘道，然後嘗試再次設定維護時段排程。

5. 完成後，選擇儲存變更。

您可以在 Storage Gateway 主控台中驗證所選閘道的詳細資訊索引標籤上的更新設定。

手動套用更新

如果閘道有可用的軟體更新，您可以依照下列程序手動套用。即使維護更新已關閉，此手動更新程序仍會忽略維護時段排程並立即套用更新。

> **Note**
>
> 下列程序說明如何使用 Storage Gateway 主控台手動套用更新。若要使用 以程式設計方式執行此動作API，請參閱 Storage Gateway 參考 UpdateGatewaySoftwareNow 中的 。 Storage Gateway API

若要使用 Storage Gateway 主控台手動套用閘道軟體更新：

1. 開啟位於首頁 的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/
2. 在導覽窗格中，選擇閘道 ，然後選擇您要更新的閘道。

   如果更新可用，主控台會在閘道詳細資訊索引標籤上顯示藍色通知橫幅，其中包含套用更新的選項。
3. 選擇立即套用更新，以立即更新閘道。

   > **Note**
   >
   > 此操作會在更新安裝時暫時中斷閘道功能。在此期間，閘道狀態會顯示在 Storage Gateway 主控台OFFLINE中。更新完成安裝後，閘道會繼續正常操作，且其狀態會變更為RUNNING。

您可以在 Storage Gateway 主控台中檢查所選閘道的詳細資訊索引標籤，以確認閘道軟體已更新至最新版本。

關閉閘道 VM

您可能需要基於維護而關機或重新啟動 VM，例如將修補程式套用至虛擬化管理程序時。關機 VM 之前，必須先停止閘道。雖然本節著重於使用 Storage Gateway 管理主控台啟動和停止閘道，但您也可以使用 VM 本機主控台或 Storage Gateway 來停止閘道API。當您開啟 VM 的電源時，請記得重新啟動閘道。

> **Important**
>
> 如果您停止並啟動使用暫時性儲存的 Amazon EC2閘道，閘道將永久離線。會發生此情況是因為已替換實體儲存磁碟。沒有解決此問題的解決方法。唯一的解決方法是刪除閘道，並在新的EC2執行個體上啟用新的閘道。

> **Note**
>
> 如果您在備份軟體寫入或讀取磁帶時停止閘道，則寫入或讀取任務可能不會成功。停止閘道之前，應該檢查備份軟體以及任何進行中任務的備份排程。

- 閘道 VM 本機主控台：請參閱 登入磁帶閘道本機主控台。
- Storage Gateway API- — 請參閱 ShutdownGateway

啟動和停止磁帶閘道

停止磁帶閘道

1. 開啟家用 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/
2. 在導覽窗格中，選擇 Gateways (閘道)，然後選擇要停止的閘道。閘道的狀態為 Running (正在執行)。
3. 在 Actions (動作) 選單上，選擇 Stop gateway (停止閘道)，並從對話方塊確認閘道 ID，然後選擇 Stop gateway (停止閘道)。

   閘道停止時，您可能會看到訊息，指出閘道的狀態。閘道關閉時，訊息和 Start gateway (啟動閘道) 按鈕會出現在 Details (詳細資訊) 標籤中。

當您停止閘道時，除非您啟動儲存，否則將無法存取儲存資源。如果閘道在停止時正在上傳資料，則會在您啟動閘道時繼續上傳。

啟動磁帶閘道

1. 開啟位於首頁 的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/
2. 在導覽窗格中，選擇 Gateways (閘道)，然後選擇要啟動的閘道。閘道的狀態為 Shutdown (關機)。
3. 選擇詳細資訊，然後選擇啟動閘道。

刪除閘道並移除相關資源

如果您不打算繼續使用閘道，請考慮刪除閘道和其相關聯資源。移除資源可避免產生您不打算繼續使用之資源的費用，並協助降低每月帳單。

當您刪除閘道時，它不會再出現在 AWS Storage Gateway 管理主控台上，而且與啟動器的 i SCSI 連線也會關閉。所有閘道類型的閘道刪除程序都會相同；不過，根據您要刪除的閘道類型以及在其上部署它的主機，您會遵循特定說明來移除相關聯資源。

> **Note**
>
> 刪除磁帶閘道時，目前處於AVAILABLE狀態的任何磁帶也會被刪除，而且這些磁帶上的任何資料都會遺失。如果要保留要刪除之閘道正在使用的磁帶中的資料，則必須先封存磁帶，然後才能刪除閘道。如需詳細資訊，請參閱存檔虛擬磁帶。

您可以使用 Storage Gateway 主控台或以程式設計方式來刪除閘道。您可以在以下內容中找到如何使用 Storage Gateway 主控台刪除閘道的相關資訊。如果您想要以程式設計方式刪除閘道，請AWS Storage Gateway API參閱參考。

主題

- 使用 Storage Gateway 主控台刪除閘道
- 從內部部署的閘道移除資源
- 從 Amazon EC2 執行個體上部署的閘道移除資源

使用 Storage Gateway 主控台刪除閘道

所有閘道類型的閘道刪除程序都相同。不過，根據您要刪除的閘道類型以及在其上部署閘道的主機，您可能需要執行額外任務才能移除與閘道建立關聯的資源。移除這些資源可協助您避免支付不打算使用之資源的費用。

> **Note**
>
> 對於部署在 Amazon EC2 執行個體上的閘道，執行個體會一直存在，直到您將其刪除為止。針對虛擬機器 (VM) 上所部署的閘道，在您刪除閘道之後，閘道 VM 仍然會存在於您的虛擬化環境中。若要移除虛擬機器，請使用用VMware vSphere 戶端、Microsoft Hyper-V 管理員或 Linux 核心型虛擬機器 (KVM) 用戶端連線至主機並移除虛擬機器。請注意，您無法重複使用已刪除的閘道 VM 來啟用新的閘道。

刪除閘道

1. 在https://console.aws.amazon.com/storagegateway/首頁開啟 Storage Gateway 主控台。
2. 選擇閘道，然後選取要刪除的一個或多個閘道。
3. 針對 Actions (動作)，選擇 Delete gateway (刪除閘道)。出現確認對話方塊。

   > **Warning**
   >
   > 執行此步驟之前，請確定目前沒有應用程式寫入至閘道的磁碟區。如果您刪除使用中的閘道，則資料可能會遺失。閘道一旦刪除，就沒有方法可以取回。

4. 確認您要刪除指定的閘道，然後在確認方塊中輸入刪除一詞，然後選擇刪除。
5. (選用) 如果您想要提供有關已刪除閘道的意見回饋，請完成意見回饋對話方塊，然後選擇提交。否則，請選擇略過。

> **Important**
>
> 刪除閘道後，您不再支付軟體費用，但虛擬磁帶、Amazon 彈性區塊存放區 (AmazonEBS) 快照和 Amazon EC2 執行個體等資源仍然存在。您將會繼續支付這些資源的費用。您可以選擇通過取消 EC2 Amazon EC2 訂閱來刪除 Amazon 實例和 Amazon EBS 快照。如果您想保留 Amazon EC2 訂閱，可以使用 Amazon EC2 控制台刪除 Amazon EBS 快照。

從內部部署的閘道移除資源

您可以使用下列說明，從內部部署的閘道移除資源。

從 VM 上所部署的磁帶閘道移除資源

刪除閘道 — 虛擬磁帶媒體櫃 (VTL) 時，請在刪除閘道之前和之後執行其他清理步驟。這些額外步驟可協助您移除不需要的資源，這樣您就不需要繼續支付其費用。

如果您要刪除的磁帶閘道部署在虛擬機器 (VM) 上，則建議您採取下列動作來清除資源。

> **Important**
>
> 在您刪除磁帶閘道之前，必須取消所有磁帶擷取操作，並退出所有擷取磁帶。
> 在您刪除磁帶閘道之後，必須移除任何與磁帶閘道建立關聯且不需要的資源，以避免支付這些資源的費用。

當您刪除磁帶閘道時，可能會遇到下列兩個案例中的其中一個。

- 磁帶閘道已連線到 AWS — 如果磁帶閘道已連線到 AWS 且您刪除閘道，則與閘道相關聯的 i SCSI 目標 (亦即虛擬磁帶機和媒體轉換器) 將無法再使用。
- 磁帶閘道未連線至 AWS — 如果磁帶閘道未連線至 (例如 AWS，如果基礎虛擬機器已關閉或網路已關閉)，則您無法刪除閘道。如果您嘗試這樣做，在您的環境備份並執行之後，您可能會有磁帶閘道在內部部署執行，其中包含可用的 i SCSI 目標。不過，不會將磁帶閘道資料上傳至或從中下載 AWS。

如果您要刪除的磁帶閘道未正常運作，則必須先停用它再予以刪除，如下所述：

- 若要從媒體櫃刪除狀態為RETRIEVED狀態的磁帶，請使用備份軟體退出磁帶。如需指示，請參閱封存磁帶。

停用磁帶閘道並刪除磁帶之後，即可刪除磁帶閘道。如需如何刪除閘道的說明，請參閱 使用 Storage Gateway 主控台刪除閘道。

如果您已存檔磁帶，則會保留這些磁帶，而且除非您刪除儲存，否則您會繼續支付其費用。如需如何從存檔刪除磁帶的說明，請參閱從磁帶閘道刪除虛擬磁帶。

> **Important**
>
> 您會支付存檔中的虛擬磁帶最少 90 天的儲存費用。如果您擷取已存放在存檔少於 90 天的虛擬磁帶，則仍然會支付 90 天的儲存費用。

從 Amazon EC2 執行個體上部署的閘道移除資源

如果您想要刪除在 Amazon EC2 執行個體上部署的閘道，建議您清理閘道所使用的 AWS 資源，特別是 Amazon EC2 執行個體、任何 Amazon 磁EBS碟區，以及部署磁帶閘道的磁帶。這樣做有助於避免意外的使用費。

從 Amazon 上部署的磁帶閘道移除資源 EC2

如果您已部署磁帶閘道，則建議您採取下列動作來刪除閘道以及清除其資源：

1. 刪除您已擷取至磁帶閘道的所有虛擬磁帶。如需詳細資訊，請參閱從磁帶閘道刪除虛擬磁帶。
2. 從磁帶館刪除所有虛擬磁帶。如需詳細資訊，請參閱從磁帶閘道刪除虛擬磁帶。
3. 刪除磁帶閘道。如需詳細資訊，請參閱使用 Storage Gateway 主控台刪除閘道。
4. 終止所有 Amazon EC2 實例，並刪除所有 Amazon EBS 卷。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的清理執行個體和磁碟區。
5. 刪除所有存檔虛擬磁帶。如需詳細資訊，請參閱從磁帶閘道刪除虛擬磁帶。

> **Important**
>
> 您會支付存檔中的虛擬磁帶最少 90 天的儲存費用。如果您擷取已存放在存檔少於 90 天的虛擬磁帶，則仍然會支付 90 天的儲存費用。

使用本機主控台執行維護任務

本節包含下列主題，提供如何使用閘道裝置本機主控台執行維護任務的相關資訊。本機主控台直接在託管閘道設備的虛擬化主機平台上執行。對於內部部署閘道，您可以透過 VMware、Hyper-v 或 Linux KVM虛擬化主機存取本機主控台。對於 Amazon EC2閘道，您可以使用 連線至 Amazon EC2執行個體來存取主控台SSH。大多數任務在不同的主機平台上都是常見的，但也有一些差異。

主題

- 存取閘道本機主控台 - 了解如何登入本機主控台，以託管在 Linux 核心型虛擬機器 （KVM）ESXi、VMware 或 Microsoft Hyper-V Manager 平台上的內部部署閘道。
- 在 VM 本機主控台上執行任務 - 了解如何使用本機主控台執行內部部署閘道的基本設定和進階組態任務，例如設定HTTP代理、檢視系統資源狀態或執行終端機命令。
- 在 Amazon EC2 Local Console 上執行任務 - 了解如何登入本機主控台，以執行 Amazon EC2閘道的基本設定和進階組態任務，例如設定HTTP代理、檢視系統資源狀態或執行終端機命令。

存取閘道本機主控台

如何存取您的 VM 的本機主控台，取決於您的閘道 VM 部署所在的 Hypervisor 類型。在本節中，您可以找到如何使用 Linux 核心型虛擬機器 （KVM）ESXi、 VMware 和 Microsoft Hyper-V Manager 存取 VM 本機主控台的相關資訊。

主題

- 使用 Linux 存取閘道本機主控台 KVM
- 使用 存取閘道本機主控台 VMware ESXi
- 使用 Microsoft Hyper-V 存取閘道本機主控台

使用 Linux 存取閘道本機主控台 KVM

設定在 上執行的虛擬機器有各種不同的方法KVM，取決於使用的 Linux 發行版本。從命令列存取KVM組態選項的指示如下。指示可能會因KVM實作而有所不同。

使用 存取閘道的本機主控台 KVM

1. 使用下列命令來列出目前 VMs 中可用的 KVM。

```
# virsh list
```

命令會傳回每個 ID VMs為 、名稱為 和狀態資訊的 清單。請注意您要為其啟動閘道本機主控台Id的 VM 的 。

2. 使用下列命令來存取本機主控台。

```
# virsh console Id
```

Replace (取代) *Id* 您在上一個步驟中記下的 VM ID。

AWS Appliance 閘道本機主控台會提示您登入，以變更網路組態和其他設定。

3. 輸入您的使用者名稱和密碼以登入閘道本機主控台。如需詳細資訊，請參閱登入磁帶閘道本機主控台 。

登入後，會顯示 AWS Appliance Activation - Configuration 功能表。您可以從選單選項中選取 來執行閘道組態任務。如需詳細資訊，請參閱在虛擬機器本機主控台上執行任務

使用 存取閘道本機主控台 VMware ESXi

使用 存取閘道的本機主控台 VMware ESXi

1. 在VMware vSphere 用戶端中，選取閘道 VM。
2. 確定閘道 VM 已開啟。

> **Note**
>
> 如果您的閘道 VM 已開啟，應用程式視窗左側的 VM 瀏覽器面板中會出現一個綠色箭頭圖示，其中包含 VM 圖示。如果您的閘道 VM 未開啟，您可以選擇應用程式視窗頂端工具列上的綠色開啟電源圖示來開啟它。

3. 選擇應用程式視窗右側的主資訊面板中的主控台索引標籤。

經過幾分鐘之後， AWS 設備閘道本機主控台會提示您登入，以變更網路組態和其他設定。

> **Note**
>
> 若要從主控台視窗釋出該游標，請按Ctrl+Alt。

4. 輸入您的使用者名稱和密碼以登入閘道本機主控台。如需詳細資訊，請參閱登入磁帶閘道本機主控台。

   登入後，會顯示 AWS Appliance Activation - Configuration 功能表。您可以從選單選項中選取 來執行閘道組態任務。如需詳細資訊，請參閱在虛擬機器本機主控台上執行任務

使用 Microsoft Hyper-V 存取閘道本機主控台

存取您閘道的本機主控台 (Microsoft Hyper-V)

1. 從 Microsoft Hyper-V Manager 應用程式視窗左側的虛擬機器面板中選取閘道設備 VM。
2. 確定已開啟閘道。

> **Note**
>
> 如果您的閘道 VM 已開啟， `Running` 會顯示在應用程式視窗左側虛擬機器面板中 VM 的狀態欄中。如果您的閘道 VM 未開啟，您可以在應用程式視窗右側的動作面板中選擇開始來開啟它。

3. 從動作面板選擇連線。

   Virtual Machine Connection (虛擬機器連線) 視窗即會顯示。若出現身分驗證視窗，請輸入虛擬化管理程序管理員提供給您的登入憑證。

   經過幾分鐘之後， AWS 設備閘道本機主控台會提示您登入，以變更網路組態和其他設定。

4. 輸入您的使用者名稱和密碼以登入閘道本機主控台。如需詳細資訊，請參閱登入磁帶閘道本機主控台。

   登入後，會顯示 AWS Appliance Activation - Configuration 功能表。您可以從選單選項中選取 來執行閘道組態任務。如需詳細資訊，請參閱在虛擬機器本機主控台上執行任務

在 VM 本機主控台上執行任務

對於您部署內部部署的磁帶閘道，您可以使用您從虛擬機器主機平台存取的閘道本機主控台執行下列維護任務。這些任務常見於 VMware、Microsoft Hyper-V 和 Linux 核心型虛擬機器 （KVM） 虛擬機器監視器。

主題

- 登入磁帶閘道本機主控台 - 了解如何登入閘道本機主控台，您可以在其中設定閘道網路設定並變更預設密碼。
- 為您的內部部署閘道設定SOCKS5代理 - 了解如何設定 Storage Gateway，透過 Socket Secure 第 5 版 （SOCKS5） 代理伺服器路由所有 AWS 端點流量。
- 設定您的閘道網路 - 了解如何設定閘道以使用或DHCP指派靜態 IP 地址。
- 測試您的閘道連線至網際網路 - 了解如何使用閘道本機主控台來測試閘道與網際網路之間的連線。
- 在本機主控台中執行內部部署閘道的儲存閘道命令 - 了解如何執行本機主控台命令，讓您執行其他任務，例如儲存路由表 AWS Support、連線至 等。
- 檢視閘道系統資源狀態 - 了解如何檢查閘道設備RAM可用的虛擬CPU核心、根磁碟區大小和 。

登入磁帶閘道本機主控台

當 VM 可供您登入時，將顯示登入畫面。如果這是您第一次登入本機主控台，請使用預設的憑證登入。這些預設的憑證可讓您存取設定閘道網路設定的選單，以及從本機主控台變更密碼。Storage Gateway 可讓您從 AWS Storage Gateway 主控台設定自己的密碼，而不是從本機主控台變更密碼。您不需要知道預設密碼就可以設定新的密碼。如需詳細資訊，請參閱從 Storage Gateway 主控台設定本機主控台密碼。

登入至閘道的本機主控台

- 如果這是您第一次登入本機主控台，請使用預設的登入資料登入 VM。預設使用者名稱為 `admin` 且密碼是 `password`。

  否則，請使用您的登入資料登入。

  > **Note**
  >
  > 建議您從 AWS 設備啟用 - 組態主功能表中輸入閘道主控台的對應數字，然後執行 `passwd` 指令，以變更預設密碼。如需如何執行命令的資訊，請參閱 在本機主控台中執行

內部部署閘道的儲存閘道命令。您也可以從 AWS Storage Gateway 主控台設定自己的密碼。如需詳細資訊，請參閱從 Storage Gateway 主控台設定本機主控台密碼。

> **Important**
>
> 對於舊版磁碟區或磁帶閘道，使用者名稱為 `sguser`，密碼為 `sgpassword`。如果您已重設密碼且閘道已更新至更新版本，使用者名稱將會變更為 admin，但仍會沿用相同的密碼

從 Storage Gateway 主控台設定本機主控台密碼

當您首次登入本機主控台時，請使用預設的憑證來登入：使用者名稱是 `admin`，密碼是 `password`。建議您一律在建立新閘道後立即設定新的密碼。如果您希望，您可以從 AWS Storage Gateway 主控台設定此密碼，而不是從本機主控台設定。您不需要知道預設密碼就可以設定新的密碼。

在 Storage Gateway 主控台中設定本機主控台密碼

1. 開啟位於首頁 的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/
2. 在導覽窗格上，選擇 Gateways (閘道)，然後選擇您要設定新密碼的閘道。
3. 對於 Actions (動作)，選擇 Set Local Console Password (設定本機主控台密碼)。
4. 在 Set Local Console Password (設定本機主控台密碼) 對話方塊中，輸入新的密碼、確認密碼，然後選擇 Save (儲存)。您的新密碼會取代預設的密碼。Storage Gateway 不儲存密碼，而是將它安全地傳輸到 VM。

> **Note**
>
> 密碼可以包含鍵盤任一字元，長度為 1 到 512 個字元。

為您的內部部署閘道設定SOCKS5代理

磁碟區閘道和磁帶閘道支援在內部部署閘道和 之間設定 Socket Secure 第 5 版 （ SOCKS5 ） 代理 AWS。

> **Note**
>
> 唯一支援的代理組態是 SOCKS5。

如果您的閘道必須使用代理伺服器與網際網路通訊，則需要設定閘道的SOCKS代理設定。您透過指定 IP 地址和執行代理的主機連接埠號碼，來完成此作業。完成此作業後，Storage Gateway 會透過您的代理伺服器路由所有流量。如需閘道之網路需求的資訊，請參閱網路與防火牆需求。

下列程序說明如何設定磁碟區閘道和磁帶閘道的SOCKS代理。

設定磁碟區和磁帶閘道的SOCKS5代理

1. 登入您閘道的本機主控台。
   - VMware ESXi – 如需詳細資訊，請參閱 使用 存取閘道本機主控台 VMware ESXi。
   - Microsoft Hyper-V：如需詳細資訊，請參閱 使用 Microsoft Hyper-V 存取閘道本機主控台。
   - KVM – 如需詳細資訊，請參閱 使用 Linux 存取閘道本機主控台 KVM。
2. 從 AWS Storage Gateway - Configuration 主功能表中，輸入對應的數字以選取 SOCKS Proxy Configuration 。
3. 從 AWS Storage Gateway SOCKS Proxy Configuration 功能表中，輸入對應的數字來執行下列其中一個任務：

執行此任務	執行此作業
設定SOCKS代理	輸入對應的數字以選取設定 SOCKS Proxy 。 您需要提供主機名稱和連接埠才能完成設定。
檢視目前的SOCKS代理組態	輸入對應的數字，以選取檢視目前的SOCKS代理伺服器組態 。 如果未設定SOCKS代理，則`SOCKS Proxy not configured` 會顯示訊息。如果設定SOCKS代理，則會顯示代理的主機名稱和連接埠。

執行此任務	執行此作業
移除SOCKS代理組態	輸入對應的數字以選取移除SOCKS代理組態 。 會顯示訊息 `SOCKS Proxy Configuration Removed` 。

4. 重新啟動您的 VM 以套用您的HTTP組態。

設定您的閘道網路

閘道的預設網路組態是動態主機組態通訊協定 （DHCP）。透過 DHCP，您的閘道會自動指派 IP 地址。在某些情況下，您可能需要手動指派您的閘道 IP 為靜態 IP 地址，如下所述。

設定您的閘道使用靜態 IP 地址

1. 登入您閘道的本機主控台。
   - VMware ESXi – 如需詳細資訊，請參閱 使用 存取閘道本機主控台 VMware ESXi。
   - Microsoft Hyper-V：如需詳細資訊，請參閱 使用 Microsoft Hyper-V 存取閘道本機主控台。
   - KVM – 如需詳細資訊，請參閱 使用 Linux 存取閘道本機主控台 KVM。
2. 從 AWS Storage Gateway - 組態主功能表中，輸入對應的數字以選取網路組態。
3. 從 AWS Storage Gateway 網路組態功能表中，執行下列其中一項工作：

執行此任務	執行此作業
說明網路轉接器	輸入對應的數字以選取描述介面卡。 隨即顯示介面卡名稱的清單，系統會提示您輸入介面卡名稱例如 **`eth0`**。若您指定的轉接器為使用中，將顯示轉接器的下列資訊： • 媒體存取控制 （MAC） 地址 • IP 地址 •

執行此任務	執行此作業
	網路遮罩 • 閘道 IP 地址 • DHCP 啟用狀態 當您設定靜態 IP 地址或設定閘道的預設介面卡時，可以使用此處列出的介面卡名稱。
設定 DHCP	輸入對應的數字以選取設定 DHCP。 系統會提示您將網路介面設定為使用 DHCP。

執行此任務	執行此作業
為閘道設定靜態 IP 地址	輸入對應的數字以選取設定靜態 IP。 系統會提示您輸入下列資訊來設定靜態 IP： • 網路轉接器名稱 • IP 地址 • 網路遮罩 • 預設閘道地址 • 主要網域名稱服務（DNS）地址 • 次要DNS地址 **Important** 如果您的閘道已啟用，您必須將其關閉並在 Storage Gateway 主控台重新啟動，設定才能生效。如需詳細資訊，請參閱關閉閘道 VM。 如果您的閘道使用多個網路介面，您必須將所有啟用的介面設定為使用 DHCP或靜態 IP 地址。 例如，假設閘道 VM 使用設定為 的兩個介面 DHCP。如果您稍後將一個界面設定為靜態 IP，另一個界面將停用。在此情況下，若要啟用界面，您必須將其設定為靜態 IP。

執行此任務	執行此作業
	如果兩個介面最初都設定為使用靜態 IP 地址，然後您將閘道設定為使用 DHCP，則兩個介面都會使用 DHCP。
設定閘道的主機名稱	輸入對應的數字以選取設定主機名稱。 系統會提示您選擇閘道將使用您指定的靜態主機名稱，或透過 DCHP或 r 自動取得DNS。 如果選取靜態 ，系統會提示您提供靜態主機名稱，例如 `testgateway.example.com` 。輸入 y 以套用組態。 **Note** 如果您為閘道設定靜態主機名稱，請確定提供的主機名稱位於閘道加入的網域中。您還必須在DNS系統中建立記錄，將閘道的 IP 地址指向其靜態主機名稱。
將閘道的所有網路組態重設為 DHCP	輸入對應的數字以選取將所有 重設為 DHCP。 所有網路介面都會設定為使用 DHCP。 **Important** 如果您的閘道已啟用，您必須將其關閉並在 Storage Gateway 主控台重新啟動您的閘道，設定才能生效。如需詳細資訊，請參閱關閉閘道 VM。

執行此任務	執行此作業
設定閘道的預設路由轉接器	輸入對應的數字以選取設定預設介面卡。 隨即顯示閘道可用的介面卡，系統會提示您選取其中一個介面卡例如 **eth0**。
檢視閘道的DNS組態	輸入對應的數字以選取檢視DNS組態 。 隨即顯示主要和次要DNS名稱伺服器的 IP 地址。
檢視路由表	輸入對應的數字以選擇檢視路線。 隨即顯示閘道的預設路由。

測試您的閘道連線至網際網路

您可使用閘道的本機主控台測試網際網路連線。此測試在您故障診斷閘道的網路問題時，很有幫助。

測試閘道的網際網路連線

1. 登入您閘道的本機主控台。
   - VMware ESXi – 如需詳細資訊，請參閱 使用 存取閘道本機主控台 VMware ESXi。
   - Microsoft Hyper-V：如需詳細資訊，請參閱 使用 Microsoft Hyper-V 存取閘道本機主控台。
   - KVM – 如需詳細資訊，請參閱 使用 Linux 存取閘道本機主控台 KVM。
2. 從 AWS Storage Gateway - 組態主功能表中，輸入對應的數字以選取測試網路連線。

   如果您的閘道已經啟動，連線測試會立即開始。對於尚未啟用的閘道，您必須指定端點類型和，AWS 區域 如下列步驟所述。
3. 如果您的閘道尚未啟動，請輸入對應的數字以選取閘道的端點類型。
4. 如果您選擇公有端點類型，請輸入對應的數字，以選取要測試 AWS 區域 的 。如需 支援的 AWS 和服務端點 AWS 區域 清單 Storage Gateway ，請參閱 中的AWS Storage Gateway 端點和配額AWS 一般參考。

隨著測試進行，每個端點會顯示 【PASSED】 或 【FAILED】 ，指出連線的狀態，如下所示：

訊息	描述
[PASSED]	Storage Gateway 具有網路連線能力。
[FAILED]	Storage Gateway 沒有網路連線能力。

在本機主控台中執行內部部署閘道的儲存閘道命令

Storage Gateway 中的 VM 本機主控台可協助提供用於設定和診斷閘道問題的安全環境。使用本機主控台命令，您可以執行維護任務，例如儲存路由表 AWS Support、連線至 等。

執行組態或診斷命令

1. 登入您閘道的本機主控台：
   - 如需登入VMwareESXi本機主控台的詳細資訊，請參閱 使用 存取閘道本機主控台 VMware ESXi。
   - 如需登入 Microsoft Hyper-V 本機主控台的詳細資訊，請參閱使用 Microsoft Hyper-V 存取閘道本機主控台。
   - 如需登入KVM本機主控台的詳細資訊，請參閱 使用 Linux 存取閘道本機主控台 KVM。
2. 從 AWS 設備啟用 - 設定主功能表中，輸入對應的數字以選取閘道主控台。
3. 在閘道主控台命令提示字元中，輸入 **h**。

   主控台會顯示 AVAILABLECOMMANDS選單，其中列出可用的命令：

Command	函式
dig	從挖掘收集輸出以進行DNS疑難排解。
exit	傳回組態功能表。
h	顯示可用的命令清單。
ifconfig	檢視或設定網路介面。

Command	函式
	Note 建議您使用 Storage Gateway 主控台或專用的本機主控台功能表選項來設定網路或 IP 設定。如需指示，請參閱設定閘道網路。
ip	顯示/操作路由、裝置和通道。 **Note** 建議您使用 Storage Gateway 主控台或專用的本機主控台功能表選項來設定網路或 IP 設定。如需指示，請參閱設定閘道網路。
iptables	IPv4 封包篩選和 的管理工具NAT。
ncport	測試網路上特定TCP連接埠的連線能力。
nping	從 nping 收集輸出以進行網路疑難排解。
open-support-channel	連線至 AWS 支援。
passwd	更新身份驗證令牌。
save-iptables	持續存取 IP 資料表。
save-routing-table	儲存新增的路由表項目。

Command	函式
sslcheck	使用憑證發行者傳回輸出 **Note** Storage Gateway 使用憑證發行者驗證，不支援 ssl 檢查。如果此命令傳回 aws-appliance@amazon.com 以外的發行者，則應用程式可能會執行 ssl 檢查。在這種情況下，我們建議略過 Storage Gateway 設備的 ssl 檢查。
tcptraceroute	收集目的地TCP流量的追蹤路由輸出。

4. 在閘道主控台命令提示字元中，輸入您要使用之功能的對應指令，然後依照指示進行。

若要了解命令，請輸入 **man** + *command name* 命令提示字元。

檢視閘道系統資源狀態

當您的閘道啟動時，它會檢查其虛擬CPU核心、根磁碟區大小和 RAM。然後判斷這些系統資源是否足夠閘道正常運作。您可以在閘道的本機主控台上檢視此檢查的結果。

檢視系統資源檢查的狀態

1. 登入您閘道的本機主控台：
   - 如需登入VMwareESXi主控台的詳細資訊，請參閱 使用 存取閘道本機主控台 VMware ESXi。
   - 如需登入 Microsoft Hyper-V 本機主控台的詳細資訊，請參閱使用 Microsoft Hyper-V 存取閘道本機主控台。
   - 如需登入KVM本機主控台的詳細資訊，請參閱 使用 Linux 存取閘道本機主控台 KVM。
2. 從 AWS 設備啟用 - 組態主功能表中，輸入相應數字以選取檢視系統資源檢查的結果。

   每個資源都會顯示 【OK】、【WARNING】 或 【FAIL】，指出資源的狀態，如下所示：

訊息	描述
[OK]	此資源已通過系統資源檢查。
[WARNING]	此資源未符合建議的要求，但您的閘道會繼續運作。Storage Gateway 會顯示說明資源檢查結果的訊息。
[FAIL]	此資源未符合最低要求。您的閘道可能無法正常運作。Storage Gateway 會顯示說明資源檢查結果的訊息。

主控台也會在資源檢查選單選項旁顯示錯誤和警告的數量。

在 Amazon EC2 Local Console 上執行任務

某些 Storage Gateway 維護任務需要您登入閘道本機主控台，才能在 Amazon EC2執行個體上部署閘道。您可以使用 Secure Shell （ SSH ） 用戶端存取 Amazon EC2執行個體上的閘道本機主控台。本節中的主題說明如何登入閘道本機主控台並執行維護任務。

主題

- 登入您的 Amazon EC2 Gateway Local Console - 了解如何使用 Secure Shell （ SSH ） 用戶端來連接和登入 Amazon EC2執行個體的閘道本機主控台。
- EC2 透過HTTP代理在 上部署閘道的路由 - 了解如何設定 Storage Gateway，透過 Socket Secure 第 5 版 （ SOCKS5 ） 代理伺服器將所有 AWS enpoint 流量路由至您的 Amazon EC2閘道執行個體。
- 測試閘道網路連線 - 了解如何使用閘道本機主控台來測試閘道與各種網路資源之間的網路連線。
- 檢視閘道系統資源狀態 - 了解如何使用閘道本機主控台來檢查閘道設備RAM可用的虛擬CPU核心、根磁碟區大小和 。
- 在本機主控台上執行 Storage Gateway 命令 - 了解如何執行本機主控台命令，讓您執行其他任務，例如儲存路由表 AWS Support、連線至 等。

登入您的 Amazon EC2 Gateway Local Console

您可以使用 Secure Shell （ SSH ） 用戶端連線至 Amazon EC2執行個體。如需詳細資訊，請參閱 Amazon EC2使用者指南 中的連線至您的執行個體。若要以這種方式連線，您需要在啟動執行個體時指定的SSH金鑰對。如需有關 Amazon EC2金鑰對的資訊，請參閱 Amazon 使用者指南中的 Amazon EC2金鑰對。 EC2

登入至閘道本機主控台

1. 登入您的本機主控台。如果您要從 Windows 電腦連線至EC2執行個體，請以 admin 身分登入。
2. 登入之後，您會看到 AWS Storage Gateway - 組態主功能表，您可以從中執行各種工作。

若要了解此項	請參閱此主題
為您的閘道設定SOCKS代理	EC2 透過HTTP代理在 上部署閘道的路由
測試網路連線	測試閘道網路連線
執行 Storage Gateway 主控台命令	在本機主控台上執行 Storage Gateway 命令
檢視系統資源檢查	檢視閘道系統資源狀態.

若要關閉閘道，請輸入 **0**。

若要結束組態工作階段，請輸入 **x**。

EC2 透過HTTP代理在 上部署閘道的路由

Storage Gateway 支援在部署在 Amazon EC2和 上的閘道之間設定 Socket Secure 第 5 版 （ SOCKS5 ） 代理 AWS。

如果您的閘道必須使用代理伺服器與網際網路通訊，則需要設定閘道的HTTP代理設定。您透過指定 IP 地址和執行代理的主機連接埠號碼，來完成此作業。這麼做之後，Storage Gateway 會透過代理伺服器路由所有 AWS 端點流量。即使使用HTTP代理，閘道和端點之間的通訊也會加密。

透過本機代理伺服器路由您的閘道網際網路流量

1. 登入您閘道的本機主控台。如需說明，請參閱 登入您的 Amazon EC2 Gateway Local Console。

2. 從 AWS Appliance Activation - Configuration 主功能表中，輸入對應的數字，以選取設定 HTTP Proxy 。
3. 從 AWS Appliance Activation HTTP Proxy Configuration 功能表中，輸入您要執行之任務的對應數字：

   - 設定HTTP代理 - 您需要提供主機名稱和連接埠才能完成組態。
   - 檢視目前的HTTP代理組態 - 如果未設定HTTP代理，則`HTTP Proxy not configured`會顯示訊息。如果設定HTTP代理，則會顯示代理的主機名稱和連接埠。
   - 移除HTTP代理組態 - 訊息`HTTP Proxy Configuration Removed`隨即顯示。

測試閘道網路連線

您可使用閘道的本機主控台測試網路連線。此測試在您故障診斷閘道的網路問題時，很有幫助。

測試閘道的連線

1. 登入您閘道的本機主控台。如需說明，請參閱 登入您的 Amazon EC2 Gateway Local Console。
2. 從 AWS 裝置啟用 - 組態主功能表中，輸入對應的數字以選取測試網路連線。

   如果您的閘道已經啟動，連線測試會立即開始。對於尚未啟用的閘道，您必須指定端點類型和，AWS 區域 如下列步驟所述。
3. 如果您的閘道尚未啟動，請輸入對應的數字以選取閘道的端點類型。
4. 如果選擇了公有端點類型，請輸入對應的數字，以選取要測試 AWS 區域 的 。如需 支援的 AWS 和服務端點 AWS 區域 清單，您可以搭配 Storage Gateway 使用，請參閱 中的AWS Storage Gateway 端點和配額AWS 一般參考。

隨著測試進行，每個端點會顯示 【PASSED】 或 【FAILED】 ，指出連線的狀態，如下所示：

訊息	描述
[PASSED]	Storage Gateway 具有網路連線能力。
[FAILED]	Storage Gateway 沒有網路連線能力。

檢視閘道系統資源狀態

當您的閘道啟動時，它會檢查其虛擬CPU核心、根磁碟區大小和 RAM。然後判斷這些系統資源是否足夠閘道正常運作。您可以在閘道的本機主控台上檢視此檢查的結果。

檢視系統資源檢查的狀態

1. 登入您閘道的本機主控台。如需說明，請參閱 登入您的 Amazon EC2 Gateway Local Console。
2. 從 AWS 設備啟用 - 組態主功能表中，輸入相應數字以選取檢視系統資源檢查的結果。

   每個資源都會顯示 【OK】、【WARNING】 或 【FAIL】，指出資源的狀態，如下所示：

訊息	描述
[OK]	此資源已通過系統資源檢查。
[WARNING]	此資源未符合建議的要求，但您的閘道會繼續運作。Storage Gateway 會顯示說明資源檢查結果的訊息。
[FAIL]	此資源未符合最低要求。您的閘道可能無法正常運作。Storage Gateway 會顯示說明資源檢查結果的訊息。

   主控台也會在資源檢查選單選項旁顯示錯誤和警告的數量。

在本機主控台上執行 Storage Gateway 命令

AWS Storage Gateway 主控台有助於提供安全的環境，以設定和診斷閘道的問題。您可以使用主控台命令來執行維護任務，例如儲存路由表或連線至 AWS Support。

執行組態或診斷命令

1. 登入您閘道的本機主控台。如需說明，請參閱 登入您的 Amazon EC2 Gateway Local Console。
2. 從 AWS 設備啟用 - 設定主功能表中，輸入對應的數字以選取閘道主控台。
3. 在閘道主控台命令提示字元中，輸入 h。

   主控台會顯示 AVAILABLECOMMANDS選單，其中列出可用的命令：

Command	函式
dig	從挖掘收集輸出以進行DNS疑難排解。
exit	傳回組態功能表。
h	顯示可用的命令清單。
ifconfig	檢視或設定網路介面。 **Note** 建議您使用 Storage Gateway 主控台或專用的本機主控台功能表選項來設定網路或 IP 設定。
ip	顯示/操作路由、裝置和通道。 **Note** 建議您使用 Storage Gateway 主控台或專用的本機主控台功能表選項來設定網路或 IP 設定。
iptables	IPv4 封包篩選和 的管理工具NAT。
ncport	測試網路上特定TCP連接埠的連線能力。
nping	從 nping 收集輸出以進行網路疑難排解。
open-support-channel	連線至 AWS 支援。
save-iptables	持續存取 IP 資料表。
save-routing-table	儲存新增的路由表項目。
sslcheck	檢查網路故障診斷SSL的有效性。

Command	函式
tcptraceroute	收集目的地TCP流量的追蹤路由輸出。

4. 在閘道主控台命令提示字元中，輸入您要使用之功能的對應指令，然後依照指示進行。

若要瞭解某個指令，請輸入指令名稱，然後輸入 -h 選項，如：`sslcheck -h`。

Tape Gateway 的效能和最佳化

本節說明 Storage Gateway 效能。

主題

適用於磁帶閘道的效能指引

在此章節，您可以找到為磁帶閘道 VM 佈建硬體的組態指引。資料表中列出的 Amazon EC2執行個體大小和類型是範例，僅供參考。

組態	寫入輸送量 (Gbps)	從快取讀取輸送量 (Gbps)	讀取來自 Amazon Web Services 雲輸送量 Gbps
主機平台：Amazon EC2執行個體 — c5.4xlarge CPU：16 vCPU | RAM：32 GB 根磁碟：80 GB、io1SSD、4，000 IOPS 快取磁碟：已分割 RAID（2 x 500 GB、io1 EBS SSD、25000 IOPs） 上傳緩衝磁碟：450 GB、io1 SSD、2000 IOPs 雲端的網路頻寬：10 Gbps	2.3	4.0	2.2
主機平台：Storage Gateway 硬體設備 快取磁碟：2.5 TB	2.3	8.8	3.8

組態	寫入輸送量 (Gbps)	從快取讀取輸送量 (Gbps)	讀取來自 Amazon Web Services 雲輸送量 Gbps
上傳緩衝磁碟：2 TB 雲端的網路頻寬：10 Gbps			
主機平台：Amazon EC2instance — c5d.9xlarge CPU：36 vCPU | RAM：72 GB 根磁碟：80 GB、io1SSD 、4，000 IOPS 快取磁碟：900 GB NVMe磁碟 上傳緩衝磁碟：900 GB NVMe磁碟 雲端的網路頻寬：10 Gbps	5.2	11.6	5.2
主機平台：Amazon EC2instance — c5d.metal CPU：96 vCPU | RAM：192 GB 根磁碟：80 GB、io1SSD 、4，000 IOPS 快取磁碟：分割 RAID（2 x 900 GB NVMe磁碟） 上傳緩衝磁碟：900 GB NVMe磁碟 雲端的網路頻寬：10 Gbps	5.2	11.6	7.2

> **Note**
>
> 同時使用 1 MB 區塊大小和十個磁帶磁碟即達成此效能。
> 上表中的EC2組態僅用於代表您在具有類似資源的實體伺服器上可能達到的效能。例如，使用條紋的EC2組態是透過我們在 上的閘道通常不支援的特殊機制RAID來完成EC2。為了達到類似的效能，您應該改用連接至執行閘道的內部部署伺服器的硬體RAID控制器。
> 效能可能會根據您的主機平台組態和網路頻寬而有所不同。

若要改善磁帶閘道的讀寫輸送量效能，請參閱 最佳化 iSCSI 設定、針對磁帶硬碟使用較大的區塊大小和 最佳化備份軟體中虛擬磁帶機的效能。

最佳化閘道效能

建議閘道伺服器組態

若要取得閘道的最佳效能，Storage Gateway 建議您為閘道的主機伺服器採用下列閘道組態：

- 至少 64 個專用實體CPU核心
- 對於磁帶閘道，您的硬體應專用以下金額的 RAM：
  - RAM 為快取大小高達 16 GiB的閘道預留至少 16 GiB TiB
  - 為快取大小RAM為 16 TiB GiB的閘道預留至少 32 TiB
  - 為快取大小RAM為 32 TiB GiB的閘道預留至少 4TiB

  > **Note**
  >
  > 為了獲得最佳閘道效能，您必須佈建至少 32 GiB 的 RAM。

- 磁碟 1，用作閘道快取，如下所示：
  - 由 NVMe 組成的條紋 RAID（獨立磁碟的備援陣列）SSDs。
- 磁碟 2，用作閘道上傳緩衝，如下所示：
  - 條紋RAID由 NVMe 組成SSDs。
- 磁碟 3，用作閘道上傳緩衝，如下所示：
  - 條紋RAID由 NVMe 組成SSDs。
- 在 VM 網路 1 上設定的網路轉接器 1：
  - 使用 VM 網路 1 並新增 VMXnet3（10 Gbps） 用於擷取。

- 在 VM 網路 2 上設定的網路轉接器 2：
  - 使用 VM 網路 2 並新增 VMXnet3（10 Gbps）來連線至 AWS。

新增資源至您的閘道

下列瓶頸可將磁帶閘道的效能降低到低於理論上持續輸送量上限（您的頻寬到 AWS 雲端）：

- CPU 核心計數
- 快取/上傳緩衝磁碟輸送量
- RAM 總金額
- 網路頻寬至 AWS
- 從啟動器到閘道的網路頻寬

本節包含最佳化閘道效能時可採取的步驟。本指南是以將資源新增至您的閘道或至您的應用程式伺服器為基礎。

您可以利用下列其中一或多個方法，將資源新增到您的閘道，以將閘道效能最佳化。

使用高效能磁碟

快取和上傳緩衝磁碟輸送量可能會限制閘道的上傳和下載效能。如果閘道的效能大幅低於預期效能，請考慮改善快取和上傳緩衝磁碟輸送量，方法如下：

- 使用如 10 RAID RAID等條紋來改善磁碟輸送量，最好使用硬體RAID控制器。

  > **Note**
  >
  > RAID（獨立磁碟的備援陣列）或特別是 10 RAID 等磁碟分割RAID組態，是將資料主體分割為區塊，並將資料區塊分散到多個儲存裝置的程序。您使用的RAID層級會影響您可以達到的確切速度和容錯能力。透過跨多個磁碟分割 IO 工作負載，RAID裝置的整體輸送量遠高於任何單一成員磁碟的總輸送量。

- 使用直接連接的高效能磁碟

  若要最佳化閘道效能，您可以新增高效能磁碟，例如固態硬碟（SSDs）和NVMe控制器。您也可以直接從儲存區域網路（SAN）而非 Microsoft Hyper-V 將虛擬磁碟連接至 VMNTFS。提升磁碟效能通常會提高輸送量，並提高每秒的輸入/輸出操作數（IOPS）。

若要測量輸送量，請使用 `ReadBytes`和 `WriteBytes`指標搭配 `Samples` Amazon CloudWatch 統計資料。例如，在 5 分鐘的取樣期間除以 300 秒的`ReadBytes`指標`Samples`統計資料會為您提供 IOPS。一般而言，當您檢閱閘道的這些指標時，請尋找低輸送量和低IOPS趨勢，以指出磁碟相關的瓶頸。如需閘道指標的詳細資訊，請參閱 測量磁帶閘道與 之間的效能 AWS。

> **Note**
>
> CloudWatch 指標並非適用於所有閘道。如需閘道指標的資訊，請參閱 監控 Storage Gateway。

新增更多上傳緩衝磁碟

若要達到更高的寫入輸送量，請至少新增兩個上傳緩衝磁碟。將資料寫入閘道時，資料會寫入並儲存在本機的上傳緩衝磁碟。之後，儲存的本機資料會以非同步方式在要處理的磁碟上讀取，並上傳至 AWS。新增更多上傳緩衝磁碟，可能會減少對每個磁碟執行的並行 I/O 作業數量。這可能會增加閘道的寫入輸送量。

具備個別實體磁碟的後端閘道虛擬磁碟

佈建閘道磁碟時，強烈建議您不要為使用相同基礎實體儲存體磁碟的上傳緩衝及快取儲存體佈建本機磁碟。例如，對於 VMware ESXi，基礎實體儲存資源會表示為資料存放區。當您部署閘道 VM 時，您會選擇要存放 VM 檔案的資料存放區。當您佈建虛擬磁碟 (例如：做為上傳緩衝) 時，您可以將虛擬磁碟存放在與 VM 相同或不同的資料存放區。

若您有超過一個資料存放區，我們強烈建議您為每一種您正在建立的本機儲存體類型選擇一個資料存放區。只用一個基礎實體磁碟支援的資料存放區，可能導致效能不佳。當您使用這種磁碟來同時支援快取儲存體和閘道設定中上傳緩衝的情形時，即為一個例子。同樣地，以效能較低的RAID組態作為後盾的資料存放區，例如 RAID 1 或 RAID 6，可能會導致效能不佳。

將CPU資源新增至閘道主機

閘道主機伺服器的最低需求為四個虛擬處理器。若要最佳化閘道效能，請確認指派給閘道 VM 的每個虛擬處理器都由專用CPU核心支援。此外，請確認您沒有過度訂閱CPUs主機伺服器的 。

當您將其他 CPUs 新增至閘道主機伺服器時，會增加閘道的處理能力。這樣做可讓您的閘道平行處理將資料從您的應用程式存放到本機儲存以及將此資料上傳至 Amazon S3。其他 CPUs也有助於確保您的閘道在與其他 共用主機時獲得足夠的CPU資源VMs。提供足夠的CPU資源具有提高輸送量的一般效果。

增加閘道與 AWS 雲端之間的頻寬

增加往返 的頻寬 AWS 將增加傳入閘道和傳出 AWS 雲端的最大資料速率。如果網路速度是閘道組態中的限制因素，而不是其他因素 (例如磁碟速度緩慢或閘道 - 啟動器連線頻寬不佳)，這樣可以改善閘道效能。

往返的網路頻寬 AWS 定義了在持續工作負載期間磁帶閘道的理論平均效能上限。

- 您可以長時間將資料寫入磁帶閘道的平均速率不會超過到 AWS的上傳頻寬。
- 長時間從磁帶閘道讀取資料的平均速率，不會超過您下載頻寬到 AWS。

> **Note**
>
> 由於此處列出的其他限制因素，例如快取/上傳緩衝區磁碟輸送量、CPU核心計數、總RAM量或啟動器和閘道之間的頻寬，您觀察到的閘道效能可能會低於網路頻寬。此外，閘道的正常操作包含許多為保護資料而採取的動作，這可能會導致觀察到的效能低於網路頻寬。

最佳化 iSCSI 設定

您可以最佳化 iSCSI 啟動器上的 iSCSI 設定，以達到更高的 I/O 效能。建議您在 `MaxReceiveDataSegmentLength` 和 `FirstBurstLength` 選擇 256 KiB，在 `MaxBurstLength` 選擇 1 MiB。如需設定 iSCSI 設定的詳細資訊，請參閱 自訂 iSCSI 設定。

> **Note**
>
> 這些建議設定可提升整體效能。不過，最佳化效能所需的特定 iSCSI 設定會因您使用的備份軟體而有所不同。如需詳細資訊，請參閱備份軟體的文件。

針對磁帶硬碟使用較大的區塊大小

針對磁帶閘道，磁帶機的預設區塊大小是 64 KB。不過，您可以將區塊大小增加至最高 1 MB，以改善 I/O 效能。

您選擇的區塊大小取決於您備份軟體支援的區塊大小上限。建議您將備份軟體中磁帶機的區塊大小，盡可能設定為越大的大小。不過，此區塊大小不能超過閘道支援的 1 MB 大小上限。

磁帶閘道會協調虛擬磁帶機的區塊大小，以自動比對備份軟體上的設定。增加備份軟體上的區塊大小時，建議您也檢查設定，以確保主機啟動器支援新的區塊大小。如需詳細資訊，請參閱您備份軟體的文件。如需特定閘道效能指導方針的詳細資訊，請參閱 Tape Gateway 的效能和最佳化。

最佳化備份軟體中虛擬磁帶機的效能

您的備份軟體可以同時在磁帶閘道上的最多 10 個虛擬磁帶機上備份資料。建議您在備份軟體中設定備份工作，以同時在磁帶閘道上使用至少 4 個虛擬磁帶機。當備份軟體同時將資料備份到多個虛擬磁帶時，您可以達到更佳的寫入傳輸量。

一般而言，您可以同時在 (讀取或寫入) 更多虛擬磁帶上作業，以達到更高的最大輸送量。藉由使用更多磁帶機，您可以讓閘道同時服務更多要求，進而提升效能。

新增資源到您的應用程式環境

增加您應用程式伺服器和閘道之間的頻寬

iSCSI 啟動器和閘道之間的連線可能會限制上傳和下載效能。如果您的閘道效能明顯比預期差，而且您已經改善了CPU核心計數和磁碟輸送量，請考慮：

- 升級您的網路纜線，使其在啟動器和閘道之間擁有更高的頻寬。
- 盡可能同時使用最多的磁帶機。 iSCSI 不支援將多個請求排入相同目標的佇列，這表示您使用的磁帶機越多，閘道可以同時進行服務的請求越多。這可讓您更充分利用閘道與啟動器之間的頻寬，從而增加閘道的明顯輸送量。

若要最佳化閘道效能，請確認您應用程式和閘道之間的頻寬足以供給您應用程式的需求。您可以使用閘道的 `ReadBytes` 和 `WriteBytes` 指標測量總資料輸送量。如需這些指標的詳細資訊，請參閱 測量磁帶閘道與 之間的效能 AWS。

針對您的應用程式，將所需要的輸送量與測量的輸送量進行比較。若測量的輸送量低於所需的輸送量，則在網路為瓶頸時，增加應用程式與閘道之間的頻寬便可改善效能。同樣地，若 VM 和本機磁碟沒有直接連接，您可以增加兩者間的頻寬。

將CPU資源新增至您的應用程式環境

如果您的應用程式可以使用其他CPU資源，則新增更多CPUs資源可協助您的應用程式擴展其 I/O 負載。

安全 in AWS Storage Gateway

的雲端安全 AWS 是最高優先順序。身為 AWS 客戶，您受益於資料中心和網路架構，其建置旨在滿足最安全敏感組織的需求。

安全性是 AWS 和 之間的共同責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 – AWS 負責保護在 Amazon Web Services Cloud 中執行 AWS 服務的基礎設施。AWS 也提供您可以安全使用的服務。第三方稽核人員會定期測試和驗證我們的安全有效性，這是AWS 合規計畫 的一部分。若要了解適用於 AWS Storage Gateway 的合規計劃，請參閱依AWS 合規計劃在範圍內的合規計劃。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件有助於您了解如何在使用 Storage Gateway 時套用共同責任模型。下列各主題將說明如何設定 Storage Gateway，以達成您的安全性與合規目標。您也會了解如何使用 AWS 其他服務來協助您監控和保護 Storage Gateway 資源。

主題

- 資料保護 in AWS Storage Gateway
- Identity and Access Management for AWS Storage Gateway
- AWS Storage Gateway 的合規驗證
- in AWS Storage Gateway 的復原能力
- AWS Storage Gateway 的基礎設施安全
- AWS 安全性最佳做法
- 登錄和監控 AWS Storage Gateway

資料保護 in AWS Storage Gateway

AWS 共同責任模型適用於 AWS Storage Gateway 中的資料保護。如本模型所述， AWS 負責保護執行所有 的全域基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權。 FAQ如需歐洲資料保護的相關資訊，請參閱AWS 安全部落格 上的AWS 共同責任模型和GDPR部落格文章。

為了資料保護目的，我們建議您保護 AWS 帳戶 憑證，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management （ ） 設定個別使用者IAM。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 對每個帳戶使用多重要素驗證 （MFA）。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 和建議 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需使用 CloudTrail 線索擷取 AWS 活動的資訊，請參閱 AWS CloudTrail 使用者指南 中的使用 CloudTrail 線索。
- 使用 AWS 加密解決方案，以及 中的所有預設安全控制項 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列界面或 FIPS 存取 時需要 140-3 個經過驗證的密碼編譯模組API，請使用FIPS端點。如需可用FIPS端點的詳細資訊，請參閱聯邦資訊處理標準 （FIPS） 140-3。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 Storage Gateway 或其他 AWS 服務 主控台API AWS CLI、 或 時 AWS SDKs。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您將URL提供給外部伺服器，強烈建議您在 中不要包含憑證資訊，URL以驗證您對該伺服器的請求。

資料加密使用 AWS KMS

Storage Gateway 使用SSL/TLS(安全通訊端層/傳輸層安全性) 來加密閘道設備與 AWS 儲存裝置之間傳輸的資料。根據預設，Storage Gateway 使用 Amazon S3 受管加密金鑰 (SSE-S3) 在伺服器端加密其存放在 Amazon S3 中的所有資料。您可以選擇使用 Storage Gateway，API將閘道設定為使用伺服器端加密使用 AWS Key Management Service (SSE-KMS) 金鑰來加密儲存在雲端的資料。

> **Important**
>
> 當您使用 AWS KMS 金鑰進行伺服器端加密時，您必須選擇對稱金鑰。Storage Gateway 不支援非對稱金鑰。如需詳細資訊，請參閱 AWS Key Management Service 開發人員指南中的使用對稱和非對稱金鑰。

加密檔案共享

對於檔案共用，您可以設定閘道使用 AWS KMS—managed 金鑰來加密物件，方法是使用 SSE-KMS。如需使用 Storage Gateway API 加密寫入檔案共用的資料的相關資訊，請參閱AWS Storage Gateway API參考資料中的 C reateNFSFile 共用。

加密磁碟區

對於快取和儲存的磁碟區，您可以使用 Storage Gateway 將儲存在雲端的磁碟區資料設定為使用 AWS KMS—managed 金鑰加密儲存在雲端中的磁碟區資料。API您可以指定其中一個受管理金鑰做為金KMS鑰。您用來加密磁碟區的金輪在磁碟區建立之後就無法變更。如需有關使用 Storage Gateway API 加密寫入快取或儲存磁碟區的資料的資訊，請參閱AWS Storage Gateway API參考資料CreateStorediSCSIVolume中的CreateCachediSCSIVolume或。

加密磁帶

對於虛擬磁帶，您可以設定閘道，使用 Storage Gate API way 使用 AWS KMS—managed 金鑰來加密儲存在雲端的磁帶資料。您可以指定其中一個受管理金鑰做為金KMS鑰。您用來加密磁帶資料的金輪在磁帶建立之後就無法變更。如需使用 Storage Gateway API 加密寫入虛擬磁帶的資料的相關資訊，請參閱AWS Storage Gateway API參考資料CreateTapes中的。

使用 AWS KMS 來加密資料時，請記住以下事項：

- 您的資料是在雲端中的靜態狀態下加密。意即資料會在 Amazon S3 中加密。
- IAM用戶必須具有所需的權限才能調用 AWS KMS API操作。如需詳細資訊，請參閱AWS Key Management Service 開發人員指南 AWS KMS中的搭配使用IAM原則。
- 如果您刪除或停用 AWS AWS KMS 金鑰或撤銷授與權杖，就無法存取磁碟區或磁帶上的資料。如需詳細資訊，請參閱AWS Key Management Service 開發人員指南中的刪除KMS金鑰。
- 如果您從KMS已加密的磁碟區建立快照，則快照會加密。快照會繼承磁碟區的KMS金鑰。
- 如果您從KMS已加密的快照建立新磁碟區，則該磁碟區會加密。您可以為新磁碟區指定不同的KMS金鑰。

> **Note**
>
> Storage Gateway 不支援從加密磁碟區或加密快照的復原點建立未KMS加密的KMS磁碟區。

如需有關的詳細資訊 AWS KMS，請參閱什麼是 AWS Key Management Service？

Identity and Access Management for AWS Storage Gateway

AWS Identity and Access Management （ IAM ） 是一種 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員會控制誰可以驗證 （ 登入 ） 和授權 （ 具有許可 ） 使用 AWS SGW 資源。IAM 是 AWS 服務 您可以免費使用的 。

主題

物件

使用 AWS Identity and Access Management （ IAM ） 的方式會有所不同，具體取決於您在 中執行的工作 AWS SGW。

服務使用者 – 如果您使用 AWS SGW服務來執行您的任務，則管理員會為您提供所需的憑證和許可。當您使用更多 AWS SGW功能來執行工作時，您可能需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取 中的功能 AWS SGW，請參閱 疑難排解 S AWS torage Gateway 識別與存取。

服務管理員 – 如果您負責 AWS SGW公司的資源，您可能擁有 的完整存取權 AWS SGW。您的任務是判斷您的服務使用者應該存取哪些 AWS SGW功能和資源。然後，您必須向IAM管理員提交請求，以變更服務使用者的許可。請檢閱此頁面上的資訊，以了解 的基本概念IAM。若要進一步了解貴公司如何IAM搭配 使用 AWS SGW，請參閱 S AWS torage Gateway 如何搭配使用 IAM。

IAM 管理員 – 如果您是IAM管理員，您可能想要了解如何撰寫政策以管理 存取權的詳細資訊 AWS SGW。若要檢視您可以在 中使用的以身分為基礎的政策範例 AWS SGWIAM，請參閱 適用於 Storage Gateway 的身分型政策範例。

使用身分驗證

驗證是您 AWS 使用身分憑證登入 的方式。您必須以 AWS 帳戶根使用者身分、IAM使用者身分或擔任IAM角色來驗證 （ 登入 AWS ）。

您可以使用透過身分來源提供的憑證，以聯合身分 AWS 身分登入 。 AWS IAM Identity Center （ IAM Identity Center ） 使用者、您公司的單一登入身分驗證，以及您的 Google 或 Facebook 憑證，都是聯

合身分的範例。當您以聯合身分登入時，您的管理員先前會使用 IAM角色設定身分聯合。當您 AWS 使用聯合來存取 時，您會間接擔任 角色。

根據您身分的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱 使用者指南 中的如何登入 AWS 帳戶您的 。 AWS 登入

如果您以 AWS 程式設計方式存取 ， AWS 會提供軟體開發套件 （SDK） 和命令列介面 （CLI），以使用您的 憑證以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需使用建議方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南 中的簽署 AWS API請求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多因素身分驗證 （MFA） 來提高帳戶的安全性。若要進一步了解，請參閱 AWS IAM Identity Center 使用者指南 中的多重要素驗證，以及 使用者指南 中的使用多重要素驗證 （MFA） AWS。 IAM

AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從一個登入身分開始，該身分可完全存取 帳戶中的所有 AWS 服務 和資源。此身分稱為 AWS 帳戶 根使用者，透過您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需需要您以根使用者身分登入的任務完整清單，請參閱 IAM 使用者指南 中的需要根使用者憑證的任務。

聯合身分

作為最佳實務， 會要求人類使用者，包括需要管理員存取權的使用者，使用 AWS 服務 臨時憑證來與身分提供者使用聯合來存取 。

聯合身分是來自您的企業使用者目錄、Web 身分提供者、 AWS Directory Service、身分中心目錄，或使用透過身分來源提供的 AWS 服務 憑證存取的任何使用者。當聯合身分存取 時 AWS 帳戶，它們會擔任 角色，而角色會提供臨時憑證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，或者您可以連線並同步到您身分來源中的一組使用者 AWS 帳戶 和群組，以便在所有 和 應用程式中使用。如需 IAM Identity Center 的相關資訊，請參閱 AWS IAM Identity Center 使用者指南 中的什麼是 IAM Identity Center？。

IAM 使用者和群組

IAM 使用者是 中具有單一個人或應用程式特定許可 AWS 帳戶 的身分。在可能的情況下，我們建議您依賴臨時憑證，而不是建立具有密碼和存取金鑰等長期憑證IAM的使用者。不過，如果您有特定的使用

案例需要IAM使用者長期憑證，建議您輪換存取金鑰。如需詳細資訊，請參閱 IAM 使用者指南 中的定期輪換需要長期憑證的使用案例存取金鑰。

IAM 群組是指定IAM使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有名為 的群組IAMAdmins，並授予該群組管理IAM資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。若要進一步了解，請參閱 IAM 使用者指南 中的何時建立IAM使用者 （ 而非角色 ）。

IAM 角色

IAM 角色是 中具有特定許可 AWS 帳戶 的身分。它類似於IAM使用者，但與特定人員無關。您可以透過 AWS Management Console 切換IAM角色 暫時在 中擔任角色。 https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html您可以透過呼叫 AWS CLI 或 AWS API 操作，或使用自訂 來擔任角色URL。如需使用角色方法的詳細資訊，請參閱 IAM 使用者指南 中的使用IAM角色。

IAM 具有臨時憑證的角色在下列情況下很有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需聯合角色的相關資訊，請參閱 IAM 使用者指南 中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，您可以設定許可集。若要控制身分在身分驗證後可以存取的內容，IAMIdentity Center 會將許可集與 中的角色相關聯IAM。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 臨時IAM使用者許可 – IAM使用者或角色可以擔任IAM角色，暫時接受特定任務的不同許可。
- 跨帳戶存取 – 您可以使用 IAM角色，允許不同帳戶中的人員 （ 受信任的主體 ） 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。不過，使用某些 AWS 服務，您可以將政策直接連接至資源 （ 而不是使用角色作為代理 ）。若要了解跨帳戶存取的角色與資源型政策之間的差異，請參閱 IAM 使用者指南 中的跨帳戶資源存取IAM。
- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。例如，當您在 服務中撥打電話時，該服務通常會在 Amazon 中執行應用程式EC2或在 Amazon S3 中儲存物件。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉送存取工作階段 （ FAS ） – 當您使用IAM使用者或角色在 中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼

叫 的委託人許可 AWS 服務，並結合 請求向下游服務 AWS 服務 提出請求。FAS 只有在服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出FAS請求的政策詳細資訊，請參閱轉送存取工作階段 。

- 服務角色 – 服務角色是服務代表您執行動作時擔任IAM的角色。IAM 管理員可以從 內部建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱 使用者指南 中的建立角色以將許可委派給 AWS 服務 。 IAM
- 服務連結角色 – 服務連結角色是連結至 的服務角色類型 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的 中 AWS 帳戶 ，並由 服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

- 在 Amazon 上執行的應用程式 EC2 – 您可以使用 IAM角色來管理在EC2執行個體上執行之應用程式的臨時憑證，以及提出 AWS CLI 或 AWS API請求。最好將存取金鑰存放在EC2執行個體中。若要將 AWS 角色指派給EC2執行個體並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體設定檔。執行個體設定檔包含 角色，並啟用在EC2執行個體上執行的程式，以取得臨時憑證。如需詳細資訊，請參閱 IAM 使用者指南 中的使用 IAM角色將許可授予在 Amazon EC2執行個體上執行的應用程式。

若要了解如何使用IAM角色或IAM使用者，請參閱 IAM 使用者指南 中的建立IAM角色 （ 而非使用者 ）的時機。

使用政策管理存取權

您可以透過建立政策並將其連接至 AWS 身分或資源 AWS 來控制 中的存取。政策是 AWS 其中的物件，當與身分或資源建立關聯時， 會定義其許可。當主體 （ 使用者、根使用者或角色工作階段 ） 發出請求時， 會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策都以JSON文件 AWS 形式儲存在 中。如需JSON政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南 中的JSON政策概觀。

管理員可以使用 AWS JSON政策來指定誰可以存取什麼。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授予使用者對所需資源執行動作的許可，IAM管理員可以建立IAM政策。然後，管理員可以將IAM政策新增至角色，使用者可以擔任角色。

IAM 無論您用來執行操作的方法為何，政策都會定義動作的許可。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該政策的使用者可以從 AWS Management Console、 AWS CLI或 AWS 取得角色資訊API。

身分型政策

身分型政策是JSON許可政策文件，您可以附加到身分，例如IAM使用者、使用者群組或角色。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分型政策，請參閱 IAM 使用者指南 中的建立IAM政策。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管政策是獨立的政策，您可以連接到 中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受管政策和客戶受管政策。若要了解如何在受管政策或內嵌政策之間進行選擇，請參閱 IAM 使用者指南 中的在受管政策與內嵌政策之間進行選擇。

資源型政策

資源型政策是您連接至資源JSON的政策文件。資源型政策的範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策 。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主體可以包括帳戶、使用者、角色、聯合使用者或 AWS 服務。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策IAM中使用來自 的 AWS 受管政策。

存取控制清單 （ACLs）

存取控制清單 （ACLs） 控制哪些主體 （帳戶成員、使用者或角色） 具有存取 資源的許可。ACLs 類似於資源型政策，雖然它們不使用JSON政策文件格式。

Amazon S3 AWS WAF和 Amazon VPC是支援 的服務範例ACLs。若要進一步了解 ACLs，請參閱 Amazon Simple Storage Service 開發人員指南 中的存取控制清單 （ACL） 概觀。

其他政策類型

AWS 支援其他較不常見的政策類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可界限是一項進階功能，您可以在其中設定身分型政策可授予IAM實體 （IAM使用者或角色） 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱 IAM 使用者指南 中的IAM實體許可界限。
- 服務控制政策 （SCPs） – SCPs是在 中指定組織或組織單位 （OU） 最大許可JSON的政策 AWS Organizations。 AWS Organizations 是一項用於分組和集中管理您企業擁有 AWS 帳戶 之多個

的服務。如果您啟用組織中的所有功能，則可以將服務控制政策 （SCPs） 套用至任何或所有帳戶。SCP 限制成員帳戶中實體的許可，包括每個 AWS 帳戶根使用者。如需 Organizations 和 的詳細資訊SCPs，請參閱 AWS Organizations 使用者指南 中的服務控制政策。

- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南 中的工作階段政策。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要了解如何 AWS 在涉及多種政策類型時決定是否允許請求，請參閱 IAM 使用者指南 中的政策評估邏輯。

S AWS torage Gateway 如何搭配使用 IAM

在您用IAM來管理存取權之前 AWS SGW，請先瞭解哪些IAM功能可搭配使用 AWS SGW。

IAM可搭配 S AWS torage Gateway 使用的功能

IAM特徵	AWS SGW支持
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵 (服務特定)	是
ACLs	否
ABAC(策略中的標籤)	部分
臨時憑證	是
轉寄存取工作階段 (FAS)	是

IAM特徵	AWS SGW支持
服務角色	是
服務連結角色	是

若要深入瞭解其他 AWS 服務如何 AWS SGW與大部分IAM功能搭配使用，請參閱IAM使用者指南IAM中的使用AWS 服務。

以身分識別為基礎的原則 AWS SGW

支援身分型政策：是

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

使用以IAM身分識別為基礎的策略，您可以指定允許或拒絕的動作和資源，以及允許或拒絕動作的條件。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。若要瞭解可在JSON策略中使用的所有元素，請參閱《使用IAM者指南》中的IAMJSON策略元素參考資料。

以身分識別為基礎的原則範例 AWS SGW

若要檢視以 AWS SGW身分為基礎的原則範例，請參閱。適用於 Storage Gateway 的身分型政策範例

以資源為基礎的政策 AWS SGW

支援資源型政策：否

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

若要啟用跨帳戶存取，您可以在以資源為基礎的策略中指定一個或多個帳戶中的一個或多個帳戶中的IAM實體作為主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主參與者和資源位於不同時 AWS 帳戶，受信任帳戶中的IAM管理員也必須授與主參與者實體 (使用者或角色) 權限，才能存

取資源。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱《IAM使用指南》IAM中的〈跨帳號資源存取〉。

的政策動作 AWS SGW

支援政策動作：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON策略Action元素描述了您可以用來允許或拒絕策略中存取的動作。策略動作通常與關聯 AWS API操作具有相同的名稱。有一些例外情況，例如沒有匹配API操作的僅限權限的操作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看 AWS SGW動作清單，請參閱服務授權參考資料中的 S AWS torage Gateway 定義的動作。

中的策略動作在動作之前 AWS SGW使用下列前置詞：

```
sgw
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

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

若要檢視以 AWS SGW身分為基礎的原則範例，請參閱。適用於 Storage Gateway 的身分型政策範例

的政策資源 AWS SGW

支援政策資源：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

ResourceJSON原則元素會指定要套用動作的一或多個物件。陳述式必須包含 Resource 或 NotResource 元素。最佳做法是使用其 Amazon 資源名稱 (ARN) 指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

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

若要查看 AWS SGW資源類型及其清單ARNs，請參閱服務授權參考資料中的 S AWS torage Gateway 定義的資源。若要瞭解可以針對每個資源指定哪些動作，請參閱 S AWS torage Gateway 定義ARN的動作。

若要檢視以 AWS SGW身分為基礎的原則範例，請參閱。適用於 Storage Gateway 的身分型政策範例

的政策條件索引鍵 AWS SGW

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，只有在IAM使用者名稱標記資源時，您才可以授與IAM使用者存取資源的權限。如需詳細資訊，請參閱《IAM使用指南》中的IAM政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《使用指南》中的AWS 全域條件內IAM容索引鍵。

若要查看 AWS SGW條件金鑰清單，請參閱服務授權參考資料中的 S AWS torage Gateway 的條件金鑰。若要瞭解可以使用條件金鑰的動作和資源，請參閱 S AWS torage Gateway 定義的動作。

若要檢視以 AWS SGW身分為基礎的原則範例，請參閱。適用於 Storage Gateway 的身分型政策範例

ACLs在 AWS SGW

支持ACLs：無

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

ABAC與 AWS SGW

支援 ABAC (策略中的標籤): 部分

以屬性為基礎的存取控制 (ABAC) 是一種授權策略，可根據屬性定義權限。在中 AWS，這些屬性稱為標籤。您可以將標籤附加至IAM實體 (使用者或角色) 和許多 AWS 資源。標記實體和資源是的第一步ABAC。然後，您可以設計ABAC策略，以便在主參與者的標籤與他們嘗試存取的資源上的標籤相符時允許作業。

ABAC在快速成長的環境中很有幫助，並且有助於原則管理變得繁瑣的情況。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需有關的詳細資訊ABAC，請參閱什麼是ABAC？ 在《IAM使用者指南》中。若要檢視包含設定步驟的自學課程ABAC，請參閱《使用指南》中的〈使用以屬性為基礎的存取控制 (ABAC) IAM 〉。

使用臨時登入資料 AWS SGW

支援臨時憑證：是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配使用 AWS 服務 ，請參閱《IAM使用指南》IAM中的使用方式。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立臨時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需有關切換角色的詳細資訊，請參閱《IAM使用者指南》中的〈切換到角色 (主控台)〉。

您可以使用 AWS CLI 或手動建立臨時認證 AWS API。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而非使用長期存取金鑰。如需詳細資訊，請參閱IAM。

轉寄存取工作階段 AWS SGW

支援轉寄存取工作階段 (FAS)：是

當您使用使用IAM者或角色在中執行動作時 AWS，您會被視為主參與者。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS會使用主參與者呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。FAS只有當服務收到需要與其他 AWS 服務 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。

AWS SGW 的服務角色

支援服務角色：是

服務角色是服務假定代表您執行動作的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色 IAM。如需詳細資訊，請參閱《IAM使用指南》 AWS 服務中的建立角色以將權限委派給

> **Warning**
>
> 變更服務角色的權限可能會中斷 AWS SGW功能。只有在 AWS SGW提供指引時才編輯服務角色。

服務連結角色 AWS SGW

支援服務連結角色：是

服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。

如需有關建立或管理服務連結角色的詳細資訊，請參閱使用IAM的AWS 服務。在表格中尋找服務，其中包含服務連結角色欄中的 Yes。選擇是連結，以檢視該服務的服務連結角色文件。

適用於 Storage Gateway 的身分型政策範例

根據預設，使用者和角色沒有建立或修改 AWS SGW資源的許可。他們也無法使用 AWS Management Console、 AWS Command Line Interface （ AWS CLI ） 或 來執行任務 AWS API。若要授予使用者對所需資源執行動作的許可，IAM管理員可以建立IAM政策。然後，管理員可以將IAM政策新增至角色，使用者可以擔任角色。

若要了解如何使用這些範例政策文件來建立IAM身分型JSON政策，請參閱 IAM 使用者指南 中的建立IAM政策。

如需 定義的動作和資源類型的詳細資訊 AWS SGW，包括ARNs每種資源類型的 格式，請參閱服務授權參考 中的 AWS Storage Gateway 的動作、資源和條件金鑰。

主題

- 政策最佳實務
- 使用 AWS SGW 主控台
- 允許使用者檢視他們自己的許可

政策最佳實務

身分型政策會判斷是否有人可以在您的帳戶中建立、存取或刪除 AWS SGW資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用受AWS 管政策，將許可授予許多常見使用案例。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需詳細資訊，請參閱 IAM 使用者指南 中的 AWS 受管政策或 AWS 任務功能的受管政策。
- 套用最低權限許可 – 當您使用IAM政策設定許可時， 只會授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的詳細資訊，請參閱 IAM 使用者指南 中的政策和許可IAM。
- 使用IAM政策中的條件來進一步限制存取：您可以將條件新增至政策，以限制對動作和資源的存取。例如，您可以撰寫政策條件來指定所有請求都必須使用 傳送SSL。如果透過特定 使用服務動作，例如 AWS 服務，您也可以使用 條件來授予其存取權 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南 中的IAMJSON政策元素：條件。
- 使用 IAM Access Analyzer 驗證您的IAM政策，以確保安全且功能許可 – IAM Access Analyzer 會驗證新的和現有的政策，讓政策遵循IAM政策語言 （JSON） 和IAM最佳實務。IAM Access Analyzer 提供超過 100 個政策檢查和可操作的建議，協助您撰寫安全且實用的政策。如需詳細資訊，請參閱 IAM 使用者指南 中的IAM存取分析器政策驗證。
- 需要多因素身分驗證 （MFA） – 如果您有需要IAM使用者或 根使用者的案例 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫API操作MFA時要求 ，請將MFA條件新增至您的政策。如需詳細資訊，請參閱 IAM 使用者指南 中的設定 MFA受保護的API存取。

如需 中最佳實務的詳細資訊IAM，請參閱 IAM 使用者指南 中的安全最佳實務IAM。

使用 AWS SGW 主控台

若要存取 AWS Storage Gateway 主控台，您必須具有一組最低許可。這些許可必須允許您列出和檢視AWS SGW中資源的詳細資訊 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

對於僅對 AWS CLI 或 進行呼叫的使用者，您不需要允許最低主控台許可 AWS API。相反地，僅允許存取與其嘗試執行API的操作相符的動作。

若要確保使用者和角色仍然可以使用主控台，也請將 AWS SGW AWS SGW*ConsoleAccess*或 *ReadOnly* AWS 受管政策連接至實體。如需詳細資訊，請參閱 IAM 使用者指南 中的新增許可給使用者。

允許使用者檢視他們自己的許可

此範例示範如何建立政策，允許使用者檢視連接至其IAM使用者身分的內嵌和受管政策。此政策包含在主控台上完成此動作或使用 或 AWS CLI 以程式設計方式完成此動作的許可 AWS API。

```
{
    "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": "*"
        }
    ]
}
```

疑難排解 S AWS torage Gateway 識別與存取

使用下列資訊可協助您診斷及修正使用和時可能會遇到的 AWS SGW常見問題IAM。

主題

- 我沒有執行操作的授權 AWS SGW
- 我沒有授權執行 iam：PassRole
- 我想允許我以外的人訪 AWS 帳戶 問我的 AWS SGW資源

我沒有執行操作的授權 AWS SGW

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

當使用mateojacksonIAM者嘗試使用主控台來檢視虛構*my-example-widget*資源的詳細資料，但沒有虛構的sgw:*GetWidget*權限時，就會發生下列範例錯誤。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 sgw:GetWidget on resource: my-example-widget
```

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 sgw:*GetWidget* 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

我沒有授權執行 iam：PassRole

如果您收到未獲授權執行iam:PassRole動作的錯誤訊息，則必須更新您的原則以允許您將角色傳遞給 AWS SGW。

有些 AWS 服務 允許您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為的使用IAM者marymajor嘗試使用主控台執行中的動作時，就會發生下列範例錯誤 AWS SGW。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 `iam:PassRole` 動作。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

我想允許我以外的人訪 AWS 帳戶 問我的 AWS SGW資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。對於支援以資源為基礎的政策或存取控制清單 (ACLs) 的服務，您可以使用這些政策授與人員存取您資源的權限。

如需進一步了解，請參閱以下內容：

- 若要瞭解是否 AWS SGW支援這些功能，請參閱S AWS torage Gateway 如何搭配使用 IAM。
- 若要瞭解如何提供您所擁有資 AWS 帳戶 源的存取權，請參閱《IAM使用者指南》中的〈提供存取權給您 AWS 帳戶 所擁有的其他IAM使用者〉。
- 若要瞭解如何將您的資源存取權提供給第三方 AWS 帳戶，請參閱《IAM使用指南》中的提供第三方 AWS 帳戶 擁有的存取權。
- 若要瞭解如何透過身分聯盟提供存取權，請參閱《使用指南》中的提供對外部驗證使用IAM者的存取權 (身分聯合)。
- 若要瞭解針對跨帳號存取使用角色與以資源為基礎的政策之間的差異，請參閱《使用IAM者指南》IAM中的〈跨帳號資源存取〉。

AWS Storage Gateway 的合規驗證

協力廠商稽核人員會評估 S AWS torage Gateway 的安全性與合規性，做為多個 AWS 合規計畫的一部分。這些包括 SOCPCI,ISO,RAMP, 美聯儲 HIPAAMTSC,,, C5, K-ISMS, ENS 高OSPAR, 和 HITRUSTCSF.

如需特定規範計劃範圍內的 AWS 服務清單，請參閱合規計劃AWS 服務範圍方案)。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用 Storage Gateway 時的合規責任，取決於資料的敏感性、您公司的合規目標，以及適用的法律和法規。 AWS 會提供以下資源協助您處理合規事宜：

- 安全性與合規快速入門指南 — 這些部署指南討論架構考量，並提供在上部署以安全性和法規遵循為重點的基準環境的步驟。 AWS
- HIPAA安全性與合規性架構白皮書 — 本白皮書說明公司如何使用建立HIPAA符合標準的應 AWS 用程式。
- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 此 AWS 服務提供安全性狀態的全面檢視，協助 AWS 您檢查您是否符合安全性產業標準和最佳做法。

in AWS Storage Gateway 的復原能力

AWS 全域基礎設施是以 AWS 區域 和可用區域為基礎。

AWS 區域 是全球資料中心叢集所在的實體位置。每個邏輯資料中心群組稱為可用區域 （ AZ ）。每個 AWS 區域 都包含至少三個在地理區域AZs內隔離且實體分隔的 。與其他雲端供應商不同，這些供應商通常將區域定義為單一資料中心，每個 的多個 AZ 設計都 AWS 區域 具有不同的優勢。每個 AZ 都有獨立的電源、冷卻和實體安全， ultra-low-latency並透過備援網路連接。如果您的部署需要專注於高可用性，您可以將 服務和資源設定為多個 AZs，以實現更大的容錯性。

AWS 區域 符合最高層級的基礎設施安全、合規和資料保護。之間的所有流量AZs都會加密。網路效能足以在 之間完成同步複寫AZs。AZs 讓分割服務和資源變得簡單，以實現高可用性。如果您的部署跨分割AZs，您的資源會受到更好的隔離和保護，免於停電、閃電、龍捲風、地震等問題。AZs 與任何其他 AZ 之間有有意義的距離，雖然彼此距離都在 100 公里 （ 60 英里 ） 內。

如需 AWS 區域 和可用區域的詳細資訊，請參閱AWS 全域基礎設施。

除了 AWS 全球基礎設施之外，Storage Gateway 還提供多種功能，以協助支援您的資料彈性和備份需求：

- 使用VMware vSphere 高可用性 （ VMware HA ） 協助保護儲存工作負載，避免硬體、Hypervisor 或網路故障。如需詳細資訊，請參閱搭配 Storage Gateway 使用VMware vSphere 高可用性。

- 封存 S3 Glacier Flexible Retrieval 中的虛擬磁帶。如需詳細資訊，請參閱存檔虛擬磁帶。

AWS Storage Gateway 的基礎設施安全

作為受管服務， AWS Storage Gateway 受到 Amazon Web Services：安全程序概觀白皮書中所述 AWS 的全球網路安全程序保護。

您可以使用 AWS 已發佈的API呼叫，透過網路存取 Storage Gateway。用戶端必須支援 Transport Layer Security （ TLS ） 1.2。用戶端還必須支援具有完美正向保密性 （ PFS ） 的密碼套件，例如 Ephemeral Diffie-Hellman （ DHE ） 或 Elliptic Curve Ephemeral Diffie-Hellman （ ） ECDHE。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，必須使用與IAM委託人相關聯的存取金鑰 ID 和秘密存取金鑰來簽署請求。或者，您可以透過 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

> **Note**
>
> 您應該將 AWS Storage Gateway 設備視為受管虛擬機器，且不應嘗試以任何方式存取或修改其安裝。嘗試使用一般閘道更新機制以外的方法安裝掃描軟體或更新任何軟體套件，可能會導致閘道故障，並可能影響我們支援或修正閘道的能力。
>
> AWS CVEs定期檢閱、分析和修復。我們會將這些問題的修正納入 Storage Gateway，作為正常軟體版本週期的一部分。這些修正通常會在排程維護時段內，作為正常閘道更新程序的一部分套用。如需閘道更新的詳細資訊，請參閱

AWS 安全性最佳做法

AWS 在您開發和實作自己的安全性原則時，提供許多安全性功能供您考量。這些最佳實務為一般準則，並不代表完整的安全解決方案。這些實務可能不適用或無法滿足您的環境需求，因此請將其視為實用建議就好，而不要當作是指示。如需詳細資訊，請參閱 AWS 安全最佳實務。

登錄和監控 AWS Storage Gateway

Storage Gateway 與一項服務整合 AWS CloudTrail，可提供 Storage Gateway 中使用者、角色或服務所採取之動作記錄的 AWS 服務。 CloudTrail 將 Storage Gateway 的所有API呼叫擷取為事件。擷取的呼叫包括來自 Storage Gateway 主控台的呼叫，以及對 Storage Gateway API 作業的程式碼呼叫。如

果您建立追蹤，您可以啟動連續交付 CloudTrail 事件至 Amazon S3 儲存貯體，包括 Storage Gateway 的事件。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail，您可以判斷向 Storage Gateway 發出的要求、提出要求的來源 IP 位址、提出要求的人員、提出要求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱使AWS CloudTrail 用者指南。

Storage Gateway 資訊 CloudTrail

CloudTrail 在您創建帳戶時，您的 Amazon Web Services 帳戶激活。當 Storage Gateway 中發生活動時，該活動會與 CloudTrail 事件歷史記錄中的其他 AWS 服務事件一起記錄在事件中。您可以檢視、搜尋和下載 Amazon Web Services 帳戶中的最近事件。如需詳細資訊，請參閱檢視具有事 CloudTrail 件記錄的事件。

如需 Amazon Web Services 帳戶中正在進行事件的記錄 (包含 Storage Gateway 的事件)，請建立線索。追蹤可 CloudTrail 將日誌檔案傳送到 Amazon S3 儲存貯體。根據預設，當您在主控台中建立追蹤時，追蹤會套用至所有 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務與整合
- 設定 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 記錄檔並從多個帳戶接收 CloudTrail 記錄檔

所有 Storage Gateway 動作都會記錄並記載在動作主題中。例如，呼叫`ActivateGateway`、`ListGateways`、和`ShutdownGateway`動作會在 CloudTrail 記錄檔中產生項目。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 要求是使用 root 或 AWS Identity and Access Management (IAM) 使用者認證提出的。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱CloudTrail userIdentity元素。

了解 Storage Gateway 日誌檔案項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。 CloudTrail 日誌文件不是公共API調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

下列範例顯示示範動作的 CloudTrail 記錄項目。

```
{ "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"
            }]
}
```

下列範例顯示示範 ListGateways動作的 CloudTrail 記錄項目。

```
{
 "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"
              }]
}
```

為您的閘道進行疑難排解

接下來，您可以找到與閘道、主機平台、虛擬磁帶、高可用性、資料復原和安全性相關的最佳實務和疑難排解問題的相關資訊。內部部署閘道疑難排解資訊涵蓋部署在支援虛擬化平台上的閘道。高可用性問題的疑難排解資訊涵蓋在VMware vSphere 高可用性 （HA） 平台上執行的閘道。

主題

- 故障診斷：閘道離線問題 - 了解如何診斷可能導致您的閘道在 Storage Gateway 主控台中離線顯示的問題。
- 疑難排解：閘道啟用期間的內部錯誤 - 了解如何在嘗試啟用 Storage Gateway 時收到內部錯誤訊息。
- 對內部部署閘道問題進行疑難排解 - 了解使用內部部署閘道時可能遇到的典型問題，以及如何允許 AWS Support 連線至閘道以協助疑難排解。
- 為 Microsoft Hyper-V 設定進行疑難排解 - 了解在 Microsoft Hyper-V 平台上部署 Storage Gateway 時可能遇到的典型問題。
- 疑難排解 Amazon EC2 閘道問題 - 尋找您在使用部署在 Amazon 上的閘道時可能遇到的典型問題的相關資訊EC2。
- 為硬體設備問題進行疑難排解 - 了解如何解決使用 Storage Gateway 硬體設備時可能遇到的問題。
- 為虛擬磁帶問題進行故障診斷 - 了解當您遇到虛擬磁帶的非預期問題時，您可以採取的動作。
- 為高可用性問題進行故障診斷 - 了解如果您遇到在 VMware HA 環境中部署的閘道問題，該怎麼做。

故障診斷：閘道離線問題

如果主控台顯示您的閘道離線， AWS Storage Gateway 請使用下列疑難排解資訊來決定該怎麼做。

由於下列一個或多個原因，您的閘道可能顯示為離線：

- 閘道無法連線 Storage Gateway 服務端點。
- 閘道意外關閉。
- 與閘道相關聯的快取磁碟已中斷連線或修改，或已失敗。

若要讓閘道重新上線，請識別並解決導致閘道離線的問題。

檢查相關聯的防火牆或代理

如果您將閘道設定為使用代理，或將閘道放置在防火牆之後，請檢閱代理或防火牆的存取規則。代理或防火牆必須允許往返 Storage Gateway 所需的網路連接埠和服務端點的流量。如需詳細資訊，請參閱網路和防火牆需求 。

檢查閘道流量的持續SSL或深度封包檢查

如果目前對閘道和 之間的網路流量執行 SSL或 深層封包檢查 AWS，則閘道可能無法與所需的服務端點通訊。若要讓閘道恢復連線，您必須停用檢查。

檢查 Hypervisor 主機上是否有停電或硬體故障

閘道的 Hypervisor 主機發生停電或硬體故障，可能會導致閘道意外關閉並變得無法連線。還原電源和網路連線後，您的閘道將再次變為可存取。

閘道恢復連線後，請務必採取步驟來復原資料。如需詳細資訊，請參閱最佳實務：復原資料最佳實務

檢查關聯快取磁碟的問題

如果至少有一個與閘道相關聯的快取磁碟遭到移除、變更或調整大小，或者已損毀，則您的閘道可能會離線。

如果已從 Hypervisor 主機移除工作快取磁碟：

1. 關機閘道。
2. 重新新增磁碟。

> **Note**
>
> 請務必將磁碟新增至相同的磁碟節點。

3. 重新啟動閘道。

如果快取磁碟損毀、已取代或已調整大小：

1. 關機閘道。
2. 重設快取磁碟。
3. 重新設定快取儲存的磁碟。

4. 重新啟動閘道。

如需針對磁帶閘道故障診斷損毀快取磁碟的詳細資訊，請參閱您需要從故障的快取磁碟復原虛擬磁帶。

疑難排解：閘道啟用期間的內部錯誤

Storage Gateway 啟用請求會周遊兩個網路路徑。用戶端傳送的傳入啟用請求會透過連接埠 80 連線至閘道的虛擬機器（VM）或 Amazon Elastic Compute Cloud（AmazonEC2）執行個體。如果閘道成功收到啟用請求，閘道會與 Storage Gateway 端點通訊，以接收啟用金鑰。如果閘道無法到達 Storage Gateway 端點，則閘道會以內部錯誤訊息回應用戶端。

使用以下疑難排解資訊，判斷當您在嘗試啟用 時收到內部錯誤訊息時該怎麼做 AWS Storage Gateway。

> **Note**
>
> - 請務必使用最新的虛擬機器映像檔案或 Amazon Machine Image（AMI）版本部署新的閘道。如果您嘗試啟用使用過時 的閘道，將會收到內部錯誤AMI。
> - 下載 之前，請確定您選取了您要部署的正確閘道類型AMI。AMIs 每個閘道類型的 .ova 檔案和 不同，且無法互換。

解決使用公有端點啟用閘道時出現的錯誤

若要解決使用公有端點啟用閘道時的啟用錯誤，請執行下列檢查和組態。

檢查所需的連接埠

對於內部部署的閘道，請檢查本機防火牆上的連接埠是否已開啟。對於部署在 Amazon EC2執行個體上的閘道，請檢查連接埠是否在執行個體的安全群組上開啟。若要確認連接埠已開啟，請從伺服器在公有端點上執行 telnet 命令。此伺服器必須與閘道位於相同的子網路中。例如，下列 telnet 命令會測試連接埠 443 的連線：

```
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
```

若要確認閘道本身可以到達端點，請存取閘道的本機 VM 主控台（適用於內部部署的閘道）。或者，您可以SSH前往閘道的執行個體（適用於部署在 Amazon 上的閘道EC2）。然後，執行網路連線測試。確認測試傳回 [PASSED]。如需詳細資訊，請參閱 測試閘道連線至網際網路 。

> **Note**
>
> 閘道主控台的預設登入使用者名稱為 admin，預設密碼為 password。

確保防火牆安全不會修改從閘道傳送至公有端點的封包

SSL 檢查、深層封包檢查或其他形式的防火牆安全可能會干擾從閘道傳送的封包。如果從啟動端點預期修改SSL憑證，SSL交握會失敗。若要確認沒有進行中的SSL檢查，請在連接埠 443 的主啟動端點（ anon-cp.storagegateway.region.amazonaws.com ）上執行 OpenSSL 命令。您必須從與閘道位於相同子網路的機器執行此命令：

```
$ openssl s_client -connect  anon-cp.storagegateway.region.amazonaws.com:443 -
servername anon-cp.storagegateway.region.amazonaws.com
```

> **Note**
>
> Replace (取代) *region* 您的 AWS 區域。

如果沒有進行中的SSL檢查，則命令會傳回類似下列的回應：

```
$ 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
---
```

如果有進行中的SSL檢查，回應會顯示已變更的憑證鏈，如下所示：

```
$ openssl s_client -connect  anon-cp.storagegateway.ap-southeast-1.amazonaws.com:443 -
servername anon-cp.storagegateway.ap-southeast-1.amazonaws.com
CONNECTED(00000003)
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.ap-southeast-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

只有在啟用端點識別SSL憑證時，才會接受SSL交握。這表示閘道對端點的傳出流量必須免於網路中防火牆執行的檢查。這些檢查可能是SSL檢查或深度封包檢查。

檢查閘道時間同步

時間過長可能會導致SSL交握錯誤。對於內部部署閘道，您可以使用閘道的本機 VM 主控台來檢查閘道的時間同步。時間偏移不應大於 60 秒。如需詳細資訊，請參閱同步閘道 VM 時間同步閘道 VM 時間。

系統時間管理選項不適用於託管在 Amazon EC2執行個體上的閘道。若要確保 Amazon EC2閘道可以正確同步時間，請確認 Amazon EC2執行個體可以透過連接埠UDP和 TCP 123 連線至下列NTP伺服器集區清單：

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

解決使用 Amazon VPC端點啟用閘道時出現的錯誤

若要解決使用 Amazon Virtual Private Cloud （ AmazonVPC ） 端點啟用閘道時的啟用錯誤，請執行下列檢查和組態。

檢查所需的連接埠

確定本機防火牆 （ 針對內部部署部署的閘道 ） 或安全群組 （ 針對 Amazon 中部署的閘道EC2 ） 內的必要連接埠已開啟。將閘道連線至 Storage Gateway VPC端點所需的連接埠，與將閘道連線至公有端點時所需的連接埠不同。連線至 Storage Gateway VPC端點需要下列連接埠：

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

如需詳細資訊，請參閱 建立 Storage Gateway 的VPC端點 。

此外，請檢查連接至 Storage Gateway VPC端點的安全群組。連接至端點的預設安全群組可能不允許必要的連接埠。建立新的安全群組，允許來自閘道 IP 地址範圍的流量透過所需的連接埠。然後，將該安全群組連接到VPC端點。

> **Note**
>
> 使用 Amazon VPC主控台來驗證連接到VPC端點的安全群組。從主控台檢視 Storage Gateway VPC端點，然後選擇安全群組索引標籤。

若要確認所需的連接埠已開啟，您可以在 Storage Gateway VPC端點上執行 telnet 命令。您必須從與閘道位於相同子網路的伺服器執行這些命令。您可以對未指定可用區域DNS的名字執行測試。

例如，下列 telnet 命令會使用DNS名稱 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 測試所需的連接埠連線：

```
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
```

確保防火牆安全不會修改從閘道傳送至 Storage Gateway Amazon VPC端點的封包

SSL 檢查、深層封包檢查或其他形式的防火牆安全可能會干擾從閘道傳送的封包。如果從啟動端點預期修改SSL憑證，SSL交握會失敗。若要確認沒有進行中的SSL檢查，請在 Storage Gateway VPC端點上執行 OpenSSL 命令。您必須從與閘道位於相同子網路的機器執行此命令。為每個必要的連接埠執行命令：

```
$ 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
```

如果沒有進行中的SSL檢查，則命令會傳回類似下列的回應：

```
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
---
```

如果有進行中的SSL檢查，回應會顯示已變更的憑證鏈，如下所示：

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.us-
east-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.us-east-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
```

```
---
```

只有在啟用端點識別SSL憑證時，才會接受SSL交握。這表示，閘道透過所需連接埠傳出至VPC端點的流量不受網路防火牆執行的檢查影響。這些檢查可能是SSL檢查或深度封包檢查。

檢查閘道時間同步

時間過長可能會導致SSL交握錯誤。對於內部部署閘道，您可以使用閘道的本機 VM 主控台來檢查閘道的時間同步。時間偏移不應大於 60 秒。如需詳細資訊，請參閱同步閘道 VM 時間同步閘道 VM 時間。

系統時間管理選項不適用於託管在 Amazon EC2執行個體上的閘道。若要確保 Amazon EC2閘道可以正確同步時間，請確認 Amazon EC2執行個體可以透過連接埠UDP和 TCP 123 連線至下列NTP伺服器集區清單：

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

檢查HTTP代理並確認相關聯的安全群組設定

啟用之前，請檢查 Amazon 上的HTTP代理是否已在內部部署閘道 VM 上EC2設定為連接埠 3128 上的 Squid 代理。在此情況下，請確認下列事項：

- 連接至 Amazon 上HTTP代理的安全群組EC2必須具有傳入規則。此傳入規則必須允許來自閘道 VM IP 地址的連接埠 3128 上的 Squid 代理流量。
- 連接至 Amazon EC2VPC端點的安全群組必須具有傳入規則。這些傳入規則必須允許來自 Amazon 上HTTP代理 IP 地址的連接埠 1026-1028、1031、2222 和 443 上的流量EC2。

解決使用公有端點啟用閘道時出現的錯誤，而且在相同 中有一個 Storage Gateway VPC端點 VPC

若要解決在相同 中有 Amazon Virtual Private Cloud （ Amazon VPC ） 時，使用公有端點啟用閘道時出現的錯誤VPC，請執行下列檢查和組態。

確認您的 Storage Gateway VPC端點上未啟用啟用私有DNS名稱設定

如果啟用私有DNS名稱已啟用，則您無法從啟用任何閘道VPC到公有端點。

若要停用私有DNS名稱選項：

1. 開啟 Amazon VPC主控台 。
2. 在導覽窗格中選擇端點。
3. 選擇 Storage Gateway VPC端點。
4. 選擇動作。
5. 選擇管理私有DNS名稱 。
6. 針對啟用私有DNS名稱 ，清除此端點 的啟用。
7. 選擇修改私有DNS名稱以儲存設定。

對內部部署閘道問題進行疑難排解

您可以在下方找到使用內部部署閘道時可能遇到的典型問題的相關資訊，以及如何啟用 AWS Support 以協助疑難排解閘道。

下表列出使用內部部署閘道時一般可能遇到的問題。

問題	採取動作
您找不到閘道的 IP 地址。	使用虛擬化管理程序用戶端連線到您的主機，尋找閘道 IP 地址。 • 對於 VMware ESXi，您可以在摘要索引標籤的 vSphere 用戶端中找到 VM 的 IP 地址。 • 若為 Microsoft Hyper-V，登入本機主控台即可找到 VM 的 IP 地址。 如果仍找不到閘道 IP 地址： • 請檢查 VM 是否開啟。只有在 VM 開啟時，才會將 IP 地址指派給您的閘道。 • 等候 VM 啟動完成。如果您的 VM 才剛開啟，閘道可能需要幾分鐘才能完成開機序列。
您有網路或防火牆的問題。	• 允許閘道使用適當的連接埠。

問題	採取動作
	• SSL 不應啟用憑證驗證/檢查。Storage Gateway 使用相互TLS身分驗證，如果任何第三方應用程式嘗試攔截/簽署其中一個憑證，則此身分驗證會失敗。 • 若您使用防火牆或路由器來篩選或限制網路流量，則必須設定防火牆和路由器，以允許這些服務端點可與 AWS進行傳出通訊。如需網路和防火牆需求的詳細資訊，請參閱 網路與防火牆需求。
當您在 Storage Gateway 管理主控台中按一下繼續啟用按鈕時，您的閘道啟用會失敗。	• 從您的用戶端 ping VM，檢查是否可存取閘道 VM。 • 檢查您的 VM 是否有網際網路的網路連線。否則，您將需要設定 SOCKS代理。如需這項作業的詳細資訊，請參閱為您的內部部署閘道設定SOCKS5代理。 • 檢查主機是否具有正確的時間、主機是否設定為自動將其時間同步到網路時間通訊協定 （NTP） 伺服器，以及閘道 VM 是否具有正確的時間。如需有關同步 Hypervisor 主機和 的時間的資訊VMs，請參閱 將 VM 時間與 Hyper-V 或 Linux KVM 主機時間同步。 • 執行完這些步驟後，您可以使用 Storage Gateway 主控台和設定與啟用閘道精靈，重試閘道部署。 • SSL 不應啟用憑證驗證/檢查。Storage Gateway 使用相互TLS身分驗證，如果任何第三方應用程式嘗試攔截/簽署其中一個憑證，則此身分驗證會失敗。 • 檢查您的 VM 是否具有至少 7.5 GB 的 。 RAM如果小於 7.5 GB 的 ，閘道配置會失敗。 RAM如需詳細資訊，請參閱設定磁帶閘道的需求。
您需要移除配置為上傳緩衝空間的磁碟。例如，您可能希望減少閘道的上傳緩衝空間，或者您可能需要替換用作上傳緩衝但故障的磁碟。	如需關於移除配置為上傳緩衝空間之磁碟的說明，請參閱 從閘道移除磁碟。

問題	採取動作
您需要改善閘道與 AWS之間的頻寬。	您可以透過在網路轉接器（ ）AWS 上設定網際網路連線，與連接應用程式和閘道 VM 的介面卡（NIC）分開， AWS 來改善從閘道到的頻寬。如果您與 有高頻寬連線， AWS 而且想要避免頻寬爭用，尤其是在快照還原期間，採取此方法非常有用。對於高輸送量工作負載的需求，您可以使用 AWS Direct Connect 在內部部署閘道和 AWS 之間建立專用網路連線。若要測量從閘道到 的連線頻寬 AWS，請使用閘道的 `CloudBytesDownloaded` 和 `CloudBytesUploaded` 指標。如需此主題的詳細資訊，請參閱測量磁帶閘道與 之間的效能 AWS。提升網際網路連線能力有助於確保您的上傳緩衝區不會用盡。

閘道的出入輸送量降到零。	• 在 Storage Gateway 主控台的閘道索引標籤上，確認閘道 VM 的 IP 地址與您使用 Hypervisor 用戶端軟體（即VMware vSphere 用戶端或 Microsoft Hyper-V Manager）看到的相同。如果您發現不相符，請從 Storage Gateway 主控台重新啟動您的閘道，如 關閉閘道 VM 所述。重新啟動後，Storage Gateway 主控台之閘道標籤中的 IP 地址清單中的地址，應該符合您從虛擬化管理程序用戶端決定的閘道 IP 地址。
	  • 對於 VMware ESXi，您可以在摘要索引標籤的 vSphere 用戶端中找到 VM 的 IP 地址。
	  • 若為 Microsoft Hyper-V，登入本機主控台即可找到 VM 的 IP 地址。
	• 檢查閘道對 的連線 AWS ，如 中所述測試您的閘道連線至網際網路。
	• 檢查您閘道的 NIC 組態，並確保所有打算為閘道啟用的介面皆已啟用。若要查看您閘道的網路轉接器組態，請按照設定您的閘道網路中的指示操作，並選取檢視您閘道網路組態的選項。
	
	您可以從 Amazon CloudWatch 主控台檢視閘道往返的輸送量。如需測量閘道和 之間輸送量的詳細資訊 AWS，請參閱 測量磁帶閘道與之間的效能 AWS。

問題	採取動作
您無法在 Microsoft Hyper-V 匯入 (部署) Storage Gateway。	請參閱 為 Microsoft Hyper-V 設定進行疑難排解，以了解在 Microsoft Hyper-V 部署閘道的常見問題。
您會收到以下訊息：「The data that has been written to the volume in your gateway isn't securely stored at AWS」。	如果您的閘道 VM 是從另一個閘道 VM 的複製或快照所建立，就會收到此訊息。如果不是這種情況，請聯絡 AWS Support。

允許 AWS Support 協助疑難排解內部部署託管的閘道

Storage Gateway 提供本機主控台，可用來執行多項維護任務，包括啟用 AWS Support 以存取閘道，協助您疑難排解閘道問題。根據預設，閘道的 AWS Support 存取已停用。您可以透過主機的本機主控台提供此存取。若要允許 AWS Support 存取閘道，請先登入主機的本機主控台，導覽至 Storage Gateway 的主控台，然後連線至支援伺服器。

允許 AWS Support存取您的閘道

1. 登入您主機的本機主控台。
   - VMware ESXi – 如需詳細資訊，請參閱 使用 存取閘道本機主控台 VMware ESXi。
   - Microsoft Hyper-V：如需詳細資訊，請參閱 使用 Microsoft Hyper-V 存取閘道本機主控台。
2. 出現提示時，輸入對應的數字以選取閘道組態。
3. 輸入 **h** 以開啟可用命令視窗。
4. 執行以下任意一項：
   - 如果您的閘道使用公有端點，請在AVAILABLECOMMANDS視窗中輸入 **`open-support-channel`** 以連線至 Storage Gateway 的客戶支援。允許TCP連接埠 22，以便您可以開啟支援頻道至 AWS。當您連線到客戶支援時，Storage Gateway 會指派一個支援號碼給您。請記下您的支援號碼。
   - 如果您的閘道使用VPC端點，請在AVAILABLECOMMANDS視窗中輸入 **`open-support-channel`**。如果您的閘道未啟用，請提供VPC端點或 IP 地址，以連線至 Storage Gateway

的客戶支援。允許TCP連接埠 22，以便您可以開啟 的支援頻道 AWS。當您連線到客戶支援時，Storage Gateway 會指派一個支援號碼給您。請記下您的支援號碼。

> **Note**
>
> 頻道號碼不是傳輸控制通訊協定/使用者資料包通訊協定（TCP/UDP）連接埠號碼。相反地，閘道會與 Storage Gateway 伺服器建立 Secure Shell（SSH）（TCP 22）連線，並提供連線的支援管道。

5. 建立支援管道後，請將支援服務號碼提供給 ， AWS Support 以便 AWS Support 提供疑難排解協助。
6. 當支援工作階段完成時，請輸入 **q** 將其結束。在 Amazon Web Services Support 通知您支援工作階段完成之前，請勿關閉工作階段。
7. 輸入 **exit** 以登出閘道主控台。
8. 依照提示結束本機主控台。

為 Microsoft Hyper-V 設定進行疑難排解

在 Microsoft Hyper-V 平台上部署 Storage Gateway 時通常可能會遇到的問題如下表所列。

問題	採取動作
您嘗試匯入閘道並收到下列錯誤訊息： "嘗試匯入虛擬機器時發生伺服器錯誤。匯入失敗。在位置 【...】 下找不到虛擬機器匯入檔案。只有在使用 Hyper-V 建立和匯出虛擬機器時，才能匯入虛擬機器。"	此錯誤的發生原因如下： • 如果您不是指向解壓縮閘道來源檔案的根目錄。您在匯入虛擬機器對話方塊中指定的最後一個部分應為 `AWS-Storage-Gateway` 。例如： `C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\` . • 如已部署閘道，但未選取複製虛擬機器選項及勾選匯入虛擬機器對話方塊中的複製所有檔案選項，則 VM 會建立在您解壓縮閘道檔案的位置，而您無法再次由此位置匯入檔案。為修正此問題，請取得原始的解壓縮閘道來源檔案，然後複製到新的位置。使用新的位置做為匯入來源。

問題	採取動作
	如果您打算從一個解壓縮來源檔案位置建立多個閘道，則必須選取複製虛擬機器，並勾選匯入虛擬機器對話方塊中的所有檔案複製方塊。
您嘗試匯入閘道並收到下列錯誤訊息： "嘗試匯入虛擬機器時發生伺服器錯誤。匯入失敗。匯入任務無法從 【...】 複製檔案：檔案存在。（0x80070050）"	如已部署閘道，而您嘗試重複使用存放虛擬硬碟檔案和虛擬機器組態檔案的預設資料夾，則會發生此錯誤。若要修正此問題，請在 Hyper-V 設定對話方塊左側面板中的伺服器下指定新位置。
您嘗試匯入閘道並收到下列錯誤訊息： "嘗試匯入虛擬機器時發生伺服器錯誤。匯入失敗。Import failed because the virtual machine must have a new identifier. Select a new identifier and try the import again."。	當您匯入閘道時，請務必選取複製虛擬機器，並勾選匯入虛擬機器對話方塊中的所有檔案複製方塊，以為虛擬機器建立新的唯一 ID。
您嘗試啟動閘道 VM 並收到下列錯誤訊息： "嘗試啟動選取的虛擬機器（s）時發生錯誤。子分割區處理器設定與父分割區不相容。'AWS-Storage-Gateway' 無法初始化。（虛擬機器 ID 【...】）	此錯誤可能是由於CPUs閘道所需的 與主機CPUs上可用的 CPU之間的差異所致。確保基礎 Hypervisor 支援 VM CPU計數。 如需關於 Storage Gateway 需求的詳細資訊，請參閱 設定磁帶閘道的需求。

問題	採取動作
您嘗試啟動閘道 VM 並收到下列錯誤訊息： "嘗試啟動選取的虛擬機器（s）時發生錯誤。'AWS-Storage-Gateway' 無法初始化。（虛擬機器 ID 【...】）無法建立分割區：系統資源不足，無法完成請求的服務。（0x800705AA）"	此錯誤可能是由於RAM閘道所需的 與主機RAM上可用的 之間存在RAM差異所致。 如需關於 Storage Gateway 需求的詳細資訊，請參閱 設定磁帶閘道的需求。
您的快照和閘道軟體更新出現的次數會和預期的稍有不同。	閘道 VM 的時鐘可能會從實際的時間偏移，稱為時鐘飄移。請使用本機閘道主控台的時間同步選項，檢查並更正 VM 的時間。如需詳細資訊，請參閱將 VM 時間與 Hyper-V 或 Linux KVM 主機時間同步。
您需要將解壓縮的 Microsoft Hyper-V Storage Gateway 檔案放在主機的檔案系統。	像您對一般 Microsoft Windows 伺服器所做的一樣，存取主機。例如，如果 Hypervisor 主機是名稱 `hyperv-server` ，則您可以使用下列UNC路徑 `\\hyperv-server\c$` ，其假設`hyperv-server` 名稱可以解析或在本機主機檔案中定義。
連線到虛擬化管理程序時，系統會提示您提供登入資料。	使用 Sconfig.cmd 工具新增您的使用者登入資料，做為虛擬化管理程序主機的本機管理員。
如果您為使用 Broadcom 網路轉接器的 Hyper-V 主機開啟虛擬機器佇列（VMQ），您可能會注意到網路效能不佳。	如需解決方法的相關資訊，請參閱 Microsoft 文件，請參閱若開啟 VMQ，則 Windows Server 2012 Hyper-V 主機上的虛擬機器網路效能不佳。

疑難排解 Amazon EC2 閘道問題

在以下各節中，您可以找到使用 Amazon 上部署的閘道時可能會遇到的典型問題EC2。如需現場部署閘道與 Amazon 中部署的閘道之間差異的詳細資訊EC2，請參閱部署適用於磁帶閘道的自訂 Amazon EC2執行個體。

主題

您的閘道在一段時間後仍未啟用

在 Amazon EC2 控制台中檢查以下內容：

- 已於執行個體相關聯的安全群組中啟用連接埠 80。如需新增安全群組規則的詳細資訊，請參閱 Amazon EC2 使用者指南中的新增安全群組規則。
- 閘道執行個體標示為執行中。在 Amazon 主EC2控台中，執行個體的 [狀態] 值應為RUNNING。
- 確保您的 Amazon EC2 執行個體類型符合最低需求，如中所述儲存需求。

更正問題後，請嘗試再次啟動閘道。若要這樣做，請開啟 Storage Gateway 主控台，選擇在 Amazon 上部署新閘道EC2，然後重新輸入執行個體的 IP 位址。

您無法在執行個體清單中找到EC2閘道執行個體

如果您並未建立執行個體的資源標籤，又有許多執行個體正在執行，要分辨您啟動了哪些執行個體會十分困難。在這種情況下，您可以執行以下動作，尋找閘道執行個體：

- 在執行個體的說明索引標籤上檢查 Amazon 機器映像 (AMI) 的名稱。以 Storage Gateway 為基礎的執行個體AMI應該以文字開頭**`aws-storage-gateway-ami`**。

- 如果您有多個以 Storage Gateway 為基礎的執行個體AMI，請檢查執行個體啟動時間以尋找正確的執行個體。

您已建立 Amazon EBS 磁碟區，但無法將其連接到EC2閘道執行個體

檢查有問題的 Amazon EBS 磁碟區是否與閘道執行個體位於相同的可用區域。如果可用區域存在差異，請在與執行個體相同的可用區域中建立新的 Amazon EBS 磁碟區。

當您嘗試新增儲存磁碟區時，收到無磁碟可用的訊息

最近啟用的閘道未定義儲存磁碟區。您必須先配置本機磁碟到閘道，用作上傳緩衝和快取儲存，才能定義磁碟區儲存。對於部署到 Amazon 的閘道EC2，本機磁碟是連接到執行個體的 Amazon EBS 磁碟區。發生此錯誤訊息可能是因為沒有為執行個體定義 Amazon EBS 磁碟區。

檢查執行閘道的執行個體是否有定義的區塊型儲存裝置。如果只有兩個區塊裝置 (隨附的預設裝置AMI)，則您應該新增儲存空間。如需這項作業的詳細資訊，請參閱部署適用於磁帶閘道的自訂 Amazon EC2執行個體。連接兩個或多個 Amazon EBS 磁碟區後，請嘗試在閘道上建立磁碟區儲存。

您想要移除配置為上傳緩衝空間的磁碟，以減少上傳緩衝空間

請遵循 判斷要配置的上傳緩衝大小 中的步驟。

進出EC2閘道的輸送量降至零

確認閘道執行個體正在執行。如果執行個體因為重新啟動等原因而啟動，請等待執行個體重新啟動。

此外，請確認閘道 IP 沒有變更。如果執行個體在停止後又重新啟動，則執行個體的 IP 地址可能會變更。在這種情況下，您需要啟用新的閘道。

您可以從 Amazon CloudWatch 主控台檢視進出閘道的輸送量。如需有關測量進出閘道輸送量的詳細資訊 AWS，請參閱測量磁帶閘道與 之間的效能 AWS。

您想 AWS Support 要協助疑難排解EC2閘道

Storage Gateway 提供了一個本機主控台，可讓您用來執行多項維護工作，包括啟動 AWS Support 以存取閘道以協助您疑難排解閘道問題。根據預設，會停用對閘道的 AWS Support 存取。您可以透過 Amazon EC2 本機主控台提供此存取權。您可以透過安全殼層 (SSH) 登入 Amazon EC2 本機主控台。若要透過成功登入SSH，執行個體的安全性群組必須具有開啟通TCP訊埠 22 的規則。

> **Note**
>
> 如果您將新的規則新增至現有的安全群組，新的規則將套用到使用該安全群組的所有執行個體。如需有關安全群組以及如何新增安全群組規則的詳細資訊，請參閱 Amazon EC2使用者指南中的 Amazon EC2 安全群組。

若要讓您 AWS Support 連線到閘道，請先登入 Amazon EC2 執行個體的本機主控台，導覽至 Storage Gateway 的主控台，然後提供存取權。

啟 AWS Support 用對 Amazon EC2 執行個體上部署閘道的存取

1. 登入 Amazon EC2 執行個體的本機主控台。如需指示，請前往 Amazon EC2 使用者指南中的 Connect 到您的執行個體。

   您可以使用下列命令登入EC2執行個體的本機主控台。

   ```
   ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
   ```

   > **Note**
   >
   > 所以此 *PRIVATE-KEY* 是包.pem含您用來啟動 Amazon EC2 執行個體之 EC2 key pair 私有憑證的檔案。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的擷取 key pair 的公開金鑰。
   > 所以此 *INSTANCE-PUBLIC-DNS-NAME* 是您的閘道執行所在的 Amazon EC2 執行個體的公有網域名稱系統 (DNS) 名稱。您可以在EC2主控台中選取 Amazon EC2 執行個體，然後按一下「說明」索引標籤，以取得此公用DNS名稱。

2. 出現提示時，輸入 **`6 - Command Prompt`** 以開啟 AWS Support 管道主控台。
3. 輸入**h**以打開AVAILABLECOMMANDS窗口。
4. 執行以下任意一項：

   - 如果您的閘道使用公用端點，請在AVAILABLECOMMANDS視窗中輸入**`open-support-channel`**以連線至 Storage Gateway 的客戶支援。允許TCP端口 22，以便您可以打開支持渠道AWS。當您連線到客戶支援時，Storage Gateway 會指派一個支援號碼給您。請記下您的支援號碼。

- 如果您的閘道使用VPC端點，請在AVAILABLECOMMANDS視窗中輸入**`open-support-channel`**。如果您的閘道未啟動，請提供VPC端點或 IP 位址，以連線至 Storage Gateway 的客戶支援。允許TCP端口 22，以便您可以打開支持渠道 AWS。當您連線到客戶支援時，Storage Gateway 會指派一個支援號碼給您。請記下您的支援號碼。

> **Note**
>
> 通道號碼不是傳輸控制通訊協定/使用者資料包通訊協定 (TCP/UDP) 連接埠號碼。而是，閘道會與 Storage Gateway 道伺服器建立安全殼層 (SSH) (TCP22) 連線，並提供連線的支援通道。

5. 建立支援管道後，請提供您的支援服務號碼， AWS Support 以 AWS Support 便提供疑難排解協助。
6. 當支援工作階段完成時，請輸入 **`q`** 將其結束。 AWS Support 在通知您支援工作階段完成之前，請勿關閉工作階段。
7. 輸入 **`exit`** 以結束 Storage Gateway 主控台。
8. 依照主控台選單操作登出 Storage Gateway 執行個體。

您想要使用 Amazon EC2 序列主控台連線到閘道執行個體

您可以使用 Amazon EC2 序列主控台對開機、網路組態和其他問題進行疑難排解。如需指示和疑難排解秘訣，請參閱 Amazon 彈性運算雲端使用者指南中的 Amazon EC2 序列主控台。

為硬體設備問題進行疑難排解

下列主題討論您可能會遇到的 Storage Gateway 硬體設備問題，以及疑難排解的建議。

您無法確定服務 IP 地址

嘗試連接到服務時，請務必使用服務的 IP 地址，而非主機 IP 地址。在服務主控台中設定服務 IP 地址，並在硬體主控台設定主機 IP 地址。當您啟動硬體設備時會看到硬體主控台。若要從硬體主控台前往服務主控台，請選擇 Open Service Console (開啟服務主控台)。

如何執行重設成出廠預設值？

如果您需要在裝置上執行重設成出廠預設值，請聯絡 Storage Gateway 硬體設備團隊以請求支援，如下列「支援」部分所述。

如何執行遠端重新啟動？

如果您需要執行裝置的遠端重新啟動，您可以使用 Dell iDRAC 管理介面執行此操作。如需詳細資訊，請參閱 Dell Technologies 網站上的 iDRAC9 Virtual Power Cycle：遠端重新啟動 Dell EMC PowerEdge Server。 InfoHub

您在何處取得 Dell iDRAC 支援？

Dell PowerEdge R640 伺服器隨附 Dell iDRAC 管理介面。我們建議下列作法：

- 如果您使用 iDRAC 管理介面，您應該變更預設密碼。如需 iDRAC 憑證的詳細資訊，請參閱 Dell PowerEdge - i 的預設登入憑證是什麼DRAC？
- 請確定韌體 up-to-date 是為了防止安全漏洞。
- 將 iDRAC 網路介面移至正常（ em ）連接埠可能會導致效能問題或導致設備無法正常運作。

您找不到硬體設備序號

您可以使用 Storage Gateway 主控台找到 Storage Gateway 硬體設備的序號。

若要尋找硬體設備序號：

1. 開啟位於首頁 的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/
2. 在頁面左側的導覽窗格選擇硬體。
3. 從清單中選取您的硬體設備。
4. 在設備的詳細資訊索引標籤上尋找序號欄位。

在何處取得硬體設備支援

若要聯絡 AWS 以取得硬體設備的技術支援，請參閱 AWS Support。

AWS Support 團隊可能會要求您啟用支援管道，以遠端疑難排解您的閘道問題。不需要將此連接埠開放給閘道的正常操作使用，但進行疑難排解時需要用到。您可以從硬體主控台啟用支援管道，如以下程序所示。

開啟 的支援管道 AWS

1. 開啟硬體主控台。
2. 選擇硬體主控台首頁底部的開放支援管道，然後按 `Enter`。

如果沒有網路連線或防火牆問題，指派的連接埠號碼應該會在 30 秒內顯示。例如：

狀態：在連接埠 19599 上開啟

3. 記下連接埠號碼，並將其提供給 AWS Support。

為虛擬磁帶問題進行故障診斷

如果您的虛擬磁帶發生非預期問題，您可在下列資訊中找到應採取的動作。

主題

- 從無法還原的閘道復原虛擬磁帶
- 為無法還原的磁帶進行故障診斷
- 高可用性運作狀態通知

從無法還原的閘道復原虛擬磁帶

雖然這種情況極少發生，但您的磁帶閘道可能遇到無法還原的故障。這種故障會發生在您的虛擬化管理程序主機、閘道本身或快取磁碟。如果發生故障，您可以依照本節的故障診斷指示復原您的磁帶。

主題

- 您需要從故障的磁帶閘道復原虛擬磁帶
- 您需要從故障的快取磁碟復原虛擬磁帶

您需要從故障的磁帶閘道復原虛擬磁帶

如果您的磁帶閘道或 Hypervisor 主機發生無法復原的故障，您可以復原任何已上傳 AWS 到其他磁帶閘道的資料。

請注意，寫入磁帶的資料可能無法完全上傳，直到磁帶成功存檔至該磁帶VTS。以此方式還原到另一個閘道的磁帶資料可能會不完整或為空白。建議您對所有復原的磁帶執行清查，確定磁帶包含預期的內容。

將磁帶復原到另一個磁帶閘道

1. 找出現有的運作中磁帶閘道，做為您的復原目標閘道。如果您沒有磁帶復原目標的磁帶閘道，請建立一個新的磁帶閘道。如需如何建立閘道的資訊，請參閱建立閘道。

2. 在https://console.aws.amazon.com/storagegateway/首頁開啟 Storage Gateway 主控台。
3. 在導覽窗格中，選擇閘道，然後選擇您想要復原磁帶的來源磁帶閘道。
4. 選擇詳細資訊索引標籤。標籤中會顯示磁帶復原的訊息。
5. 選擇建立復原磁帶以停用閘道。
6. 在出現的對話方塊中，選擇 Disable gateway (停用閘道)。

   此程序會永久停止磁帶閘道的正常功能，並公開任何可用的復原點。如需指示，請參閱停用磁帶閘道。
7. 從停用閘道所顯示的磁帶，選擇您要復原的虛擬磁帶和復原點。虛擬磁帶可有多個復原點。
8. 若要開始將任何您所需的磁帶復原至目標磁帶閘道，請選擇建立復原磁帶。
9. 在 Create recovery tape (建立復原磁帶) 對話方塊中，確認您想要復原的虛擬磁帶條碼。
10. 針對閘道，選擇您要復原虛擬磁帶的目標磁帶閘道。
11. 選擇 Create recovery tape (建立復原磁帶)。
12. 刪除故障的磁帶閘道，以免付費。如需說明，請參閱 刪除閘道並移除相關資源。

Storage Gateway 會將磁帶從故障的磁帶閘道移至您指定的磁帶閘道。磁帶閘道會將磁帶狀態標記為 RECOVERED。

您需要從故障的快取磁碟復原虛擬磁帶

如果您的快取磁碟發生錯誤，閘道會阻止閘道中對虛擬磁帶的讀寫操作。例如，當磁碟損毀或從閘道移除時可能會發生錯誤。Storage Gateway 主控台會顯示有關錯誤的訊息。

在錯誤訊息中，Storage Gateway 會提示您從兩個可以復原磁帶的動作中，採取其中一個動作：

- 關閉和重新新增磁碟：如果磁碟資料不變且已移除，請採用此方法。例如，如果因為意外從主機移除磁碟而發生錯誤，不過磁碟和資料皆保持不變，您可以重新新增磁碟。若要執行此作業，請參閱本主題後文的程序。
- 重設快取磁碟：如果快取磁碟損毀或無法存取，請採用此方法。如果磁碟錯誤導致快取磁碟無法存取、無法使用或損毀，您可以重設磁碟。您若重設快取磁碟，則資料無誤的磁帶 (也就是快取磁碟和 Amazon S3 的資料已經過同步處理的磁帶)，會繼續供您使用。不過，資料未與 Amazon S3 同步的磁帶會自動復原。這些磁帶的狀態設定為RECOVERED，但磁帶將是唯讀的。如需如何從主機移除磁碟的資訊，請參閱判斷要配置的上傳緩衝大小。

> **Important**
>
> 如果您要重設的快取磁碟包含尚未上傳到 Amazon S3 的資料，該資料可能會遺失。在您重設快取磁碟後，閘道中不會留下任何已設定的快取磁碟，因此您至少必須設定一部新的快取磁碟，讓您的閘道正常運作。

若要重設快取磁碟，請參閱本主題後文的程序。

關閉並重新新增磁碟

1. 關機閘道。如需如何關閉閘道的資訊，請參閱關閉閘道 VM。
2. 將磁碟新增回您的主機，並確保磁碟的磁碟節點數目未變化。如需如何新增磁碟的資訊，請參閱判斷要配置的上傳緩衝大小。
3. 重新啟動閘道。如需如何重新啟動閘道的資訊，請參閱關閉閘道 VM。

重新啟動閘道之後，您就可以驗證快取磁碟的狀態。磁碟的狀態可以是下列其中一個：

- present (出現) – 磁碟可供使用。
- missing (遺漏) – 磁碟不再連線到閘道。
- mismatch (不符) – 有錯誤中繼資料的磁碟佔用磁碟節點，或磁碟內容損毀。

重設和重新設定快取磁碟

1. 在前述的 A disk error has occurred (磁碟發生錯誤) 錯誤訊息中，選擇 Reset Cache Disk (重設快取磁碟)。
2. 在設定閘道頁面上，設定磁碟用於快取儲存。如需如何設定磁帶閘道的相關資訊，請參閱設定磁帶閘道。
3. 在您設定快取儲存後，請關閉並重新啟動閘道，如之前程序中所述。

閘道應會在重新啟動後復原。然後，您可以驗證快取磁碟的狀態。

驗證快取磁碟的狀態

1. 在https://console.aws.amazon.com/storagegateway/首頁開啟 Storage Gateway 主控台。

2. 在導覽窗格中，選擇 Gateways (閘道)，然後選擇您的閘道。
3. 在 Actions (動作) 上，選擇 Configure Local Storage (設定本機儲存) 以顯示 Configure Local Storage (設定本機儲存) 對話方塊。此對話方塊會顯示閘道中的所有本機磁碟。

快取磁碟節點狀態顯示在磁碟旁。

> **Note**
>
> 如果您不完成復原程序，閘道會顯示一個橫幅，提示您設定本機儲存。

為無法還原的磁帶進行故障診斷

如果您的虛擬磁帶意外故障，儲存裝置閘道會將故障虛擬磁帶的狀態設定為IRRECOVERABLE。您採取的動作視情況而定。您可在以下資訊中找到一些您可能發現的問題，以及如何對其故障診斷。

您需要從IRRECOVERABLE磁帶復原資料

如果您的虛擬磁帶具有狀態IRRECOVERABLE，而且需要使用它，請嘗試下列其中一種方法：

- 如未啟用磁帶閘道，請啟用新的磁帶閘道。如需詳細資訊，請參閱建立閘道。
- 停用包含無法還原磁帶的磁帶閘道，並從新磁帶閘道的復原點復原磁帶。如需詳細資訊，請參閱您需要從故障的磁帶閘道復原虛擬磁帶。

  > **Note**
  >
  > 您必須重新設定 i SCSI 啟動器和備份應用程式，才能使用新的磁帶閘道。如需詳細資訊，請參閱連接VTL您的裝置。

您不需要未封存的IRRECOVERABLE磁帶

如果您的虛擬磁帶狀態IRRECOVERABLE不需要，而且磁帶從未封存，您應該刪除磁帶。如需詳細資訊，請參閱從磁帶閘道刪除虛擬磁帶。

您閘道的快取磁碟發生故障

如果您閘道的一個或多個快取磁碟發生故障，閘道會阻止對虛擬磁帶和磁碟區的讀寫操作。若要還原正常功能，請依照下列說明重新設定閘道：

- 如果快取磁碟無法存取或無法使用，請從閘道組態中刪除磁碟。
- 如果快取磁碟仍然可以存取且可使用，請將其重新連線到閘道。

> **Note**
>
> 當閘道恢復正常功能時，如果刪除具有清除資料 (亦即快取磁碟和 Amazon S3 中的資料同步處理的快取磁碟、磁帶或磁碟區)仍可用。例如，如果閘道有三個快取磁碟，而您刪除兩個快取磁碟，則清除的磁帶或磁碟區就會有AVAILABLE狀態。其他磁帶和磁碟區將會有IRRECOVERABLE狀態。
>
> 如果您使用暫時磁碟做為閘道的快取磁碟，或將快取磁碟掛載到暫時磁碟機上，當您關閉閘道時，快取磁碟將會遺失。在快取磁碟和 Amazon S3 不同步時關閉閘道可能會導致資料遺失。因此，我們建議您不要使用臨時磁碟機或磁碟。

高可用性運作狀態通知

在VMware vSphere 高可用性 (HA) 平台上執行閘道時，您可能會收到健全狀況通知。如需運作狀態通知的詳細資訊，請參閱為高可用性問題進行故障診斷。

為高可用性問題進行故障診斷

如果發生可用性問題，您可在下列資訊中找到應採取的動作。

主題

運作狀態通知

當您在 VMware vSphere HA 上執行閘道時，所有閘道都會向您設定的 Amazon CloudWatch 日誌群組產生下列運作狀態通知。這些通知會進入名為 `AvailabilityMonitor` 的日誌串流。

主題

- 通知： HealthCheckFailure
- 通知： AvailabilityMonitorTest

通知：重新啟動

當閘道 VM 重新啟動時，您可能會收到重新啟動通知。您可以使用 VM Hypervisor Management 主控台或 Storage Gateway 主控台來重新啟動閘道 VM。您也可以在閘道維護週期期間使用閘道軟體來重新啟動。

採取動作

如果重新啟動的時間在閘道所設定之維護開始時間的 10 分鐘以內，這可能是正常的情況，而不是任何問題的徵兆。如果重新啟動很常在維護時段外發生，請檢查閘道是否已手動重新啟動。

通知： HardReboot

當閘道 VM 意外重新啟動時，您可能會收到 `HardReboot` 通知。這種重新啟動可能是因為電源中斷、硬體故障或其他事件。若是 VMware 閘道，由 vSphere High Availability Application Monitoring 執行的重設可能會啟動此事件。

採取動作

當閘道在這種環境中執行時，請檢查 `HealthCheckFailure` 通知是否存在，並參閱 VM 的 VMware 事件記錄。

通知： HealthCheckFailure

若是 VMware vSphere HA 上的閘道，當運作狀態檢查失敗且請求 VM 重新啟動時，您可能會收到 `HealthCheckFailure` 通知。此事件也會在監控可用性的測試期間發生，並顯示於 `AvailabilityMonitorTest` 通知中。在此情況下，則預期會收到`HealthCheckFailure` 通知。

> **Note**
>
> 此通知僅適用於 VMware 閘道。

採取動作

如果此事件在沒有 `AvailabilityMonitorTest` 通知的情況下重複發生，請檢查您的 VM 基礎設施是否有問題 (儲存空間、記憶體等)。如果您需要其他協助，請聯絡 AWS Support。

通知： AvailabilityMonitorTest

對於 VMware vSphere HA 上的閘道，您可以在 VMware 中執行可用性和應用程式監控系統的測試時收到 `AvailabilityMonitorTest` 通知。

指標

`AvailabilityNotifications` 指標可在所有閘道上使用。此指標會計算閘道產生的可用相關運作狀態通知數目。使用 `Sum` 統計資料，即可觀察閘道是否發生任何可用性相關事件。如需有關事件的詳細資訊，請洽詢您設定的 CloudWatch 記錄群組。

Tape Gateway 的最佳實務

本節包含下列主題，提供有關使用閘道、本機磁碟、快照和資料之最佳實務的資訊。我們建議您熟悉本節中概述的資訊，並嘗試遵循這些準則，以避免 發生問題 AWS Storage Gateway。如需診斷和解決部署時可能遇到的常見問題的其他指引，請參閱 為您的閘道進行疑難排解。

主題

- 最佳實務：復原資料
- 清除不必要的資源

最佳實務：復原資料

雖然這種情況極少發生，但您的閘道可能遇到無法復原的故障。這種故障可能發生在您的虛擬機器 (VM)、閘道本身、本機儲存體或其他地方。如果發生故障，我們建議您按照下列合適各節中的指示來復原資料。

> **Important**
>
> Storage Gateway 不支援從 Hypervisor 或 Amazon Machine Image （ ） EC2 建立的快照復原閘道 VMAMI。若您的閘道 VM 發生問題，請啟用新的閘道，並使用下列指示將您的資料復原至該閘道。

主題

- 從非預期的虛擬機器關機復原
- 從故障的閘道或 VM 復原資料
- 從無法復原的磁帶復原資料
- 從故障的快取磁碟復原資料
- 從無法存取的資料中心復原資料

從非預期的虛擬機器關機復原

如果您的 VM 因非預期原因關閉 (例如停電)，您的閘道就會無法連接。當電力和網路連線還原後，您的閘道就可以連接並開始正常運作。下列是您可在此時採取的步驟，有利於復原您的資料：

- 如果中斷導致網路連線問題，您可以故障診斷此問題。如需如何測試網路連線的資訊，請參閱測試您的閘道連線至網際網路。
- 對於磁帶設定，當閘道可連線時，磁碟磁帶會進入BOOTSTRAPPING狀態。此功能可確保本機儲存的資料持續與 同步 AWS。如需此狀態的詳細資訊，請參閱了解磁帶狀態。
- 如果您的閘道發生磁碟區或磁帶故障和問題，以致非預期關機，您可以復原您的資料。有關如何復原資料的資訊，請參閱下列適用於您案例的各節。

從故障的閘道或 VM 復原資料

如果您的磁帶閘道或 Hypervisor 主機發生無法復原的故障，您可以使用下列步驟將故障磁帶閘道的磁帶復原至另一個磁帶閘道的磁帶：

1. 識別您想要用作復原目標的磁帶閘道，或建立新的磁帶閘道。
2. 停用故障閘道。
3. 為每個您希望復原的磁帶建立復原磁帶，並指定目標磁帶閘道。
4. 刪除故障磁帶閘道。

如需如何將故障磁帶閘道中的磁帶復原至另一個磁帶閘道的詳細資訊，請參閱 您需要從故障的磁帶閘道復原虛擬磁帶。

從無法復原的磁帶復原資料

如果您的磁帶遇到故障，且磁帶的狀態為 IRRECOVERABLE，我們建議您使用下列其中一個選項來復原資料或根據您的情況解決故障：

- 如果您需要無法復原磁帶上的資料，您可以將該磁帶復原到新的閘道。
- 如果您不需要磁帶上的資料，而且磁帶從未存檔，僅要從磁帶閘道刪除磁帶即可。

  如需有關磁帶為 時如何復原資料或解決失敗的詳細資訊IRRECOVERABLE，請參閱 為無法還原的磁帶進行故障診斷。

從故障的快取磁碟復原資料

如果您的快取磁碟發生故障，我們建議根據您的情況，使用下列步驟復原您的資料：

- 如果發生故障的原因是快取磁碟已從您的主機移除，請關閉閘道、重新新增磁碟並重新啟動閘道。

- 如果快取磁碟損毀或無法存取，請關閉閘道、重設快取磁碟、重設快取儲存磁碟並重新啟動閘道。

如需詳細資訊，請參閱 您需要從故障的快取磁碟復原虛擬磁帶。

從無法存取的資料中心復原資料

如果您的閘道或資料中心因某種原因而無法存取，您可以將資料復原至不同資料中心的另一個閘道，或復原至託管在 Amazon EC2執行個體上的閘道。如果您無法存取其他資料中心，建議您在 Amazon EC2執行個體上建立閘道。您遵循的步驟取決於處理資料的閘道類型。

從無法存取之資料中心的磁帶閘道復原資料

1. 在 Amazon EC2 主機上建立新的磁帶閘道。如需詳細資訊，請參閱部署適用於磁帶閘道的自訂 Amazon EC2執行個體。
2. 將磁帶從資料中心的來源閘道復原到您在 Amazon 上建立的新閘道EC2。如需詳細資訊，請參閱 從無法還原的閘道復原虛擬磁帶。

   您的磁帶應涵蓋在新的 Amazon EC2閘道。

清除不必要的資源

如果您已建立閘道做為範例練習或測試，請考慮清除，避免產生意外或非必要的費用。

如果您打算繼續使用磁帶閘道，請參閱 接下來做些什麼？ 中的其他資訊

清除不需要的資源

1. 從閘道的虛擬磁帶程式庫（VTL）和封存中刪除磁帶。如需詳細資訊，請參閱刪除閘道並移除相關資源。

   a. 封存閘道 RETRIEVED中狀態為 的任何磁帶VTL。如需說明，請參閱 存檔磁帶。
   b. 從閘道的 刪除任何剩餘的磁帶VTL。如需說明，請參閱 從磁帶閘道刪除虛擬磁帶。
   c. 刪除您在存檔中的任何磁帶。如需說明，請參閱 從磁帶閘道刪除虛擬磁帶。
2. 除非您打算繼續使用磁帶閘道，否則請予以刪除：如需說明，請參閱 刪除閘道並移除相關資源。
3. 從內部部署主機刪除 Storage Gateway VM。如果您在 Amazon EC2執行個體上建立閘道，請終止執行個體。

其他 Storage Gateway 資源

本節說明可協助您設定或管理閘道 AWS 的第三方軟體、工具和資源，以及 Storage Gateway 配額。

主題

- 部署和設定閘道 VM 主機 - 了解如何部署和設定閘道的虛擬機器主機。
- 使用磁帶閘道儲存資源 - 了解與磁帶閘道儲存資源相關的程序，例如移除本機磁碟、管理 Amazon EBS磁碟區、使用虛擬磁帶程式庫裝置，以及管理虛擬磁帶程式庫中的磁帶。
- 取得閘道的啟用金鑰 - 了解部署新閘道時，在哪裡可以找到您需要提供的啟用金鑰。
- 連接 iSCSI 啟動器 - 了解如何使用公開為網際網路小型電腦系統介面 （iVTL） 目標的磁碟區或虛擬磁帶程式庫 （SCSI） 裝置。
- AWS Direct Connect 搭配 Storage Gateway 使用 - 了解如何在內部部署閘道與 AWS 雲端之間建立專用網路連線。
- Tape Gateway 的連接埠需求 - 尋找磁帶閘道所需網路連接埠的特定資訊。
- 取得閘道設備的 IP 地址 - 了解在哪些位置可以找到部署新閘道時必須提供的閘道虛擬機器主機 IP 地址。
- 了解 Storage Gateway 資源與資源 IDs - 了解如何 AWS 識別 Storage Gateway 建立的資源和子資源。
- 為 Storage Gateway 資源加上標籤 - 了解如何使用中繼資料標籤來分類您的資源，並使其更容易管理。
- 使用 Storage Gateway 的開放原始碼元件 - 了解用於提供 Storage Gateway 功能的第三方工具和授權。
- AWS Storage Gateway 配額 - 了解磁帶閘道的限制和配額，包括磁帶大小和數量的最大限制，以及本機磁碟大小建議。

部署和設定閘道 VM 主機

本節中的主題描述如何設定和管理 Storage Gateway 設備的虛擬機器主機，包括在 VMware、Hyper-V 或 Linux 上執行的就地部署設備KVM，以及在 AWS 雲端 Amazon EC2執行個體上執行的設備。

主題

- 部署磁帶閘道的預設 Amazon EC2 主機 - 了解如何使用預設規格在 Amazon Elastic Compute Cloud （Amazon EC2） 執行個體上部署和啟用磁帶閘道。

- 部署適用於磁帶閘道的自訂 Amazon EC2執行個體 - 了解如何使用自訂設定在 Amazon Elastic Compute Cloud （ Amazon EC2 ） 執行個體上部署和啟用磁帶閘道。
- 修改 Amazon EC2 執行個體中繼資料 - 了解如何設定您的 Amazon EC2閘道執行個體，以接受使用第 1 IMDS版 （ IMDSv1 ） 的傳入中繼資料請求，或要求所有中繼資料請求使用第 2 IMDS版 （ ）IMDSv2。
- 將 VM 時間與 Hyper-V 或 Linux KVM 主機時間同步 - 了解如何檢視內部部署 Hyper-V 或 Linux KVM 閘道虛擬機器的時間，並將其同步至網路時間通訊協定 （ NTP ） 伺服器。
- 將 VM 時間與VMware主機時間同步 - 了解如何檢查VMware閘道虛擬機器的主機時間，並視需要設定時間並設定主機將其時間自動同步到網路時間通訊協定 （ NTP ） 伺服器。
- 在VMware主機上設定半虛擬化 - 了解如何設定 Storage Gateway 設備的VMware主機平台，以使用平行網際網路小型電腦系統介面通訊協定 （ iSCSI ） 控制器。
- 設定閘道的網路轉接器 - 了解如何重新設定閘道以使用 VMXNET3 （ 10 GbE ） 網路轉接器，或使用多個網路轉接器，以便存取 Fron nultiple IP 地址。
- 搭配 Storage Gateway 使用VMware vSphere 高可用性 - 了解如何透過將 Storage Gateway 設定為使用VMware vSphere 高可用性，以保護您的儲存工作負載免受硬體、Hypervisor 或網路故障的影響。

部署磁帶閘道的預設 Amazon EC2 主機

本主題列出使用預設規格部署 Amazon EC2 主機的步驟。

您可以在 Amazon Elastic Compute Cloud （ AmazonEC2 ） 執行個體上部署和啟用磁帶閘道。 AWS Storage Gateway Amazon Machine Image （ AMI ） 可作為社群 提供AMI。

> **Note**
>
> Storage Gateway 社群AMIs由 發佈並完全支援 AWS。您可以看到發佈者是 AWS，這是經過驗證的提供者。

1. 若要設定 Amazon EC2instance，請在工作流程的平台選項區段中選擇 Amazon EC2 作為主機平台。如需設定 Amazon EC2執行個體的指示，請參閱部署 Amazon EC2執行個體以託管您的磁帶閘道
2. 選取啟動執行個體以在 Amazon EC2主控台中開啟 AWS Storage Gateway AMI 範本，並自訂其他設定，例如執行個體類型 、網路設定 和 設定儲存體 。

3. 或者，您可以在 Storage Gateway 主控台中選取使用預設設定，以部署具有預設組態的 Amazon EC2執行個體。

   使用預設設定建立的 Amazon EC2執行個體具有下列預設規格：

   - 執行個體類型：m5.xlarge
   - 網路設定
     - 針對 VPC，選取您希望EC2執行個體在其中執行VPC的 。
     - 針對子網路 ，指定EC2執行個體應該在其中啟動的子網路。

     > **Note**
     >
     > VPC 只有當子網路從 VPC 管理主控台啟用自動指派公有IPv4地址設定時，子網路才會出現在下拉式清單中。

     - 自動分配公用 IP：已啟動

   EC2 安全群組已建立並與EC2執行個體相關聯。安全群組具有下列傳入連接埠規則：

   > **Note**
   >
   > 在閘道啟動期間，您需要開啟連接埠 80。啟動後，連接埠會立即關閉。此後，您的EC2執行個體只能透過所選 的其他連接埠存取VPC。
   > 閘道上的 iSCSI 目標只能從與VPC閘道相同的主機存取。如果需要從 外部的主機存取 iSCSI 目標VPC，您應該更新適當的安全群組規則。
   > 您可以隨時編輯安全群組，方法是導覽至 Amazon EC2執行個體詳細資訊頁面、選取安全 、導覽至安全群組詳細資訊 ，然後選擇安全群組 ID。

連接埠	通訊協定	檔案系統協定				
80	TCP	HTTP 用於啟用的存取				
3260	TCP	iSCSI				

- 設定儲存

預設設定	AMI 根磁碟區	磁碟區 2 快取	磁碟區 3 快取			
裝置名稱		'/dev/sdb'	'/dev/sdc'			
大小	80 GiB	165 GiB	150 GiB			
磁碟區類型	gp3	gp3	gp3			
IOPS	3000	3000	3000			
在終止時刪除	是	是	是			
Encrypted	否	否	否			
輸送量	125	125	125			

部署適用於磁帶閘道的自訂 Amazon EC2執行個體

您可以在 Amazon Elastic Compute Cloud （ AmazonEC2 ） 執行個體上部署和啟用磁帶閘道。 AWS Storage Gateway Amazon Machine Image （ AMI ） 可作為社群 提供AMI。

> **Note**
>
> Storage Gateway 社群AMIs由 發佈並完全支援 AWS。您可以看到發佈者是 AWS，這是經過驗證的提供者。
> 磁帶閘道AMIs使用以下命名慣例。附加至AMI名稱的版本編號會隨每個版本版本而變更。
> `aws-storage-gateway-CLASSIC-2.9.0`

部署 Amazon EC2執行個體以託管您的磁帶閘道

1. 使用 Storage Gateway 主控台開始設定新閘道。如需指示，請參閱設定磁帶閘道。當您到達平台選項區段時，請選擇 Amazon EC2 作為主機平台 ，然後使用下列步驟啟動將託管磁帶閘道的 Amazon EC2執行個體。
2. 選擇啟動執行個體以在 Amazon EC2主控台中開啟 AWS Storage Gateway AMI範本，您可以在其中設定其他設定。

   使用 Quicklaunch 以預設設定啟動 Amazon EC2執行個體。如需 Amazon EC2 Quicklaunch 預設去連結的詳細資訊，請參閱 Quicklaunch Configuration Specifications for Amazon EC2。
3. 針對名稱 ，輸入 Amazon EC2執行個體的名稱。部署執行個體之後，您可以搜尋此名稱，以在 Amazon EC2主控台的清單頁面上尋找執行個體。
4. 在執行個體類型區段中，從執行個體類型清單中，為執行個體選擇硬體組態。硬體組態必須符合特定的最低需求，才能支援閘道。建議您從 m5.xlarge 執行個體類型開始，它符合您閘道正常運作的最低硬體要求。如需詳細資訊，請參閱Amazon EC2執行個體類型的需求。

   必要時，您可以在啟動執行個體之後調整執行個體的大小。如需詳細資訊，請參閱 Amazon EC2 使用者指南 中的調整執行個體大小。

   > **Note**
   >
   > 某些執行個體類型，特別是 i3 EC2，會使用NVMeSSD磁碟。它們會在您啟動或停止磁帶閘道時產生問題；例如，您可能會遺失快取的資料。監控 `CachePercentDirty` Amazon CloudWatch 指標，並只在 參數為 時啟動或停止您的系統0。若要進一步了解監控閘道的指標，請參閱 CloudWatch 文件中的 Storage Gateway 指標和維度。
5. 在金鑰對 (登入) 區段中，針對金鑰對名稱(必要)，選取您要用來安全連線至執行個體的金鑰對。如有必要，您可以建立新的金鑰對。如需詳細資訊，請參閱《適用於 Linux 執行個體的 Amazon Elastic Compute Cloud 使用者指南》中的建立金輪對。
6. 在網路設定區段中，檢閱預先設定的設定值，然後選擇編輯以變更下列欄位：

   a. 對於 VPC- 必要 ，請選擇您要啟動 Amazon EC2執行個體VPC的 。如需詳細資訊，請參閱 Amazon Virtual Private Cloud 使用者指南 中的 Amazon VPC運作方式。 Amazon Virtual Private Cloud

   b. （選用） 針對子網路 ，選擇您要啟動 Amazon EC2執行個體的子網路。

   c. 在 Auto-assign Public IP (自動指派公有 IP) 中，選擇 Enable (啟用)。

7. 在防火牆 (安全群組) 子區段中，檢閱預先設定的設定值。您可以視需要變更要為 Amazon EC2執行個體建立之新安全群組的預設名稱和描述，或者選擇套用現有安全群組的防火牆規則。
8. 在傳入安全群組規則子區段中，新增防火牆規則，以開啟用戶端將用來連線至執行個體的連接埠。如需磁帶閘道所需連接埠的詳細資訊，請參閱連接埠需求。如需詳細資訊，請參閱《適用於 Linux 執行個體的 Amazon Elastic Compute Cloud 使用者指南》中的安全群組規則。

> **Note**
>
> 磁帶閘道要求TCP連接埠 80 開放用於傳入流量，以及在閘道啟用期間進行一次性HTTP存取。啟用後，您可以關閉此連接埠。
> 此外，您必須開啟TCP連接埠 3260 才能存取 iSCSI。

9. 在進階網路組態子區段中，檢閱預先設定的設定，並視需要進行變更。
10. 在新增儲存體頁面上，選擇新增新的磁碟區將儲存體新增到您的閘道執行個體。

> **Important**
>
> 除了預先設定的根EBS磁碟區 之外，您還必須至少新增一個具有至少 165 GiB 快取儲存容量的 Amazon EBS磁碟區，以及至少一個具有至少 150 GiB 上傳緩衝區容量的 Amazon 磁碟區。 為了提高效能，我們建議您為快取儲存配置多個EBS磁碟區，每個磁碟區至少要有 150 GiB。

11. 在進階詳細資訊區段中，檢閱預先設定的設定值，並視需要進行變更。
12. 選擇啟動執行個體，以使用已設定的設定啟動新的 Amazon EC2閘道執行個體。
13. 若要驗證新執行個體是否已成功啟動，請導覽至 Amazon EC2主控台中的執行個體頁面，並依名稱搜尋新執行個體。確定執行個體狀態顯示為執行中以及具有綠色核取記號，且狀態核取方塊已完成，並顯示綠色核取記號。
14. 從詳細資訊頁面選取執行個體。從執行個體摘要區段複製公有IPv4地址，然後返回 Storage Gateway 主控台中的設定閘道頁面，以繼續設定您的磁帶閘道

您可以使用 Storage Gateway Gateway 主控台或查詢參數存放區，來決定用來啟動磁帶閘道閘道的 AMI ID。 AWS Systems Manager

若要判斷 AMI ID，請執行下列其中一項操作：

- 使用 Storage Gateway 主控台開始設定新閘道。如需指示，請參閱設定磁帶閘道。當您到達平台選項區段時，請選擇 Amazon EC2 作為主機平台 ，然後選擇啟動執行個體以在 Amazon EC2主控台中開啟 AWS Storage Gateway AMI範本。

  系統會將您重新導向至EC2社群AMI頁面，您可以在其中查看 中 AWS 區域的 AMI IDURL。

- 查詢 Systems Manager 參數存放區。您可以使用 AWS CLI 或 Storage Gateway API 來查詢命名空間 下的 Systems Manager 公有參數`/aws/service/storagegateway/ami/VTL/latest`。例如，使用下列CLI命令會傳回 AWS 區域 您指定之 AMI中目前 的 ID。

  ```
  aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/VTL/
  latest
  ```

  CLI 命令會傳回類似下列的輸出。

  ```
  {
      "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 執行個體中繼資料

執行個體中繼資料服務 (IMDS) 是執行個體上元件，可提供對 Amazon EC2 執行個體中繼資料的安全存取。執行個體可設定為接受使用IMDS版本 1 (IMDSv1) 的傳入中繼資料要求，或要求所有中繼資料要求都使用IMDS版本 2 (IMDSv2)。IMDSv2使用工作階段導向要求，並緩解可用來嘗試存取. IMDS 如需相關資訊IMDSv2，請參閱 Amazon 彈性運算雲端使用者指南中的執行個體中繼資料服務第 2 版的運作方式。

建議您對託管 Storage Gateway 的所有 Amazon EC2 執行個體都需要IMDSv2。IMDSv2依預設，所有新啟動的閘道執行個體都是必需的。如果您的現有執行個體仍設定為接受中IMDSv1繼資料請求，請參閱 Amazon Elastic Compute Cloud 使用者指南IMDSv2中的「需要使用」，以取得修改執行個體中繼資料選項以要求使用的指示IMDSv2。套用此變更不需要重新啟動執行個體。

將 VM 時間與 Hyper-V 或 Linux KVM 主機時間同步

對於部署在 VMware 上的閘道ESXi，設定 Hypervisor 主機時間並將虛擬機器時間同步到主機就足以避免時間偏離。如需詳細資訊，請參閱將 VM 時間與VMware主機時間同步。對於部署在 Microsoft Hyper-V 或 Linux 上的閘道KVM，我們建議您使用下列程序定期檢查虛擬機器時間。

檢視 Hypervisor 閘道虛擬機器的時間並將其同步至網路時間通訊協定 （NTP） 伺服器

1. 登入您閘道的本機主控台：
   - 如需登入 Microsoft Hyper-V 本機主控台的詳細資訊，請參閱使用 Microsoft Hyper-V 存取閘道本機主控台。
   - 如需登入 Linux 核心型虛擬機器本機主控台 （KVM） 的詳細資訊，請參閱 使用 Linux 存取閘道本機主控台 KVM。
2. 在 Storage Gateway Configuration 主選單畫面上，輸入對應的數字以選取 System Time Management 。
3. 在系統時間管理選單畫面上，輸入對應的數字，以選取檢視和同步系統時間 。

   閘道本機主控台會顯示目前的系統時間，並將其與NTP伺服器報告的時間進行比較，然後報告兩次之間的確切差異，以秒為單位。
4. 如果時間差異大於 60 秒，請輸入 **y**來同步系統時間與NTP時間。否則，輸入 **n**。

   時間同步可能需要一些時間。

將 VM 時間與VMware主機時間同步

若要成功啟用您的閘道，您必須確定 VM 時間與主機時間同步，而且主機時間設定正確。在本節中，您先同步 VM 上的時間與主機時間。然後檢查主機時間，並視需要設定主機時間，並設定主機將其時間自動同步到網路時間通訊協定 （NTP） 伺服器。

> **Important**
>
> 需要同步 VM 時間與主機時間，才能成功啟用閘道。

同步 VM 時間與主機時間

1. 設定 VM 時間。

a. 在 vSphere 用戶端中，在應用程式視窗左側面板中的閘道 VM 名稱上按一下滑鼠右鍵，以開啟 VM 的內容選單，然後選擇編輯設定 。

   Virtual Machine Properties (虛擬機器屬性) 對話方塊隨即開啟。

b. 選擇選項索引標籤，然後從選項清單中選擇VMware工具。

c. 在虛擬機器屬性對話方塊右側的進階區段中，檢查使用主機同步訪客時間選項，然後選擇確定。

   VM 會同步其時間與主機。

2. 設定主機時間。

請務必確定您的主機時鐘設定為正確時間。如果您尚未設定主機時鐘，請執行下列步驟，以設定主機時鐘並與NTP伺服器同步。

a. 在VMware vSphere 用戶端中，選取左側面板中的 vSphere 主機節點，然後選擇組態索引標籤。

b. 選取 Software (軟體) 面板中的 Time Configuration (時間組態)，然後選擇 Properties (屬性) 連結。

   Time Configuration (時間組態) 對話方塊隨即出現。

c. 在日期和時間 下，設定 vSphere 主機的日期和時間。

d. 設定主機將其時間自動同步到NTP伺服器。

   i. 在時間組態對話方塊中選擇選項，然後在 NTP Daemon （ ntpd ） 選項對話方塊中，選擇左側面板中的NTP設定。

   ii. 選擇新增以新增NTP伺服器。

   iii. 在新增NTP伺服器對話方塊中，輸入NTP伺服器的 IP 地址或完整網域名稱，然後選擇確定。

      您可以使用 `pool.ntp.org`作為網域名稱。

   iv. 在 NTP Daemon （ ntpd ） 選項對話方塊中，選擇左側面板中的一般。

   v. 在服務命令 下，選擇開始以啟動服務。

      請注意，如果您變更此NTP伺服器參考或稍後新增另一個伺服器參考，則需要重新啟動服務才能使用新的伺服器。

e. 選擇確定以關閉 NTP Daemon （ ntpd ） 選項對話方塊。

f. 選擇 OK (確定) 以關閉 Time Configuration (時間組態) 對話方塊。

在VMware主機上設定半虛擬化

下列程序說明如何設定 Storage Gateway 設備的VMware主機平台，以使用橫向網際網路小型電腦系統介面通訊協定（iSCSI）控制器。Paravirtual iSCSI 控制器是高效能儲存控制器，可能會導致更高的輸送量和更低CPU的使用率。這些控制器最適合高效能儲存環境。當您以這種方式設定 iSCSI 控制器時，Storage Gateway 虛擬機器會與主機作業系統搭配使用，以允許閘道主控台識別您新增至虛擬機器的虛擬磁碟。

> **Note**
>
> 您需要完成此步驟，以避免在閘道主控台中設定這些磁碟時發生問題。

若要設定您的VMware主機平台以使用半虛擬化控制器

1. 在VMware vSphere 用戶端中，用滑鼠右鍵按一下應用程式視窗左側導覽窗格中的閘道虛擬機器名稱，以開啟內容選單，然後選擇編輯設定 。
2. 在虛擬機器屬性對話方塊中，選擇硬體索引標籤。
3. 在硬體索引標籤上，選取SCSI控制器 0，然後選擇變更類型 。
4. 在變更SCSI控制器類型對話方塊中，選取 VMware Paravirtual SCSI控制器類型，然後選擇確定以儲存組態。

設定閘道的網路轉接器

根據預設，Storage Gateway 設定為使用 E1000 網路轉接器類型，但您可以重新設定閘道以使用 VMXNET3（10 GbE ）網路轉接器。您也可以設定 Storage Gateway，讓它可由多個 IP 地址存取。設定您的閘道使用多個網路轉接器以完成此作業。

主題

- 設定閘道以使用VMXNET3網路轉接器
- 將閘道設定為多個 NICs

設定閘道以使用VMXNET3網路轉接器

Storage Gateway 在 VMwareESXi和 Microsoft Hyper-V Hypervisor 主機中都支援 E1000 網路轉接器類型。不過，VMwareESXiHypervisor 僅支援 VMXNET3（10 GbE ）網路轉接器類型。如果您的閘道託管在 VMware ESXi Hypervisor 上，您可以重新設定閘道以使用 VMXNET3（10 GbE ）轉接器類型。如需這些轉接器的詳細資訊，請參閱 Broadcom （VMware）網站上的為您的虛擬機器選擇網路轉接器。

> **Important**
>
> 若要選取 VMXNET3，您的訪客作業系統類型必須是其他 Linux64。

以下是您設定閘道以使用VMXNET3轉接器的步驟：

1. 移除預設的 E1000 轉接器。
2. 新增VMXNET3轉接器。
3. 重新啟動您的閘道。
4. 設定網路轉接器。

如何執行後續每個步驟的詳細資訊。

若要移除預設 E1000 轉接器，並設定閘道以使用VMXNET3轉接器

1. 在 中VMware，開啟閘道的內容（按一下滑鼠右鍵）選單，然後選擇編輯設定 。
2. 在 Virtual Machine Properties (虛擬機器屬性) 視窗中，選擇 Hardware (硬體) 標籤。
3. 針對 Hardware (硬體)，請選擇 Network adapter (網路轉接器)。請注意，Adapter Type (轉接器類型) 區段目前的轉接器是 E1000。您將將此轉接器取代為VMXNET3轉接器。
4. 選擇 E1000 網路轉接器，然後選擇 Remove (移除)。在本例中，E1000 網路轉接器是 Network adapter 1 (網路轉接器 1)。

   > **Note**
   >
   > 雖然您可以同時在閘道中執行 E1000 和VMXNET3網路轉接器，但我們不建議這麼做，因為它可能會導致網路問題。

5. 選擇 Add (新增) 開啟 Add Hardware (新增硬體) 精靈。

6. 請選擇 Ethernet Adapter (乙太網路卡)，然後選擇 Next (下一步)。
7. 在網路類型精靈中，針對介面卡類型，選取 **VMXNET3**，然後選擇 下一步。
8. 在虛擬機器屬性精靈中，在轉接器類型區段中確認 Current Adapter 已設定為 VMXNET3，然後選擇確定 。
9. 在VMwareVSphere用戶端中，關閉閘道。
10. 在VMwareVSphere用戶端中，重新啟動閘道。

重新啟動您的閘道後，請重新設定剛剛新增的轉接器，以確保建立網際網路的網路連線。

設定網路轉接器

1. 在VSphere用戶端中，選擇主控台索引標籤以啟動本機主控台。使用預設的登入資料來登入閘道的本機主控台以處理此組態任務。如需如何使用預設憑證的相關資訊，請參閱使用預設憑證登入本機主控台。
2. 出現提示時，輸入對應的數字以選取網路組態。
3. 在提示中，輸入對應的數字以選取全部重設為 DHCP，然後在提示中輸入 **y**（是），將所有轉接器設定為使用動態主機組態通訊協定 （DHCP）。所有可用的轉接器都會設定為使用 DHCP。

   如果您的閘道已啟用，您必須先關閉它，再從 Storage Gateway 管理主控台重新啟動。閘道重新啟動之後，您必須測試網際網路的網路連線。如需如何測試網路連線的詳細資訊，請參閱測試網際網路的閘道連線。

將閘道設定為多個 NICs

如果您將閘道設定為使用多個網路轉接器 （NICs），則可以透過多個 IP 地址存取。建議您在下列其中一種狀況中執行此作業：

- 最大化輸送量 – 當網路轉接器遇到瓶頸時，建議您最大化閘道輸送量。
- 分隔應用程式：您可能需要區隔應用程式寫入閘道磁碟區的方式。例如，您可以選擇只讓關鍵儲存應用程式使用一種為您閘道定義的特定轉接器。
- 網路限制 – 您的應用程式環境可能會要求您將 iSCSI 目標和連接到它們的啟動器保留在與閘道與 通訊的網路不同的隔離網路中 AWS。

在典型的多轉接器使用案例中，會將一個轉接器設定為閘道通訊的路由 AWS （即預設閘道）。除了此轉接器之外，啟動者必須與包含其所連線之 iSCSI 目標的轉接器位於相同的子網路中。否則，可能

無法與預定目標通訊。如果在用於與 通訊的相同轉接器上設定目標 AWS，則該目標的 iSCSI 流量和 AWS 流量會流經相同的轉接器。

當您設定一個介面卡連線到 Storage Gateway 主控台，然後新增第二個介面卡時，Storage Gateway 會自動設定路由表使用第二個介面卡為慣用的路由。如需如何設定多個轉接器的指示，請參閱下列各節。

- 在VMwareESXi主機上設定多個網路轉接器
- 在 Microsoft Hyper-V 主機上設定多個網路轉接器

在VMwareESXi主機上設定多個網路轉接器

下列程序假設閘道 VM 已定義一個網路轉接器，並說明如何在 VMware 上新增轉接器ESXi。

若要設定閘道在VMwareESXi主機中使用其他網路轉接器

1. 關機閘道。
2. 在VMware vSphere 用戶端中，選取閘道 VM。

   此程序的 VM 可以保持開啟狀態。
3. 在用戶端中，開啟閘道 VM 的內容 (按右鍵) 選單，然後選擇 Edit Settings (編輯設定)。
4. 在 Virtual Machine Properties (虛擬機器屬性) 對話方塊的 Hardware (硬體) 標籤上，選擇 Add (新增) 新增裝置。
5. 遵循 Add Hardware (新增硬體) 精靈來新增網路轉接器。

   a. 在 Device Type (裝置類型) 窗格中，選擇 Ethernet Adapter (乙太網路轉接器) 新增轉接器，然後選擇 Next (下一步)。

   b. 在網路類型窗格中，確定已針對類型選取在開機時連線，然後選擇 下一步。

      建議您將VMXNET3網路轉接器與 Storage Gateway 搭配使用。如需可能會出現在轉接器清單中的轉接器類型的詳細資訊，請參閱 中的網路轉接器類型ESXi和 vCenter 伺服器文件 。

   c. 在 Ready to Complete (準備好完成) 窗格中，檢閱資訊，然後選擇 Finish (完成)。
6. 選擇 VM 的摘要 標籤，然後選擇 IP 地址方塊旁的檢視全部。虛擬機器 IP 地址視窗會顯示您可用來存取閘道的所有 IP 地址。確認針對閘道列出第二個 IP 地址。

> **Note**
>
> 可能需要一些時間，轉接器變更才會生效並重新整理 VM 摘要資訊。

7. 在 Storage Gateway 主控台中，開啟閘道。
8. 在 Storage Gateway 主控台的導覽窗格中，選擇閘道，然後選擇您已新增介面卡的閘道。確認在 Details (詳細資訊) 標籤中列出第二個 IP 地址。

如需 VMware、Hyper-V 和 KVM 主機常用的本機主控台任務相關資訊，請參閱 在 VM 本機主控台上執行任務

在 Microsoft Hyper-V 主機上設定多個網路轉接器

下列程序假設您的閘道 VM 已定義一個網路轉接器，而且您將會新增第二個轉接器。此程序顯示如何為 Microsoft Hyper-V 主機新增轉接器。

在 Microsoft Hyper-V 主機中設定您的閘道，以使用額外的網路轉接器

1. 在 Storage Gateway 主控台上，關閉閘道。
2. 在 Microsoft Hyper-V Manager 中，從虛擬機器面板選取閘道 VM。
3. 如果閘道 VM 尚未關閉，請在 VM 名稱上按一下滑鼠右鍵以開啟內容選單，然後選擇關閉 。
4. 在閘道 VM 名稱上按一下滑鼠右鍵以開啟內容選單，然後選擇設定 。
5. 在設定對話方塊中的硬體 下，選擇新增硬體 。
6. 在設定對話方塊右側的新增硬體面板中，選擇網路轉接器 ，然後選擇新增以新增裝置。
7. 設定網路轉接器，然後選擇 Apply (套用) 以套用設定。
8. 在設定對話方塊中的硬體 下，確認新的網路轉接器已新增至硬體清單，然後選擇確定 。
9. 使用 Storage Gateway 主控台開啟閘道。
10. 在 Storage Gateway 主控台的導覽面板中，選擇閘道 ，然後選擇您新增轉接器的閘道。確認第二個 IP 地址已列在詳細資訊索引標籤中。

如需 VMware、Hyper-V 和 KVM 主機常用的本機主控台任務相關資訊，請參閱 在 VM 本機主控台上執行任務

搭配 Storage Gateway 使用VMware vSphere 高可用性

Storage Gateway VMware 透過與高可用性（VMware HA）整合的一組應用程式層級運作狀態檢查，在 上提供VMware vSphere 高可用性。此方法可協助防範儲存工作負載出現硬體、Hypervisor 或網路故障。這也有助於防範軟體錯誤，例如連線逾時和檔案共用或磁碟區無法使用。

vSphere HA 的運作方式是將虛擬機器及其所在的主機集區到叢集中，以進行備援。叢集中的主機會受到監控，如果發生故障，故障主機上的虛擬機器會在替代主機上重新啟動。一般而言，此復原會快速進行，不會遺失資料。如需 vSphere HA 的詳細資訊，請參閱 VMware 文件中的 vSphere HA 運作方式。

> **Note**
>
> 重新啟動故障虛擬機器並在新主機上重新建立 iSCSI 連線所需的時間取決於許多因素，例如主機作業系統和資源負載、磁碟速度、網路連線和 SAN/ 儲存基礎設施。為了將容錯移轉停機時間降至最低，請實作最佳化閘道效能 中概述的建議。
>
> 若要將 Storage Gateway 與 VMware HA 搭配使用，建議您執行下列動作：
>
> - 在叢集中僅一個主機上部署包含 Storage Gateway VM 的可VMwareESX.ova下載套件。
> - 部署 .ova 套件時，請選取不在某個主機本機的資料存放區。相反地，使用叢集中所有主機都可以存取的資料存放區。如果您選取在主機本機的資料存放區，而且主機故障，則可能無法從叢集的其他主機存取資料來源，而且容錯移轉到另一個主機可能不會成功。
> - 若要防止啟動者在容錯移轉期間中斷與儲存磁碟區目標的連線，請遵循作業系統的建議 iSCSI 設定。在容錯移轉事件中，可能需要幾秒到幾分鐘的時間，才能在容錯移轉叢集的新主機中啟動閘道 VM。Windows 和 Linux 用戶端的建議 iSCSI 逾時大於容錯移轉發生的典型時間。如需自訂 Windows 用戶端逾時設定的詳細資訊，請參閱自訂 Windows iSCSI 設定。如需自訂 Linux 用戶端逾時設定的詳細資訊，請參閱自訂 Linux iSCSI 設定。
> - 使用叢集處理時，如果您將 .ova 套件部署至叢集，則請在系統提示您選取主機時選取主機。或者，您可以直接部署至叢集中的主機。

下列主題說明如何在 VMware HA 叢集中部署 Storage Gateway：

主題

- 設定您的 vSphere VMware HA 叢集
- 從 Storage Gateway 主控台下載 .ova 映像
- 部署閘道

- （選用）新增叢集VMs上其他 的覆寫選項
- 啟用閘道
- 測試您的VMware高可用性組態

設定您的 vSphere VMware HA 叢集

首先，如果您尚未建立VMware叢集，請建立一個叢集。如需有關如何建立VMware叢集的資訊，請參閱 VMware 文件中的建立 vSphere HA 叢集。

接下來，將VMware叢集設定為使用 Storage Gateway 。

若要設定VMware叢集

1. 在 的編輯叢集設定頁面上VMwarevSphere，確定已設定 VM 監控以進行 VM 和應用程式監控。若要這麼做，請為每個選項設定下列值：
   - 主機失敗回應：重新啟動 VMs
   - 主機隔離的回應：關閉並重新啟動 VMs
   - 具有 的資料存放區PDL：已停用
   - 具有 的資料存放區APD：已停用
   - VM 監控：VM 和應用程式監控
2. 調整下列的值以微調叢集敏感度：
   - 失敗間隔：在此間隔後，如果沒有收到 VM 訊號，則會重新啟動 VM。
   - 最短執行時間：在 VM 啟動以開始監控 VM 工具的訊號後，叢集會等待這段指定的時間。
   - 每個 VM 的最大重設：在最大重設時間範圍內，叢集會重新啟動 VM 的最大次數。
   - 最大重設時間範圍：計算每個 VM 重設的最大重設次數的時間範圍。

   如果您不確定要設定哪些值，請使用這些設定範例：
   - 失敗間隔：**30** 秒
   - 最短執行時間：**120** 秒
   - 每個 VM 的最大重設次數：**3**
   - 最大重設時間範圍：**1** 小時

如果您在叢集上執行其他 VMs ，建議您特別為 VM 設定這些值。在從 .ova 部署 VM 前，您無法這樣做。如需設定這些值的詳細資訊，請參閱（選用） 新增叢集VMs上其他 的覆寫選項。

從 Storage Gateway 主控台下載 .ova 映像

下載您的閘道的 .ova 映像

- 在 Storage Gateway 主控台的設定閘道頁面上，選取您的閘道類型和主機平台，然後使用主控台中提供的連結來下載 .ova，如設定磁帶閘道所述。

部署閘道

在您設定的叢集中，將 .ova 映像部署到其中一個叢集主機。

部署閘道 .ova 映像

1. 將 .ova 映像部署到叢集中的其中一個主機。
2. 確認您選擇用於根磁碟的資料存放區以及快取可供叢集中的所有主機使用。在 VMware或內部部署環境中部署 Storage Gateway .ova 檔案時，磁碟會描述為半虛擬化SCSI磁碟。「全虛擬化」是閘道 VM 與主機作業系統搭配運作的模式，讓主控台可以識別您新增至 VM 的虛擬磁碟。

   設定 VM 以使用全虛擬化控制器

   1. 在VMware vSphere 用戶端中，開啟閘道 VM 的內容（按一下滑鼠右鍵）選單，然後選擇編輯設定 。
   2. 在虛擬機器屬性對話方塊中，選擇硬體索引標籤，選擇SCSI控制器 0，然後選擇變更類型 。
   3. 在 Change SCSI Controller Type 對話方塊中，選取 VMware Paravirtual SCSI 控制器類型，然後選擇 OK 。

（選用） 新增叢集VMs上其他 的覆寫選項

如果您的叢集上執行其他 VMs ，您可能想要特別為每個 VM 設定叢集值。如需指示，請參閱VMware vSphere 線上文件中的自訂個別虛擬機器。

為叢集VMs上的其他 新增覆寫選項

1. 在 的摘要頁面上VMwarevSphere，選擇叢集以開啟叢集頁面，然後選擇設定 。
2. 選擇 組態 標籤，然後選擇 VM 覆寫。

3. 新增 VM 覆寫選項以變更每個值。

   在 vSphere HA - VM 監控 下為每個選項設定下列值：

   - VM 監控：啟用覆寫 - VM 和應用程式監控
   - VM 監控敏感度：啟用覆寫 - VM 和應用程式監控
   - VM 監控：自訂
   - 失敗間隔：**30**秒
   - 最短運作時間： **120** 秒
   - 每個 VM 的最大重設次數：**5**
   - 重設時間區間上限：**1**小時以內

啟用閘道

部署閘道的 .ova 後，請啟用您的閘道。做法說明會依各個閘道類型而有所不同。

啟用閘道

- 請遵循下列主題中概述的程式：

  a. 將您的磁帶閘道連接至 AWS

  b. 檢閱設定並啟動磁帶閘道

  c. 設定您的磁帶閘道

測試您的VMware高可用性組態

啟用閘道後，請測試您的組態。

測試您的 VMware HA 組態

1. 開啟位於首頁 的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/
2. 在導覽窗格中，選擇閘道 ，然後選擇您要測試 VMware HA 的閘道。
3. 針對動作 ，選擇驗證 VMware HA 。
4. 在出現的驗證VMware高可用性組態方塊中，選擇確定 。

> **Note**
>
> 測試您的 VMware HA 組態會重新啟動閘道 VM，並中斷與閘道的連線。測試可能需要幾分鐘的時間才會完成。

如果測試成功，Verified (已驗證) 狀態會顯示在主控台閘道的詳細資訊標籤中。

5. 選擇 退出。

您可以在 Amazon CloudWatch 日誌群組中找到 VMware HA 事件的相關資訊。如需詳細資訊，請參閱使用 CloudWatch 日誌群組取得磁帶閘道運作狀態日誌。

使用磁帶閘道儲存資源

本節中的主題描述如何管理與磁帶閘道相關聯的儲存資源，例如連接至閘道虛擬主機平台的實體磁碟、連接至閘道 Amazon EC2執行個體的 Amazon EBS磁碟區、媒體變更器等虛擬磁帶庫裝置，以及虛擬磁帶庫中的磁帶。

主題

- 從閘道移除磁碟 - 了解如果您需要從閘道的虛擬主機平台移除磁碟時該怎麼做，例如，如果您的磁碟失敗。
- 在 Amazon EC2閘道上管理 Amazon EBS磁碟區 - 了解您可以如何增加或減少配置作為 Amazon EC2執行個體上託管之閘道的上傳緩衝區或快取儲存體的 Amazon EBS磁碟區數量。
- 使用 VTL 裝置 - 了解如何管理您的虛擬磁帶程式庫裝置，包括如何選取磁帶閘道的媒體變更器、如何更新媒體變更器的裝置驅動程式，以及如何在 Microsoft System Center Data Protection Manager 中顯示磁帶的條碼。
- 管理虛擬磁帶程式庫中的磁帶 - 了解如何管理與磁帶閘道相關聯的磁帶和虛擬磁帶程式庫，包括如何手動封存磁帶和取消正在進行的磁帶封存。

從閘道移除磁碟

雖然不建議從閘道移除基礎磁碟，但建議您從閘道移除磁碟 (例如，您有一個故障的磁碟時)。

從託管於 的閘道移除磁碟 VMware ESXi

您可以使用下列程序，從託管在 VMware Hypervisor 上的閘道移除磁碟。

若要移除為上傳緩衝區配置的磁碟 （ VMware ESXi ）

1. 在 vSphere 用戶端中，開啟內容 （ 按一下滑鼠右鍵 ） 選單，選擇閘道 VM 的名稱，然後選擇編輯設定 。
2. 在 Virtual Machine Properties (虛擬機器屬性) 對話方塊的 Hardware (硬體) 標籤上，選取配置為上傳緩衝區空間的磁碟，然後選擇 Remove (移除)。

   請確認虛擬機器屬性對話方塊中的虛擬裝置節點值具有您先前記下的相同值。這樣做有助於確保您移除正確的磁碟。
3. 選擇 Removal Options (移除選項) 面板中的選項，然後選擇 OK (確定) 來完成移除磁碟程序。

從 Microsoft Hyper-V 上託管的閘道移除磁碟

您可以使用下列程序，從 Microsoft Hyper-V 虛擬化管理程序上託管的閘道移除磁碟。

移除針對上傳緩衝區所配置的基礎磁碟 (Microsoft Hyper-V)

1. 在 Microsoft Hyper-V Manager 中，開啟內容 (按右鍵) 選單，並選擇閘道 VM 名稱，然後選擇 Settings (設定)。
2. 在 Settings (設定) 對話方塊的 Hardware (硬體) 清單中，選取要移除的磁碟，然後選擇 Remove (移除)。

   您新增至閘道的磁碟會出現在硬體清單中的SCSI控制器項目下方。請確認 Controller (控制器) 和 Location (位置) 值具有您先前記下的相同值。這樣做有助於確保您移除正確的磁碟。

   Microsoft Hyper-V Manager 中顯示的第一個SCSI控制器是控制器 0。
3. 選擇 OK (確定) 以套用變更。

從 Linux 上託管的閘道移除磁碟 KVM

若要將磁碟與託管在 Linux 核心型虛擬機器 （ KVM ） Hypervisor 上的閘道分離，您可以使用類似下列的`virsh`命令。

```
$ virsh detach-disk domain_name /device/path
```

如需管理KVM磁碟的詳細資訊，請參閱 Linux 發行版本的文件。

在 Amazon EC2閘道上管理 Amazon EBS磁碟區

當您最初將閘道設定為以 Amazon EC2執行個體執行時，您會將 Amazon EBS磁碟區配置為用作上傳緩衝區和快取儲存體。隨著時間的推移，隨著您的應用程式需要變更，您可以配置額外的 Amazon EBS磁碟區以供此使用。您也可以透過移除先前配置的 Amazon EBS磁碟區來減少您配置的儲存體。如需 Amazon 的詳細資訊EBS，請參閱 Amazon 使用者指南 中的 Amazon Elastic Block Store（Amazon EBS）。 EC2

在閘道中新增更多儲存體之前，您應該先檢閱如何根據閘道的應用程式需求，決定上傳緩衝和快取儲存的大小。若要執行此作業，請參閱判斷要配置的上傳緩衝大小和判斷要配置的快取儲存體大小。

您可配置為上傳緩衝和快取儲存的儲存體配額有限制。您可以將任意數量的 Amazon EBS磁碟區連接至執行個體，但您只能將這些磁碟區設定為上傳緩衝區，並將儲存空間快取到這些儲存配額。如需詳細資訊，請參閱AWS Storage Gateway 配額。

若要新增 Amazon EBS磁碟區並針對閘道進行設定

1. 建立 Amazon EBS磁碟區。如需指示，請參閱 Amazon 使用者指南 中的建立或還原 Amazon EBS磁碟區。 EC2
2. 將 Amazon EBS磁碟區連接至您的 Amazon EC2執行個體。如需指示，請參閱 Amazon 使用者指南 中的將 Amazon EBS磁碟區連接至執行個體。 EC2
3. 將新增的 Amazon EBS磁碟區設定為上傳緩衝區或快取儲存體。如需說明，請參閱 管理 Storage Gateway 的本機磁碟。

有時候您可能發現您不需要為上傳緩衝所配置的儲存量。

若要移除 Amazon EBS磁碟區

> **Warning**
>
> 這些步驟僅適用於配置為上傳緩衝區空間的 Amazon EBS磁碟區，不適用於配置到快取的磁碟區。如果您從磁帶閘道移除配置為快取儲存體的 Amazon EBS磁碟區，閘道上的虛擬磁帶將具有 IRRECOVERABLE 狀態，而且您會面臨資料遺失的風險。如需 IRRECOVERABLE 狀態的詳細資訊，請參閱 了解 中的磁帶狀態資訊 VTL。

1. 依照關閉閘道 VM 一節中所述的方法關閉閘道。

2. 從 Amazon EC2執行個體分離 Amazon EBS磁碟區。如需指示，請參閱 Amazon 使用者指南 中的從執行個體分離 Amazon EBS磁碟區。 EC2
3. 刪除 Amazon EBS磁碟區。如需指示，請參閱 Amazon 使用者指南 中的刪除 Amazon EBS磁碟區。 EC2
4. 依照關閉閘道 VM 一節中所述的方法啟動閘道。

使用 VTL 裝置

您的磁帶閘道設定提供下列裝置，您可以在啟用閘道時選取這些SCSI裝置。

主題

- 在啟用閘道後選取媒體變更器
- 更新媒體變更器的裝置驅動程式
- 在 Microsoft System Center 中顯示磁帶的條碼 DPM

對於中型換片機， AWS Storage Gateway 可與下列項目搭配使用：

- AWS-Gateway-VTL – 此裝置隨閘道提供。
- STK-L700 – 此裝置模擬隨閘道提供。

  啟用磁帶閘道時，您可以從清單選取備份應用程式，而 Storage Gateway 會使用適當的媒體變更器。如果未列出您的備份應用程式，則請選擇 Other (其他)，然後選擇使用備份應用程式的媒體變更器。

  您選擇的媒體變更器類型取決於您計劃使用的備份應用程式。下表列出了已通過測試且發現與磁帶閘道相容的第三方備份應用程式。此表格包含建議用於每個備份應用程式的媒體變更器類型。

備份應用程式	媒體變更器類型
Arcserve Backup	`AWS-Gateway-VTL`
Bacula Enterprise V10.x	`AWS-Gateway-VTL` 或 `STK-L700`
Commvault V11	`STK-L700`
Dell EMC NetWorker 19.5	`AWS-Gateway-VTL`

備份應用程式	媒體變更器類型
IBM Spectrum Protect v8.1.10	`IBM-03584L32-0402`
Micro Focus （HPE） Data Protector 9 或 11.x	`AWS-Gateway-VTL`
Microsoft System Center 2012 R2 或 2016 Data Protection Manager	`STK-L700`
NovaStor DataCenter/Network 6.4 或 7.1	`STK-L700`
Quest NetVault Backup 12.4 或 13.x	`STK-L700`
Veeam Backup & Replication 11A	`AWS-Gateway-VTL`
Veritas Backup Exec 2014 或 15 或 16 或 20 或 22.x	`AWS-Gateway-VTL`
Veritas Backup Exec 2012 **Note** Veritas 已終止對 Backup Exec 2012 的支援。	`STK-L700`
Veritas 7.x 版或 8.x NetBackup 版	`AWS-Gateway-VTL`

Important

我們強烈建議您選擇為備份應用程式列出的媒體變更器。其他媒體變更器可能無法正常運作。啟用閘道之後，您可以選擇不同的媒體變更器類型。如需詳細資訊，請查閱在啟用閘道後選取媒體變更器。

針對磁帶硬碟，Storage Gateway 使用下列項目：

- IBM-ULT3580-TD5—此裝置模擬會隨閘道提供。

在啟用閘道後選取媒體變更器

啟用閘道之後，您可以選擇選取不同的媒體變更器類型。

在啟用閘道之後選取不同的媒體變更器類型

1. 停止備份軟體中正在執行的任何相關任務。
2. 在 Windows 伺服器上，開啟 iSCSI 啟動器屬性視窗。
3. 選擇 Targets (目標) 標籤，以顯示已搜索到的目標。
4. 在 Discovered targets (已搜索到的目標) 窗格上，選擇您要變更的媒體變更器，並選擇 Disconnect (中斷連線)，然後選擇 OK (確定)。
5. 在 Storage Gateway 主控台上，從導覽窗格選擇閘道，然後選擇您要變更其媒體變更器的閘道。
6. 選擇 VTL 裝置索引標籤，選擇您要變更的媒體變更器，然後選擇變更媒體變更器 。
7. 在出現的 Change Media Changer Type (變更媒體變更器類型) 對話方塊中，從下拉清單方塊選取您要的媒體變更器，然後選擇 Save (儲存)。

更新媒體變更器的裝置驅動程式

1. 開啟 Windows 伺服器上的裝置管理員，然後展開 Medium Changer devices (媒體變更器裝置) 樹狀目錄。
2. 開啟 Unknown Medium Changer (不明媒體變更器) 的內容 (按右鍵) 選單，然後選擇 Update Driver Software (更新驅動程式軟體) 以開啟 Update Driver Software-unknown Medium Changer (更新驅動程式軟體 - 不明媒體變更器) 視窗。
3. 在 How do you want to search for driver software? (您要如何搜尋驅動程式軟體？) 區段中，選擇 Browse my computer for driver software (瀏覽電腦上的驅動程式軟體)。
4. 選擇 Let me pick from a list of device drivers on my computer (讓我從電腦上的裝置驅動程式清單挑選)。

> **Note**
>
> 我們建議搭配 Veeam Backup & Replication 11A 和 Microsoft System Center Data Protection Manager 備份軟體使用 Sony TSL-A500C Autoloader 驅動程式。此新力驅動程序已透過這些類型的備份軟體進行了測試，且包括 Windows Server 2019 的測試。

5. 在選取您要為此硬體安裝的裝置驅動程式區段中，清除顯示相容的硬體核取方塊，在製造商清單中選擇 Sony，在模型清單中選擇 Sony - TSL-A500C Autoloader，然後選擇下一步。

6. 在出現的警告方塊中，選擇 Yes (是)。如果成功安裝驅動程式，則請關閉 Update drive software (更新驅動程式軟體) 視窗。

在 Microsoft System Center 中顯示磁帶的條碼 DPM

如果您使用 Sony TSL-A500C Autoloader 的媒體變更器驅動程式，Microsoft System Center Data Protection Manager 不會自動顯示在 Storage Gateway 中建立的虛擬磁帶的條碼。若要正確顯示磁帶的條碼，請將媒體變更器驅動程式變更為 Sun/StorageTek Library。

顯示條碼

1. 確保所有備份任務已完成，而且沒有任務等待中或進行中。
2. 退出磁帶並將其移至離線儲存 （S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive），然後結束DPM管理員主控台。如需有關如何在 中退出磁帶的資訊DPM，請參閱 使用 封存磁帶DPM。
3. 在 管理工具 中，選擇 服務 ，並在詳細資訊窗格中開啟DPM服務的內容 （按一下滑鼠右鍵） 選單，然後選擇 屬性 。
4. 在一般索引標籤上，確定啟動類型設定為自動，然後選擇停止以停止DPM服務。
5. 從 Microsoft 網站上的 Microsoft Update Catalog 取得 StorageTek 驅動程式。

   > **Note**
   >
   > 請記下不同大小的驅動程式。

   Size (大小) 18K，請選擇 x86 drivers (x86 驅動程式)。

   Size (大小) 19K，請選擇 x64 drivers (x64 驅動程式)。
6. 開啟 Windows 伺服器上的裝置管理員，然後展開 Medium Changer Devices (媒體變更器裝置) 樹狀目錄。
7. 開啟 Unknown Medium Changer (不明媒體變更器) 的內容 (按右鍵) 選單，然後選擇 Update Driver Software (更新驅動程式軟體) 以開啟 Update Driver Software-unknown Medium Changer (更新驅動程式軟體 - 不明媒體變更器) 視窗。
8. 瀏覽到新驅動程式的路徑位置並安裝。驅動程式顯示為 Sun/StorageTek Library 。磁帶機會保留為 IBM ULT3580 TD5SCSI序列裝置。
9. 重新啟動DPM伺服器。

10. 在 Storage Gateway 主控台建立新磁帶。
11. 開啟DPM管理員主控台，選擇管理 ，然後選擇重新掃描新的磁帶庫 。您應該會看到 Sun/StorageTek library 。
12. 選擇程式庫，然後選擇 Inventory (清單)。
13. 選擇新增磁帶，將新的磁帶新增至 DPM。新的磁帶現在應該會顯示條碼。

管理虛擬磁帶程式庫中的磁帶

Storage Gateway 為您啟用的每個磁帶閘道提供一個虛擬磁帶程式庫 （VTL）。一開始，磁帶館並未包含任何磁帶，但您只要需要就可以建立磁帶。您的應用程式可以讀取和寫入至磁帶閘道上可用的任何磁帶。磁帶的狀態必須AVAILABLE可讓您寫入磁帶。這些磁帶由 Amazon Simple Storage Service (Amazon S3) 提供支援，也就是說，當您寫入這些磁帶時，磁帶閘道會將資料存放在 Amazon S3 中。如需詳細資訊，請參閱了解 中的磁帶狀態資訊 VTL。

主題

- 存檔磁帶
- 取消磁帶存檔

磁帶館會顯示磁帶閘道中的磁帶。此磁帶館會顯示所使用磁帶的磁帶條碼、狀態、大小和數量，以及與磁帶建立關聯的閘道。

當您在磁帶館中有大量磁帶時，主控台支援依條碼、狀態或兩者來搜尋磁帶。當您依條碼搜尋時，可以依狀態和閘道篩選。

依條碼、狀態和閘道搜尋

1. 開啟位於首頁 的 Storage Gateway 主控台。 https://console.aws.amazon.com/storagegateway/
2. 在導覽窗格中，選擇 Tapes (磁帶)，然後在搜尋方塊中輸入值。此值可以是條碼、狀態或閘道。根據預設，Storage Gateway 會搜尋所有虛擬磁帶。不過，您也可以依狀態篩選搜尋。

   如果您篩選狀態，則符合條件的磁帶會出現在 Storage Gateway 主控台的磁帶館中。

   如果您篩選閘道，則與閘道建立關聯的磁帶會出現在 Storage Gateway 主控台的磁帶館中。

   > **Note**
   >
   > 根據預設，無論狀態為何，Storage Gateway 都會顯示所有磁帶。

存檔磁帶

您可以存檔磁帶閘道中的虛擬磁帶。當您存檔磁帶時，Storage Gateway 會將磁帶移至存檔。

若要存檔磁帶，您可以使用備份軟體。磁帶封存程序包含三個階段，視為磁帶狀態 IN TRANSIT TO VTS、 ARCHIVING和 ARCHIVED：

- 若要存檔磁帶，請使用備份應用程式所提供的命令。封存程序開始時，磁帶狀態會變更為 IN TRANSIT TOVTS，且備份應用程式無法再存取磁帶。在此階段中，您的磁帶閘道正在將資料上傳至 AWS。需要時，您可以取消進行中的存檔。如需取消存檔的詳細資訊，請參閱取消磁帶存檔。

  > **Note**
  >
  > 存檔磁帶的步驟取決於您的備份應用程式。如需詳細說明，請參閱備份應用程式的文件。

- 資料上傳 AWS 完成後，磁帶狀態會變更為 ARCHIVING，而 Storage Gateway 會開始將磁帶移至封存。您目前無法取消存檔程序。
- 磁帶移至封存後，其狀態會變更為 ，而且ARCHIVED您可以將磁帶擷取至任何閘道。如需磁帶擷取的詳細資訊，請參閱擷取已存檔的磁帶。

存檔磁帶所含的步驟取決於您的備份軟體。如需如何使用 Symantec NetBackup 軟體封存磁帶的說明，請參閱封存磁帶 。

取消磁帶存檔

在您開始存檔磁帶之後，可能會決定需要取回磁帶。例如，您可以取消存檔程序、因存檔程序所花時間太長而取回磁帶，或從磁帶讀取資料。所存檔的磁帶會經歷三個狀態，如下所示：

- IN TRANSIT TO VTS：您的磁帶閘道正在將資料上傳至 AWS。
- ARCHIVING：資料上傳已完成，磁帶閘道正在將磁帶移至封存。
- ARCHIVED：磁帶已移動且封存，可供擷取。

只有當磁帶的狀態為 IN TRANSIT TO 時，您才能取消封存VTS。根據上傳頻寬和上傳資料量這類因素，在 Storage Gateway 主控台中可能會看不到此狀態。若要取消磁帶封存，請使用 API 參考中的 CancelRetrieval 動作。

取得閘道的啟用金鑰

若要接收閘道的啟用金鑰，請向閘道虛擬機器 (VM) 發出網頁請求。虛擬機器會傳回包含啟用金鑰的重新導向，該重新導向會當做 `ActivateGateway` API 動作的其中一個參數傳遞，以指定閘道的組態。如需詳細資訊，請參閱 ActivateGatewayS torage Gateway API 參考中的。

> **Note**
>
> 如果未使用，閘道啟用金鑰會在 30 分鐘內過期。

您對閘道虛擬機器發出的要求包括啟用發生的 AWS 區域。重新導向在回應中傳回的 URL 會包含稱為 `activationkey` 的查詢字串參數。此查詢字串參數便是您的啟用金鑰。查詢字串的格式如下：`http://`*`gateway_ip_address`*`/?activationRegion=`*`activation_region`*。此查詢的輸出傳回啟用區域和金鑰。

此 URL 也包含 `vpcEndpoint` 使用 VPC 端點類型連線之閘道的 VPC 端點識別碼。

> **Note**
>
> Storage Gateway 硬體設備、虛擬機器映像範本和 Amazon EC2 Amazon 機器映像 (AMI) 已預先設定好接收和回應本頁所述的 Web 請求所需的 HTTP 服務。您不需要或建議您在閘道上安裝任何其他服務。

主題

- Linux (curl)
- Linux (bash/zsh)
- Microsoft 視窗 PowerShell
- 使用本機主控台

Linux (curl)

以下範例顯示如何使用 Linux (curl) 取得啟用金鑰。

> **Note**
>
> 將反白顯示的變數取代為閘道的實際值。可接受的值如下：

- *gateway_ip_address*：例如，閘道器的 IPV4 地址 172.31.29.201
- *####*-您要啟動的閘道類型，例如STORED、、CACHEDVTL、FILE_S3或。FILE_FSX_SMB
- *region_code*：您要啟用閘道的區域。請參閱《AWS 一般參考指南》中的區域端點。如果未指定此參數，或者提供的值拼寫錯誤或與有效區域不相符，則該命令將預設為該us-east-1區域。
- *vpc_endpoint*：例如，閘道的 VPC 端點名稱 vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com。

若要取得公用端點的啟用金鑰：

```
curl "http://gateway_ip_address/?activationRegion=region_code&no_redirect"
```

若要取得 VPC 端點的啟用金鑰：

```
curl "http://gateway_ip_address/?
activationRegion=region_code&vpcEndpoint=vpc_endpoint&no_redirect"
```

Linux (bash/zsh)

下列範例顯示如何使用 Linux (bash/zsh) 擷取 HTTP 回應、剖析 HTTP 標頭及取得啟用金鑰的方式。

```
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
```

```
}
```

Microsoft 視窗 PowerShell

下列範例說明如何使用 Microsoft 視窗擷 PowerShell 取 HTTP 回應、剖析 HTTP 標頭，以及取得啟用金鑰。

```
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]
    }
  }
}
```

使用本機主控台

以下範例顯示如何使用本機主控台產生並顯示啟用金鑰。

從本機主控台取得閘道的啟用金鑰

1. 登入您的本機主控台。如果您是從 Windows 電腦連線到您的 Amazon EC2 執行個體，請以 admin 身分登入。
2. 登入並查看 AWS 設備啟用 - 設定主功能表後，選取 0 以選擇取得啟用金鑰。
3. 為閘道系列選項選取 Storage Gateway。
4. 出現提示時，輸入您要啟用閘道的 AWS 區域。
5. 輸入 1 公用端點或 2 VPC 端點做為網路類型。
6. 輸入 1 標準或 2 美國聯邦資訊處理標準 (FIPS) 做為端點類型。

連接 iSCSI 啟動器

管理閘道時，您會使用公開為網際網路小型電腦系統介面 （iVTL） 目標的磁碟區或虛擬磁帶程式庫 （SCSI） 裝置。對於磁碟區閘道，iSCSI 目標為磁碟區。對於磁帶閘道，目標為 VTL 裝置。作為此工作的一部分，您可以執行這些任務，例如連線至這些目標、自訂 iSCSI 設定、從 Red Hat Linux 用戶端連線，以及設定 Challenge-Handshake 身分驗證通訊協定 （CHAP）。

主題

iSCSI 標準是網際網路通訊協定 （IP） 型儲存聯網標準，用於啟動和管理 IP 型儲存裝置與用戶端之間的連線。下列清單定義一些用來描述 iSCSI 連線和相關元件的術語。

iSCSI 啟動器

iSCSI 網路的用戶端元件。啟動者將請求傳送至 iSCSI 目標。啟動器可以在軟體或硬體中予以實作。Storage Gateway 僅支援軟體啟動器。

iSCSI 目標

iSCSI 網路的伺服器元件，可接收並回應來自啟動者的請求。您的每個磁碟區都會公開為 iSCSI 目標。僅將一個 iSCSI 啟動器連接到每個 iSCSI 目標。

Microsoft iSCSI 啟動器

Microsoft Windows 電腦上的軟體程式，可讓您將用戶端電腦 （即執行應用程式的電腦，其資料要寫入閘道） 連接至外部 i SCSI型陣列 （即閘道）。使用主機電腦的乙太網路轉接卡建立連線。Microsoft iSCSI 啟動器已透過 Windows 8.1、Windows 10、Windows Server 2012 R2、Windows Server 2016 和 Windows Server 2019 上的 Storage Gateway 進行驗證。啟動器內建於這些作業系統中。

Red Hat iSCSI 啟動器

`iscsi-initiator-utils` Resource Package Manager （RPM） 套件為您提供在 Red Hat Linux 軟體中實作的 iSCSI 啟動器。此套件包含 iSCSI 通訊協定的伺服器常駐程式。

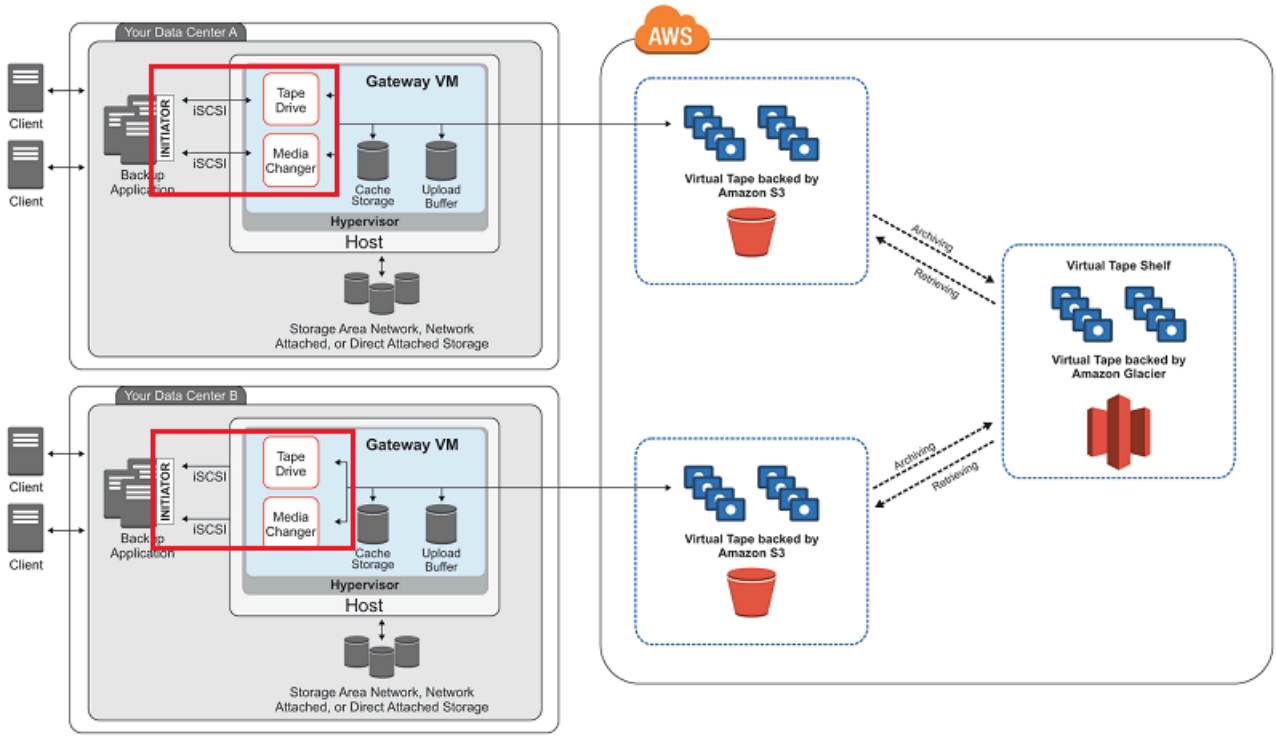
每種閘道類型都可以連線至 iSCSI 裝置，而且您可以自訂這些連線，如下所述。

將VTL裝置連線至 Windows 用戶端

磁帶閘道公開了數個磁帶機和媒體變更器，統稱為VTL裝置，稱為 iSCSI 目標。如需詳細資訊，請參閱設定磁帶閘道的需求。

> **Note**
>
> 您只能將一個應用程式連接到每個 iSCSI 目標。

下圖在 Storage Gateway 架構的較大圖中強調 iSCSI 目標。如需 Storage Gateway 架構的詳細資訊，請參與磁帶閘道的運作方式 (架構)。



將 Windows 用戶端連線至VTL裝置

1. 在 Windows 用戶端電腦的開始功能表上，**`iscsicpl.exe`**輸入搜尋程式和檔案方塊中的 ，找到 iSCSI 啟動器程式，然後執行。

   > **Note**
   >
   > 您必須在用戶端電腦上具有管理員權限，才能執行 iSCSI 啟動器。

2. 如果出現提示，請選擇是來啟動 Microsoft iSCSI 啟動器服務。
3. 在 iSCSI Initiator Properties 對話方塊中，選擇探索索引標籤，然後選擇探索入口網站 。
4. 在探索目標入口網站對話方塊中，輸入磁帶閘道的 IP 地址，以取得 IP 地址或DNS名稱 ，然後選擇確定 。若要取得閘道的 IP 地址，請檢查 Storage Gateway 主控台上的閘道標籤。如果您在 Amazon EC2執行個體上部署閘道，您可以在 Amazon EC2主控台的描述索引標籤中找到公有 IP 或DNS地址。

   > ⚠ Warning
   >
   > 對於部署在 Amazon EC2執行個體上的閘道，不支援透過公有網際網路連線存取閘道。Amazon EC2執行個體的彈性 IP 地址無法用作目標地址。

5. 選擇 Targets (目標) 標籤，然後選擇 Refresh (重新整理)。所有 10 個磁帶硬碟和媒體變更器都會出現在已搜索到的目標方塊中。目標的狀態為 Inactive (非使用中)。
6. 選取第一個裝置，然後選擇 Connect (連線)。您一次可以連線一個裝置。
7. 在 Connect to Target (連線至目標) 對話方塊中，選擇 OK (確定)。
8. 針對每個裝置重複步驟 6 和 7 來連接所有裝置，然後在 iSCSI Initiator Properties 對話方塊中選擇確定。

在 Windows 用戶端上，磁帶硬碟的驅動程式提供者必須是 Microsoft。使用下列程序來驗證驅動程式提供者，並在需要時更新驅動程式和提供者。

在 Windows 用戶端上驗證驅動程式提供者並 (在需要時) 更新的提供者和驅動程式

1. 在 Windows 用戶端上，啟動 [裝置管理員]。
2. 展開 Tape drives (磁帶硬碟)，並選擇磁帶硬碟的內容 (按右鍵) 選單，然後選擇 Properties (屬性)。
3. 在裝置屬性對話方塊的驅動程式標籤中，確認驅動程式提供者為 Microsoft。
4. 若驅動程式提供者並非 Microsoft，請將值設定如下：

   a. 選擇 Update Driver (更新驅動程式)。

   b. 在 Update Driver Software (更新驅動程式軟體) 對話方塊中，選擇 Browse my computer for driver software (瀏覽我的電腦以搜尋驅動程式軟體)。

   c. 在 Update Driver Software (更新驅動程式軟體) 對話方塊中，選擇 Let me pick from a list of device drivers on my computer (讓我從電腦上的裝置驅動程式清單中挑選)。

d. 選取LTO磁帶機，然後選擇下一個 。

e. 選擇關閉以關閉更新驅動程式軟體視窗，然後確認驅動程式提供者的值已設為 Microsoft。

5. 重複步驟 4.1 到 4.5，以更新所有磁帶硬碟。

將VTL裝置連接至 Linux 用戶端

使用 Red Hat Enterprise Linux （ RHEL ） 時，您可以使用 `iscsi-initiator-utils`RPM套件連線到閘道 iSCSI 目標 （ 磁碟區或VTL裝置 ）。

將 Linux 用戶端連線至 iSCSI 目標

1. 如果您的用戶端尚未安裝`iscsi-initiator-utils`RPM套件，請安裝套件。

   您可以使用下列命令來安裝套件。

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

2. 確保 iSCSI 常駐程式正在執行。

   a. 確認 iSCSI 常駐程式正在使用下列其中一個命令執行。

      對於 RHEL 5 或 6，請使用下列命令。

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

      對於 RHEL 7，請使用下列命令。

      ```
      sudo service iscsid status
      ```

   b. 如果狀態命令未傳回狀態正在執行，則請使用下列其中一個命令來啟動常駐程式。

      對於 RHEL 5 或 6，請使用下列命令。

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

      對於 RHEL 7，請使用下列命令。對於 RHEL 7，您通常不需要明確啟動`iscsid`服務。

      ```
      sudo service iscsid start
      ```

3. 若要探索為閘道定義的磁碟區或VTL裝置目標，請使用下列探索命令。

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

將閘道的 IP 地址替換為 *[GATEWAY_IP]* 上一個命令中的 變數。您可以在 Storage Gateway 主控台磁碟區的 iSCSI Target Info 屬性中找到閘道 IP。

搜索命令的輸出看起來會像下列範例輸出。

若為磁碟區閘道：*[GATEWAY_IP]*:3260, 1 iqn.1997-05.com.amazon:myvolume

若為磁帶閘道，請參閱：iqn.1997-05.com.amazon:*[GATEWAY_IP]*-tapedrive-01。

您的 iSCSI 合格名稱 （IQN） 會與上述顯示的名稱不同，因為IQN值對組織而言是唯一的。目標的名稱就是您在建立磁碟區時指定的名稱。當您在 Storage Gateway 主控台上選取磁碟區時，您也可以在 iSCSI Target Info 屬性窗格中找到此目標名稱。

4. 若要連線至目標，請使用下列命令。

請注意，您需要指定正確的 *[GATEWAY_IP]* 和 IQN 。

> **Warning**
>
> 對於部署在 Amazon EC2執行個體上的閘道，不支援透過公有網際網路連線存取閘道。Amazon EC2執行個體的彈性 IP 地址無法用作目標地址。

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

5. 若要確認磁碟區連接至用戶端機器 (啟動器)，請使用下列命令。

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

命令的輸出看起來會像下列範例輸出。

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

強烈建議您在設定啟動器之後，依照 中所述自訂您的 iSCSI 設定自訂 Linux iSCSI 設定。

自訂 iSCSI 設定

設定啟動器後，強烈建議您自訂 iSCSI 設定，以防止啟動器與目標中斷連線。

如下列步驟所示增加 iSCSI 逾時值，可讓您的應用程式更妥善地處理耗時很長的寫入操作和其他暫時性問題，例如網路中斷。

> **Note**
>
> 變更登錄之前，您應該先備份一份登錄。如需製作備份複本的資訊，以及使用登錄檔時應遵循的其他最佳實務，請參閱 Microsoft TechNet Library 中的登錄檔最佳實務。

主題

- 自訂 Windows iSCSI 設定
- 自訂 Linux iSCSI 設定

自訂 Windows iSCSI 設定

對於磁帶閘道設定，使用 Microsoft iSCSI 啟動器連線至VTL您的裝置是一個兩步驟程序：

1. 將您的磁帶閘道裝置連線到您的 Windows 用戶端。
2. 如果您使用的是備份應用程式，請設定應用程式以使用裝置。

入門範例設定提供的指示適用於這兩個步驟。它使用 Symantec NetBackup 備份應用程式。如需詳細資訊，請參閱 連接VTL您的裝置 和 設定 NetBackup 儲存裝置。

自訂 Windows iSCSI 設定

1. 提高請求佇列的時間上限。

   a. 啟動登錄編輯器 (`Regedit.exe`)。

   b. 導覽至包含 iSCSI 控制器設定之裝置類別的全域唯一識別碼 （GUID） 索引鍵，如下所示。

> **Warning**
>
> 請確定您在CurrentControlSet子金鑰中作業，而不是使用其他控制集，例如 ControlSet001 或 ControlSet002。

```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}
```

c. 尋找 Microsoft iSCSI 啟動器的子金鑰，如下所示 *[<Instance Number]*.

此機碼由四位數的號碼組成，例如 `0000`。

```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\[<Instance Number]
```

根據您電腦上安裝的內容，Microsoft iSCSI 啟動器可能不是子金鑰 `0000`。您可以透過驗證字串`DriverDesc`具有 值 來確保已選取正確的子金鑰`Microsoft iSCSI Initiator`。

d. 若要顯示 iSCSI 設定，請選擇參數子金鑰。

e. 開啟（32 位元）值的內容 MaxRequestHoldTimeDWORD（按滑鼠右鍵）選單，選擇修改，然後將該值變更為 **600**。

MaxRequestHoldTime 指定在通知`Device Removal`事件上層之前，Microsoft iSCSI 啟動器應保留並重試未完成命令的秒數。此值表示保留通話時間為 600 秒。

2. 您可以修改下列參數，以增加 iSCSI 封包傳送的資料量上限：

- FirstBurstLength 控制可在主動寫入請求中傳輸的資料量上限。將此值設為 **262144** 或 Windows 作業系統預設值，以較高者為準。
- MaxBurstLength 類似於 FirstBurstLength，但它會設定可在請求寫入序列中傳輸的資料量上限。將此值設為 **1048576** 或 Windows 作業系統預設值，以較高者為準。
- MaxRecvDataSegmentLength 控制與單一通訊協定資料單位（）相關聯的資料區段大小上限 PDU。將此值設為 **262144** 或 Windows 作業系統預設值，以較高者為準。

> **Note**
>
> 不同的備份軟體可以最佳化，以使用不同的 iSCSI 設定達到最佳效果。如要確認這些參數的哪些值能夠帶來最佳效能，請參閱備份軟體的文件。

3. 提高磁碟逾時值，如下所示：

   a. 如尚未啟動，請啟動登錄編輯器 (`Regedit.exe`)。

   b. 在 的服務子金鑰中導覽至磁碟子金鑰CurrentControlSet，如下所示。

   ```
   HKEY_Local_Machine\SYSTEM\CurrentControlSet\Services\Disk
   ```

   c. 開啟 （ 32 位元 ） 值的內容 TimeOutValueDWORD （ 按滑鼠右鍵 ） 選單，選擇修改 ，然後將該值變更為 **`600`**。

      TimeOutValue 指定啟動器在嘗試工作階段復原之前，捨棄並重新建立連線，等待目標回應的秒SCSI數。此值代表 600 秒的逾時期間。

4. 為確保新的組態值生效，請重新啟動您的系統。

   重新啟動之前，您必須確定磁碟區所有寫入操作的結果都已排清。若要執行此作業，請先將所有映射儲存磁碟區的磁碟離線，再重新啟動。

自訂 Linux iSCSI 設定

為您的閘道設定啟動器後，強烈建議您自訂 iSCSI 設定，以防止啟動器與目標中斷連線。透過增加如下所示的 iSCSI 逾時值，您可以讓您的應用程式更好地處理耗時很長的寫入操作和其他暫時性問題，例如網路中斷。

> **Note**
>
> 用於 Linux 其他類型的命令可能稍有不同。下列範例是以 Red Hat Linux 為基礎。

若要自訂 Linux iSCSI 設定

1. 提高請求佇列的時間上限。

   a. 開啓 `/etc/iscsi/iscsid.conf` 檔案並尋找下列各行。

```
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. 將 *[replacement_timeout_value]* 值為 **600**。

將 *[noop_out_interval_value]* 值為 **60**。

將 *[noop_out_timeout_value]* 值為 **600**。

這三種值全以秒為單位。

> **Note**
>
> 必須先設定 iscsid.conf 設定才能探索閘道。如已探索到您的閘道或登入目標，或兩項都完成，您可以使用下列命令從探索資料庫刪除項目。然後，您可以重新探索或再次登入以挑選新的組態。
>
> ```
> iscsiadm -m discoverydb -t sendtargets -p [GATEWAY_IP]:3260 -o delete
> ```

2. 增加每個回應可傳輸的資料量上限值。

a. 開啓 /etc/iscsi/iscsid.conf 檔案並尋找下列各行。

```
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. 建議您使用下列值，以提升效能。您的備份軟體可能需使用不同值來進行最佳化，因此請參閱備份軟體文件以取得最佳結果。

將 *[replacement_first_burst_length_value]* 或 **262144** Linux 作業系統預設值的值，以較高者為準。

將 *[replacement_max_burst_length_value]* 或 Linux 作業系統預設值**1048576**的值，以較高者為準。

將 *[replacement_segment_length_value]* 或 **262144** Linux 作業系統預設值的值，以較高者為準。

> **Note**
>
> 不同的備份軟體可以最佳化，以使用不同的 iSCSI 設定達到最佳效果。如要確認這些參數的哪些值能夠帶來最佳效能，請參閱備份軟體的文件。

3. 為確保新的組態值生效，請重新啟動您的系統。

   重新啟動之前，您必須確定磁帶所有寫入操作的結果都已排清。若要這麼做，請先卸載磁帶再重新啟動。

設定 iSCSI 目標的CHAP身分驗證

Storage Gateway 使用 Challenge-Handshake 身分驗證通訊協定 （ ） 支援閘道與 iSCSI 啟動器之間的身分驗證CHAP。CHAP 會定期驗證 iSCSI 啟動器身分，以存取磁碟區和VTL裝置目標。

> **Note**
>
> CHAP 組態是選用的，但強烈建議這麼做。

若要設定 CHAP，您必須在 Storage Gateway 主控台和用於連線至目標的 iSCSI 啟動器軟體中同時設定它。Storage Gateway 使用相互 CHAP，也就是啟動者驗證目標，而目標驗證啟動者。

CHAP 為您的目標設定相互

1. 在 Storage Gateway 主控台CHAP上設定 ，如 中所述在 Storage Gateway 主控台上CHAP設定 VTL裝置目標。
2. 在用戶端啟動器軟體中，完成CHAP組態：

   - 若要在 Windows 用戶端CHAP上設定相互，請參閱 在 Windows 用戶端CHAP上設定相互。
   - 若要在 Red Hat Linux 用戶端CHAP上設定相互，請參閱 在 Red Hat Linux 用戶端CHAP上設定相互。

在 Storage Gateway 主控台上CHAP設定VTL裝置目標

在此程序中，您指定兩個用於讀取和寫入虛擬磁帶的秘密金鑰。在此程序中，會使用這些相同的金鑰來設定用戶端啟動器。

1. 在導覽窗格中，選擇 Gateways (網際網路閘道)。
2. 選擇您的閘道，然後選擇VTL裝置索引標籤以顯示您的所有VTL裝置。
3. 選擇您要CHAP設定的裝置。
4. 在設定CHAP身分驗證對話方塊中提供請求的資訊。

   a. 在啟動器名稱 中，輸入 iSCSI 啟動器的名稱。此名稱是 Amazon iSCSI 合格名稱 （IQN），前面加上`iqn.1997-05.com.amazon:`目標名稱。以下是範例。

      `iqn.1997-05.com.amazon:`*`your-tape-device-name`*

      您可以使用您的 iSCSI 啟動器軟體來尋找啟動器名稱。例如，對於 Windows 用戶端，名稱是 iSCSI 啟動器的組態索引標籤上的值。如需詳細資訊，請參閱在 Windows 用戶端CHAP上設定相互。

      > **Note**
      >
      > 若要變更啟動器名稱，您必須先停用 CHAP，變更 iSCSI 啟動器軟體中的啟動器名稱，然後使用CHAP新名稱啟用。

   b. 針對啟動器驗證所用的秘密，輸入所請求的秘密。

      此秘密的長度必須最少為 12 個字元，最多為 16 個字元。此值是啟動者 （即 Windows 用戶端） 必須知道的秘密金鑰，才能CHAP參與目標。

   c. 對於用於驗證目標的秘密 （相互 CHAP），輸入請求的秘密。

      此秘密的長度必須最少為 12 個字元，最多為 16 個字元。此值是目標必須知道的秘密金鑰，才能CHAP與發起者一起參與。

      > **Note**
      >
      > 用來驗證目標的秘密必須與驗證啟動器的秘密不同。

   d. 選擇 Save (儲存)。

5. 在VTL裝置索引標籤上，確認 iSCSI CHAP身分驗證欄位設定為 true 。

在 Windows 用戶端CHAP上設定相互

在此程序中，您可以使用您在主控台CHAP上為磁碟區設定的相同金鑰，CHAP在 Microsoft iSCSI 啟動器中設定 。

1. 如果尚未啟動 iSCSI 啟動器，請在 Windows 用戶端電腦的開始功能表上，選擇執行 ，輸入 **`iscsicpl.exe`**，然後選擇確定執行程式。
2. 為啟動器 （即 Windows 用戶端 ） 設定相互CHAP組態：

   a. 選擇 Configuration (組態) 索引標籤。

   > **Note**
   >
   > Initiator Name (啟動器名稱) 值對於啟動器和公司必須是唯一的。前面顯示的名稱是您在 Storage Gateway 主控台的設定CHAP身分驗證對話方塊中使用的值。
   > 範例影像中所顯示的名稱僅供示範之用。

   b. 選擇 CHAP。

   c. 在 iSCSI Initiator Mutual Chap Secret 對話方塊中，輸入相互CHAP秘密值。

      在此對話方塊中，您輸入啟動器 (Windows 用戶端) 用來驗證目標 (儲存磁碟區) 的秘密。此秘密可讓目標讀取和寫入啟動器。此秘密與在設定CHAP驗證對話方塊中用於驗證目標 （ 相互 CHAP ） 的秘密中輸入的秘密相同。如需詳細資訊，請參閱設定 iSCSI 目標的CHAP身分驗證。

   d. 如果您輸入的金鑰少於 12 個字元或超過 16 個字元，則會出現啟動者CHAP秘密錯誤對話方塊。

      選擇確定，然後重新輸入金鑰。

3. 使用啟動者的秘密來設定目標，以完成相互CHAP組態。

   a. 選擇 Targets (目標) 標籤。

   b. 如果您要為 設定的目標CHAP目前已連線，請選擇目標，然後選擇中斷連線 以中斷連線。

   c. 選取您要為 設定的目標CHAP，然後選擇連線 。

   d. 在 Connect to Target (連線至目標) 對話方塊中，選擇 Advanced (進階)。

   e. 在進階設定對話方塊中，設定 CHAP。

i. 選取在 上啟用CHAP登入。

ii. 輸入驗證啟動器所需的秘密。此秘密與在設定CHAP身分驗證對話方塊中用於驗證啟動器的秘密中輸入的秘密相同。如需詳細資訊，請參閱設定 iSCSI 目標的CHAP身分驗證。

iii. 選取 Perform mutual authentication (執行交互身分驗證)。

iv. 若要套用變更，請選擇 OK (確定)。

f. 在 Connect to Target (連線至目標) 對話方塊中，選擇 OK (確定)。

4. 如果您已提供正確的秘密金鑰，則目標會顯示 Connected (已連線) 狀態。

在 Red Hat Linux 用戶端CHAP上設定相互

在此程序中，您可以使用您在 Storage Gateway 主控台CHAP上為磁碟區設定的相同金鑰CHAP，在 Linux iSCSI 啟動器中設定 。

1. 確保 iSCSI 常駐程式正在執行，且您已連線到目標。如果您尚未完成這兩項工作，請參閱連線到 Linux 用戶端。

2. 中斷連線並移除您即將設定 之目標的任何現有組態CHAP。

a. 若要尋找目標名稱，並確保它是已定義的組態，請使用下列命令列出儲存的組態。

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

b. 與目標中斷連線。

下列命令會與 **myvolume** Amazon iSCSI 合格名稱 （ ） 中定義的名為 的目標中斷連線IQN。變更目標名稱，並IQN依您的情況所需變更目標名稱和 。

```
sudo /sbin/iscsiadm --mode node --logout GATEWAY_IP:3260,1
 iqn.1997-05.com.amazon:myvolume
```

c. 移除目標的組態。

下列命令會移除 **myvolume** 目標的組態。

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

3. 編輯 iSCSI 組態檔案以啟用 CHAP。

a. 取得啟動器的名稱 (即您正在使用的用戶端)。

下列命令會從 /etc/iscsi/initiatorname.iscsi 檔案取得啟動器名稱。

```
sudo cat /etc/iscsi/initiatorname.iscsi
```

此命令的輸出如下所示：

```
InitiatorName=iqn.1994-05.com.redhat:8e89b27b5b8
```

b. 開啟 /etc/iscsi/iscsid.conf 檔案。

c. 取消註解檔案中的下列資料行，並指定正確的值 *username*, *password*, *username_in* 和 *password_in*.

```
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
```

如需所要指定值的指導，請參閱下表。

組態設定	Value
username	您在此程序的前一個步驟中找到的啟動器名稱。此值的開頭為 iqn。例如，**iqn.1994-05.com.redhat:8e89b27b5b8** 是有效的 *username* 值。
password	啟動器 (您正在使用的用戶端) 與磁碟區通訊時，用來驗證啟動器的秘密金鑰。
username_in	IQN 目標磁碟區的 。此值的開頭為 iqn，且結尾為目標名稱。例如，**iqn.1997-05.com.amazon:myvolume** 是有效的 *username_in* 值。
password_in	目標 (磁碟區) 與啟動器通訊時，用來驗證目標的秘密金鑰。

d. 儲存組態檔案中的變更，然後關閉檔案。

4. 搜索和登入目標。若要這麼做，請依照連線至 Linux 用戶端中的步驟進行。

AWS Direct Connect 搭配 Storage Gateway 使用

AWS Direct Connect 將您的內部網路連結至 Amazon Web Services 雲端。透過 AWS Direct Connect 與 Storage Gateway 搭配使用，您可以建立連線以滿足高輸送量工作負載需求，在內部部署閘道和 AWS.

Storage Gateway 使用公用端點。建立 AWS Direct Connect 連線後，您可以建立公用虛擬介面，以允許將流量路由到 Storage Gateway 端點。公有虛擬界面會略過您網路路徑中的網際網路服務提供者。Storage Gateway 服務公用端點可以位於與 AWS Direct Connect 位置相同的 AWS 區域，也可以位於不同的 AWS 區域中。

下圖顯示如何與 Storage Gateway AWS Direct Connect 搭配使用的範例。
網絡架構顯示使用 AWS 直接連接連接到雲端的 Storage Gateway。

下列程序假設您已建立正常運作的閘道。

AWS Direct Connect 搭配 Storage Gateway 使用

1. 在內部部署資料中心和 Storage Gateway 端點之間建立並建立 AWS Direct Connect 連線。如需關於如何建立連線的詳細資訊，請參閱《AWS Direct Connect 使用者指南》中的AWS Direct Connect入門指南。
2. 將內部部署 Storage Gateway 設備 Connect 至 AWS Direct Connect 路由器。
3. 建立公有虛擬界面，然後以同樣方式設定您的內部部署路由器。即使使用直 Connect，VPC端點也必須使用HAProxy. 如需詳細資訊，請參閱《AWS Direct Connect 使用者指南》中的建立虛擬介面。

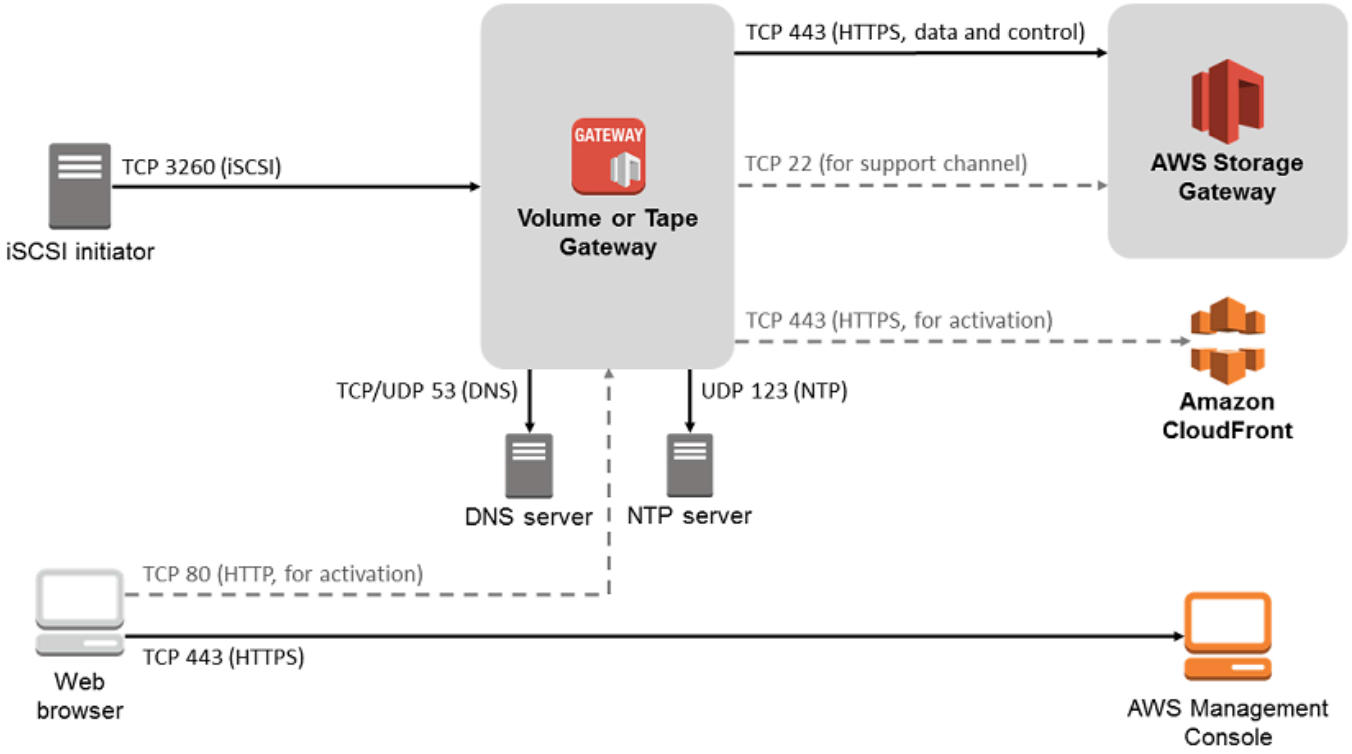
如需詳細資訊 AWS Direct Connect，請參閱「什麼是 AWS Direct Connect？」 在《AWS Direct Connect 使用者指南》中。

Tape Gateway 的連接埠需求

Storage Gateway 需要下列連接埠才能進行操作。有些連接埠是所有閘道類型常見的，也是所有閘道類型均需使用的。有些則是特定閘道類型需要的連接埠。在本節中，您可以找到磁帶閘道所需連接埠的圖例和清單。

磁帶閘道

下圖顯示要為磁帶閘道閘道操作開啟的所有連接埠。



以下連接埠是所有閘道類型常見的，也是所有閘道類型均需使用的。

從	到	通訊協定	連線埠	使用方式	
Storage Gateway VM	AWS	傳輸控制通訊協定（TCP）	443（HTTPS）	用於從 Storage Gateway 傳出 VM 到 AWS 服務端點的通訊。如需服務端點的資訊，請參閱[允許透過防火牆和路由器 AWS Storage	

從	到	通訊協定	連線埠	使用方式	
				Gateway 存取。	
您的 Web 瀏覽器	Storage Gateway VM	TCP	80 （HTTP）	由本機系統取得 Storage Gateway 啟用金鑰。只有在啟用 Storage Gateway 裝置時，才會使用連接埠 80。 Storage Gateway VM 不需要讓連接埠 80 可公開存取。連接埠 80 所需的存取權限級別取決於您的網路設定。若您是以 Storage Gateway 管理主控台啟動您的閘道，則您連線至主控台的主機必須擁有閘道連接埠 80 的存取權限。	

從	到	通訊協定	連線埠	使用方式	
Storage Gateway VM	網域名稱服務（DNS）伺服器	使用者資料包通訊協定（UDP）/ UDP	53（DNS）	用於 Storage Gateway VM 與DNS伺服器之間的通訊。	
Storage Gateway VM	AWS	TCP	22 (支援通道)	允許 AWS Support 存取您的閘道，以協助您疑難排解閘道問題。不需要將此埠開放給閘道的正常操作使用，但進行疑難排解時需要用到。	

從	到	通訊協定	連線埠	使用方式	
Storage Gateway VM	網路時間通訊協定（NTP）伺服器	UDP	123（NTP）	本機系統用來將 VM 的時間與主機時間同步。Storage Gateway VM 設定為使用下列NTP伺服器： • 0.amazon.pool.ntp.org • 1.amazon.pool.ntp.org • 2.amazon.pool.ntp.org • 3.amazon.pool.ntp.org	
Storage Gateway 硬體設備	超文字傳輸通訊協定（HTTP）代理	TCP	8080（HTTP）	短暫需要啟用。	

除了常用的連接埠之外，磁帶閘道還需下要下列連接埠。

從	到	通訊協定	連線埠	使用方式	
iSCSI 啟動器	Storage Gateway VM	TCP	3260（iSCSI）	由本機系統連線到閘道公開	

從	到	通訊協定	連線埠	使用方式	
				的 iSCSI 目標。	

取得閘道設備的 IP 地址

在您選擇主機以及部署閘道 VM 之後，即可連線和啟用閘道。若要執行此作業，您需要閘道 VM 的 IP 地址。您可以從閘道的本機主控台取得 IP 地址。您登入本機主控台，並從主控台頁面頂端取得 IP 地址。

針對在內部部署所部署的閘道，您也可以從虛擬化管理程序取得 IP 地址。對於 Amazon EC2閘道，您也可以從 Amazon EC2管理主控台取得 Amazon EC2執行個體的 IP 地址。若要了解如何取得閘道的 IP 地址，請參閱下列其中一項：

- VMware 主機： 使用 存取閘道本機主控台 VMware ESXi
- HyperV 主機：使用 Microsoft Hyper-V 存取閘道本機主控台
- Linux 核心型虛擬機器 （KVM） 主機： 使用 Linux 存取閘道本機主控台 KVM
- EC2 主機： 從 Amazon EC2 主機取得 IP 地址

當您找到 IP 地址時，請記下它。然後，傳回 Storage Gateway 主控台，並在主控台中輸入 IP 地址。

從 Amazon EC2 主機取得 IP 地址

若要取得閘道部署的 Amazon EC2執行個體 IP 地址，請登入EC2執行個體的本機主控台。然後，從主控台頁面頂端取得 IP 地址。如需說明，請參閱 登入您的 Amazon EC2 Gateway Local Console。

您也可以從 Amazon EC2 Management Console 取得 IP 地址。建議您使用公有 IP 地址予以啟用。若要取得公有 IP 地址，請使用程序 1。如果您選擇改為使用彈性 IP 地址，請參閱程序 2。

程序 1：使用公有 IP 地址連線至閘道

1. 在 開啟 Amazon EC2主控台https://console.aws.amazon.com/ec2/。
2. 在導覽窗格中，選擇執行個體 ，然後選擇閘道部署所在的EC2執行個體。
3. 選擇底部的 Description (描述) 標籤，然後記下公有 IP。您可以使用此 IP 地址連線至閘道。傳回 Storage Gateway 主控台，並輸入 IP 地址。

如果您要使用彈性 IP 地址予以啟用，請使用下列程序。

程序 2：使用彈性 IP 地址連線至閘道

1. 在 開啟 Amazon EC2主控台https://console.aws.amazon.com/ec2/。
2. 在導覽窗格中，選擇執行個體 ，然後選擇閘道部署所在的EC2執行個體。
3. 選擇底部的 Description (描述) 標籤，然後記下 Elastic IP (彈性 IP) 值。您可以使用此彈性 IP 地址連線至閘道。傳回 Storage Gateway 主控台，並輸入彈性 IP 地址。
4. 閘道啟用後，請選擇您剛啟用的閘道，然後選擇底部面板中的VTL裝置索引標籤。
5. 取得所有VTL裝置的名稱。
6. 針對每個目標，執行下列命令來設定目標。

   ```
   iscsiadm -m node -o new -T [$TARGET_NAME] -p [$Elastic_IP]:3260
   ```
7. 針對每個目標，執行下列命令來登入。

   ```
   iscsiadm -m node -p [$ELASTIC_IP]:3260 --login
   ```

   您的閘道現在已使用EC2執行個體的彈性 IP 地址連線。

了解 Storage Gateway 資源與資源 IDs

在 Storage Gateway 中，主要資源是閘道，但其他資源類型包括：磁碟區、虛擬磁帶、i SCSI 目標和 vtl 裝置。它們稱為子資源，必須與閘道相關聯才能存在。

這些資源和子資源具有唯一的 Amazon 資源名稱 (ARNs) 與它們相關聯，如下表所示。

資源類型	ARN格式
閘道器 ARN	arn:aws:storagegateway: *region*:*account-id* :gateway/ *gateway-id*
膠帶 ARN	arn:aws:storagegateway: *region*:*account-id* :tape/*tapebarcode*
目標ARN (i SCSI 目標)	arn:aws:storagegateway: *region*:*account-id* :gateway/ *gateway-id* /target/*iSCSItarget*
VTL裝置 ARN	arn:aws:storagegateway: *region*:*account-id* :gateway/ *gateway-id* /device/*vtldevice*

Storage Gateway 也支援使用EC2執行個體、EBS磁碟區和快照。這些資源是 Storage Gateway 中使用的 Amazon EC2 資源。

使用資源 IDs

當您建立資源時，Storage Gateway 會將唯一資源 ID 指派給資源。此資源 ID 是資源的一部分ARN。資源 ID 的形式為資源識別符 (其後伴隨連字號) 以及唯一的八個字母與數字組合。例如，閘道 ID 的形式為 `sgw-12A3456B`，其中 `sgw` 是閘道的資源識別符。磁碟區 ID 的形式為 `vol-3344CCDD`，其中 `vol` 是磁碟區的資源識別符。

針對虛擬磁帶，您最多可以在條碼 ID 前面加上四個字元的字首，以協助組織磁帶。

Storage Gateway IDs 資源為大寫。但是，當您將這些資源IDs與 Amazon 一起使用時 EC2API，Amazon EC2 希望資源IDs為小寫。您必須將資源 ID 變更為小寫，才能與 EC2API. 例如，在 Storage Gateway 中，磁碟區的 ID 可能是 `vol-1122AABB`。當您搭配使用此 ID 時 EC2API，必須將其變更為`vol-1122aabb`。否則，EC2API可能無法如預期般運作。

為 Storage Gateway 資源加上標籤

在 Storage Gateway 中，您可以使用標籤來管理您的資源。標籤可讓您將中繼資料新增到您的資源並對您的資源進行分類，使資源更易於管理。每個標籤都是由您定義的金鑰/值對所構成。您可以將標籤新增到閘道、磁碟區和虛擬磁帶。您可以根據您新增的標籤搜尋及篩選這些資源。

例如，您可以使用標籤來識別您組織中各部門所使用的 Storage Gateway 資源。您可以為會計部門所使用的閘道和磁碟區新增標籤如下：(`key=department` 和 `value=accounting`)。您接著可以使用此標籤進行篩選，識別您的會計部門所使用的所有閘道和磁碟區，然後運用此資訊來判斷成本。如需詳細資訊，請參閱使用成本配置標籤和使用標籤編輯器。

若您存檔已加上標籤的虛擬磁帶，磁帶會在存檔中維持其標籤。同樣地，若您從存檔將磁帶擷取至另一個閘道，標籤也會保留在新的閘道中。

標籤不具有任何語意意義，而是會解譯成字元字串。

以下限制適用於標籤：

- 標籤金鑰與值皆區分大小寫。
- 每個資源的標籤數上限為 50。
- 標籤金鑰的開頭不可為 `aws:`。此字首已保留供 AWS 使用。

- 索引鍵屬性的有效字元為 UTF -8 個字母和數字、空格和特殊字元 +-=。_:/和 @。

處理標籤

您可以使用 Storage Gateway 主控台、儲存裝置閘道或 Storage Gate API way 命令列介面 (CLI) 來處理標籤。以下程序顯示在主控台上新增、編輯及刪除標籤的方式。

新增標籤

1. 在https://console.aws.amazon.com/storagegateway/首頁開啟 Storage Gateway 主控台。
2. 在導覽窗格中，選擇您希望新增標籤的資源。

   例如，若要為閘道新增標籤，請選擇 閘道，然後從閘道清單中選擇您希望新增標籤的閘道。
3. 選擇 Tags (標籤)，然後選擇 Add/edit tags (新增/編輯標籤)。
4. 在 Add/edit tags (新增/編輯標籤) 對話方塊中，選擇 Create tag (建立標籤)。
5. 針對 金鑰 輸入金鑰，並針對 值 輸入值。例如，您可以針對金鑰輸入 **`Department`**，並針對值輸入 **`Accounting`**。

   > **Note**
   >
   > 您可以將 Value (值) 方塊保留空白。

6. 選擇 建立標籤 以新增更多標籤。您可以為單一資源新增多個標籤。
7. 完成新增標籤後，請選擇 儲存。

編輯標籤

1. 在https://console.aws.amazon.com/storagegateway/首頁開啟 Storage Gateway 主控台。
2. 選擇您要編輯標籤的資源。
3. 選擇 Tags (標籤) 以開啟 Add/edit tags (新增/編輯標籤) 對話方塊。
4. 選擇您希望編輯之標籤旁的鉛筆圖示，然後編輯標籤。
5. 完成編輯標籤後，選擇儲存。

若要刪除標籤

1. 在https://console.aws.amazon.com/storagegateway/首頁開啟 Storage Gateway 主控台。

2. 選擇您要刪除標籤的資源。
3. 選擇 Tags (標籤)，然後選擇 Add/edit tags (新增/編輯標籤) 以開啟 Add/edit tags (新增/編輯標籤) 對話方塊。
4. 選擇您要刪除之標籤旁的 X 圖示，然後選擇 儲存。

使用 Storage Gateway 的開放原始碼元件

本節說明我們為提供 Storage Gateway 功能所仰賴的第三方工具和授權。

下列位置提供 AWS Storage Gateway 軟體所隨附之特定開放原始碼軟體元件的來源碼，以供下載：

- 對於部署在 VMware 上的閘道ESXi，請下載 sources.tar
- 對於部署在 Microsoft Hyper-V 上的閘道，請下載 sources_hyperv.tar
- 對於部署在 Linux 核心型虛擬機器 （KVM） 上的閘道，請下載 sources_KVM.tar

此產品包含 OpenSSL Project 開發的軟體，可用於 OpenSSL Toolkit （http://www.openssl.org/：//）。如需所有相依第三方工具的相關授權，請參閱第三方授權。

AWS Storage Gateway 配額

在本主題中，您可以找到 Storage Gateway 磁碟區與磁碟配額、組態和效能配額的相關資訊。

主題

- 磁帶的配額
- 適用於您閘道的建議本機磁碟大小

磁帶的配額

下表列出磁帶的配額。

描述	磁帶閘道
虛擬磁帶的大小下限	100 GiB
虛擬磁帶的大小上限	15 TiB

描述	磁帶閘道
指派給閘道的虛擬磁帶數目上限	1,500
指派給閘道的所有磁帶總大小	1 PiB
存檔中虛擬磁帶的總數目	沒有限制
存檔中所有磁帶的總大小	沒有限制

適用於您閘道的建議本機磁碟大小

下表針對您所部署的閘道建議本機磁碟儲存體大小。

閘道類型	快取 (最小值)	快取 (最大值)	上傳緩衝區 (最小值)	上傳緩衝區 (最大值)	其他必要的本機磁碟
磁帶閘道	150 GiB	64 TiB	150 GiB	2 TiB	—

> **Note**
>
> 您可以為快取和上傳緩衝區設定一個或多個本機磁碟機，上限為最大容量。
> 新增快取或將緩衝區上傳到現有閘道時，請務必在主機 (Hypervisor 或 Amazon EC2 執行個體) 中建立新磁碟。如果先前已將磁碟配置為快取或上傳緩衝區，請勿變更現有磁碟的大小。

APIStorage Gateway 的參考資料

除了使用主控台之外，您還可以使用 AWS Storage Gateway API以程式設計方式設定和管理閘道。本節說明作 AWS Storage Gateway 業、驗證要求簽署以及錯誤處理。如需 Storage Gateway 可用區域和端點的詳細資訊，請參閱 AWS 一般參考 中的 AWS Storage Gateway 端點與配額。

> **Note**
>
> 您也可以在使用開發應用程式 AWS SDKs時使用 AWS Storage Gateway。對 AWS SDKs於爪哇，. NET，並PHP包裝底層 AWS Storage Gateway API，簡化您的編程任務。如需下載程式SDK庫的詳細資訊，請參閱範例程式碼程式庫。

主題

Storage Gateway 的必要請求標頭

本節說明您必須隨著每個要POST求傳送至 Storage Gateway 的必要標頭。您可以加入HTTP標頭來識別要求的相關主要資訊，包括您要呼叫的作業、要求的日期，以及指出您作為要求傳送者授權的資訊。標頭不區分大小寫，並且標頭的順序也不重要。

下列範例顯示ActivateGateway作業中使用的標頭。

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120425/us-east-2/
storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target,
 Signature=9cd5a3584d1d67d57e61f120f35102d6b3649066abdd4bf4bbcf05bd9f2f8fe2
```

```
x-amz-date: 20120912T120000Z
x-amz-target: StorageGateway_20120630.ActivateGateway
```

以下是您對 Storage Gateway 的POST要求中必須包含的標頭。下面顯示以「x-amz」開頭的標題是AWS特定的標題。列出的所有其他標題都是HTTP交易中使用的通用標頭。

標頭	描述
`Authorization`	授權標頭包含幾段請求的資訊，讓 Storage Gateway 能判斷該請求對申請者而言是否為有效動作。此標頭的格式如下 (為求可讀性已新增分行)： `Authorization: AWS4-HMAC_SHA456 Credentials= YourAccessKey /yyymmdd/region/storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature= CalculatedSignature` 在上述語法中，您可以指定YourAccessKey年、月和日 (yyyymmdd)、區域和. CalculatedSignature 授權標頭的格式由 AWS V4 簽名過程的要求決定。簽章的詳細資訊會在簽署請求主題中討論。
`Content-Type`	使用 `application/x-amz-json-1.1` 做為所有傳送至 Storage Gateway 請求的內容類型。 `Content-Type: application/x-amz-json-1.1`
`Host`	使用主機標頭來指定您要傳送請求的 Storage Gateway 端點。舉例來說，`storagegateway.us-east-2.amazonaws.com` 代表美國東部 (俄亥俄) 區域的端點。如需 Storage Gateway 可用端點的詳細資訊，請參閱 AWS 一般參考 中的 AWS Storage Gateway 端點與配額。 `Host: storagegateway. region.amazonaws.com`
`x-amz-date`	您必須在HTTPDate標頭或標頭中提供時間戳記。 AWS `x-amz-date` （某些HTTP客戶端庫不允許您設置Date標題。）當 `x-amz-dat`

標頭	描述
	e 標頭存在時，Storage Gateway 會在請求身分驗證時略過任何 Date 標頭。格x-amz-date 式必須是 ISO86 01 基本的 YYYYMMDD 'THHMMSS' Z '格式。如果同時使用Date和x-amz-date 標頭，則 Date 標頭的格式不一定是 ISO86 01。 `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
x-amz-target	此標頭會指定您要求API之作業的版本和作業。目標標頭值是透過將API版本與API名稱連接而形成，且格式如下。 `x-amz-target: StorageGateway_ APIversion .operationName` 您可以從API清單中找到operationName值 (例如 ActivateGateway「」) APIStorage Gateway 的參考資料。

簽署請求

Storage Gateway 會要求您簽署請求，對您發送的每個請求進行身分驗證。若要簽署請求，請使用加密雜湊函數來計算數位簽章。加密雜湊是一個函數, 其根據輸入傳回一個唯一的雜湊值。此雜湊函數的輸入包含請求和私密存取金鑰的文字。雜湊函數會傳回一個雜湊值，您將此值包含在請求中做為簽章。該簽章是請求 Authorization 標頭中的一部分。

收到請求後，Storage Gateway 會使用您原先用以簽署請求的相同雜湊函數與輸入，重新計算簽章。如果產生的簽章符合請求中的簽章，Storage Gateway 將處理請求。否則，請求會遭到拒絕。

Storage Gateway 支援使用 AWS Signature 第 4 版進行身分驗證。計算簽章的程序可以分成三個任務：

- 任務 1：建立正式請求

  將您的HTTP請求重新排列為標準格式。使用標準表單是必要的，因為 Storage Gateway 在重新計算簽章以與所傳送的簽章進行比較時，會使用相同的標準表單。
- 任務 2：建立登入字串

建立一個字串，您會使用此字串做為密碼編譯雜湊函數的其中一個輸入值。此字串，稱為登入字串，是雜湊演算法的名稱、請求日期、登入資料範圍字串和前一個任務的正式請求的串連。登入資料範圍字串本身是日期、區域和服務資訊的串連。

- 任務 3：建立簽章

  使用接受兩個輸入字串的密碼編譯雜湊函數來建立請求的簽章：您的 登入字串和衍生金鑰。衍生金鑰的計算方式是從您的秘密存取金鑰開始，並使用認證範圍字串建立一系列雜湊型訊息驗證碼 (HMACs)。

簽章計算範例

下列範例會逐步引導您建立簽名的詳細資訊ListGateways。此範例可用作檢查簽名簽章計算方法的參考。Amazon Web Services 詞彙表的 Signature Version 4 Test Suite 包含其他參考計算。

該範例假設如下：

- 申請的時間戳記為「二零一二年九月十日（星期一）00:00:00」GMT。
- 端點是美國東部 (俄亥俄) 區域。

一般的請求語法（包括JSON主體）是：

```
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
{}
```

針對 任務 1：建立正式請求 所計算之請求的正式格式為：

```
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
```

正式請求的最後一行是請求內文的雜湊值。另外，請注意正式請求中的空的第三行。這是因為沒有這個 API（或任何 Storage GatewayAPIs）的查詢參數。

的「登入字串」任務 2：建立登入字串為：

```
AWS4-HMAC-SHA256
20120910T000000Z
20120910/us-east-2/storagegateway/aws4_request
92c0effa6f9224ac752ca179a04cecbede3038b0959666a8160ab452c9e51b3e
```

「登入字串」的第一行是演算法、第二行是時間戳記、第三行是「登入資料範圍」，而最後一行是來自任務 1 的正式請求雜湊。

針對任務 3：建立簽章，「衍生金鑰」可以呈現為：

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey,"20120910"),"us-
east-2"),"storagegateway"),"aws4_request")
```

如果使用私密存取金鑰 wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY，則計算簽章是：

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

最後步驟是建立 Authorization 標頭。對於演示訪問密鑰AKIAIOSFODNN7EXAMPLE，標題（為了可讀性而添加了換行符）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
```

錯誤回應

主題

- 例外狀況
- 操作錯誤代碼
- 錯誤回應

本節提供有關 AWS Storage Gateway 錯誤的參考資訊。這些錯誤會以錯誤異常及操作錯誤代碼表示。例如，如果要求簽章有問題，則會由任何API回應傳回錯誤例外InvalidSignatureException狀況。不過，只會傳回ActivationKeyInvalid的作業錯誤碼ActivateGatewayAPI。

根據錯誤的類型，Storage Gateway 可能只會傳回異常，或是同時傳回異常及操作錯誤代碼。錯誤回應的範例會在錯誤回應中顯示。

例外狀況

下表列出 AWS Storage Gateway API例外狀況。當 AWS Storage Gateway 作業傳回錯誤回應時，回應主體會包含下列其中一個例外狀況。InternalServerError 和 InvalidGatewayRequestException 會傳回 操作錯誤代碼 訊息代碼中的其中一項操作錯誤代碼，提供特定操作錯誤代碼。

異常情形	訊息	HTTP狀態碼
IncompleteSignatureException	指定的簽章不完整。	400 錯誤的請求
InternalFailure	由於不明的錯誤、異常或故障，處理請求失敗。	500 內部伺服器錯誤
InternalServerError	操作錯誤代碼 的其中一項操作錯誤代碼訊息。	500 內部伺服器錯誤
InvalidAction	請求的動作或操作無效。	400 錯誤的請求
InvalidClientTokenId	提供的 X.509 憑證或存 AWS 取金鑰識別碼不存在於我們的記錄中。	403 Forbidden (403 禁止)
InvalidGatewayRequestException	操作錯誤代碼 中的其中一項操作錯誤代碼訊息。	400 錯誤的請求

異常情形	訊息	HTTP狀態碼
InvalidSignatureException	我們計算的請求簽章不符合您提供的簽章。檢查您的 AWS 訪問密鑰和簽名方法。	400 錯誤的請求
MissingAction	請求中遺失動作或操作參數。	400 錯誤的請求
MissingAuthenticationToken	要求必須包含有效 (已註冊) AWS 存取金鑰識別碼或 X.509 憑證。	403 Forbidden (403 禁止)
RequestExpired	請求已超過過期日期或請求日期 (兩者皆具有 15 分鐘的填補)，或是請求日期的發生時間超過未來的 15 分鐘。	400 錯誤的請求
SerializationException	序列化時發生錯誤。檢查您的JSON有效載荷是否格式良好。	400 錯誤的請求
ServiceUnavailable	由於伺服器暫時故障，請求失敗。	503 Service Unavailable (503 服務無法使用)
SubscriptionRequiredException	AWS 存取金鑰 ID 需要服務的訂閱。	400 錯誤的請求
ThrottlingException	超過費率。	400 錯誤的請求
TooManyRequests	請求過多。	429 要求太多
UnknownOperationException	指定的操作不明。有效操作會在 Storage Gateway 中的操作 中列出。	400 錯誤的請求
UnrecognizedClientException	包含在請求中的安全性權杖無效。	400 錯誤的請求
ValidationException	輸入參數的值不符或超出範圍。	400 錯誤的請求

操作錯誤代碼

下表顯示了 AWS Storage Gateway 操作錯誤代碼和APIs可以返回代碼之間的映射。所有的操作錯誤代碼都會使用InternalServerError中所說明之兩種一般異常 (InvalidGatewayRequestException 和 例外狀況) 中的其中一種傳回。

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
ActivationKeyExpired	指定的啟用金鑰已過期。	ActivateGateway
ActivationKeyInvalid	指定的啟用金鑰無效。	ActivateGateway
ActivationKeyNotFound	找不到指定的啟用金鑰。	ActivateGateway
BandwidthThrottleScheduleNotFound	找不到指定的頻寬調節。	DeleteBandwidthRateLimit
CannotExportSnapshot	無法匯出指定的快照。	CreateCachediSCSIVolume CreateStorediSCSIVolume
InitiatorNotFound	找不到指定的啟動器。	DeleteChapCredentials
DiskAlreadyAllocated	指定的磁碟已配置。	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
DiskDoesNotExist	指定的磁碟不存在。	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
DiskSizeNotGigAligned	指定的磁碟未調整為 GB。	CreateStorediSCSIVolume
DiskSizeGreaterThanVolumeMaxSize	指定的磁碟大小大於磁碟區大小上限。	CreateStorediSCSIVolume
DiskSizeLessThanVolumeSize	指定的磁碟大小小於磁碟區大小。	CreateStorediSCSIVolume
DuplicateCertificateInfo	指定的憑證資訊重複。	ActivateGateway

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
GatewayInternalError	發生閘道內部錯誤。	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
GatewayNotConnected	指定的閘道並未連線。	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
GatewayNotFound	找不到指定的閘道。	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
		ListLocalDisks ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
GatewayProxyNetworkConnectionBusy	指定的閘道代理網路連線忙碌中。	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
InternalError	發生內部錯誤。	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
InvalidParameters	指定的請求包含不正確的參數。	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
LocalStorageLimitExceeded	超過本機儲存限制。	AddCache AddUploadBuffer AddWorkingStorage
LunInvalid	指定的不LUN正確。	CreateStorediSCSIVolume
MaximumVolumeCountExceeded	超過磁碟區計數上限。	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
NetworkConfigurationChanged	閘道網路組態已變更。	CreateCachediSCSIVolume CreateStorediSCSIVolume

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
NotSupported	不支援指定的操作。	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
OutdatedGateway	指定的閘道已過期。	ActivateGateway
SnapshotInProgress Exception	指定的快照正在進行。	DeleteVolume
SnapshotIdInvalid	指定的快照無效。	CreateCachediSCSIVolume CreateStorediSCSIVolume
StagingAreaFull	預備區域已滿。	CreateCachediSCSIVolume CreateStorediSCSIVolume

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
TargetAlreadyExists	指定的目標已存在。	CreateCachediSCSIVolume CreateStorediSCSIVolume
TargetInvalid	指定的目標無效。	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials UpdateChapCredentials
TargetNotFound	找不到指定的目標。	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials DeleteVolume UpdateChapCredentials

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
UnsupportedOperationForGatewayType	指定的操作對於閘道類型無效。	AddCache AddWorkingStorage CreateCachediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteSnapshotSchedule DescribeCache DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
VolumeAlreadyExists	指定的磁碟區已存在。	CreateCachediSCSIVolume CreateStorediSCSIVolume
VolumeIdInvalid	指定的磁碟區無效。	DeleteVolume
VolumeInUse	指定的磁碟區已在使用。	DeleteVolume

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
VolumeNotFound	找不到指定的磁碟區。	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint DeleteVolume DescribeCachediSCSIVolumes DescribeSnapshotSchedule DescribeStorediSCSIVolumes UpdateSnapshotSchedule
VolumeNotReady	指定的磁碟區尚未準備就緒。	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

錯誤回應

當發生錯誤時，回應標頭資訊會包含：

- 內容類型：應用程式 /-1.1 x-amz-json
- 適當的4xx或5xxHTTP狀態碼

錯誤回應的內文會包含發生錯誤的資訊。以下範例錯誤回應會顯示所有錯誤回應常見的回應元素輸出語法。

```
{
    "__type": "String",
    "message": "String",
    "error":
        { "errorCode": "String",
          "errorDetails": "String"
        }
```

```
}
```

下表說明上述語法中顯示的JSON錯誤回應欄位。

__type

其中一個來自例外狀況的異常。

類型：字串

error

包含API特定錯誤詳細資訊。在一般錯誤（即不特定於任何錯誤API）中，不會顯示此錯誤信息。

類型：集合

errorCode

其中一項操作錯誤代碼 。

類型：字串

errorDetails

此欄位不用於目前版本的API。

類型：字串

message

的其中一項操作錯誤代碼訊息。

類型：字串

錯誤回應範例

如果您使用 DescribeStorediSCSIVolumesAPI並指定不存在的閘道ARN要求輸入，則會傳回下列JSON主體。

```
{
  "__type": "InvalidGatewayRequestException",
  "message": "The specified volume was not found.",
  "error": {
    "errorCode": "VolumeNotFound"
  }
```

```
}
```

如果 Storage Gateway 計算的簽章與要求傳送的簽章不符，則會傳回下列JSON主體。

```
{
  "__type": "InvalidSignatureException",
  "message": "The request signature we calculated does not match the signature you
 provided."
}
```

Storage Gateway 中的操作

如需 Storage Gateway 作業的清單，請參閱AWS Storage Gateway API參考資料中的動作。

磁帶閘道使用者指南的文件歷史記錄

- API 版本：2013-06-30
- 文件最新更新時間：2020 年 11 月 24 日

下表會說明 2018 年 4 月後《AWS Storage Gateway 使用者指南》每個版本的重要變更。如需本文件更新通知，您可以訂閱RSS摘要。

變更	描述	日期
FSx File Gateway 的可用性變更通知	AWS Storage Gateway的 FSx File Gateway 在 10/28/24 之後將不再提供給新客戶。若要使用 服務，您必須在該日期之前註冊。FSx File Gateway 的現有客戶可以繼續正常使用 服務。如需類似 FSx File Gateway 的功能，請造訪此部落格文章 。	2024 年 9 月 26 日
新增開啟或關閉維護更新的選項	Storage Gateway 會收到定期維護更新，其中包括作業系統和軟體升級、解決穩定性、效能和安全性的修正，以及新功能的存取。您現在可以設定 設定，為部署中的每個個別閘道開啟或關閉這些更新。如需詳細資訊，請參閱使用 AWS Storage Gateway 主控台管理閘道更新	2024 年 6 月 6 日
Snowball Edge 上磁帶閘道的已棄用支援	無法在 Snowball Edge 裝置上託管磁帶閘道。	2024 年 3 月 14 日
更新使用第三方應用程式測試閘道設定的指示	使用第三方應用程式測試閘道設定的說明現在會說明閘道在	2023 年 10 月 24 日

	進行中的備份工作期間重新啟動時的預期行為。如需詳細資訊，請參閱使用您的備份軟體來測試您的閘道設定。	
更新建議 CloudWatch 警示	此 CloudWatch `HealthNotifications` 警示現在適用於所有閘道類型和主機平台，並建議用於 和 。建議的組態設定也已針對 `HealthNotifications` 和 `AvailabilityNotifications` 更新。如需詳細資訊，請參閱了解 CloudWatch 警示	2023 年 10 月 2 日
將磁帶閘道的最大磁帶大小增加到 15 TiB	針對磁帶閘道，虛擬磁帶的大小上限現在已從 5 TiB 提高至 15 TiB。如需詳細資訊，請參閱《Storage Gateway 使用者指南》中的磁帶配額。	2022 年 10 月 4 日
獨立的磁帶與磁碟區閘道使用者指南	《Storage Gateway 使用者指南》先前包含磁帶和磁碟區閘道類型的相關資訊，已分為《磁帶閘道使用者指南》和《磁碟區閘道使用者指南》，每一種僅包含一種閘道類型的資訊。如需詳細資訊，請參閱磁帶閘道使用者指南和磁碟區閘道使用者指南。	2022 年 3 月 23 日
更新的閘道建立程序	已更新使用 Storage Gateway 主控台建立所有閘道類型的程序。如需詳細資訊，請參閱建立閘道。	2022 年 1 月 18 日

全新磁帶介面	AWS Storage Gateway 主控台中的磁帶概觀頁面已更新為新的搜尋和篩選功能。本指南中的所有相關程序已更新以說明新功能。如需詳細資訊，請參閱管理磁帶閘道。	2021 年 9 月 23 日
支援適用於磁帶閘道的 Quest NetVault Backup 13	Tape Gateways 現在支援在 Microsoft Windows Server 2012 R2 或 Microsoft Windows Server 2016 上執行的 Quest NetVault Backup 13。如需詳細資訊，請參閱使用 Quest NetVault Backup 測試您的設定。	2021 年 8 月 22 日
從磁帶和磁碟區閘道指南移除的 S3 檔案閘道主題	為了讓客戶設定各自的閘道類型時，更容易遵循磁帶閘道和磁碟區閘道的使用者指南，部分不必要的主題已移除。	2021 年 7 月 21 日
支援 Windows 和 Linux for Tape Gateway 上的 IBM Spectrum Protect 8.1.10	Tape Gateways 現在支援在 Microsoft Windows Server 和 Linux 上執行的 IBM Spectrum Protect 8.1.10 版。如需詳細資訊，請參閱使用 IBM Spectrum Protect 測試您的設定。	2020 年 11 月 24 日
聯RAMP準會合規	Storage Gateway 現在符合 FedRAMP 標準。如需詳細資訊，請參閱 Storage Gateway 的合規驗證 。	2020 年 11 月 24 日

以排程為基礎的頻寬限流	Storage Gateway 現在支援磁帶和磁碟區閘道的排程式頻寬限流。如需詳細資訊，請參閱使用 Storage Gateway 主控台排程頻寬限流使用 Storage Gateway 主控台。	2020 年 11 月 9 日
快取磁碟區和磁帶閘道本機快取儲存體增至 4 倍	Storage Gateway 現在針對快取磁碟區和磁帶閘道支援高達 64 TB 的本機快取，藉由提供低延遲存取較大的工作資料集，提升內部部署應用程式的效能。如需詳細資訊，請參閱建議的閘道本機磁碟大小。	2020 年 11 月 9 日
閘道移轉	Storage Gateway 現在支援將快取的磁碟區閘道移轉至新的虛擬機器。如需詳細資訊，請參閱將快取磁碟區移至新的快取磁碟區閘道虛擬機器。	2020 年 9 月 10 日
支援磁帶保留鎖定和 write-once-read-many （WORM） 磁帶保護	Storage Gateway 支援虛擬磁帶上的磁帶保留鎖定，並在讀取多個（ ）後寫入。WORM 磁帶保留鎖定可讓您指定封存虛擬磁帶上的保留模式和期間，防止它們遭到刪除，最長可達 100 年的固定時間。其中包括誰可以刪除磁帶或修改保留設定的權限控制。如需詳細資訊，請參閱使用磁帶保留鎖定。WORM啟用的虛擬磁帶有助於確保虛擬磁帶程式庫中作用中磁帶上的資料不會被覆寫或刪除。如需詳細資訊，請參閱寫入一次、讀取許多（WORM）磁帶保護。	2020 年 8 月 19 日

透過主控台訂購硬體設備	您現在可以透過 AWS Storage Gateway 主控台訂購硬體設備。如需詳細資訊，請參閱使用 Storage Gateway 硬體設備。	2020 年 8 月 12 日
支援新 AWS 區域中的聯邦資訊處理標準（FIPS）端點	您現在可以使用美國東部（俄亥俄）、美國東部（維吉尼亞北部）、美國西部（加利福尼亞北部）、美國西部（奧勒岡）和加拿大（中部）區域中的FIPS端點啟用閘道。如需詳細資訊，請參閱 AWS 一般參考 中的 AWS Storage Gateway 端點和配額。	2020 年 7 月 31 日
閘道移轉	Storage Gateway 現在支援將磁帶和儲存磁碟區閘道移轉至新的虛擬機器。如需詳細資訊，請參閱將資料移至新閘道。	2020 年 7 月 31 日
在 Storage Gateway 主控台中檢視 Amazon CloudWatch 警示	您現在可以在 Storage Gateway 主控台中檢視 CloudWatch 警示。如需詳細資訊，請參閱了解 CloudWatch 警示	2020 年 5 月 29 日
支援聯邦資訊處理標準（FIPS）端點	您現在可以使用區域中的FIPS端點 AWS GovCloud (US) 啟用閘道。若要選擇磁碟區閘道的FIPS端點，請參閱選擇服務端點 。若要選擇磁帶閘道的FIPS端點，請參閱將您的磁帶閘道連線至 AWS。	2020 年 5 月 22 日

新 AWS 區域	Storage Gateway 現已在非洲 (開普敦) 和歐洲 (米蘭) 區域提供。如需詳細資訊，請參閱 AWS 一般參考 中的 AWS Storage Gateway 端點和配額。	2020 年 5 月 7 日
S3 Intelligent-Tiering 儲存體方案的支援	Storage Gateway 現支援 S3 Intelligent-Tiering 儲存體方案。S3 Intelligent-Tiering 儲存體方案旨在透過自動將資料移動到最具成本效益的儲存體存取層，將儲存成本最佳化，且不會影響效能或帶來額外負荷。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的自動最佳化經常存取物件與不常存取物件的儲存體方案。	2020 年 4 月 30 日
磁帶閘道讀寫效能增至 2 倍	Storage Gateway 將磁帶閘道上的虛擬磁帶讀寫效能增至 2 倍，讓您可比以前更快速的執行備份和復原。如需詳細資訊，請參閱《Storage Gateway 使用者指南》中的磁帶閘道效能指引。	2020 年 4 月 23 日

自動磁帶建立的支援	Storage Gateway 現能夠自動建立新的虛擬磁帶。磁帶閘道可自動建立新的虛擬磁帶，以維持您設定的可用磁帶數目下限，然後這些新磁帶可供備份應用程式進行匯入，讓您執行備份任務時無須中斷。如需詳細資訊，請參閱《Storage Gateway 使用者指南》中的自動建立磁帶。	2020 年 4 月 23 日
新 AWS 區域	Storage Gateway 現在可在 AWS GovCloud （美國東部）區域使用。如需詳細資訊，請參閱 AWS 一般參考 中的 AWS Storage Gateway 端點和配額。	2020 年 3 月 12 日
支援 Linux 核心型虛擬機器（KVM）Hypervisor	Storage Gateway 現在可在KVM虛擬化平台上部署內部部署閘道。部署在 上的閘道KVM具有與現有內部部署閘道相同的所有功能和特徵。如需詳細資訊，請參閱《Storage Gateway 使用者指南》中的支援的 Hypervisor 和主機需求。	2020 年 2 月 4 日

支援VMware vSphere 高可用性	Storage Gateway 現在支援的高可用性VMware，協助保護儲存工作負載免受硬體、Hypervisor 或網路故障的影響。如需詳細資訊，請參閱 Storage Gateway 使用者指南中的使用VMware vSphere 高可用性與 Storage Gateway。Storage Gateway 此版本也包含了效能改善。如需詳細資訊，請參閱《Storage Gateway 使用者指南》中的 效能。	2019 年 11 月 20 日
磁帶閘道的新 AWS 區域	磁帶閘道正式於南美洲 (聖保羅) 區域推出。如需詳細資訊，請參閱 AWS 一般參考 中的 AWS Storage Gateway 端點和配額。	2019 年 9 月 24 日
支援 Linux 上的 IBM Spectrum Protect 7.1.9 版，以及磁帶閘道的磁帶大小上限增加至 5 TiB	除了在 Microsoft Windows 上執行之外，磁帶閘道現在還支援在 Linux 上執行的 IBM Spectrum Protect （ Tivoli Storage Manager ） 7.1.9 版。如需詳細資訊，請參閱 Storage Gateway 使用者指南中的使用 IBM Spectrum Protect 測試您的設定。Storage Gateway 此外，針對磁帶閘道，虛擬磁帶的大小上限現在已從 2.5 TiB 提高至 5 TiB。如需詳細資訊，請參閱《Storage Gateway 使用者指南》中的磁帶配額。	2019 年 9 月 10 日

支援 Amazon CloudWatch Logs	您現在可以使用 Amazon CloudWatch Log Groups 設定 File Gateways，以接收有關錯誤和閘道及其資源運作狀態的通知。如需詳細資訊，請參閱 Storage Gateway 使用者指南 中的使用 Amazon CloudWatch Log Groups 通知閘道運作狀態和錯誤。 Storage Gateway	2019 年 9 月 4 日
新 AWS 區域	Storage Gateway 現已在亞太區域 (香港) 提供。如需詳細資訊，請參閱 AWS 一般參考 中的 AWS Storage Gateway 端點和配額。	2019 年 8 月 14 日
新 AWS 區域	Storage Gateway 現已在中東 (巴林) 區域提供。如需詳細資訊，請參閱 AWS 一般參考 中的 AWS Storage Gateway 端點和配額。	2019 年 7 月 29 日
支援在虛擬私有雲端中啟用閘道 （ VPC ）	您現在可以在 中啟用閘道 VPC。您可以在內部部署軟體裝置以及雲端儲存基礎設施之間建立私有連線。如需詳細資訊，請參閱在 VPC 中啟用閘道。	2019 年 6 月 20 日

支援將虛擬磁帶從 S3 Glacier Flexible Retrieval 遷移至 S3 Glacier Deep Archive	您現在可以將存檔在 S3 Glacier Flexible Retrieval 儲存類別的虛擬磁帶移到 S3 Glacier Deep Archive 儲存類別，以獲得經濟效益與長期資料保留。如需詳細資訊，請參閱從 S3 Glacier Flexible Retrieval 移動磁帶到 S3 Glacier Deep Archive。	2019 年 5 月 28 日
SMB Microsoft Windows 的檔案共用支援 ACLs	對於檔案閘道，您現在可以使用 Microsoft Windows 存取控制清單（ACLs）來控制對伺服器訊息區塊（SMB）檔案共用的存取。如需詳細資訊，請參閱使用 Microsoft Windows ACLs 控制對SMB檔案共用 的存取。	2019 年 5 月 8 日
與 S3 Glacier Deep Archive 整合	磁帶閘道可與 S3 Glacier Deep Archive 整合。您現在可以將虛擬磁帶存檔在 S3 Glacier Deep Archive 以進行長期資料保留。如需詳細資訊，請參閱存檔虛擬磁帶。	2019 年 3 月 27 日
歐洲 Storage Gateway 硬體設備的可用性	可在歐洲購買 Storage Gateway 硬體設備。如需詳細資訊，請參閱 AWS 一般參考中的 AWS Storage Gateway 硬體設備區域。此外，您現在可以將 Storage Gateway 硬體設備上可使用的儲存體從 5 TB 增加至 12 TB，並將所安裝的銅線網路卡以 10 Gb 光纖網路卡取代。如需詳細資訊，請參閱設定您的硬體設備。	2019 年 2 月 25 日

與 整合 AWS Backup	Storage Gateway 與 整合 AWS Backup。您現在可以使用 AWS Backup 來備份使用 Storage Gateway 磁碟區進行雲端備份的內部部署業務應用程式。如需詳細資訊，請參閱備份您的磁碟區。	2019 年 1 月 16 日
支援 Bacula Enterprise 和 IBM Spectrum Protect	Tape Gateways 現在支援 Bacula Enterprise 和 IBM Spectrum Protect。Storage Gateway 現在也支援較新版本的 Veritas NetBackup 、Veritas Backup Exec 和 Quest NetVault 備份。您現在可以使用這些備份應用程式將您的資料備份到 Amazon S3，並直接存檔到離線儲存體 (S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive)。如需詳細資訊，請參閱使用您的備份軟體來測試您的閘道設定。	2018 年 11 月 13 日
支援 Storage Gateway 硬體設備	Storage Gateway 硬體設備包含預先安裝在第三方伺服器的 Storage Gateway 軟體。您可以從 AWS Managemen t Console管理裝置。設備可以託管檔案、磁帶和磁碟區閘道。如需詳細資訊，請參閱使用 Storage Gateway 硬體設備。	2018 年 9 月 18 日

與 Microsoft System Center 2016 Data Protection Manager （DPM）的相容性	Tape Gateways 現在與 Microsoft System Center 2016 Data Protection Manager （ ）相容DPM。您現在可以使用 Microsoft DPM 將資料備份至 Amazon S3，並直接封存至離線儲存（S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）。如需詳細資訊，請參閱使用 Microsoft System Center Data Protection Manager 測試設定。	2018 年 7 月 18 日
支援伺服器訊息區塊（SMB）通訊協定	File Gateways 已新增對伺服器訊息區塊（SMB）通訊協定的支援，以將共用檔案。如需詳細資訊，請參閱建立檔案共享。	2018 年 6 月 20 日
支援檔案共享、快取磁碟區和虛擬磁帶加密	您現在可以使用 AWS Key Management Service（AWS KMS）加密寫入檔案共用、快取磁碟區或虛擬磁帶的資料。目前，您可以使用 來執行此操作 AWS Storage Gateway API。如需詳細資訊，請參閱使用 AWS KMS進行資料加密。	2018 年 6 月 12 日

支援 NovaStor DataCenter/Network	Tape Gateways 現在支援 NovaStor DataCenter/Network。您現在可以使用 NovaStor DataCenter/Network 6.4 或 7.1 版將資料備份至 Amazon S3，並直接封存至離線儲存（S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）。如需詳細資訊，請參閱使用 NovaStor DataCenter/Network 測試您的設定。	2018 年 5 月 24 日

舊版更新

下表說明 2018 年 5 月前每個《AWS Storage Gateway 使用者指南》版本的重要變更。

變更	描述	變更日期
支援 S3 One Zone_IA 儲存類別	您現在可為檔案閘道選擇 S3 One Zone_IA，做為您檔案共享的預設儲存類別。使用此儲存類別，您可以將您的物件資料存放在 Amazon S3 的單一可用區域中。如需詳細資訊，請參閱建立檔案共享。	2018 年 4 月 4 日
新 區域	磁帶閘道現已在亞太區域 (新加坡) 提供。如需詳細資訊，請參閱 AWS 區域 支援 Storage Gateway。	2018 年 4 月 3 日
支援重新整理快取通知、請求者付款，以及 Amazon S3 儲存貯體ACLs的固定。	當閘道完成重新整理您 Amazon S3 儲存貯體的快取時，您現在可以使用檔案閘道收到通知。如需詳細資訊，請參閱 Storage Gateway API參考 中的 RefreshCache.html。 檔案閘道現可讓申請者或讀者支付存取的費用，而不是儲存貯體擁有者支付存取的費用。 File Gateways 現在可讓您將完全控制權授予映射至NFS檔案共用的 S3 儲存貯體擁有者。	2018 年 3 月 1 日

變更	描述	變更日期
	如需詳細資訊，請參閱建立檔案共享。	
支援 Dell EMC NetWorker V9.x	Tape Gateways 現在支援 Dell EMC NetWorker V9.x。您現在可以使用 Dell EMC NetWorker V9.x 將資料備份至 Amazon S3，並直接封存至離線儲存（S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）。如需詳細資訊，請參閱使用 Dell 測試您的設定EMC NetWorker。	2018 年 2 月 27 日
新 區域	Storage Gateway 現已在歐洲 (巴黎) 區域提供。如需詳細資訊，請參閱 AWS 區域 支援 Storage Gateway。	2017 年 12 月 18 日
支援檔案上傳通知和類型猜測 MIME	檔案閘道現在可以在寫入NFS檔案共用的所有檔案都上傳至 Amazon S3 時通知您。如需詳細資訊，請參閱 NotifyWhenUploaded 中的 Storage Gateway API參考。 File Gateways 現在允許根據副檔名猜測上傳物件的MIME類型。如需詳細資訊，請參閱建立檔案共享。	2017 年 11 月 21 日
支援 VMware ESXi Hypervisor 6.5 版	AWS Storage Gateway 現在支援 VMware ESXi Hypervisor 6.5 版。這是 4.1、5.0、5.1、5.5 和 6.0 版以外的支援。如需詳細資訊，請參閱支援的 Hypervisor 與主機需求。	2017 年 9 月 13 日
Commvault 11 相容性	磁帶閘道現在與 Commvault 11 相容。您現在可以使用 Commvault 將您的資料備份到 Amazon S3，並直接存檔到離線儲存體 (S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive)。如需詳細資訊，請參閱使用 Commvault 測試您的設定。	2017 年 9 月 12 日
檔案閘道支援 Microsoft Hyper-V Hypervisor	您現在可以將檔案閘道部署在 Microsoft Hyper-V Hypervisor。如需相關資訊，請參閱 支援的 Hypervisor 與主機需求。	2017 年 6 月 22 日

變更	描述	變更日期
支援 3 到 5 小時的存檔磁帶擷取	您現在可使用磁帶閘道從存檔擷取磁帶，為時 3 到 5 小時。您也可以判斷從備份應用程式或虛擬磁帶程式庫寫入磁帶的資料量（VTL）。如需詳細資訊，請參閱檢視磁帶使用情況。	2017 年 5 月 23 日
新 區域	Storage Gateway 現已在亞太區域 (孟買) 提供。如需詳細資訊，請參閱 AWS 區域 支援 Storage Gateway。	2017 年 5 月 02 日
更新檔案共享設定 支援檔案共享的快取重新整理	檔案閘道現於檔案共享設定中新增掛載選項。您現在可為您的檔案共享設定 squash 和唯讀選項。如需詳細資訊，請參閱建立檔案共享。 檔案閘道現可在 Amazon S3 儲存貯體中尋找自閘道上次列出儲存貯體內容並快取結果後，曾新增或移除的物件。如需詳細資訊，請參閱 API 參考RefreshCache中的 。	2017 年 3 月 28 日
支援複製磁碟區	對於快取的磁碟區閘道， AWS Storage Gateway 現在支援從現有磁碟區複製磁碟區的功能。如需複製磁碟區的詳細資訊，請參閱複製磁碟區。	2017 年 3 月 16 日
支援 Amazon 上的檔案閘道 EC2	AWS Storage Gateway 現在提供在 Amazon 中部署檔案閘道的功能EC2。您現在可以EC2在 Amazon 中使用 Storage Gateway Amazon Machine Image（AMI）在 Amazon 中啟動檔案Storage Gateway，作為社群 AMI。如需如何建立檔案閘道並將其部署到EC2執行個體上的詳細資訊，請參閱建立和啟用 Amazon S3 檔案閘道或建立和啟用 Amazon FSx 檔案閘道。如需有關如何啟動 File Gateway 的資訊AMI，請參閱在 Amazon EC2 主機上部署 S3 File Gateway 或在 Amazon EC2 主機上部署 FSx File Gateway。	2017 年 2 月 08 日
Arcserve 17 相容性	磁帶閘道現在與 Arcserve 17 相容。您現在可以使用 Arcserve 將您的資料備份到 Amazon S3 並直接存檔到 S3 Glacier Flexible Retrieval。如需詳細資訊，請參閱使用 Arcserve Backup r17.0 來測試您的設定。	2017 年 1 月 17 日

變更	描述	變更日期
新 區域	Storage Gateway 現已在歐洲 (倫敦) 區域提供。如需詳細資訊，請參閱 AWS 區域 支援 Storage Gateway。	2016 年 12 月 13 日
新 區域	Storage Gateway 現已在加拿大 (中部) 區域提供。如需詳細資訊，請參閱 AWS 區域 支援 Storage Gateway。	2016 年 12 月 08 日
支援檔案閘道	除了磁碟區閘道和磁帶閘道之外，Storage Gateway 道現在還提供檔案閘道。File Gateway 結合了服務和虛擬軟體設備，可讓您使用 Network File System （ ） 等業界標準檔案通訊協定，在 Amazon S3 中存放和擷取物件NFS。閘道提供 Amazon S3 中物件的存取，作為NFS掛載點上的檔案。	2016 年 11 月 29 日
Backup Exec 16	磁帶閘道現在與 Backup Exec 16 相容。您現在可以使用 Backup Exec 16 將您的資料備份到 Amazon S3，並直接存檔到離線儲存體 (S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive)。如需詳細資訊，請參閱使用 Veritas Backup Exec 測試您的設定。	2016 年 11 月 7 日
與 Micro Focus （ HPE ） Data Protector 9.x 的相容性	Tape Gateway 現在與 Micro Focus （ HPE ） Data Protector 9.x 相容。您現在可以使用 HPE Data Protector 將資料備份至 Amazon S3，並直接封存至 S3 Glacier Flexible Retrieval。如需詳細資訊，請參閱使用 Micro Focus （ HPE ） Data Protector 測試您的設定。	2016 年 11 月 2 日
新 區域	Storage Gateway 現已在美國東部 (俄亥俄) 區域提供。如需詳細資訊，請參閱 AWS 區域 支援 Storage Gateway。	2016 年 10 月 17 日
重新設計 Storage Gateway 主控台	Storage Gateway 管理主控台已重新設計，讓閘道、磁碟區和虛擬磁帶的設定、管理和監控變得更容易。使用者介面現在提供可篩選的檢視，並提供整合 AWS 服務的直接連結，例如 CloudWatch 和 Amazon EBS。如需詳細資訊，請參閱註冊 AWS Storage Gateway。	2016 年 8 月 30 日

變更	描述	變更日期
Veeam Backup & Replication V9 Update 2 或更新版本相容性	磁帶閘道現在與 Veeam Backup & Replication V9 Update 2 或更新版本相容 (即 9.0.0.1715 版或更新版本)。您現在可以使用 Veeam Backup Replication V9 Update 2 或更新版本將您的資料備份到 Amazon S3，並直接存檔到離線儲存體 (S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive)。如需詳細資訊，請參閱使用 Veeam Backup & Replication 測試設定。	2016 年 8 月 15 日
更長的磁碟區和快照 IDs	Storage Gateway IDs為磁碟區和快照引入的時間更長。您可以為磁碟區、快照和其他支援 AWS 的資源啟用較長的 ID 格式。如需詳細資訊，請參閱了解 Storage Gateway 資源與資源 IDs。	2016 年 4 月 25 日
新 區域 支援存放磁碟區大小上限為 512 TiB 的儲存體 Storage Gateway 本機主控台的其他閘道更新和增強功能	亞太區域 (首爾) 區域現在可以使用磁帶閘道。如需詳細資訊，請參閱AWS 區域 支援 Storage Gateway。 您現在可以建立上限 32 個儲存體磁碟區、每個磁碟區大小上限 16 TiB、儲存總量上限 512 TiB 的存放磁碟區。如需詳細資訊，請參閱儲存磁碟區架構和 AWS Storage Gateway 配額。 虛擬磁帶櫃中所有磁帶的總大小增加到 1 PiB。如需詳細資訊，請參閱AWS Storage Gateway 配額。 您現在可以在 Storage Gateway 主控台上設定您 VM 本機主控台的密碼。如需相關資訊，請參閱 從 Storage Gateway 主控台設定本機主控台密碼。	2016 年 3 月 21 日
與 for Dell EMC NetWorker 8.x 的相容性	Tape Gateway 現在與 Dell EMC NetWorker 8.x 相容。您現在可以使用 Dell EMC NetWorker 將資料備份至 Amazon S3，並直接封存至離線儲存 （ S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive ）。如需詳細資訊，請參閱使用 Dell 測試您的設定EMC NetWorker。	2016 年 2 月 29 日

變更	描述	變更日期
支援 VMware ESXi Hypervisor 6.0 版和 Red Hat Enterprise Linux 7 iSCSI 啟動器	AWS Storage Gateway 現在支援 VMware ESXi Hypervisor 6.0 版和 Red Hat Enterprise Linux 7 iSCSI 啟動器。如需詳細資訊，請參閱 支援的 Hypervisor 與主機需求 和 支援的 iSCSI 啟動器。	2015 年 10 月 20 日
內容重組	此版本包含這項改善：文件現在包含管理啟用的閘道一節，其結合所有閘道解決方案常見的管理任務。您可在後文中找到在部署和啟用閘道後，如何管理閘道的說明。如需詳細資訊，請參閱管理您的磁帶閘道。	
支援快取磁碟區大小上限為 1,024 TiB 的儲存體	您現在可以建立上限 32 個儲存磁碟區、每個磁碟區大小上限 32 TiB、儲存總量上限 1,024 TiB 的快取磁碟區。如需詳細資訊，請參閱快取磁碟區架構和 AWS Storage Gateway 配額。	2015 年 9 月 16 日
支援 VMware ESXi Hypervisor 中的 VMXNET3（10 GbE ）網路轉接器類型	如果您的閘道託管在 VMware ESXi Hypervisor 上，您可以重新設定閘道以使用VMXNET3轉接器類型。如需詳細資訊，請參閱設定閘道的網路轉接器。	
效能增強功能	Storage Gateway 上傳率上限已增加到每秒 120 MB，下載速率上限也已增加到每秒 20 MB。	
Storage Gateway 本機主控台的其他增強功能和更新	Storage Gateway 本機主控台已更新並使用額外的功能強化，協助您執行維護任務。如需詳細資訊，請參閱設定您的閘道網路。	
支援標籤	Storage Gateway 現在支援資源標籤。您現在可以將標籤新增到閘道、磁碟區和虛擬磁帶，以便更容易管理它們。如需詳細資訊，請參閱為 Storage Gateway 資源加上標籤。	2015 年 9 月 2 日

變更	描述	變更日期
與 Quest （先前為 Dell） NetVault Backup 10.0 的相容性	Tape Gateway 現在與 Quest NetVault Backup 10.0 相容。您現在可以使用 Quest NetVault Backup 10.0 將資料備份至 Amazon S3，並直接封存至離線儲存 （S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）。如需詳細資訊，請參閱使用 Quest NetVault Backup 測試您的設定。	2015 年 6 月 22 日
支援存放磁碟區閘道設定的 16 TiB 的儲存體磁碟區 支援 Storage Gateway 本機主控台的系統資源檢查 支援 Red Hat Enterprise Linux 6 iSCSI 啟動器	Storage Gateway 現在支援存放磁碟區閘道設定的 16 TiB 的儲存體磁碟區。您現在可以建立 12 個 16 TiB 的儲存磁碟區，儲存總量上限為 192 TiB。如需詳細資訊，請參閱儲存磁碟區架構。 您現在可以判斷您的系統資源 （虛擬CPU核心、根磁碟區大小和 RAM） 是否足以讓您的閘道正常運作。如需詳細資訊，請參閱 檢視閘道系統資源狀態 或 檢視閘道系統資源狀態。 Storage Gateway 現在支援 Red Hat Enterprise Linux 6 iSCSI 啟動器。如需詳細資訊，請參閱設定磁帶閘道的需求。 此版本包含下列 Storage Gateway 改善功能和更新： • 您現在可在 Storage Gateway 主控台中查看到您閘道上次成功套用軟體更新的日期和時間。如需詳細資訊，請參閱管理閘道更新。 • Storage Gateway 現在提供 API，您可以使用 來列出連接至儲存磁碟區的 iSCSI 啟動器。如需詳細資訊，請參閱 API 參考ListVolumeInitiators中的 。	2015 年 6 月 3 日

變更	描述	變更日期
支援 Microsoft Hyper-V 虛擬化管理程序 2012 版和 2012 R2	Storage Gateway 現在支援 Microsoft Hyper-V Hypervisor 2012 版和 2012 R2。這是 Microsoft Hyper-V 虛擬化管理程序 2008 R2 版以外的支援。如需詳細資訊，請參閱支援的 Hypervisor 與主機需求。	2015 年 4 月 30 日
Symantec Backup Exec 15 相容性	磁帶閘道現在與 Symantec Backup Exec 15 相容。您現在可以使用 Symantec Backup Exec 15 將您的資料備份到 Amazon S3，並直接存檔到離線儲存體 (S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive)。如需詳細資訊，請參閱使用 Veritas Backup Exec 測試您的設定。	2015 年 4 月 6 日
CHAP 儲存磁碟區的身分驗證支援	Storage Gateway 現在支援設定儲存磁碟區的CHAP身分驗證。如需詳細資訊，請參閱設定磁碟區的CHAP身分驗證。	2015 年 4 月 2 日
支援 VMware ESXi Hypervisor 5.1 和 5.5 版	Storage Gateway 現在支援 VMware ESXi Hypervisor 5.1 和 5.5 版。這是 VMware ESXi Hypervisor 4.1 版和 5.0 版的附加支援。如需詳細資訊，請參閱支援的 Hypervisor 與主機需求。	2015 年 3 月 30 日
支援 Windows CHKDSK公用程式	Storage Gateway 現在支援 Windows CHKDSK公用程式。您可以使用此公用程式來驗證磁碟區的完整性以及修正磁碟區的錯誤。如需詳細資訊，請參閱針對磁碟區問題進行疑難排解。	2015 年 3 月 04 日

變更	描述	變更日期
與 整合 AWS CloudTrail 以擷取 API通話	Storage Gateway 現在已與 Amazon Web Services 帳戶中由 Storage Gateway 或代表 Storage Gateway 進行的 AWS CloudTrail. AWS CloudTrail captures API 呼叫整合，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。如需詳細資訊，請參閱登錄和監控 AWS Storage Gateway。 此版本包含下列 Storage Gateway 改善功能和更新： • 在快取儲存中有髒數據的虛擬磁帶 (亦即包含已上傳至 AWS的內容)，現在會在閘道的快取磁碟機發生變更時復原。如需詳細資訊，請參閱從無法還原的閘道復原虛擬磁帶。	2014 年 12 月 16 日

變更	描述	變更日期
其他備份軟體和媒體更換器相容性	磁帶閘道現在與下列備份軟體相容： • Symantec Backup Exec 2014 • Microsoft System Center 2012 R2 Data Protection Manager • Veeam Backup & Replication V7 • Veeam Backup & Replication V8 您現在可以將這四種備份軟體產品與 Storage Gateway 虛擬磁帶程式庫（VTL）搭配使用，以備份至 Amazon S3 並直接封存至離線儲存（S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive）。如需詳細資訊，請參閱使用您的備份軟體來測試您的閘道設定。 Storage Gateway 現在提供的額外媒體更換器，可使用新的備份軟體。 此版本包含各種 AWS Storage Gateway 改進和更新。	2014 年 11 月 3 日
歐洲 (法蘭克福) 區域	Storag Gateway 現已在歐洲 (法蘭克福) 區域提供。如需詳細資訊，請參閱 AWS 區域 支援 Storage Gateway。	2014 年 10 月 23 日
內容重組	已建立入門一節，其適用於所有閘道解決方案。您可在後文中尋找下載、部署和啟用閘道的指示。在您部署和啟用閘道之後，您可以繼續進一步了解存放磁碟區、快取磁碟區和磁帶閘道設定的特定說明。如需詳細資訊，請參閱建立磁帶閘道。	2014 年 5 月 19 日

變更	描述	變更日期
Symantec Backup Exec 2012 相容性	磁帶閘道現在與 Symantec Backup Exec 2012 相容。您現在可以使用 Symantec Backup Exec 2012 將您的資料備份到 Amazon S3，並直接存檔到離線儲存體 (S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive)。如需詳細資訊，請參閱使用 Veritas Backup Exec 測試您的設定。	2014 年 4 月 28 日
支援 Windows Server 容錯移轉叢集 對VMwareESX啟動器的支援 支援在 Storage Gateway 本機主控台上執行組態任務	• 如果主機使用 Windows Server 容錯移轉叢集 （ ） 協調存取，Storage Gateway 現在支援將多個主機連接到相同的磁碟區WSFC。但是，如果沒有使用 ，則無法將多個主機連接到相同的磁碟區WSFC。 • Storage Gateway 現在可讓您直接透過ESX主機管理儲存連線。這提供了在 的訪客作業系統中使用駐留啟動器的替代方案VMs。 • Storage Gateway 現可支援在 Storage Gateway 本機主控台上執行組態任務。如需在部署於內部部署之閘道上執行組態任務的資訊，請參閱在 VM 本機主控台上執行任務或在 VM 本機主控台上執行任務。如需在EC2執行個體上部署的閘道上執行組態任務的相關資訊，請參閱 在 Amazon EC2 Local Console 上執行任務或 在 Amazon EC2 Local Console 上執行任務。	2014 年 1 月 31 日

變更	描述	變更日期
支援虛擬磁帶程式庫（VTL）和推出2013-06-30 API版	Storage Gateway 會將內部部署軟體設備與雲端儲存連線，以整合您的內部部署 IT 環境與 AWS 儲存基礎設施。除了磁碟區閘道（快取磁碟區和儲存磁碟區）之外，Storage Gateway 現在還支援閘道虛擬磁帶程式庫（VTL）。您可以設定磁帶閘道在每個閘道最多 10 個虛擬磁帶機。每個虛擬磁帶機都會回應SCSI命令集，因此您現有的內部部署備份應用程式將運作而不進行修改。如需詳細資訊，請參閱《AWS Storage Gateway 使用者指南》中的以下主題： • 如需架構概觀，請參閱磁帶閘道的運作方式 (架構)。 • 若要開始使用磁帶閘道，請參閱建立磁帶閘道。	2013 年 11 月 5 日
支援 Microsoft Hyper-V	Storage Gateway 現在能夠讓您在 Microsoft Hyper-V 虛擬化平台上部署內部部署閘道。部署在 Microsoft Hyper-V 的閘道擁有和現有內部部署 Storage Gateway 相同的所有功能和特性。若要開始使用 Microsoft Hyper-V 部署閘道，請參閱支援的 Hypervisor 與主機需求。	2013 年 4 月 10 日
支援在 Amazon 上部署閘道 EC2	Storage Gateway 現在提供在 Amazon Elastic Compute Cloud（Amazon）中部署閘道的功能EC2。您可以使用 中AMI提供的 Storage Gateway EC2 在 Amazon 中啟動閘道執行個體AWS Marketplace。若要使用 Storage Gateway 開始部署閘道AMI，請參閱部署適用於磁帶閘道的自訂 Amazon EC2執行個體。	2013 年 1 月 15 日

變更	描述	變更日期
支援快取磁碟區和推出 2012-06-30 API版	在此版本中，Storage Gateway 引入了對快取磁碟區的支援。快取磁碟區可將擴展內部部署儲存基礎設施的需求減到最低，同時讓應用程式以低延遲方式存取其作用中的資料。您最多可以建立 32 TiB 大小的儲存磁碟區，並將其掛載為內部部署應用程式伺服器的 iSCSI 裝置。寫入您快取磁碟區的資料，會存放在 Amazon Simple Storage Service (Amazon S3) 中，而只有最近寫入和讀取資料的快取，才會存放在您內部部署儲存硬體的本機上。快取磁碟區允許您利用 Amazon S3 處理接受較高延遲的資料，例如不常存取的較舊資料，同時為需要低延遲存取的資料保持內部部署儲存體。 在此版本中，Storage Gateway 也會推出新API版本，除了支援目前的操作之外， 還提供支援快取磁碟區的新操作。 如需兩種 Storage Gateway 解決方案的詳細資訊，請參閱 磁帶閘道的運作方式。 您也可以嘗試測試設定。如需相關指示，請參閱建立磁帶閘道。	2012 年 10 月 29 日

變更	描述	變更日期
API 和 IAM 支援	在此版本中，Storage Gateway 引入對 AWS Identity and Access Management（ ）的API支援和支援IAM。 • API 支援：您現在可以以程式設計方式設定和管理 Storage Gateway 資源。如需 的詳細資訊API，請參閱 使用者指南 APIStorage Gateway 的參考資料 中的 。 AWS Storage Gateway • IAM 支援 – AWS Identity and Access Management（IAM）可讓您建立使用者，並管理使用者透過IAM政策存取 Storage Gateway 資源的權限。如需 IAM 政策範例，請參閱Identity and Access Management for AWS Storage Gateway。如需 的詳細資訊IAM，請參閱 AWS Identity and Access Management（IAM） 詳細資訊頁面。	2012 年 5 月 9 日
靜態 IP 支援	您現在可以為本機閘道指定靜態 IP。如需詳細資訊，請參閱設定您的閘道網路。	2012 年 3 月 5 日
新指南	這是《AWS Storage Gateway 使用者指南》的第一版。	2012 年 1 月 24 日

Tape Gateway 設備軟體的版本備註

這些版本備註描述了磁帶閘道設備每個版本隨附的新功能和更新功能、改進和修正。每個軟體版本都會以其發行日期和唯一的版本編號來識別。

您可以在 Storage Gateway 主控台中檢查閘道的詳細資訊頁面，或使用類似下列的 AWS CLI 命令呼叫 DescribeGatewayInformationAPI動作，以判斷閘道的軟體版本編號： Storage Gateway

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

版本編號會傳回API回應的 `SoftwareVersion` 欄位。

> **Note**
>
> 在下列情況下，閘道不會報告軟體版本資訊：
>
> - 閘道已離線。
> - 閘道正在執行不支援版本報告的較舊軟體。
> - 閘道類型為 FSx File Gateway。

如需磁帶閘道更新的詳細資訊，包括如何修改閘道的預設自動維護和更新排程，請參閱使用 AWS Storage Gateway 主控台。

版本日期	軟體版本	版本備註
2024-08-30	2.11.0	• 新閘道和現有閘道的作業系統更新
2024-07-29	2.10.0	• 新閘道和現有閘道的作業系統更新 • 其他錯誤修正和增強功能
2024-06-17	2.9.2	• 新閘道和現有閘道的作業系統更新

版本日期	軟體版本	版本備註
2024-05-28	2.9.0	• 減少軟體更新期間的閘道重新啟動時間 • 減少用於估計網路頻寬的傳輸資料量
2024-05-08	2.8.3	• 解決使用 SOCKS5 Proxy 時的雲端連線問題 • 已解決特定條件下的上傳效能降級問題（例如，磁帶清除操作次數過多）
2024-04-10	2.8.1	• 解決 2.8.0 中引入的記憶體用量問題 • 安全修補程式更新 • 改善軟體更新程序 • 已解決新閘道遺失的網路時間通訊協定（NTP）元件
2024-03-06	2.8.0	• 新閘道的作業系統更新 • 安全修補程式更新 • 改善並行備份和還原工作負載的效能
2023-12-19	2.7.0	• 新閘道的作業系統更新
2023-12-14	2.6.6	• 已修正在大於 5TiB 磁帶上相對定位的問題
2023-10-19	2.6.5	• 新增閘道重新啟動後用戶端覆寫磁帶的防護措施

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。