使用者指南

AWSStorage Gateway

API 版本 2013-06-30

AWSStorage Gateway: 使用者指南

Table of Contents

什麼是 Amazon S3 檔案閘道

AWSStorage Gateway 可連線現場部署軟體應用裝置與雲端類型儲存，在您的現場部署 IT 環境與AWS儲存基礎設施。您可以使用該服務將數據存儲在AWS可擴展且具有成本效益的儲存，幫助維護資料安全。AWSStorage Gateway 提供檔案類型、磁碟區類型和磁帶類型儲存解決方案。

主題

Amazon S3 檔案閘道

Amazon S3 檔案閘道— 亞馬遜 S3 文件網關支持Amazon Simple Storage Service (Amazon S3)，並結合服務與虛擬軟體應用裝置。通過使用這個組合，您可以使用產業標準檔案通訊協定 (例如網路檔案系統 (NFS) 和伺服器消息塊 (SMB) 將物件存放和檢索至 Amazon S3。軟體設備或閘道會部署至您的內部部署環境做為在 VMware ESXi、Microsoft Hyper-V 或 Linux 核心型虛擬機器 (KVM) Hypervisor 上執行的虛擬機器 (VM)。閘道可存取 S3 中的物件做為檔案或檔案共享掛載點。使用 S3 檔案閘道，您可以執行下列作業：

- 您可以使用 NFS 第 3 版或 4.1 版通訊協定直接存放和擷取檔案。
- 您可以使用 SMB 檔案系統第 2 版和第 3 版通訊協定直接存放和擷取檔案。
- 您可以從 Amazon S3 何AWS雲應用程序或服務。
- 您可以使用生命週期政策、跨區域複寫和版本控制來管理 S3 資料。您可以將 S3 檔案閘道視為 Amazon S3 上的檔案系統掛載。

S3 檔案閘道可簡化 Amazon S3 中的檔案儲存、透過產業標準檔案系統通訊協定整合至現有應用程式，以及提供現場部署儲存的具成本效益替代方案。它也透過透明本機快取來提供資料的低延遲存取。S3 文件網關管理傳入和傳出的數據傳輸AWS可緩衝應用程式的網路擁塞、最佳化和平行串流資料，以及管理頻寬耗用量。S3 文件網關與AWS服務，例如下列項目：

- 使用 AWS Identity and Access Management (IAM) 的常用存取管理
- 使用 AWS Key Management Service (AWS KMS) 加密
- 使用 Amazon CloudWatch 進行監控
- 稽核使用AWS CloudTrail（CloudTrail）
- 使用AWS Management Console和 AWS Command Line Interface (AWS CLI) 的操作

- 帳單與成本管理

在下列文件中，您可以找到涵蓋所有閘道通用設定資訊的入門小節，也可以找到閘道特定設定小節。入門小節顯示如何部署、啟用和設定閘道的儲存。管理小節顯示如何管理閘道和資源：

- 提供如何建立和使用 S3 檔案閘道的說明。它顯示如何建立檔案共享、將磁碟機對應至 Amazon S3 儲存貯體，以及將檔案和資料夾上傳至 Amazon S3。

- 說明如何執行所有閘道類型和資源的管理任務。

在本指南中，您主要可以找到如何使用 AWS Management Console來使用閘道操作。如果您想要以程式設計方式執行這些操作，請參閱AWSStorage Gateway API 參考。

Storage Gateway 的工作原理（體繫結構）

之後，您可以尋找可用 Storage Gateway 解決方案的架構概觀。

主題

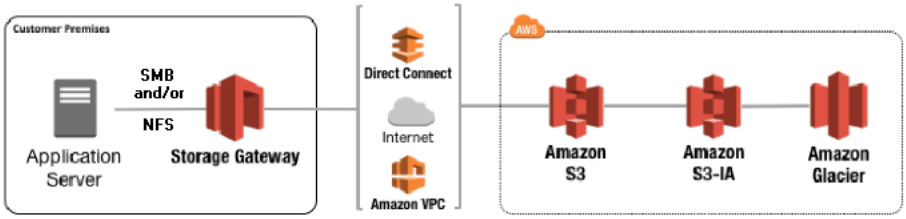
Amazon S3 檔案閘道

若要使用 S3 檔案閘道，可以從下載適用於閘道的 VM 映像開始。然後，您可以從AWS Management Console或通過 Storage Gateway API 進行訪問。您也可以使用 Amazon EC2 映像建立 S3 檔案閘道。

啟用 S3 檔案閘道之後，您可以建立和設定檔案共享，並建立該共享與 Simple Storage Service (Amazon S3) 體的關聯。這樣，客户端可以使用網路檔案系統 (NFS) 或伺服器訊息區塊 (SMB) 通訊協定存取共享。寫入至檔案共享的檔案會成為 Amazon S3 中路徑作為金鑰的物件。檔案與物件之間具有一對一映射，而閘道會在您變更檔案時非同步更新 Amazon S3 中的物件。Amazon S3 儲存貯體中的現有物件會顯示為檔案，而金鑰會成為路徑。使用 Amazon S3 — 伺服器端加密金鑰 (SSE-S3) 進行加密。所有資料傳輸都是透過 HTTPS 完成。

該服務優化了網關和AWS使用分段平行上傳或位元組範圍下載，以更適當地使用可用的頻寬。維護本機快取，以提供最近存取資料的低延遲存取，並降低資料傳出費用。CloudWatch 指標可以深入瞭解 VM 上的資源使用以及進出的資料傳輸AWS。雲端追蹤所有 API 呼叫。

使用 S3 檔案閘道儲存，您可以在將雲端工作負載攝取至 Amazon S3、執行備份和存檔、分層儲存資料並將其遷移至AWS雲端。下圖概述了儲存閘道的檔案儲存部署。



S3 文件網關在將文件上傳到 Amazon S3 時將文件轉換為 S3 對象。針對 S3 文件網關和 S3 對象上的文件共享執行的文件操作之間的交互需要在文件和對象之間進行轉換時仔細考慮某些操作。

常見文件操作會更改文件元數據，從而導致刪除當前 S3 對象並創建新的 S3 對象。下表顯示了示例文件操作以及對 S3 對象的影響。

文件操作	S3 物件影響	儲存方案含義
重新命名檔案	替換現有 S3 對象併為每個文件創建一個新的 S3 對象	可能會收取提前刪除費用和檢索費
重新命名檔案	替換所有現有 S3 對象，併為文件夾結構中的每個文件夾和文件創建新的 S3 對象	可能會收取提前刪除費用和檢索費
更改文件/文件夾權限	替換現有 S3 對象併為每個文件或文件夾創建一個新的 S3 對象	可能會收取提前刪除費用和檢索費
更改文件/文件夾所有權	替換現有 S3 對象併為每個文件或文件夾創建一個新的 S3 對象	可能會收取提前刪除費用和檢索費
附加到文件	替換現有 S3 對象併為每個文件創建一個新的 S3 對象	可能會收取提前刪除費用和檢索費

當文件由 NFS 或 SMB 客户端寫入 S3 文件網關時，文件網關會將文件的數據上傳到 Amazon S3，後跟其元數據（所有權、時間戳等）。上傳文件數據會創建一個 S3 對象，上傳文件的元數據會更新 S3 對象的元數據。此過程將創建對象的另一個版本，從而產生兩個版本的對象。如果啟用 S3 版本控制，則會儲存這兩個版本。

當文件上傳到 Amazon S3 後，NFS 或 SMB 客户端在 S3 文件網關中修改文件時，S3 文件網關將上傳新數據或修改後的數據，而不是上傳整個文件。文件修改將導致正在創建 S3 對象的新版本。

當 S3 文件網關上傳較大的文件時，它可能需要在客户端完成寫入 S3 文件網關之前上傳較小的文件塊。這樣做的一些原因包括釋放緩存空間或高寫入文件共享的速率。這會導致 S3 儲存貯體中具有多個物件版本。

在設置生命週期策略以將對象移動到不同的存儲類之前，您應該監視 S3 存儲桶以確定存在多少個對象版本。您應該為早期版本配置生命週期過期，以最大限度地減少 S3 存儲桶中對象的版本數量。在 S3 存儲桶之間使用相同區域複製 (SRR) 或跨區域複製 (CRR) 將增加所使用的存儲空間。

設定 Amazon S3 檔案閘道

本節提供 Amazon S3 檔案閘道入門指示。若要開始，首先您必須註冊AWS。如果您是第一次使用，我們建議您讀區域和要求章節位置。

主題

- 註冊 Amazon Web Services
- 建立 IAM 使用者
- 檔案閘道設定要求
- 存取 AWS Storage Gateway
- 支援的 AWS 區域

註冊 Amazon Web Services

如果您還沒有 AWS 帳戶，請完成下列步驟建立新帳戶。

註冊 AWS 帳戶

1. 開啟 https://portal.aws.amazon.com/billing/signup。
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。

建立 IAM 使用者

建立AWS帳戶，請使用下列步驟來建立AWS Identity and Access Management(IAM) 用戶。然後，您會將該用戶加入到具有管理員許可的羣組中。

為您自己建立一個管理員使用者，並將使用者新增至管理員群組 (主控台)

1. 選擇 Root user (根使用者) 並輸入您的 AWS 帳戶 電子郵件地址，以帳戶擁有者身分登入 IAM 主控台。在下一頁中，輸入您的密碼。

> **Note**
>
> 強烈建議您遵循 **Administrator** IAM 使用者的最佳實務，並妥善保管根使用者憑證。只在需要執行少數帳戶和服務管理任務時，才以根使用者身分登入。

2. 在導覽窗格中，選擇 Users (使用者)，然後選擇 Add user (新增使用者)。
3. 在 User name (使用者名稱) 中輸入 **Administrator**。
4. 選取 AWS Management Console access (AWS Management Console 管理主控台存取) 旁的核取方塊。然後選取 Custom password (自訂密碼)，接著在文字方塊中輸入您的新密碼。
5. (選用) 在預設情況下，AWS 會要求新使用者在第一次登入時建立新的密碼。您可以清除 User must create a new password at next sign-in (使用者下次登入必須建立新的密碼) 旁的核取方塊，讓新使用者登入時可以重設密碼。
6. 選擇 Next: (下一步：) Permissions (許可)。
7. 在 Set permissions (設定許可) 下，選擇 Add user to group (將使用者新增至群組)。
8. 選擇 Create group (建立群組)。
9. 在 Create group (建立群組) 對話方塊中，請於 Group name (群組名稱) 輸入 **Administrators**。
10. 選擇 Filter policies (篩選政策)，然後選取 AWS managed -job function (AWS 受管 - 任務職能) 以篩選表格內容。
11. 在政策清單中，選取 AdministratorAccess 的核取方塊。接著選擇 Create group (建立群組)。

> **Note**
>
> 您必須啟用 IAM 使用者和角色對帳單的存取權，才能使用 AdministratorAccess 許可來存取 AWS Billing and Cost Management 主控台。若要這樣做，請遵循委派對帳單主控台的存取權相關教學課程的步驟 1 中的指示。

12. 回到群組清單，選取新群組的核取方塊。必要時，選擇 Refresh (重新整理) 以顯示清單中的群組。
13. 選擇 Next: (下一步：) Tags (標籤)。
14. (選用) 藉由連接標籤作為金鑰/值組，將中繼資料新增至使用者。如需有關在 IAM 中使用標籤的詳細資訊，請參閱《IAM 使用者指南》中的標記 IAM 實體。
15. 選擇 Next: (下一步：) 檢閱，查看要新增至新使用者的羣組成員資格清單。準備好繼續時，請選擇 Create user (建立使用者)。

您可以使用相同的程序建立更多群組和使用者，並授予使用者存取您的 AWS 帳戶 資源的權限。欲了解以政策限制使用者對特定 AWS 資源的許可，請參閱存取管理和範例政策。

檔案閘道設定要求

除非另有說明，否則以下需求皆為AWS Storage Gateway。您的設置必須符合本節中的要求。在部署網關之前，請查看適用於網關設置的要求。

主題

必需的先決條件

在使用 Amazon FsX 檔案閘道 (FSx 檔案閘道) 之前，您必須符合以下要求：

- 建立和設 FSx for Windows File Server 檔案系統。如需說明，請參閱「」步驟 1：建立檔案系統中的Amazon FSx for Windows File Server 用户指南。
- 配置 Microsoft Active Directory (AD)。
- 確保網關和AWS。成功下載、激活和更新網關至少需要 100 Mbps。
- 配置您的專用網絡、VPN 或AWS Direct Connect在您的 Amazon Virtual Private Cloud (Amazon VPC) 和您將部署 FSX 檔案閘道的現場環境之間。
- 確保您的網關可以解析您的活動目錄域控制器的名稱。您可以在 Active Directory 域中使用 DHCP 來處理解析，或者從網關本地控制台的「網絡配置設置」菜單中手動指定 DNS 服務器。

硬體及儲存體需求

下列部分提供閘道所需的最少硬體和設定的相關信息，以及為所需的儲存體分配的最小磁碟空間。

如需檔案閘道效能最佳實務的詳細資訊，請參閱 關於文件網關的效能指南。

現場部署 VM 的硬體需求

在現場部署您的閘道時，您必須確保閘道虛擬機器 (VM) 將部署至的底層硬體可專用於下列最少資源：

- 指派給 VM 的四個虛擬處理器
- 16 GiB 預留 RAM 用於檔案閘道
- 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 檔案共享的配額。

Amazon EC2 執行個體類型的要求

在 Amazon Elastic Compute Cloud (Amazon EC2) 上部署您的閘道時，執行個體的大小必須至少為**`xlarge`**以便您的網關正常工作。但是，針對運算最佳化執行個體系列，大小必須至少為**`2xlarge`**。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。

檔案閘道類型的建議項目

- 一般用途執行個體系列 — m4 或 m5 執行個體類型。
- 運算最佳化執行個體系列 — c4 或 c5 執行個體類型。選取 2xlarge 或更高的執行個體大小來符合必要的 RAM 需求。
- 記憶體最佳化執行個體系列 — r3 執行個體類型。
- 儲存體最佳化執行個體系列 — i3 執行個體類型。

> **Note**
>
> 當您在 Amazon EC2 中啟動您的閘道，並且您選取的執行個體類型支援暫時性儲存時，磁碟會自動列出。如需 Amazon EC2 執行個體儲存體的詳細資訊，請參執行個體存儲中的Amazon EC2 使用者指南。
>
> 應用程式寫入會同步存放在快取中，並會非同步上傳至 Amazon S3 中的耐用儲存體。若暫時性儲存因執行個體在上傳完成前停止而遺失，仍在快取中並且還未寫入 Amazon Simple Storage Service (Amazon S3) 的資料將可能遺失。在您停止主控閘道的執行個體前，請確認`CachePercentDirty`CloudWatch 指標是`0`。如需暫時性儲存的詳細資訊，請參閱將臨時存儲與 EC2 網關結合使用。如需 Storage Gateway 之監控指標的詳細資訊，請參監視檔案閘道。

若您在您的 S3 儲存貯體中有超過 500 萬個物件，並且您使用的是一般用途 SSD 磁碟區，則為了讓您的閘道在啟動時獲得可接受的效能，至少需要 350 GiB 的根 EBS 磁碟區。如需如何增加磁碟區大小的資訊，請參使用 Elastic Volumes 修改 EBS 磁碟區 (主控台)。

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。

閘道類型	高速緩存（最小值）	高速緩存（最大值）			
檔案閘道	150 GiB	64 TiB			

Note

您可以為緩存配置一個或多個本地驅動器，最多可達到最大容量。
將快取添加至現有的閘道時，請務必在您的主機 (虛擬化管理程序或 Amazon EC2 執行個體) 中建立新的磁碟。若先前已將磁碟配置為快取，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 檔案共享的配額。

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。

網絡帶寬要求因網關上傳和下載的數據量而異。成功下載、激活和更新網關至少需要 100Mbps。您的數據傳輸模式將決定支持工作負載所需的帶寬。

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，您可能會在 Amazon EC2 上部署 FSx File Gateway，或是使用其他部署類型 (包括現場部署) 與限制AWSIP 地址範圍。在這些情況下，您的閘道可能會發生服務連線問題，當AWSIP 範圍值發生變化。所以此AWS您需使用的 IP 地址範圍值，位於AWS您在中激活閘道的區域。有關當前 IP 範圍值，請參閱AWSIP 地址範圍中的AWS一般參考。

主題

連接埠需求

Storage Gateway 需要允許特定的連接埠才能進行操作。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。

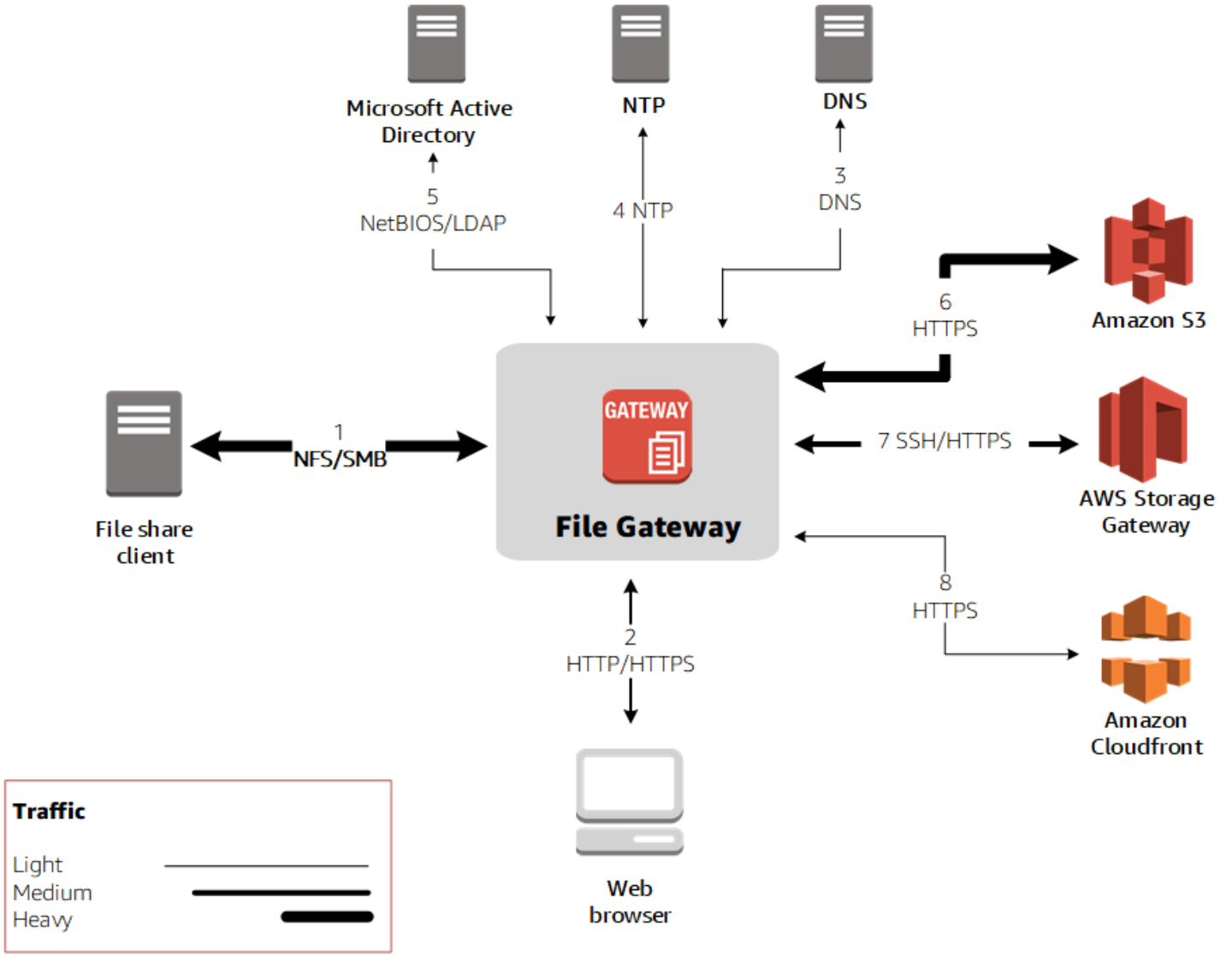
通訊協定	連接埠	Direction	來源	Destination (目的地)	使用方式
TCP	443 (HTTPS)	傳出	Storage Gateway	AWS	對於從 Storage Gateway 到AWS服務端點。如需服務端點的資訊，請參閱 允許透過防火牆和路由器的 AWS Storage Gateway 存取。
TCP	80 (HTTP)	傳入	從中連接到AWS Management Console。	Storage Gateway	由本機系統取得儲存閘道啟用金鑰。僅有在

通訊協定	連接埠	Direction	來源	Destination (目的地)	使用方式
					啟用 Storage Gateway 設備時，才會使用連接埠 80。 Storage Gateway 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 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。
UDP/UDP	53 (DNS)	傳出	Storage Gateway	DNS 伺服器	用於 Storage Gateway 與 DNS 伺服器之間的通訊。

通訊協定	連接埠	Direction	來源	Destination (目的地)	使用方式
TCP	22 (支援通道)	傳出	Storage Gateway	AWS Support	允許AWS Support，以訪問閘道，以幫助您排解閘道問題。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 客户端	NTP 伺服器	本機系統用來將 VM 的時間與主機時間同步。

檔案閘道的連接埠

下圖顯示要為 S3 檔案閘道開啟的連接埠。



> **Note**
>
> 如需特定端口要求，請參閱連接埠需求。

若您想讓網域使用者能夠存取服務器訊息區塊 (SMB) 檔案共享時，您只需使用 Microsoft Active Directory 網關。您可以將您的檔案閘道加入任何有效的 Microsoft Windows 網域 (可由 DNS 解析)。

您也可以使用AWS Directory Service建立「AWS Managed Microsoft AD」(位於 Amazon Web Services Cloud)。對於大多數AWS Managed Microsoft AD部署時，您需要為您的 VPC 設定動態主機設定協議 (DHCP) 服務。如需建立 DHCP 選項集的詳細資訊，請參建立 DHCP 選項集中的AWS Directory Service管理指南。

除了常用的連接埠之外，Amazon S3 檔案閘道還需下要下列連接埠。

通訊協定	連接埠	Direction	來源	Destination (目的地)	使用方式
TCP/UDP	2049 (NFS)	傳入	NFS 客户端	Storage Gateway	使本機系統能夠連線至閘道公開的 NFS 共享。
TCP/UDP	111 (非政府組織第三屆會議)	傳入	NFS3 客户端	Storage Gateway	用於本地系統連接到網關公開的端口映射器。 Note 此端口僅用於 NFSv3。
TCP/UDP	第三屆會議	傳入	NFS3 客户端	Storage Gateway	使本機系統能夠連線至閘道公開的掛載。 Note 此端口僅用於 NFSv3。

Storage Gateway 硬體設備的網路與防火牆需求

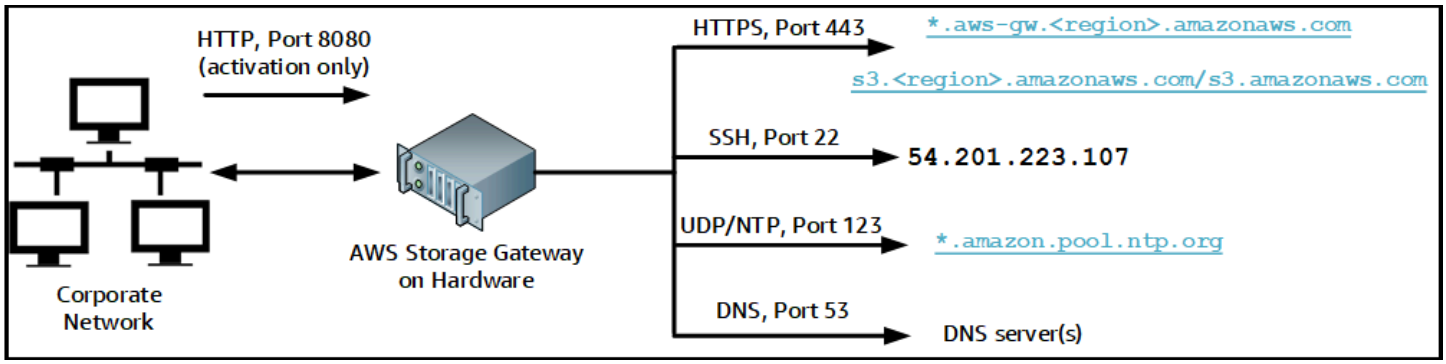
每個 Storage Gateway 硬體設備都需要以下網路服務：

- 網路存取— 通過服務器上的任何網路接口，始終在線與 Internet 連線。
- DNS 服務— 用於硬體設備與 DNS 伺服器之間通訊的 DNS 服務。
- 時間同步— 必須能夠存取自動設定的 Amazon NTP 時間服務。
- IP 地址— 指派的 DHCP 或靜態 IPv4 地址。您不能指派 IPv6 地址。

Dell PowerEdge R640 伺服器後方有 5 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

您可以將 iDRAC 連接埠用於遠端伺服器管理。



硬體設備需要以下連接埠才能運作。

通訊協定	連接埠	Direction	來源	Destination (目的地)	使用方式
SSH	22	傳出	硬體設備	54.201.223.107	支援通道

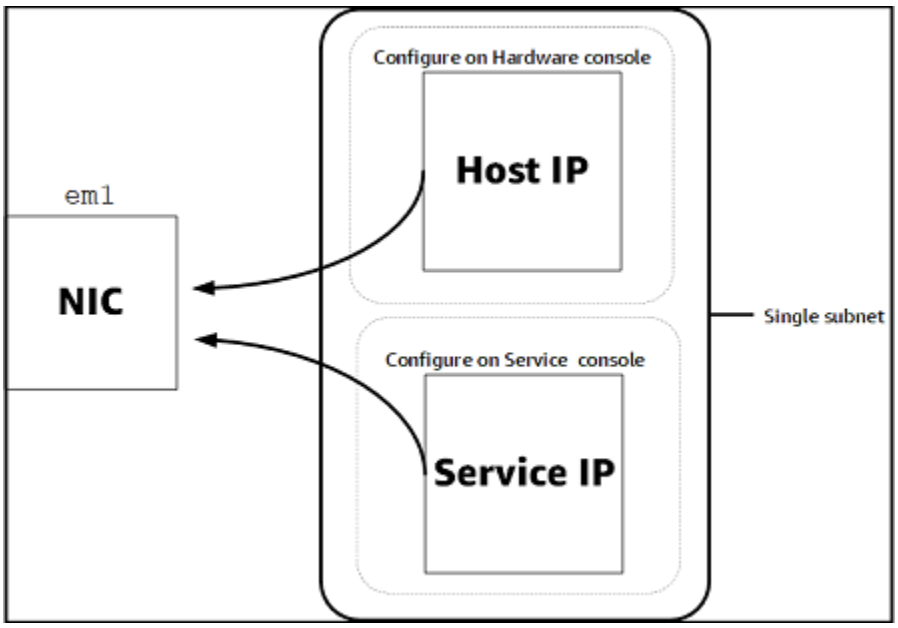
通訊協定	連接埠	Direction	來源	Destination (目的地)	使用方式
DNS	53	傳出	硬體設備	DNS 伺服器	名稱解析
UDP/NTP	123	傳出	硬體設備	`*.amazon.pool.ntp.org`	時間同步
HTTPS	443	傳出	硬體設備	`*.amazonaws.com`	資料傳輸
HTTP	8080	傳入	AWS	硬體設備	啟用 (只需短暫時間)

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 設定閘道參數。

> **Note**
>
> 若要查看顯示伺服器背面及其連接埠的插圖，請參閱機架安裝您的硬件設備並將其連接到電源。

同一個網路介面 (NIC) 上的所有 IP 地址都必須位在同一個子網路，無論是用於閘道或主機。下圖顯示了定址配置。



如需啟用和設定硬體設備的詳細資訊，請參使用 Storage Gateway 硬體設備。

允許透過防火牆和路由器的 AWS Storage Gateway 存取

您的閘道必須存取下列端點，才能與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。

> **Important**
>
> 取決於您的網關AWS區域，替換*##*在服務終端節點中使用正確的區域字符串。

下列服務端點為所有閘道頭部署操作的必要項目。

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

所有網關都需要以下服務端點來控制路徑（anon-cp、client-cp、proxy-app）和數據路徑（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
```

進行 API 呼叫時必須使用下列閘道服務端點。

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

下列範例是美國西部 (奧勒岡) 區域 (us-west-2。

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

下圖顯示的 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 Amazon S3 儲存貯體。

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

下列範例是 Amazon S3 美國東部 (俄亥俄州) 區域 (us-east-2。

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

> **Note**
>
> 如果您的網關無法確定AWSS3 儲存儲體所在的區域中，此服務端點默認為s3.us-east-1.amazonaws.com。我們建議您允許訪問美國東部（弗吉尼亞北部）區域 (us-east-1)，以及您的閘道啟用所在的區域，以及 S3 儲存貯體所在的區域。

下列是 Amazon S3 服務端點，用於AWS GovCloud (US)地區。

```
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 S3 儲存儲體的 FIPS 服務端點。AWSGovCloud (美國西部) 區域。

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

Amazon CloudFront 端點為的必要項目，Storage Gateway 才能取得可用AWS地區。

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

儲存體閘道 VM 會設定為使用下列 NTP 伺服器。

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

- 存儲網關 — 用於支持AWS區域和AWS可與 Storage Gateway 一起使用的服務終端節點，請參閱AWS Storage Gateway端點和配額中的AWS一般參考。
- Storage Gateway 硬體設備 — 針對支援的AWS可與硬件設備一起使用的區域，請參閱Storage Gateway 硬件設備區域中的AWS一般參考。

為 Amazon EC2 閘道執行個體設定安全組

InAWS Storage Gateway時，安全組控制流向 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其安全群組外部連線至閘道，則建議您只允許連接埠 3260 (適用於 iSCSI 連線) 和 80 (適用於啟用) 上的連線。
- 若您想從閘道安全組外部的 Amazon EC2 主機啟用閘道，則允許連接埠 80 上來自該主機之 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。
- 只有在您基於故障診斷而使用 AWS Support 時，才允許連接埠 22 存取。如需詳細資訊，請參閱 你想要的AWS Support幫助您排除 EC2 網關故障。

在某些情況下，您可能會使用 Amazon EC2 執行個體做為啟動器 (也就是說，連線至 Amazon EC2 上部署閘道上的 iSCSI 目標)。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，請參閱連接埠需求。

支援的 Hypervisor 與主機需求

您可以 Storage Gateway 擬機器 (VM) 裝置或物理硬體設備形式，或是在AWS執行個體設定為 Amazon EC2 執行個體。

Storage Gateway 支援下列虛擬化管理程序版本與主機：

- VMware ESXi 虛擬化管理程序 (6.0、6.5 或 6.7 版) — VMware 的免費版本可自VMware 官方網站。針對此設定，您也需要 VMware vSphere 用戶端以連線到主機。
- Microsoft Hyper-V 虛擬化管理程序 (2012 R2 或 2016 版本) — Hyper-V 的免費、獨立版本可自微軟下載中心。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) — 免費的開放源碼虛擬化技術。KVM 包含在所有版本 2.6.20 及更新版本中。已針對 CentOS/RHEL 7.7、Ubuntu 16.04 LTS 與 Ubuntu 18.04 LTS 發行版進行測試和支援。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，而且您已經熟悉 KVM 的運作方式，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)。如需如何在 Amazon EC2 上部署閘道的資訊，請參在 Amazon EC2 主機上部署檔案閘道。
- Storage Gateway 硬體設備 — Storage Gateway 以現場部署選項形式，為具有有限虛擬機器基礎設施的位置提供物理硬體設備。

> **Note**
>
> Storage Gateway 道不支援透過從快照、另一個閘道 VM 的複製，或是從您的 Amazon EC2 AMI 建立的 VM 復原閘道。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 從意外的虛擬機關閉中恢復。
> Storage Gateway 不支援動態記憶體和虛擬記憶體佔用。

檔案閘道支援的 NFS 用戶端

檔案閘道支援下列網路檔案系統 (NFS) 用戶端：

- Amazon Linux

- Mac OS X

> **Note**
>
> 我們建議您將`rsize`和`wsize`裝載選項設置為 64KB，以提高在 Mac OS X 上掛載 NFS 文件共享時的性能。

- RHEL 7
- SUSE Linux Enterprise Server 11 及 SUSE Linux Enterprise Server 12
- Ubuntu 14.04
- Microsoft Windows 10 企業版、Windows Server 2012 及 Windows Server 2016。原生用戶端只支援 NFS 版本 3。
- Windows 7 企業版及 Windows Server 2008。

  原生用戶端只支援 NFS v3。支援的最大 NFS I/O 大小為 32 KB，因此您可能會在這些版本的 Windows 上遇到效能降低的問題。

> **Note**
>
> 您現在可以在需要透過 Windows (SMB) 用戶端 (而非 Windows NFS 用戶端) 進行存取時，使用 SMB 檔案共享。

檔案閘道支援的 SMB 用戶端

檔案閘道支援下列服務訊息區塊 (SMB) 用戶端：

- Microsoft Windows Server 2008 及更新版本
- Windows 桌面版本：10、8 及 7。
- Windows Server 2008 及更新版本上運行的 Windows Terminal Server

> **Note**
>
> 服務器消息塊加密需要支持 SMB v2.1 的客户端。

檔案閘道支援的檔案系統操作

您的 NFS 或 SMB 用戶端可寫入、讀取、刪除和截斷檔案。當客户端將寫入發送到AWS Storage Gateway，則會同步寫入本地緩存。接著會透過最佳化傳輸，非同步寫入 Amazon S3。讀取會先透過本機快取提供。若資料無法使用，便會從 S3 做為直接讀取快取擷取。

寫入和讀取已進行最佳化。只有變更或請求的部分才會透過您的閘道傳輸。刪除 Amazon S3 移除物件。目錄會在 S3 中做為資料夾物件管理，使用與 Amazon S3 主控台中相同的語法。

HTTP 操作 (例如 GET、PUT、UPDATE 及 DELETE) 可修改檔案共享中的檔案。這些操作符合不可部分完成的建立、讀取、更新及刪除 (CRUD) 功能。

存取 AWS Storage Gateway

您可以使用AWS Storage Gateway安慰來執行各種閘道設定與管理任務。本指南的入門一節及其他各種不同的章節都會使用主控台來示範閘道的功能。

此外，您可以使用 AWS Storage Gateway API 來以程式設計方式設定及管理您的閘道。如需 API (匯入 API) 的詳細資訊，請參閱「Storage Gateway 的 API 參考」。

您也可以使用AWS開發套件，開發與 Storage Gateway 互動的應用程式。所以此AWS適用於 Java、.NET、PHP 的開發套件都會包裝基礎 Storage Gateway API，有助於簡化您的程式設計任務。如需下載 SDK 庫的詳細資訊，請參AWS開發者中心。

如需定價的詳細資訊，請參閱 AWS Storage Gateway 定價。

支援的 AWS 區域

- Storage Gateway — 對於受支持AWS區域和AWS可與 Storage Gateway 一起使用的服務終端節點，請參閱AWS Storage Gateway端點和配額中的AWS一般參考。
- Storage Gateway 硬件設備 — 有關可與硬件設備配合使用的受支持區域，請參閱AWS Storage Gateway硬體設備區域中的AWS一般參考。

使用 Storage Gateway 硬體設備

Storage Gateway 硬體設備是預先安裝在經驗證的服務器配置上的 Storage Gateway 軟體設備。您可以從硬體頁面上的AWS Storage Gateway主控台。

硬體設備是高效能的 1U 伺服器，您可以部署在您的資料中心內或現場部署在公司防火牆內。購買並啟用硬體設備時，啟用程序會將硬體設備關聯至AWS帳户。啟用之後，您的硬體設備會出現在主控台中，作為硬體(憑證已建立！) 頁面上的名稱有些許差異。您可以將硬體設備設備設定為檔案閘道、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。

Storage Gateway 硬件設備可以直接從AWS Storage Gateway主控台。

訂購硬件設備

1. 打開 Storage Gateway 主控台，位於https://console.aws.amazon.com/storagegateway/home，然後選擇AWS您希望設備所在的區域。
2. 選擇硬體透過導覽窗格。
3. 選擇訂購設備，然後選擇繼續。您會被重新導向至AWS元素設備和軟件管理控制台請求銷售報價。
4. 填寫必要信息並選擇提交。

信息經過審核後，將生成銷售報價，您可以繼續訂購流程並提交採購訂單，或安排預付款。

查看硬件設備的銷售報價或訂單歷史記錄

1. 打開 Storage Gateway 主控台，位於https://console.aws.amazon.com/storagegateway/home。
2. 選擇硬體透過導覽窗格。
3. 選擇報價和訂單，然後選擇繼續。您會被重新導向至AWS元素設備和軟件管理控制台查看銷售報價和訂單歷史記錄。

在下列章節中，您可以找到如何設定、設定、啟動和使用 Storage Gateway 硬體設備的相關說明。

主題

- 機架安裝您的硬件設備並將其連接到電源
- 設定閘道參數
- 啟用您的硬體設備
- 啟動閘道
- 為閘道設定 IP 地址
- 設定您的閘道
- 從硬件設備中刪除網關
- 刪除您的硬體設備

支援的 AWS 區域

Storage Gateway 硬件設備在美國政府法律允許和允許出口的情況下，可在全球範圍內運輸。如需有關支援的資訊AWS區域，請參閱Storage Gateway 硬體設備區域中的AWS一般參考。

設定您的硬體設備

收到 Storage Gateway 硬體設備之後，您可以使用硬體設備主控台來設定聯網，為AWS並激活您的設備。激活將您的設備與AWS帳户啟用程序。啟用設備之後，您可以從 Storage Gateway 主控台啟動檔案、磁碟區或磁帶閘道。

若要安裝和設定您的硬體設備

1. 將設備掛載到機架上，並插上電源和網路連線。如需詳細資訊，請參閱 機架安裝您的硬件設備並將其連接到電源。
2. 為硬體設備 (主機) 和 Storage Gateway (服務) 設定 Internet 協定第 4 版 (IPv4) 地址。如需詳細資訊，請參閱 設定閘道參數。
3. 激活控制台上的硬件設備硬體頁面上的AWS您選擇的區域。如需詳細資訊，請參閱 啟用您的硬體設備。
4. 在您的硬體設備上安裝 Storage Gateway。如需詳細資訊，請參閱 設定您的閘道。

   您可以使用與在 VMware ESXi、Microsoft Hyper-V、Linux 核心型虛擬機器 (KVM) 或 Amazon EC2 上設定閘道的相同方式來設定的閘道。

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。這可為對AWS。如果您訂購 5 TB 型號，您可以購買 5 個 1.92 TB 固態硬碟 (固態硬碟)，將可用儲存體增加到 12 TB。硬體(憑證已建立！) 頁面上的名稱有些許差異。您可以按照訂購硬件設備並從 Storage Gateway 控制台請求銷售報價相同的訂購流程來訂購額外的 SSD。

然後，您可以將它們加入到硬體設備中，然後再啟用硬體設備。如果您已經啟用硬體設備並想要將設備上的可用儲存體增加到 12 TB，請執行下列動作：

1. 將硬體設備重設為原廠設定。聯絡AWSSupport 如何執行此作業的說明。
2. 將五個 1.92 TB SSD 新增到設備。

網路接口卡選項

根據您訂購的設備型號，它可能附帶 10G-Base-T 銅質網卡或 10G DA/SFP+ 網卡。

- 10G 基礎 T 網卡配置：
  - 對於 1G，使用 10 克或五類電纜
- 10G DA/SFP+ 網卡配置：
  - 使用長達 5 米的雙軸銅直接連接電纜
  - 戴爾/英特爾兼容 SFP+ 光學模塊（SR 或 LR）
  - SFP/SFP+ 銅收發器，適用於 1G 底座 T 或 10G-Base T

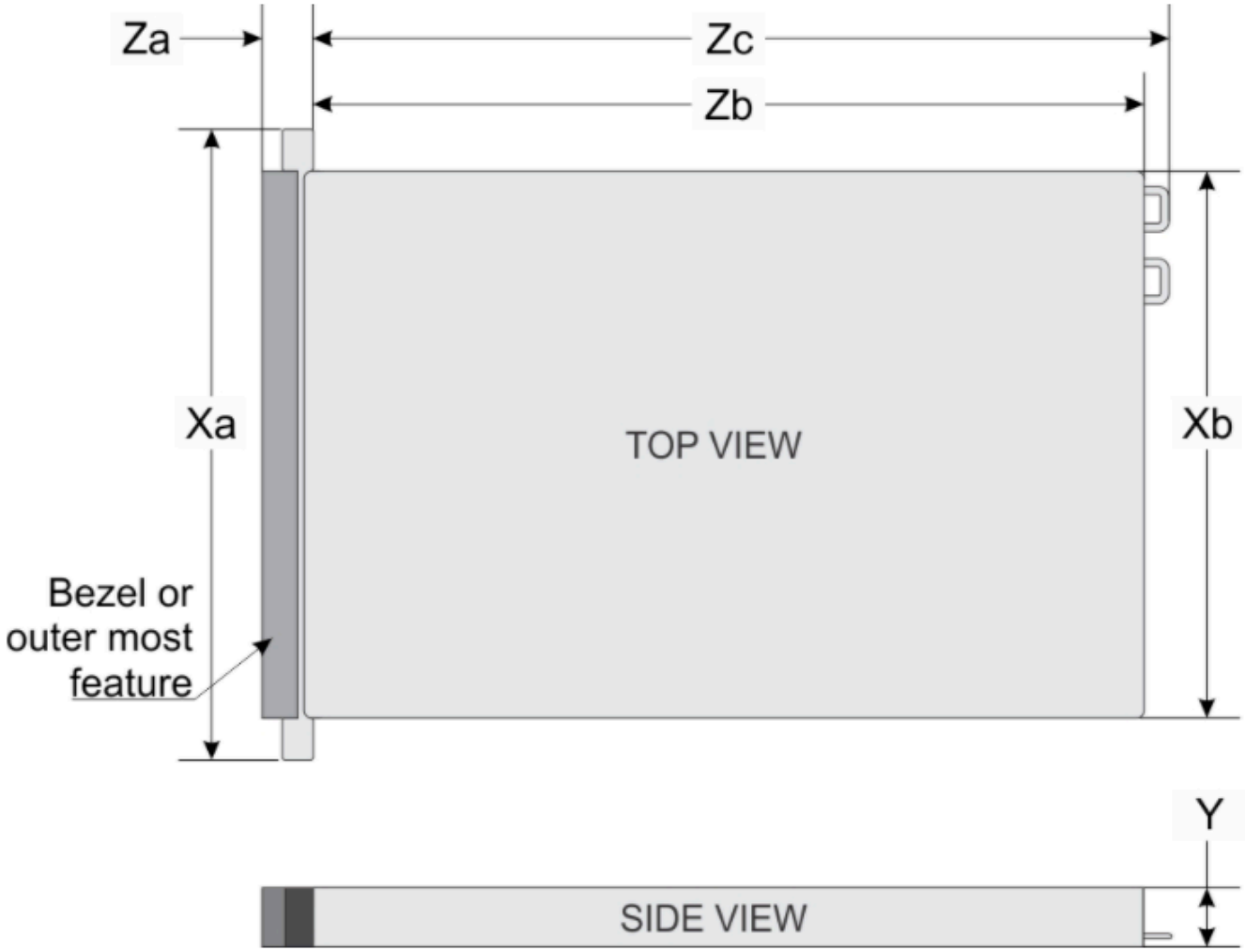
機架安裝您的硬件設備並將其連接到電源

將 Storage Gateway 道硬體設備取消包裝箱後，請按照包裝盒內的說明，將伺服器掛載到機架上。您的設備擁有 1U 機型並符合國際電工委員會 (IEC) 標準規定的 19 吋機架。

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。
- 支持的網絡佈線（取決於硬件裝置中包含的網絡接口卡 (NIC)）。雙軸銅線 DAC、SFP+ 光模塊（英特爾兼容）或 SFP 至基礎 T 銅收發器。
- 鍵盤和顯示器，或鍵盤、視訊和滑鼠 (KVM) 切換解決方案。

硬體設備尺寸



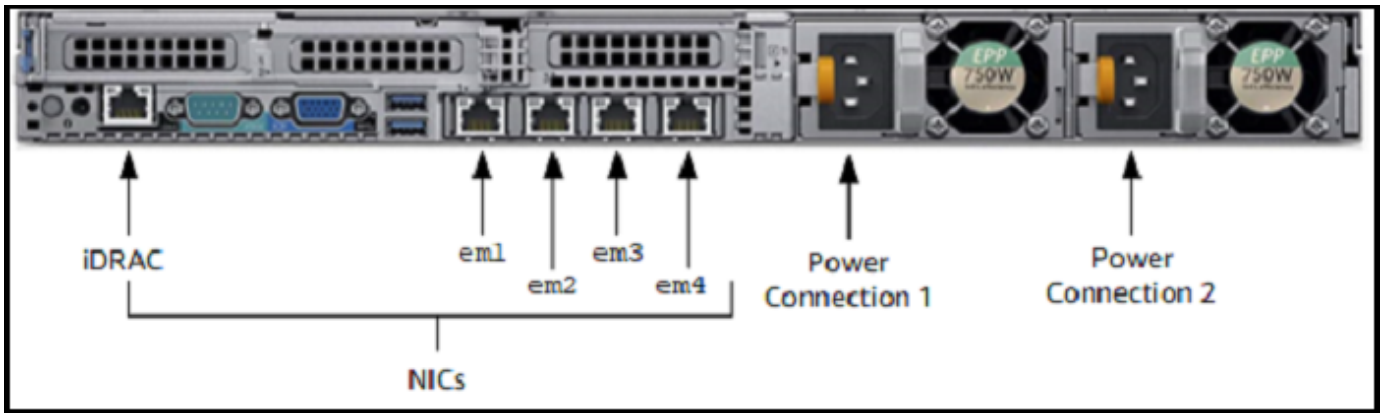
System	Xa	Xb	Y	Za (with bezel)	Za (without bezel)	Zb*	Zc
10 x 2.5-inches	482.0 mm (18.97-inches)	434.0 mm (17.08-inches)	42.8 mm (1.68-inches)	35.84 mm (1.41-inches)	22.0 mm (0.87-inches)	733.82 mm (29.61-inches)	772.67 mm (30.42-inches)

將硬體設備連接至電源

> **Note**
>
> 執行下列程序之前，請確定您符合 Storage Gateway 硬體設備的所有要求，如Storage Gateway 硬體設備的網路與防火牆需求。

1. 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。

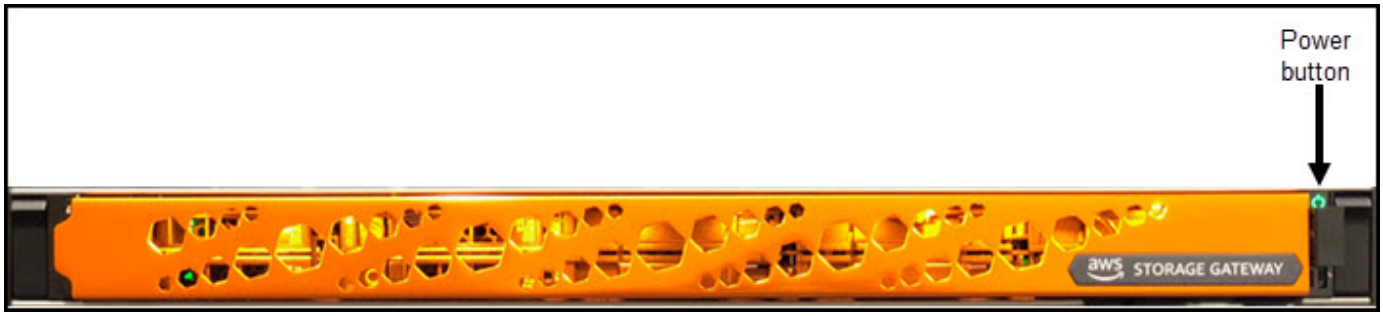
   在下圖中，您會看到具有不同連線的硬體設備。



2. 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。將硬體設備連接至的交換機端口設定為非中繼 VLAN 端口。

3. 插入鍵盤和顯示器。
4. 按前面板的 Power (電源) 按鈕 (如下圖所示)，開啟伺服器電源。

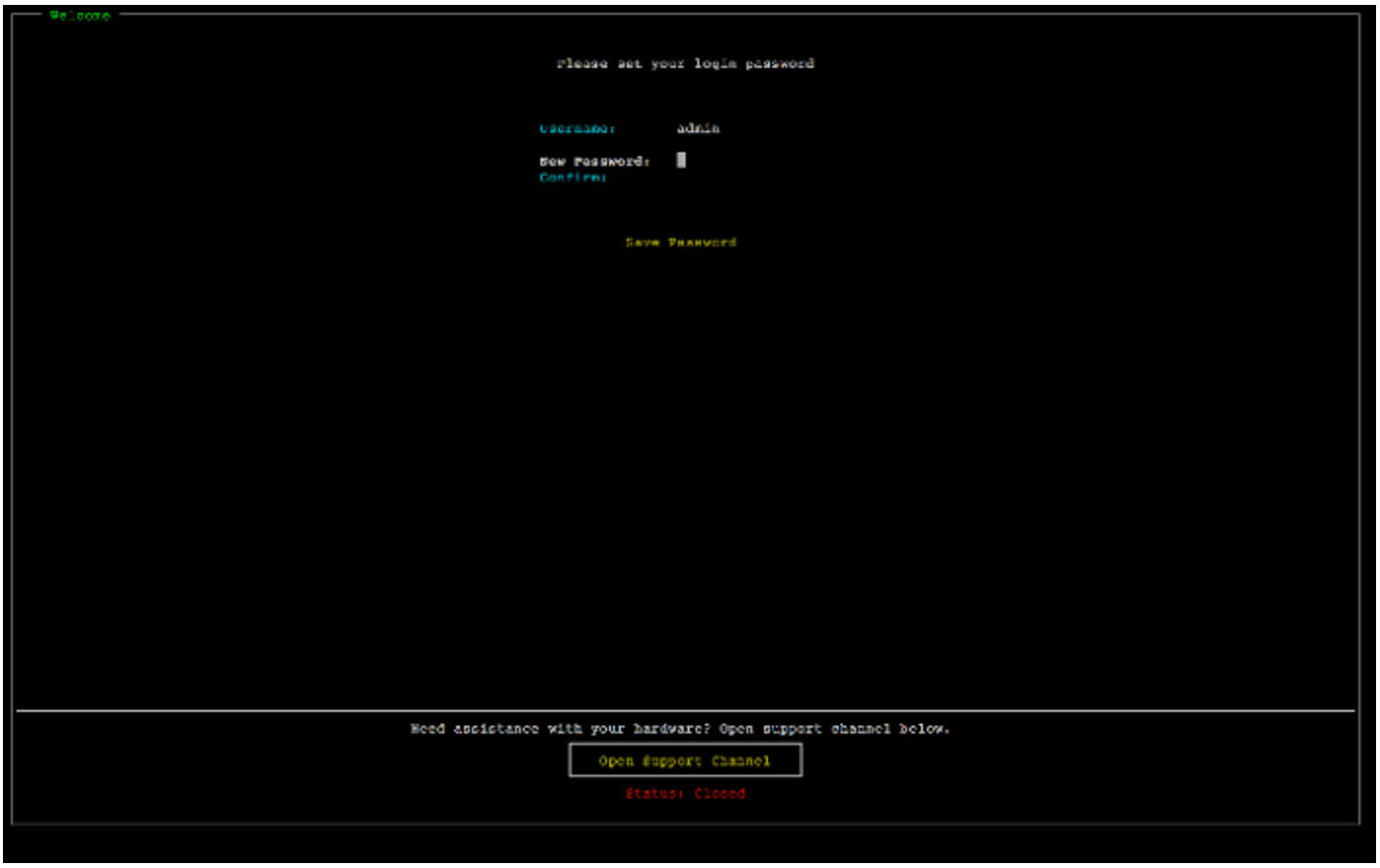


伺服器開機後，硬體主控台會出現在顯示器上。硬體主控台提供專屬於AWS，您可以使用它來設定初始網路參數。您可以設定這些參數，將設備連接至AWS並開啟支援渠道以進行故障排除，通過AWSSupport。

若要使用硬體主控台，請從鍵盤輸入文字並使用 Up、Down、Right 和 Left Arrow 鍵以指定方向在螢幕上移動。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。

若要首次設定密碼

1. 在 Set Password (設定密碼) 中，輸入密碼然後按 Down arrow。
2. 在 Confirm (確認) 中，再次輸入您的密碼，然後選擇 Save Password (儲存密碼)。



此時，您位在硬體主控台中，如下所示。

下一步驟

設定閘道參數

設定閘道參數

伺服器開機後，您可以在硬體主控台中輸入您的第一個密碼，如機架安裝您的硬件設備並將其連接到電源所述。

接著，在硬體主控台執行下列步驟來設定網路參數，讓您的硬體設備可以連接到AWS。

若要設定網路位址

1. 選擇 Configure Network (設定網路) 並按 `Enter` 鍵。會顯示以下所示的 Configure Network (設定網路) 畫面。

2. 對於 IP Address (IP 地址)，從以下其中一個來源輸入有效的 IPv4 地址：

   - 使用動態主機設定通訊協定 (DHCP) 伺服器指派給您實體網路連接埠的 IPv4 地址。

     如果您這樣做，請記下這個 IPv4 地址，以供稍後用於啟用步驟。
   - 指派靜態 IPv4 地址。若要執行此作業，請選擇靜態中的em1部分並按下Enter，查看 Configuration (設定靜態 IP) 畫面，如下所示。

     em1 部分位於連接埠設定群組的左上部分。

   輸入有效的 IPv4 地址後，按 Down arrow 或 Tab。

   > **Note**
   >
   > 如果您設定任何其他接口，則必須提供與AWS要求中列出的端點。

3. 對於 Subnet (子網路)，輸入有效的子網路遮罩，然後按下 Down arrow。
4. 對於 Gateway (閘道)，輸入您網路閘道的 IPv4 地址，然後按下 Down arrow。
5. 對於 DNS1，輸入網域名稱服務 (DNS) 伺服器的 IPv4 地址，然後按下 Down arrow。
6. (選用) 對於 DNS2，輸入第二個 IPv4 地址，然後按下 Down arrow。指派第二個 DNS 伺服器可以在第一個 DNS 伺服器無法運作時，提供額外的備援。
7. 選擇 Save (儲存)，然後按 Enter 以儲存設備的靜態 IPv4 地址設定。

若要登出硬體主控台

1. 選擇 Back (上一頁) 以返回主畫面。
2. 選擇 Logout (登出) 以返回登入畫面。

下一步驟

[啟用您的硬體設備]

啟用您的硬體設備

設定 IP 地址後，您會在主控台 Hardware (硬體) 頁面上輸入此 IP 地址，如下所述。啟用程序會驗證您的硬體設備擁有適當的安全憑證並將設備註冊到AWS帳戶。

您可以選擇在任一個支援的AWS地區。如需支援的清單AWS區域，請參閱Storage Gateway 硬體設備區域中的AWS一般參考。

若要首次啟用設備或在AWS未部署網關的區域

1. 登入AWS Management Console，然後打開 Storage Gateway 控制台，請訪問AWS Storage Gateway管理主控台以及用於激活硬件的帳户憑據。

   如果這是您在AWS區域中，您會看到啟動畫面。在此建立閘道後AWS區域，屏幕將不再顯示。

   > **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連接埠 8080 上對設備的輸入流量 HTTP 存取。

2. 選擇開始使用以查看「創建網關」嚮導，然後選擇硬體設備在選擇主機平台頁面上的詳細資訊，如下所示。
3. 選擇 Next (下一步) 檢視 Connect to hardware (連接到硬體) 畫面，如下所示。
4. 適用於IP 地址中的Connect 至硬體設備部分，輸入設備的 IPv4 地址，然後選擇連線移至 Activate Hardware (啟用硬體) 畫面，如下所示。
5. 為 Hardware name (硬體名稱) 輸入設備的名稱。名稱最多可包含 255 個字元，不可包含斜線字元。
6. 適用於硬體時區下，輸入您的本機設定。

   時區控制何時進行硬體更新，以當地時間上午 2 點做為更新時間。

   > **Note**
   >
   > 我們建議設定設備的時區，因為這會決定一般工作天以外的標準更新時間。

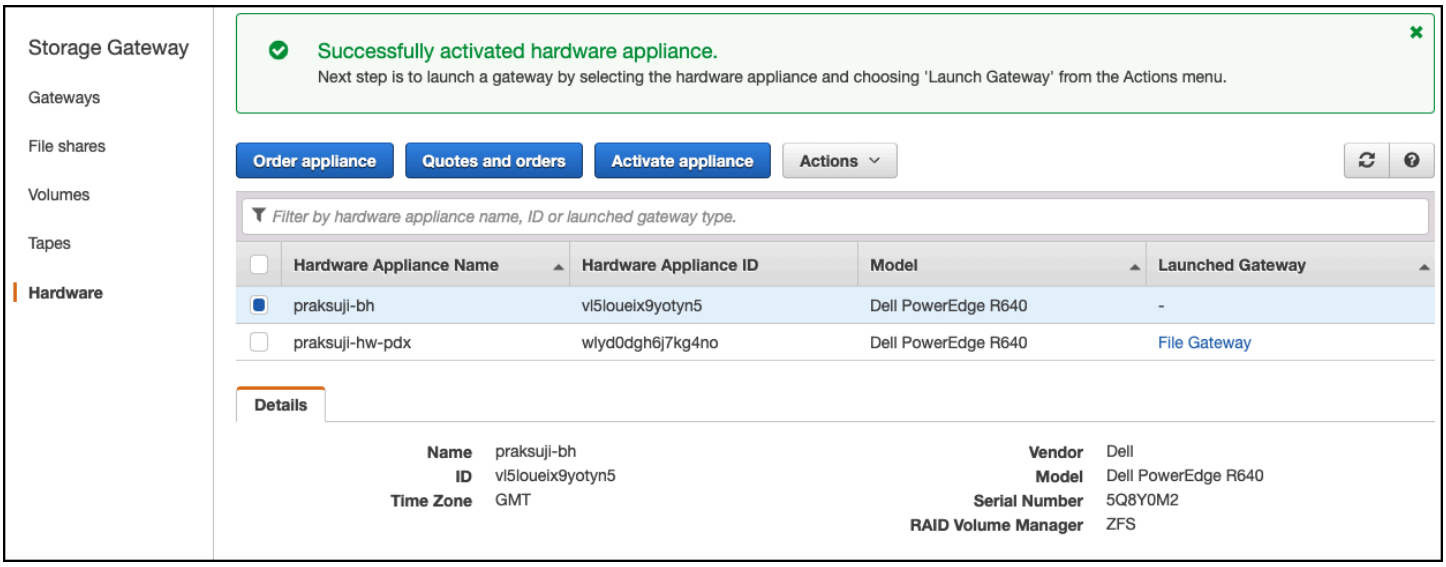
7. (選用) 將 RAID Volume Manager RAID (磁碟區管理工具) 設定為 ZFS。

ZFS 用作硬件設備上的 RAID 卷管理器，以提供更好的性能和數據保護。ZFS 是軟體式開放原始碼檔案系統和邏輯磁碟區管理工具。硬體設備專門針對 ZFS RAID 進行了調整。如需 ZFS RAID 的詳細資訊，請參閱 ZFS Wikipedia 頁面。

8. 選擇 Next (下一步) 完成啟用。

硬體頁面上顯示的主控台橫幅，指出硬體設備已成功啟用，如下所示。

此時，設備已與您的帳戶關聯。下一個步驟是在您的設備上啟動檔案、磁帶或快取磁碟區閘道。



下一步驟

啟動閘道

啟動閘道

您可以在設備上啟動三個儲存閘道的任何一種檔案閘道 — 檔案閘道、磁碟區閘道 (快取) 或磁帶閘道。

若要在硬體設備上啟動閘道

1. 登入AWS Management Console，然後打開 Storage Gateway 控制台，請訪問https://console.aws.amazon.com/storagegateway/home。
2. 選擇 Hardware (硬體)。
3. 對於 Actions (動作)，選擇 Launch Gateway (啟動閘道)。
4. 對於 Gateway Type (閘道類型)，選擇 File Gateway (檔案閘道)、Tape Gateway (磁帶閘道) 或 Volume Gateway (Cached) (磁碟區閘道 (快取))。

5. 為 Gateway name (閘道名稱) 輸入閘道的名稱。名稱可包含 255 個字元，不可包含斜線字元。
6. 選擇 Launch gateway (啟動閘道)。

您所選閘道類型的 Storage Gateway 軟體會安裝在設備上。最多可能需要 5-10 分鐘的時間，閘道才會顯示為線上在主控台中。

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

[為閘道設定 IP 地址]

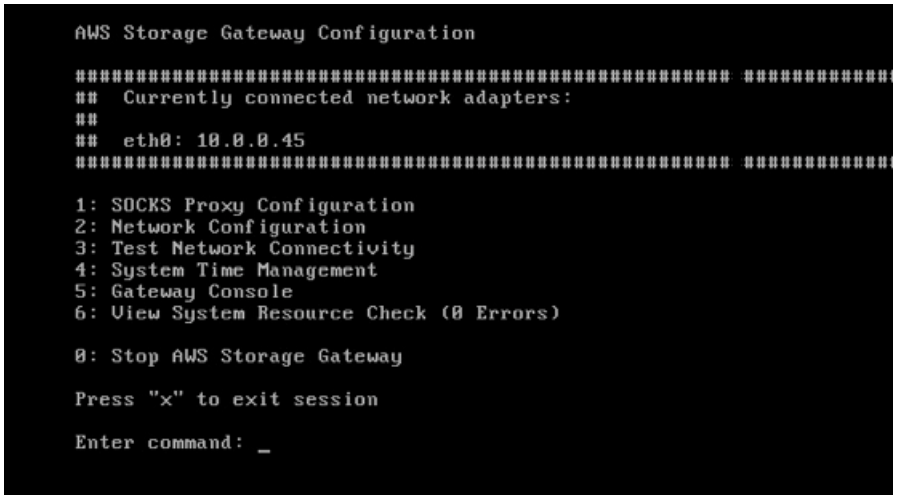
為閘道設定 IP 地址

在激活硬件設備之前，您將 IP 地址分配給其物理網絡接口。現在您已激活設備並在其上啟動了 Storage Gateway，您需要為在硬件設備上運行的 Storage Gateway 虛擬機分配另一個 IP 地址。若要將靜態 IP 地址指派給硬體設備上安裝的閘道，請從本機主控台設定 IP 地址。您的應用程式 (例如 NFS 或 SMB 用戶端、iSCSI 啟動器等等) 會連接到這個 IP 地址。您可以從硬體設備主控台存取閘道本機主控台。

若要在設備上設定 IP 地址以使用應用程式

1. 在硬體主控台上，選擇 Open Service Console (開啟服務主控台) 以開啟閘道本機主控台的登入畫面。
2. 輸入 localhost 登入密碼，然後按 `Enter`。

   預設帳戶是 `admin`，預設密碼是 `password`。
3. 變更預設的密碼。選擇 Actions (動作)，接著 Set Local Password (設定本機密碼)，然後在 Set Local Password (設定本機密碼) 對話方塊中輸入新的登入資料。
4. (選用) 設定 Proxy 設定。如需說明，請參閱 機架安裝您的硬件設備並將其連接到電源。
5. 導覽至閘道本機主控台的 Network Settings (網路設定) 頁面，如下所示。



6. 輸入 2 前往 Network Configuration (網路組態) 頁面，如下所示。

7. 在硬體設備上設定網路連接埠的靜態或 DHCP IP 地址，以顯示檔案、磁碟區和磁帶閘道給應用程式。這個 IP 地址必須位於硬體設備啟用期間所用 IP 地址的同一個子網路上。

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。

下一步驟

[設定您的閘道]

設定您的閘道

啟用並設定硬體設備後，您的設備會顯示在主控台中。現在您可以建立您想要的閘道類型。繼續安裝您的閘道類型。如需指示，請參閱 配置您的 Amazon S3 文件網關。

從硬件設備中刪除網關

若要從硬體設備移除閘道軟體，請使用下列步驟。執行此操作後，閘道軟體會從您的硬體設備解除安裝。

若要從硬體設備移除閘道

1. 選擇閘道的核取方塊。
2. 對於 Actions (動作)，選擇 Remove Gateway (移除閘道)。
3. 在 Remove gateway from hardware appliance (從硬體設備移除閘道) 對話方塊中，選擇 Confirm (確認)。

> **Note**
>
> 刪除閘道後，您無法復原此動作。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，請參閱使用 AWS Storage Gateway 主控台刪除閘道以及移除相關聯資源。

刪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。

刪除您的硬體設備

激活您的硬件設備之後AWS帳號，您可能需要移動並在不同的AWS帳户。在這種情況下，您會從AWS帳户並在另一個AWS帳户。您可能還需要從AWS帳號，因為您不再需要它。按照這些說明來刪除您的硬體設備。

刪除硬件設備

1. 如果您已在硬體設備上安裝閘道，您必須先移除該閘道，之後才能刪除設備。如需如何從您的硬體設備移除閘道的詳細資訊，請參閱從硬件設備中刪除網關。
2. 在 Hardware (硬體) 頁面上，選擇您想刪除的硬體設備。

3. 在 Actions (動作) 中選擇 Delete Appliance (刪除設備)。
4. 在 Confirm deletion of resource(s) (確認刪除資源) 對話方塊中，選擇確認核取方塊，然後選擇 Delete (刪除)。指出成功刪除的訊息隨即顯示。

   刪除硬體設備時，也會刪除設備上安裝的所有閘道資源，但不會刪除硬體設備本身上的資料。

AWS Storage Gateway 入門

在本節中，您可以找到如何建立和啟用檔案閘道的說明，請參見AWS Storage Gateway。開始之前，請確定您的設定符合所需的先決條件和設定 Amazon S3 檔案閘道。

主題

- 建立和激活 Amazon S3 檔案閘道

建立和激活 Amazon S3 檔案閘道

在本節中，您可以找到如何在AWS Storage Gateway。

主題

- 設定 Amazon S3 檔案閘道
- 將您的 Amazon S3 文件網關 Connect 到AWS
- 查看設置並激活您的 Amazon S3 文件網關
- 配置您的 Amazon S3 文件網關

設定 Amazon S3 檔案閘道

若要設定新的 S3 檔案閘道

1. 開啟AWS Management Console在https://console.aws.amazon.com/storagegateway/home/，然後選擇AWS 區域，您要建立閘道的位置。
2. 選擇建立閘道開啟設定閘道(憑證已建立！) 頁面上的名稱有些許差異。
3. 在 中網關設置部分中執行下列動作：

    a. 為 Gateway name (閘道名稱) 輸入閘道的名稱。創建網關後，您可以搜索此名稱，以便在AWS Storage Gateway主控台。

    b. 適用於閘道時區中，為要在其中部署網關的世界部分選擇本地時區。
4. 在 中閘道選項部分，閘道類型，選擇Amazon S3 檔案閘道。
5. 在 中平台選項部分中執行下列動作：

    a. 適用於主機平台中，選擇您想要部署閘道的平台。然後按照 Storage Gateway 控制台頁面上顯示的特定於平台的說明設置您的主機平台。您可以從下列選項來選擇：

- VMware ESXi— 使用 VMware ESXi 下載、部署和配置網關虛擬機。
- Microsoft Hyper-V— 使用微軟 Hyper-V 下載、部署和配置網關虛擬機。
- Linux KVM— 使用 Linux 核心型虛擬機器 (KVM) 下載、部署和配置閘道虛擬機。
- Amazon EC2— 配定和啟動 Amazon EC2 執行個體來託管閘道。
- 硬體設備— 訂購專用的物理硬件設備，請從AWS託管您的閘道。

b. 適用於確認設置網關中，選取此複選方塊以確認您已為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. 現在您的閘道已建立，您必須選擇您希望它如何連線並與之通信AWS。選擇下一頁繼續執行「」。

將您的 Amazon S3 文件網關 Connect 到AWS

要將新的 S3 文件網關連接到AWS

1. 若尚未執行此作業，請完成設定 Amazon S3 檔案閘道。完成時，請選擇下一頁開啟連線到AWS的名稱有些許不同AWS Storage Gateway主控台。
2. 在 中端點選項部分，服務端點中，選擇您閘道將用於與之通信的端點類型AWS。您可以從下列選項來選擇：

   - 可公開存取— 您的網關與AWS在公有網際網路連線。若您選取此選項，請使用FIPS 啟用端點複選方塊，以指定連線是否必須遵守聯邦資訊處理標準 (FIPS)。

     > **Note**
     >
     > 如果您在存取時，需要 FIPS 140-2 驗證的加密模組AWS，請使用 FIPS 標準的端點。如需詳細資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2。
     > FIPS 服務端點只在部分AWS地區。如需詳細資訊，請參閱「」AWS Storage Gateway 端點和配額中的AWS一般參考。

   - 託管 VPC— 您的網關與AWS與您的 Virtual Private Cloud (VPC) 建立私有連線，允許您控制您的閘道設定。如果選擇此選項，則必須通過從下拉列表中選擇其 VPC 終端節點 ID 來指定現有 VPC 終端節點。您還可以提供其 VPC 端點域名稱系統 (DNS) 名稱或 IP 地址。

3. 在 中閘道連線選項部分，連線選項中，選擇如何識別您的網關AWS。您可以從下列選項來選擇：

- IP 地址— 在相應的字段中提供閘道的 IP 地址。此 IP 地址必須是公開的，或者可從當前網絡中訪問，並且您必須能夠從 Web 瀏覽器連接到該 IP 地址。

  您可以通過從虛擬機管理程序客户端登錄網關的本地控制台或從 Amazon EC2 實例詳細信息頁面複製該網關 IP 地址來獲取網關 IP 地址。

- 啟用金鑰— 在相應的字段中為您閘道提供啟用金鑰。您可以使用閘道的本機主控台來生成激活密鑰。如果網關的 IP 地址不可用，請選擇此選項。

4. 現在，您已經選擇了您希望網關連接到AWS，則必須激活網關。選擇下一頁繼續執行「」。

查看設置並激活您的 Amazon S3 文件網關

激活新的 S3 文件網關

1. 若尚未執行此作業，請完成下列主題中介紹的程序：

   - 設定 Amazon S3 檔案閘道
   - 將您的 Amazon S3 文件網關 Connect 到AWS

   完成時，請選擇下一頁開啟檢和啟用的名稱有些許不同AWS Storage Gateway主控台。

2. 查看頁面上每個部分的初始網關詳細信息。
3. 如果某個部分包含錯誤，請選擇Edit (編輯)返回到相應的設置頁面並進行更改。

   > **Important**
   >
   > 激活網關後，您無法修改網關選項或連接設置。

4. 現在您已激活網關，您必須首次執行配置以分配本地存儲磁盤和配置日誌記錄。選擇下一頁繼續執行「」。

配置您的 Amazon S3 文件網關

在新 S3 文件網關上執行首次配置

1. 若尚未執行此作業，請完成下列主題中介紹的程序：

   - 設定 Amazon S3 檔案閘道

- 將您的 Amazon S3 文件網關 Connect 到AWS
- 查看設置並激活您的 Amazon S3 文件網關

完成時，請選擇下一頁開啟設定閘道的名稱有些許不同AWS Storage Gateway主控台。

2. 在 中設定快取儲存部分中，使用下拉列表至少分配一個容量至少為 150 千兆字節 (GiB) 的本地磁盤以快取。本節中列出的本地磁盤與您在主機平台上預配置的物理存儲相對應。
3. 在 中CloudWatch 日誌部分中，選擇如何設置 Amazon CloudWatch Logs 以監控網關的運行狀況。您可以從下列選項來選擇：

   - 建立新日誌— 設定新的日誌組來監視閘道。
   - 使用現有的日誌羣組— 從相應的下拉列表中選擇現有日誌組。
   - 停用日誌記錄— 請勿使用 Amazon CloudWatch Logs 來監控您的網關。
4. 在 中CloudWatch 警示部分中，選擇如何設置 Amazon CloudWatch 警報，以便在網關的指標偏離定義的限制時通知您。您可以從下列選項來選擇：

   - 停用警示— 不要使用 CloudWatch 警報來接收有關網關指標的通知。
   - 建立 CloudWatch 警示— 配置新的 CloudWatch 警報以接收有關網關指標的通知。選擇建立警示在 Amazon CloudWatch 主控台中定義指標並指定警報動作。如需說明，請參閱「」使用 Amazon CloudWatch 警示中的Amazon CloudWatch 使用者指南。
5. （可選）在標籤部分中，選擇添加新標記，然後輸入區分大小寫的索引鍵值組，以協助您在AWS Storage Gateway主控台。重複此步驟來新增任意數量的標籤。
6. （可選）在驗證 VMware High Avile 組態部分，如果您的閘道部署於 VMware 主機上，作為已啟用 VMware High Avalvate (HA) 的羣集的一部分，請選擇檢 VMware HA以測試 HA 配置是否正常工作。

   > **Note**
   >
   > 此部分僅針對在 VMware 主機平台上運行的網關顯示。
   > 完成網關配置過程不需要執行此步驟。您可以隨時測試閘道的 HA 組態。驗證需要幾分鐘時間，然後重新啟動 Storage Gateway 虛擬機 (VM)。

7. 選擇設定來完成閘道的建立程序。

若要檢查新閘道的狀態，請在閘道的所有位置頁面AWS Storage Gateway主控台。

現在您已經建立閘道，您必須建立檔案共享以供其使用。如需說明，請參閱「」建立檔案共享。

建立檔案共享

在本節中，您可以找到如何建立檔案共享的說明。您可以建立可透過網路檔案系統 (NFS) 或伺服器訊息區塊 (SMB) 通訊協定存取的檔案共享。

> **Note**
>
> 當文件由 NFS 或 SMB 客户端寫入文件網關時，文件網關會將文件的數據上傳到 Amazon S3，後跟其元數據（所有權、時間戳等）。上傳文件數據會創建一個 S3 對象，上傳文件的元數據會更新 S3 對象的元數據。此過程將創建對象的另一個版本，從而產生兩個版本的對象。如果啟用了 S3 版本控制，則存放兩個版本。
>
> 如果更改存儲在文件網關中的文件的元數據，則會創建一個新的 S3 對象並替換現有 S3 對象。此行為不同於在文件系統中編輯文件，在文件系統中編輯文件不會導致創建新文件。測試您計劃使用的所有文件操作AWSStorage Gateway，以便您瞭解每個文件操作如何與 Amazon S3 存儲交互。
>
> 當您從文件網關上傳數據時，請仔細考慮在 Amazon S3 中使用 S3 版本控制和跨區域複製 (CRR)。如果啟用 S3 版本控制，將文件從您的文件網關上傳到 Amazon S3，則至少會產生兩個版本的 S3 對象。
>
> 某些涉及大型文件和文件寫入模式的工作流（如文件上傳），通過多個步驟執行，可能會增加存儲 S3 對象版本的數量。如果文件網關緩存因文件寫入速率高而需要釋放空間，則可能會創建多個 S3 對象版本。如果啟用了 S3 版本控制，這些方案會增加 S3 存儲，並增加與 CRR 相關的傳輸成本。測試您計劃與 Storage Gateway 一起使用的所有文件操作，以便瞭解每個文件操作如何與 Amazon S3 存儲交互。
>
> 將 Rsync 實用程序與您的文件網關結合使用可以在緩存中創建臨時文件，並在 Amazon S3 中創建臨時 S3 對象。此情況會在 S3 標準 — 不常存取 (S3 標準 — IA) 和 S3 智慧型分層儲存類別中產生早期刪除費用。

當您建立 NFS 共享時，根據預設，任何可以存取 NFS 伺服器的人員皆能存取 NFS 檔案共享。您可以透過 IP 地址限制存取用戶端。

針對 SMB，您可以使用三種不同身份驗證模式中的其中一種：

- 具備 Microsoft Active Directory (AD) 存取的檔案共享。任何通過身份驗證的 Microsoft AD 使用者都能存取此檔案共享類型。
- 具備有限存取的 SMB 檔案共享。只有您指定的特定網域使用者和羣組可以存取 (透過允許列表)。也可以拒絕使用者和羣組的存取 (通過拒絕清單)。

- 具備訪客存取的 SMB 檔案共享。任何能夠提供訪客密碼的使用者都能存取此檔案共享。

> **Note**
>
> 針對 NFS 檔案共享而透過閘道匯出的檔案共享，都支援 POSIX 許可。對於 SMB 檔案共享，您可以使用存取控制清單 (ACL) 來管理檔案共享中檔案和資料夾的許可。如需詳細資訊，請參閱 使用 Microsoft Windows ACL 來控制 SMB 檔案共享的存取。

檔案閘道可主控一或多個不同類型的檔案共享。您可以在檔案閘道上擁有多個 NFS 和 SMB 檔案共享。

> **Important**
>
> 若要建立檔案共享，檔案閘道需要您啟用AWS Security Token Service(AWS STS。確定AWS STS被激活在AWS 區域，您正在創建文件網關。如果AWS STS未激活AWS 區域，將其激活。如需如何激活AWS STS，請參啟用和停用AWS STS在AWS 區域中的AWS Identity and Access Management使用者指南。

> **Note**
>
> 您可以使用AWS Key Management Service(AWS KMS)，加密您的檔案閘道儲存在 Amazon S3 中的物件。若要使用 Storage Gateway 主控台執行此操作，請參建立 NFS 檔案共享或者建立 SMB 檔案共享。您也可以使用 Storage Gateway API 來執行此操作。如需說明，請參閱「」CreateNFSFileShare或者CreateSMBFileShare中的AWSStorage Gateway API 參考。
> 根據預設，將資料寫入 S3 儲存貯體時，檔案閘道會使用 Amazon S3 (SSE-S3) 管理的伺服器端加密。如果您建立 SSE-KMS (使用AWS KMS— 管金鑰) 您 S3 儲存貯體的預設加密，檔案閘道存放的物件就會使用 SSE-KMS 加密。
> 若要使用 SSE-KMS 以您自己的 AWS KMS 金鑰加密，您即必須啟用 SSE-KMS 加密。當您執行此作業時，請在建立您的檔案共享時提供 KMS 金鑰的 Amazon Resource Name (ARN)。您也可以使用 UpdateNFSFileShare 或 UpdateSMBFileShare API 操作，為您的檔案共享更新 KMS 設定。此更新適用於更新後存放在 Amazon S3 儲存貯體中的物件。
> 如果將文件網關配置為使用 SSE-KMS 進行加密，則必須手動添加`kms:Encrypt`、`kms:Decrypt`、`kms:ReEncrypt`、`kms:GenerateDataKey`，和`kms:DescribeKey`權限設定為與檔案共享相關聯的 IAM 角色。如需詳細資訊，請參閱「」使用 Storage Gateway 的身分類型政策 (IAM 政策)。

主題

建立 NFS 檔案共享

使用下列程序建立網路檔案系統 (NFS) 檔案共享。

> **Note**
>
> NFS 客户端將文件寫入文件網關時，文件網關會將文件的數據上傳到 Amazon S3，然後是其元數據（所有權、時間戳等）。上傳文件數據會創建一個 S3 對象，上傳文件的元數據會更新 S3 對象的元數據。此過程將創建對象的另一個版本，從而產生兩個版本的對象。如果啟用了 S3 版本控制，則存放兩個版本。
>
> 如果更改存儲在文件網關中的文件的元數據，則會創建一個新的 S3 對象並替換現有 S3 對象。此行為不同於在文件系統中編輯文件，在文件系統中編輯文件不會導致創建新文件。測試您計劃使用的所有文件操作AWSStorage Gateway，以便您瞭解每個文件操作如何與 Amazon S3 存儲交互。
>
> 當您從文件網關上傳數據時，請仔細考慮在 Amazon S3 中使用 S3 版本控制和跨區域複製 (CRR)。如果啟用 S3 版本控制，將文件從您的文件網關上傳到 Amazon S3，則至少會產生兩個版本的 S3 對象。
>
> 某些涉及大型文件和文件寫入模式的工作流（如文件上傳），通過多個步驟執行，可能會增加存儲 S3 對象版本的數量。如果文件網關緩存因文件寫入速率高而需要釋放空間，則可能會創建多個 S3 對象版本。如果啟用了 S3 版本控制，這些方案會增加 S3 存儲，並增加與 CRR 相關的傳輸成本。測試您計劃與 Storage Gateway 一起使用的所有文件操作，以便瞭解每個文件操作如何與 Amazon S3 存儲交互。
>
> 將 Rsync 實用程序與您的文件網關結合使用可以在緩存中創建臨時文件，並在 Amazon S3 中創建臨時 S3 對象。此情況會在 S3 標準 — 不常存取 (S3 標準 — IA) 和 S3 智慧型分層儲存類別中產生早期刪除費用。

建立 NFS 檔案共享

1. 開啟AWSStorage Gateway 於https://console.aws.amazon.com/storagegateway/home/。
2. 選擇建立檔案共享開啟檔案共享設定(憑證已建立！) 頁面上的名稱有些許差異。
3. 適用於門戶，請從清單中選擇 Amazon S3 檔案閘道。

4. 適用於Amazon S3 位置，執行下列其中一項動作：

   - 若要將檔案共享直接連接至 S3 儲存貯體，請選擇S3 儲存儲體名稱，然後輸入 S3 存儲桶名稱和文件共享創建的對象的前綴名稱（可選）。您的網關使用此存儲桶來存儲和檢索文件。如需有關建立新儲存貯體的詳細資訊，請參如何建立 S3 儲存貯體？中的Amazon S3 使用者指南。
   - 若要將檔案共享連接至 S3 儲存貯體透過存取點，請選擇S3 存取點，然後輸入 S3 接入點名稱和文件共享創建的對象的前綴名稱（可選）。您的存儲桶策略必須配置為將訪問控制委派給接入點。如需存取點的詳細資訊，請參使用 Amazon S3 存取點管理資料存取和將存取控制委派給存取點中的Amazon S3 使用者指南。
   - 要通過接入點別名將文件共享連接到 S3 存儲桶，請選擇S3 存取點別名，然後輸入 S3 接入點別名和文件共享創建的對象的前綴名稱（可選）。如果選擇此選項，則文件網關無法創建新的 AWS Identity and Access Management(IAM) 角色並代您存取政策。您必須選擇現有 IAM 角色並在存取 S3 儲存貯體部分。如需存取點別名的詳細資訊，請參為您的存取點使用儲存貯體型別名中的Amazon S3 使用者指南。

   > **Note**
   >
   > - 如果輸入前綴名稱，或選擇通過接入點或接入點別名進行連接，則必須輸入文件共享名稱。
   > - 字首名稱必須以正斜線 (/。
   > - 建立檔案共享後，無法修改或刪除。
   > - 如需使用前綴名稱的詳細資訊，請參使用字首整理物件中的Amazon S3 使用者指南。

5. 適用於AWS 區域中，選擇AWS 區域S3 儲存儲體。
6. 適用於檔案共享名稱中，輸入檔案共享的名稱。默認名稱為 S3 儲存貯體名稱或存取點名稱。

   > **Note**
   >
   > - 如果輸入了前綴名稱，或選擇通過接入點或接入點別名進行連接，則必須輸入文件共享名稱。
   > - 創建文件共享後，無法刪除文件共享名稱。

7. （可選）對於AWS PrivateLinkS3，執行下列操作：

1. 若要將檔案共享配定為透過在虛擬私有雲端 (VPC) 內的接口端點連接至 S3，由AWS PrivateLink，選擇使用 VPC 端點。
2. 要標識您希望文件共享連接的 VPC 接口終端節點，請選擇VPC 端點 ID或者VPC 端點 DNS 名稱，然後在相應字段中提供所需信息。

> **Note**
>
> - 如果文件共享通過 VPC 接入點或通過與 VPC 接入點關聯的別名連接到 S3，則需要執行此步驟。
> - 使用檔案共享用AWS PrivateLink在 FIPS 網關上不受支持。
> - 如需AWS PrivateLink，請參AWS PrivateLink適用於 Amazon S3中的Amazon S3 使用者指南。

8. 針對 Access objects using (使用下列方式存取物件)，請選擇 Network File System (NFS) (網路檔案系統 (NFS))。
9. 針對 Audit logs (稽核日誌)，選擇下列其中一項：
   - 若要關閉日誌，選擇Disable logging (停用日誌記錄)。
   - 若要建立新的審核日誌，選擇建立新的日誌。
   - 要使用現有審核日誌，請選擇使用現有的日誌，然後從清單中選擇審核日誌。

   如需稽核的詳細資訊，請參閱瞭解文件網關審核日誌。
10. 適用於從 S3 自動刷新緩存，選擇設定刷新間隔，並設置使用生存時間 (TTL) 刷新文件共享緩存的時間（天、小時和分鐘）。TTL 是自上次刷新以來的時間長度。TTL 間隔過後，訪問目錄會導致文件網關首先從 Amazon S3 存儲桶刷新該目錄的內容。
11. 適用於檔案上傳通知，選擇建立時間 (秒)以便在文件網關完全上傳到 S3 時收到通知。將建立時間以秒為單位控制在客户端寫入文件的最後一個時間點之後等待的秒數，然後再生成`ObjectUploaded`通知。由於客户端可以對文件進行許多小寫入，因此最好儘可能長地設置此參數，以避免在較短的時間內為同一文件生成多個通知。如需詳細資訊，請參閱 獲取文件上傳通知。

> **Note**
>
> 此設置對象上傳到 S3 的時間沒有影響，僅影響通知的時間。

12. (選用) 在 Add tags (新增標籤) 區段中，輸入金鑰和值，以將標籤新增至您的檔案共享。標籤為區分大小寫的索引鍵值組，可協助您管理、篩選和搜尋檔案共享。
13. 選擇 Next (下一步)。所以此配置 Amazon S3 中存放檔案的方式頁面隨即出現。
14. 適用於新對象的存儲類下，請選擇在 Amazon S3 儲存貯體中建立的新物件要使用的儲存體類別：

    - 若要透過備援方式在多個不同地理位置可用區域存放經常存取的物件資料，請選擇S3 標準。如需 S3 標準儲存類別的詳細資訊，請參經常存取物件的儲存體方案中的Amazon Storage Service 使用者指南。
    - 若要自動將資料移至最經濟實惠的儲存存取層，以最佳化儲存成本，請選擇S3 Intelligent-Tiering。如需 S3 智慧型分層儲存類別的詳細資訊，請參自動最佳化經常存取物件與不常存取物件的儲存體方案中的Amazon Storage Service 使用者指南。
    - 若要透過備援方式在多個不同地理位置可用區域存放不常存取的物件資料，請選擇S3 標準 – IA。如需 S3 標準 IA 儲存類別的詳細資訊，請參不常存取物件的儲存體方案中的Amazon Storage Service 使用者指南。
    - 若要將不常存取的物件資料存放在單一可用區域中，請選擇S3 單區域 – IA。如需 S3 單區域 — IA 儲存類別的詳細資訊，請參不常存取物件的儲存體方案中的Amazon Storage Service 使用者指南。

    要幫助監控 S3 賬單，請使用AWS Trusted Advisor。如需詳細資訊，請參閱「」監控工具中的Amazon Storage Service 使用者指南。
15. 針對 Object metadata (物件中繼資料)，選擇您要使用的中繼資料：

    - 若要啟用以副檔名為基礎的上傳物件使用 MIME 類型的猜想，請選擇猜測 MIME 類型。
    - 若要將完整控制權授予映射至 NFS 檔案共享的 S3 儲存貯體擁有者，請選擇讓存儲桶擁有者完全控制。如需使用檔案共享存取另一個賬户擁有儲存貯體中之物件的詳細資訊，請參使用檔案共享進行跨賬户存取。
    - 如果您在儲存貯體上使用此檔案共享，而儲存貯體需要申請者或讀者付費，而不是儲存貯體擁有者付費，請選擇啟用請求者付款。如需詳細資訊，請參閱請求者付款儲存貯體。
16. 適用於存取 S3 儲存貯體中，選擇AWS Identity and Access Management(IAM) 角色，您希望檔案閘道用來存取您的 Amazon S3 儲存貯體：

- 若要啟用檔案閘道代您建立新的 IAM 角色並代您存取政策，請選擇創建新的 IAM 角色。如果文件共享使用接入點別名連接到 Amazon S3，則此選項不可用。
- 要選擇現有 IAM 角色並手動設置訪問策略，請選擇使用現有 IAM 角色。如果您的文件共享使用接入點別名連接到 Amazon S3，則必須使用此選項。在 中IAM 角色框中，輸入用於存取您儲存貯體的角色的 Amazon Resource Name (ARN)。如需 IAM 角色的資訊，請參。IAM 角色中的AWS Identity and Access Management使用者指南。

如需存取 S3 儲存貯體的詳細資訊，請參閱授予對 Amazon S3 儲存貯體的存取權。

17. 適用於Encryption (加密)下，請選擇您的檔案閘道存放在 Amazon S3 中的物件加密所用的加密金鑰類型：

    - 若要使用 Amazon S3 (SSE-S3) 管理的伺服器端加密，請選擇S3 受管金鑰 (SSE-S3)。
    - 若要使用伺服器端加密AWS Key Management Service(SSE-KMS)，選擇KMS 管理金鑰 (SSE-KMS)。在 中Primary key (主索引鍵)框中，選擇現有的AWS KMS key或選擇建立新的 KMS 金鑰在AWS Key Management Service(AWS KMS) 主控台。如需有關 的詳細資訊AWS KMS，請參什麼是AWS Key Management Service?中的AWS Key Management Service開發人員指南。

    > **Note**
    >
    > 指定AWS KMS鍵與未列出的別名一起使用AWS KMS鍵來自不同的AWS 帳戶，您必須使用AWS Command Line Interface(AWS CLI。如需詳細資訊，請參閱「」CreateNFSFileShare中的AWSStorage Gateway API 參考。
    > 不支持非對稱 KMS 密鑰。

18. 選擇下一頁配置文件訪問設置。

配置檔案存取設置

1. 適用於允許的用戶端下，指定是允許還是限制每個用户端存取您的檔案共享的存取權。為您要允許的用户端提供 IP 地址或 CIDR 標記法。如需支援 NFS 用戶端的相關資訊，請參閱檔案閘道支援的 NFS 用戶端。
2. 適用於掛載選項中，指定您想要用於壁球等級和匯出為。

   使用 Squash 層級時，選擇下面其中一個選項：

   - 全部壁球：所有使用者存取權都會映射至使用者 ID (UID) (65534) 和 GID (GID) (65534)。

- 無根壁球：遠端超級使用者 (root) 會接收 root 的存取權。
- 根壁球（默認值）：遠端超級使用者 (root) 的存取權會映射至 UID (65534) 和 GID (65534)。

使用 Export as (匯出為) 時，選擇下面其中一個選項：

- 讀取/寫入
- 唯讀

> **Note**
>
> 對於掛載在 Microsoft Windows 客户端上的文件共享，如果選擇唯讀，則可能會看到內容關於您無法建立資料夾之意外錯誤的訊息。您可以略過此訊息。

3. 使用 File metadata defaults (檔案中繼資料預設值) 時，您可以編輯 Directory permissions (目錄許可)、File permissions (檔案許可)、User ID (使用者 ID) 和 Group ID (群組 ID)。如需詳細資訊，請參閱 編輯 NFS 檔案共享的元數據默認值。
4. 選擇 Next (下一步)。
5. 檢您的檔案共享組態設定，然後選擇完成。

   在您的 NFS 檔案共享建立之後，您可以在檔案共享的 Details (詳細資訊) 標籤中看到您的檔案共享設定。

後續步驟

在用户端掛載您的 NFS 檔案共享

建立 SMB 檔案共享

建立伺服器訊息塊 (SMB) 檔案共享之前，請確定已設定檔案閘道的 SMB 安全設定。您還必須配置 Microsoft Active Directory (AD) 或訪客存取來進行身分驗證。檔案共享只提供一個類型的 SMB 存取。如需說明，請參閱「」編輯網關的 SMB 設置。

> **Note**
>
> 除非您的安全組中已打開所需的端口，否則 SMB 檔案共享將無法正常運作。如需詳細資訊，請參閱 連接埠需求。

> **Note**
>
> SMB 客户端將文件寫入文件網關時，文件網關會將文件的數據上傳到 Amazon S3，然後是其元數據（所有權、時間戳等）。上傳文件數據會創建一個 S3 對象，上傳文件的元數據會更新 S3 對象的元數據。此過程將創建對象的另一個版本，從而產生兩個版本的對象。如果啟用了 S3 版本控制，則存放兩個版本。
>
> 如果更改存儲在文件網關中的文件的元數據，則會創建一個新的 S3 對象並替換現有 S3 對象。此行為不同於在文件系統中編輯文件，在文件系統中編輯文件不會導致創建新文件。測試您計劃使用的所有文件操作AWSStorage Gateway，以便您瞭解每個文件操作如何與 Amazon S3 存儲交互。
>
> 當您從文件網關上傳數據時，請仔細考慮在 Amazon S3 中使用 S3 版本控制和跨區域複製 (CRR)。如果啟用 S3 版本控制，將文件從您的文件網關上傳到 Amazon S3，則至少會產生兩個版本的 S3 對象。
>
> 某些涉及大型文件和文件寫入模式的工作流（如文件上傳），通過多個步驟執行，可能會增加存儲 S3 對象版本的數量。如果文件網關緩存因文件寫入速率高而需要釋放空間，則可能會創建多個 S3 對象版本。如果啟用了 S3 版本控制，這些方案會增加 S3 存儲，並增加與 CRR 相關的傳輸成本。測試您計劃與 Storage Gateway 一起使用的所有文件操作，以便瞭解每個文件操作如何與 Amazon S3 存儲交互。
>
> 將 Rsync 實用程序與您的文件網關結合使用可以在緩存中創建臨時文件，並在 Amazon S3 中創建臨時 S3 對象。此情況會在 S3 標準 — 不常存取 (S3 標準 — IA) 和 S3 智慧型分層儲存類別中產生早期刪除費用。

建立 SMB 檔案共享

建立 SMB 檔案共享

1. 開啟AWSStorage Gateway 於https://console.aws.amazon.com/storagegateway/home/。
2. 選擇建立檔案共享開啟檔案共享設定(憑證已建立！) 頁面上的名稱有些許差異。
3. 適用於門戶，請從清單中選擇 Amazon S3 檔案閘道。

4. 適用於Amazon S3 位置，執行下列其中一項動作：

   - 若要將檔案共享直接連接至 S3 儲存貯體，請選擇S3 儲存儲體名稱，然後輸入存儲桶名稱和文件共享創建的對象的前綴名稱（可選）。您的網關使用此存儲桶來存儲和檢索文件。如需有關建立新儲存貯體的詳細資訊，請參如何建立 S3 儲存貯體？中的Amazon S3 使用者指南。
   - 若要將檔案共享連接至 S3 儲存貯體透過存取點，請選擇S3 存取點，然後輸入 S3 接入點名稱和文件共享創建的對象的前綴名稱（可選）。您的存儲桶策略必須配置為將訪問控制委派給接入點。如需存取點的詳細資訊，請參使用 Amazon S3 存取點管理資料存取和將存取控制委派給存取點中的Amazon S3 使用者指南。
   - 要通過接入點別名將文件共享連接到 S3 存儲桶，請選擇S3 存取點別名，然後輸入 S3 接入點別名和文件共享創建的對象的前綴名稱（可選）。如果選擇此選項，則文件網關無法創建新的 AWS Identity and Access Management(IAM) 角色並代您存取政策。您必須選擇現有 IAM 角色並在存取 S3 儲存貯體部分。如需存取點別名的詳細資訊，請參為您的存取點使用儲存貯體型別名中的Amazon S3 使用者指南。

   > **Note**
   >
   > - 如果輸入前綴名稱，或選擇通過接入點或接入點別名進行連接，則必須輸入文件共享名稱。
   > - 字首名稱必須以正斜線 (/。
   > - 建立檔案共享後，無法修改或刪除。
   > - 如需使用前綴名稱的詳細資訊，請參使用字首整理物件中的Amazon S3 使用者指南。

5. 適用於AWS 區域中，選擇AWS 區域S3 儲存儲體。
6. 適用於檔案共享名稱中，輸入檔案共享的名稱。默認名稱為 S3 儲存貯體名稱或存取點名稱。

   > **Note**
   >
   > - 如果輸入了前綴名稱，或選擇通過接入點或接入點別名進行連接，則必須輸入文件共享名稱。
   > - 創建文件共享後，無法刪除文件共享名稱。

7. （可選）對於AWS PrivateLinkS3，執行下列操作：

1. 若要將檔案共享配定為透過在虛擬私有雲端 (VPC) 內的接口端點連接至 S3，由AWS PrivateLink，選擇使用 VPC 端點。
2. 要標識您希望文件共享連接的 VPC 接口終端節點，請選擇VPC 端點 ID或者VPC 端點 DNS 名稱，然後在相應字段中提供所需信息。

> **Note**
>
> - 如果文件共享通過 VPC 接入點或通過與 VPC 接入點關聯的別名連接到 S3，則需要執行此步驟。
> - 使用檔案共享用AWS PrivateLink在 FIPS 網關上不受支持。
> - 如需AWS PrivateLink，請參AWS PrivateLink適用於 Amazon S3中的Amazon Storage Service 使用者指南。

8. 針對 Access objects using (使用下列方式存取物件)，選擇 Server Message Block (SMB) (伺服器訊息區塊 (SMB))。
9. 針對 Audit logs (稽核日誌)，選擇下列其中一項：

   - 若要關閉日誌，選擇Disable logging (停用日誌記錄)。
   - 若要建立新的審核日誌，選擇建立新的日誌。
   - 若要使用現有的日誌組，選擇使用現有的日誌，然後從清單中選擇審核日誌。

   如需稽核的詳細資訊，請參閱瞭解文件網關審核日誌。
10. 適用於從 S3 自動刷新緩存，選擇設定刷新間隔，然後設置使用生存時間 (TTL) 刷新文件共享緩存的時間（天、小時和分鐘）。TTL 是自上次刷新以來的時間長度。TTL 間隔過後，訪問目錄會導致文件網關首先從 Amazon S3 存儲桶刷新該目錄的內容。
11. 適用於檔案上傳通知，選擇建立時間 (秒)以便在文件網關完全上傳到 S3 時收到通知。將建立時間以秒為單位控制在客户端寫入文件的最後一個時間點之後等待的秒數，然後再生成`ObjectUploaded`通知。由於客户端可以對文件進行許多小寫入，因此最好儘可能長地設置此參數，以避免在較短的時間內為同一文件生成多個通知。如需詳細資訊，請參閱 獲取文件上傳通知。

> **Note**
>
> 此設置對象上傳到 S3 的時間沒有影響，僅影響通知的時間。

12. （可選）在標籤部分中，選擇添加新標記，然後輸入金鑰和值以將標籤新增至您的檔案共享。標籤為區分大小寫的索引鍵值組，可協助您管理、篩選和搜尋檔案共享。
13. 選擇 Next (下一步)。所以此Amazon S3 儲存設置頁面隨即出現。
14. 適用於新對象的存儲類下，請選擇在 Amazon S3 儲存貯體中建立的新物件要使用的儲存體類別：

    - 若要透過備援方式在多個不同地理位置可用區域存放經常存取的物件資料，請選擇S3 標準。如需 S3 標準儲存類別的詳細資訊，請參經常存取物件的儲存體方案中的Amazon Storage Service 使用者指南。
    - 若要自動將資料移至最經濟實惠的儲存存取層，以最佳化儲存成本，請選擇S3 Intelligent-Tiering。如需 S3 智慧型分層儲存類別的詳細資訊，請參自動最佳化經常存取物件與不常存取物件的儲存體方案中的Amazon Storage Service 使用者指南。
    - 若要透過備援方式在多個不同地理位置可用區域存放不常存取的物件資料，請選擇S3 標準 – IA。如需 S3 標準 IA 儲存類別的詳細資訊，請參不常存取物件的儲存體方案中的Amazon Storage Service 使用者指南。
    - 若要將不常存取的物件資料存放在單一可用區域中，請選擇S3 單區域 – IA。如需 S3 單區域 — IA 儲存類別的詳細資訊，請參不常存取物件的儲存體方案中的Amazon Storage Service 使用者指南。

    要幫助監控 S3 賬單，請使用AWS Trusted Advisor。如需詳細資訊，請參閱「」監控工具中的Amazon Storage Service 使用者指南。
15. 針對 Object metadata (物件中繼資料)，選擇您要使用的中繼資料：

    - 若要啟用以副檔名為基礎的上傳物件使用 MIME 類型的猜想，請選擇猜測 MIME 類型。
    - 若要將完整控制權授予映射至 SMB 檔案共享的 S3 儲存貯體擁有者，請選擇讓存儲桶擁有者完全控制。如需使用檔案共享存取另一個賬户擁有儲存貯體中之物件的詳細資訊，請參使用檔案共享進行跨賬户存取。
    - 若要將完整控制權授予映射至 SMB 檔案共享的 S3 儲存貯體擁有者，請選擇啟用請求者付款。如需詳細資訊，請參閱請求者付款儲存貯體。
16. 適用於存取 S3 儲存貯體中，選擇AWS Identity and Access Management(IAM) 角色，您希望檔案閘道用來存取您的 Amazon S3 儲存貯體：

- 若要啟用檔案閘道代您建立新的 IAM 角色並代您存取政策，請選擇創建新的 IAM 角色。如果文件共享使用接入點別名連接到 Amazon S3，則此選項不可用。
- 要選擇現有 IAM 角色並手動設置訪問策略，請選擇使用現有 IAM 角色。如果您的文件共享使用接入點別名連接到 Amazon S3，則必須使用此選項。在 中IAM 角色框中，輸入用於存取您儲存貯體的角色的 Amazon Resource Name (ARN)。如需 IAM 角色的資訊，請參。IAM 角色中的AWS Identity and Access Management使用者指南。

如需存取 S3 儲存貯體的詳細資訊，請參閱授予對 Amazon S3 儲存貯體的存取權。

17. 適用於Encryption (加密)下，請選擇您的檔案閘道存放在 Amazon S3 中的物件加密所用的加密金鑰類型：

    - 若要使用 Amazon S3 (SSE-S3) 管理的伺服器端加密，請選擇S3 受管金鑰 (SSE-S3)。
    - 若要使用伺服器端加密AWS Key Management Service(SSE-KMS)，選擇KMS 管理金鑰 (SSE-KMS)。在 中Primary key (主索引鍵)框中，選擇現有的AWS KMS key或選擇建立新的 KMS 金鑰在AWS Key Management Service(AWS KMS) 主控台。如需有關 的詳細資訊AWS KMS，請參什麼是AWS Key Management Service?中的AWS Key Management Service開發人員指南。

    > **Note**
    >
    > 若要指定AWS KMS鍵與未列出的別名一起使用AWS KMS鍵來自不同的AWS 帳戶，您必須使用AWS Command Line Interface(AWS CLI。如需詳細資訊，請參閱「」CreateNFSFileShare中的AWSStorage Gateway API 參考。
    > 不支持非對稱 KMS 密鑰。

18. 選擇 Next (下一步)。所以此檔案存取設定頁面隨即出現。
19. 適用於身份驗證方法中，選擇您想要使用的身份驗證方法。

    - 若要使用您的公司 Microsoft AD，進行 SMB 檔案共享的使用者驗證存取權，請選擇Active Directory。您的檔案閘道必須加入網域。
    - 要僅提供來賓訪問權限，請選擇訪客存取。如果您選擇此身份驗證方法，檔案閘道不需要是 Microsoft AD 網域的一部分。您也可以使用身為 AD 網域成員的檔案閘道，來建立具有訪客存取權的檔案共享。您必須在相應的字段中為 SMB 服務器設置來賓密碼。

> **Note**
>
> 兩種存取類型皆可同時使用。

20. 在 中SMB 共用設定部分中，選擇您的設置。

    使用 Export as (匯出為) 時，選擇下面其中一個選項：

    - 讀取/寫入 (預設值)
    - 唯讀

    > **Note**
    >
    > 對於掛載在 Microsoft Windows 客户端上的文件共享，如果選擇唯讀，則可能會看到內容關於您無法建立資料夾之意外錯誤的訊息。您可以略過此訊息。

    對於 File/directory access controlled by (檔案/目錄存取控制者)，請選擇以下其中一項：

    - 若要設定 SMB 檔案共享中檔案和資料夾之精確的許可，請選擇Windows Storage Control List (。如需詳細資訊，請參閱 使用 Microsoft Windows ACL 來控制 SMB 檔案共享的存取。
    - 若要使用 POSIX 許可來控制透過 NFS 或 SMB 檔案共享存放之檔案和目錄的存取權，請選擇POSIX 權限。

    如果您的身份驗證方法是Active Directory, 用於管理員用户/組中，輸入 AD 使用者和羣組的逗號分隔清單。如果您希望管理員使用者具有更新檔案共享中所有檔案和資料夾之存取控制清單 (ACL) 的權限，請這麼做。這些使用者和群組就會對檔案共享具有管理員權限。一個羣組前面必須加上@字符，例如，`@group1`。

    適用於區分大小寫下，選擇下列其中一項：

    - 要允許網關控制區分大小寫，請選擇客户端指定。
    - 要允許客户端控制區分大小寫，請選擇強制區分大小寫。

> **Note**
>
> - 如果選中此項，此設置將立即應用於新的 SMB 客户端連接。現有 SMB 客户端連接必須斷開與文件共享的連接，然後重新連接，設置才能生效。

適用於基於存取的枚舉下，選擇下列其中一項：

- 要使共享上的文件和文件夾僅對具有讀取訪問權限的用户可見，請選擇對文件和目錄禁用。
- 要在目錄枚舉期間使共享上的文件和文件夾對所有用户可見，請選擇為文件和目錄啟用。

> **Note**
>
> 基於訪問的枚舉是一個系統，它根據共享的訪問控制列表 (ACL) 過濾 SMB 文件共享上的文件和文件夾枚舉。

適用於機會鎖定下，選擇下列其中一項：

- 要允許文件共享使用機會鎖定來優化文件緩衝策略，請選擇Enabled。在大多數情況下，啟用機會鎖定可提高性能，特別是在 Windows 上下文菜單方面。
- 要防止使用機會鎖定，請選擇已停用。如果環境中的多個 Windows 客户端經常同時編輯相同的文件，則禁用機會鎖定有時會提高性能。

> **Note**
>
> 對於涉及訪問不同大小寫的同名文件的工作負載，不建議對區分大小寫的共享啟用機會鎖定。

21. （可選）在用户和組文件共享訪問部分中，選擇您的設置。

適用於允許的用户和組，選擇新增允許使用者或者新增允許的組並輸入您要允許存取檔案共享的 AD 使用者或 group。重複此過程以允許根據需要允許儘可能多的用户和組。

適用於被拒絕的用户和組，選擇新增拒絕使用者或者新增拒絕的羣組並輸入您要拒絕檔案共享存取權限的 AD 使用者或 group。重複此過程可根據需要拒絕任意數量的用户和組。

> **Note**
>
> 所以此用户和組文件共享訪問部分僅在Active Directory已選取。
> 僅輸入 AD 使用者或群組名稱。網域名稱是由閘道加入之特定 AD 閘道的成員資格所暗示。
> 如果您未指定任何允許或拒絕的使用者或羣組，則任何已驗證的 AD 使用者都可以匯出檔案共享。

22. 選擇 Next (下一步)。
23. 檢您的檔案共享組態設定，然後選擇完成。

在您的 SMB 檔案共享建立之後，您可以在檔案共享的 Details (詳細資訊) 標籤中看到您的檔案共享設定。

後續步驟

[在用户端掛載您的 SMB 檔案共享]

裝載並使用您的文件共享

在下文中，您可以找到如何在用户端掛載檔案共享、使用您的共享、測試您的檔案閘道，以及視需要清除資源的相關說明。如需受支援之網路檔案系統 (NFS) 用戶端的詳細資訊，請參閱檔案閘道支援的 NFS 用戶端。如需受支援之服務訊息區塊 (SMB) 用戶端的詳細資訊，請參閱檔案閘道支援的 SMB 用戶端。

您可以找到將檔案共享掛載在 AWS Management Console的範例命令。在下列各節中，您可以找到如何在用戶端掛載檔案共享、使用您的共享、測試您的檔案閘道，以及視需要清除資源的詳細資訊。

主題

在用户端掛載您的 NFS 檔案共享

現在您要將 NFS 檔案共享掛載在您用户端的某個磁盤上，然後將它映射到您的 Amazon S3 儲存貯體。

掛載檔案共享並將其映射到 Amazon S3 儲存貯體

1. 如果您使用的是 Microsoft Windows 用戶端，建議您建立 SMB 檔案共享，並使用已安裝在 Windows 用戶端的 SMB 用戶端來存取。如果您使用 NFS，請開啟 Windows 中的 Services for NFS。
2. 掛載您的 NFS 檔案共享：
   - 若為 Linux 用戶端，請在命令提示時輸入下列命令。

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

   - 若為 MacOS 用戶端，請在命令提示輸入下列命令。

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

- 若為 Windows 用戶端，請在命令提示時輸入下列命令。

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

例如，假設您在 Windows 用戶端中的 VM IP 地址為 123.123.1.2，而您的 Amazon S3 儲存貯體名稱是`test-bucket`。同時假設您想要映射到磁碟機 T。在這種情況下，您的命令看起來會如下文中所示。

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

> **Note**
>
> 掛載檔案共享時，請注意下列事項：
>
> - 您可能碰到 Amazon S3 儲存貯體中有同名之資料夾和物件的狀況。在這種情況下，如果物件名稱結尾不包含斜線，檔案閘道中只會顯示資料夾。例如，如果儲存貯體包含名為`test`或者`test/`和名為`test/test1`，僅`test/`和`test/test1`在文件網關中可見。
> - 您可能需要在用戶端重新開機後，重新掛載您的檔案共享。
> - Windows 預設使用軟性掛載來掛載您的 NFS 共享。發生連線問題時，軟性掛載更容易逾時。我們建議您使用硬性掛載，因為硬性掛載更安全，也能更好保存資料。軟性掛載命令會省略 **`-o mtype=hard`** 參數。Windows 硬性掛載命令使用 `-o mtype=hard` 參數。
> - 如果您使用的是 Windows 用戶端，請在掛載之後，執行 `mount` 命令且不搭配任何選項來檢查您的 `mount` 選項。回應應該會確認檔案共享已使用您提供的最新選項來掛載。同時應該也會確認您不是使用快取的舊項目，這需要至少 60 秒時間來清除。

後續步驟

測試您的 S3 文件網關

在用户端掛載您的 SMB 檔案共享

現在您要掛載 SMB 檔案共享，並將它映射到您用戶端可存取的某個磁碟機。主控台的檔案閘道區段會顯示您可用於 SMB 用户端的受支援掛載命令。您可在下文中找到一些額外的選項來試試看。

您可以使用多種不同的方法來掛載 SMB 檔案共享，包括下列方法：

- 命令提示 (`cmdkey`和`net use`) — 使用命令提示字元掛載檔案共享。將您的憑據存儲在`cmdkey`，然後將驅動器安裝到`net use`，然後包括`/persistent:yes`和`/savecred`開關，如果您希望連接在系統重新引導期間保持連接。具體命令會有所不同，具體取決於您是否要掛載 Microsoft Active Directory (AD) 存取或訪客存取的磁盤。以下提供範例。
- 文件資源管理器（映射網絡驅動器）— 使用 Windows 文件資源管理器掛載您的文件共享。配置設置以指定是否希望連接在系統重新引導期間保留並提示輸入網絡憑據。
- PowerShell 腳本 — 創建自定義 PowerShell 腳本以裝載文件共享。根據您在腳本中指定的參數，連線可在系統重新啟動時持久，而且共享可在掛載時向作業系統顯示或隱藏。

> **Note**
>
> 如果您是 Microsoft AD 的使用者，請洽詢您的管理員，確定您有權存取 SMB 檔案共享，再將檔案共享掛載到您的本機系統。
> 如果您是訪客使用者，請確定您有訪客使用者帳戶的密碼，再嘗試掛載檔案共享。

使用命令提示字元掛載您適用於授權 Microsoft AD 使用者的 SMB 檔案共享：

1. 請確定 Microsoft AD 使用者具有必要的 SMB 檔案共享，再將檔案共享掛載到用户的系統。
2. 在命令提示時輸入下列命令以掛載檔案共享：

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

使用命令提示字元掛載您具有特定用户名和密碼的 SMB 檔案共享：

1. 請確定用户帳户有權存取 SMB 檔案共享，再將檔案共享掛載到系統。
2. 在命令提示時輸入下列命令，在 Windows 憑據管理器中保存用户憑據：

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

3. 在命令提示時輸入下列命令以掛載檔案共享：

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

使用命令提示字元掛載您適用於訪客使用者的 SMB 檔案共享：

1. 請確定您有訪客使用者帳戶的密碼，再掛載檔案共享。
2. 在命令提示符處鍵入以下命令，以在 Windows 憑據管理器中保存來賓憑據：

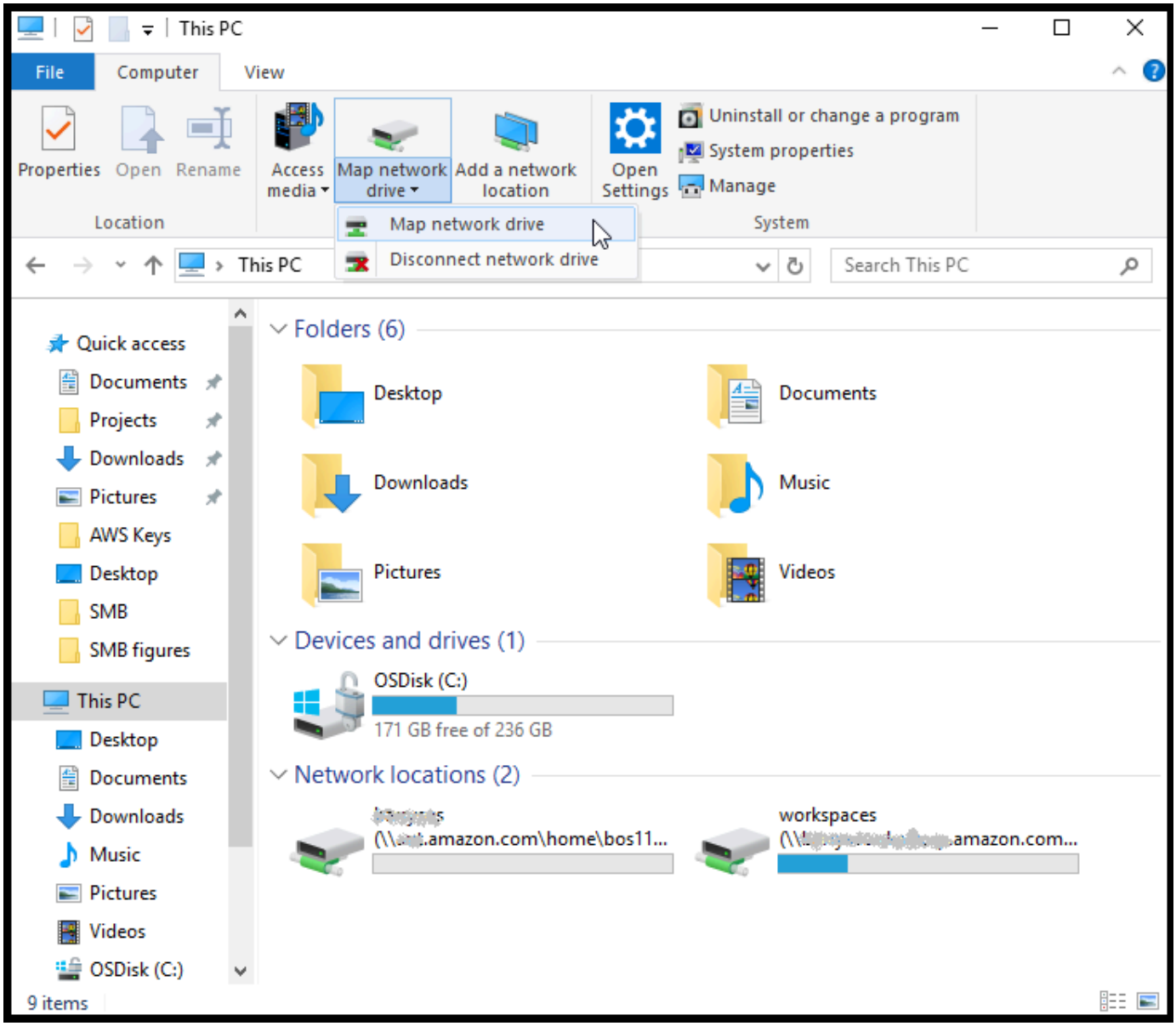
   ```
   cmdkey /add:GatewayIPAddress /user:DomainName\smbguest /pass:Password
   ```
3. 在命令提示中輸入下列命令。

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

> **Note**
>
> 掛載檔案共享時，請注意下列事項：
>
> - 您可能碰到 Amazon S3 儲存貯體中有同名之資料夾和物件的狀況。在這種情況下，如果物件名稱結尾不包含斜線，檔案閘道中只會顯示資料夾。例如，如果儲存貯體包含名為`test`或者`test/`和名為`test/test1`，僅`test/`和`test/test1`在文件網關中可見。
> - 除非您將文件共享連接配置為保存用户憑據並在系統重新啟動期間保留，否則您可能需要在每次重新啟動客户端系統時重新裝載文件共享。

使用 Windows 檔案總管掛載 SMB 檔案共享

1. 按下 Windows 鍵並輸入**File Explorer**中的搜尋窗口框中，或按**Win+E**。
2. 在導覽窗格中，選擇此 PC，然後在電腦標籤的連線網路磁碟機選擇連線網路磁碟機，如下列螢幕擷取畫面中所示。



3. 在連線網路磁碟機對話方塊中，選擇磁碟機的磁碟機代號。
4. 對於資料夾，輸入 ***[File Gateway IP]**[SMB File Share Name]***，或選擇瀏覽來從對話方塊選取 SMB 檔案共享。
5. (選用) 選取 Reconnect at sign-up (登入時重新連線)，如果您希望在重新開機後保持掛載點。
6. (選用) 選取 Connect using different credentials (使用不同的登入資料連線)，如果您希望使用者輸入 Microsoft AD 登入或訪客帳戶使用者密碼。
7. 選擇 Finish (完成) 完成您的掛載點。

您可以在 Storage Gateway 管理主控台中編輯檔案共享設定、編輯獲得允許和受到拒絕的使用者和群組，以及變更訪客存取密碼。您也可以重新整理檔案共享快取中的資料，並從主控台刪除檔案共享。

修改 SMB 檔案共享的屬性

1. Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home。
2. 在導覽窗格上，選擇 File Shares (檔案共享)。
3. 在 File Share (檔案共享) 頁面上，依您想要修改的 SMB 檔案共享選取核取方塊。
4. 針對 Actions (動作)，選擇您希望的動作：
   - 選擇 Edit file share settings (編輯檔案共享設定) 修改共享存取。
   - 選擇 Edit allowed/denied users (編輯允許/拒絕的使用者) 新增或刪除使用者和群組，然後在 Allowed Users (允許的使用者)、Denied Users (拒絕的使用者)、群 Allowed Groups (允許的群組) 和 Denied Groups (拒絕的群組) 方塊中輸入允許和拒絕的使用者和群組。使用 Add Entry (新增項目) 按鈕建立新的存取權，並使用 (X) 按鈕移除存取權。
5. 完成後，請選擇 Save (儲存)。

   當您輸入允許的使用者和羣組時，您就在建立允許列表。若無允許列表，則任何通過身份驗證的 Microsoft AD 使用者都能存取 SMB 檔案共享。任何標記拒絕的使用者和組都會新增到拒絕列表，不能存取 SMB 檔案共享。在拒絕列表和允許列表中的使用者或用户組時，拒絕列表優先。

   您可以在 SMB 檔案共享上啟用存取控制清單 (ACL)。如需如何啟用 ACL 的詳細資訊，請參閱使用 Microsoft Windows ACL 來控制 SMB 檔案共享的存取。

後續步驟

測試您的 S3 文件網關

在具有預先存在的對象的存儲桶上使用文件共享

您可以使用 NFS 或 SMB，在具有於檔案閘道外所建物件的 Amazon S3 儲存貯體上匯出檔案共享。儲存貯體中在閘道外建立的物件，在您的檔案系統用戶端存取它們時，會顯示為 NFS 或 SMB 檔案系統中的檔案。標準的可攜式作業系統界面 (POSIX) 存取權和許可是用於檔案共享。當您將檔案寫回 Amazon S3 儲存貯體時，檔案即具有您為他們提供的屬性和存取權。

您可以隨時將物件上傳到 S3 儲存貯體。若要檔案共享將這些最近新增的物件顯示為檔案，您需要重新整理 S3 儲存貯體。如需詳細資訊，請參閱 the section called “刷新 Amazon S3 儲存貯體中的物件”。

> **Note**
>
> 我們不建議一個 Amazon S3 儲存貯體有多位作者。如果您有多位作者，請務必讀「我的 Amazon S3 儲存貯體是否可有多位作者？」一節 中的Storage Gateway 常見。

若要將中繼資料預設值指派給使用 NFS 存取的物件，請參閱管理您的 Amazon S3 檔案網關中的編輯中繼資料預設值。

針對 SMB，您可以使用 Microsoft AD 或訪客存取為具有預先存在物件的 Amazon S3 儲存貯體匯出共享。透過 SMB 檔案共享匯出的物件會繼承其上一層父目錄的 POSIX 所有權和許可。根資料夾下的物件則繼承根目錄存取控制清單 (ACL)。根目錄 ACL 的擁有者為 `smbguest`，檔案許可為 666，目錄為 777。這適用於所有形式的驗證存取 (Microsoft AD 和訪客)。

測試您的 S3 文件網關

您可將檔案和資料夾複製到您的映射磁碟機。檔案會自動上傳至您的 Amazon S3 儲存貯體。

從您的 Windows 用户端將檔案上傳至 Amazon S3

1. 在您的 Windows 用戶端上，導覽到您掛載檔案共享的磁碟機。您的磁碟機名稱前面是您的 S3 儲存貯體名稱。
2. 將檔案或資料夾複製到磁碟機。
3. 在 Amazon S3 管理主控台上，導覽到您的映射儲存貯體。您應該會看到您複製到指定 Amazon S3 儲存貯體的檔案和資料夾。

   您可以看到您在檔案共享標籤中的AWSStorage Gateway 管理控制台。

您的 NFS 或 SMB 用戶端可寫入、讀取、刪除、重新命名和截斷檔案。

> **Note**
>
> 檔案閘道不支援在檔案共享建立硬性或符號連結。

請注意下列檔案閘道如何使用 S3 的事項：

- 從直接讀取快取讀取。換言之，如果資料不可用，即從 S3 擷取並新增到快取。

- 寫入會使用回寫快取，透過最佳化的分段上傳傳送到 S3。
- 寫入和讀取已經過最佳化，所以只有請求或變更過的部分才會透過網路傳輸。
- 刪除會從 S3 移除物件。
- 目錄會在 S3 中做為資料夾物件管理，使用與 Amazon S3 主控台中相同的語法。您可以重新命名空目錄。
- 遞迴檔案系統操作效能 (例如 `ls -l`) 取決於您儲存貯體中的物件數目。

後續步驟

接下來做些什麼？

接下來做些什麼？

在前文各節中，您建立並開始使用檔案閘道，包括掛載檔案共享和測試您的設定。

本指南的其他章節包含如何執行下列作業的相關資訊：

- 若要管理檔案閘道，請參閱管理您的 Amazon S3 檔案網關。
- 若要最佳化檔案閘道，請參閱最佳化閘道效能。
- 若要為閘道問題進行故障診斷，請參閱 為您的閘道進行故障診斷。
- 若要了解 Storage Gateway 指標及監控您閘道執行狀況的方式，請參見。

清除不需要的資源

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。

清除不需要的資源

1. 除非您計劃繼續使用閘道，否則請將其刪除。如需詳細資訊，請參閱 使用 AWS Storage Gateway 主控台刪除閘道以及移除相關聯資源。
2. 從現場部署主機刪除 Storage Gateway 體 VM。如果您已在 Amazon EC2 執行個體上建立閘道，請終止執行個體。

在虛擬私有雲端中啟用閘道

您可以在現場部署軟體設備以及雲端儲存基礎設施之間建立私有連線。然後您可以使用軟體設備將資料傳輸到AWS存儲，而無需與網關通信AWS在公有網際網路上提供儲存服務。使用亞馬遜 VPC 服務，您可以啟動AWS資源。您可利用 Virtual Private Cloud (VPC) 來控制您的網路設定，例如 IP 地址範圍、子網路、路由表和網路閘道。如需 VPC 的詳細資訊，請參「」「什麼是 Amazon VPC？」中的Amazon VPC User Guide。

若要在 VPC 中搭配 Storage Gateway 道 VPC 端點使用閘道，請執行下列動作：

- 使用 VPC 控制台來建立適用於 Storage Gateway 的 VPC 端點，並取得 VPC 端點 ID。在創建和激活網關時指定此 VPC 終端節點 ID。
- 如果您啟用檔案閘道，請為 Amazon S3 建立 VPC 端點。在為網關創建文件共享時，請指定此 VPC 終端節點。
- 如果您要啟動檔案閘道，請設定 HTTP 代理，並在該檔案閘道 VM 本機主控台中進行設定。您需要為以 Hypervisor 為基礎的內部部署檔案閘道 (例如以 VMware、Microsoft HyperV 和 Linux 核心型虛擬機器 (KVM) 為基礎的內部部署檔案閘道) 設定此代理。在這些情況下，您需要代理以讓閘道從 VPC 外部存取 Amazon S3 私有端點。如需設定 HTTP 代理的詳細資訊，請參閱設定 HTTP 代理。

> **Note**
>
> 您的閘道必須在建立 VPC 端點的同一區域中啟動。
> 對於檔案閘道，為檔案共享設定的 Amazon S3 存儲必須位在建立適用於 Amazon S3 的 VPC 端點同一個區域。

主題

- 建立適用於 Storage Gateway 的 VPC 端點
- 設置和配置 HTTP 代理（僅限本地文件網關）
- 允許流量到 HTTP 代理中所需端口

建立適用於 Storage Gateway 的 VPC 端點

按照這些指示來建立 VPC 端點。如果您已經有適用於 Storage Gateway 的 VPC 端點，則您可以使用它。

建立適用於 Storage Gateway 的 VPC 端點

1. 登入 AWS Management Console，並在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoints (端點)，然後選擇 Create Endpoint (建立 端點)。
3. 在建立端點頁面上，選擇AWS服務為了服務目錄。
4. 在 Service Name (服務名稱) 中，選擇 `com.amazonaws.region.storagegateway`。例如：`com.amazonaws.us-east-2.storagegateway`。
5. 針對 VPC，選擇您的 VPC，並記下其可用區域和子網路。
6. 確認未選取 Enable Private DNS Name (啟用私有 DNS 名稱)。
7. 針對 Security group (安全群組)，選擇要用於您的 VPC 的安全群組。您可以接受預設的安全群組。驗證您的安全群組中已允許所有下列 TCP 連接埠：
   - TCP 443
   - TCP 1026
   - TCP 1027
   - TCP 1028
   - TCP 1031
   - TCP 2222
8. 選擇 Create endpoint (建立端點)。端點的最初狀態是 pending (擱置中)。建立端點後，記下所新建 VPC 端點的 ID。
9. 建立端點後，請選擇 Endpoints (端點)，然後選擇新的 VPC 端點。
10. 在 DNS Names (DNS 名稱) 區段，使用未指定可用區域的第一個 DNS 名稱。您的 DNS 名稱看起來會像這樣：`vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

現在您有一個 VPC 端點，您可以建立您的閘道。

> **Important**
>
> 如果您要建立檔案閘道，則您也需要建立適用於 Amazon S3 的端點。依照上方「建立適用於 Storage Gateway 的 VPC 端點」章節中的相同步驟，但這次在`com.amazonaws.us-east-2.s3`在「服務名稱」下。接著選取您希望 S3 端點關聯的路由表，而不是子網路/安全群組。如需說明，請參閱「」建立閘道端點。

設置和配置 HTTP 代理（僅限本地文件網關）

如果您啟動檔案閘道，您需要安裝 HTTP 代理並使用檔案閘道虛擬機器本機主控台配置。從現場部署檔案閘道存取 VPC 外部的 Amazon S3 私有端點需要此代理。如果您在 Amazon EC2 中已有 HTTP 代理，則您可以使用它。不過，您需要驗證安全性群組中是否已允許所有下列 TCP 連接埠：

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

如果您沒有 Amazon EC2 代理，請使用下列程序來設定和配置 HTTP 代理。

設定代理伺服器

1. 啟動 Amazon EC2 執行個體。我們建議使用已網路最佳化的執行個體系列，例如 c5n.large。
2. 請使用下列命令安裝 squid：：**sudo yum install squid**。 這會在`/etc/squid/squid.conf`。
3. 將此組態檔的內容以下列內容取代：

```
#
# Recommended minimum configuration:
#

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

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

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

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

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

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

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

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

# Squid normally listens to port 3128
http_port 3128

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

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

4. 如果您不需要鎖定代理伺服器，也不需要進行任何變更，則請啟用並開始使用下列命令。這些命令會在伺服器開機時將其啟動。

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

您現在可以設定適用於 Storage Gateway 的 HTTP 代理來使用它。設定閘道以使用代理時，請使用預設的 squid 連接埠 3128。產生的 squid conf 檔案預設會涵蓋下列要求的 TCP 連接埠：

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

使用虛擬機器本機主控台設定 HTTP 代理

1. 登入您閘道的 VM 本機主控台。如需關於登入的詳細資訊，請參閱登入到文件閘道本機主控台。
2. 在主要功能表中，選擇 Configure HTTP proxy (設定 HTTP 代理)。
3. 在 Configuration (組態) 功能表中，選擇 Configure HTTP proxy (設定 HTTP 代理)。
4. 提供代理伺服器的主機名稱和連接埠。

如需如何設定 HTTP 代理的詳細資訊，請參閱設定 HTTP 代理。

允許流量到 HTTP 代理中所需端口

如果您使用 HTTP 代理，請確定允許從 Storage Gateway 道到下列目的地和連接埠的流量。

當 Storage Gateway 通過公有端點通訊時，它會與下列 Storage Gateway 服務通訊。

```
anon-cp.storagegateway.region.amazonaws.com:443
client-cp.storagegateway.region.amazonaws.com:443
proxy-app.storagegateway.region.amazonaws.com:443
dp-1.storagegateway.region.amazonaws.com:443
storagegateway.region.amazonaws.com:443 (Required for making API calls)
s3.region.amazonaws.com (Required only for File Gateway)
```

> **Important**
>
> 取決於您的網關AWS區域，替換##在端點中使用對應的區域字串。例如，若您在美國西部（俄勒岡州）區域建立閘道，端點即為：：：`storagegateway.us-west-2.amazonaws.com:443`。

當 Storage Gateway 通過 VPC 端點通訊時，它會與AWS服務通過 Storage Gateway VPC 端點上的多個連接埠以及 Amazon S3 私有端點上的連接埠 443，來執行個體。

- Storage Gateway VPC 端點上的 TCP 連接埠。
  - 443、1026、1027、1028、1031 和 2222
- S3 私有端點上的 TCP 連接埠
  - 443

管理您的 Amazon S3 檔案網關

您可以在以下找到有關如何管理 Amazon S3 檔案閘道資源的資訊。

主題

新增檔案共享

在您啟用和執行 S3 檔案閘道之後，可以新增其他檔案共享，以及授予 Amazon S3 儲存貯體存取權。您可以授予存取權以將儲存貯體包含在不同AWS 帳戶比您的文件共享。如需如何新增檔案共享的資訊，請參閱建立檔案共享。

主題

授予對 Amazon S3 儲存貯體的存取權

創建文件共享時，您的文件網關需要訪問權限才能將文件上傳到 Amazon S3 存儲桶，並對其用於連接到存儲桶的任何接入點或虛擬私有雲 (VPC) 終端節點執行操作。要授予此訪問權限，您的文件網關假定AWS Identity and Access Management(IAM) 角色，此角色與授予此存取權的 IAM 政策相關聯。

此角色需要此 IAM 政策和 Security Token Service (STS) 的信任關係。政策決定角色可以執行的動作。此外，您的 S3 儲存貯體和任何關聯的存取點或 VPC 終端節點必須有允許 IAM 角色存取它們的存取政策。

您可以自行建立角色和存取政策，或者檔案閘道可以為您建立它們。如果檔案閘道為您建立政策，此政策會包含 S3 動作的清單。如需角色和許可的相關資訊，請參建立角色以將許可委派給AWS 服務中的IAM User Guide。

下列範例是信任政策，允許您的檔案閘道擔任 IAM 角色。

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

如果您不希望檔案閘道代您建立政策，您可以建立自己的政策，並將它連接到您的檔案共享。如需如何進行該服務的詳細資訊，請參閱建立檔案共享。

下列範例政策允許您的檔案閘道執行政策所列的所有 Amazon S3 動作。陳述式的第一部分允許對名為 `TestBucket` 的 S3 儲存貯體執行所有列出的動作。第二個部分允許對 `TestBucket` 的所有物件執行列出的動作。

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

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

以下示例策略與前面的策略類似，但允許您的文件網關執行通過接入點訪問存儲桶所需的操作。

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

```
    ]
}
```

> **Note**
>
> 如果您需要通過 VPC 終端節點將文件共享連接到 S3 存儲桶，請參閱Amazon S3 的端點政策中的AWS PrivateLink使用者指南。

預防跨服務混淆代理人

混淆代理人問題屬於安全性議題，其中沒有執行動作許可的實體可以強制具有更多許可的實體執行該動作。在 AWS 中，跨服務模擬可能會導致混淆代理人問題。在某個服務 (呼叫服務) 呼叫另一個服務 (被呼叫服務) 時，可能會發生跨服務模擬。可以操縱呼叫服務來使用其許可，以其不應有存取許可的方式對其他客戶的資源採取動作。為了預防這種情況，AWS 提供的工具可協助您保護所有服務的資料，而這些服務主體已獲得您帳戶中資源的存取權。

若要限制 AWS Storage Gateway 為資源提供另一項服務的許可，我們建議在資源政策中使用 `aws:SourceArn` 和 `aws:SourceAccount` 全域條件內容索引鍵。如果同時使用全域條件內容索引鍵，則在相同政策陳述式中使用`aws:SourceAccount` 值和 `aws:SourceArn` 值中的帳戶時，必須使用相同的帳戶 ID。

的值`aws:SourceArn`必須是與文件共享關聯的 Storage Gateway 的 ARN。

防止混淆副手問題的最有效方法是使用`aws:SourceArn`全局條件上下文鍵與資源的完整 ARN。如果不知道資源的完整 ARN，或者您要指定多個資源，請使用`aws:SourceArn`具有通配符的全局上下文條件鍵（`*`），查看 ARN 的未知部分。例如：`arn:aws:`*`servicename`*`::`*`123456789012`*`:*`。

以下範例顯示如何使用`aws:SourceArn`和`aws:SourceAccount`全局條件上下文鍵 Storage Gateway 防止混淆副本問題。

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

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

使用檔案共享進行跨賬户存取

跨賬户存取意指的是 Amazon Web Services 帳户及使用者獲得授權，得以存取屬於另一個 Amazon Web Services 帳户之資源的情況。透過檔案閘道，您可以使用一個 Amazon Web Services 帳户中的檔案共享，存取屬於另外一個 Amazon Web Services 帳户之 Amazon S3 儲存貯體中的物件。

若要使用由一個 Amazon Web Services 帳户擁有的檔案共享，存取另外一個 Amazon Web Services 帳户中的 S3 儲存貯體

1. 確認 S3 儲存貯體擁有者已授予您的 Amazon Web Services 帳户存取您需要存取之 S3 儲存貯體，以及位於該儲存貯體中物件的權限。如需如何授予此存取權的資訊，請參範例 2：擁有者授予跨賬户儲存貯體許可中的Amazon Simple Storage Service 用户指南。如需必要許可的清單，請參閱授予對 Amazon S3 儲存貯體的存取權。
2. 確認您檔案共享用來存取 S3 儲存貯體的 IAM 角色包含像是 `s3:GetObjectAcl` 和 `s3:PutObjectAcl` 等操作的許可。此外，請確認 IAM 角色包含允許您的帳戶取得該 IAM 角色的信任政策。如需此類信任政策的範例，請參閱授予對 Amazon S3 儲存貯體的存取權。

   若您的檔案共享使用現有角色存取 S3 儲存貯體，您應包含 `s3:GetObjectAcl` 和 `s3:PutObjectAcl` 操作的許可。角色也會需要允許您的帳戶取得此角色的信任政策。如需此類信任政策的範例，請參閱授予對 Amazon S3 儲存貯體的存取權。
3. 打開 Storage Gateway 主控台https://console.aws.amazon.com/storagegateway/home。
4. 選擇 Configure file share setting (設定檔案共享設定) 對話方塊中的 Object metadata (物件中繼資料) 內的 Give bucket owner full control (給予儲存貯體擁有者完整控制)。

當您建立或更新您的跨帳戶存取檔案共享，並且在現場部署掛載檔案共享時，我們強烈建議您測試您的設定。您可以透過列出目錄的內容，或寫入測試檔案並確認檔案在 S3 儲存貯體中顯示為物件，來執行此作業。

> **Important**
>
> 請務必將政策設定正確，授予跨帳戶存取給您檔案共享使用的帳戶。若您沒有執行此作業的話，透過您現場部署應用程式進行的檔案更新將不會傳播至您使用的 Amazon S3 儲存貯體。

資源

如需存取政策和存取控制清單的其他資訊，請參閱以下內容：

使用提供之存取政策選項的準則中的Amazon Simple Storage Service 用户指南

存取控制清單 (ACL) 概觀中的Amazon Simple Storage Service 用户指南

刪除檔案共享

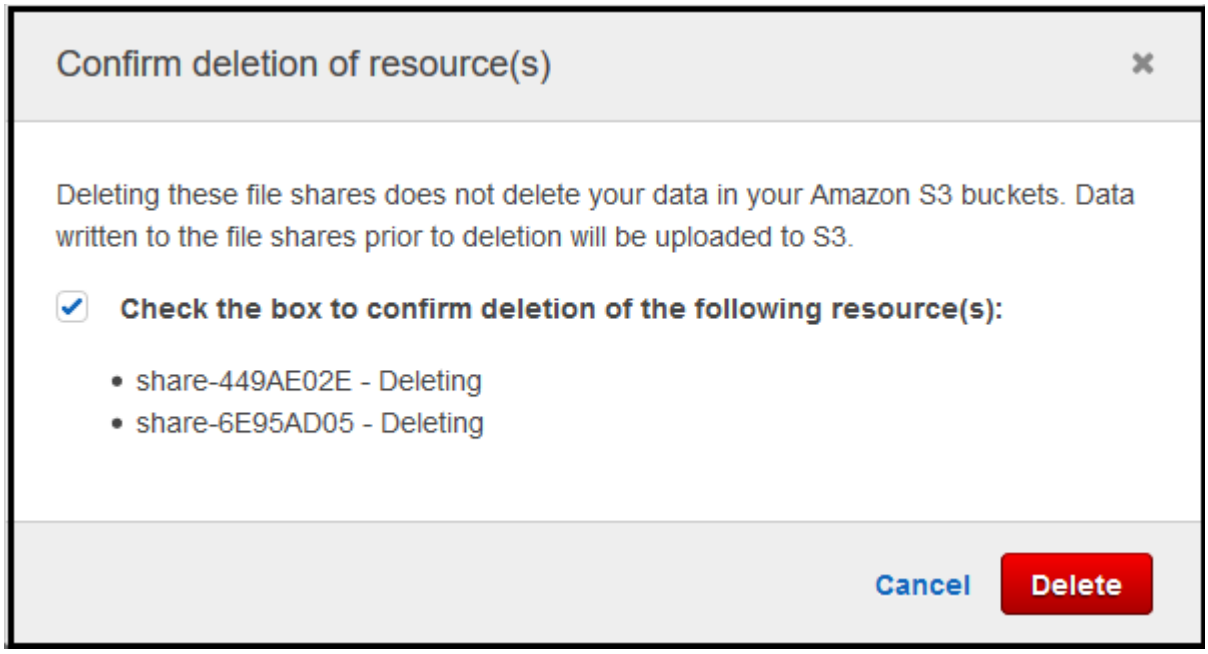
如果您不再需要檔案共享，則可以從 Storage Gateway 主控台予以刪除。當您刪除檔案共享時，會分離閘道與檔案共享所映射的 Amazon S3 儲存貯體。不過，不會刪除 S3 儲存貯體和其內容。

當您刪除檔案共享時，如果您的閘道正在將資料上傳至 S3 儲存貯體，則除非上傳所有資料，否則刪除程序不會完成。除非完全上傳資料，否則檔案共享具有 DELETING (正在刪除) 狀態。

如果您要完全上傳資料，請直接使用以下的 To delete a file share (刪除檔案共享) 程序。如果您不想要等待資料完全上傳，請參閱本主題中稍後的 To forcibly delete a file share (強制刪除檔案共享) 程序。

刪除檔案共享

1. 打開 Storage Gateway 主控台https://console.aws.amazon.com/storagegateway/home。
2. 選擇 File shares (檔案共享)，然後選擇您要刪除的檔案共享。
3. 針對 Actions (動作)，選擇 Delete file share (刪除檔案共享)。下列確認對話方塊隨即出現。



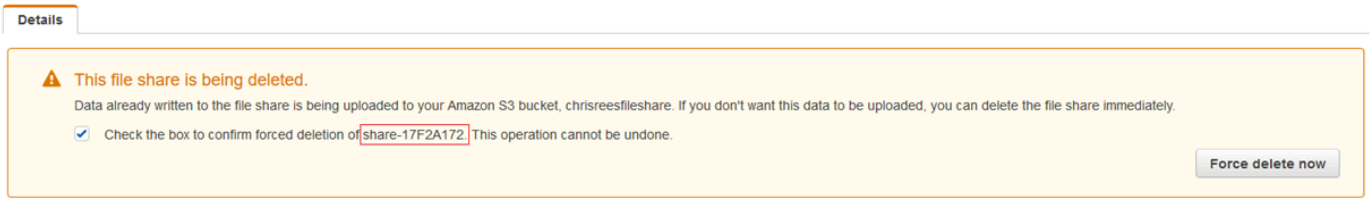
4. 在確認對話方塊中，選取您要刪除之一或多個檔案共享的核取方塊，然後選擇 Delete (刪除)。

在某些情況下，建議您在刪除檔案共享之前，不要等到上傳寫入至網路檔案系統 (NFS) 檔案共享上檔案的所有資料。例如，建議您故意捨棄已寫入但尚未上傳的資料。在另一個範例中，可能已刪除支援檔案共享的 Amazon S3 儲存貯體或物件，這表示已無法再上傳指定的資料。

在這些情況下，您可以使用AWS Management Console或`DeleteFileShare`API 操作。此操作會中止資料上傳程序。這麼做時，檔案共享會進入 FORCE_DELETING (正在強制刪除) 狀態。若要從主控台強制刪除檔案共享，請參閱下列程序。

強制刪除檔案共享

1. 打開 Storage Gateway 主控台https://console.aws.amazon.com/storagegateway/home。
2. 選擇 File shares (檔案共享)，然後選擇您要強制刪除的檔案共享，並等待幾秒鐘的時間。刪除訊息會顯示在 Details (詳細資訊) 標籤中。



> **Note**
>
> 您無法復原強制刪除操作。

3. 在 Details (詳細資訊) 標籤中所出現的訊息中，確認您要強制刪除的檔案共享 ID，並選取確認方塊，然後選擇 Force delete now (立即強制刪除)。

您也可以使用 DeleteFileShare API 操作來強制刪除檔案共享。

編輯 NFS 檔案共享的組態設定

您可以編輯 Amazon S3 存儲桶的存儲類、文件共享名稱、對象元數據、擠壓級別、導出為和自動緩存刷新設置。

> **Note**
>
> 您不能編輯現有文件共享以指向新的存儲桶或接入點，也不能修改 VPC 終端節點設置。您只能在建立新檔案共享時才能配置這些設定。

編輯檔案共享設定

1. 打開 Storage Gateway 主控台https://console.aws.amazon.com/storagegateway/home。
2. 選擇 File shares (檔案共享)，然後選擇您要更新的檔案共享。
3. 適用於動作，選擇編輯共享設定。
4. 執行下列其中一項或多項：
   - （可選）對於檔案共享名中，輸入檔案共享的新名稱。
   - 針對 Audit logs (稽核日誌)，選擇下列其中一項：
     - 選擇Disable logging (停用日誌記錄)以關閉日誌。
     - 選擇建立新的日誌組建立新的審核日誌。
     - 選擇使用現有的日誌組，然後從清單中選擇現有的稽核日誌。

     如需稽核的詳細資訊，請參閱瞭解文件網關審核日誌。

- （可選）對於來自 S3 的自動緩存刷新中，選中複選框並設置使用生存時間 (TTL) 刷新文件共享緩存的時間（以天、小時和分鐘為單位）。TTL 是自上次刷新以來的時間長度。TTL 間隔過後，訪問目錄會導致文件網關首先從 Amazon S3 存儲桶刷新該目錄的內容。
- （可選）對於檔案上傳通知中，選中 S3 文件網關已將文件完全上載到 S3 時收到通知的複選框。將建立時間以秒為單位控制在客户端寫入文件的最後一個時間點之後等待的秒數，然後再生成`ObjectUploaded`通知。由於客户端可以對文件進行許多小寫入，因此最好儘可能長地設置此參數，以避免在較短的時間內為同一文件生成多個通知。如需詳細資訊，請參閱 獲取文件上傳通知。

  > **Note**
  >
  > 此設置對象上傳到 S3 的時間沒有影響，僅影響通知的時間。

- 適用於新對象的存儲類下，選擇在 Amazon S3 儲存貯體中建立的新物件要使用的儲存體類別：
  - 選擇 S3 Standard，透過備援方式在多個可用區域 (不同地理位置) 存放經常存取的物件資料。如需 S3 標準儲存類別的詳細資訊，請參經常存取物件的儲存體方案中的Amazon Simple Storage Service 用户指南。
  - 選擇 S3 Intelligent-Tiering (S3 智慧型分層)，自動將資料移至最經濟實惠的儲存存取層，以最佳化儲存成本。如需 S3 智能分層儲存類別的詳細資訊，請參自動最佳化經常存取物件與不常存取物件的儲存體方案中的Amazon Simple Storage Service 用户指南。
  - 選擇 S3 Standard-IA，透過備援方式在多個可用區域 (不同地理位置) 存放不常存取的物件資料。如需 S3 標準 — IA 儲存類別的詳細資訊，請參不常存取物件的儲存體方案中的Amazon Simple Storage Service 用户指南。
  - 選擇 S3 One Zone-IA，在單一可用區域中存放不常存取的物件資料。如需 S3 單區域 — IA 儲存類別的詳細資訊，請參不常存取物件的儲存體方案中的Amazon Simple Storage Service 用户指南。
- 針對 Object metadata (物件中繼資料)，選擇您要使用的中繼資料：
  - 選擇 Guess MIME type (推測 MIME 類型)，啟用依據副檔名推測上傳物件的 MIME 類型。
  - 選擇 Give bucket owner full control (給予儲存貯體擁有者完整控制) 將完整控制權授予映射至檔案之網路檔案系統 (NFS) 或伺服器訊息區塊 (SMB) 檔案共享的 S3 儲存貯體擁有者。如需使用檔案共享存取另一個帳戶所擁有儲存貯體中之物件的詳細資訊，請參閱使用檔案共享進行跨賬户存取。
  - 如果您在儲存貯體上使用此檔案共享，而儲存貯體需要申請者或讀者支付存取的費用，而不是儲存貯體擁有者付費，請選擇 Enable requester pays (啟用申請者付款)。如需詳細資訊，請參閱申請者付款儲存貯體。

- 針對 Squash level (Squash 層級)，選擇您要用於 NFS 檔案共享的 squash 層級設定，然後選擇 Save (儲存)。

  > **Note**
  >
  > 您只能選擇 NFS 檔案共享的 squash 層級設定。SMB 檔案共享不會使用 squash 設定。

  可能的值如下：

  - Root squash (default) (Root squash (預設)) – 遠端超級使用者 (root) 的存取權會映射至 UID (65534) 和 GID (65534)。
  - No root squash (無 root squash) – 遠端超級使用者 (root) 會接收 root 的存取權。
  - All squash (所有 squash) – 所有使用者存取權都會映射至 UID (65534) 和 GID (65534)。

  squash 層級的預設值為 Root squash。
- 適用於將匯出為中，選擇檔案共享的選項。預設值為 Read-write (讀寫)。

  > **Note**
  >
  > 對於掛載在微軟客户端上的文件共享，如果選擇唯讀為了將匯出為時，您可能會看到有關讓您無法建立資料夾之意外錯誤的錯誤訊息。此錯誤訊息是已知的 NFS 第 3 版問題。您可以忽略此訊息。

5. 選擇 Save (儲存)。

編輯 NFS 檔案共享的元數據默認值

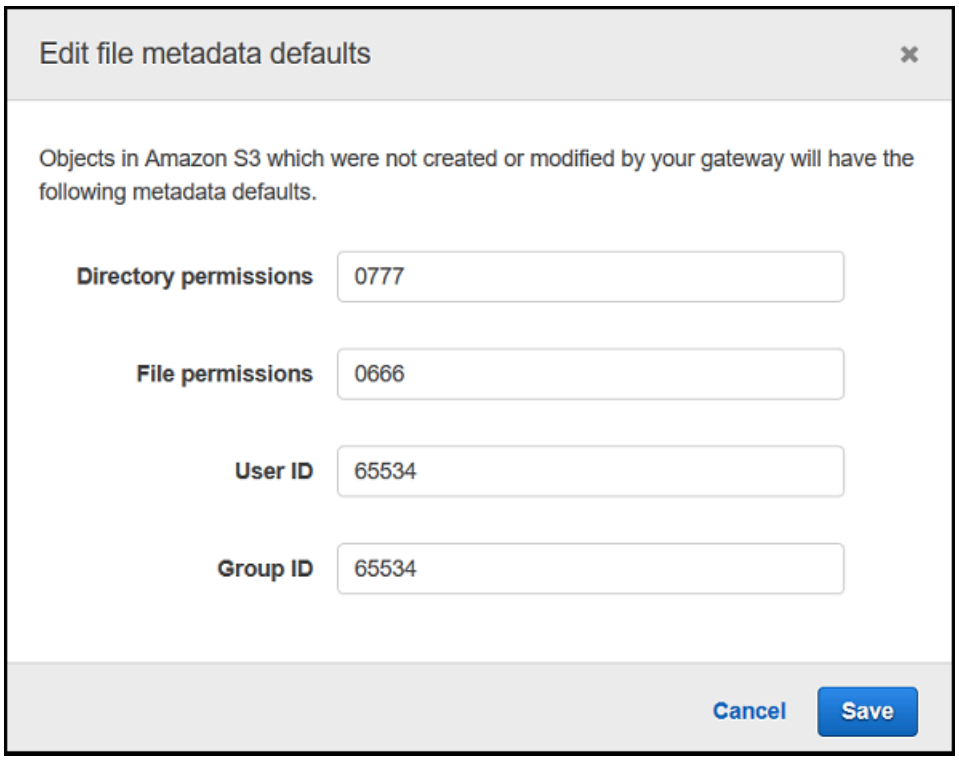
如果您未設定儲存貯體中檔案或目錄的中繼資料值，則 S3 檔案閘道會設定預設中繼資料值。這些值包含檔案和資料夾的 Unix 許可。您可以在 Storage Gateway 主控台上編輯元數據默認值。

當您的 S3 檔案閘道將檔案和資料夾存放至 Amazon S3 時，Unix 檔案許可會存放至物件中繼資料內。當您的 S3 檔案閘道探索到 S3 檔案閘道未存放的物件時，這些物件會獲指派預設 Unix 檔案許可。您可以在下表中找到預設 Unix 許可。

中繼資料	描述
目錄許可	Unix 目錄模式，格式為 "nnnn"。例如，"0666" 代表檔案共享內所有目錄的存取模式。預設值為 0777。
檔案許可	Unix 檔案模式，格式為 "nnnn"。例如，"0666" 代表檔案共享內的檔案模式。預設值為 0666。
使用者 ID	檔案共享中檔案的預設擁有者 ID。預設值為 65534。
群組 ID	檔案共享的預設群組 ID。預設值為 65534。

編輯中繼資料預設值

1. 打開 Storage Gateway 主控台https://console.aws.amazon.com/storagegateway/home。
2. 選擇 File shares (檔案共享)，然後選擇您要更新的檔案共享。
3. 針對 Actions (動作)，選擇 Edit file metadata defaults (編輯檔案中繼資料預設值)。
4. 在 Edit file metadata defaults (編輯檔案中繼資料預設值) 對話方塊中，提供中繼資料資訊，然後選擇 Save (儲存)。



編輯 NFS 檔案共享的存取設定

建議您變更 NFS 檔案共享的允許 NFS 用戶端設定。否則，網路上的任何用戶端都可以掛載至檔案共享。

編輯 NFS 存取設定

1. 打開 Storage Gateway 主控台https://console.aws.amazon.com/storagegateway/home。
2. 選擇 File shares (檔案共享)，然後選擇您要編輯的 NFS 檔案共享。
3. 針對 Actions (動作)，選擇 Edit share access settings (編輯共享存取設定)。
4. 在 中編輯允許的用户端對話方塊中，選擇新增項目，為您要允許的用户端提供 IP 位址或 CIDR 標記法，然後選擇Save (儲存)。

編輯網關的 SMB 設置

網關級 SMB 設置允許您為網關上的 SMB 文件共享配置安全策略、Active Directory 身份驗證、來賓訪問、本地組權限和文件共享可見性。

編輯網關級 SMB 設置

1. 打開 Storage Gateway 主控台https://console.aws.amazon.com/storagegateway/home。
2. 選擇閘道，然後選擇要為其編輯 SMB 設定的閘道。
3. 從動作下拉式選單中選擇編輯 SMB 設定，然後選擇您要編輯的設定。

如需詳細資訊，請參閱下列主題。

主題

- 為網關設置安全級別
- 使用 Active Directory 來驗證用户
- 提供訪客對文件共享的訪問權限
- 為您的網關配置本地羣組
- 設置文件共享可見性

為網關設置安全級別

使用 S3 檔案閘道時，您可以為閘道指定安全級別。透過指定此安全層級，您可以設定閘道應該需要伺服器訊息區塊 (SMB) 簽署或是 SMB 加密，或是要啟用 SMB 版本 1。

設定安全層級

1. 打開 Storage Gateway 主控台https://console.aws.amazon.com/storagegateway/home。
2. 選擇閘道，然後選擇要為其編輯 SMB 設定的閘道。
3. 從動作下拉式選單中選擇編輯 SMB 設定，然後選擇SMB 安全設定。
4. 對於 Security level (安全層級)，請選擇以下其中一項：

> **Note**
>
> 這個設定在 API 參考中稱為 `SMBSecurityStrategy`。
> 較高的安全層級會影響效能。

- 強制施行加密— 如果您選擇此選項，S3 檔案閘道只允許來自已啟用加密之 SMBv3 用户端的連線。對於處理敏感資料的環境，強烈建議使用此選項。此選項適用於 Microsoft Windows 8、Windows Server 2012 或更新版本的 SMB 用户端。

- 強制執行簽名— 如果您選擇此選項，S3 檔案閘道只允許來自已啟用簽署之 SMBv2 或 SMBv3 用户端的連線。此選項適用於 Microsoft Windows Vista、Windows Server 2008 或更新版本的 SMB 用户端。
- 通過用户議價— 如果您選擇此選項，請求會根據用户端所交涉的內容而建立。當您想要最大化環境中不同用戶端之間的相容性，建議使用此選項。

> **Note**
>
> 對於在 2019 年 6 月 20 日之前啟用的閘道，預設的安全層級是 Client negotiated (交涉的用戶端)。
> 對於在 2019 年 6 月 20 日 (含) 之後啟用的閘道，預設的安全層級是 Enforce encryption (強制加密)。

5. 選擇 Save (儲存)。

使用 Active Directory 來驗證用户

若要使用您的公司 Active Directory，讓使用者驗證 SMB 檔案共享的存取權，請使用 Microsoft AD 網域登入資料來編輯閘道的 SMB 設定。這麼做可讓您的閘道加入 Active Directory 網域，並允許網域成員存取 SMB 檔案共享。

> **Note**
>
> 使用AWS Directory Service，您可以在AWS 雲端。

任何可提供正確密碼的人員都會取得 SMB 檔案共享的訪客存取權。

您也可以在 SMB 檔案共享上啟用存取控制清單 (ACL)。如需如何啟用 ACL 的詳細資訊，請參閱使用 Microsoft Windows ACL 來控制 SMB 檔案共享的存取。

啟用 Active Directory 身份驗證

1. 打開 Storage Gateway 主控台https://console.aws.amazon.com/storagegateway/home。
2. 選擇閘道，然後選擇要為其編輯 SMB 設定的閘道。
3. 從動作下拉式功能表中，選擇編輯 SMB 設定，然後選擇Active Directory 設定。

4. 針對 Domain name (網域名稱)，提供您要閘道加入的網域。您可以使用網域的 IP 地址或組織單位來加入網域。組織單位是 Active Directory 分區，可持有使用者、群組、電腦和其他組織單位。

> **Note**
>
> 如果您的閘道無法加入 Active Directory 目錄，請試著使用 JoinDomain API 操作，使用目錄的 IP 地址來加入。

> **Note**
>
> 若閘道從未加入網域，Active Directory status (Active Directory 狀態) 會顯示 Detached (已卸除)。

5. 提供網域使用者和網域密碼，然後選擇 Save (儲存)。

   主控台之 Gateways (閘道) 區段頂端的訊息指出您的閘道已成功加入 AD 網域。

限制檔案共享對特定 AD 使用者和群組的存取

1. 在 Storage Gateway 主控台中，選擇您要限制其存取的檔案共享。
2. 從動作下拉式功能表中，選擇編輯文件共享訪問設置。
3. 在 中用户和組文件共享訪問部分中，選擇您的設置。

   適用於允許的用户和組，選擇新增允許的用者或者新增允許的羣組並輸入您要允許存取檔案共享的 AD 使用者或羣組。重複此過程以允許根據需要允許儘可能多的用户和組。

   適用於被拒絕的用户和組，選擇新增拒絕使用者或者新增拒絕的羣組並輸入您要拒絕檔案共享存取權的 AD 使用者或羣組。重複此過程可根據需要拒絕任意數量的用户和組。

> **Note**
>
> 所以此用户和組文件共享訪問部分僅在Active Directory處於選中狀態。
> 僅輸入 AD 使用者或群組名稱。網域名稱是由閘道加入之特定 AD 閘道的成員資格所暗示。
> 如果您未指定任何允許或拒絕的使用者或組，則任何已驗證的 AD 使用者都可以匯出檔案共享。

4. 當您完成新增項目時，請選擇 Save (儲存)。

提供訪客對文件共享的訪問權限

如果您只要提供訪客存取權，則 S3 檔案閘道不要求一定是 Microsoft AD 網域的一部分。您也可以使用身為 AD 網域成員的 S3 檔案閘道，來建立具有訪客存取權的檔案共享。您必須先變更預設密碼，才能使用訪客存取權來建立檔案共享。

變更訪客存取密碼

1. 打開 Storage Gateway 主控台https://console.aws.amazon.com/storagegateway/home。
2. 選擇閘道，然後選擇要為其編輯 SMB 設定的閘道。
3. 從動作下拉式功能表中，選擇編輯 SMB 設定，然後選擇訪客訪客訪問設定。
4. 適用於訪客密碼，提供密碼，然後選擇Save (儲存)。

為您的網關配置本地羣組

本地組設置允許您授予 Active Directory 用户或組對網關上 SMB 文件共享的特殊權限。

您可以使用本地組設置分配網關管理員權限。網關管理員可以使用共享文件夾 Microsoft 管理控制台管理單元強制關閉打開和鎖定的文件。

> **Note**
>
> 您必須添加至少一個網關管理員用户或組，然後才能將網關加入到 Active Directory 域。

分配網關管理員

1. 打開 Storage Gateway 主控台https://console.aws.amazon.com/storagegateway/home。
2. 選擇閘道，然後選擇要為其編輯 SMB 設定的閘道。
3. 從動作下拉式選單中選擇編輯 SMB 設定，然後選擇Local group 設定。
4. 在 中Local group 設定部分中，選擇您的設置。此部分僅針對使用活動目錄的文件共享顯示。

   適用於網關管理員中，添加要授予本地網關管理員權限的活動目錄用户和組。每行添加一個用户或組，包括域名。例如：**`corp\Domain Admins`**。要建立其他行，請選擇新的網關管理員。

> **Note**
>
> 編輯網關管理員斷開連接並重新連接所有 SMB 文件共享。

5. 選擇儲存變更，然後選擇繼續以確認顯示的警告消息。

設置文件共享可見性

當向用户發佈共享時，檔案共享可見性可以控制閘道上的共享。

設置文件共享可見性

1. 打開 Storage Gateway 主控台https://console.aws.amazon.com/storagegateway/home。
2. 選擇閘道，然後選擇要為其編輯 SMB 設定的閘道。
3. 從動作下拉式功能表中，選擇編輯 SMB 設定，然後選擇文件共享可見性設置。
4. 適用於可見度狀態中，選中該複選框可在向用户列出共享時顯示此網關上的共享。保持清除該複選框，以便在向用户列出共享時不顯示此網關上的共享。

編輯 SMB 檔案共享的設定

創建 SMB 文件共享後，您可以編輯 Amazon S3 存儲桶的存儲類、對象元數據、區分大小寫、基於訪問的枚舉、審核日誌、自動緩存刷新，以及作為文件共享的設置導出。

> **Note**
>
> 您不能編輯現有文件共享以指向新的存儲桶或接入點，也不能修改 VPC 終端節點設置。您只能在建立新檔案共享時才能配置這些設定。

若要編輯 SMB 檔案共享設定

1. 打開 Storage Gateway 主控台https://console.aws.amazon.com/storagegateway/home。
2. 選擇 File shares (檔案共享)，然後選擇您要更新的檔案共享。
3. 適用於動作，選擇編輯共享設定。
4. 執行下列其中一項或多項：

- （可選）對於檔案共享名中，輸入檔案共享的新名稱。
- 針對 Audit logs (稽核日誌)，選擇下列其中一項：
  - 選擇Disable logging (停用日誌記錄)以關閉日誌。
  - 選擇建立新的日誌組建立新的審核日誌。
  - 選擇使用現有的日誌組，然後從清單中選擇現有的稽核日誌。

  如需稽核的詳細資訊，請參閱瞭解文件網關審核日誌。
- （可選）對於從 S3 自動刷新緩存中，選中複選框並設置使用生存時間 (TTL) 刷新文件共享緩存的時間（以天、小時和分鐘為單位）。TTL 是自上次刷新以來的時間長度。TTL 間隔過後，訪問目錄會導致文件網關首先從 Amazon S3 存儲桶刷新該目錄的內容。
- （可選）對於檔案上傳通知中，選中 S3 文件網關已將文件完全上載到 S3 時收到通知的複選框。將建立時間以秒為單位控制在客户端寫入文件的最後一個時間點之後等待的秒數，然後再生成`ObjectUploaded`通知。由於客户端可以對文件進行許多小寫入，因此最好儘可能長地設置此參數，以避免在較短的時間內為同一文件生成多個通知。如需詳細資訊，請參閱 獲取文件上傳通知。

  > **Note**
  >
  > 此設置對象上傳到 S3 的時間沒有影響，僅影響通知的時間。

- 適用於新對象的存儲類下，選擇在 Amazon S3 儲存貯體中建立的新物件要使用的儲存體類別：
  - 選擇 S3 Standard，透過備援方式在多個可用區域 (不同地理位置) 存放經常存取的物件資料。如需 S3 標準儲存類別的詳細資訊，請參經常存取物件的儲存體方案中的Amazon Simple Storage Service 用户指南。
  - 選擇 S3 Intelligent-Tiering (S3 智慧型分層)，自動將資料移至最經濟實惠的儲存存取層，以最佳化儲存成本。如需 S3 智能分層儲存類別的詳細資訊，請參自動最佳化經常存取物件與不常存取物件的儲存體方案中的Amazon Simple Storage Service 用户指南。
  - 選擇 S3 Standard-IA，透過備援方式在多個可用區域 (不同地理位置) 存放不常存取的物件資料。如需 S3 標準 — IA 儲存類別的詳細資訊，請參不常存取物件的儲存體方案中的Amazon Simple Storage Service 用户指南。
  - 選擇 S3 One Zone-IA，在單一可用區域中存放不常存取的物件資料。如需 S3 單區域 — IA 儲存類別的詳細資訊，請參不常存取物件的儲存體方案中的Amazon Simple Storage Service 用户指南。
- 針對 Object metadata (物件中繼資料)，選擇您要使用的中繼資料：

- 選擇 Guess MIME type (推測 MIME 類型)，啟用依據副檔名推測上傳物件的 MIME 類型。
- 選擇 Give bucket owner full control (給予儲存貯體擁有者完整控制) 將完整控制權授予映射至檔案之網路檔案系統 (NFS) 或伺服器訊息區塊 (SMB) 檔案共享的 S3 儲存貯體擁有者。有關使用檔案共享存取另一個帳户擁有儲存貯體中物件的詳細資訊，請參閱使用檔案共享進行跨賬户存取。
- 如果您在儲存貯體上使用此檔案共享，而儲存貯體需要申請者或讀者支付存取的費用，而不是儲存貯體擁有者付費，請選擇 Enable requester pays (啟用申請者付款)。如需詳細資訊，請參閱申請者付款儲存貯體。

- 適用於將匯出為中，選擇檔案共享的選項。預設值為 Read-write (讀寫)。

> **Note**
>
> 對於掛載在 Microsoft Windows 客户端上的文件共享，如果選擇唯讀為了將匯出為時，您可能會看到有關讓您無法建立資料夾之意外錯誤的錯誤訊息。此錯誤訊息是已知的 NFS 第 3 版問題。您可以忽略此訊息。

- 對於 File/directory access controlled by (檔案/目錄存取控制者)，請選擇以下其中一項：
  - 選擇 Windows Access Control List (Windows 存取控制清單) 以在 SMB 檔案共享的檔案和資料夾上設定精確的許可。如需詳細資訊，請參閱 使用 Microsoft Windows ACL 來控制 SMB 檔案共享的存取。
  - 選擇 POSIX permissions (POSIX 許可) 來使用 POSIX 許可，以控制透過 NFS 或 SMB 檔案共享存放之檔案和目錄的存取權。

  如果您的身份驗證方法是Active Directory, 用於管理員用户/組中，輸入 AD 使用者和羣組的逗號分隔清單。如果您希望管理員使用者具有更新檔案共享中所有檔案和資料夾之 ACL 的權限，請這麼做。這些使用者和群組就會對檔案共享具有管理員權限。羣組前面必須加上@字符，例如`@group1`。
- 適用於區分大小寫中，選中該複選框以允許網關控制區分大小寫，或清除該複選框以允許客户端控制區分大小寫。

> **Note**
>
> - 如果選中此複選框，此設置將立即應用於新的 SMB 客户端連接。現有 SMB 客户端連接必須斷開與文件共享的連接，然後重新連接，設置才能生效。

- 如果要清除此複選框，此設置可能會導致您失去對名稱僅在其大小寫不同的文件的訪問權限。

- 適用於基於存取的枚舉中，選中複選框以使共享上的文件和文件夾僅對具有讀取訪問權限的用户可見。保持清除該複選框，以使共享上的文件和文件夾在目錄枚舉期間對所有用户可見。

> **Note**
>
> 基於訪問的枚舉是一個系統，它根據共享的訪問控制列表 (ACL) 過濾 SMB 文件共享上的文件和文件夾枚舉。

- 適用於機會鎖 (oplock)中，選擇下列其中一項：
  - 選擇Enabled允許文件共享使用機會鎖定來優化文件緩衝策略，這在大多數情況下可以提高性能，特別是在 Windows 上下文菜單方面。
  - 選擇已停用以防止使用機會主義鎖定。如果環境中的多個 Windows 客户端經常同時編輯相同的文件，則禁用機會鎖定有時會提高性能。

> **Note**
>
> 對於涉及訪問不同大小寫的同名文件的工作負載，建議不要對區分大小寫的共享啟用機會鎖定。

5. 選擇 Save changes (儲存變更)。

刷新 Amazon S3 儲存貯體中的物件

NFS 或 SMB 用户端執行檔案系統操作時，閘道會維護與檔案共享建立關聯之 S3 儲存貯體中物件的清查。您的閘道使用此快取清查，來降低 S3 請求的延遲和頻率。此操作不會將文件導入 S3 文件網關緩存存儲中。它僅更新緩存清單以反映 S3 存儲桶中對象清單中的更改。

若要重新整理檔案共享的 S3 儲存貯體，您可以使用 Storage Gateway 主控台、RefreshCache操作，或者AWS Lambda函數。

從主控台刷新 S3 儲存貯體中的物件

1. 打開 Storage Gateway 主控台https://console.aws.amazon.com/storagegateway/home。
2. 選擇 File shares (檔案共享)，然後選擇與您要重新整理之 S3 儲存貯體建立關聯的檔案共享。

3. 針對 Actions (動作)，選擇 Refresh cache (重新整理快取)。

   重新整理程序所需的時間取決於閘道上快取的物件數量，以及新增至 S3 儲存貯體或從中移除的物件數量。

使用AWS Lambda功能

1. 確定 S3 文件網關使用的 S3 存儲桶。
2. 檢查事件部分為空白。它稍後會自動填充。
3. 創建 IAM 角色，並允許 Lambda 的信任關係`lambda.amazonaws.com`。
4. 使用下列政策。

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

5. 從 Lambda 主控台建立 Lambda 函數。
6. 對您的 Lambda 任務使用以下函數。

```
import json
import boto3
client = boto3.client('storagegateway')
```

```
def lambda_handler(event, context):
    print(event)
    response = client.refresh_cache(
        FileShareARN='arn:aws:storagegateway:ap-southeast-2:672406774878:share/
share-E51FBD9C'
    )
    print(response)
    return 'Your FileShare cache has been refreshed'
```

7. 適用於執行角色中，選擇您建立的 IAM 角色。
8. 可選：為 Amazon S3 添加觸發器並選擇事件ObjectCreated或者ObjectRemoved。

> **Note**
>
> RefreshCache需要在啟動另一個進程之前完成一個進程。當您在存儲桶中創建或刪除許多對象時，性能可能會降低。因此，我們建議不要使用 S3 觸發器。相反，請使用以下描述的 Amazon CloudWatch 規則。

9. 在 CloudWatch 控制台上創建 CloudWatch 規則並添加計劃。一般來說，我們建議固定頻率30 分鐘。但是，您可以在大型 S3 存儲桶上使用 1—2 小時。
10. 為 CloudWatch 事件添加新觸發器，然後選擇剛剛創建的規則。
11. 保存您的 Lambda 配置。選擇 Test (測試)。
12. 選擇S3 把並根據您的要求自定義測試。
13. 測試應該會成功。如果沒有，請根據您的要求修改 JSON 並重新測試。
14. 打開 Amazon S3 控制台，並驗證您創建的事件和 Lambda 函數 ARN 存在。
15. 使用 Amazon S3 主控台將物件上傳至 S3 儲存貯體AWS CLI。

CloudWatch 主控台會產生類似如下的 CloudWatch 輸出。

```
{
    u'Records': [
        {u'eventVersion': u'2.0', u'eventTime': u'2018-09-10T01:03:59.217Z',
 u'requestParameters': {u'sourceIPAddress': u'MY-IP-ADDRESS'},
        u's3': {u'configurationId': u'95a51e1c-999f-485a-b994-9f830f84769f',
 u'object': {u'sequencer': u'00549CC2BF34D47AED', u'key': u'new/filename.jpeg'},
        u'bucket': {u'arn': u'arn:aws:s3:::MY-BUCKET', u'name': u'MY-GATEWAY-
NAME', u'ownerIdentity': {u'principalId': u'A3OKNBZ72HVPP9'}}, u's3SchemaVersion':
 u'1.0'},
```

```
        u'responseElements': {u'x-amz-id-2':
 u'76tiugjhvjfyriugiug87t890nefevbck0iA3rPU9I/s4NY9uXwtRL75tCyxasgsdgfsq+IhvAg5M=',
 u'x-amz-request-id': u'651C2D4101D31593'},
        u'awsRegion': u'MY-REGION', u'eventName': u'ObjectCreated:PUT',
 u'userIdentity': {u'principalId': u'AWS:AROAI5LQR5JHFHDFHDFHJ:MY-USERNAME'},
 u'eventSource': u'aws:s3'}
    ]
}
```

Lambda 調用會給您類似如下的輸出。

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

您的客户端上掛載的 NFS 共享將反映此更新。

> **Note**
>
> 對於在具有數百萬個對象的大型存儲桶中更新大型對象創建或刪除的緩存，更新可能需要數小時。

16. 使用 Amazon S3 主控台手動刪除物件或AWS CLI。
17. 查看客户端上裝載的 NFS 共享。驗證您的對象已消失（因為您的緩存刷新）。
18. 檢查您的 CloudWatch 日誌，查看事件中刪除的日誌`ObjectRemoved:Delete`。

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

```
}
```

> **Note**
>
> 對於 cron 作業或計劃任務，您的 CloudWatch 日誌事件為`u'detail-type': u'Scheduled Event'`。

重新整理快取只會起始重新整理操作。快取重新整理完成時，並不表示檔案重新整理已完成。若要判斷檔案重新整理操作是否已完成，在檢查閘道檔案共用上的新檔案之前，請使用 `refresh-complete` 通知。若要執行此動作，您可以透過 Amazon CloudWatch 事件訂您的RefreshCache操作完成。如需詳細資訊，請參閱 取得關於檔案操作的通知。

搭配 Amazon S3 檔案閘道使用 S3 物件鎖定

Amazon S3 檔案閘道支援存取已啟用 Amazon S3 物件鎖定的 S3 儲存貯體。Amazon S3 物件鎖定功能可讓您使用「單寫多讀」(WORM) 模式來存放物件。當您使用 Amazon S3 物件鎖定時，可以防止您的 S3 儲存貯體中的物件遭到刪除或覆寫。Amazon S3 物件鎖定可搭配物件版本控制來保護您的資料。

如果您啟用 Amazon S3 物件鎖定，仍可以修改物件。例如，可以透過 S3 檔案閘道上的檔案共享進行寫入、刪除或重新命名。當您以此方式修改物件時，S3 檔案閘道會放置物件的新版本，而不會影響舊版本（即鎖定的物件）。

例如，如果您使用 S3 檔案閘道 NFS 或 SMB 界面來刪除檔案，並且對應的 S3 物件已鎖定，閘道會放置 S3 刪除標記做為下一個版本的物件，並將原始的物件版本放在原處。同樣地，如果 S3 檔案閘道修改已鎖定物件的內容或中繼資料，即會上傳具有變更的物件新版本，但物件的原始鎖定版本將保持不變。

如需 Amazon S3 物件鎖定的詳細資訊，請參使用 S3 Object Lock 鎖定物件中的Amazon Simple Storage Service 用户指南。

瞭解文件共享狀態

每個檔案共享都有一個相關聯的狀態，可讓您一眼得知檔案共享的運作狀態。大多數時間，該狀態指出檔案共享正常運作，而且您不需要採取任何動作。在某些情況下，該狀態指出可能發生或許需要您採取動作的問題。

您可以在 Storage Gateway 主控台上查看檔案共享狀態。閘道中每個檔案共享的檔案共享狀態都會出現在 Status (狀態) 欄。正常運作之檔案共享的狀態為 AVAILABLE (可用)。

在下表中，您可以找到每個檔案共享狀態的描述，而且是您應該根據狀態採取動作時。檔案共享在使用中時，所有或大部分時間都應該具有 AVAILABLE (可用) 狀態。

狀態	意義
AVAILABLE (可用)	檔案共享的設定正確，而且可供使用。AVAILABLE (可用) 狀態為檔案共享的正常執行狀態。
CREATING (正在建立)	檔案共享正在建立，並且尚無法使用。CREATING (正在建立) 狀態是過渡的。無需採取任何動作。如果檔案共享停滯在此狀態，則原因可能是閘道 VM 已中斷與AWS。
UPDATING (正在更新)	正在更新檔案共享組態。如果檔案共享停滯在此狀態，則原因可能是閘道 VM 已中斷與AWS。
DELETING (正在刪除)	正在刪除檔案共享。在將所有資料都上傳至AWS。DELETING (正在刪除) 狀態是過渡的，而且不需要採取任何動作。
FORCE_DELETING (正在強制刪除)	正在強制刪除檔案共享。檔案共享會立即予以刪除，並上傳至AWS中止。FORCE_DELETING (正在強制刪除) 狀態是過渡的，而且不需要採取任何動作。
UNAVAILABLE (無法使用)	檔案共享處於狀況不良狀態。有些問題可能會導致檔案共享進入狀況不良狀態。例如，角色政策錯誤可能會造成此問題，或者檔案共享映射至不存在的 Amazon S3 儲存貯體時。解決造成狀況不良狀態的問題時，檔案會恢復為 AVAILABLE (可用) 狀態。

檔案共享最佳實務

在本節中，您可以找到檔案共享建立最佳實務的資訊。

主題

- 阻止多個檔案共享寫入您的 Amazon S3 儲存貯體
- 允許特定的 NFS 客户端掛載文件共享

阻止多個檔案共享寫入您的 Amazon S3 儲存貯體

當您建立檔案共享時，建議您設定 Amazon S3 儲存貯體，讓唯一個檔案共享可以寫入其中。如果您設定多個檔案共享要寫入的 S3 儲存貯體，則可能會發生無法預測的結果。若要避免發生這種狀況，請建立 S3 儲存貯體政策，來拒絕所有角色 (但用於檔案共享的角色除外) 以在儲存貯體中放置或刪除物件。然後將此政策連接至 S3 儲存貯體。

下列範例政策會拒絕所有角色，但已建立儲存貯體來寫入至 S3 儲存貯體的角色除外。拒絕 `s3:DeleteObject` 以外之所有角色的 `s3:PutObject` 和 `"TestUser"` 動作。此政策適用於 `"arn:aws:s3:::TestBucket/*"` 儲存貯體中的所有物件。

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

允許特定的 NFS 客户端掛載文件共享

建議您變更檔案共享的允許 NFS 用戶端設定。否則，網路上的任何用戶端都可以掛載檔案共享。如需如何編輯 NFS 用戶端設定的資訊，請參閱編輯 NFS 檔案共享的存取設定。

監視檔案閘道

您可以監控文件網關和相關資源AWS Storage Gateway使用 Amazon CloudWatch 指標和文件共享審核日誌。您還可以使用 CloudWatch 事件在檔案操作完成時收到通知。如需檔案閘道類型指標的相關資訊，請參閱監視檔案閘道。

主題

- 使用 CloudWatch 日誌組獲取文件網關運行狀況日誌
- 使用 Amazon CloudWatch 指標
- 取得關於檔案操作的通知
- 了解閘道指標
- 瞭解文件共享度量
- 瞭解文件網關審核日誌

使用 CloudWatch 日誌組獲取文件網關運行狀況日誌

您可以使用 Amazon CloudWatch Logs 取得有關檔案閘道運作狀態和相關資源的資訊。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 訂篩選條件，自動即時處理日誌資訊。如需詳細資訊，請參閱「」使用訂閱即時處理日誌資料中的Amazon CloudWatch 使用者指南。

例如，您可以設定 CloudWatch 日誌組來監控閘道，並在檔案閘道無法將檔案上傳至 Amazon S3 儲存貯體時收到通知。您可以在啟用閘道時或在啟用、啟動和運作及執行之後，設定羣組。如需有關如何在啟用閘道時設定 CloudWatch 日誌羣組的資訊，請參配置您的 Amazon S3 文件網關。如需 CloudWatch 日誌羣組的一般資訊，請參使用日誌群組、日誌串流進行工作中的Amazon CloudWatch 使用者指南。

以下是檔案閘道報告的錯誤範例。

```
{
    "severity": "ERROR",
    "bucket": "bucket-smb-share2",
    "roleArn": "arn:aws:iam::123456789012:role/my-bucket",
    "source": "share-E1A2B34C",
    "type": "InaccessibleStorageClass",
    "operation": "S3Upload",
```

```
    "key": "myFolder/myFile.text",
    "gateway": "sgw-B1D123D4",
    "timestamp": "1565740862516"
}
```

此錯誤意味着文件網關無法上傳對象myFolder/myFile.text到 Amazon S3，因為它已從 Amazon S3 標準儲存類別轉移到 S3 Glacier 靈活檢索或 S3 Glacier Deep Archive 儲存類別。

在前述閘道運作狀態日誌中，這些項目指定給定的資訊：

- source: share-E1A2B34C 表示發生此錯誤的檔案共享。
- "type": "InaccessibleStorageClass" 表示發生的錯誤類型。在此情況下，閘道嘗試將指定的物件上傳至 Amazon S3 或從 Amazon S3 讀取時，發生此錯誤。但是，在這種情況下，數據元已轉換為 Amazon S3 Glacier。"type" 的值可以是檔案閘道遇到的任何錯誤。如需可能的錯誤清單，請參閱疑難排解檔案閘道問題。
- "operation": "S3Upload"表示閘道嘗試將此物件上傳至 S3 時發生此錯誤。
- "key": "myFolder/myFile.text" 指出造成失敗的物件。
- gateway": "sgw-B1D123D4 表示發生此錯誤的檔案閘道。
- "timestamp": "1565740862516"表示錯誤發生的時間。

如需有關如何疑難排解和修正這些類型錯誤的詳細資訊，請參閱疑難排解檔案閘道問題。

激活閘道之後設定 CloudWatch 日誌

下列程序顯示如何在啟用閘道之後設定 CloudWatch 日誌羣組。

將 CloudWatch 日誌組設定為使用您的檔案閘道

1. 登入AWS Management Console，然後打開 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home。
2. 在導覽窗格中，選擇閘道，然後選擇您要為其設定 CloudWatch 日誌羣的閘道。
3. 適用於動作，選擇編輯閘道資訊。或者，在詳細資訊選項卡，在運行 Health 日誌和未啟用，選擇設定日誌羣組開啟Edit (編輯)客户網關名稱對話方塊。
4. 適用於閘道運作狀態日誌，選擇下列其中一項：
    - Disable logging (停用日誌記錄)（如果您不希望使用 CloudWatch 日誌組監視網關）。

- 建立新的日誌羣組創建新的 CloudWatch 日誌羣組。
- 使用現有的日誌羣組以使用已存在的 CloudWatch 日誌組。

  從現有日誌組列表。

5. 選擇 Save changes (儲存變更)。
6. 要檢視您的閘道的運作狀態日誌，請執行下列動作：

   1. 在導覽窗格中，選擇閘道，然後選擇您為其設定 CloudWatch 日誌羣的閘道。
   2. 選擇詳細資訊選項卡，在運行 Health 日誌，選擇CloudWatch Logs。所以此日誌羣組詳細資訊頁面將在 CloudWatch 控制台中打開。

將 CloudWatch 日誌羣組設定為使用您的檔案閘道

1. 登入AWS Management Console，然後打開 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home。
2. 選擇閘道，然後選擇您要為其設定 CloudWatch 日誌羣的閘道。
3. 適用於動作，選擇編輯閘道資訊。或者，在詳細資訊選項卡，旁邊的日誌, 在下方未啟用，選擇設定日誌羣組開啟編輯閘道資訊對話方塊。
4. 適用於閘道日誌，選擇使用現有的日誌羣組，然後選擇您要使用的日誌羣組。

   如果您沒有日誌群組，請選擇 Create new log group (建立新的日誌群組) 來建立日誌群組。系統會將您導向至 CloudWatch Logs 主控台，您可以在其中建立日誌羣組。如果您建立新的日誌羣組，請選擇重新整理按鈕，從下拉式清單中檢視新的日誌羣組。
5. 完成後，選擇 Save (儲存)。
6. 若要查看您閘道的日誌，請選擇閘道，然後選擇詳細資訊標籤。

如需如何疑難排解錯誤的詳細資訊，請參閱疑難排解檔案閘道問題。

使用 Amazon CloudWatch 指標

您可以使用AWS Management Console或 CloudWatch API。主控台會根據 CloudWatch API 的原始資料顯示一系列圖形。CloudWatch API 也可以通過AWS開發套件或者Amazon CloudWatch API工具。根據需求，您可能偏好使用顯示於主控台中的圖形或自 API 擷取的圖形。

無論您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 控制台中，您可以使用Gateway Metrics視圖選擇特定於網關的維。如需維度的詳細資訊，請參維度中的Amazon CloudWatch 使用者指南。
- 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，來識別要使用的檔案閘道。 閘道的輸送量和延遲資料是以閘道中的所有磁碟區為基礎。 每隔 5 分鐘免費自動提供資料。

閘道和檔案指標的使用方式類似其他服務指標的使用方式。您可以在以下列出的 CloudWatch 文件中找到一些最常見指標任務的討論：

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

取得關於檔案操作的通知

當您的檔案操作完成時，Storage Gateway 可以啟動 CloudWatch 事件：

- 您可以在閘道完成將檔案從檔案共享非同步上傳至 Amazon S3 時收到通知。使用NotificationPolicy參數請求檔案上傳通知。這將針對每個已完成的文件上傳到 Amazon S3 發送通知。如需詳細資訊，請參閱 獲取文件上傳通知。

- 您可以在閘道完成將您的工作檔案集非同步上傳至 Amazon S3 時收到通知。使用NotifyWhenUploadedAPI 操作請求工作文件集上傳通知。這會在工作檔案集中的所有檔案都已上傳至 Amazon S3 時，會發送通知。如需詳細資訊，請參閱 獲取工作文件集上傳通知。
- 您可以在閘道完成重新整理您 S3 儲存貯體的快取時收到通知。當您調用RefreshCache操作，請在操作完成時訂通知。如需詳細資訊，請參閱 獲取刷新緩存通知。

當您所請求的檔案操作完成時，Storage Gateway 會透過 CloudWatch Events 向您傳送通知。您可以設定 CloudWatch Events 透過事件目標 (例如 Amazon SNS、Amazon SQS 或AWS Lambda函數。例如，您可以設定 Amazon SNS 目標以將通知傳送給 Amazon SNS 消費者 (例如電子郵件或簡訊)。有關 CloudWatch 事件的信息，請參閱什麼是 CloudWatch 活動？

設定 CloudWatch Events 通知

1. 建立目標 (例如 Amazon SNS 主題或 Lambda 函數)，以在觸發您在 Storage Gateway 中請求的事件時呼叫。
2. 在 CloudWatch Events 主控台中建立規則，以根據 Storage Gateway 中的事件呼叫目標。
3. 在規則中，創建事件類型的事件模式。事件符合此規則模式時，即會觸發通知。
4. 選取目標，以及設定這些設定。

下列範例所顯示的規則會啟動所指定閘道中的指定事件類型，並在AWS區域。例如，您可以指定 `Storage Gateway File Upload Event` 做為事件類型。

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

如需如何使用 CloudWatch 事件觸發規則的資訊，請參建立由事件觸發的 CloudWatch 事件規則中的Amazon CloudWatch Events 使用者指南。

獲取文件上傳通知

您可以使用檔案上傳通知的兩個使用案例：

- 對於所上傳檔案在雲端中處理的自動化，您可以呼叫NotificationPolicy參數並返回一個通知 ID。當上傳之檔案的通知 ID 與 API 傳回的通知 ID 相同時，就會觸發通知。如果您比對此通知 ID 以追蹤您上傳的檔案清單，您可觸發在AWS當生成具有相同 ID 的事件時。
- 對於內容分發使用案例，您可以有兩個檔案閘道對應到相同 Amazon S3 存儲體。Gateway1 的檔案共享用户端可以將新的檔案上傳到 Amazon S3，而檔案會供 Gateway2 上的檔案共享用户端讀取。這些檔案會上傳至 Amazon S3，但不會對 Gateway2 顯示，因為它使用 Amazon S3 中檔案的本機快取版本。要使文件在網關 2 中可見，可以使用NotificationPolicy參數請求來自 Gateway1 的檔案上傳通知，以在上傳完成時通知您。然後，您可以使用 CloudWatch 事件自動發佈RefreshCache請求在 Gateway2 上檔案共享。當RefreshCache請求已完成，則新文件在網關 2 中可見。

Example 範例 — 檔案上傳通知

下列範例顯示當事件符合您建立的規則時，透過 CloudWatch 傳送給您的檔案上傳通知。此通知為 JSON 格式。您可以設定這個通知，以文字簡訊傳送至目標。`detail-type` 為 `Storage Gateway Object Upload Event`。

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

```
        "bucket-name": "my-bucket",
    }
}
```

欄位名稱	描述
version	IAM 政策的目前版本。
id	識別 IAM 政策的 ID。
詳細資訊類型	觸發傳送通知之事件的描述。
source	所以此AWS服務，它是請求和通知來源。
帳戶	的 IDAWS產生請求和通知的帳號。
time	請求將檔案上傳至 Amazon S3 的時間。
region	所以此AWS傳送請求和通知的來源區域。
resources	政策適用的儲存閘道資源。
物件大小	物件的大小 (位元組)。
修改時間	客户端修改文件的時間。
物件索引鍵	指向檔案的路徑。
event-type	觸發通知的 CloudWatch Events。
字首	S3 儲存貯體的前綴名稱。
bucket-name	S3 儲存貯體的名稱。

獲取工作文件集上傳通知

在兩種用例中，您可以使用工作文件集上傳通知：

- 對於所上傳檔案在雲端中處理的自動化，您可以呼叫NotifyWhenUploadedAPI 並返回一個通知 ID。當上傳之檔案的工作集時觸發的通知 ID 與 API 傳回的通知 ID 相同時，就會觸發通知。如果您比對此通知 ID 以追蹤您上傳的檔案清單，您可觸發在AWS當生成具有相同 ID 的事件時。
- 對於內容分發使用案例，您可以有兩個檔案閘道對應到相同 Amazon S3 存儲體。Gateway1 的檔案共享用户端可以將新的檔案上傳到 Amazon S3，而檔案會供 Gateway2 上的檔案共享用户端讀取。這些檔案會上傳至 Amazon S3，但不會對 Gateway2 顯示，因為它使用 S3 中檔案的本機快取版本。要使文件在網關 2 中可見，請使用NotifyWhenUploadedAPI 操作請求來自 Gateway1 的檔案上傳通知，以在上傳完成時通知您。然後，您可以使用 CloudWatch 事件自動發佈RefreshCache請求在 Gateway2 上檔案共享。當RefreshCache請求已完成，則新的檔案會顯示在 Gateway2 中。此操作不會將文件導入文件網關緩存存儲中。它僅更新緩存清單以反映 S3 存儲桶中對象清單中的更改。

Example 示例-工作文件集上傳通知

下列範例顯示當事件符合您建立的規則時，透過 CloudWatch 傳送給您的工作檔案集上傳通知。此通知為 JSON 格式。您可以設定這個通知，以文字簡訊傳送至目標。`detail-type` 為 `Storage Gateway File Upload Event`。

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

欄位名稱	描述
version	IAM 政策的目前版本。
id	識別 IAM 政策的 ID。
詳細資訊類型	觸發傳送通知之事件的描述。
source	所以此AWS服務，它是請求和通知來源。
帳戶	的 IDAWS產生請求和通知的帳號。
time	請求將檔案上傳至 Amazon S3 的時間。
region	所以此AWS傳送請求和通知的來源區域。
resources	政策適用的 Storage Gateway 資源。
event-type	觸發通知的 CloudWatch Events。
notification-id	傳送的通知隨機產生的 ID。此 ID 使用 UUID 格式。這是呼叫 `NotifyWhenUploaded` 時傳回的通知 ID。
request-received	閘道收到 `NotifyWhenUploaded` 請求的時間。
completed	工作集中的所有檔案已上傳到 Amazon S3 時。

獲取刷新緩存通知

針對重新整理快取通知使用案例，您可以有兩個檔案閘道映射至相同 Amazon S3 儲存貯體，而 Gateway1 的 NFS 用户端會將新的檔案上傳至 S3 儲存貯體。除非您重新整理快取，否則這些檔案將會上傳至 Amazon S3，但不會出現在 Gateway2 中。這是因為 Gateway2 使用 Amazon S3 中檔案的本機快取版本。重新整理快取完成時，建議您在 Gateway2 中使用檔案執行某項作業。大型檔案可能需要一段時間才會顯示在 Gateway2 中，因此您可能需要在快取重新整理完成時收到通知。您可以請求來自 Gateway2 的重新整理快取通知，以在所有檔案顯示於 Gateway2 時通知您。

Example 範例 — 重新整理快取通知

下列範例顯示當事件符合您建立的規則時，透過 CloudWatch 傳送給您的重新整理快取通知。此通知為 JSON 格式。您可以設定這個通知，以文字簡訊傳送至目標。`detail-type` 為 `Storage Gateway Refresh Cache Event`。

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

欄位名稱	描述
version	IAM 政策的目前版本。
id	識別 IAM 政策的 ID。
詳細資訊類型	觸發傳送通知之事件類型的描述。
source	所以此AWS服務，作為請求和通知來源。
帳戶	的 IDAWS產生請求和通知的帳號。
time	請求重新整理工作集中之檔案的時間。

欄位名稱	描述
region	所以此AWS傳送請求和通知的來源區域。
resources	政策適用的 Storage Gateway 資源。
event-type	觸發通知的 CloudWatch Events。
notification-id	傳送的通知隨機產生的 ID。此 ID 使用 UUID 格式。這是呼叫 `RefreshCache` 時傳回的通知 ID。
started	閘道收到`RefreshCache` 請求並開始重新整理刷新。
completed	工作集的重新整理完成的時間。
folderList	在快取中重新整理、以逗號分隔的資料夾路徑清單。預設為 ["/"]。

了解閘道指標

下表說明 S3 檔案閘道的指標。每個閘道都有一組相關聯的指標。有些閘道專屬指標與特定檔案共享專屬指標的名稱相同。這些指標代表相同類型的測量，但範圍為閘道而非檔案共享。

一律在使用特定指標時指定您要使用閘道還是檔案共享。具體而言，使用閘道指標時，您必須指定`Gateway Name`針對您想要檢視其指標資料的閘道。如需詳細資訊，請參閱 使用 Amazon CloudWatch 指標。

下表說明指標，您可以用於取得S3 檔案閘道s。

指標	描述
`AvailabilityNotifications`	此指標會報告期間閘道產生的可用相關運作狀態通知數目。 個單位: 計數
`CacheFileSize`	此指標會追蹤 Gateway Cache 中檔案的大小。

指標	描述
	將此指標與Average統計數據來測量網關緩存中文件的平均大小。將此指標與Max統計數據來測量網關緩存中文件的最大大小。 個單位: 位元組
CacheFree	此指標會報告閘道快取中的可用字節數。 個單位: 位元組
CacheHitPercent	來自閘道的應用程式讀取操作百分比。報告期間結束時會取樣。 當沒有來自閘道的應用程式讀取操作時，此指標會回報 100%。 個單位: 百分比
CachePercentDirty	尚未保存到的閘道快取總百分比AWS。報告期間結束時會取樣。 個單位: 百分比
CachePercentUsed	所使用的網關緩存存儲的總百分比。報告期間結束時會取樣。 個單位: 百分比
CacheUsed	這個指標會報告閘道快取中的使用字節數。 個單位: 位元組

指標	描述
CloudBytesDownloaded	閘道上傳至的位元組總數AWS在本報告所述期間. 使用此指標搭配 Sum 統計資料可測量輸送量，搭配 Samples 統計資料可測量每秒輸入/輸出操作數目 (IOPS)。 個單位: 位元組
CloudBytesUploaded	閘道從下載的位元組總數AWS在本報告所述期間. 使用此指標搭配 Sum 統計資料可測量輸送量，搭配 Samples 統計資料可測量 IOPS。 個單位: 位元組
FilesFailingUpload	這個指標會追蹤未能上傳到AWS。這些文件將生成包含有關該問題的詳細信息的運行狀況通知。 將此指標與Sum統計數據來顯示當前無法上傳到AWS。 個單位: 計數
FileSharesUnavailable	此度量提供此網關上的文件共享數，這些文件共享位於Unavailable狀態。 如果此指標報告任何文件共享不可用，則網關可能存在問題，可能會導致工作流程中斷。建議您在此指標會報告非零值時建立警報。 個單位: 計數
FilesRenamed	這個指標會追蹤報告期間重命名的檔案數量。 個單位: 計數

指標	描述
HealthNotifications	此指標報告報告期間由此網關生成的運行狀況通知的數量。 個單位: 計數
IoWaitPercent	此指標會報 CPU 等待本機磁碟回應的時間百分比。 個單位: 百分比
MemTotalBytes	此指標報告網關上的內存總量。 個單位: 位元組
MemUsedBytes	此指標報告網關上已使用的內存量。 個單位: 位元組
NfsSessions	這個指標會報告閘道上作用中的 NFS 工作階段數量。 個單位: 計數
RootDiskFreeBytes	此指標會報告閘道根磁盤上的可用字節數。 如果此指標報告空閒小於 20 GB，則應增加根磁盤的大小。 個單位: 位元組
S3GetObjectRequestTime	此指標報告網關完成 S3 獲取對象請求的時間。 個單位: 毫秒
S3PutObjectRequestTime	此指標報告網關完成 S3 放置對象請求的時間。 個單位: 毫秒

指標	描述
S3UploadPartRequestTime	此指標報告網關完成 S3 上傳分段請求的時間。 個單位: 毫秒
SmbV1Sessions	這個指標會報告閘道上作用中的 SMBv1 工作階段數量。 個單位: 計數
SmbV2Sessions	這個指標會報告閘道上作用中的 SMBv2 工作階段數量。 個單位: 計數
SmbV3Sessions	這個指標會報告閘道上作用中的 SMBv3 工作階段數量。 個單位: 計數
TotalCacheSize	此指標報告高速緩存的總大小。 個單位: 位元組
UserCpuPercent	此度量報告用於網關處理的時間百分比。 個單位: 百分比

瞭解文件共享度量

您可以在以下找到涵蓋檔案共享之 Storage Gateway 指標的相關資訊。每個檔案共享都有一組相關聯的指標。有些檔案共享專屬指標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，但範圍改為檔案共享。

一律在使用指標之前指定您要使用閘道還是檔案共享指標。明確而言，當使用檔案共享指標時，您必須指定 `File share ID`，識別您要檢視指標的檔案共享。如需詳細資訊，請參閱 使用 Amazon CloudWatch 指標。

下表說明您可以用於取得檔案共享資訊的 Storage Gateway 指標。

指標	描述
CacheHitPercent	來自快取服務之檔案共享的應用程式讀取操作百分比。報告期間結束時會取樣。 當沒有來自檔案共享的應用程式讀取操作時，此指標會回報 100%。 個單位: 百分比
CachePercentDirty	尚未保存到的閘道快取整體百分比中檔案共享的比重AWS。報告期間結束時會取樣。 使用CachePercentDirty 指標，以查看尚未保存到的閘道快取整體百分比AWS。 個單位: 百分比
CachePercentUsed	閘道快取儲存體整體使用百分比中檔案共享的比重。報告期間結束時會取樣。 使用 CachePercentUsed 指標可檢視閘道快取儲存體的整體使用百分比。 個單位: 百分比
CloudBytesUploaded	閘道上傳至的位元組總數AWS在本報告所述期間. 使用此指標搭配 Sum 統計資料可測量輸送量，搭配 Samples 統計資料可測量 IOPS。 個單位: 位元組
CloudBytesDownloaded	閘道從下載的位元組總數AWS在本報告所述期間. 使用此指標搭配 Sum 統計資料可測量輸送量，搭配 Samples 統計資料可測量每秒輸入/輸出操作數目 (IOPS)。

指標	描述
	個單位: 位元組
ReadBytes	報告期間針對檔案共享，從您現場部署應用程式讀取的位元組總數。 使用此指標搭配 Sum 統計資料可測量輸送量，搭配 Samples 統計資料可測量 IOPS。 個單位: 位元組
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 統計資料可測量輸送量，搭配 Samples 統計資料可測量 IOPS。 個單位: 位元組

瞭解文件網關審核日誌

Amazon S3 檔案閘道 (S3 檔案閘道) 稽核日誌可提供您有關使用者存取檔案共享內的檔案和資料夾的詳細資訊。您可以使用它們來監視使用者活動，並在識別不當的活動模式時採取行動。

操作

下表說明檔案閘道稽核日誌存取操作。

操作名稱	定義
讀取資料	讀取檔案的內容。
寫入資料	更改檔案的內容。
建立	建立新的檔案或資料夾。
重新命名	重新命名現有的檔案或資料夾。
Delete	刪除檔案或資料夾。

操作名稱	定義
寫入屬性	更新檔案或資料夾中繼資料 (ACL、擁有者、群組、許可)。

屬性

下表說明 S3 檔案閘道稽核日誌存取屬性。

屬性	定義
accessMode	物件的許可設定。
accountDomain （僅限中小型企業）	用戶端帳戶所屬的 Active Directory (AD) 網域。
accountName （僅限中小型企業）	用戶端的活動目錄 (動態) 使用者名稱。
bucket	S3 儲存貯體名稱。
clientGid (僅 NFS)	訪問對象的用戶羣標識。
clientUid (僅 NFS)	訪問物件的用戶的識別碼。
ctime	由用戶端設定修改物件內容或中繼資料的時間。
groupId	物件的羣組擁有者的識別碼。
fileSizeInBytes	由用戶端在檔案建立時設定的檔案大小 (以位元組為單位)。
gateway	Storage Gateway ID。
mtime	由用戶端設定修改物件內容的時間。
newObjectName	新物件重新命名後的完整路徑。
objectName	物件的完整路徑。
objectType	定義物件是檔案還是資料夾。

屬性	定義
operation	物件存取操作的名稱。
ownerId	物件擁有者的識別碼。
securityDescriptor （僅限中小型企業）	以 SDDL 格式顯示物件上設定的判別式存取控制清單 (DACL)。
shareName	正在存取的共用名稱。
source	正在稽核的檔案共享 ID。
sourceAddress	檔案共享用用戶端機器的 IP 地址。
status	操作的狀態。只會記錄成功 (會記錄失敗，但由許可遭拒所產生的失敗除外)。
timestamp	根據閘道的作業系統時間戳記執行操作的時間。
version	稽核日誌格式的版本。

每個操作記錄的屬性

下表說明在每個檔案存取操作中記錄的 S3 檔案閘道稽核日誌屬性。

	讀取資料	寫入資料	建立資料夾	建立檔案	重命名文件/文件夾	刪除文件/文件夾	寫入屬性（更改 ACL-僅中小型企業)	寫入屬性（填寫）	寫入屬性	寫入屬性 (chgrp)
access e			X	X					X	

	讀取資料	寫入資料	建立資料夾	建立檔案	重命名文件/文件夾	刪除文件/文件夾	寫入屬性（更改ACL-僅中小型企業)	寫入屬性（填寫）	寫入屬性	寫入屬性(chgrp)
accoun main（僅限中小型企業）	X	X	X	X	X	X	X	X	X	X
accoun me（僅限中小型企業）	X	X	X	X	X	X	X	X	X	X
bucket	X	X	X	X	X	X	X	X	X	X
client (僅NFS)	X	X	X	X	X	X		X	X	X
client (僅NFS)	X	X	X	X	X	X		X	X	X
ctime			X	X						
groupI			X	X						

	讀取資料	寫入資料	建立資料夾	建立檔案	重命名文件/文件夾	刪除文件/文件夾	寫入屬性（更改ACL-僅中小型企業)	寫入屬性（填寫）	寫入屬性	寫入屬性(chgrp)
fileSinBytes				X						
gatewa	X	X	X	X	X	X	X	X	X	X
mtime			X	X						
newObjName					X					
objecte	X	X	X	X	X	X	X	X	X	X
objecte	X	X	X	X	X	X	X	X	X	X
operat	X	X	X	X	X	X	X	X	X	X
ownerI			X	X				X		
securiescrip（僅限中小型企業）							X	X		

	讀取資料	寫入資料	建立資料夾	建立檔案	重命名文件/文件夾	刪除文件/文件夾	寫入屬性（更改ACL-僅中小型企業)	寫入屬性（填寫）	寫入屬性	寫入屬性(chgrp)
shareN	X	X	X	X	X	X	X	X	X	X
source	X	X	X	X	X	X	X	X	X	X
source ress	X	X	X	X	X	X	X	X	X	X
status	X	X	X	X	X	X	X	X	X	X
timest	X	X	X	X	X	X	X	X	X	X
versio	X	X	X	X	X	X	X	X	X	X

維護您的閘道

維護您的閘道包含像是設定快取儲存體及上傳緩衝空間，以及進行一般性維護工作以維護您閘道的效能等任務。這些任務對於所有閘道類型而言非常常見。

主題

關閉您的閘道 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。針對檔案閘道，您只需要關機 VM。雖然本節著重於使用儲存閘道管理主控台啟動和停止閘道，但您也可以使用 VM 本機主控台或儲存閘道 API 啟動和停止閘道。當您開啟 VM 的電源時，請記得重新啟動閘道。

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。針對檔案閘道，您只需要關機 VM。您未關機閘道。雖然本節著重於使用儲存閘道管理主控台啟動和停止閘道，但您也可以使用 VM 本機主控台或儲存閘道 API 啟動和停止閘道。當您開啟 VM 的電源時，請記得重新啟動閘道。

- 閘道 VM 本機主控台 — 請參在本機主控台上執行維護任務。
- Storage Gateway API — 請參閱ShutdownGateway

管理 Storage Gateway 的本地磁盤

閘道虛擬機器 (VM) 使用您現場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 磁碟區做為本機磁碟。

主題

- 決定本地磁盤存儲量
- 確定要分配的緩存存儲大小
- 新增快取儲存
- 將臨時存儲與 EC2 網關結合使用

決定本地磁盤存儲量

您希望為閘道配置的磁碟數目及大小皆由您決定。閘道需要下列額外的儲存體：

檔案閘道需要至少一個磁碟，用來做為快取。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	描述	閘道類型
快取儲存體	快取儲存體做為現場部署耐久存放區，存放等待上傳至 Amazon S3 或文件系統的資料。	• 檔案閘道

> **Note**
>
> 基礎實體儲存體資源會在 VMware 中以資料存放區表示。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) 時，您可選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。當使用只有一個底層物理磁碟支援的資料存放區時，會在用作兩個快取儲存體的備份時，可能會在某些情況下導致性能不佳。這在備份為效能較差的 RAID 組態 (例如 RAID1) 時也相同。

在您閘道的初始設定和部署完成後，您可以透過新增快取儲存磁碟來調整本機儲存體。

確定要分配的緩存存儲大小

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。快取儲存體做為現場部署耐久存放區，存放等待上傳至 Amazon S3 或文件系統的資料。如需如何估計您快取儲存體大小的詳細資訊，請參閱管理 Storage Gateway 的本地磁盤。

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

新增快取儲存

隨著您應用程式的需求變更，您可以增加閘道的快取儲存體容量。您可以新增更多快取儲存容量至您的閘道，而無須中斷現有的閘道功能。在您新增更多存放容量時，您的閘道 VM 會同時維持開啟狀態。

> **Important**
>
> 新增快取至現有的閘道時，請務必在您的主機 (虛擬化管理程序或 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儲存體，則請勿變更現有磁碟的大小。請不要移除已配置為快取儲存體的快取磁碟。

下列程序顯示為您的閘道設定或快取儲存體的方式。

新增及設定或緩存儲體

1. 在您的主機中佈建新的磁碟 (虛擬化管理程序或 Amazon EC2 執行個體)。如需如何在虛擬化管理程序中佈建磁碟的資訊，請參閱虛擬化管理程序使用者手冊。您可以將此磁盤設為緩存儲體。
2. Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home。
3. 在導覽窗格中，選擇 Gateways (網際網路閘道)。
4. 在 Actions (動作) 選單中，選擇 Edit local disks (編輯本機磁碟)。
5. 在 Edit local disk (編輯本機磁碟) 對話方塊中，識別您佈建的磁碟，並決定您希望用作快取儲存體的磁碟。

   若您的磁碟未顯示，請選擇 Refresh (重新整理) 按鈕。
6. 選擇 Save (儲存) 以儲存您的組態設定。

將臨時存儲與 EC2 網關結合使用

本節說明當您選取暫時性磁碟做為閘道快取的儲存空間時，為防止資料遺失所需採取的步驟。

暫時磁碟為 Amazon EC2 執行個體提供暫時的區塊層級儲存空間。暫時磁碟適合當做經常變更資料的暫時儲存體，例如閘道快取儲存體中的資料。當您使用 Amazon EC2 Amazon Machine Image 來啟動您的閘道，且您選擇的執行個體類型支援暫時性儲存，則系統會自動列出磁碟，您可以選擇其中一個

磁碟來存放閘道快取中的資料。如需詳細資訊，請參閱「」Amazon EC2 執行個體存放區中的Amazon EC2 Linux 執行個體使用者指南。

應用程式寫入磁碟會同步存放在快取中，並會非同步上傳至 Amazon S3 中的耐用儲存體。若存放在暫時性儲存中的資料因 Amazon EC2 執行個體在上傳完成前停止而遺失，仍在快取中並且還未上傳至 Amazon S3 的資料將可能遺失。重新啟動或停止裝載您閘道的 EC2 執行個體之前，請依照下列步驟執行，即可避免這類資料遺失。

> **Note**
>
> 如果您正使用暫時性儲存，且停止然後啟動閘道，此閘道將永久離線。會發生此情況是因為已替換實體儲存磁碟。此問題沒有解決方法，因此您必須刪除此閘道，並在新的 EC2 執行個體上啟用新閘道。

下列程序的步驟專用於檔案閘道。

避免使用暫時性磁碟的檔案閘道中發生資料遺失

1. 停止正在寫入檔案共享的所有處理程序。
2. 訂閱以接收來自 CloudWatch 事件的通知。如需相關資訊，請參閱 取得關於檔案操作的通知。
3. 呼叫上傳 API 時通知當直到暫時性儲存遺失為止，寫入的資料已被持久地儲存在 Amazon S3 中儲存在時收到通知。
4. 等待 API 完成，您會收到通知 ID。

   您收到具有相同通知 ID 的 CloudWatch 事件。
5. 確認您檔案共享的 `CachePercentDirty` 指標為 0。這可確認所有資料已寫入 Amazon S3。如需檔案共享指標的詳細資訊，請參閱瞭解文件共享度量。
6. 您現在可以重新啟動或停止檔案閘道，而不具遺失任何資料的風險。

管理您的 Amazon S3 文件閘道頻寬

您可以將網關的上傳吞吐量限製為AWS，以控制閘道所用的網路頻寬。默認情況下，激活的閘道沒有速率限制。

您可以使用AWS Management Console，一個AWS軟體開發套件 (SDK) 或AWS Storage GatewayAPI（請參閱更新帶寬限制時間表中的AWSStorage Gateway API 參考。）。使用帶寬速

率限制計劃，您可以將限制配置為在一天或一週內自動更改。如需詳細資訊，請參閱 使用 Storage Gateway 控制台查看和編輯網關的帶寬速率限制計劃。

> **Note**
>
> Amazon FSX 文件網關類型目前不支持配置帶寬速率限制和時間表。

主題

使用 Storage Gateway 控制台查看和編輯網關的帶寬速率限制計劃

本節說明如何檢視和編輯閘道的頻寬速率限制時間表。

若要查看和編輯頻寬速率限制排程

1. Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home。
2. 在左側導覽窗格中，選擇閘道，然後選擇您要管理的閘道。
3. 適用於動作，選擇編輯帶寬速率限制計劃。

   網關的當前帶寬速率限制計劃顯示在編輯帶寬速率限制計劃(憑證已建立！) 頁面上的名稱有些許差異。默認情況下，新網關沒有定義的帶寬速率限制。
4. (選用) 選擇添加新的帶寬速率限制將新的可配置間隔添加到計劃中。對於您新增的每個間隔，輸入下列資訊：

   - 上傳率— 輸入上傳速率限制，以兆位每秒 (Mbps) 為單位。最小值為 100 Mbps。
   - 週中的日— 選擇要應用時間間隔的日期或每週中的天數。您可以在工作日（星期一至週五）、週末（星期六和星期日）、一週中的每一天或每週一個特定日期應用時間間隔。要在所有日子和任何時間均勻、持續地應用帶寬速率限制，請選擇無排程。
   - 開始時間— 輸入帶寬間隔的開始時間，使用 HH: MM 格式和網關的 UTC 時區偏移量。

> **Note**
>
> 帶寬速率限制間隔從您在此指定的分鐘開始。

- 結束時間— 輸入帶寬間隔的結束時間，使用 HH: MM 格式和網關的 GMT 時區偏移量。

> **Important**
>
> 帶寬速率限制間隔在此處指定的分鐘結束時結束。要計劃在一小時結束時結束的時間間隔，請輸入**59**。
> 要安排連續的連續間隔，在小時開始時進行轉換，而不間斷時間間隔，請輸入**59**作為第一個間隔的結束分鐘。Enter**00**作為後續時間間隔的開始分鐘。

5. (選用) 根據需要重複之前的步驟，直到您的頻寬速率限制計劃完成。如果需要從計劃中刪除時間間隔，請選擇Remove (移除)。

> **Important**
>
> 帶寬速率限制間隔不能重疊。時間間隔的開始時間必須發生在前一個時間間隔的結束時間之後，並在以下時間間隔的開始時間之前。

6. 完成時，請選擇儲存變更。

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這些限制，例如使用排程的任務。下列範例示範如何使用AWS SDK for Java。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「」入門中的AWS SDK for Java開發人員指南。

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。若要使用此示例代碼，您必須提供服務端點、閘道 Amazon Resource Name (ARN)，以及上傳限制。的清單AWS可與 Storage Gateway 一起使用的服務終端節點，請參閱AWS Storage Gateway端點和配額中的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.
UpdateBandwidthRateLimitScheduleRequest;
   import com.amazonaws.services.storagegateway.model.
UpdateBandwidthRateLimitScheduleReturn;

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

   public class UpdateBandwidthExample {

       public static AWSStorageGatewayClient sgClient;

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

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

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

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

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

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

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

       }

       private static void UpdateBandwidth(String gatewayArn, long uploadRate, long
downloadRate) {
           try
           {
               BandwidthRateLimit bandwidthRateLimit = new
BandwidthRateLimit(downloadRate, uploadRate);
```

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

                UpdateBandwidthRateLimitScheduleReturn
updateBandwidthRateLimitScheuduleResponse =
sgClient.UpdateBandwidthRateLimitSchedule(updateBandwidthRateLimitScheduleRequest);

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

使用更新閘道頻寬速率限制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這些限制，例如使用排程的任務。下列範例示範如何使用AWS.NET 軟體開發套件 (SDK)。若要使用範例程式碼，您應該熟悉如何執行 .NET 主控台應用程式。如需詳細資訊，請參閱「」入門中的AWS SDK for .NET開發人員指南。

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。若要使用此示例代碼，您必須提供服務端點、閘道 Amazon Resource Name (ARN)，以及上傳限制。的清單AWS可與 Storage Gateway 一起使用的服務終端節點，請參閱AWS Storage Gateway端點和配額中的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 = 100 * 1024 * 1024;  // Bits per second, minimum
 100 Megabits/second

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

                UpdateBandwidth(gatewayARN, uploadRate, null);

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

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

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

使用更新閘道頻寬速率限制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這些限制，例如使用排程的任務。下列範例示範如何使用AWS Tools for Windows PowerShell。若要使用範例程式碼，您應該熟悉如何執行 PowerShell 指令碼。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，您必須提供服務端點、閘道 Amazon Resource Name (ARN) 和上傳限制。

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

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


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

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

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

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

```
                                        -BandwidthRateLimitInterval
@($bandwidthRateLimitInterval)

   $schedule =  Get-SGBandwidthRateLimitSchedule -GatewayARN $gatewayARN

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

使用 AWS Storage Gateway 主控台管理閘道更新

Storage Gateway 定期發行您閘道的重要軟體更新。您可以手動將更新套用在 Storage Gateway 管理主控台上，或者等待在設定的維護排程中自動應用更新。雖然 Storage Gateway 每分鐘會檢查是否有更新，但只會完成維護並在有更新時重新啟動。

網關軟件定期發行包括操作系統更新和安全修補程序，這些修補程序已由AWS。這些更新通常每六個月發佈一次，並在計劃的維護時段中作為正常網關更新過程的一部分應用。

> **Note**
>
> 應將 Storage Gateway 設備視為受管嵌入式設備，並且不應嘗試以任何方式訪問或修改其安裝。嘗試使用普通網關更新機制以外的方法（例如 SSM 或虛擬機管理程序工具）安裝或更新任何軟件包可能會導致網關出現故障。

在將任何更新應用到您的網關之前，AWS會在 Storage Gateway 控制台上顯示一條消息通知您，並且AWS Health Dashboard。如需詳細資訊，請參閱 AWS Health Dashboard。VM 不會重新啟動，但在更新和重新啟動時，閘道在短時間內會無法使用。

當您部署和啟用您的閘道時，即會設定預設的每週維護排程。您可以隨時修改維護排程。有更新可用時，Details (詳細資訊) 標籤會顯示維護訊息。您會在 Details (詳細資訊) 標籤中看到您閘道上次成功套用更新的日期和時間。

修改維護排程

1. Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home。
2. 在導覽窗格上，選擇 Gateways (閘道)，然後選擇您想要修改更新排程的閘道。
3. 在 Actions (動作) 功能表上，選擇 Edit maintenance window (編輯維護時段)，以填寫 Edit maintenance window start time (編輯維護時段開始時間) 的對話方塊。

4. 對於 Schedule (排程)，選擇 Weekly (每週) 或 Monthly (每月) 以排定更新。
5. 如果您選擇 Weekly (每週)，修改 Day of the week (星期幾) 和 Time (時間) 的值。

   如果您選擇 Monthly (每月)，修改 Day of the month (月中的日) 和 Time (時間) 的值。如果您選擇此選項且發生錯誤，表示您的閘道為舊版且尚未升級至更新版本。

   > **Note**
   >
   > 可以為月中的某天設置的最大值為 28。如果選擇了 28，則維護開始時間將在每月的第 28 天。

   您的維護開始時間將顯示在詳細資訊選項卡下次打開詳細資訊選項卡。

在本機主控台上執行維護任務

您可以使用主機的本機主控台來執行下列維護任務。您可以在 VM 主機或 Amazon EC2 執行個體上執行本機主控台任務。許多任務在不同主機都通用，但還是有一些差異。

主題

- 在 VM 本機主控台（文件閘道）上執行任務
- 在 Amazon EC2 本地控制台（文件網關）上執行任務
- 存取閘道本機主控台
- 為您的閘道設定網路轉接器

在 VM 本機主控台（文件閘道）上執行任務

針對在現場部署的檔案閘道，您可以使用 VM 主機的本機主控台執行下列維護任務。這些工作是 VMware、Microsoft Hyper-V 和 Linux 核心型虛擬機器 (KVM) Hypervisor 的常見任務。

主題

- 登入到文件閘道本機主控台
- 設定 HTTP 代理
- 配置網關網絡設置
- 測試網關的網絡連接

- 查看網關系統資源狀態
- 為閘道設定網路時間協定 (NTP) 伺服器
- 在本地控制台上運行存儲網關命令
- 為您的閘道設定網路適配器

登入到文件閘道本機主控台

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，您要使用預設的使用者名稱和密碼登入。這些預設的登入資料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。AWS Storage Gateway可讓您從 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 登入到文件閘道本機主控台。

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**
>
> 我們建議變更預設密碼。本機主控台選單 (主選單上的第 6 項) 執行 passwd 命令即可完成此步驟。如需如何執行命令的資訊，請參閱 在本地控制台上運行存儲網關命令。您也可以從 Storage Gateway 主控台設定密碼。如需詳細資訊，請參閱 登入到文件閘道本機主控台。

從 Storage Gateway 控制台設置本地控制台密碼

當您第一次登入本機主控台時，您使用預設的登入資料登入 VM。對於所有類型的閘道，您使用預設登入資料。使用者名稱為 admin 且密碼是 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。

在存放閘道主控台中設定本機主控 Storage Gateway 碼

1. Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home。
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 道不儲存密碼，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—512 個字元。

設定 HTTP 代理

檔案閘道支援 HTTP 代理的組態。

> **Note**
>
> 檔案閘道唯一支援的代理組態是 HTTP。

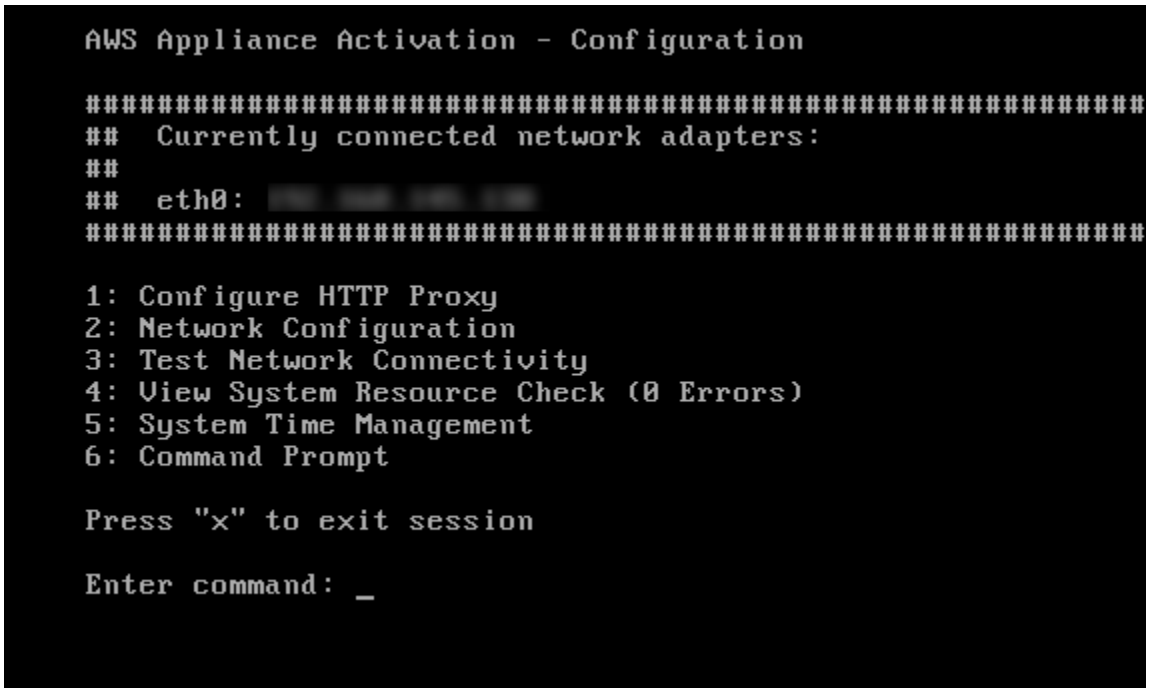
如果您的閘道必須使用代理伺服器與網際網路通訊，您即需要為閘道設定 HTTP 代理設定。您透過指定 IP 地址和執行代理的主機連接埠號碼，來完成此作業。完成此作業後，Storage Gateway 會透過所有AWS終端流量通過您的代理伺服器。網關和終端之間的通信將被加密，即使在使用 HTTP 代理時也是如此。如需閘道之網路需求的資訊，請參閱網路與防火牆需求。

設定文件閘道的 HTTP 代理

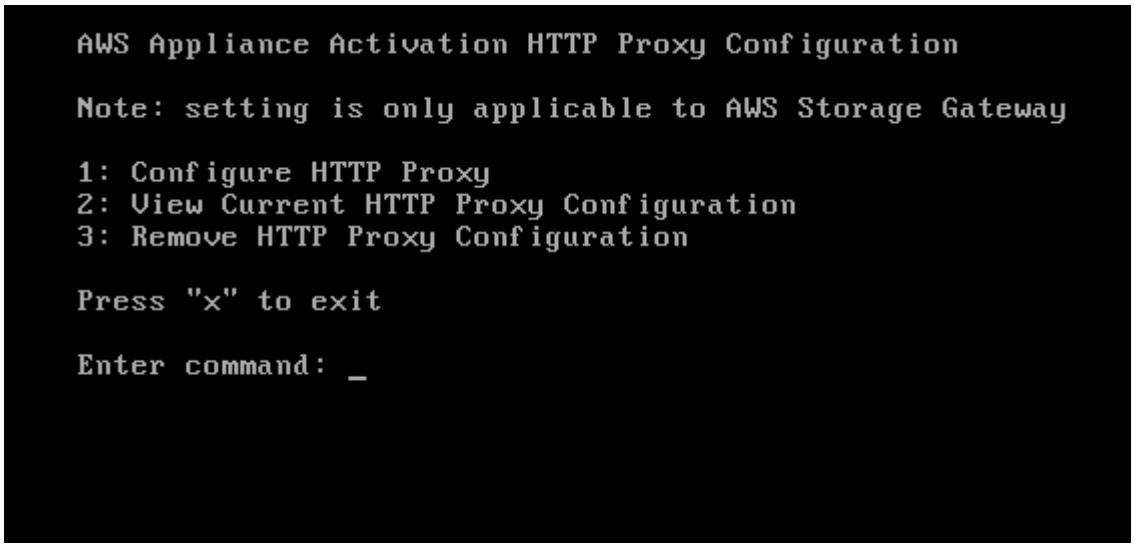
1. 登入您閘道的本機主控台：
   - 如需登入 VMware ESXi 本機主控台的詳細資訊，請參閱使用 VMware ESXi 存取閘道本機主控台。

- 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 (KVM) 的本機主控台的詳細資訊，請參閱使用 Linux KVM 存取閘道本機主控台。

2. 在AWS裝置激活-配置輸入主要功能表**1**開始設定 HTTP 代理。



3. 在 HTTP Proxy Configuration (HTTP 代理組態) 選單上，輸入 **1** 並提供 HTTP 代理伺服器的主機名稱。



您可以由此選單設定其他 HTTP 設定，如下所示。

若要	執行此作業
設定 HTTP 代理	輸入 **1**。 您需要提供主機名稱和連接埠才能完成設定。
檢視目前的 HTTP 代理組態	輸入 **2**。 如果未設定 HTTP 代理，則會顯示訊息 `HTTP Proxy not configured` 。如已設定 HTTP 代理，即會顯示主機名稱和代理的連接埠。
移除 HTTP 代理組態	輸入 **3**。 會顯示訊息 `HTTP Proxy Configuration Removed` 。

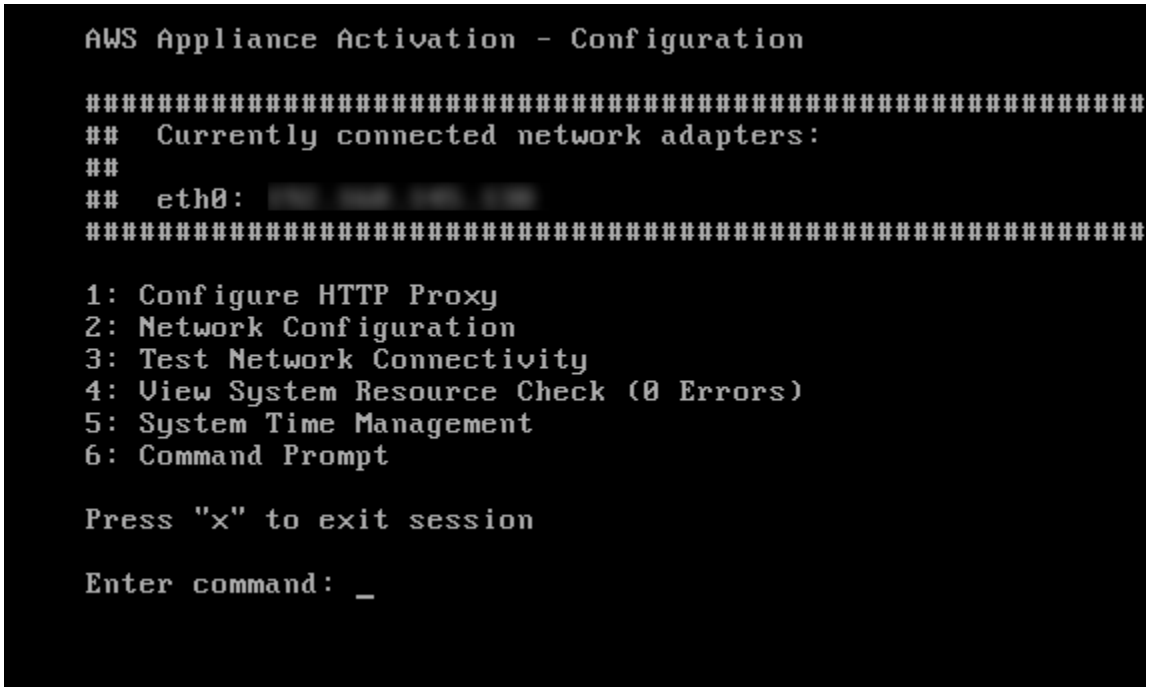
4. 重新啟動您的 VM 以套用您的 HTTP 組態設定。

配置網關網絡設置

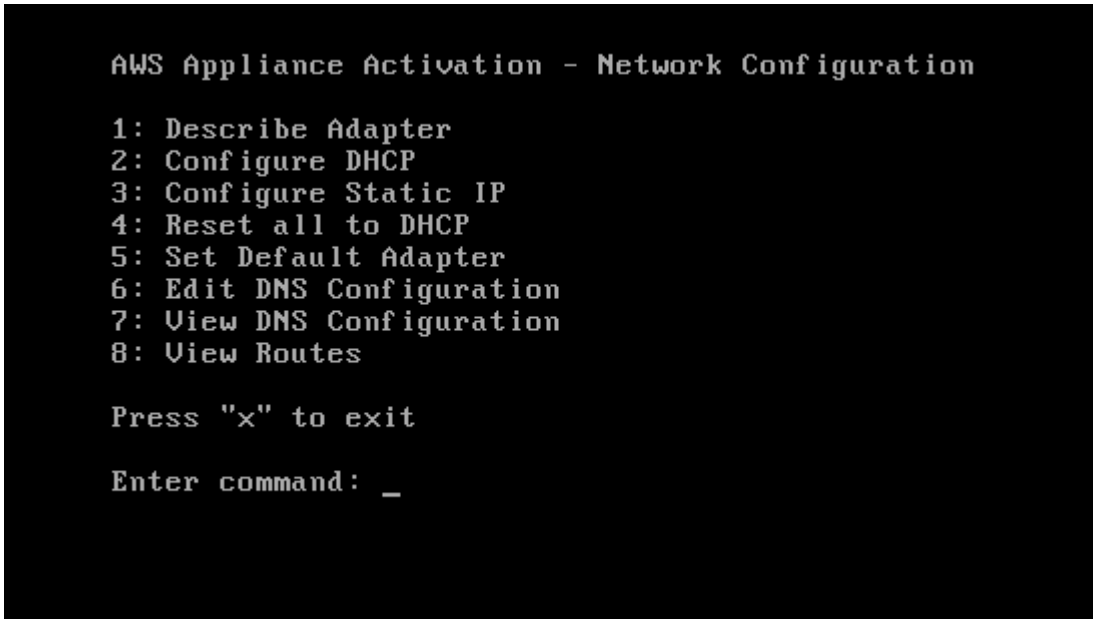
閘道的預設網路組態為動態主機設定通訊協定 (DHCP)。使用 DHCP，您的閘道會自動指派 IP 地址。在某些情況下，您可能需要手動指派您的閘道 IP 為靜態 IP 地址，如下所述。

設定您的閘道使用靜態 IP 地址

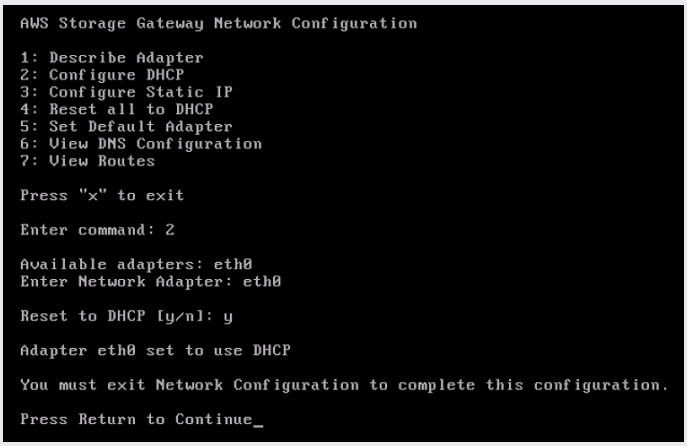
1. 登入您閘道的本機主控台：
   - 如需登入 VMware ESXi 本機主控台的詳細資訊，請參閱使用 VMware ESXi 存取閘道本機主控台。
   - 如需登入 Microsoft Hyper-V 本機主控台的詳細資訊，請參閱使用 Microsoft Hyper-V 存取閘道本機主控台。
   - 如需登入 KVM 本機主控台的詳細資訊，請參閱使用 Linux KVM 存取閘道本機主控台。
2. 在AWS裝置激活-配置輸入主要功能表**2**開始配置網絡。



3. 在 Network Configuration (網路組態) 選單上，選擇下列其中一個選項。



若要	執行此作業
取得網路轉接器的相關資訊	輸入 **1**。

若要	執行此作業
	隨即顯示轉接器名稱的清單，系統會提示您輸入轉接器名稱，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 • 網路遮罩 • 閘道 IP 地址 • DHCP 已啟用狀態 您設定靜態 IP 地址 (選項 3) 和設定您閘道的預設路由連接器 (選項 5) 時，皆使用相同的轉接器名稱。
設定 DHCP	輸入 **2**。 系統會提示您設定網路界面使用 DHCP。 

若要	執行此作業
為閘道設定靜態 IP 地址	輸入 **3**。 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 • 輔助 DNS 地址 **Important** 如果您的閘道已啟用，您必須將其關閉並在 Storage Gateway 主控台重啟，設定才能生效。如需詳細資訊，請參閱 關閉您的閘道 VM。 如果您的閘道使用一個以上的網路界面，您必須將所有已啟用的界面設定為使用 DHCP 或靜態 IP 地址。 例如，假設您的閘道 VM 使用兩個設定為 DHCP 的界面。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。

若要	執行此作業
	如果兩個界面最初都設定為使用靜態 IP 地址，且您之後設定閘道使用 DHCP，則兩個界面都將使用 DHCP。
重設所有閘道的網路組態為 DHCP	輸入 **4**。 所有的網路界面皆設定為使用 DHCP。 **Important** 如果您的閘道已啟用，您必須將其關閉並在 Storage Gateway 主控台重啟您的閘道，設定才能生效。如需詳細資訊，請參閱 關閉您的閘道 VM。
設定閘道的預設路由轉接器	輸入 **5**。 隨即顯示閘道可用的轉接器，系統會提示您選取其中一個轉接器 — 例如**eth0**。
編輯閘道的 DNS 組態	輸入 **6**。 隨即顯示主要和次要 DNS 名稱伺服器的可用轉接器。系統會提示您提供新的 IP 地址。

若要	執行此作業
檢視閘道的 DNS 組態	輸入 **7**。 隨即顯示主要和次要 DNS 名稱伺服器的可用轉接器。 **Note** 對於有些版本的 VMware Hypervisor，您可以在此選單中編輯轉接器組態。
檢視路由表	輸入 **8**。 隨即顯示閘道的預設路由。

測試網關的網絡連接

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。

測試閘道的網際網路連通性

1. 登入您閘道的本機主控台：
   - 如需登入 VMware ESXi 本機主控台的詳細資訊，請參閱使用 VMware ESXi 存取閘道本機主控台。
   - 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 KVM 本機主控台的詳細資訊，請參閱使用 Linux KVM 存取閘道本機主控台。
2. 從AWS裝置激活-配置主菜單中，輸入相應的數字以選擇測試網路連線能力。

   如果您的網關已激活，連接測試將立即開始。對於尚未激活的網關，您必須指定終端節點類型和 AWS 區域，如以下步驟所述。
3. 如果您的網關尚未激活，請輸入相應的數字以選擇網關的終端節點類型。

4. 如果選擇了公共終端節點類型，請輸入相應的數字以選擇AWS 區域你想要測試的。支援AWS 區域的清單AWS可與 Storage Gateway 一起使用的服務終端節點，請參閱AWS Storage Gateway端點和配額中的AWS一般參考。

隨着測試的進展，每個端點都會顯示[PASSED]或者[失敗]，表示連線的狀態，如下所示：

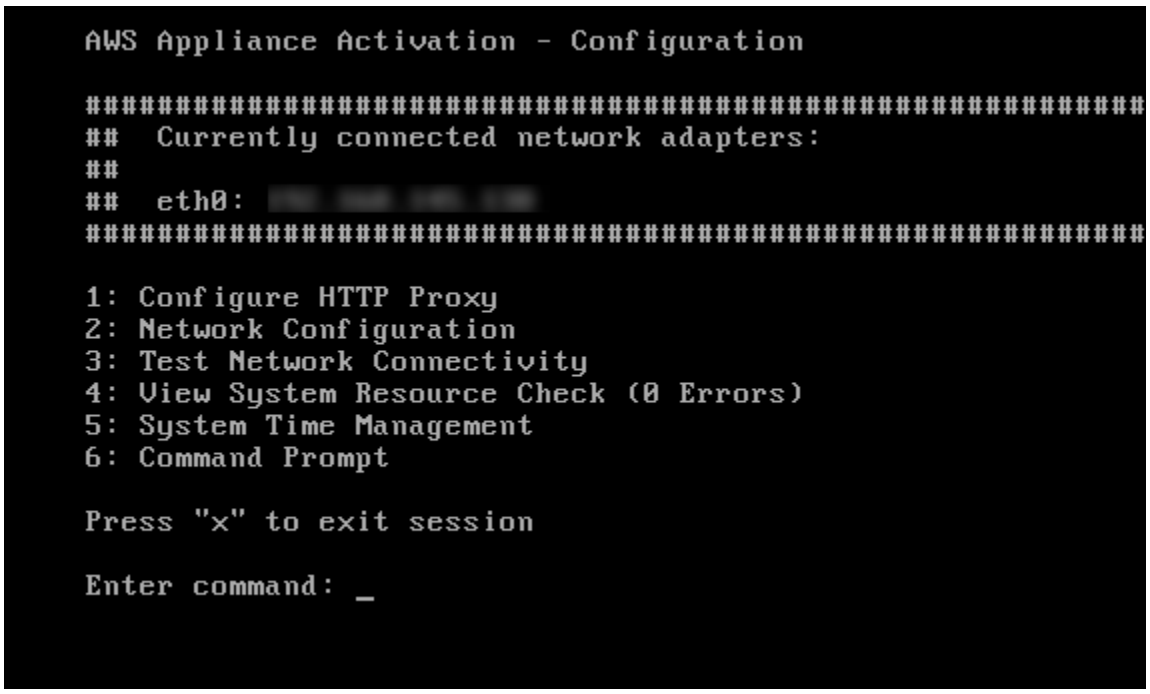
Message	描述
[PASSED] ([通過])	Storage Gateway 具有網絡連接。
[FAILED] ([失敗])	Storage Gateway 沒有網絡連接。

查看網關系統資源狀態

當閘道啟動時，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 VMware ESXi 主控台的詳細資訊，請參閱使用 VMware ESXi 存取閘道本機主控台。
   - 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 KVM 本機主控台的詳細資訊，請參閱使用 Linux KVM 存取閘道本機主控台。
2. 在 中AWS裝置激活-配置輸入主要功能表**4**以檢視系統資源檢查的結果。



主控台會針對每個資源顯示 [OK] (OK)、[WARNING] (警告) 或 [FAIL] (失敗) 的訊息，如下表所述。

Message	描述
[OK]	此資源已通過系統資源檢查。
[WARNING] (警告)	此資源未符合建議的要求，但您的閘道可繼續運作。Storage Gateway 會顯示說明資源檢查結果的訊息。
[FAIL] (失敗)	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。

為閘道設定網路時間協定 (NTP) 伺服器

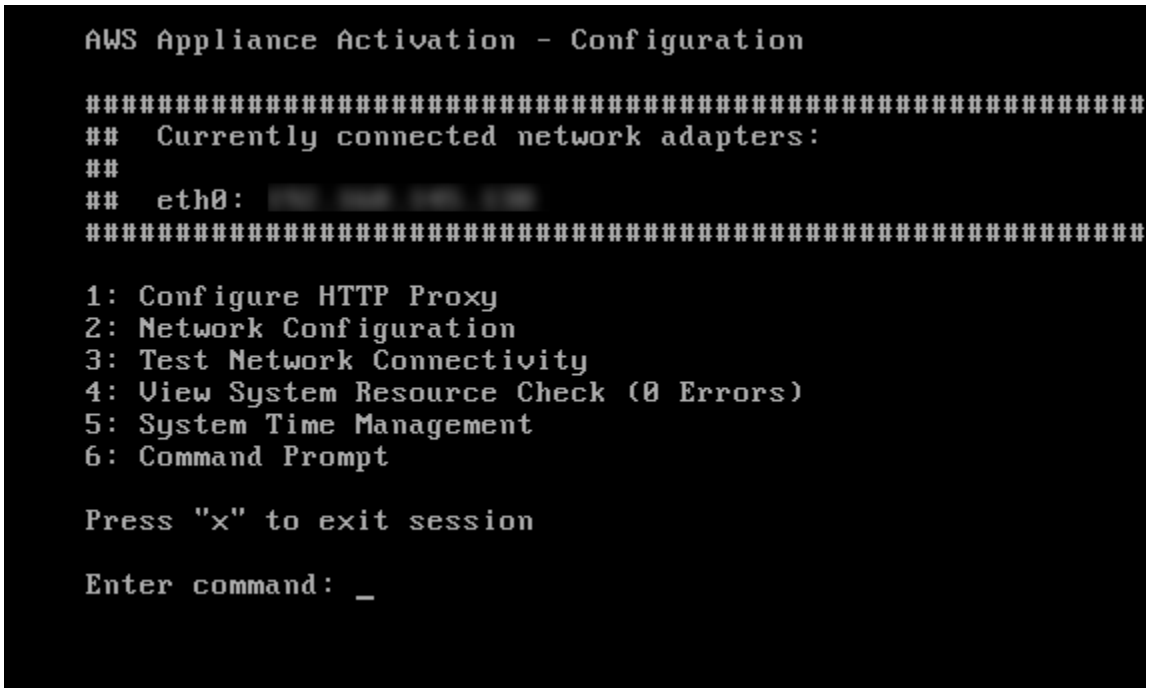
您可以檢視和編輯網路時間協定 (NTP) 伺服器組態，並將閘道上的 VM 時間與您的 Hypervisor 主機同步。

若要管理系統時間

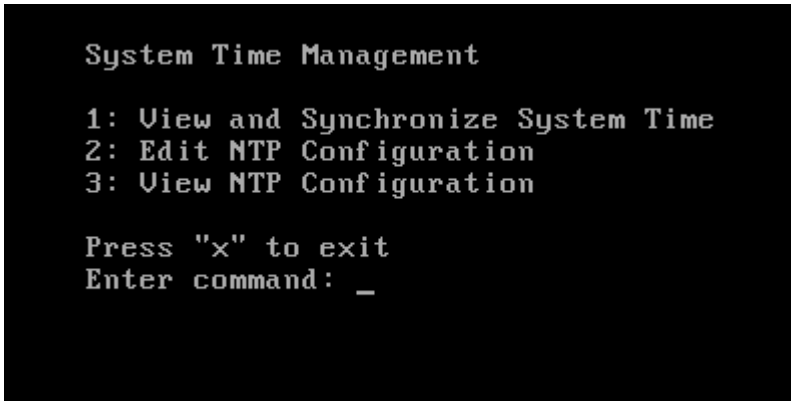
1. 登入您閘道的本機主控台：

   - 如需登入 VMware ESXi 本機主控台的詳細資訊，請參閱使用 VMware ESXi 存取閘道本機主控台。
   - 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 KVM 本機主控台的詳細資訊，請參閱使用 Linux KVM 存取閘道本機主控台。

2. 在 中AWS裝置激活-配置輸入主要功能表**5**來管理系統的時間。



3. 在 System Time Management (系統時間管理) 選單中，選擇下列其中一個選項。



若要	執行此作業
檢視並同步 VM 時間與 NTP 伺服器時間。	輸入 **1**。 即顯示 VM 上目前的時間。您的檔案閘道會判斷閘道 VM 的時間差異，NTP 伺服器時間會提示您同步 VM 時間與 NTP 時間。 部署並執行閘道後，在某些情況下，閘道 VM 的時間可能會產生差異。例如，假設出現長時間網路中斷，而您的 Hypervisor 主機和閘道無法取得時間更新。在此情況下，閘道 VM 的時間會與真實時間不同。時間產生差異時，執行操作 (例如快照) 的指定時間和操作發生的實際時間會出現差異。 針對部署在 VMware ESXi 上的閘道，設定虛擬化管理程序主機時間並讓 VM 時間與主機同步便足以避免時間產生差異。如需詳細資訊，請參閱 同步 VM 時間與主機時間。 針對在 Microsoft Hyper-V 上部署的閘道，建議您定期檢查 VM 的時間。如需詳細資訊，請參閱 同步閘道的 VM 時間。 對於在 KVM 上部署的閘道，您可以使用 KVM 的 `virsh` 命令列界面來檢查並同步虛擬機器時間。
編輯 NTP 伺服器組態	輸入 **2**。 系統會提示您提供偏好的和次要的 NTP 伺服器。
檢視 NTP 伺服器組態	輸入 **3**。 隨即顯示您的 NTP 伺服器組態。

在本地控制台上運行存儲網關命令

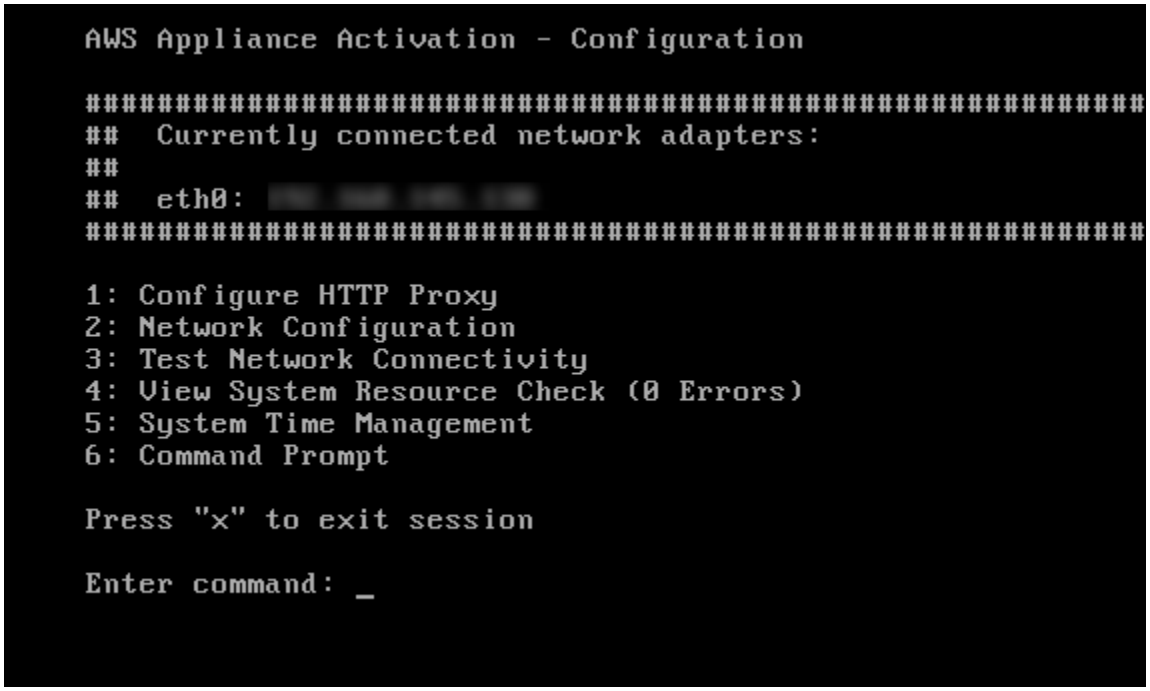
Storage Gateway 中的 VM 本機主控台可協助提供用於設定和診斷閘道問題的安全環境。使用本機主控台命令，您便可執行維護任務，例如儲存路由表或連接到 Amazon Web Services vice Support 等。

執行組態或診斷命令

1. 登入您閘道的本機主控台：

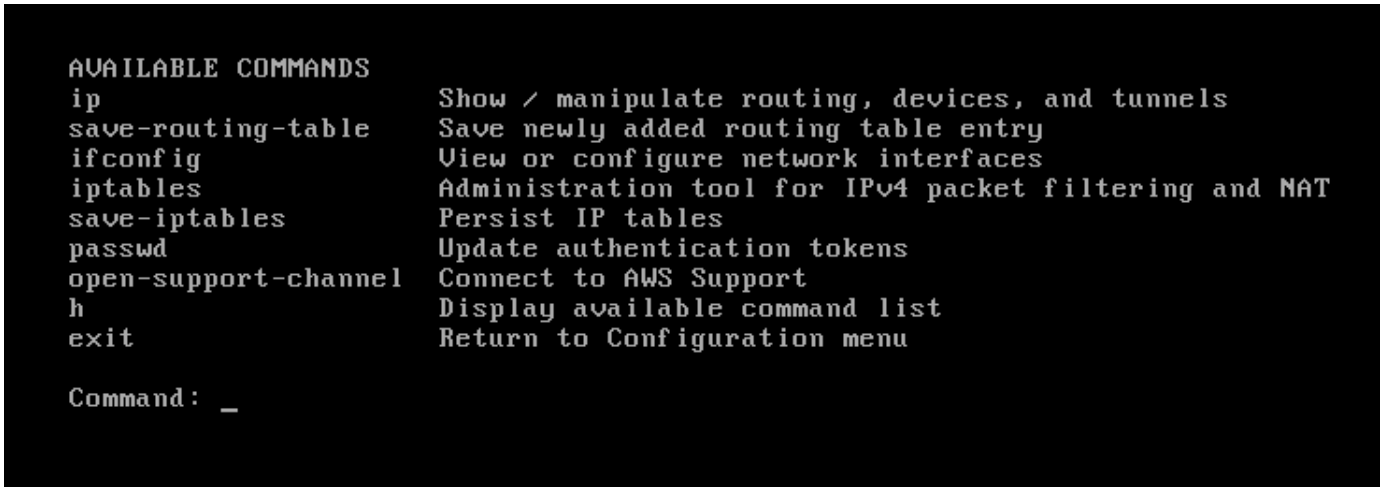
   - 如需登入 VMware ESXi 本機主控台的詳細資訊，請參閱使用 VMware ESXi 存取閘道本機主控台。
   - 如需登入 Microsoft Hyper-V 本機主控台的詳細資訊，請參閱使用 Microsoft Hyper-V 存取閘道本機主控台。
   - 如需登入 KVM 本機主控台的詳細資訊，請參閱使用 Linux KVM 存取閘道本機主控台。

2. 在AWS裝置激活-配置輸入主要功能表**6**為了命令提示。



3. 在AWS裝置激活-命令提示符控制台，輸入**h**(下一步)，然後按傳回鍵。

   該主控台會顯示 AVAILABLE COMMANDS (可用命令) 選單與命令的用途，如下列螢幕擷取畫面所示。



4. 在命令提示字元中輸入您要使用的命令並遵照指示進行。

若要了解命令，請在命令提示字元中提示輸入命令名稱。

為您的閘道設定網路適配器

根據預設，Storage Gateway 道會設定為使用 E1000 網路轉接器類型，但您可以重新設定您的閘道使用 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

- 設定您的閘道使用 VMXNET3 網路適配器

設定您的閘道使用 VMXNET3 網路適配器

Storage Gateway 在 VMware ESXi 和 Microsoft Hyper-V 虛擬化管理程序主機中都支援 E1000 網路轉接器類型。不過，VMware ESXi 虛擬化管理程序只支援 VMXNET3 (10 GbE) 網路轉接器類型。如果您的閘道是裝載在 VMware ESXi Hypervisor 中，您就可以重新設定您的閘道使用 VMXNET3 (10 GbE) 轉接器類型。如需此轉接器的詳細資訊，請參閱 VMware 網站。

針對 KVM 虛擬化管理程序主機，Storage Gateway 支援使用`virtio`網絡設備驅動程序。不支援 KVM 主機使用 E1000 網路卡轉接器類型。

> **Important**
>
> 您的訪客作業系統必須是 Other Linux64 (其他 Linux64)，才能選取 VMXNET3。

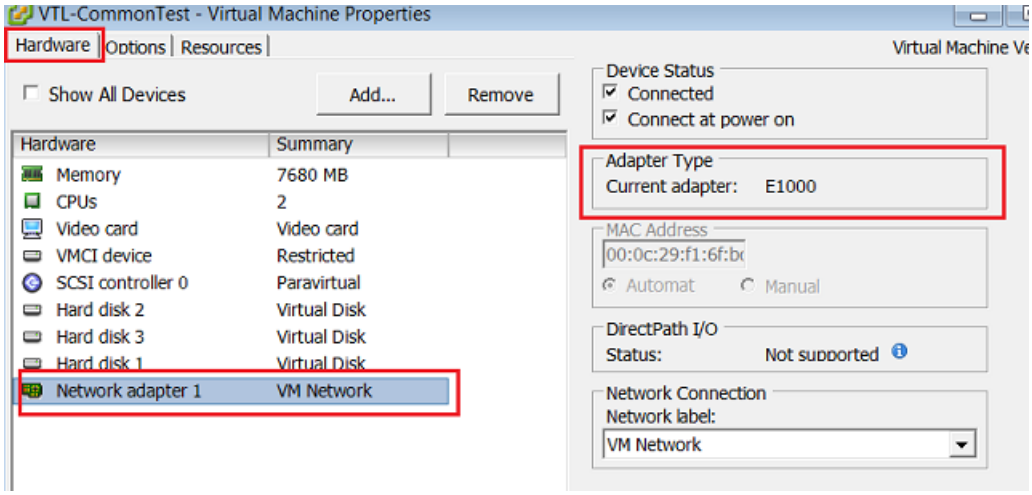
請採取下列步驟來設定您的閘道使用 VMXNET3 轉接器：

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。

移除預設的 E1000 轉接器並設定您的閘道使用 VMXNET3 轉接器

1. 在 VMware 中，開啟閘道的內容 (按右鍵) 選單，然後選擇 Edit Settings (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 Enter (轉接器類型) 區段目前的轉接器是 E1000。您使用 VMXNET3 轉接器取代此轉接器。



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**
>
> 雖然您可以在您的閘道同時執行 E1000 和 VMXNET3 網路轉接器，但我們不建議您這樣做，因為它會導致網路問題。

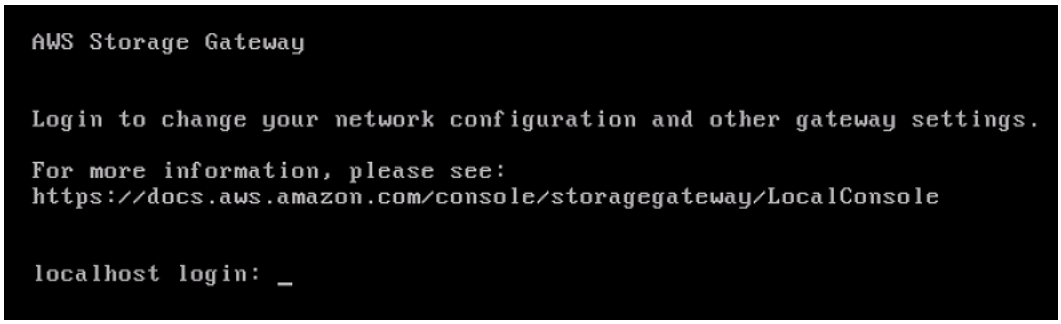
5. 選擇 Add (新增) 開啟 Add Hardware (新增硬體) 精靈。
6. 請選擇 Ethernet Adapter (乙太網路卡)，然後選擇 Next (下一步)。

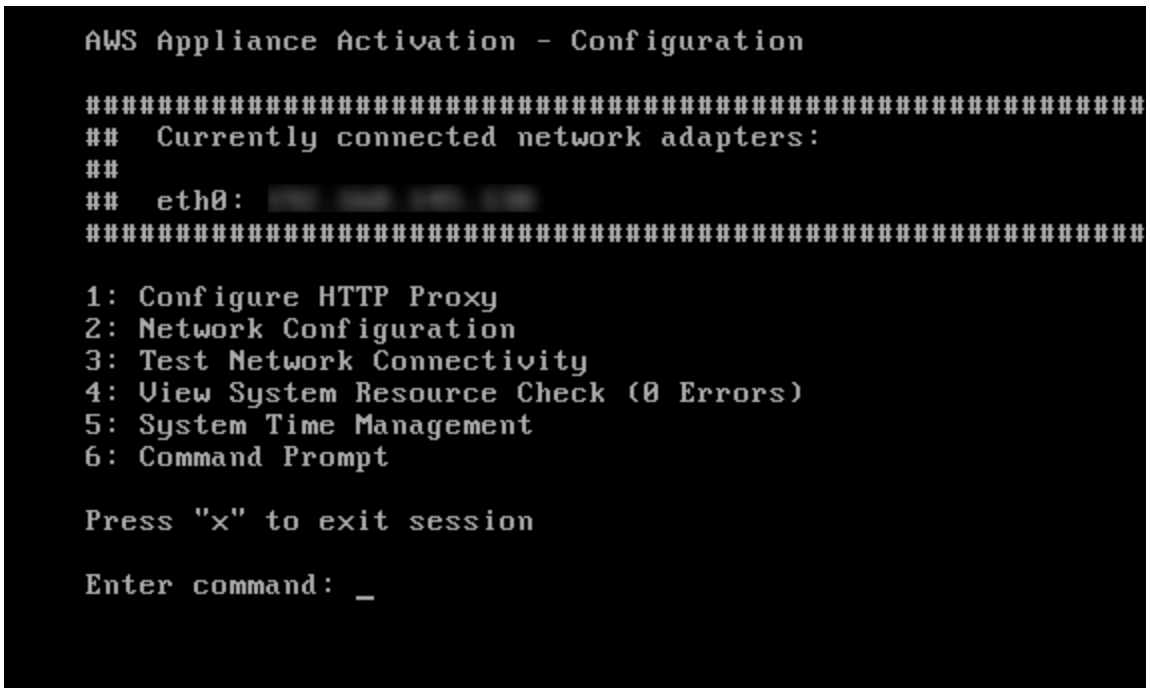
7. 在「網絡輸入」嚮導中，選擇**VMXNET3**為了轉換器輸入，然後選擇下一頁。
8. 在 Virtual Machine properties (虛擬機器屬性) 精靈中，確認 Adapter Enter (轉接器類型) 區段的 Current Adapter (目前的轉接器) 是否設為 VMXNET3，然後選擇 OK (確定)。
9. 在 VMware VSphere 用戶端中，關閉您的閘道。
10. 在 VMware VSphere 用戶端中，重新啟動您的閘道。

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。

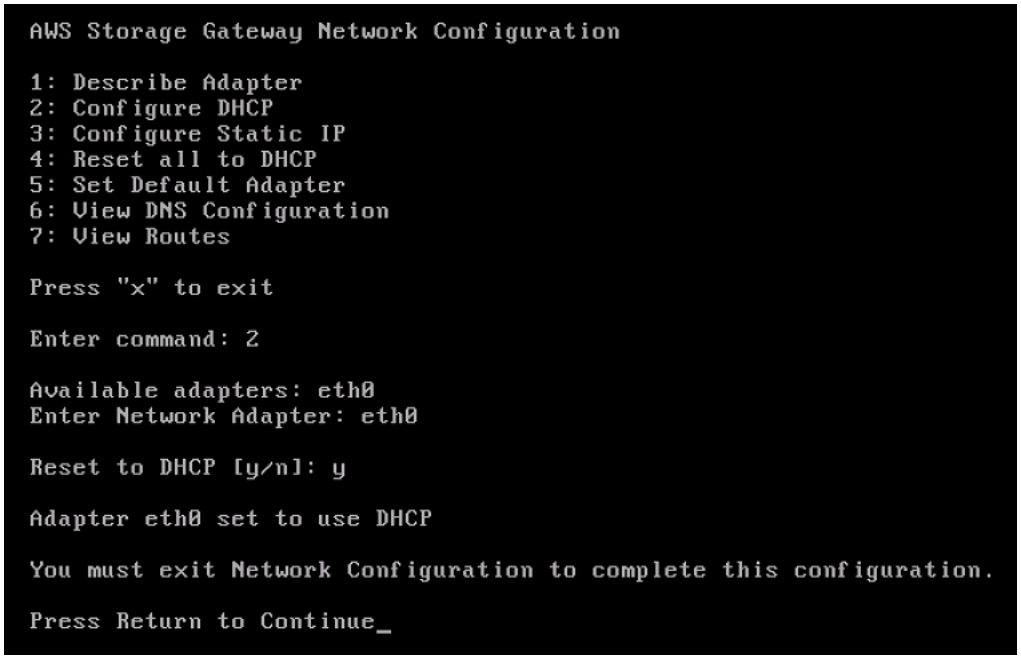
設定網路轉接器

1. 在 VSphere 用戶端中，選擇 Console (主控台) 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。如需如何使用預設登入資料來登入的資訊，請參閱[登入到文件閘道本機主控台]。





2. 系統提示時，輸入 **2** 以選取 Network Configuration (網路組態)，然後按 **Enter** 開啟網路組態選單。
3. 系統提示時，輸入 **4** 以選取 Reset all to DHCP (全部重設為 DHCP)，然後在系統提示重設所有轉接器以使用動態主機設定通訊協定 (DHCP) 時，輸入 **y** (表示 yes (是))。所有可用轉接器設定為使用 DHCP。



如果您的閘道已啟用，您必須將其關閉並從存放閘道管理主控台重啟。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資訊，請參閱測試網關的網絡連接。

在 Amazon EC2 本地控制台（文件網關）上執行任務

當執行部署在 Amazon EC2 執行個體的閘道時，有些維護任務需要您登入本機主控台。在本區段中，您可以找到有關如何登入本機主控台並執行維護任務的資訊。

主題

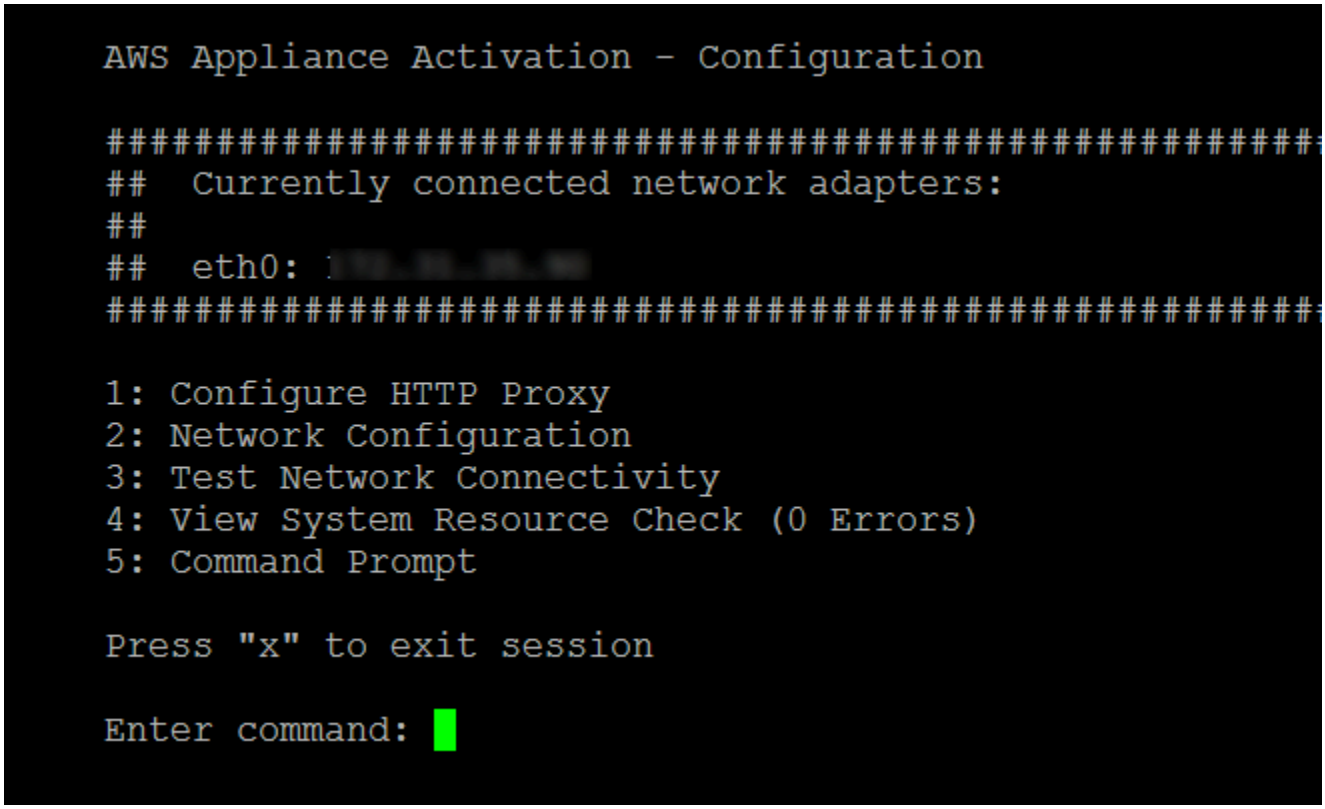
- 登錄到您的 Amazon EC2 網關本地控制台
- 通過 HTTP 代理路由部署在 EC2 上的網關
- 配置網關網絡設置
- 測試網關的網絡連接
- 查看網關系統資源狀態
- 在本地控制台上運行 Storage Gateway 命令

登錄到您的 Amazon EC2 網關本地控制台

您可以使用 Secure Shell (SSH) 用户端連線到 Amazon EC2 執行個體。如需詳細資訊，請參連接至您的執行個體中的Amazon EC2 使用者指南。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 Amazon EC2 密鑰對的資訊，請參Amazon EC2 金鑰對中的Amazon EC2 使用者指南。

登入至閘道本機主控台

1. 登入您的本機主控台。如果您是從 Windows 電腦連線到您的 EC2 執行個體，請以 admin 身分登入。
2. 在您登入後，您會看到AWS裝置激活-配置主選單，如下列螢幕快照所示。



若要進一步了解此項	請參閱此主題
為您的閘道設定 HTTP 代理	通過 HTTP 代理路由部署在 EC2 上的網關
為您的閘道設定網路設定	測試網關的網絡連接
測試網路連線	測試網關的網絡連接

若要進一步了解此項	請參閱此主題
檢視系統資源檢查	登錄到您的 Amazon EC2 網關本地控制台.
運行 Storage Gateway 控台命令	在本地控制台上運行 Storage Gateway 命令

若要關閉閘道，請輸入 **0**。

若要結束組態工作階段，請輸入 **x** 來結束選單。

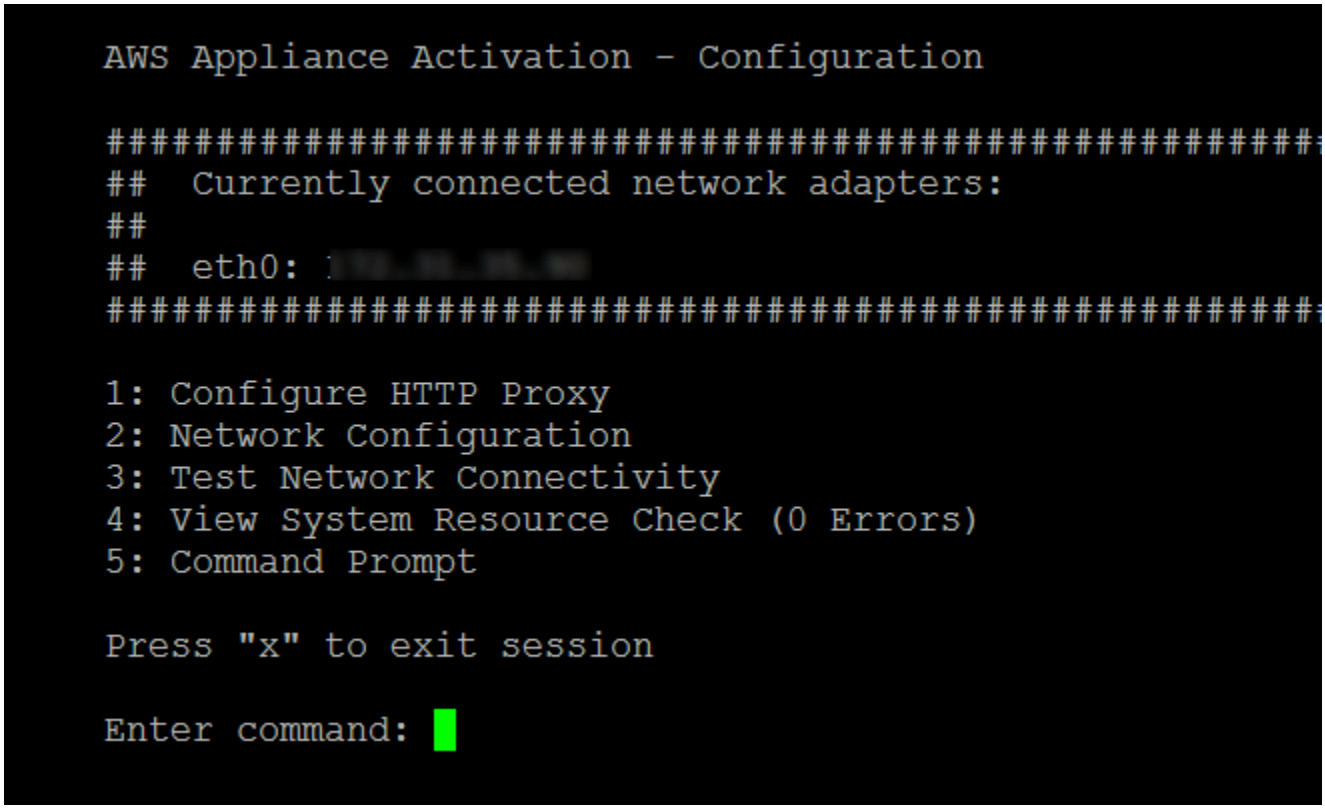
通過 HTTP 代理路由部署在 EC2 上的網關

Storage Gateway 支援部署在 Amazon EC2 和 SOCKS5AWS。

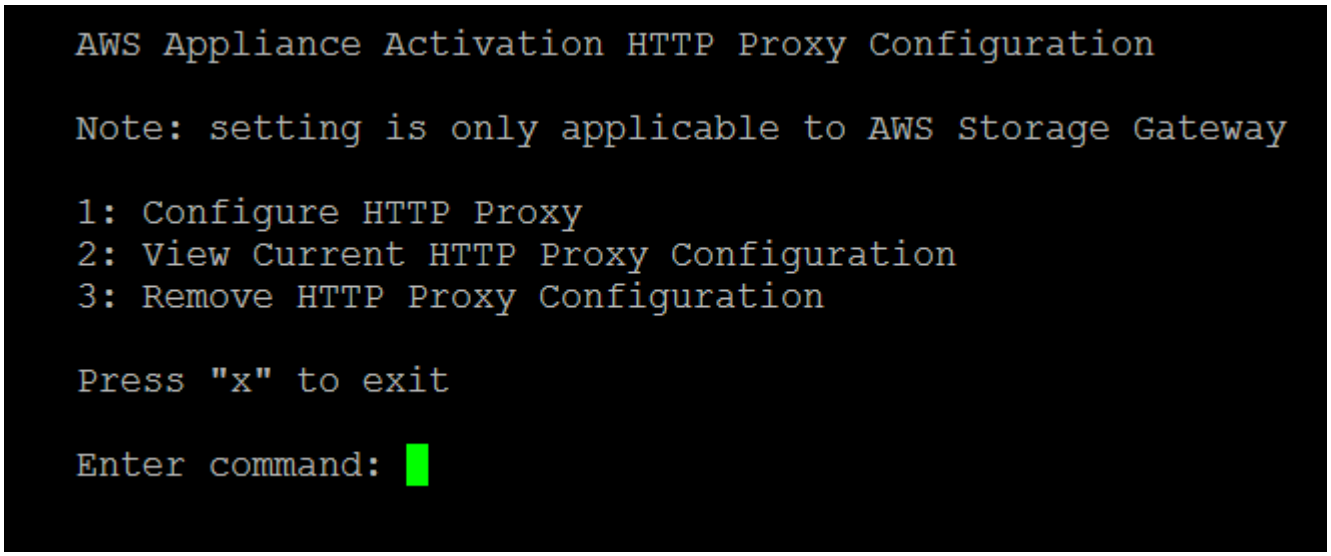
如果您的閘道必須使用代理伺服器與網際網路通訊，您即需要為閘道設定 HTTP 代理設定。您透過指定 IP 地址和執行代理的主機連接埠號碼，來完成此作業。完成此作業後，Storage Gateway 會透過所有AWS終端流量通過您的代理伺服器。網關和終端之間的通信將被加密，即使在使用 HTTP 代理時也是如此。

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。如需指示，請參閱 登錄到您的 Amazon EC2 網關本地控制台。
2. 在AWS裝置激活-配置輸入主要功能表**1**開始設定 HTTP 代理。



3. 選擇下列其中一個選項，請在AWS裝置激活-配置HTTP 代理組態選單。



若要	執行此作業
設定 HTTP 代理	輸入 **1**。

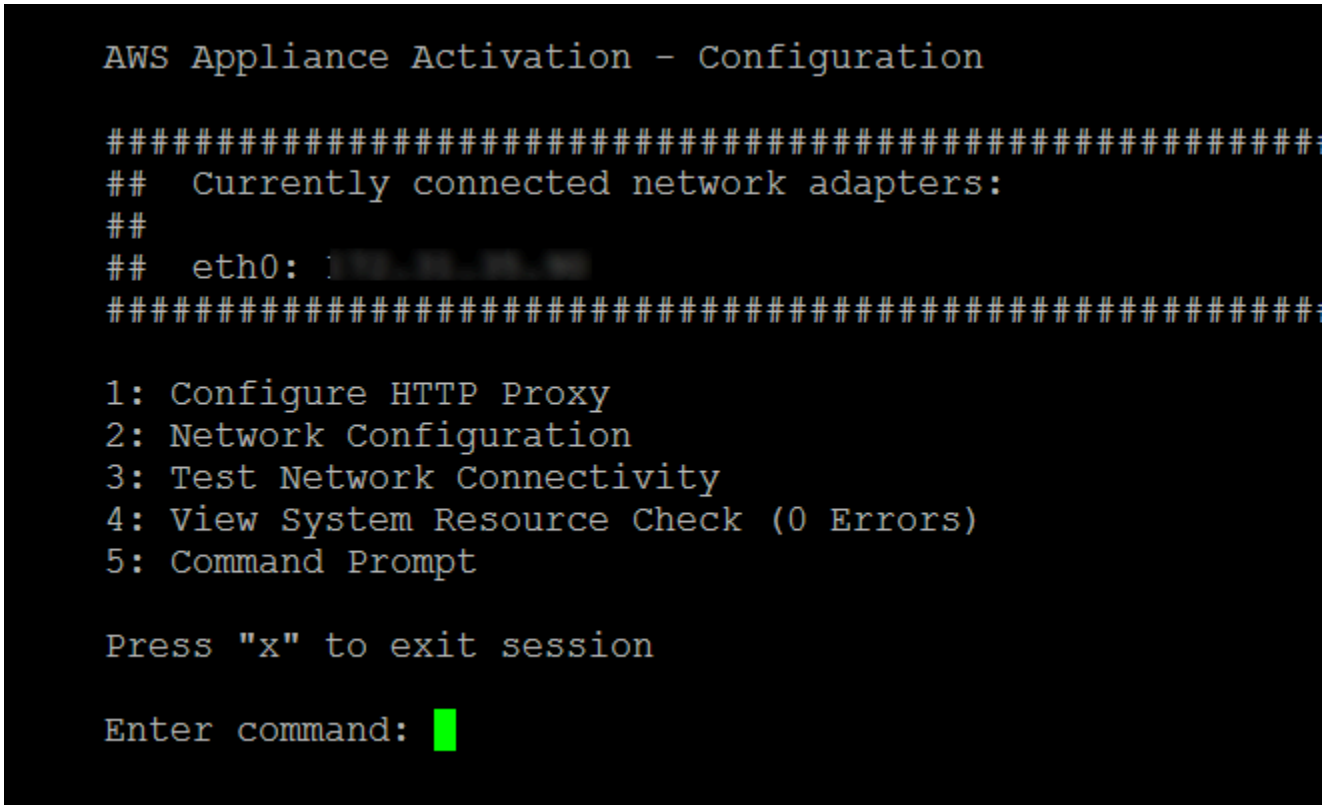
若要	執行此作業
	您需要提供主機名稱和連接埠才能完成設定。
檢視目前的 HTTP 代理組態	輸入 **2**。 如果未設定 HTTP 代理，會顯示訊息 `HTTP Proxy not configured` 。如已設定 HTTP 代理，即會顯示主機名稱和代理的連接埠。
移除 HTTP 代理組態	輸入 **3**。 會顯示訊息 `HTTP Proxy Configuration Removed` 。

配置網關網絡設置

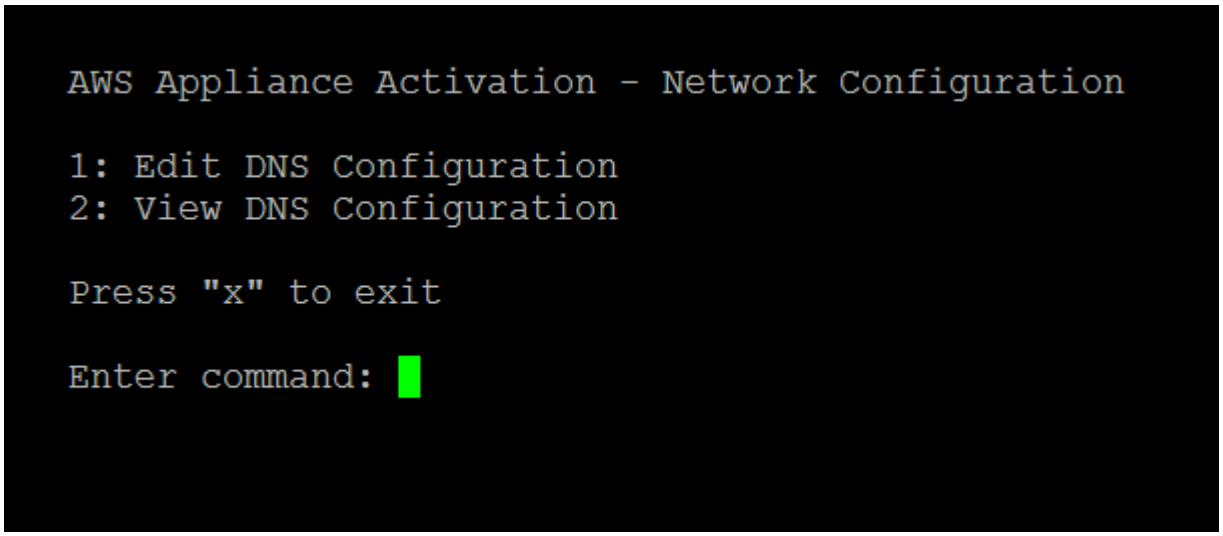
您可以透過本機主控台，檢視和設定您的網域名稱伺服器 (DNS) 設定。

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。如需指示，請參閱 登錄到您的 Amazon EC2 網關本地控制台。
2. 在AWS裝置激活-配置輸入主要功能表**2**開始配置 DNS 服務器。



3. 在 Network Configuration (網路組態) 選單上，選擇下列其中一個選項。



若要	執行此作業
編輯閘道的 DNS 組態	輸入 **1**。

若要	執行此作業
	隨即顯示主要和次要 DNS 名稱伺服器的可用轉接器。系統會提示您提供新的 IP 地址。
檢視閘道的 DNS 組態	輸入 **2**。 隨即顯示主要和次要 DNS 名稱伺服器的可用轉接器。

測試網關的網絡連接

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。

測試閘道的連通性

1. 登入您閘道的本機主控台。如需指示，請參閱 登錄到您的 Amazon EC2 網關本地控制台。
2. 從AWS裝置激活-配置主菜單中，輸入相應的數字以選擇測試網路連線能力。

   如果您的網關已激活，連接測試將立即開始。對於尚未激活的網關，您必須指定終端節點類型和 AWS 區域，如以下步驟所述。
3. 如果您的網關尚未激活，請輸入相應的數字以選擇網關的終端節點類型。
4. 如果選擇了公共終端節點類型，請輸入相應的數字以選擇AWS 區域你想要測試的。支援AWS 區域的清單AWS可與 Storage Gateway 一起使用的服務終端節點，請參閱AWS Storage Gateway端點和配額中的AWS一般參考。

隨着測試的進展，每個端點都會顯示[PASSED]或者[失敗]，表示連線的狀態，如下所示：

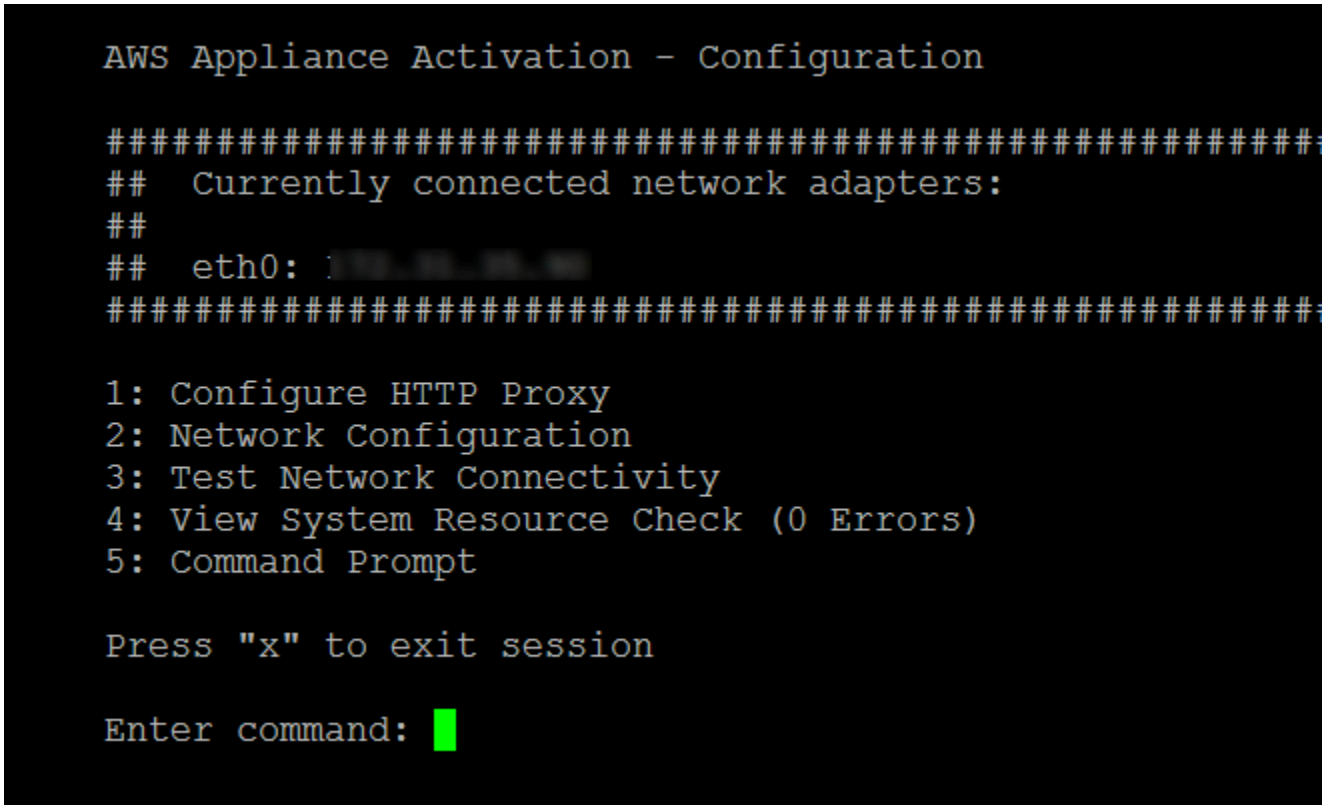
Message	描述
[PASSED] ([通過])	Storage Gateway 具有網絡連接。
[FAILED] ([失敗])	Storage Gateway 沒有網絡連接。

查看網關系統資源狀態

當閘道啟動時，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。如需指示，請參閱 登錄到您的 Amazon EC2 網關本地控制台。
2. 在 中Storage Gateway 組態輸入主要功能表**4**以檢視系統資源檢查的結果。



主控台會針對每個資源顯示 [OK] (OK)、[WARNING] (警告) 或 [FAIL] (失敗) 的訊息，如下表所述。

Message	描述
[OK]	此資源已通過系統資源檢查。
[WARNING] (警告)	此資源未符合建議的要求，但您的閘道可繼續運作。Storage Gateway 會顯示說明資源檢查結果的訊息。

Message	描述
[FAIL] (失敗)	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。

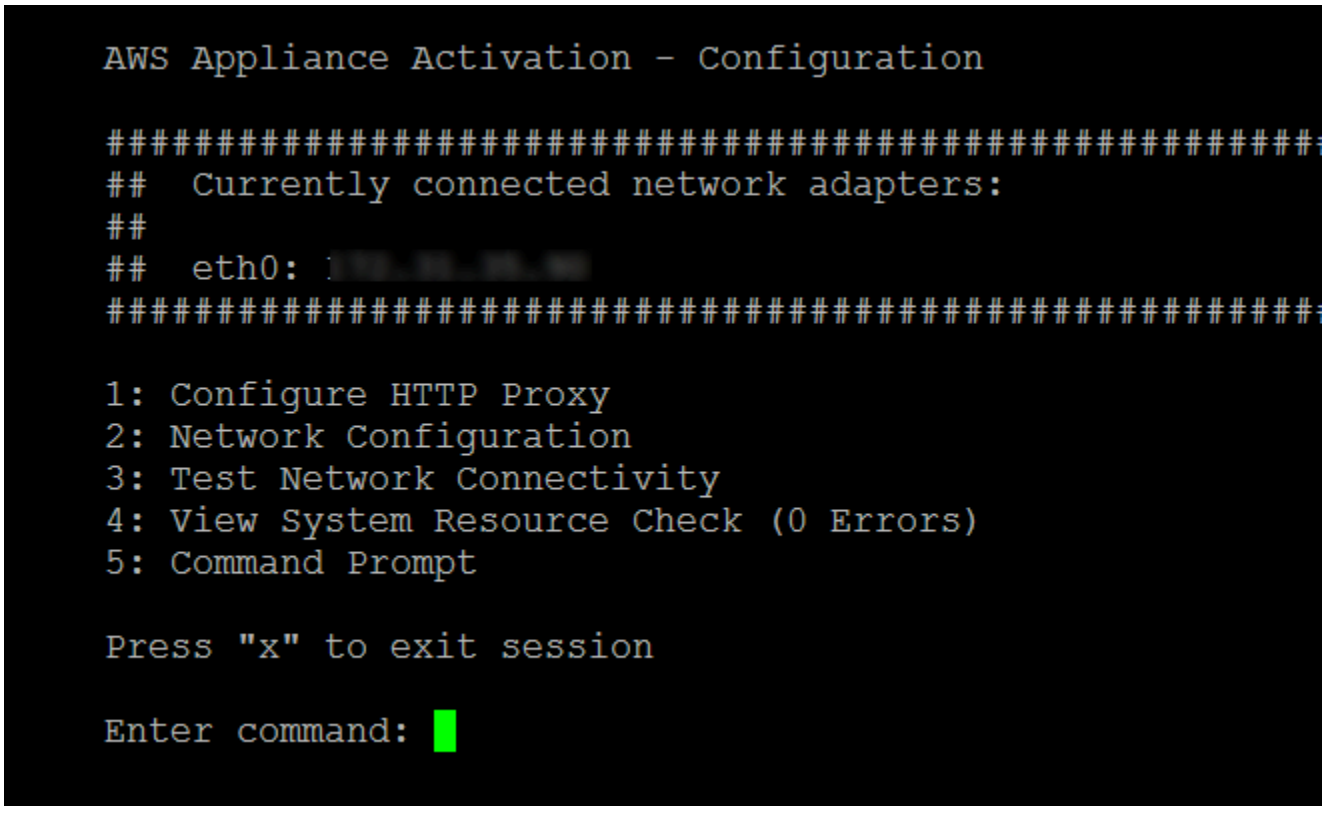
主控台也會在資源檢查選單選項旁顯示錯誤和警告的數量。

在本地控制台上運行 Storage Gateway 命令

AWS Storage Gateway 主控台可協助提供用於設定和診斷閘道問題的安全環境。使用主控台命令，您便可執行維護任務，例如儲存路由表或連接到 Amazon Web Services vice Support。

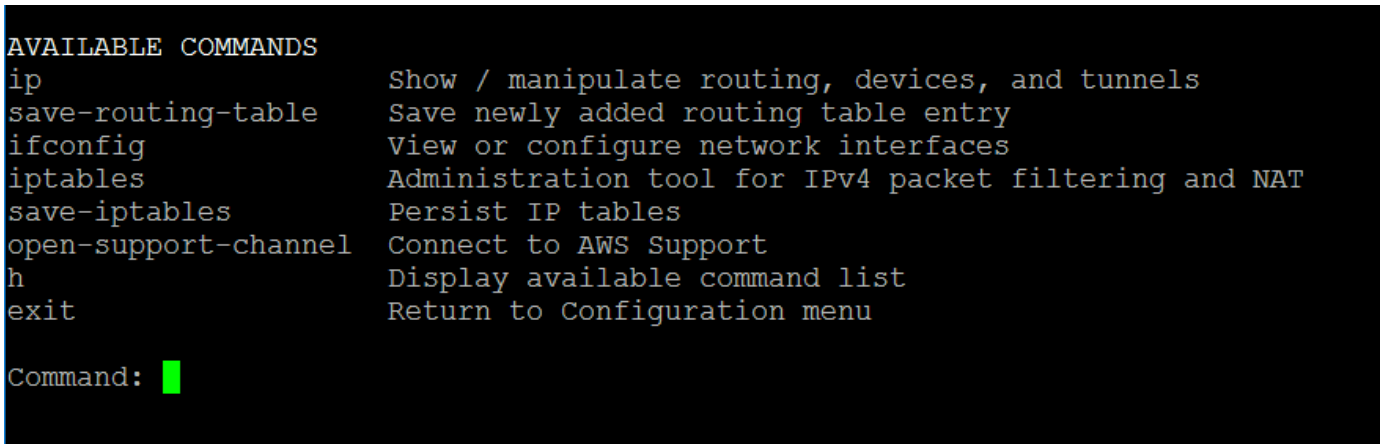
執行組態或診斷命令

1. 登入您閘道的本機主控台。如需指示，請參閱 登錄到您的 Amazon EC2 網關本地控制台。
2. 在 中AWS設備激活輸入主要功能表**5**為了閘道主控台。



3. 在命令提示中輸入 **h**，然後按 Return 鍵。

該主控台會顯示 AVAILABLE COMMANDS (可用命令) 選單與可用的命令。閘道主控台提示將出現在該選單之後，如下列螢幕擷取畫面所示。



4. 在命令提示字元中輸入您要使用的命令並遵照指示進行。

若要了解命令，請在命令提示字元中提示輸入命令名稱。

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)、VMware ESXi 和 Microsoft Hyper-V 管理員存取 VM 本機主控台的資訊。

主題

- 使用 Linux KVM 存取閘道本機主控台
- 使用 VMware ESXi 存取閘道本機主控台
- 使用 Microsoft Hyper-V 存取閘道本機主控台

使用 Linux KVM 存取閘道本機主控台

根據使用的 Linux 發行版，在 KVM 上執行的虛擬機器有不同的方法。從指令行存取 KVM 組態選項的指示如下。指示可能會因您的 KVM 實作而有所不同。

使用 KVM 存取閘道的本機主控台

1. 使用下列命令列出 KVM 中目前可用的虛擬機器。

```
# virsh list
```

您可以透過 Id 選擇可用的虛擬機器。

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

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

2. 使用下列命令來存取本機主控台。

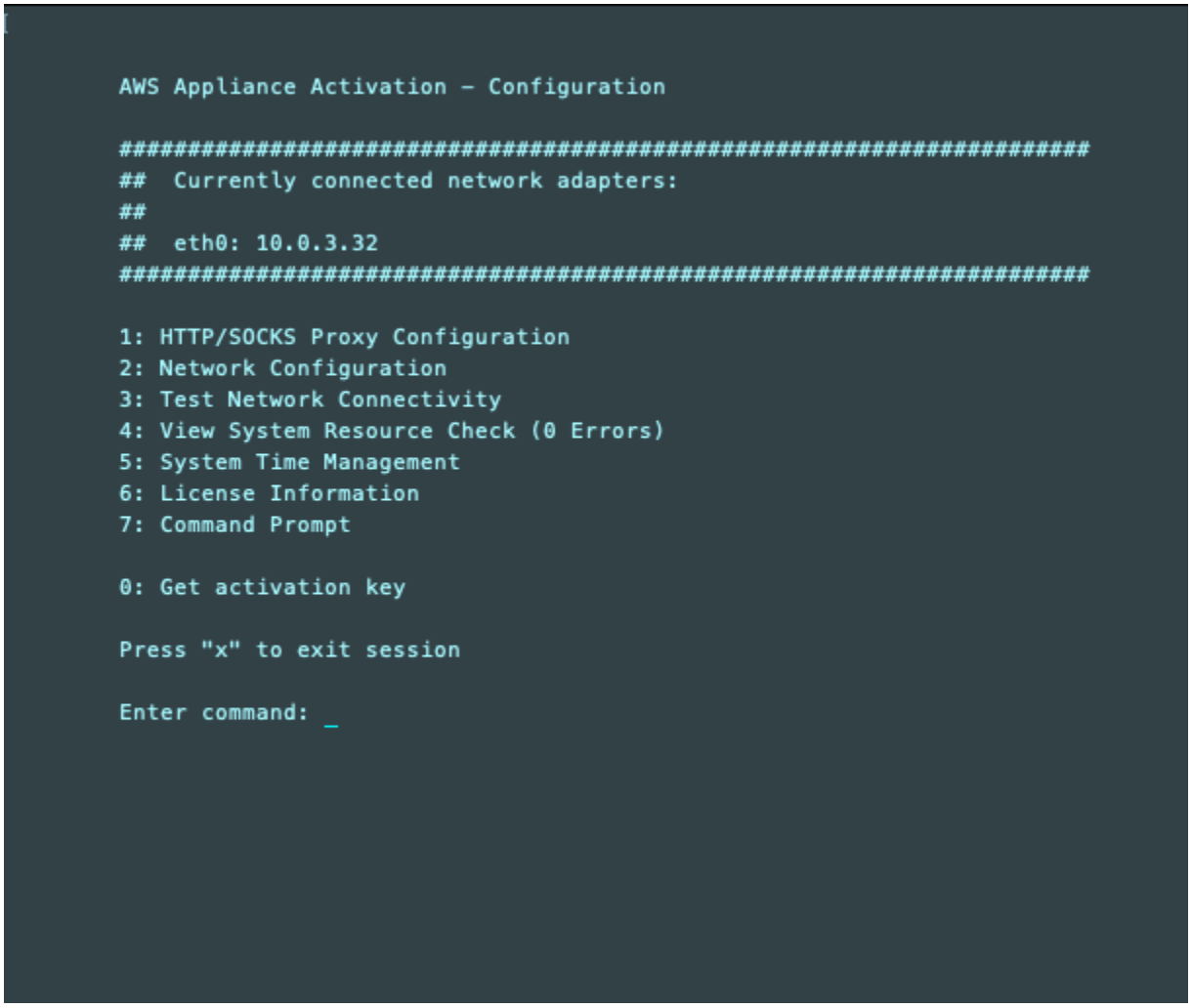
```
# virsh console VM_Id
```

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

AWS Appliance

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

3. 若要取得登入本機主控台的預設登入資料，請參閱 登入到文件閘道本機主控台。
4. 登入後，您可以啟用和設定您的閘道。

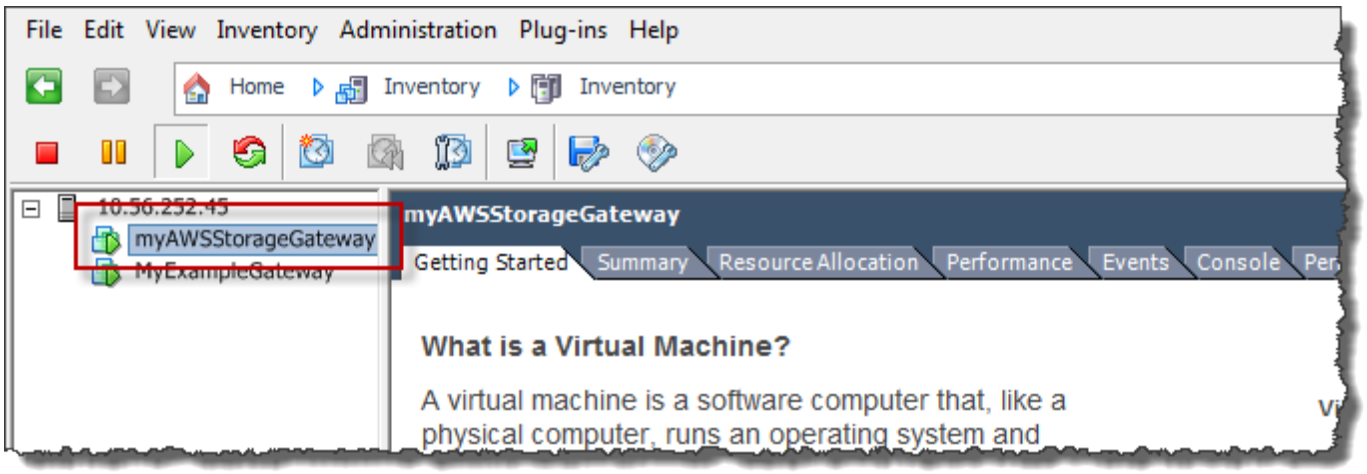


使用 VMware ESXi 存取閘道本機主控台

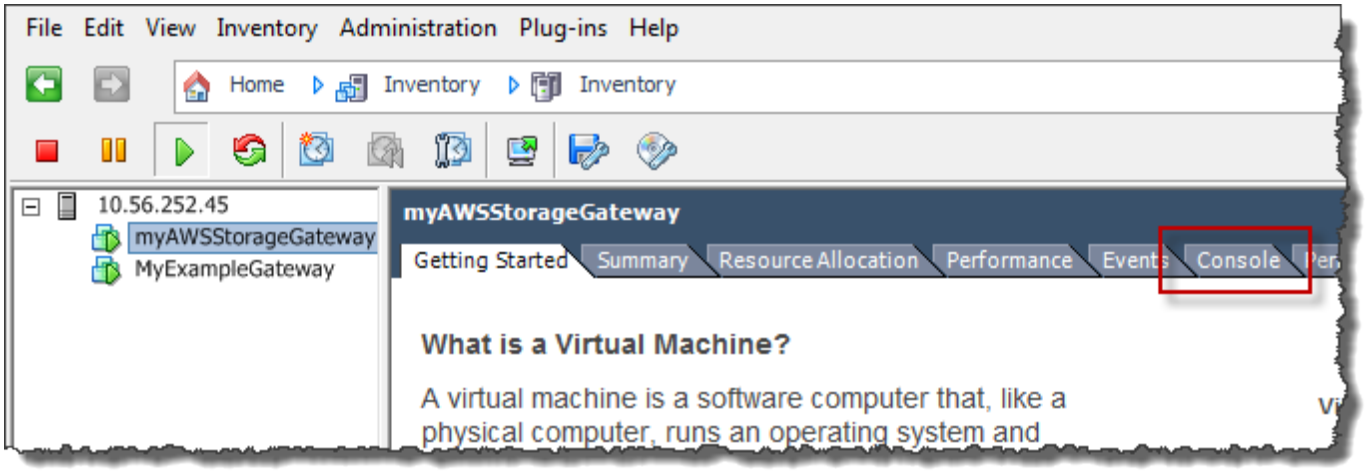
使用 VMware ESXi 存取閘道的本機主控台

1. 在 VMware vSphere 用戶端中，選取您的閘道 VM。
2. 確定已開啟閘道。

> **Note**
>
> 如果已開啟您的閘道 VM，則會顯示綠色箭頭圖示與 VM 圖示，如下列螢幕擷取畫面所示。如果未開啟您的閘道 VM，則可以選擇 Toolbar (工具列) 選單上的綠色 Power On (開機) 圖示予以開啟。

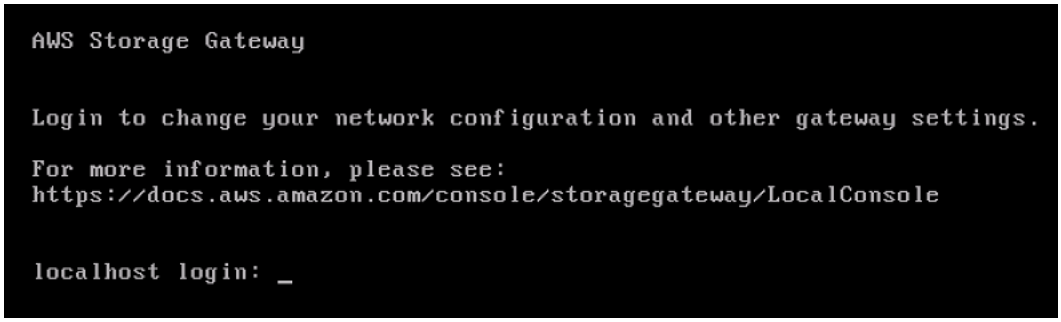


3. 選擇 Console (主控台) 標籤。



在一段時間之後，VM 就會準備好可供您登入。

> **Note**
>
> 若要從主控台視窗釋出該游標，請按 Ctrl+Alt。



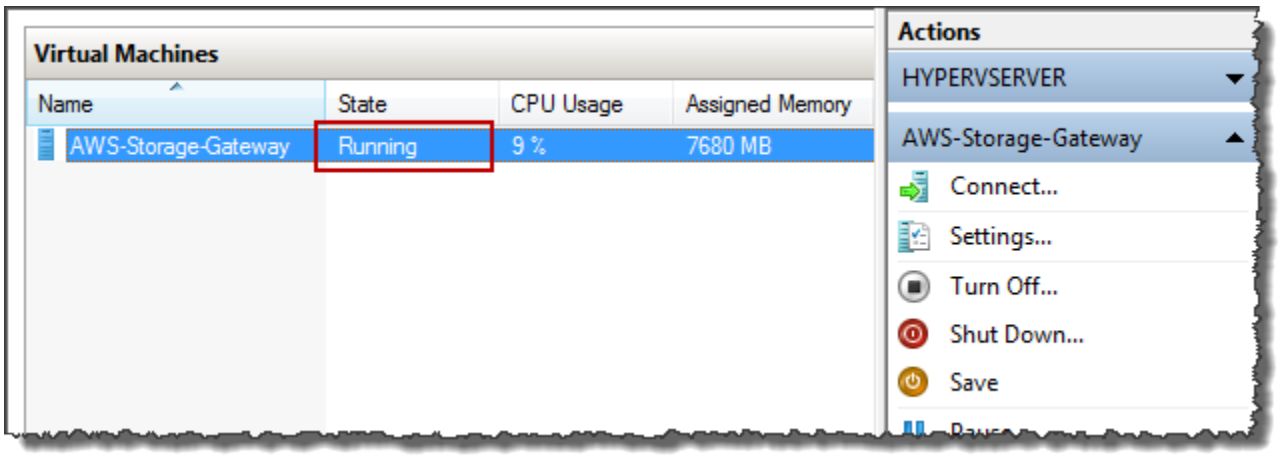
4. 若要使用預設登入資料登入，請繼續登入到文件閘道本機主控台程序。

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)

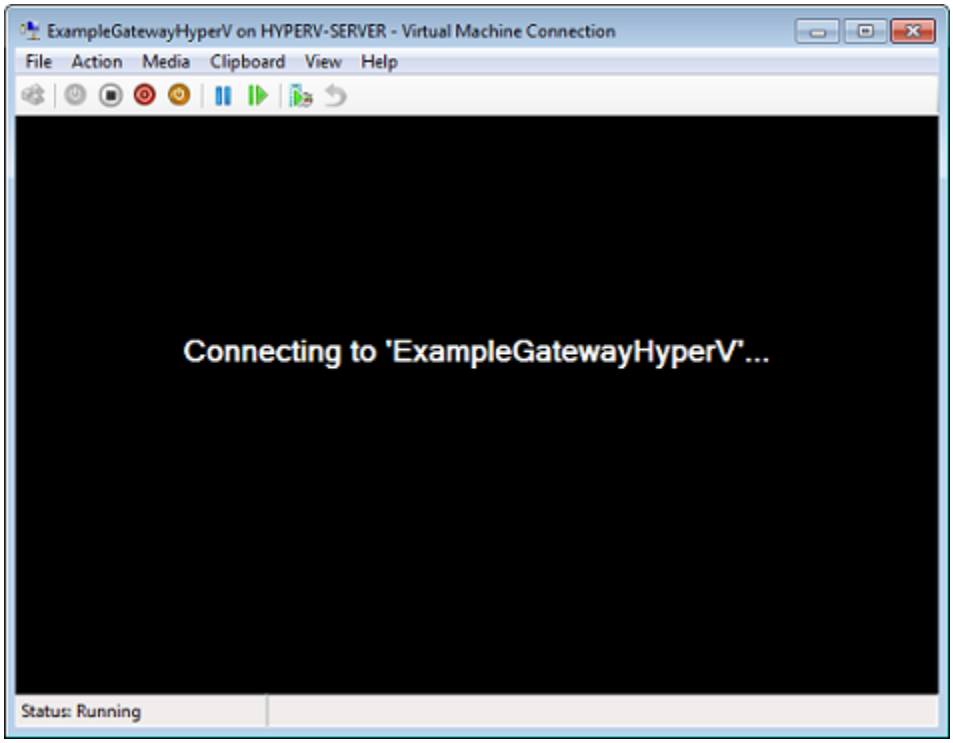
1. 在 Microsoft Hyper-V 管理員的 Virtual Machines (虛擬機器) 清單中，選取您的閘道 VM。
2. 確定已開啟閘道。

> **Note**
>
> 如果您的閘道 VM 處於開啟狀態，Running顯示為國家，如下列螢幕快照所示。若您的閘道 VM 尚未開啟，您可以透過在 Actions (動作) 窗格中選擇 Start (啟動) 來開啟它。



3. 在 Actions (動作) 窗格中，選擇 Connect (連線)。

Virtual Machine Connection (虛擬機器連線) 視窗即會顯示。若出現身份驗證視窗，請輸入虛擬化管理程序管理員提供給您的使用者名稱及密碼。



在一段時間之後，VM 就會準備好可供您登入。

4. 若要使用預設登入資料登入，請繼續登入到文件閘道本機主控台程序。

為您的閘道設定網路轉接器

在本章節中，您可以找到有關如何為您的閘道設定多個網路轉接器的資訊。

主題

- 針對 VMware ESXi 主機中的多張 NIC 設定您的閘道

- 在 Microsoft Hyper-V 主機中為多張 NIC 設定您的閘道

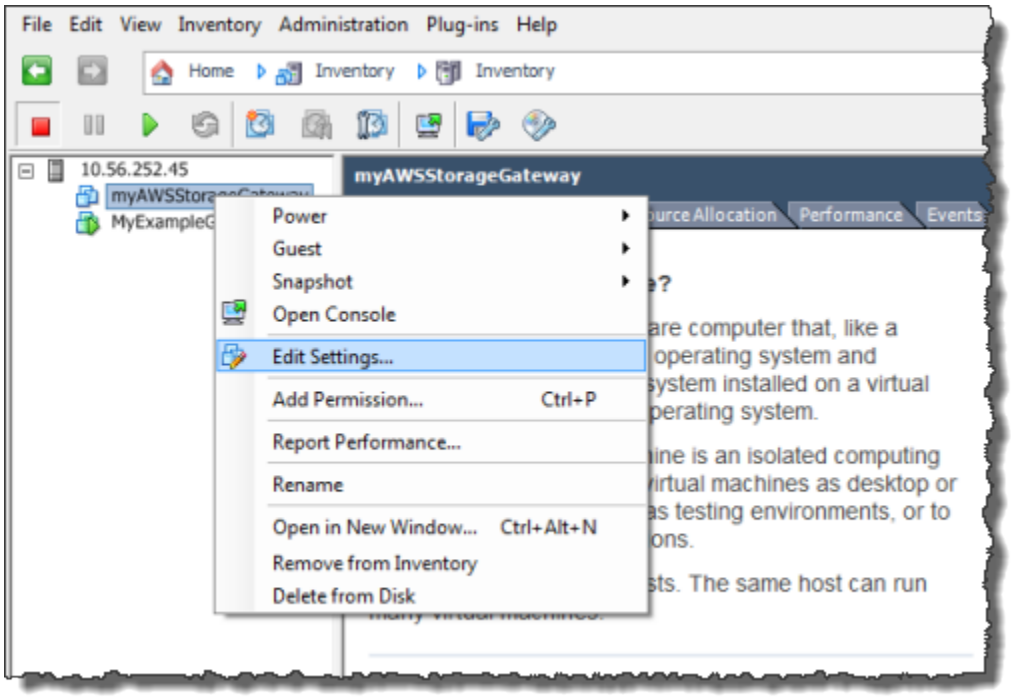
針對 VMware ESXi 主機中的多張 NIC 設定您的閘道

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。下列程序顯示如何新增 VMware ESXi 的轉接器。

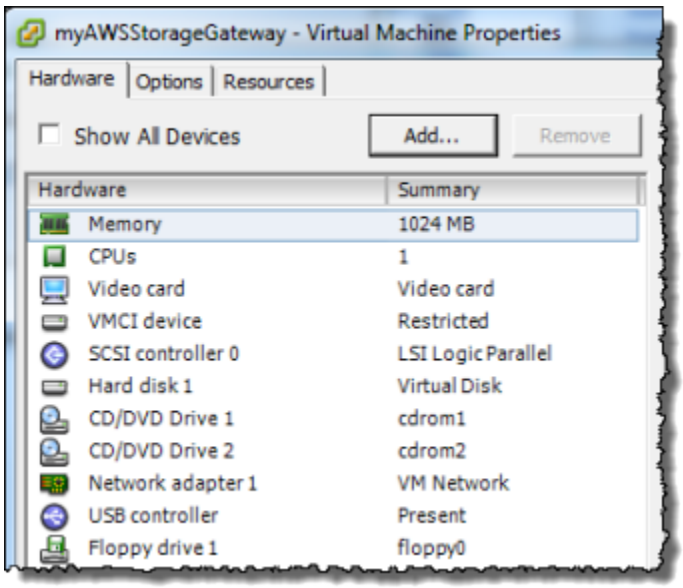
將閘道設定為使用 VMware ESXi 主機中的其他網路轉接器

1. 關機閘道。
2. 在 VMware vSphere 用戶端中，選取您的閘道 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)。

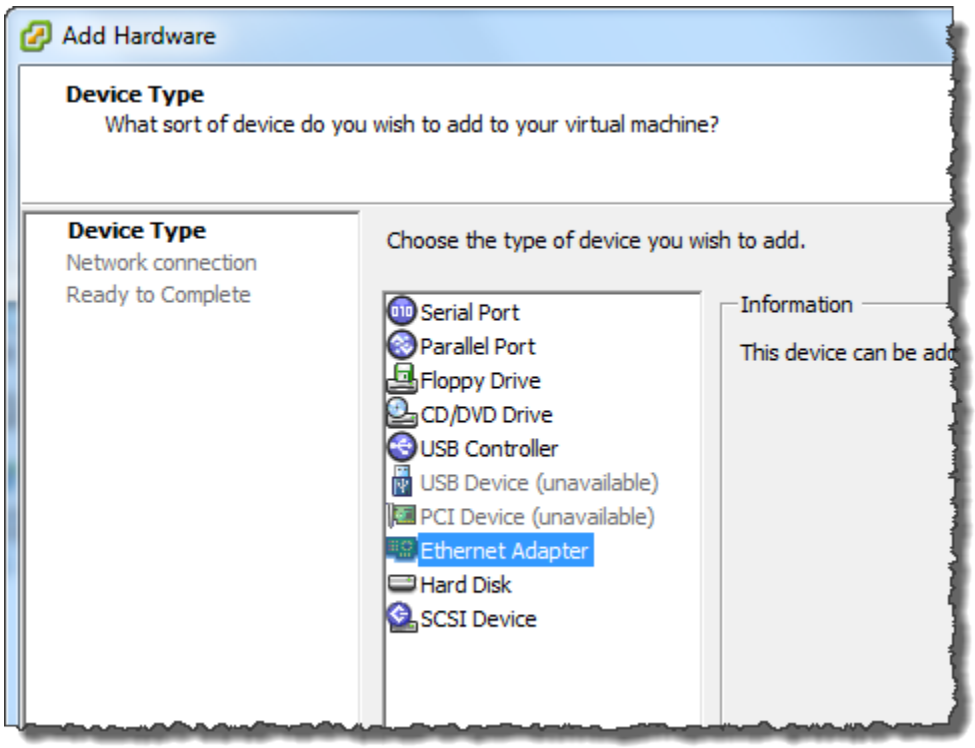


4. 在 Virtual Machine Properties (虛擬機器屬性) 對話方塊的 Hardware (硬體) 標籤上，選擇 Add (新增) 新增裝置。



5. 遵循 Add Hardware (新增硬體) 精靈來新增網路轉接器。

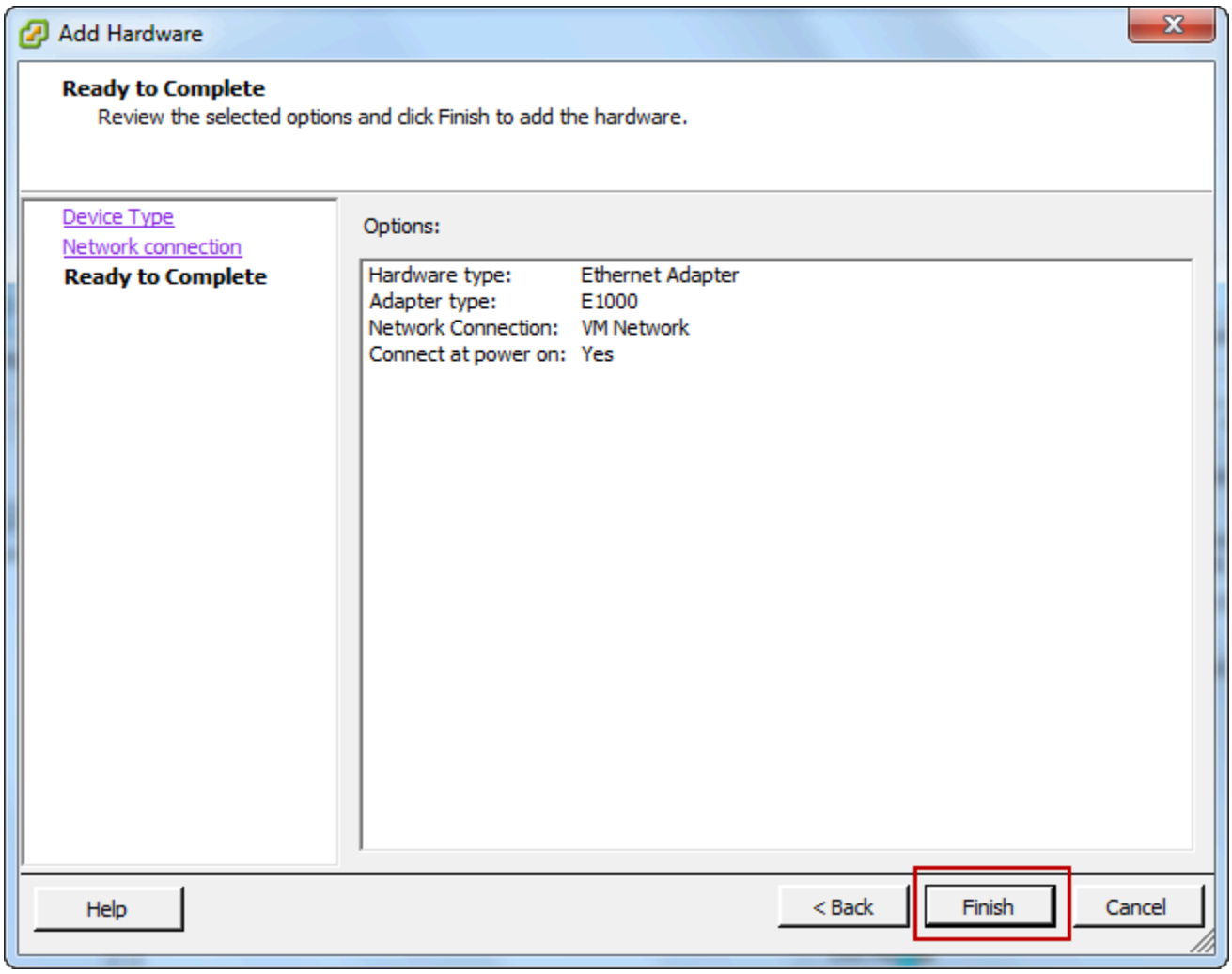
   a. 在 Device Type (裝置類型) 窗格中，選擇 Ethernet Adapter (乙太網路轉接器) 新增轉接器，然後選擇 Next (下一步)。



   b. 在 Network Type (網路類型) 窗格中，確定已針對 Type (類型) 選取 Connect at power on (在開機時連線)，然後選擇 Next (下一步)。

建議您搭配使用 E1000 網路轉接器與 Storage Gateway。如需可能出現在轉接器清單中之轉接器類型的詳細資訊，請參閱 ESXi 和 vCenter 伺服器文件中的網路轉接器類型。

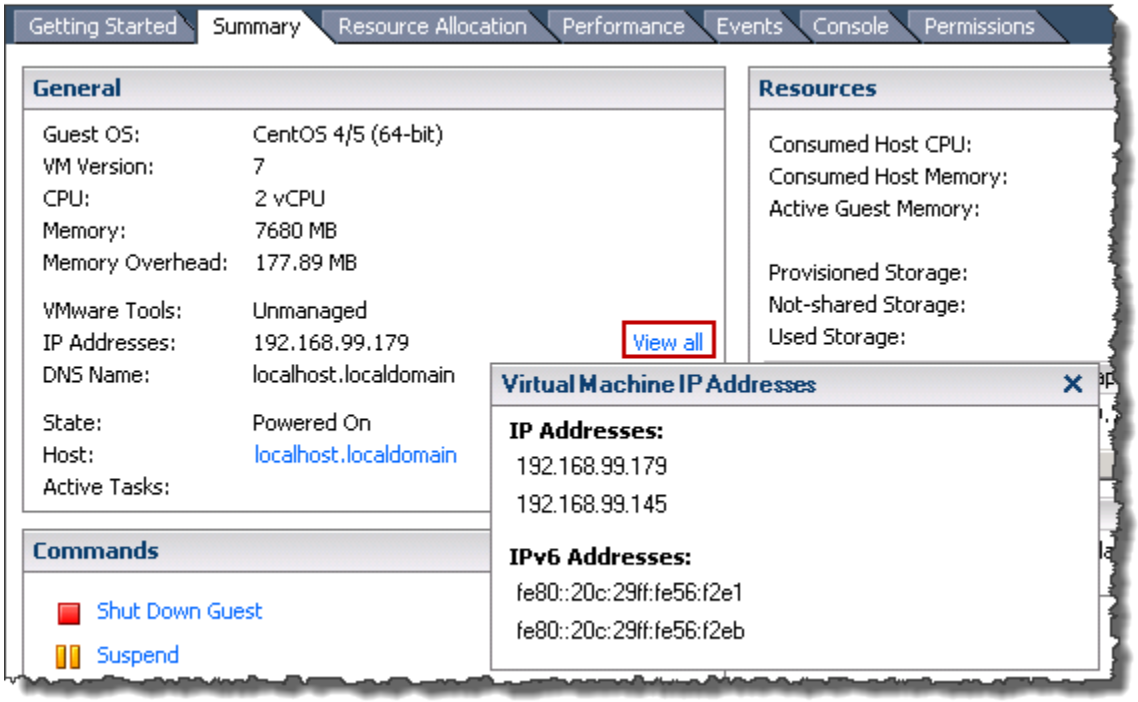
c. 在 Ready to Complete (準備好完成) 窗格中，檢閱資訊，然後選擇 Finish (完成)。



6. 選擇摘要選項卡，然後選擇查看全部旁邊的IP 地址框。Virtual Machine IP Addresses (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。

下圖僅供說明。實際上，其中一個 IP 地址會是閘道用來與 AWS 通訊的地址，而另一個地址會是不同子網路中的地址。



7. 在 Storage Gateway 主控台上，開啟閘道。
8. 在 中Navigation (導覽)窗格 Storage Gateway，選擇閘道，然後選擇您已新增轉接器的閘道。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 主機之本機主控台常見任務的詳細資訊，請參閱在 VM 本機主控台（文件閘道）上執行任務

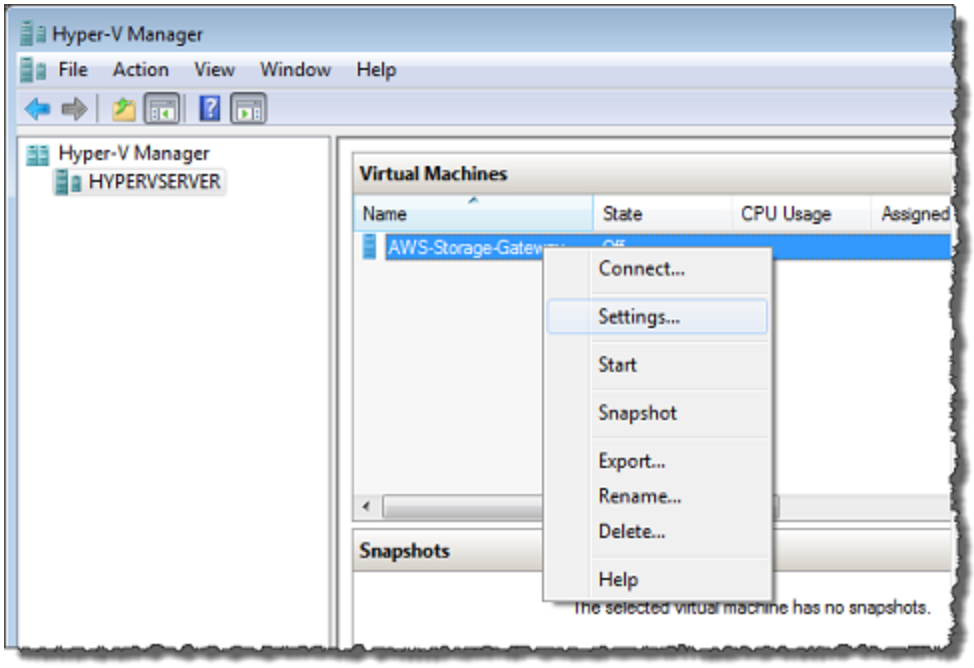
在 Microsoft Hyper-V 主機中為多張 NIC 設定您的閘道

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

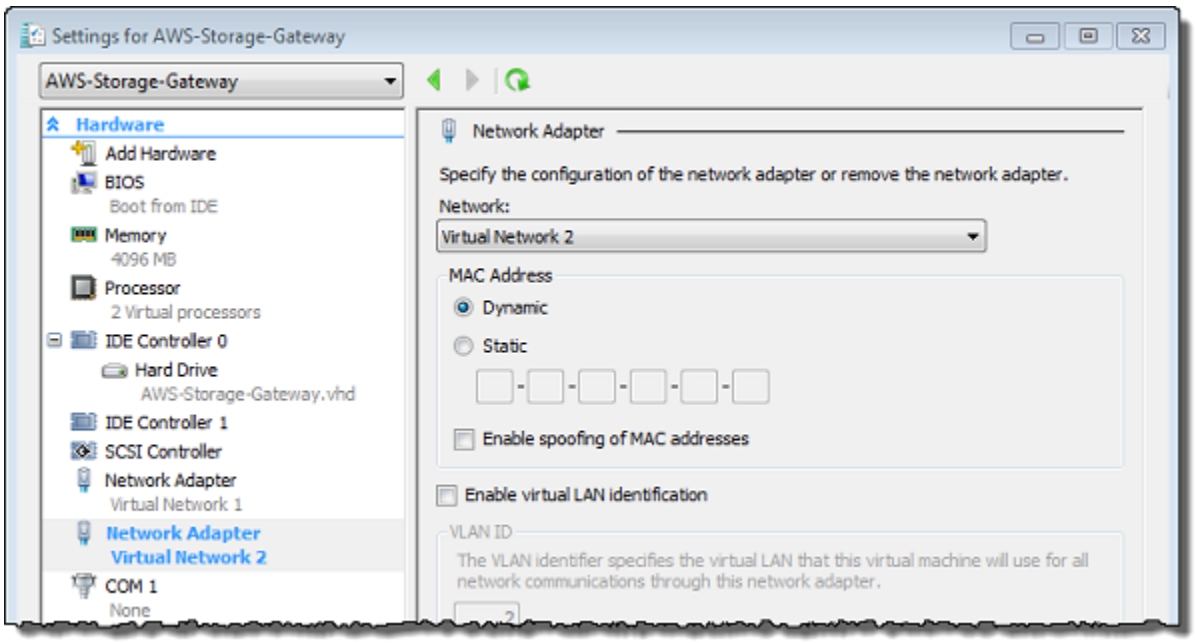
1. 在 Storage Gateway 主控台上，關閉閘道。
2. 在 Microsoft Hyper-V 管理員中，選取您的閘道 VM。
3. 若 VM 尚未關閉，請開啟您閘道的內容 (按右鍵) 選單，然後選擇 Turn Off (關閉)。

4. 在用戶端中，開啟您閘道 VM 的內容選單，然後選擇 Settings (設定)。



5. 在 VM 的 Settings (設定) 對話方塊中，針對 Hardware (硬體)，選擇 Add Hardware (新增硬體)。
6. 在 Add Hardware (新增硬體) 窗格中，選擇 Network Adapter (網路轉接器)，然後選擇 Add (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。

   在下列範例中，已為新的轉接器選取 Virtual Network 2 (虛擬網路 2)。



8. 在 Settings (設定) 對話方塊中，針對 Hardware (硬體)，確認已新增第二個轉接器，然後選擇 OK (確定)。
9. 在 Storage Gateway 主控台上，開啟閘道。
10. 在 Navigation (導覽) 窗格中，選擇 Gateways (閘道)，然後選取您已新增轉接器的閘道。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 主機之本機主控台常見任務的詳細資訊，請參閱在 VM 本機主控台（文件閘道）上執行任務

使用 AWS Storage Gateway 主控台刪除閘道以及移除相關聯資源

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。

閘道一旦刪除，就不會再顯示於 AWS Storage Gateway 管理主控台中，並會關閉其與啟動器的 iSCSI 連線。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。

您可以使用存放閘道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閘道主控台刪除 Storage Gateway 的相關資訊。如果您要以程式設計方式刪除閘道，請參AWS Storage GatewayAPI 參考。

主題

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。

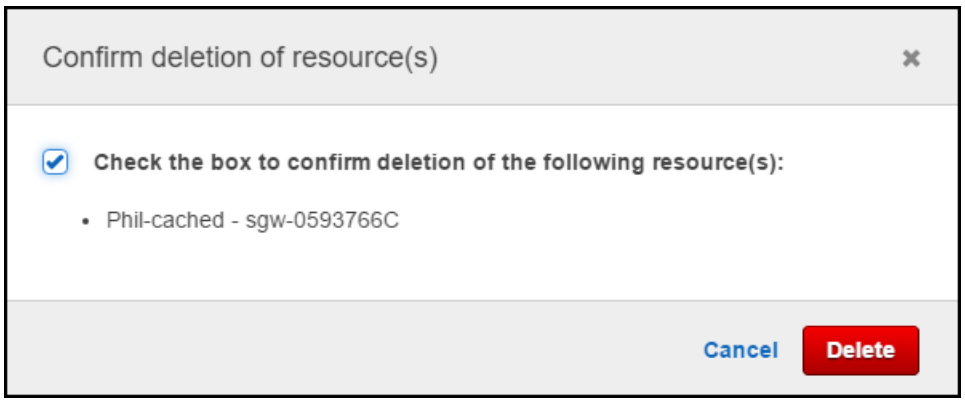
> **Note**
>
> 針對 Amazon EC2 執行個體上所部署的閘道，除非您刪除執行個體，否則執行個體會持續存在。
> 針對虛擬機器 (VM) 上所部署的閘道，在您刪除閘道之後，閘道 VM 仍然會存在於您的虛擬化環境中。若要移除虛擬機器，請使用 VMware vSphere 用戶端、Microsoft Hyper-V 管理員或 Linux 核心型虛擬機器 (KVM) 用戶端來連線到主機並移除該虛擬機器。請注意，您無法重複使用已刪除的閘道 VM 來啟用新的閘道。

刪除閘道

1. Storage Gatewayhttps://console.aws.amazon.com/storagegateway/home。
2. 在導覽窗格中，選擇 Gateways (閘道)，然後選擇您要刪除的閘道。
3. 針對 Actions (動作)，選擇 Delete gateway (刪除閘道)。
4.

> **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，就無法可以復原。

在出現的確認對話方塊中，選取核取方塊以確認刪除。請確定列出的閘道 ID 指定您要刪除的閘道，然後選擇 Delete (刪除)。



Important

在您刪除閘道之後，就不再需要支付軟體費用，但會保留虛擬磁帶、Elastic Block Store (Amazon EBS) 快照和 Amazon EC2 執行個體這類資源。您將會繼續支付這些資源的費用。您可以取消 Amazon EC2 訂閱，以選擇移除 Amazon EC2 執行個體和 Amazon EBS 快照。如果您想要保留訂，則可以使用 Amazon EC2 主控台刪除 Amazon EBS 快照。

從現場部署的閘道移除資源

您可以使用下列說明，從現場部署的閘道移除資源。

從 VM 上所部署的磁碟區閘道移除資源

如果您要刪除的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：

- 刪除閘道。

從 Amazon EC2 執行個體上所部署的閘道移除資源

如果您要刪除 Amazon EC2 執行個體上所部署的閘道，則建議您清除AWS與閘道搭配使用的資源，這樣做有助於避免意外的使用費。

從 Amazon EC2 上所部署的快取磁碟區移除資源

如果您已在 EC2 上部署具有快取磁碟區的閘道，則建議您採取下列動作來刪除閘道以及清除其資源：

1. 在 Storage Gateway 主控台中，刪除閘道，如使用 Storage Gateway 主控台刪除閘道。

2. 在 Amazon EC2 主控台中，如果您打算再次使用執行個體，則請停止 EC2 執行個體。否則，請終止執行個體。如果您打算刪除磁碟區，則請先記下連接至執行個體的區塊型儲存設備以及儲存設備的識別符，再終止執行個體。您需要這些項目才能識別您要刪除的磁碟區。
3. 在 Amazon EC2 主控台中，如果您不打算再次使用所有連接至執行個體的 Amazon EBS 磁碟區，則請予以移除。如需詳細資訊，請參閱「」清理您的實例和卷中的Amazon EC2 Linux 執行個體使用者指南。

將現有文件網關替換為新實例

您可以隨着數據和性能需求的增長或收到AWS通知遷移閘道。如果您希望將網關移動到更好的主機平台或更新的 Amazon EC2 實例，或刷新底層服務器硬件，則可能需要執行此操作。

有兩種方法可以替換現有的文件網關。下表描述了每種方法的優點和缺點。使用此信息，選擇最適合您的網關環境的方法，然後參閱下面相應部分中的過程步驟。

	方法 1：將緩存磁盤和網關 ID 遷移到替換實例	方法 2：使用空緩存磁盤和新網關 ID 替換實例
緩存磁碟區數據	緩存磁盤上的數據將被保留。如果您的網關具有較大的緩存磁盤，或者您的應用程序對緩存超出讀取操作導致的延遲敏感，則此方法非常有用。	緩存中的數據從AWS雲端。如果您的應用程序能夠容忍緩存外讀取導致的延遲，則此方法最適合寫入繁重的工作負載。
停機時間	在遷移過程中，您的網關將處於離線狀態 1-2 小時。	沒有停機時間。現有網關可以與替換網關同時使用，直到您選擇將其刪除為止。在使用兩個網關時，不支持多個寫入程序。
閘道 ID	新網關從它替換的網關繼承網關 ID。	現有網關和替換網關具有獨立的唯一網關 ID。

> **Note**
>
> 數據只能在相同類型的閘道之間移動。

方法 1：將緩存磁盤和網關 ID 遷移到替換實例

要將文件網關的緩存磁盤和網關 ID 遷移到替換實例，請執行以下操作：

1. 停止正在寫入現有檔案閘道的所有應用程式。

2. 請驗證CachePercentDirty的指標監控選項卡為0。
3. 通過使用虛擬機管理程序控件關閉主機虛擬機 (VM) 的電源來關閉現有文件網關。

   如需關閉 Amazon EC2 執行個體的詳細資訊，請參停止和啟動執行個體中的Amazon EC2 使用者指南。

   有關關閉 KVM、VMware 或 Hyper-V 虛擬機的詳細信息，請參閱虛擬機管理程序文檔。
4. 從舊網關 VM 分離所有磁盤，包括根磁盤、緩存磁盤和上傳緩衝區磁盤。

   > **Note**
   >
   > 記下根磁盤的卷 ID 以及與該根磁盤關聯的網關 ID。您需要在稍後的步驟中將此磁盤與新的存儲網關虛擬機管理程序分離。

   如果您使用 Amazon EC2 實例作為文件網關的 VM，請參閱將 Amazon EBS 磁碟區與 Windows 執行個體分開或者將 Amazon EBS 磁碟區與 Linux 執行個體分開中的Amazon EC2 使用者指南。

   如需將磁碟區與 KVM、VMware 或 Hyper-V VM 分離開磁碟區的信息，請參您的虛擬機管理程序的檔案。
5. 建立新AWSStorage Gateway 虛擬機管理程序虛擬機實例，但不要將其激活為網關。在後面的步驟中，此新 VM 將採用舊網關的標識。

   如需建立新的 Storage Gateway VM 的詳細資訊，請參選擇主機平台並下載 VM。

   > **Note**
   >
   > 請勿為新 VM 添加緩存磁盤。此 VM 將使用與舊 VM 使用的相同緩存磁盤。
6. 將新的 Storage Gateway VM 配置為使用與舊 VM 相同的網絡設置。

   閘道的預設網路組態為動態主機設定通訊協定 (DHCP)。使用 DHCP，您的閘道會自動指派 IP 地址。

   如果您需要手動設定閘道 VM 的靜態 IP 地址，請參設定您的閘道網路。

   如果您的閘道 VM 必須使用 Socket Secure 5 版 (SOCKS5) 代理組態，請參透過代理路由您的現場部署閘道。
7. 啟動新的 Storage Gateway 虛擬機。

8. 將您從舊網關 VM 分離的磁盤附加到新的網關 VM。請勿將現有根磁盤與新網關 VM 分離。

> **Note**
>
> 要成功遷移，所有磁盤必須保持不變。更改磁盤大小或其他值會導致元數據不一致，從而阻止成功遷移。

9. 通過使用以下格式的 URL 連接到新 VM 來啟動網關遷移過程：

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

   對於新網關 VM，您可以使用與舊網關 VM 相同的 IP 地址。您的 URL 看起來應該如下列範例：

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

   從瀏覽器或使用 cURL 從命令行使用此 URL。

   成功啟動網關遷移後，將顯示以下消息：

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

10. 等待閘道狀態顯示為執行中中的AWSStorage Gateway 控台。根據可用帶寬，此操作最多需要 10 分鐘的時間。
11. 停止新的 Storage Gateway 虛擬機。
12. 從新網關分離舊網關的根磁盤（您先前記錄了其卷 ID）。
13. 啟動新的 Storage Gateway 虛擬機。
14. 如果您的閘道加入 Active Directory 網域，請重新加入該域。如需說明，請參閱「」設定 Microsoft Active Directory 存取。

> **Note**
>
> 即使文件網關的狀態顯示為已參加。

15. 確認您的共享在新網關 VM 的 IP 地址上可用，然後刪除舊網關 VM。

> **Warning**
>
> 閘道一旦刪除，就無法可以復原。

如需刪除 Amazon EC2 執行個體的詳細資訊，請參終止您的執行個體中的Amazon EC2 使用者指南。如需刪除 KVM、VMware 或 Hyper-V VM 的詳細資訊，請參您的虛擬機管理程序的檔案。

方法 2：使用空緩存磁盤和新網關 ID 替換實例

要使用空緩存磁盤和新的網關 ID 設置替換文件網關實例，請執行以下操作：

1. 停止正在寫入現有檔案閘道的所有應用程式。請驗證CachePercentDirty的指標監控標籤為0，然後再在新網關上設置文件共享。
2. 使用AWS Command Line Interface(AWS CLI），通過執行以下操作來收集並保存有關現有文件網關和文件共享的配置信息：

   a. 保存文件網關的網關配置信息。

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

   此命令輸出 JSON 塊，其中包含閘道相關的元數據，例如其名稱、網路界面、設定的時區，以及狀態 (無論閘道是否在執行中)。

   b. 保存檔案閘道的伺服器訊息區塊 (SMB) 設置。

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

   此命令輸出一個 JSON 塊，其中包含有關 SMB 文件共享的元數據，例如其域名、Microsoft 活動目錄狀態、是否設置來竇密碼以及安全策略的類型。

   c. 為文件網關的每個 SMB 和網絡文件系統 (NFS) 文件共享保存文件共享信息：

   - 對 SMB 文件共享使用以下命令。

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

     此命令輸出一個 JSON 塊，其中包含有關 NFS 文件共享的元數據，例如其名稱、存儲類、狀態、IAM 角色 Amazon 資源名稱 (ARN)、允許訪問文件網關的客户端列表以及 SMB 客户端用於標識裝載點的路徑。

- 使用 NFS 檔案共享的下列命令。

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

此命令輸出一個 JSON 塊，其中包含有關 NFS 文件共享的元數據，例如其名稱、存儲類、狀態、IAM 角色 ARN、允許訪問文件網關的客户端列表以及 NFS 客户端用於標識裝載點的路徑。

3. 通過執行以下操作停止現有文件網關：

   a. 停止正在寫入現有檔案閘道的所有應用程式。請驗證`CachePercentDirty`的指標監控標籤為`0`，然後再在新網關上設置文件共享。

   b. 通過關閉託管網關的虛擬機 (VM) 電源來停止現有文件網關。

4. 建立新檔案閘道。
5. 裝載在舊網關上配置的文件共享。
6. 確認新網關工作正常，然後從 Storage Gateway 控制台中刪除舊網關。

> **Important**
>
> 刪除閘道之前，請確定目前沒有應用程式寫入至檔案閘道的緩存中。如果您刪除使用中的檔案閘道，則資料可能會丟失。

> **Warning**
>
> 閘道一旦刪除，就無法可以復原。

7. 刪除舊網關虛擬機或 EC2 實例。

效能

在本節中，您可以找到有 Storage Gateway 效能的資訊。

主題

關於文件網關的效能指南

在此章節，您可以找到為檔案閘道 VM 佈建硬體的組態指引。資 Amazon EC2 表中的執行個體大小和類型為範例，僅供參考。

若要獲得最佳效能，必須將快取磁碟大小調整到實際運作集合的大小。使用多個本機磁碟的快取，藉由平行存取資料提高寫入效能，並提高 IOPS。

在下表中,快取命中讀取作業是指來自快取服務之檔案共享的讀取數。快取未命中讀取作業是指來自 Amazon S3 服務之檔案共享的讀取數。

> **Note**
>
> 我們不建議使用暫時性儲存。如需使用暫時性儲存的詳細資訊，請參閱將臨時存儲與 EC2 網關結合使用。

以下是示例文件網關配置。

S3 文件網關在 Linux 客户端上的性能

範例組態	通訊協定	寫入吞吐量（文件大小為 1 GB）	快取命中讀取輸送量	快取遺漏讀取輸送量
根磁碟：80 GB、4,000 IOPS	NFS3-1 個線程	110 兆字/秒 (0.92 千兆位)	590 MiB/s (4.9 Gbps)	310 兆兆/秒 (2.6 千兆位)

範例組態	通訊協定	寫入吞吐量（文件大小為 1 GB）	快取命中讀取輸送量	快取遺漏讀取輸送量
快取磁碟：512 GiB 快取、io1、1,500 個預配 IOPS 最低網路效能：10 Gbps CPU：16 vCPU | RAM：32 GB 推薦用於 Linux 的 NFS 協議	NFS3-8 個線程	160 MiB/s (1.3 Gbps)	590 MiB/s (4.9 Gbps)	335 MiB/s (2.8 Gbps)
	NFS4-1 個線程	130 兆兆/秒 (1.1 千兆位)	590 MiB/s (4.9 Gbps)	295 MiB/s (2.5 Gbps)
	8 個線程	160 MiB/s (1.3 Gbps)	590 MiB/s (4.9 Gbps)	335 MiB/s (2.8 Gbps)
	SMBV3-1 個線程	115 MiB/s (1.0 Gbps)	每秒 325 兆幣/秒 (2.7 千兆位)	255 兆兆/秒 (2.1 千兆位)
	SMBV3-8 個線程	190 兆兆/秒 (1.6 千兆位)	590 MiB/s (4.9 Gbps)	335 MiB/s (2.8 Gbps)
Storage Gateway 硬體設備 最低網路效能：10 Gbps	NFS3-1 個線程	265 MiB/s (2.2 Gbps)	590 MiB/s (4.9 Gbps)	310 兆兆/秒 (2.6 千兆位)
	NFS3-8 個線程	385 兆兆/秒 (3.1 千兆位)	590 MiB/s (4.9 Gbps)	335 MiB/s (2.8 Gbps)
	NFS4-1 個線程	310 兆兆/秒 (2.6 千兆位)	590 MiB/s (4.9 Gbps)	295 MiB/s (2.5 Gbps)
	8 個線程	385 兆兆/秒 (3.1 千兆位)	590 MiB/s (4.9 Gbps)	335 MiB/s (2.8 Gbps)
	SMBV3-1 個線程	275 兆兆/秒 (2.4 千兆/秒)	每秒 325 兆幣/秒 (2.7 千兆位)	255 兆兆/秒 (2.1 千兆位)
	SMBV3-8 個線程	455 MiB/s (3.8 Gbps)	590 MiB/s (4.9 Gbps)	335 MiB/s (2.8 Gbps)

範例組態	通訊協定	寫入吞吐量（文件大小為 1 GB）	快取命中讀取輸送量	快取遺漏讀取輸送量
根磁碟：80 GB、io1 SSD、4,000 IOPS 緩存磁盤：4 x 2 TB NVME 緩存磁盤 最低網路效能：10 Gbps CPU：32 vCPU | RAM：244 GB 推薦用於 Linux 的 NFS 協議	NFS3-1 個線程	300 MiB/s (2.5 Gbps)	590 MiB/s (4.9 Gbps)	每秒 325 兆幣/秒 (2.7 千兆位)
	NFS3-8 個線程	585 MiB/s (4.9 Gbps)	590 MiB/s (4.9 Gbps)	580 MiB/s (4.8 Gbps)
	NFS4-1 個線程	355 MiB/s (3.0 Gbps)	590 MiB/s (4.9 Gbps)	340 MiB/s (2.9 Gbps)
	8 個線程	575 MiB/s (4.8 Gbps)	590 MiB/s (4.9 Gbps)	575 MiB/s (4.8 Gbps)
	SMBV3-1 個線程	230 MiB/s (1.9 Gbps)	每秒 325 兆幣/秒 (2.7 千兆位)	245 MiB/s (2.0 Gbps)
	SMBV3-8 個線程	585 MiB/s (4.9 Gbps)	590 MiB/s (4.9 Gbps)	580 MiB/s (4.8 Gbps)

Windows 客户端上的文件網關性能

範例組態	通訊協定	寫入吞吐量（文件大小為 1 GB）	快取命中讀取輸送量	快取遺漏讀取輸送量
根磁碟：80 GB io1、4,000 IOPS 快取磁碟：512 GiB 快取、io1、1,500 個預配 IOPS 最低網路效能：10 Gbps CPU：16 vCPU | RAM：32 GB	SMBV3-1 個線程	150 MiB/s (1.3 Gbps)	180 MiB/s (1.5 Gbps)	20 MiB/s (0.2 Gbps)
	SMBV3-8 個線程	190 兆兆/秒 (1.6 千兆位)	335 MiB/s (2.8 Gbps)	195 兆兆/秒 (1.6 千兆位)
	NFS3-1 個線程	95 MiB/s (0.8 Gbps)	130 兆兆/秒 (1.1 千兆位)	20 MiB/s (0.2 Gbps)
	NFS3-8 個線程	190 兆兆/秒 (1.6 千兆位)	330 MiB/s (2.8 Gbps)	190 兆兆/秒 (1.6 千兆位)

範例組態	通訊協定	寫入吞吐量（文件大小為 1 GB）	快取命中讀取輸送量	快取遺漏讀取輸送量
建議用於視窗的中小型企業協議				
Storage Gateway 硬體設備 最低網路效能：10 Gbps	SMBV3-1 個線程	230 MiB/s (1.9 Gbps)	255 兆兆/秒 (2.1 千兆位)	20 MiB/s (0.2 Gbps)
	SMBV3-8 個線程	835 MiB/s (7.0 Gbps)	475 MiB/s (4.0 Gbps)	195 兆兆/秒 (1.6 千兆位)
	NFS3-1 個線程	135 兆兆/秒 (1.1 千兆位)	185 兆兆/秒 (1.6 千兆位)	20 MiB/s (0.2 Gbps)
	NFS3-8 個線程	545 兆兆/秒 (4.6 千兆位)	470 MiB/s (4.0 Gbps)	190 兆兆/秒 (1.6 千兆位)
根磁碟：80 GB、io1 SSD、4,000 IOPS 緩存磁盤：4 x 2 TB NVME 緩存磁盤 最低網路效能：10 Gbps CPU：32 vCPU | RAM：244 GB 建議用於視窗的中小型企業協議	SMBV3-1 個線程	230 MiB/s (1.9 Gbps)	265 MiB/s (2.2 Gbps)	30 MiB/s (0.3 Gbps)
	SMBV3-8 個線程	835 MiB/s (7.0 Gbps)	780 MiB/s (6.5 Gbps)	250 兆兆/秒 (2.1 千兆位)
	NFS3-1 個線程	每秒 Gbps)	220 MiB/s (1.8 Gbps)	30 MiB/s (0.3 Gbps)
	NFS3-8 個線程	545 兆兆/秒 (4.6 千兆位)	570 MiB/s (4.8 Gbps)	240 MiB/s (2.0 Gbps)

> **Note**
>
> 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。

最佳化閘道效能

您可以在下列內容中找到最佳化閘道效能的方法資訊。本指南是以將資源新增至您的閘道，以及將資源新增至您的應用程式伺服器為基礎。

新增資源至您的閘道

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

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 (SSD) 和 NVMe 控制器。您也可以將虛擬磁碟從儲存區區域網路 (SAN) 直接連接到您的 VM，而非從 Microsoft Hyper-V NTFS。改善的磁碟效能通常得以提供更高的輸送量及每秒輸入/輸出操作數 (IOPS)。如需新增磁碟的資訊，請參閱新增快取儲存。

若要測量輸送量，請使用`ReadBytes`和`WriteBytes`指標`Samples`Amazon CloudWatch 統計資訊。例如，將 5 分鐘範例期間內 `Samples` 指標的 `ReadBytes` 統計資料除以 300 秒，便可取得 IOPS。做為一般規則，當您檢閱閘道的這些指標時，請尋找低輸送量及低 IOPS 趨勢，以指出磁碟相關的瓶頸。

> **Note**
>
> CloudWatch 指標不適用於所有網關。有关网关指标的信息，请参阅监視檔案閘道。

新增 CPU 資源至您的閘道主機

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 的四個虛擬處理器受到四個核心的支援。此外，確認您沒有過度訂閱主機伺服器的 CPU。

將額外的 CPU 新增到閘道主機伺服器時，您會提高閘道的處理容量。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至您的本機儲存以及將此資料上傳至 Amazon S3。額外的 CPU 也可

協助確保您的閘道在主機與其他 VM 共享時，也能取得足夠的 CPU 資源。提供足夠的 CPU 資源對於改善輸送量具有一般性的效果。

「Storage Gateway」支援在您的網關主機服務器中使用 24 個 CPU。您可以使用 24 個 CPU 大幅改善您的閘道效能。我們建議您的閘道主機伺服器使用下列閘道組態：

- 24 個 CPU。
- 16 GiB 預留 RAM 用於文件網關
  - 16 GiB 的保留內存，用於高速緩存大小高達 16 TiB 的網關
  - 32 GiB 的保留內存，用於高速緩存大小為 16 TiB 至 32 TiB 的網關
  - 48 GiB 的保留內存，用於高速緩存大小為 32 TiB 至 64 TiB 的網關
- 連接到全虛擬控制器 1 的磁碟 1，做為閘道快取使用，如下所示：
  - 使用 NVMe 控制器的 SSD。
- 連接到全虛擬控制器 1 的磁碟 2，做為閘道上傳緩衝使用，如下所示：
  - 使用 NVMe 控制器的 SSD。
- 連接到全虛擬控制器 2 的磁碟 3，做為閘道上傳緩衝使用，如下所示：
  - 使用 NVMe 控制器的 SSD。
- 在 VM 網路 1 上設定的網路轉接器 1：
  - 使用 VM 網路 1 及新增用於擷取的 VMXnet3 (10 Gbps)。
- 在 VM 網路 2 上設定的網路轉接器 2：
  - 使用 VM 網路 2 及新增用於連線至 AWS 的 VMXnet3 (10 Gbps)。

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本機儲存體佈建本機磁碟。例如，針對 VMware ESXi，基礎實體儲存體資源會以資料存放區表示。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，使用較少高效能 RAID 組態 (例如 RAID 1) 支援的資料存放區，可能導致效能不佳。

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

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`ReadBytes`和`WriteBytes`度量來測量總數據吞吐量。

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。

新增 CPU 資源到您的應用程式環境

若您的應用程式可使用額外的 CPU 資源，則增加更多 CPU 可協助您的應用程式擴展其 I/O 負載。

將 VMware vSphere (VMware vSphere) 與 Storage Gateway 搭配使用

Storage Gateway 透過與 VMware vSphere High AvAvAvaisphere High Avalable (VMware HA) 整合應用程式層級運作狀態檢查，在 VMware 上提供高可用性 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。

藉由此整合，在 VMware 環境內部部署中或在 VMware Cloud on AWS 中部署的閘道，會在大多數服務中斷時自動復原。此操作通常會在 60 秒以內完成，而且不會遺失資料。

若要將 VMware HA 與 Storage Gateway 搭配使用，請執行下列步驟。

主題

- 設定 vSphere VMware HA 叢集
- 下載您的閘道類型的 .ova 映像
- 部署閘道
- (選用) 為叢集上的其他 VM 新增覆寫選項
- 啟用閘道
- 測試 VMware High Availability 組態

設定 vSphere VMware HA 叢集

首先，如果您尚未建立 VMware 叢集，請立即建立。如需如何建立 VMware 叢集的相關資訊，請參閱 VMware 文件中的建立 vSphere HA 叢集。

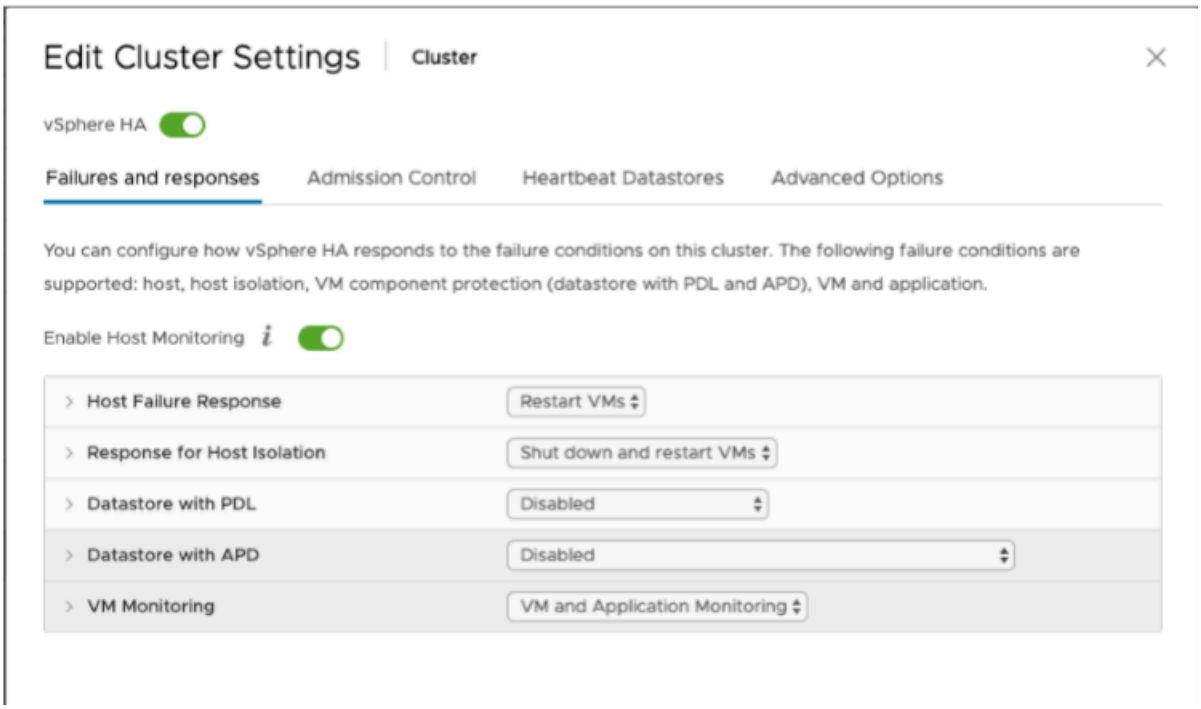
接下來，將 VMware 羣集配置為與 Storage Gateway 搭配使用。

設定 VMware 叢集

1. 在 VMware vSphere 的 Edit Cluster Settings (編輯叢集設定) 頁面上，確認已針對 VM 和應用程式監控設定 VM 監控。若要執行此操作，請依照列出內容設定下列選項：

   - 主機故障響應：重新啟動 VM
   - 主機隔離響應：關閉並重新啟動 VM
   - 具有 PDL 的資料存放區：已停用
   - 具有 APD 的資料存放區：已停用
   - VM 監控：VM 和應用程式監控

   如需範例，請參閱下列螢幕擷取畫面。



2. 調整下列的值以微調叢集敏感度：

   - 失敗間隔— 在此間隔後，如果未收到 VM 檢測信號，則會重新啟動 VM。

- 最短正常運行時間— 在 VM 啟動以開始監控 VM 工具的訊號後，羣集會等待這段指定的時間。
- 每個 VM 的最大重設次數— 在最大重設時間範圍內，羣集會重新啟動 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：

- Failure interval (失敗間隔)：**30** 秒
- Minimum uptime (最短執行時間)：**120** 秒
- 每個 VM 的最大重設次數：**3**
- Maximum resets time window (最大重設時間範圍)：**1** 小時

如果您在叢集上有其他正在執行的 VM，您可能會想要設定可供 VM 專用的這些值。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) 為叢集上的其他 VM 新增覆寫選項。

下載您的閘道類型的 .ova 映像

使用下列程序下載 .ova 映像。

下載您的閘道類型的 .ova 映像

- 從下列其中一個位置下載您的閘道類型的 .ova 映像：
  - 檔案閘道 —

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。

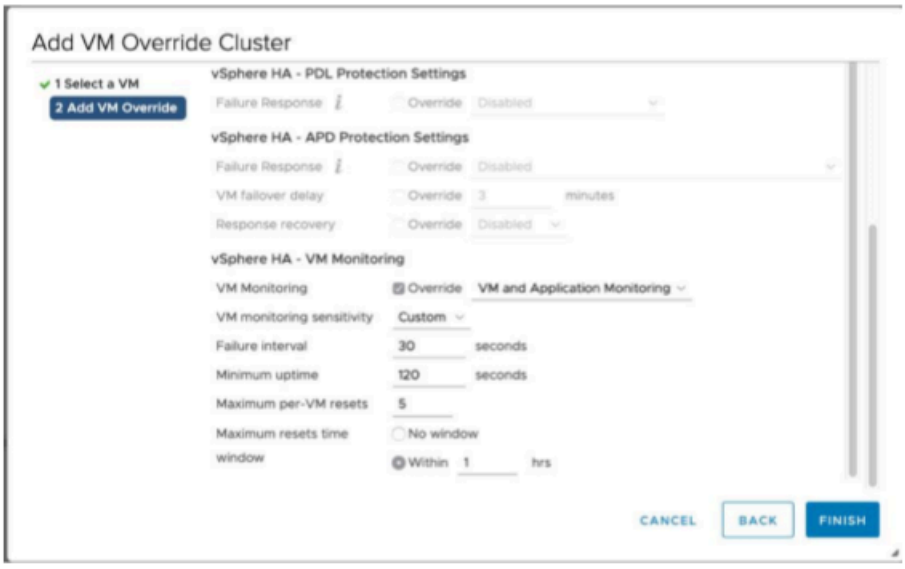
(選用) 為叢集上的其他 VM 新增覆寫選項

如果您在叢集上有其他正在執行的 VM，您可能會想要設定可供每個 VM 專用的叢集值。

為叢集上的其他 VM 新增覆寫選項

1. 在 VMware vSphere 的 Summary (摘要) 頁面上，選擇叢集以開啟叢集頁面，然後選擇 Configure (設定)。
2. 選擇 Configuration (組態) 標籤，然後選擇 VM Overrides (VM 覆寫)。
3. 新增 VM 覆寫選項以變更每個值。

   如需覆寫選項，請參閱下列螢幕擷取畫面。



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

- 根據您的閘道類型選擇啟用說明：
  - 檔案閘道 —

測試 VMware High Availability 組態

啟用閘道後，請測試您的組態。

測試 VMware HA 組態

1. 打開「Storage Gateway」控制台，請訪https://console.aws.amazon.com/storagegateway/home。
2. 在導覽窗格中，選擇 Gateways (閘道)，然後選擇您要測試 VMware HA 的閘道。
3. 針對 Actions (動作)，選擇 Verify VMware HA (驗證 VMware HA)。
4. 在出現的 Verify VMware High Availability Configuration (驗證 VMware High Availability 組態) 方塊中，選擇 OK (確定)。

   > **Note**
   >
   > 測試 VMware HA 組態會重新啟動閘道 VM 並中斷閘道連線。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料標籤中。
5. 選擇 Exit (退出)。

您可以在 Amazon CloudWatch 日誌組中找到有關 VMware HA 事件的資訊。如需詳細資訊，請參閱使用 CloudWatch 日誌組獲取文件網關運行狀況日誌。

中的安全AWSStorage Gateway

雲端安全是 AWS 最重視的一環。身為 AWS 客戶的您，將能從資料中心和網路架構的建置中獲益，以滿足組織最為敏感的安全要求。

安全是 AWS 與您共同肩負的責任。共同的責任模式將其稱為雲端的安全性和雲端中的安全性：

- 雲端本身的安全：AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。AWS 也提供您可安全使用的服務。第三方稽核人員會定期測試和驗證我們安全性的有效性，作為 AWS 合規計劃的一部分。若要了解適用於AWSStorage Gateway，請參AWS合規計劃的服務範圍。
- 雲端內部的安全 – 您的責任取決於所使用的 AWS 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。您還可以學習如何使用其他AWS服務，幫助您監控並保護 Storage Gateway 資源。

主題

- 中的資料保護AWSStorage Gateway
- 存儲 Gateway 的身份驗證和存取控制
- AWS Storage Gateway 中的記錄和監控
- 的合規驗證AWSStorage Gateway
- 中的恢復能力AWSStorage Gateway
- 中的基礎設施安全AWSStorage Gateway
- Storage Gateway 的安全最佳實務

中的資料保護AWSStorage Gateway

所以此AWS 共同責任模型適用於AWSStorage Gateway。如此模型所述，AWS 負責保護執行所有 AWS 雲端 的全球基礎設施。您必須負責維護在此基礎設施上託管之內容的控制權。此內容包括您所使用 AWS 服務的安全組態和管理任務。如需有關資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

基於資料保護目的，建議您使用 AWS 帳戶 (IAM) 保護 AWS Identity and Access Management 憑證，並設定個別使用者帳戶。如此一來，每個使用者都只會獲得授予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：

- 每個帳戶都使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。建議使用 TLS 1.2 或更新版本。
- 使用 AWS CloudTrail 設定 API 和使用者活動記錄。
- 使用 AWS 加密解決方案，以及 AWS 服務內的所有預設安全控制。
- 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 的個人資料。
- 如果您在透過命令列介面或 API 存取 AWS 時，需要 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的詳細資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

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欄位中，例如 Name (名稱) 欄位。這包括當您使用 Storage Gateway 或其他AWS服務使用控制台、API、AWS CLI, 或AWS軟體開發套件。您在標籤或自由格式欄位中輸入的任何資料都可能用於計費或診斷記錄。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

使用的資料加密AWS KMS

Storage Gateway 道使用 SSL/TLS (安全套接字層/傳輸層安全性) 來加密在您閘道裝置和AWS儲存體。在預設情況下，Storage Gateway 使用 Amazon S3 受管加密金鑰 (SSE-S3) 在伺服器端加密存放在 Amazon S3 中的所有資料。您可以選擇使用 Storage Gateway API 來設定閘道，將伺服器端加密功能與AWS Key Management Service(SSE-KMS) 客戶主金鑰 (CMK)。

> **Important**
>
> 當您使用AWS KMSCMK 用於服務器端加密時，您必須選擇對稱 CMK。Storage Gateway 不支援非對稱 CMK。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

對於文件共享，您可以將網關配置為使用AWS KMS— 通過使用 SSE-KMS 託管密鑰。如需使用 Storage Gateway API 來加密寫入檔案共享的資料，請參CreateNFSFileShare中的AWS Storage GatewayAPI 參考。

加密文件系統

如需相關資訊，請參亞馬遜 FSX 中的數據加密中的Amazon FSx for Windows File Server 使用者指南。

當使用 AWS KMS 加密您的資料時，請謹記下列事項：

- 您的資料是在雲端中的靜態狀態下加密。也就是說，這些資料會在 Amazon S3 中加密。
- IAM 使用者必須具備必要的許可，才能呼叫AWS KMSAPI 操作。如需詳細資訊，請參閱「」使用 IAM 政策AWS KMS中的AWS Key Management Service開發人員指南。
- 若您刪除或停用您的 CMK 或撤銷授予的字符，您將無法存取磁碟區或磁帶上的資料。如需詳細資訊，請參閱「」刪除客戶主金鑰中的AWS Key Management Service開發人員指南。
- 若您從 KMS 加密的磁碟區建立快照，快照也會處於加密狀態。快照會繼承磁碟區的 KMS 金鑰。
- 若您從 KMS 加密的快照建立新的磁碟區，那麼磁碟區也會處於加密狀態。您可以為新的磁碟區指定不同的 KMS 金鑰。

> **Note**
>
> Storage Gateway 道不支援從 KMS 加密磁碟區或 KMS 加密快照的復原點建立未加密的磁碟區。

如需 AWS KMS 的詳細資訊，請參閱什麼是 AWS Key Management Service？

存儲 Gateway 的身份驗證和存取控制

存取 AWS Storage Gateway 時需要提供登入資料，以供 AWS 驗證您的請求。這些登入資料必須有存取的許可AWS資源，例如閘道、檔案共享、卷或磁帶。下列各節提供了詳細資訊，說明您可如何使用AWS Identity and Access Management(IAM)和 Storage Gateway，透過控制可存取的人員，協助確保您資源的安全：

- 身分驗證
- 存取控制

身分驗證

您可以使用下列身分類型來存取 AWS：

- AWS 帳戶 根使用者：在您首次建立 AWS 帳戶 時，您會先有單一的登入身分，可以完整存取帳戶中所有 AWS 服務與資源。此身分稱為 AWS 帳戶 根使用者，使用建立帳戶時所使用的電子郵件地址和密碼即可登入並存取。強烈建議您不要以根使用者處理日常作業，即使是管理作業。反之，請遵循僅將根使用者用來建立您第一個 IAM 使用者的最佳實務。接著請妥善鎖定根使用者憑證，只用來執行少數的帳戶與服務管理作業。
- IAM 使用者— 一個IAM 使用者是您的AWS 帳戶) 擁有特定的自訂許可 (例如在儲存閘道中建立閘道的許可)。您可以使用 IAM 使用者名稱和密碼登入安全 AWS 網頁，例如，AWS Management Console、AWS 開發論壇或 AWS Support 中心。

  除了使用者名稱和密碼之外，您也可以為每個使用者產生存取金鑰。您可以使用這些金鑰，以程式設計的方式存取 AWS 服務，無論是透過其中一個 SDK 或使用 AWS Command Line Interface (CLI)。此 SDK 和 CLI 工具使用存取金鑰，以加密方式簽署您的請求。如果您不使用 AWS 工具，您必須自行簽署請求。Storage Gateway 支援Signature 第 4 版，這是用來驗證傳入 API 請求的協定。如需驗證請求的詳細資訊，請參閱《AWS 一般參考》中的簽章版本 4 簽署程序。

- IAM 角色：IAM 角色是您可以在帳戶中建立的另一種 IAM 身分，具有特定的許可。IAM 角色類似於 IAM 使用者，因為同樣是 AWS 身分，也有許可政策可決定該身分在 AWS 中可執行和不可執行的操作。但是，角色的目的是讓需要它的任何人可代入，而不是單獨地與某個人員關聯。此外，角色沒有與之關聯的標準長期憑證，例如密碼或存取金鑰。反之，當您擔任角色時，其會為您的角色工作階段提供臨時安全性登入資料。使用臨時登入資料的 IAM 角色在下列情況中非常有用：

  - 聯合身分使用者存取：並非建立 IAM 使用者，而是使用來自 AWS Directory Service、您的企業使用者目錄或 Web 身分供應商現有的使用者身分。這些稱為聯合身分使用者。透過身分供應商來請求存取時，AWS 會指派角色給聯合身分使用者。如需聯合身份使用者的詳細資訊，請參閱IAM 使用者指南中的聯合身份使用者和角色。

  - AWS 服務存取 – 服務角色是服務擔任的 IAM 角色，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。

- 在 Amazon EC2 上執行的應用程式：針對在 EC2 執行個體上執行並提出 AWS CLI 和 AWS API 請求的應用程式，您可以使用 IAM 角色來管理臨時登入資料。這是在 EC2 執行個體內存放存取金鑰的較好方式。若要指派 AWS 角色給 EC2 執行個體並提供其所有應用程式使用，您可以建立連接到執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得臨時憑證。如需詳細資訊，請參閱IAM 使用者指南中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

存取控制

您可以持有效登入資料為自己的要求進行身份驗證，但還須具備許可才能建立或存取 Storage Gateway 資源。例如，您必須具有許可，才能在 Storage Gateway 中建立閘道。

以下章節說明如何管理 Storage Gateway 的許可。我們建議您先閱讀概觀。

- 管理 Storage Gateway 取許可概觀
- 身分類型政策 (IAM 政策)

管理 Storage Gateway 取許可概觀

每個AWS資源由 Amazon Web Services vice 帳户所持有，而建立或存取資源的許可則由許可政策管理。帳戶管理員可以將許可政策連接到 IAM 身分 (即使用者、群組與角色) 以及某些服務 (例如 AWS Lambda) 也支援將許可政策連接到資源。

> **Note**
>
> 帳戶管理員 (或管理員使用者) 是具有管理員權限的使用者。如需詳細資訊，請參《IAM 使用者指南》中的 IAM 最佳實務。

當您授予許可時，能夠決定取得許可的對象、這些對象取得許可的資源，以及可對上述資源進行的特定動作。

主題

- Storage Gateway 資源和操作
- 了解資源所有權
- 管理資源存取
- 指定政策元素：動作、效果、資源及委託人
- 在政策中指定條件

Storage Gateway 資源和操作

在 Storage Gateway 中，主要資源是閘道。Storage Gateway 還支援下列其他資源類型：檔案共享、磁碟區、虛擬磁帶、iSCSI 目標和虛擬磁帶庫 (VTL) 裝置。它們稱為子資源，必須與閘道相關聯才能存在。

這些資源和子資源都有獨一無二的 Amazon Resource Name (ARN) 與其相關聯，如下表所示。

資源類型	ARN 格式
閘道 ARN	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`*
檔案共享 ARN	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:share/`*`share-id`*

> **Note**
>
> Storage Gateway 資源 ID 為大寫。當您使用這些資源 ID 配合 Amazon EC2 API 時，Amazon EC2 希望資源 ID 為小寫。您必須將資源 ID 變更為小寫，才能將它與 EC2 API 搭配使用。例如，在 Storage Gateway 中，磁碟區的 ID 可能是 `vol-1122AABB`。但當您使用此 ID 配合 EC2 API 時，您必須將它變更為 `vol-1122aabb`。否則，EC2 API 可能無法如預期運作。2015 年 9 月 2 日之前已啟用的閘道 ARN，包含的是閘道名稱而不是閘道 ID。請使用 `DescribeGatewayInformation` API 操作，以取得您閘道的 ARN。

若要授予特定 API 操作的許可 (如建立磁帶)，Storage Gateway 會為您提供一組 API 動作，以建立和管理這些資源和子資源。如需 API 動作清單，請參動作中的AWS Storage GatewayAPI 參考。

若要授予特定 API 操作的許可 (如建立磁帶)，Storage Gateway 會定義一組您可在許可政策中指定的動作，授予特定 API 操作的許可。API 操作會需要多個動作的許可。如需詳列所有 Storage Gateway API 動作及其所套用之資源的資料表，請參Storage Gateway API 權限：動作、資源和條件參考。

了解資源所有權

一個資源擁有者是創建資源的 Amazon Web Services 帳户。也就是説，資源擁有者就是委託人實體(根帳户、IAM 使用者或 IAM 角色)，來驗證建立資源的請求。下列範例說明其如何運作：

- 如果您使用 Amazon Web Services vice 帳户的根帳户登入資料來啟用閘道，您的 Amazon Web Services vice 帳户即為資源擁有者 (在 Storage Gateway 中，資源為閘道)。
- 如果您在 Amazon Web Services 帳户中建立 IAM 使用者並授予`ActivateGateway`動作，該使用者就可以啟用閘道。不過，您的 Amazon Web Services vice 帳户(也是該使用者所屬的帳户) 擁有該閘道資源。
- 如果您在 Amazon Web Services vice 帳户中建立具有啟用閘道許可的 IAM 角色，則任何可以擔任該角色的人都能啟用閘道。您的 Amazon Web Services 帳户 (也是該角色所屬的帳户) 擁有閘道資源。

管理資源存取

許可政策描述誰可以存取哪些資源。下一節說明可用來建立許可政策的選項。

> **Note**
>
> 本節討論如何在 Storage Gateway 環境中使用 IAM。它不提供 IAM 服務的詳細資訊。如需完整的 IAM 文件，請參什麼是 IAM中的IAM 使用者指南。如需有關 IAM 政策語法和說明的資訊，請參閱IAM 使用者指南中的 AWS IAM 政策參考。

連接到 IAM 身分的政策稱為身分類型政策 (IAM 政策)，而連接到資源的政策稱為資源類型政策。Storage Gateway 僅支援以身分為基礎的政策 (IAM 政策)。

主題

- 身分類型政策 (IAM 政策)
- 資源型政策

身分類型政策 (IAM 政策)

您可以將政策連接到 IAM 身分。例如，您可以執行下列操作：

- 將許可政策連接至您帳户中的使用者或組— 帳户管理員可使用與特定使用者相關聯的許可政策，來授予該使用者建立 Storage Gateway 資源 (例如閘道、磁碟區或磁帶) 的許可。
- 將許可政策連接至角色 (授予跨帳戶許可)：您可以將身分類型許可政策連接至 IAM 角色，藉此授予跨帳戶許可。例如，帳户A 中的管理員可以建立角色，將跨帳户許可授予另一個 Amazon Web Services vice 帳户(例如帳户B) 或AWS服務，如下所示：
  1. 帳戶 A 管理員建立 IAM 角色，並將許可政策連接到可授與帳戶 A 中資源許可的角色。
  2. 帳戶 A 管理員將信任政策連接至該角色，識別帳戶 B 做為可擔任該角的委託人。
  3. 帳戶 B 管理員即可將擔任該角色的許可委派給帳戶 B 中的任何使用者。這麼做可讓帳戶 B 的使用者建立或存取帳戶 A 的資源。如果您想要授予 AWS 服務擔任該角色的許可，則信任政策中的委託人也可以是 AWS 服務委託人。

  如需使用 IAM 來委派許可的詳細資訊，請參閱《IAM 使用者指南》中的存取管理。

下列為一個範例政策，該政策授予對所有資源進行所有 `List*` 動作的許可。此動作是唯讀動作。因此，政策不允許使用者變更資源的狀態。

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "AllowAllListActionsOnAllResources",
            "Effect": "Allow",
            "Action": [
                "storagegateway:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

如需搭配 Storage Gateway 使用以身分為基礎的政策的詳細資訊，請參將以身分為基礎的政策 (IAM 政策) 用於 Storage Gateway。如需使用者、群組、角色和許可的詳細資訊，請參閱 IAM 使用者指南中的身分 (使用者、群組和角色)。

資源型政策

其他服務 (例如 Amazon S3) 也支援以資源為基礎的許可政策。例如，您可以將政策連接至 S3 儲存貯體，以管理該儲存貯體的存取許可。Storage Gateway 不支援資源類型政策。

指定政策元素：動作、效果、資源及委託人

對於每個 Storage Gateway 資源（請參閱Storage Gateway API 權限：動作、資源和條件參考），該服務定義了一組 API 操作 (請參動作。若要授予對這些 API 操作的許可，Storage Gateway 會定義一組您可以在政策中指定的動作。例如，針對 Storage Gateway 資源定義的動作如下：`ActivateGateway`、`DeleteGateway`，以及`DescribeGatewayInformation`。請注意，執行 API 操作可能需要多個動作的許可。

以下是最基本的政策元素：

- 資源 – 在政策中，您可以使用 Amazon Resource Name (ARN) 來識別要套用政策的資源。對於 Storage Gateway 資源，則一律使用萬用字元(*)。如需詳細資訊，請參閱 Storage Gateway 資源和操作。
- 動作：您使用動作關鍵字識別您要允許或拒絕的資源操作。例如，根據指定的`Effect`，`storagegateway:ActivateGateway`許可允許或拒絕執行 Storage Gateway 的使用者許可`ActivateGatewayoperation.`
- 效果 - 您可以指定使用者要求特定動作時會有什麼效果；可為允許或拒絕。如果您未明確授予存取 (允許) 資源，則隱含地拒絕存取。您也可以明確拒絕資源存取，這樣做可確保使用者無法存取資源，即使不同政策授予存取也是一樣。

- 委託人：在以身分為基礎的政策 (IAM 政策) 中，政策所連接的使用者就是隱含委託人。對於資源類型政策，您可以指定想要收到許可的使用者、帳戶、服務或其他實體 (僅適用於資源類型政策)。Storage Gateway 不支援資源類型政策。

如需進一步了解有關 IAM 政策語法和說明的詳細資訊，請參閱《IAM 使用者指南》 中的 AWS IAM 政策參考。

如需詳列所有 Storage Gateway API 動作的資料表，請參Storage Gateway API 權限：動作、資源和條件參考。

在政策中指定條件

當您授予許可時，您可使用 IAM 政策語言來指定授予許可時，政策應該何時生效的條件。例如，建議只在特定日期之後套用政策。如需使用政策語言指定條件的詳細資訊，請參閱IAM 使用者指南中的條件。

欲表示條件，您可以使用預先定義的條件金鑰。沒有 Storage Gateway 特定的條件金鑰。不過，您可以使用適合的完整 AWS 條件金鑰。如需全 AWS 金鑰的完整清單，請參閱《IAM 使用者指南》中的「可用的金鑰」。

將以身分為基礎的政策 (IAM 政策) 用於 Storage Gateway

這個主題提供以身分為基礎的政策範例，在該政策中帳戶管理員可以將許可政策連接至 IAM 身分 (即使用者、群組和角色)。

> **Important**
>
> 建議您先檢可供您管理儲存 Gateway 資源存取之基本概念與選項的介紹主題。如需詳細資訊，請參閱 管理 Storage Gateway 取許可概觀。

本主題中的各節涵蓋下列內容：

- 使用 Storage Gateway 主控台所需的許可
- AWSStorage Gateway 的託管策略
- 客戶受管政策範例

以下顯示許可政策範例。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsSpecifiedActionsOnAllGateways",
            "Effect": "Allow",
            "Action": [
                "storagegateway:ActivateGateway",
                "storagegateway:ListGateways"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowsSpecifiedEC2ActionsOnAllGateways",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSnapshots",
                "ec2:DeleteSnapshot"
            ],
            "Resource": "*"
        }
    ]
}
```

政策有兩個陳述式 (請注意兩個陳述式都有 Action 和 Resource 元素)：

- 第一個陳述式會授予兩個 Storage Gateway 動作的許可 (storagegateway:ActivateGateway和storagegateway:ListGateways) 在網關資源上。

  萬用字元 (*) 表示此陳述式可以符合任何資源。在這種情況下，該語句允許storagegateway:ActivateGateway和storagegateway:ListGateways在任何網關上執行操作。此處使用萬用字元，因為您在建立閘道後才會知道資源 ID。如需如何在政策中使用萬用字元 (*) 的資訊，請參閱範例 2：允許對 Gateway 的唯讀存取。

  > **Note**
  >
  > ARN 唯一識別AWS的費用。如需 ARN 的詳細資訊，請參閱 AWS 一般參考中的 Amazon 資源名稱 (ARN) 與 AWS 服務命名空間。

若只要限制特定閘道的特定動作許可，請在政策中為該動作建立單獨的陳述式，並在該陳述式中指定閘道 ID。

- 第二個陳述式授予 `ec2:DescribeSnapshots` 和 `ec2:DeleteSnapshot` 動作的許可。這些 Amazon Elastic Compute Cloud (Amazon EC2) 動作需要許可，因為存放 Storage Gateway 道產生的快照存放在 Amazon 彈性區塊儲存 (Amazon EBS) 且受管為 Amazon EC2 資源，因此它們需要對應的 EC2 動作。如需詳細資訊，請參閱「」動作中的Amazon EC2 API 參考。因為這些 Amazon EC2 動作不支援資源層級許可，所以政策會指定萬用字元 (*) 為`Resource`值，而不是指定網關 ARN。

如需詳列所有 Storage Gateway API 動作及其所套用之資源的表格，請參Storage Gateway API 權限：動作、資源和條件參考。

使用 Storage Gateway 主控台所需的許可

若要使用 Storage Gateway 主控台，您需要授予唯讀許可。如果您打算說明快照，您還需要如下列許可政策所示，授予額外動作的許可：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsSpecifiedEC2ActionOnAllGateways",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        }
    ]
}
```

此為必要的額外許可，因為從 Storage Gateway 產生的 Amazon EBS 快照受管為 Amazon EC2 資源。

若要設定瀏覽 Storage Gateway 主控台所需的最低許可，請參範例 2：允許對 Gateway 的唯讀存取。

AWSStorage Gateway 的託管策略

Amazon Web Services vice 透過提供獨立的 IAM 政策來解決許多常用案例，這些政策由AWS。受管政策授與常見使用案例中必要的許可，讓您免於查詢需要哪些許可。如需有關 的詳細資訊AWS託管政策，請參AWS受管政策中的IAM User Guide。

如下所示AWS受管政策專屬於 Storage Gateway，可連接到您帳户中的使用者：

- AWSStorageGatewayReadOnlyAccess – 授予 AWS Storage Gateway 資源的唯讀存取權。
- AWSStorageGatewayFullAccess – 授予 AWS Storage Gateway 資源的完整存取權。

> **Note**
>
> 您可以登入 IAM 主控台並在該處搜尋特定政策，來檢閱這些許可政策。

您也可以建立自己的自訂 IAM 政策，以允許 AWS Storage Gateway API 動作的許可。您可以將這些自訂政策連接至需要這些許可的 IAM 使用者或群組。

客戶受管政策範例

在本節中，您可以找到授予各種 Storage Gateway 動作許可的使用者政策範例。這些政策會在您使用AWS軟體開發套件和AWS CLI。當您使用主控台時，需要授予主控台特定的額外許可，這會在「使用 Storage Gateway 主控台所需的許可」中予以討論。

> **Note**
>
> 所有範例皆使用美國西部 (奧勒岡) 區域 (`us-west-2`) 及虛構帳戶 ID。

主題

- 範例 1：允許在所有網關上執行任何 Storage Gateway 操作
- 範例 2：允許對 Gateway 的唯讀存取
- 範例 3：允許存取特定 Gateway
- 範例 4：允許用户訪問特定卷

- 範例 5：允許在具有特定前綴的網關上執行所有操作

範例 1：允許在所有網關上執行任何 Storage Gateway 操作

以下政策允許使用者執行所有 Storage Gateway 動作。此政策也允許使用者執行 Amazon EC2 動作 (DescribeSnapshots和DeleteSnapshot) 在 Storage Gateway 生成的 Amazon EBS 快照上。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllAWSStorageGatewayActions",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {You can use Windows ACLs only with file shares that are enabled for Active
 Directory.
            "Sid": "AllowsSpecifiedEC2Actions",
            "Action": [
                "ec2:DescribeSnapshots",
                "ec2:DeleteSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

範例 2：允許對 Gateway 的唯讀存取

下列政策允許對所有資源執行所有 `List*` 和 `Describe*` 動作。請注意，這些動作是唯讀動作。因此，此政策不允許使用者變更任何資源的狀態，也就是說，此政策不允許使用者執行 `DeleteGateway`、`ActivateGateway` 和 `ShutdownGateway` 等動作。

此政策也允許 `DescribeSnapshots` Amazon EC2 動作。如需詳細資訊，請參閱「」DescribeSnapshots中的Amazon EC2 API 參考。

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "AllowReadOnlyAccessToAllGateways",
            "Action": [
                "storagegateway:List*",
                "storagegateway:Describe*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "AllowsUserToDescribeSnapshotsOnAllGateways",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

前述政策中不是使用萬用字元 (*)，您可以將範圍限制在特定閘道政策所涵蓋的資源，如下列範例所示。然後，政策只允許對特定的閘道執行動作。

```
"Resource": [
             "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
             "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
            ]
```

在閘道內，您可以進一步將資源範圍限制在僅限閘道磁碟區，如下列範例所示：

```
"Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/volume/
*"
```

範例 3：允許存取特定 Gateway

下列政策允許對特定閘道執行所有動作。使用者受限制，不能存取您可能已部署的其他閘道。

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "AllowReadOnlyAccessToAllGateways",
            "Action": [
                "storagegateway:List*",
                "storagegateway:Describe*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "AllowsUserToDescribeSnapshotsOnAllGateways",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "AllowsAllActionsOnSpecificGateway",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
            ]
        }
    ]
}
```

如果政策連接的使用者使用 API 或AWSSDK 訪問網關。不過，如果使用者要使用 Storage Gateway 主控台，您即必須也授予允許`ListGateways`動作，如下列範例所示。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllActionsOnSpecificGateway",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
```

```
            "Resource": [
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
            ]
        },
        {
            "Sid": "AllowsUserToUseAWSConsole",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

範例 4：允許用户訪問特定卷

下列政策允許使用者對閘道的特定磁碟區執行所有動作。因為使用者預設未取得任何許可，所以政策會限制使用者只能存取特定的磁碟區。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantsPermissionsToSpecificVolume",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-
id/volume/volume-id"
        },
        {
            "Sid": "GrantsPermissionsToUseStorageGatewayConsole",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

如果政策連接的使用者使用 API 或AWS軟件開發工具包來訪問卷。但是，如果此用户要使用AWS Storage Gateway主控台，您必須授予許可，以允許ListGateways動作，如下列範例所示。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantsPermissionsToSpecificVolume",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/volume/volume-id"
        },
        {
            "Sid": "GrantsPermissionsToUseStorageGatewayConsole",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

範例 5：允許在具有特定前綴的網關上執行所有操作

下列政策允許使用者在名稱開頭為的閘道上執行所有 Storage Gateway 動作。DeptX。此政策還允許DescribeSnapshotsAmazon EC2 動作，如果您計畫描述快照，此為必要動作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsActionsGatewayWithPrefixDeptX",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/DeptX"
        },
```

```
        {
            "Sid": "GrantsPermissionsToSpecifiedAction",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

如果政策連接的使用者使用 API 或AWSSDK 訪問網關。但是，如果此用户計劃使用AWS Storage Gateway主控台，您必須授予其他許可，如範例 3：允許存取特定 Gateway。

使用標籤來控制對您的 Gateway 和資源的存取

若要控制對閘道資源和動作的存取，您可以根據標籤使用 AWS Identity and Access Management (IAM) 政策。您可以透過兩個方式提供控制：

1. 根據這些資源的標籤控制對閘道資源的存取。
2. 控制您可以在 IAM 請求條件中傳遞哪些標籤。

如需如何使用標籤來控制存取的詳細資訊，請參閱使用標籤控制存取。

根據資源上的標籤控制存取權限

若要控制使用者或角色可以在閘道資源上執行的動作，您可以使用閘道資源的標籤。例如，您可能想要根據資源上標籤的金鑰值組，允許或拒絕檔案閘道資源上的特定 API 操作。

以下範例會允許使用者或角色在所有資源上執行 `ListTagsForResource`、`ListFileShares` 和 `DescribeNFSFileShares` 動作。只有在資源上的標籤已將金鑰設定為 `allowListAndDescribe` 和將值設定為 `yes` 時，才會套用此政策。

```
{
  "Version": "2012-10-17",
   "Statement": [
      {
          "Effect": "Allow",
                    "Action": [
                        "storagegateway:ListTagsForResource",
```

```
                        "storagegateway:ListFileShares",
                        "storagegateway:DescribeNFSFileShares"
                    ],
                    "Resource": "*",
                    "Condition": {
                        "StringEquals": {
                            "aws:ResourceTag/allowListAndDescribe": "yes"
                        }
                    }
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:*"
            ],
            "Resource": "arn:aws:storagegateway:region:account-id:*/*"
        }
    ]
}
```

根據 IAM 請求中的標籤控制存取權限

若要控制 IAM 使用者可以在閘道資源上執行的動作，您可以根據標籤使用 IAM 政策中的條件。例如，您可以編寫一個政策，根據使用者建立資源時所提供的標籤，來允許或拒絕 IAM 使用者執行特定 API 操作的能力。

在下列範例中，第一個陳述式只會在使用者建立閘道時提供的標籤金鑰值組為 **Department** 和 **Finance** 時，允許使用者建立閘道。使用 API 操作時，您會將此標籤新增到啟用請求。

第二個陳述式只會在閘道上的標籤金鑰值組符合時，允許使用者在閘道上建立網路檔案系統 (NFS) 或伺服器訊息區塊 (SMB) 檔案共用**Department**和**Finance**。此外，使用者必須將標籤新增到共用檔案，而且標籤的金鑰值組必須為 **Department** 和 **Finance**。您會在建立檔案共用時將標籤新增到檔案共用。沒有 AddTagsToResource 或 RemoveTagsFromResource 操作的權限，因此使用者無法在閘道或檔案共用上執行這些操作。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "storagegateway:ActivateGateway"
```

```
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/Department":"Finance"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":[
            "storagegateway:CreateNFSFileShare",
            "storagegateway:CreateSMBFileShare"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/Department":"Finance",
               "aws:RequestTag/Department":"Finance"
            }
         }
      }
   ]
}
```

使用 Microsoft Windows ACL 來控制 SMB 檔案共享的存取

Amazon S3 檔案 Gateway 支援兩種不同的方法，來控制透過 SMB 檔案共享存放之檔案和目錄的存取權：POSIX 權限或視窗 ACL。

在本節中，您可以找到如何在已啟用 Microsoft Active Directory (AD) 的 SMB 檔案共享上，使用 Microsoft Windows 存取控制清單 (ACL) 的相關資訊。使用 Windows ACL，您可以在 SMB 檔案共享的檔案和資料夾上設定精確的許可。

以下是 SMB 檔案共享上 Windows ACL 的一些重要的特性：

- 當文件網關加入到活動目錄域時，默認情況下為 SMB 文件共享選擇 Windows ACL。
- ACL 啟用時，ACL 資訊會保留在 Amazon S3 物件中繼資料。
- 針對每個檔案或資料夾，閘道最多保留 10 個 ACL。
- 使用已啟用 ACL 的 SMB 檔案共享來存取在閘道外部建立的 S3 物件時，物件會繼承父資料夾的 ACL 資訊。

- SMB 檔案共享的預設根 ACL 提供完整存取權限給每個人，但您可以變更根 ACL 的許可。您可以使用根 ACL 來控制檔案共享的存取。您可以設定誰可以掛載檔案共享 (映射磁碟機)，以及使用者在檔案共享中以遞迴方式可對檔案和資料夾取得那些許可。不過，我們建議您在 S3 儲存貯體的最上層資料夾設定此許可，如此可以保存您的 ACL。

當您使用 CreateSMBFileShare API 操作建立新的 SMB 檔案共享時，可以啟用 Windows ACL。或者，您也可以使用 UpdateSMBFileShare API 操作，在現有的 SMB 檔案共享上啟用 Windows ACL。

在新 SMB 檔案共享上啟用 Windows ACL

請依照下列步驟，在新的 SMB 檔案共享上啟用 Windows ACL。

若要建立新 SMB 檔案共享時啟用 Windows ACL

1. 如果您還沒有檔案閘道，請建立一個。如需詳細資訊，請參閱 。
2. 如果閘道尚未加入網域，請將其新增到網域。如需詳細資訊，請參閱 。
3. 建立 SMB 檔案共享。
4. 從 Storage Gateway 主控台在檔案共享上啟用 Windows ACL。

   若要使用 Storage Gateway 主控台，請執行下列動作：

   a. 選擇檔案共享，然後選擇 Edit file share (編輯檔案共享)。

   b. 對於 File/directory access controlled by (檔案/目錄存取控制者) 選項，選擇 Windows Access Control List (Windows 存取控制清單)。
5. (選用) 如果您希望管理員使用者具有更新檔案共享中所有檔案和資料夾之 ACL 的權限，請新增管理員使用者到 AdminUsersList。
6. 更新根資料夾下方父資料夾的 ACL。若要這樣做，請使用 Windows 檔案總管在 SMB 檔案共享的資料夾上設定 ACL。

   > **Note**
   >
   > 如果您在根資料夾上設定 ACL，而非在根下方的父資料夾上設定，ACL 許可不會保留在 Amazon S3 中。

   我們建議在檔案共享根目錄的最上層資料夾設定 ACL，而不是在檔案共享的根目錄直接設定 ACL。這種方法會將資訊保存為 Amazon S3 中的物件中繼資料。

7. 視需要啟用繼承。

> **Note**
>
> 您可以為 2019 年 5 月 8 日之後建立的檔案共享啟用繼承。

如果您啟用繼承並以遞迴方式遞迴更新許可，Storage Gateway 會更新 S3 儲存貯體中的所有物件。根據儲存貯體中的物件數量，更新可能作需要一些時間才能完成。

在現有 SMB 檔案共享上啟用 Windows ACL

請依照下列步驟，在具有 POSIX 許可的現有 SMB 檔案共享上啟用 Windows ACL。

若要使用 Storage Gateway 道主控台在現有 SMB 檔案共享上啟用 Windows ACL

1. 選擇檔案共享，然後選擇 Edit file share (編輯檔案共享)。
2. 對於 File/directory access controlled by (檔案/目錄存取控制者) 選項，選擇 Windows Access Control List (Windows 存取控制清單)。
3. 視需要啟用繼承。

> **Note**
>
> 我們不建議您在根層級設定 ACL，因為如果您這麼做並刪除了閘道，您需要再次重設 ACL。

如果您啟用繼承並以遞迴方式遞迴更新許可，Storage Gateway 會更新 S3 儲存貯體中的所有物件。根據儲存貯體中的物件數量，更新可能作需要一些時間才能完成。

使用 Windows ACL 時的限制

使用 Windows ACL 來控制 SMB 檔案共享的存取時，請謹記下列限制：

- 當您使用 Windows SMB 用戶端來存取檔案共享時，Windows ACL 僅支援啟用 Active Directory 的檔案共享。
- 針對每個檔案和目錄，檔案閘道最多支援 10 個 ACL 項目。
- 檔案 Gateway 不支援`Audit`和`Alarm`項目，這是系統存取控制清單 (SACL) 項目。檔案閘道支援 `Allow` 和 `Deny` 項目，這是判別式存取控制清單 (DACL) 項目。

- SMB 檔案共享的根 ACL 設定只位於閘道上，並且此設定會在閘道更新和重新啟動之間持續存在。

> **Note**
>
> 如果您在根資料夾上設定 ACL，而非在根下方的父資料夾上設定，ACL 許可不會保留在 Amazon S3 中。

在這些條件下，請務必執行下列動作：

- 如果您設定多個閘道存取相同的 Amazon S3 儲存貯體，請在每個閘道上設定根 ACL 以保持許可一致性。
- 如果您刪除檔案共享並在相同的 Amazon S3 儲存貯體上重新建立，請確保您使用相同的根 ACL 設定。

Storage Gateway API 權限：動作、資源和條件參考

當您設定存取控制及撰寫可連接到 IAM 身分的許可政策 (以身分為基礎的政策) 時，可參考下表。下表列出每個 Storage Gateway API 操作、您可以針對這些項目授予執行動作的許可的相應動作，以及AWS資源，您可以授予這些資源的許可。您在政策的 `Action` 欄位中指定動作，然後在政策的 `Resource` 欄位中指定資源值。

您可以使用AWS來表示條件金鑰。如需全 AWS 金鑰的完整清單，請參閱《IAM 使用者指南》中的「可用的金鑰」。

> **Note**
>
> 若要指定動作，請使用後接 API 操作名稱的 `storagegateway:` 字首 (例如，`storagegateway:ActivateGateway`)。您可以為每個 Storage Gateway 動作指定萬用字元 (*) 做為資源。

如需 ARN 格式的 Storage Gateway 資源清單，請參Storage Gateway 資源和操作。

存 Storage Gateway API 與動作所需的許可如下所示。

ActivateGateway

動作：`storagegateway:ActivateGateway`

資源：*

AddCache

動作：storagegateway:AddCache

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

AddTagsToResource

動作：storagegateway:AddTagsToResource

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

或

arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

或

arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

AddUploadBuffer

動作：storagegateway:AddUploadBuffer

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

AddWorkingStorage

動作：storagegateway:AddWorkingStorage

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

CancelArchival

動作：storagegateway:CancelArchival

資源：arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

CancelRetrieval

動作：storagegateway:CancelRetrieval

資源：arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

CreateCachediSCSIVolume

動作：storagegateway:CreateCachediSCSIVolume

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

CreateSnapshot

動作：storagegateway:CreateSnapshot

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

CreateSnapshotFromVolumeRecoveryPoint

動作：storagegateway:CreateSnapshotFromVolumeRecoveryPoint

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

CreateStorediSCSIVolume

動作：storagegateway:CreateStorediSCSIVolume

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

CreateTapes

動作：storagegateway:CreateTapes

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteBandwidthRateLimit

動作：storagegateway:DeleteBandwidthRateLimit

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteChapCredentials

動作：storagegateway:DeleteChapCredentials

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/target/*iSCSItarget*

DeleteGateway

動作：storagegateway:DeleteGateway

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteSnapshotSchedule

動作：storagegateway:DeleteSnapshotSchedule

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DeleteTape

動作：storagegateway:DeleteTape

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteTapeArchive

動作：storagegateway:DeleteTapeArchive

資源：*

DeleteVolume

動作：storagegateway:DeleteVolume

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DescribeBandwidthRateLimit

動作：storagegateway:DescribeBandwidthRateLimit

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeCache

動作：storagegateway:DescribeCache

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeCachediSCSIVolumes

動作：storagegateway:DescribeCachediSCSIVolumes

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DescribeChapCredentials

動作：storagegateway:DescribeChapCredentials

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/target/*iSCSItarget*

DescribeGatewayInformation

動作：storagegateway:DescribeGatewayInformation

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeMaintenanceStartTime

動作：storagegateway:DescribeMaintenanceStartTime

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeSnapshotSchedule

動作：storagegateway:DescribeSnapshotSchedule

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DescribeStorediSCSIVolumes

動作：storagegateway:DescribeStorediSCSIVolumes

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DescribeTapeArchives

動作：storagegateway:DescribeTapeArchives

資源：*

DescribeTapeRecoveryPoints

動作：storagegateway:DescribeTapeRecoveryPoints

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeTapes

動作：storagegateway:DescribeTapes

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeUploadBuffer

動作：storagegateway:DescribeUploadBuffer

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeVTLDevices

動作：storagegateway:DescribeVTLDevices

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeWorkingStorage

動作：storagegateway:DescribeWorkingStorage

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DisableGateway

動作：storagegateway:DisableGateway

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ListGateways

動作：storagegateway:ListGateways

資源：*

ListLocalDisks

動作：storagegateway:ListLocalDisks

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ListTagsForResource

動作：storagegateway:ListTagsForResource

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

或

arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

或

arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

ListTapes

動作：storagegateway:ListTapes

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ListVolumeInitiators

動作：storagegateway:ListVolumeInitiators

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

ListVolumeRecoveryPoints

動作：storagegateway:ListVolumeRecoveryPoints

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ListVolumes

動作：storagegateway:ListVolumes

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

RemoveTagsFromResource

動作：storagegateway:RemoveTagsFromResource

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

或

arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

或

arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

ResetCache

動作：storagegateway:ResetCache

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

RetrieveTapeArchive

動作：storagegateway:RetrieveTapeArchive

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

RetrieveTapeRecoveryPoint

動作：storagegateway:RetrieveTapeRecoveryPoint

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ShutdownGateway

動作：storagegateway:ShutdownGateway

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

StartGateway

動作：storagegateway:StartGateway

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

UpdateBandwidthRateLimit

動作：storagegateway:UpdateBandwidthRateLimit

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

UpdateChapCredentials

動作：storagegateway:UpdateChapCredentials

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/target/*iSCSItarget*

UpdateGatewayInformation

動作：storagegateway:UpdateGatewayInformation

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

UpdateGatewaySoftwareNow

動作：storagegateway:UpdateGatewaySoftwareNow

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

UpdateMaintenanceStartTime

動作：storagegateway:UpdateMaintenanceStartTime

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

UpdateSnapshotSchedule

動作：storagegateway:UpdateSnapshotSchedule

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

UpdateVTLDeviceType

動作：storagegateway:UpdateVTLDeviceType

資源：arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/device/*vtldevice*

相關主題

- 存取控制
- 客戶受管政策範例

使用 Storage Gateway 的服務連結角色

Storage Gateway 使用AWS Identity and Access Management(IAM)服務連結角色。服務連結角色是直接連結至 Storage Gateway 的一種特殊 IAM 角色類型。服務連結角色由 Storage Gateway 預先定義，內含該服務呼叫其他AWS服務代您。

服務連結角色可讓設定 Storage Gateway 更為簡單，因為您不必手動新增必要的許可。Storage Gateway 會定義其服務連結角色的許可，除非另外定義，否則只有 Storage Gateway 可擔任該角色。定義的許可包含信任政策和許可政策，並且該許可政策不能附加到任何其他 IAM 實體。

如需有關支援服務連結角色的其他服務的資訊，請參閱可搭配 IAM 運作的 AWS 服務，並尋找 Service-Linked Role (服務連結角色) 資料欄顯示為 Yes (是) 的服務。選擇具有連結的 Yes (是)，以檢視該服務的服務連結角色文件。

Storage Gateway 的服務連結角色許可

Storage Gateway 使用名為的服務連結角色AWS 服務存儲網關— AWS 服務存儲網關。

AWSServiceRoleForStorage Gateway 服務連結角色信任下列服務擔任該角色：

- `storagegateway.amazonaws.com`

此角色許可政策允許 Storage Gateway 在指定資源上完成下列動作：

- 動作：`fsx:ListTagsForResourceonarn:aws:fsx:*:*:backup/*`

您必須設定許可，IAM 實體 (例如使用者、羣組或角色) 才可建立和編輯服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的服務連結角色許可。

建立 Storage Gateway 的服務連結角色

您不需要手動建立一個服務連結角色。創建 Storage Gateway 時`AssociateFileSystem`API 呼叫 AWS Management Console，AWS CLI，或AWSAPI 時，Storage Gateway 會為您建立服務連結角色。

> **Important**
>
> 此服務連結角色可以顯示在您的帳戶，如果您於其他服務中完成一項動作時，可以使用支援此角色的功能。另外，若您在 2021 年 3 月 31 日之前使用 Storage Gateway 道服務，當開始支援服務連結角色時，存放閘道會於您帳戶中建立 AWSServiceRoleForElasgeway 角色。若要進一步了解，請參閱我的 IAM 帳戶中出現的新角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。創建 Storage Gateway 時`AssociateFileSystem`API 呼叫時，Storage Gateway 會為您再次建立服務連結角色。

您也可以使用 IAM 主控台建立服務連結角色，並使用AWS 服務存儲網關使用案例。在 AWS CLI CLI 或 AWS API 中，建立一個服務名稱為 `storagegateway.amazonaws.com` 的服務連結角色。如需

詳細資訊，請參閱 IAM 使用者指南中的建立服務連結角色。如果您刪除此服務連結角色，您可以使用此相同的程序以再次建立該角色。

編輯 Storage Gateway 的服務連結角色

存放閘道不允許您編輯 AWSServiceRoleForStorage Gateway 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的編輯服務連結角色。

刪除 Storage Gateway 的服務連結角色

Storage Gateway 道不會自動刪除 AWSServiceRoleForAWSServiceRole 角色。要刪除 AWS 服務存儲網關角色，您需要調用`iam:DeleteSLR`API。如果沒有依賴於服務鏈接角色的存儲網關資源，則刪除將成功，否則刪除將失敗。如果要刪除服務鏈接角色，則需要使用 IAM API`iam:DeleteRole`或者`iam:DeleteServiceLinkedRole`。在這種情況下，您需要使用 Storage Gateway API 首先刪除帳户中的任何網關或文件系統關聯，然後通過使用`iam:DeleteRole`或者`iam:DeleteServiceLinkedRole`API。當您使用 IAM 刪除服務鏈接角色時，您需要使用 Storage Gateway`DisassociateFileSystemAssociation`API 首先刪除帳户中的所有文件系統關聯。否則刪除操作會失敗。

> **Note**
>
> 如果 Storage Gateway 服務在您試圖刪除資源時正在使用該角色，刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

刪除 AWSServiceRoleForAWSServiceRoleForMateway 所使用的存儲閘道資源

1. 使用我們的服務控制台、CLI 或 API 進行調用，清理資源並刪除角色，或使用 IAM 控制台、CLI 或 API 執行刪除操作。在這種情況下，您需要使用 Storage Gateway API 來首先刪除帳户中的任何網關和文件系統關聯。
2. 如果您使用 IAM 主控台、CLI 或 API，請使用 IAM 刪除服務連結角色`DeleteRole`或者`DeleteServiceLinkedRole`API。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台，AWS CLI，或AWSAPI 刪除 AWSServiceRoleForAWSServiceRoleForAWSServiceRoleForAWSServiceRole 角色。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

Storage Gateway 服務連結角色的支援區域

Storage Gateway 支援在所有提供服務的區域中，使用服務連結角色。如需詳細資訊，請參閱 AWS 服務端點。

在提供服務的每一個區域中，Storage Gateway 不支援使用服務連結角色。您可以在下列區域中使用 AWSServiceRoleForAWSServiceRoleForAWSServiceRole 角色。

區域名稱	區域身分	Storage Gateway
美國東部 (維吉尼亞北部)	us-east-1	是
美國東部 (俄亥俄)	us-east-2	是
美國西部 (加利佛尼亞北部)	us-west-1	是
美國西部 (奧勒岡)	us-west-2	是
亞太區域 (孟買)	ap-south-1	是
亞太區域 (大阪)	ap-northeast-3	是
亞太區域 (首爾)	ap-northeast-2	是
亞太區域 (新加坡)	ap-southeast-1	是
亞太區域 (雪梨)	ap-southeast-2	是
亞太區域 (東京)	ap-northeast-1	是
加拿大 (中部)	ca-central-1	是
歐洲 (法蘭克福)	eu-central-1	是
歐洲 (愛爾蘭)	eu-west-1	是
歐洲 (倫敦)	eu-west-2	是
歐洲 (巴黎)	eu-west-3	是
南美洲 (聖保羅)	sa-east-1	是

區域名稱	區域身分	Storage Gateway
AWS GovCloud (US)	us-gov-west-2	是

AWS Storage Gateway 中的記錄和監控

Storage Gateway 與AWS CloudTrail，這是一種提供記錄使用者、角色或AWS服 Storage Gateway。CloudTrail 會將 Storage Gateway 道的所有 API 呼叫捕獲為事件。此外，捕獲的呼叫包括從 Storage Gateway 主控台進行的呼叫，以及對 Storage Gateway API 操作發出的程式碼呼叫。如果您建立線索，就可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 Storage Gateway 道的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的 Event history (事件歷史記錄) 檢視最新事件。您可以利用 CloudTrail 所收集的資訊來判斷向 Storage Gateway 發出的請求，以及發出請求的 IP 地址、人員、時間和其他詳細資訊。

若要進一步了解 CloudTrail，請參閱《AWS CloudTrail 使用者指南》。

CloudTrail 中的 Storage Gateway 資訊

當您建立帳戶時，系統即會在 AWS 帳戶中啟用 CloudTrail。此外，Storage Gateway 道發生活動時，系統便會將該活動記錄至 CloudTrail 事件，並將其他AWS服務事件事件歷史記錄。您可以檢視、搜尋和下載 AWS 帳戶的最新事件。如需詳細資訊，請參閱使用 CloudTrail 事件歷史記錄檢視事件。

若要持續記錄AWS帳户（包含 Storage Gateway 的事件），請建立線索。追蹤能讓 CloudTrail 將日誌檔交付至 Amazon S3 儲存貯體。根據預設，當您在主控台建立線索時，線索會套用到所有 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，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 從多個區域接收 CloudTrail 日誌檔案，以及從多個帳戶接收 CloudTrail 日誌檔案

所有的 Storage Gateway 動作都會記錄並記載在動作主題。例如，對 `ActivateGateway`、`ListGateways` 以及 `ShutdownGateway` 動作發出的呼叫會在 CloudTrail 日誌檔案中產生項目。

每一筆事件或日誌項目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：

- 該請求是否透過根或 AWS Identity and Access Management (IAM) 使用者憑證來提出。
- 提出該要求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 該請求是否由另一項 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，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔包含一或多個日誌項目。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

以下範例顯示的是展示 動作的 CloudTrail 日誌項目。

```
{ "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"
             }]
}
```

以下範例顯示的是展示 ListGateways 動作的 CloudTrail 日誌項目。

```
{
 "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"
            }]
}
```

的合規驗證AWSStorage Gateway

第三方稽核人員會評估AWSStorage Gateway 作為多個AWS合規計劃。這些措施包括 SOC、PCI、ISO、FedRAMP、HIPAA、MTCS、C5、K-ISMS、ENS High、OSPAR 和 HITRUST CSF。

如需特定合規計畫的 AWS 服務範圍清單，請參閱合規計畫的 AWS 服務範圍。如需一般資訊，請參閱 AWS 合規計劃。

您可使用 AWS Artifact 下載第三方稽核報告。如需詳細資訊，請參閱 AWS Artifact 中的下載報告。

您使用 Storage Gateway 的合規責任，取決於資料的機密性、您公司的合規目標及適用法律和法規。AWS提供下列資源，以協助合規：

- 安全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 AWS 上部署以安全及合規為重心之基準環境的步驟。
- HIPAA 安全與合規架構白皮書 – 本白皮書說明公司可如何運用 AWS 來建立 HIPAA 合規的應用程式。
- AWS 合規資源 – 這組手冊和指南可能適用於您的產業和位置。
- 《AWS Config 開發人員指南》中的使用規則評估資源 – AWS Config 服務會評估資源組態在內部實務、業界準則和法規方面的合規程度。
- AWS Security Hub – 此 AWS 服務可供您檢視 AWS 中的安全狀態，可助您檢查是否符合安全產業標準和最佳實務。

中的恢復能力AWSStorage Gateway

AWS 全球基礎設施是以 AWS 區域與可用區域為中心建置的。AWS區域提供多個分開且隔離的實際可用區域，並以低延遲、高輸送量和高度備援聯網功能相互連結。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

如需有關 AWS 區域與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，Storage Gateway 提供數種功能，可協助支援資料的彈性和備份需求。

- 使用 VMware vSphere 高可用性 (VMware HA)，協助保護儲存工作負載免於硬體、虛擬層或網路故障。如需詳細資訊，請參閱「」將 VMware vSphere 與 Storage Gateway 搭配使用。
- 使用 AWS Backup 來備份您的磁碟區。如需詳細資訊，請參閱「」使用AWS Backup備份您的磁帶。
- 從復原點複製您的磁碟區。如需詳細資訊，請參閱「」複製磁帶。
- 將虛擬磁帶存檔在 Amazon S3 冰川中。如需詳細資訊，請參閱「」存檔虛擬磁帶。

中的基礎設施安全AWSStorage Gateway

作為託管服務，AWSStorage Gateway 受AWS全局網絡安全過程，詳情請參閱Amazon Web Services：安全流程概觀白皮書。

您使用AWS發佈的 API 呼叫，透過網路存取存儲閘道。用戶端必須支援 Transport Layer Security (TLS) 1.0 或更新版本。建議使用 TLS 1.2 或更新版本。用戶端也必須支援具備完美轉送私密 (PFS) 的密碼套件，例如臨時 Diffie-Hellman (DHE) 或橢圓曲線臨時 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，請求必須使用存取金鑰 ID 和與 IAM 委託人相關聯的私密存取金鑰來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

Storage Gateway 的安全最佳實務

AWS在您開發和實作自己的安全政策時，可考慮使用 Storage Gateway 提供的多種安全功能。以下最佳實務為一般準則，並不代表完整的安全解決方案。這些最佳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。

為您的閘道進行故障診斷

您可於下述找到有關閘道、檔案共享、磁碟區、虛擬磁帶和快照的故障診斷問題資訊。現場部署閘道故障診斷資訊，包括部署在 VMware ESXi 和 Microsoft Hyper-V 用戶端的閘道。檔案共享的故障診斷資訊適用於 Amazon S3 檔案閘道類型。磁碟區的故障診斷資訊適用於磁碟區閘道類型。磁帶的故障診斷資訊適用於磁帶閘道類型。閘道問題的故障診斷資訊適用於使用 CloudWatch 指標的情況。高可用性問題的故障診斷資訊涵蓋了在 VMware vSphere High Availability (HA) 平台上執行的閘道。

主題

為現場部署閘道故障診斷

您可以在下列信息中找到使用現場部署閘道時一般可能遇到的問題，以及如何啟用AWS Support以幫助您的閘道進行故障診斷。

下表列出使用現場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。 • 若為 VMware ESXi，VM 的 IP 地址可在 Summary (摘要) 標籤的 vSphere 用戶端中找到。 • 若為 Microsoft Hyper-V，登入本機主控台即可找到 VM 的 IP 地址。

問題	採取動作
	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。 • 如果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。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。
當您單擊繼續執行「激活」按鈕。	• 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，您需要設定 SOCKS 代理。如需這項作業的詳細資訊，請參閱測試網關的網絡連接。 • 檢查主機時間是否正確、主機是否設定將其時間自動與網路時間協定 (NTP) 伺服器同步，以及閘道 VM 時間是否正確。如需同步虛擬化管理程序主機和 VM 時間的資訊，請參閱為閘道設定網路時間協定 (NTP) 伺服器。 • 執行完這些步驟後，您可以使用 Storage Gateway 主控台和設置和激活閘道嚮導。 • 確認您的 VM 至少有 7.5 GB 的 RAM。如果 RAM 少於 7.5 GB，閘道配置會失敗。如需詳細資訊，請參閱 檔案閘道設定要求。
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。	

問題	採取動作
您需要改善閘道與AWS。	您可以在網路轉接器 (NIC) 設定網際網路到 AWS 的連線，與連接您應用程式和閘道 VM 的連線區隔開，改善從您閘道到 AWS 的頻寬。如果您有高頻寬的 AWS 連線，而您想要避免頻寬爭用，尤其是在快照恢復期間，此方法非常有用。對於高吞吐量工作負載需求，您可以使用AWS Direct Connect建立內部部署閘道和AWS。若要測量您閘道到 AWS 的連線頻寬，請使用閘道的 `CloudBytesDownloaded` 和 `CloudBytesUploaded` 指標。如需此主題的詳細資訊，請參閱效能。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。	• 在門戶標籤上，驗證您 Storage Gateway 道 VM 的 IP 地址是否和您看到使用您的虛擬化管理程序用户端軟體 (也就是 VMware vSphere 用户端或 Microsoft Hyper-V Manager) 的 IP 地址相同。如果您發現不相符，請從儲存閘道主控台重新啟動您的閘道，如關閉您的閘道 VM。重新啟動後，IP 地址列表中 Storage Gateway 控制台的門戶標籤中的 IP 地址，應該符合您從虛擬化管理程序用户端決定的閘道 IP 地址。
	  • 若為 VMware ESXi，VM 的 IP 地址可在 Summary (摘要) 標籤的 vSphere 用戶端中找到。
	  • 若為 Microsoft Hyper-V，登入本機主控台即可找到 VM 的 IP 地址。
	• 檢查您閘道到 AWS 的連線，如測試網關的網絡連接中所述。
	• 檢查您閘道的網路轉接器組態，並確保所有打算為閘道啟用的界面皆已啟用。若要查看您閘道的網路轉接器組態，請按照為您的閘道設定網路適配器中的指示操作，並選取檢視您閘道網路組態的選項。
	
	您可以從 Amazon CloudWatch 主控台檢視在您閘道出入的輸送量。如需測量您閘道與 AWS 之間輸送量的詳細資訊，請參閱效能。

您無法在 Microsoft Hyper-V 匯入 (部署) Storage Gateway。	請參閱為 Microsoft Hyper-V 安裝進行故障診斷，以了解在 Microsoft Hyper-V 部署閘道的常見問題。

問題	採取動作
您會收到一條消息：「閘道中的磁盤區中的資料無法安全儲存在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，請聯繫AWS Support。

啟用AWS Support幫助排除本地託管的網關故障

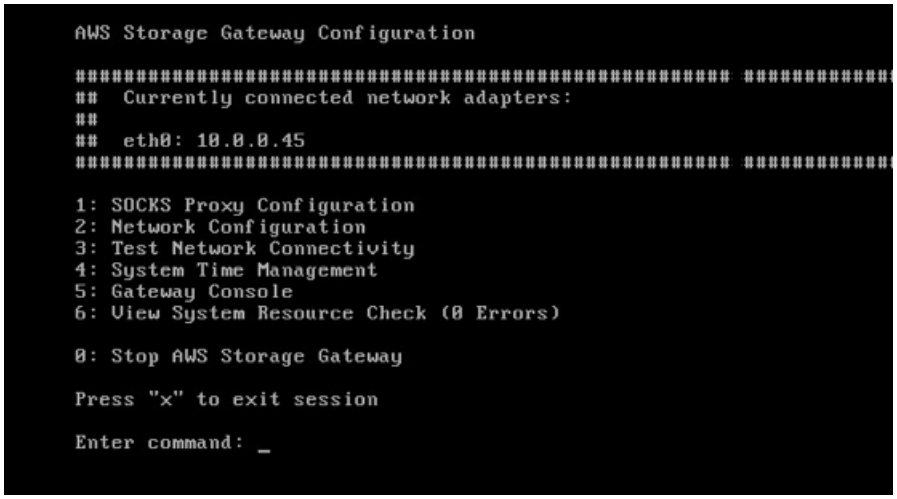
Storage Gateway 提供一個本機主控台，您可以用來執行數種維護任務，包括啟用AWS Support以存取閘道，協助疑難排解閘道的問題。根據預設，AWS Support您的閘道這項功能是停用的。您可以透過主機的本機主控台啟用此存取。給AWS Support存取您的閘道時，您必須先登入主機的本機主控台，然後導覽至 Storage Gateway 的主控台，連線到支援伺服器。

啟用AWS Support存取您的閘道

1. 登入您主機的本機主控台。

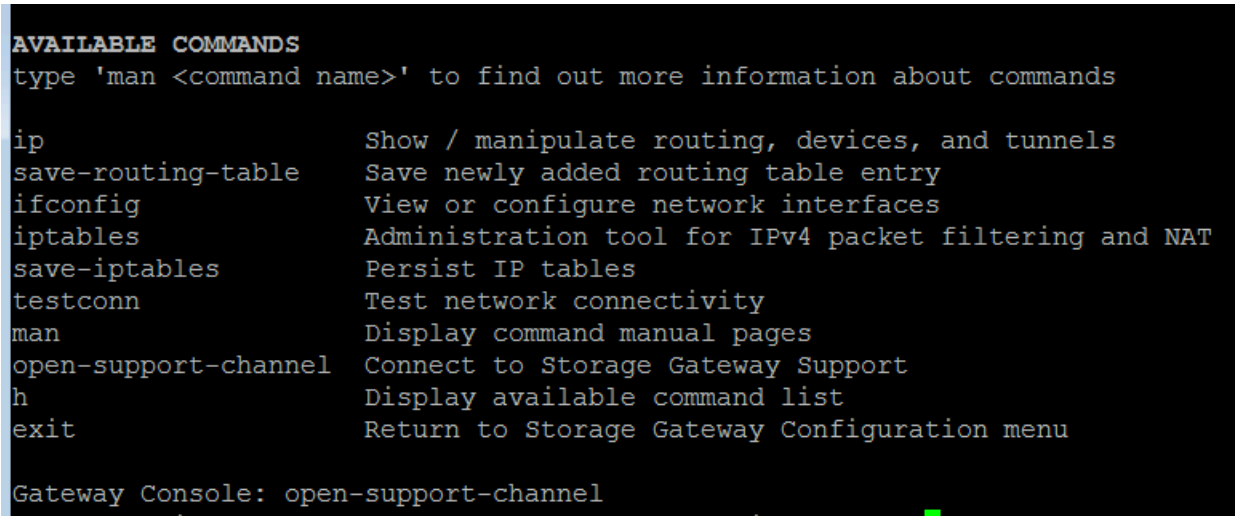
   - VMware ESXi — 如需詳細資訊，請參使用 VMware ESXi 存取閘道本機主控台。
   - Microsoft Hyper-V — 如需詳細資訊，請參使用 Microsoft Hyper-V 存取閘道本機主控台。

   本機主控台如下所示。

2. 出現提示時，輸入**5**開啟AWS Support通道控制台。
3. 輸入 **h** 以開啟 AVAILABLE COMMANDS (可用命令) 視窗。
4. 執行下列任一步驟：

- 如果您的閘道使用公有端點，請在可用命令窗口中，輸入**open-support-channel**連接到 Storage Gateway 的客户支持。允許 TCP 連接埠 22，即可開啟支援管道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 AVAILABLE COMMANDS (可用命令) 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，以連接到 Storage Gateway 的用户支援。允許 TCP 連接埠 22，即可開啟支援管道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。

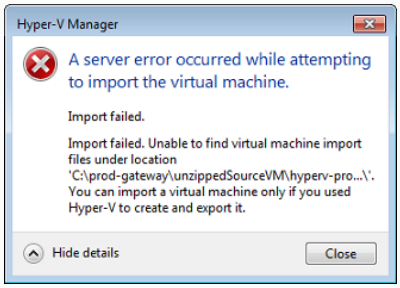
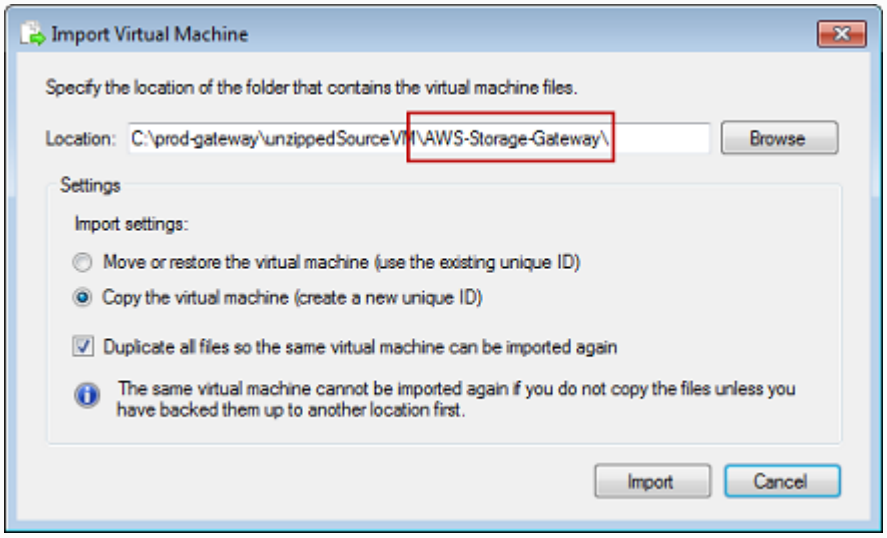


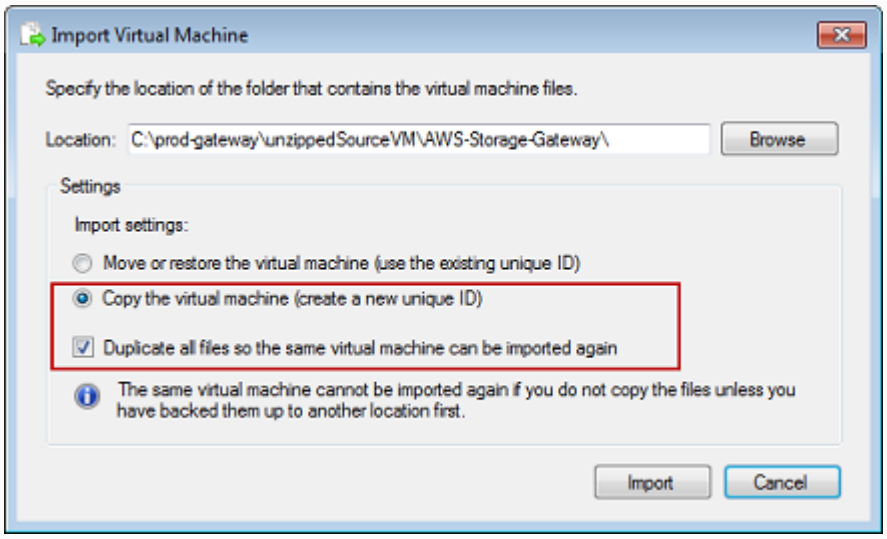
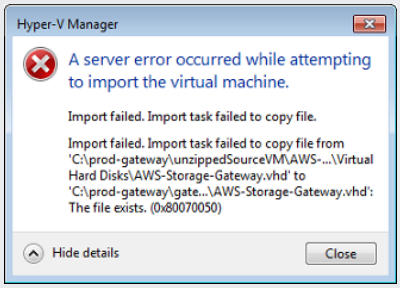
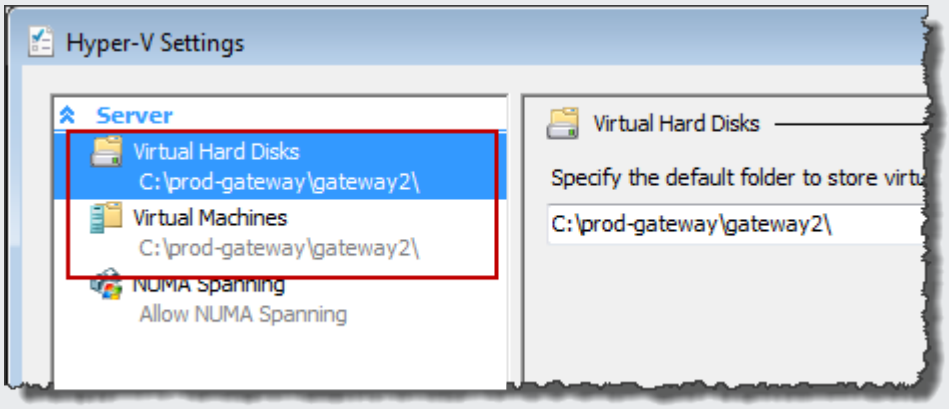
> **Note**
>
> 此管道號碼不是傳輸控制通訊協定/使用者資料包通訊協定 (TCP/UDP) 連接埠號碼。反之，閘道以 Secure Shell (SSH) (TCP 22) 連線到 Storage Gateway 伺服器，並提供此連線的支援管道。

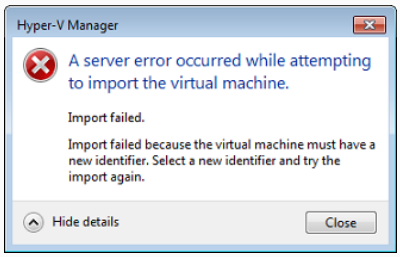
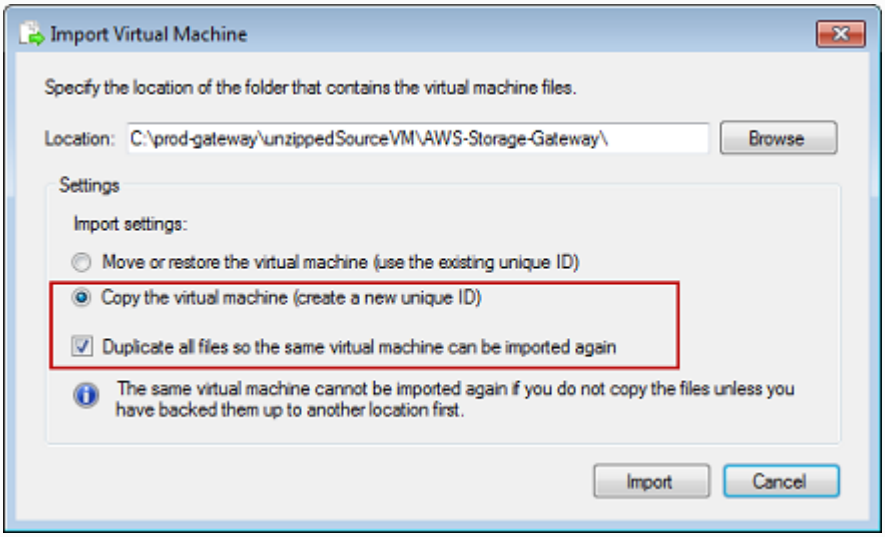
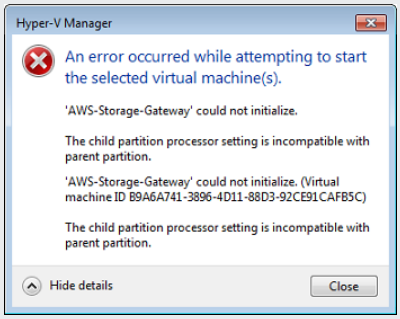
5. 建立支援管道後，請提供您的支援服務號碼至AWS Support所以AWS Support可以提供故障排除幫助。
6. 當支援工作階段完成時，請輸入 **q** 將其結束。在 Amazon Web Services Support 部門通知您支持會話完成之前，請勿關閉會話。
7. Enter**exit**登出 Storage Gateway 主控台。
8. 依照提示結束本機主控台。

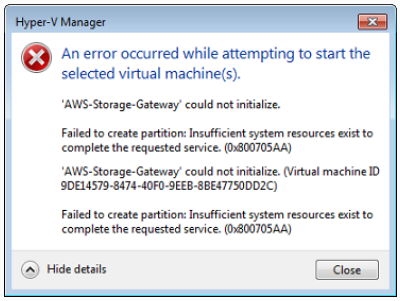
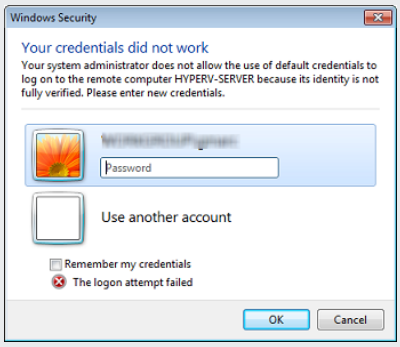
為 Microsoft Hyper-V 安裝進行故障診斷

下表列出在 Microsoft Hyper-V 平台上部署 Storage Gateway 時，一般可能遇到的問題。

問題	採取動作
您嘗試匯入閘道，不過收到以下錯誤訊息：「導入失敗。Unable to find virtual machine import file under location ..."。 	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 Import Virtual Machine (匯入虛擬機器) 對話方塊中指定之位置的最後一個部分應該是 `AWS-Storage-Gateway` ，如下列範例所示：  • 如果您已部署網關，但未選擇複製虛擬機器選項並選中複製所有檔案選項中的導入虛擬機器對話框中，VM 會在您的閘道檔案所在的位置建立，並且無法從此位置再次導入。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。如果您打算從一個解壓縮來源檔案的位置建立多個閘道，以下範例顯示您必須勾選的選項。

問題	採取動作
	
您嘗試匯入閘道，不過收到以下錯誤訊息：「導入失敗。Import task failed to copy file."。 	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。為修正此問題，請在 Hyper-V Settings (Hyper-V 設定) 對話方塊中指定新的位置。 

問題	採取動作
您嘗試匯入閘道，不過收到以下錯誤訊息：「導入失敗。Import failed because the virtual machine must have a new identifier. Select a new identifier and try the import again."。 	導入網關時，請確保選擇複製虛擬機器選項並選中複製所有檔案選項中的導入虛擬機器對話框為 VM 創建新的唯一 ID。以下範例顯示 Import Virtual Machine (匯入虛擬機器) 對話方塊中您應該使用的選項。 
您嘗試啟動閘道 VM，不過收到以下錯誤訊息："The child partition processor setting is incompatible with parent partition."。 	此錯誤可能是因為閘道所需 CPU 和主機可用 CPU 之間的 CPU 差異所造成。請確定基礎虛擬化管理程序支援 VM CPU 計數。 如需 Storage Gateway 需求的詳細資訊，請參檔案閘道設定要求。

問題	採取動作
您嘗試啟動閘道 VM，不過收到以下錯誤訊息："無法建立分區: 資源不足，無法完成請求的服務。」 	此錯誤可能是因為閘道所需 RAM 和主機可用 RAM 之間的 RAM 差異所造成。 如需 Storage Gateway 需求的詳細資訊，請參檔案閘道設定要求。
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 為閘道設定網路時間協定 (NTP) 伺服器。
您需要將解壓縮的 Microsoft Hyper-V Storage Gateway 道檔案放在主機檔案系統。	像您對一般 Microsoft Windows 伺服器所做的一樣，存取主機。例如，如果虛擬化管理程序主機名為 `hyperv-server` ，則您可使用以下 UNC 路徑 `\\hyperv-server\c$` ，其假設 `hyperv-server` 名稱可在本機主機檔案中解析或定義。
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。

排除 Amazon EC2 網關問題

在下列各節中，您會發現使用部署在 Amazon EC2 的閘道時，一般可能遇到的問題。如需現場部署閘道和部署在 Amazon EC2 閘道兩者間之差異的詳細資訊，請參閱在 Amazon EC2 主機上部署檔案閘道。

如需使用暫時性儲存的詳細資訊，請參閱將臨時存儲與 EC2 網關結合使用。

主題

- 您的網關激活幾分鐘後還沒有發生
- 您無法在實例列表中找到 EC2 網關實例
- 你想要的AWS Support幫助您排除 EC2 網關故障

您的網關激活幾分鐘後還沒有發生

請在 Amazon EC2 主控台中檢查下列資訊：

- 已於執行個體相關聯的安全群組中啟用連接埠 80。如需新增安全分組規則的詳細資訊，請參添加安全組規則中的Amazon EC2 Linux 執行個體使用者指南。
- 閘道執行個體標示為執行中。在 Amazon EC2 主控台中，國家值應為 RINNING (執行中)。
- 請確定您的 Amazon EC2 執行個體類型符合最低要求，如儲存需求。

更正問題後，請嘗試再次啟動閘道。若要執行此操作，請打開 Storage Gateway 控制台，選擇在 Amazon EC2 上部署新閘道，然後重新輸入執行個體的 IP 地址。

您無法在實例列表中找到 EC2 網關實例

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 Description (描述) 標籤上檢查 Amazon Machine Image (AMI) 的名稱。以 Storage Gateway AMI 為基礎的執行個體，開頭文字應為**`aws-storage-gateway-ami`**。
- 如果您有數個以 Storage Gateway AMI 為基礎的執行個體，請檢查執行個體的啟動時間，以尋找正確的執行個體。

你想要的AWS Support幫助您排除 EC2 網關故障

Storage Gateway 提供一個本機主控台，您可以用來執行數種維護任務，包括啟用AWS Support以存取閘道，協助疑難排解閘道的問題。根據預設，AWS Support您的閘道這項功能是停用的。您可以透過 Amazon EC2 本機主控台啟用此存取。您可以透過 Secure Shell (SSH) 登入 Amazon EC2 本機主控台。若要透過 SSH 成功登入，您執行個體的安全群組必須有開啟 TCP 連接埠 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。如需安全用組以及如何新增安全分組規則的詳細資訊，請參Amazon EC2 安全群組中的Amazon EC2 使用者指南。

為了讓AWS Support連線至您的閘道時，您必須先登入 Amazon EC2 執行個體的本機主控台，然後導覽至 Storage Gateway 的主控台並提供存取。

啟用AWS Support訪問 Amazon EC2 實例上部署的閘道

1. 登入 Amazon EC2 執行個體的本機主控台。如需取得詳細資訊，請前往連接至您的執行個體中的Amazon EC2 使用者指南。

   您可以使用以下命令登入 EC2 執行個體的本機主控台。

   ```
   ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
   ```

   > **Note**
   >
   > 所以此*####*是.pem檔案，其中包含 EC2 金 key pair 的私有憑證，您可用來啟動 Amazon EC2 執行個體。如需詳細資訊，請參閱「」擷取金鑰對的公有金鑰中的Amazon EC2 使用者指南。
   > 所以此*##-## DNS-NAME*是用於執行閘道之 Amazon EC2 執行個體的公有域名稱系統 (DNS) 名稱。您可以在 EC2 主控台中選取 Amazon EC2 執行個體，然後按一下描述標籤。

2. 在提示下輸入**6 - Command Prompt**開啟AWS Support通道控制台。
3. 輸入 **h** 以開啟 AVAILABLE COMMANDS (可用命令) 視窗。
4. 執行下列任一步驟：

- 如果您的閘道使用公有端點，請在可用命令窗口中，輸入**open-support-channel**連接到 Storage Gateway 的客户支持。允許 TCP 連接埠 22，即可開啟支援管道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 AVAILABLE COMMANDS (可用命令) 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，以連接到 Storage Gateway 的用户支援。允許 TCP 連接埠 22，即可開啟支援管道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**
>
> 此管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。反之，閘道以 Secure Shell (SSH) (TCP 22) 連線到 Storage Gateway 伺服器，並提供此連線的支援管道。

5. 建立支援管道後，請提供您的支援服務號碼至AWS Support所以AWS Support可以提供故障排除幫助。
6. 當支援工作階段完成時，請輸入 **q** 將其結束。在 Amazon Web Services Support 部門通知您支持會話完成之前，請勿關閉會話。
7. Enter**exit**退出 Storage Gateway 控台。
8. 依照主控台選單操作登出 Storage Gateway 執行個體。

故障診斷硬體設備問題

下列主題討論您可能會遇到的問 Storage Gateway，以及故障診斷的建議。

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)。

如何執行重設出廠預設值？

如果您需要在設備上執行重設成出廠預設值，請聯絡 Storage Gateway 硬件設備團隊以請求 Support，如下列「支援」部分所述。

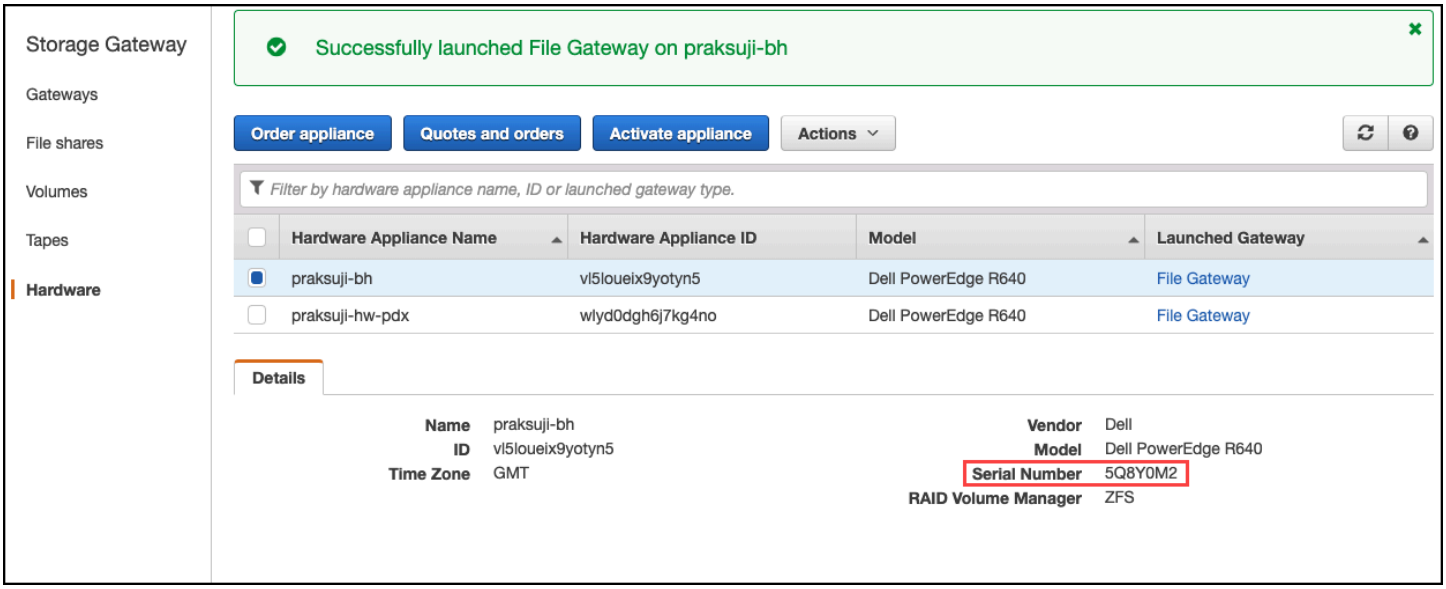
您在哪裏獲得戴爾 iDRAC 支持？

Dell PowerEdge R640 伺服器隨附 Dell iDRAC 管理界面。我們建議下列作法：

- 如果您使用 iDRAC 管理界面，則應該變更默認密碼。如需 iDRAC 憑證的詳細資訊，請參戴爾 PowerEdge-iDRAC 的默認用户名和密碼是什麼？。
- 請確定韌體是最新狀態，以防止安全漏洞。
- 將 iDRAC 網路界面移到一般 (em) 連接埠，可能導致效能問題或阻止設備正常運作。

找不到硬件裝置序列號

要查找硬件裝置的序列號，請轉到硬體頁面 Storage Gateway 下所示。



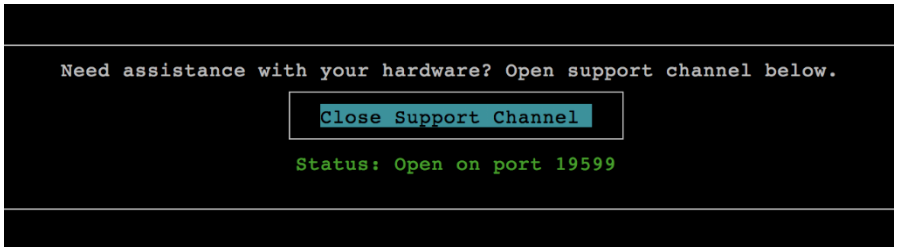
從何處獲得硬件設備支持

要聯繫 Storage Gateway 硬件設備支持部門，請參閱AWS Support。

所以此AWS Support團隊可能會要求您啟用支援渠道，以便從遠端排除閘道問題。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。

若要打開支援管道AWS

1. 開啟硬體主控台。
2. 選擇 Open Support Channel (開啟支援管道)，如下所示。



如果沒有網路連線或防火牆問題的話，指派的連接埠號碼應該會在 30 秒內顯示。

3. 請記下端口號並提供給AWS Support。

疑難排解檔案閘道問題

當您執行 VMware vSphere 高可用性 (HA) 時，您可以使用 Amazon CloudWatch 日誌組設定檔案閘道。如果您這麼做，您會收到檔案閘道運作狀態及檔案閘道遇到的錯誤的相關通知。您可以在 CloudWatch Logs 中找到這些錯誤和運作狀態通知的相關資訊。

在下列各節，您可以找到相關資訊，協助您了解每個錯誤的原因、運作狀態通知，以及修正問題的方法。

主題

錯誤：InaccessibleStorageClass

你可以得到一個`InaccessibleStorageClass`當物件已移出 Amazon S3 標準儲存類別時發生錯誤。

在此，您的檔案閘道嘗試將指定物件上傳到 S3 儲存貯體或從 S3 儲存貯體讀取物件時，通常會發生錯誤。出現此錯誤時，物件通常已移至 Amazon S3 Glacier，並位於 S3 Glacier 或 S3 Glacier Deep Archive 儲存類別。

解決 InaccessibleStorageClass 錯誤

- 將物件從 S3 Glacier 或 S3 Glacier Deep Archive 儲存類別移回 S3。

  如果您將物件移至 S3 儲存貯體以修正上傳錯誤，檔案最終會上傳。如果您將物件移至 S3 儲存貯體以修正讀取錯誤，那麼檔案閘道的 SMB 或 NFS 用户端即可讀取檔案。

錯誤：S3 訪問被拒絕

你可以得到一個`S3AccessDenied`檔案共享的 Amazon S3 儲存貯體存取時出錯AWS Identity and Access Management(IAM) 角色。在此情況下，S3 儲存貯體存取 IAM 角色由`roleArn`在錯誤中不允許涉及的操作。由於 Amazon S3 前綴指定之目錄中的物件許可，不允許此操作。

若要解決 S3AccessDenessDening 錯誤

- 修改附加到的 Amazon S3 訪問策略`roleArn`以允許 Amazon S3 操作的許可。請確認存取政策可允許導致該錯誤的操作許可。此外，請允許 `prefix` 之日誌中所指定的目錄許可。如需 Amazon S3 許可的詳細資訊，請參在政策中指定許可在Amazon Simple Simple Storage Service 用户指南

  這些操作可能會導致 `S3AccessDenied` 錯誤發生：

  - `S3HeadObject`
  - `S3GetObject`
  - `S3ListObjects`
  - `S3DeleteObject`
  - `S3PutObject`

錯誤：InvalidObjectState

你可以得到一個`InvalidObjectState`當指定的檔案閘道以外的寫入器修改指定的 S3 儲存貯體中的指定檔案時，會發生錯誤。因此，檔案閘道的檔案狀態不符合其在 Amazon S3 中的狀態。後續上傳檔案至 Amazon S3 或從 Amazon S3 檢索檔案會失敗。

解決無效狀態錯誤的步驟

如果修改檔案的操作為S3Upload或者S3GetObject，執行下列動作：

1. 將檔案的最新副本儲存至 SMB 或 NFS 用户端的本機檔案系統（您需要在步驟 4 中複製此檔案）。如果 Amazon S3 中的檔案版本是最新版本，請下載該版本。您可以使用 AWS Management Console 或 AWS CLI 執行此作業。
2. Amazon S3 用AWS Management Console或者AWS CLI。
3. 使用您的 SMB 或 NFS 用端，從檔案閘道刪除檔案。
4. 使用您的 SMB 或 NFS 用户端，將您在步驟 1 中儲存的檔案的最新版本複製到 Amazon S3。透過您的檔案閘道執行此作業。

錯誤：ObjectMissing

你可以得到一個ObjectMissing當指定的檔案閘道以外的寫入者從 S3 儲存貯體刪除指定的檔案時，會發生錯誤。後續任何物件上傳至 Amazon S3 或從 Amazon S3 檢索該物件都會失敗。

解決 ObjectMissing 錯誤

如果修改檔案的操作為S3Upload或者S3GetObject，執行下列動作：

1. 將檔案的最新副本儲存至 SMB 或 NFS 用户端的本機檔案系統（您需要在步驟 3 中複製此檔案）。
2. 使用您的 SMB 或 NFS 用端，從檔案閘道刪除檔案。
3. 使用您的 SMB 或 NFS 用户端，複製您在步驟 1 中儲存的檔案的最新版本。透過您的檔案閘道執行此作業。

：Notification 重新開機

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 主控台或儲存閘道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。

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，此重新啟動可能是正常的情況，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。

：Notification 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 執行的重設可能會觸發此事件。

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。

：Notification 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。

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。

：Notification AvailabilityMonitorTest

你會得到一個AvailabilityMonitorTest當您運行測試的可用性和應用程序監控系統上運行在 VMware vSphere HA 平台上的網關上。

錯誤：RoleTrustRelationshipInvalid

當檔案共享的 IAM 角色有配置錯誤的 IAM 信任關係時 (也就是 IAM 角色不信任名為storagegateway.amazonaws.com。因此，檔案閘道無法取得登入資料來在備份檔案共享的 S3 儲存貯體上執行任何操作。

解決 RoleTrustRelationshipInvalid 錯誤

- 使用 IAM 主控台或 IAM API 包含storagegateway.amazonaws.com作為您檔案共享 iAMRole 所信任的委託人。如需 IAM 角色的詳細資訊，請參教程：跨AWS使用 IAM 角色的賬户。

使用 CloudWatch 指標進行故障

您可在下列資訊中找到應對使用 Amazon CloudWatch 指標與 Storage Gateway 相結合的問題所需採取的動作。

主題

瀏覽目錄時，網關反應緩慢

如果檔案閘道反應緩慢，當您執行ls命令或瀏覽目錄，請檢查IndexFetch和IndexEvictionCloudWatch 指標：

- 如果IndexFetch量度大於 0，當您運行ls命令或瀏覽目錄時，您的檔案閘道已在沒有受影響目錄內容的信息的情況下啟動，並且必須存取 Amazon S3。後續列出該目錄內容的動作應會更快完成。
- 如果IndexEviction指標大於 0，表示檔案閘道已達到其在當下可以管理的數量限制。在此情況下，檔案閘道必須從最近存取的目錄釋放一些儲存空間，才能列出新目錄。如果經常發生此問題，並對性能有影響，請聯繫AWS Support。

  與之開發AWS Support相關 S3 儲存貯體的內容和建議，以根據您的使用案例提升效能。

您的網關沒有響應

如果檔案閘道沒有回應，請執行下列操作：

- 如果有最近的重新開機或軟體更新，則請查看 IOWaitPercent 指標。此指標會顯示在有未完成磁碟 I/O 請求時 CPU 閒置時間的百分比。在某些情況下，百分比可能偏高 (10 或以上)，而且可能已在伺服器重新啟動或更新後上升。在這些情況下，檔案閘道會重建索引高速緩存至 RAM，因此檔案閘道可能因根磁碟較慢而存在瓶頸。您可以將速度較快的實體磁碟用於根磁碟來解決此問題。

- 如果MemUsedBytes指標等於或幾乎與MemTotalBytes指標，則檔案閘道的可用 RAM 即將用盡。請確認檔案閘道至少有所需的最小 RAM。如果已有此容量，請根據您的工作負載和使用案例，考慮增加更多 RAM 到檔案閘道。

  如果檔案共享是 SMB，此問題也可能是因為連線到檔案共享的 SMB 用戶端數目所造成。若要查看在任何指定時間連線的用戶端數目，請檢查 SMBV(1/2/3)Sessions 指標。如果有許多用户端連線，您可能需要增加更多 RAM 到檔案閘道。

您的閘道傳輸資料到 Amazon S3 的速度緩慢

如果檔案閘道傳輸資料到 Amazon S3 的速度緩慢，請執行下列操作：

- 如果CachePercentDirty指標是 80 或以上，則檔案閘道寫入資料到磁碟的速度會比上傳資料到 Amazon S3 的速度更快。請考慮從檔案閘道增加上傳頻寬、增加一或多個快取磁碟，或降低用户端寫入速度。
- 如果CachePercentDirty指標偏低，請檢查IoWaitPercent指標。如果IoWaitPercent大於 10，檔案閘道可能因本機快取磁碟速度而存在瓶頸。建議將本機固態硬碟 (SSD) 磁碟用於快取，最好是 NVM Express (NVMe)。如果無法取得這種磁碟，請嘗試使用來自個別實體磁碟的多個快取磁碟，以提升效能。
- 如果S3PutObjectRequestTime、S3UploadPartRequestTime, 或S3GetObjectRequestTime很高，則可能存在網絡瓶頸。嘗試分析您的網絡以驗證網關是否具有預期帶寬。

您的網關執行的 Amazon S3 操作比預期要多

如果您的文件網關執行的 Amazon S3 操作比預期要多，請檢查FilesRenamed指標。在 Amazon S3 中執行重命名操作的成本很高。優化工作流以最大限度地減少重命名操作的次數。

您在 Amazon S3 儲存貯體中看不到檔案

如果您注意到閘道上的檔案未反映在 Amazon S3 儲存貯體中，請檢查FilesFailingUpload指標。如果指標報告某些文件上傳失敗，請檢查您的運行狀況通知。當文件上傳失敗時，網關會生成一個運行狀況通知，其中包含有關該問題的更多詳細信息。

您的閘道備份任務失敗，或寫入至閘道時發生錯誤

如果檔案閘道備份任務失敗，或寫入至檔案閘道時發生錯誤，請執行下列動作：

- 如果CachePercentDirty指標是 90% 或以上，由於快取磁碟上無足夠的可用空間，您的檔案閘道則無法接受對磁碟的新寫入。若要查看檔案閘道上傳至 Amazon FSX 或 Amazon S3 的速度，請參CloudBytesUploaded指標。將該指標與WriteBytes指標，該指標會顯示客户端向檔案閘道寫入檔案的速度。如果您的檔案閘道寫入速度比上傳到 Amazon FSX 或 Amazon S3 的速度更快，請增加更多快取磁碟，以至少涵蓋備份任務的大小。或者，增加上傳頻寬。
- 如果備份作業失敗，但CachePercentDirty指標小於 80%，則檔案閘道可能遇到用户端會話超時。若是 SMB，您可使用 PowerShell 命令 `Set-SmbClientConfiguration -SessionTimeout 300` 來增加此逾時設定。執行此命令會將逾時設為 300 秒。

  若是 NFS，請確認用戶端是採用硬性掛載的方式掛載，而非是軟性掛載。

疑難排解檔案共享問題

如果您的檔案共享發生非預期問題，您可在下列資訊中找到應採取的動作。

主題

您的文件共享卡在創建狀態

當您的檔案共享正在建立時，其狀態為 CREATING (建立中)。檔案共享建立後，狀態會轉換為 AVAILABLE (可用) 狀態。如果您的檔案共享停滯在 CREATING (建立中) 狀態，請執行下列動作：

1. 請在 https://console.aws.amazon.com/s3/ 開啟 Amazon S3 主控台。

2. 確認您檔案共享所映射的 S3 儲存貯體存在。如果儲存貯體不存在，請予以建立。儲存貯體建立後，檔案共享狀態會轉換為 AVAILABLE (可用)。如需如何建立 S3 儲存貯體的詳細資訊，請參建立儲存貯體中的Amazon Simple Storage Service 用户指南。
3. 請確認您的儲存貯體名稱遵守 Amazon S3 儲存貯體的命名規則。如需詳細資訊，請參閱 Amazon Simple Storage Service 使用者指南中的儲存貯體命名規則。
4. 請確定您用來存取 S3 儲存貯體的 IAM 角色有正確的許可，並確認 S3 儲存貯體列為 IAM 政策的資源。如需詳細資訊，請參閱 授予對 Amazon S3 儲存貯體的存取權。

您無法建立檔案共享

1. 如果您因為檔案共享停滯在 CREATING (建立中) 狀態而無法建立檔案共享，請確認您的檔案共享所映射的 S3 儲存貯體存在。如需如何執行作業的資訊，請參閱上一篇的您的文件共享卡在創建狀態。
2. 如果 S3 儲存貯體存在，請驗證AWS Security Token Service在您建立檔案共享的區域中已啟用。如未啟用安全權杖，您應予以啟用。如需如何使用AWS Security Token Service，請參啟用和停用AWSSTS 在AWSRegion (區域)中的IAM User Guide。

SMB 檔案共享不允許多種不同的存取方法

SMB 檔案共享有以下限制：

1. 當相同的用戶端嘗試同時掛載 Active Directory 和訪客存取 SMB 檔案共享，會顯示以下錯誤訊息：`Multiple connections to a server or shared resource by the same user, using more than one user name, are not allowed. Disconnect all previous connections to the server or shared resource and try again.`
2. Windows 使用者不能保持連線到兩個訪客存取 SMB 檔案共享，當新的訪客存取連線建立時可能會中斷連線。
3. Windows 用戶端無法同時掛載訪客存取和由相同閘道匯出的 Active Directory SMB 檔案共享。

多個文件共享無法寫入映射的 S3 存儲桶

我們不建議您設定 S3 儲存貯體允許多個檔案共享寫入一個 S3 儲存貯體。這種方法會造成無法預測的結果。

相反地，我們建議您只允許一個檔案共享寫入一個 S3 儲存貯體。您建立一個儲存貯體政策，僅允許與您檔案共享相關聯的角色寫入儲存貯體。如需詳細資訊，請參閱 檔案共享最佳實務。

無法將文件上傳到您的 S3 存儲桶

如果您無法將檔案上傳到 S3 儲存貯體，請執行下列操作：

1. 請確定您已授予 Amazon S3 檔案閘道所需的存取權，將檔案上傳到您的 S3 儲存貯體。如需詳細資訊，請參閱 授予對 Amazon S3 儲存貯體的存取權。
2. 確定建立儲存貯體的角色具有寫入 S3 儲存貯體的許可。如需詳細資訊，請參閱 檔案共享最佳實務。
3. 如果您的文件網關使用 SSE-KMS 進行加密，請確保與文件共享關聯的 IAM 角色包含kms:Encrypt、kms:Decrypt、KMS: 重新加密、kms:GenerateDataKey，和kms:DescribeKey許可。如需詳細資訊，請參閱「」在 Storage Gateway 使用以身分為基礎的政策 (IAM 政策)。

無法更改默認加密以使用 SSE-KMS 加密存儲在我的 S3 存儲桶中的對象

如果您改變默認加密，使 SSE-KMS（使用AWS KMS— 託管密鑰) S3 儲存貯體的默認值，Amazon S3 檔案閘道儲存在儲存貯體中的物件不會使用 SSE-KMS 加密。默認情況下，S3 檔案閘道會在將資料寫入 S3 儲存貯體時，使用以 Amazon S3 (SSE-S3) 管理的伺服器端加密。變更預設值不會自動變更您的加密。

若要變更加密為使用 SSE-KMS 搭配您自己的 AWS KMS 金鑰，您必須啟用 SSE-KMS 加密。若要這樣做，當您建立檔案共享時要提供 KMS 金鑰的 Amazon Resource Name (ARN)。您也可以使用 `UpdateNFSFileShare` 或 `UpdateSMBFileShare` API 操作，更新您檔案共享的 KMS 設定。此更新適用於更新後存放在 S3 儲存貯體中的物件。如需詳細資訊，請參閱 使用的資料加密AWS KMS。

在啟用了對象版本控制的 S3 存儲桶中直接進行的更改可能會影響您在文件共享中看到的內容

如果您 S3 儲存貯體中有另一個用户端寫入的物件，由於 S3 儲存貯體物件版本控制的緣故，您的 S3 儲存貯體檢視可能不是最新的。您應一律先重新整理您的快取，再檢查感興趣的檔案。

物件版本控制是選用的 S3 儲存貯體功能，透過存放多個同名物件的副本以利保護資料。每個副本都有一個獨立的 ID 值，例如`file1.jpg：ID="xxx"`和`file1.jpg：ID="yyy"`。 同名物件的數目及其生命週期都由 Amazon S3 生命週期政策控制。如需這些 Amazon S3 概念的詳細資訊，請參使用版本控制和物件生命週期管理中的Amazon S3 開發人員指南。

當您刪除版本控制的物件時，該物件會以刪除標記加以標記並保留下來。只有 S3 儲存貯體擁有者才能永久刪除開啟版本控制的物件。

在 S3 File Gateway 中，提取物件或重新整理快取時所顯示的檔案，會是 S3 儲存貯體中最新版的物件。S3 檔案閘道會忽略任何較舊的版本或任何標記刪除的物件。讀取檔案時，您讀取的資料是來自最新的版本。在您的檔案共享中寫入檔案時，S3 File Gateway 會使用您的更改建立新版的命名物件，並且該版本會成為最新的版本。

您的 S3 File Gateway 會持續從早期版本讀取，而在您的應用程式外新增到 S3 儲存貯體的新版本，您所做的更新會基於早期版本。若要讀取最新版的物件，請從主控台使用 RefreshCache API 動作或重新整理，如 刷新 Amazon S3 儲存貯體中的物件 中所述。

> **Important**
>
> 我們不建議從檔案共享以外將物件或檔案寫入您的 S3 File Gateway S3 儲存貯體。

當寫入啟用了對象版本控制的 S3 存儲桶時，Amazon S3 文件網關可能會創建 S3 對象的多個版本

啟用對象版本控制後，您可能會在從 NFS 或 SMB 客户端對文件進行每次更新時在 Amazon S3 中創建的對象的多個版本。以下是可能導致在 S3 存儲桶中創建多個數據元版本的方案：

- 當文件上傳到 Amazon S3 後，NFS 或 SMB 客户端在 Amazon S3 文件網關中修改文件時，S3 文件網關將上傳新數據或修改後的數據，而不是上傳整個文件。文件修改將導致創建新版本的 Amazon S3 對象。
- 當文件由 NFS 或 SMB 客户端寫入 S3 文件網關時，S3 文件網關會將文件的數據上傳到 Amazon S3，後跟其元數據（所有權、時間戳等）。上傳文件數據會創建 Amazon S3 對象，上傳文件的元數據會更新 Amazon S3 對象的元數據。此過程將創建對象的另一個版本，從而產生兩個版本的對象。
- 當 S3 文件網關上傳較大的文件時，它可能需要在客户端完成寫入文件網關之前上傳較小的文件塊。這樣做的一些原因包括釋放緩存空間或高寫入文件的速率。這會導致 S3 儲存貯體中的物件存在多個版本。

在設置生命週期策略以將對象移動到不同的存儲類之前，您應該監視 S3 存儲桶以確定存在多少個對象版本。您應該為早期版本配置生命週期過期，以最大限度地減少 S3 存儲桶中對象的版本數量。在 S3 存儲桶之間使用同區域複製 (SRR) 或跨區域複製 (CRR) 將增加所使用的存儲空間。如需複寫的詳細資訊，請參複寫。

> **Important**
>
> 在您瞭解啟用對象版本控制時使用的存儲量之前，請勿在 S3 存儲桶之間配置複製。

使用版本控制的 S3 儲存貯體可以大幅增加 Amazon S3 的儲存量，因為每次修改檔案都會建立新版的 S3 物件。在默認情況下，除非您專門建立政策，覆寫此行為並限制保留的版本數目，否則 Amazon S3 會持續存放所有這些版本。如果在物件版本控制啟用時發現不尋常的大量儲存使用量，請檢查您的儲存政策是否正確設定。瀏覽器請求的 HTTP 503-slow down 回應數增加，也會導致物件版本控制問題。

如果您在安裝 S3 File Gateway 後啟用物件版本控制，所有唯一的物件皆會保留 (ID="NULL")，您可以在檔案系統中看到它們。新版的物件會獲指派唯一的 ID (保留較舊版本)。以物件的時間戳記為基礎，只有最新的版本控制物件會出現在 NFS 檔案系統中。

在您啟用物件版本控制之後，您的 S3 儲存貯體即無法回到無版本控制的狀態。但是您可以暫停版本控制。當您暫停版本控制時，新的物件會獲指派一個 ID。如有值為 ID="NULL" 的相同具名物件存在，則會覆寫較舊的版本。但仍保留包含非 NULL ID 的任何版本。時間戳記會將新的物件視為最新的物件，這也是出現在 NFS 檔案系統中的物件。

對 S3 存儲桶的更改不會反映在 Storage Gateway 中

當您使用文件共享本地將文件寫入緩存時，Storage Gateway 會自動更新文件共享緩存。但是，當您將文件直接上傳到 Amazon S3 時，Storage Gateway 不會自動更新緩存。執行此操作時，您必須執行`RefreshCache`操作以查看文件共享上的更改。如果您有多個檔案共享，則必須運行`RefreshCache`對每個文件共享進行操作。

您可以使用 Storage Gateway 控制台和AWS Command Line Interface(AWS CLI)：

- 要使用 Storage Gateway 控制台刷新緩存，請參閱刷新 Amazon S3 存儲桶中的對象。
- 若要使用AWS CLI：
  1. 執行命令`aws storagegateway list-file-shares`
  2. 將檔案共享的 Amazon Resource Name (ARN) 與您要刷新的緩存一起複製。
  3. 執行`refresh-cache`命令中的值，您的 ARN 作為`--file-share-arn`：

     ```
     aws storagegateway refresh-cache --file-share-arn
     arn:aws:storagegateway:eu-west-1:12345678910:share/share-FFDEE12
     ```

自動化RefreshCache操作，請參閱如何在 Storage Gateway 上自動執行 RefreshCache 操作？

ACL 許可未如預期般運作

如果存取控制清單 (ACL) 許可未如預期搭配 SMB 檔案共享運作，您可以執行測試。

若要這樣做，請先在 Microsoft Windows 檔案伺服器或本機 Windows 檔案共享上測試許可。接著，將其行為與閘道的檔案共享進行比較。

執行遞歸操作後，您的網關性能下降

在某些情況下，您可能會執行遞迴操作，例如重新命名目錄或啟用 ACL 的繼承，以及強制沿著樹狀目錄向下進行。如果您這麼做，S3 File Gateway 會以遞迴方式套用操作到檔案共享中的所有物件。

例如，假設您套用繼承到 S3 儲存貯體中的現有物件。您的 S3 檔案閘道會以遞迴方式套用繼承到儲存貯體中的所有物件。這類操作可能會導致閘道的效能下降。

高可用性運作狀態通知

在 VMware vSphere High Availability (HA) 平台上執行閘道時，您可能會收到運作狀態通知。如需運作狀態通知的詳細資訊，請參閱故障診斷高可用性問題。

故障診斷高可用性問題

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 Health 態通知
- 指標

運作 Health 態通知

在 VMware vSphere HA 上執行閘道時，所有閘道都會對您設定的 Amazon CloudWatch 日誌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

- ：Notification 重新開機
- ：Notification HardReboot

- ：Notification HealthCheckFailure
- ：Notification AvailabilityMonitorTest

：Notification 重新開機

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 主控台或儲存閘道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。

：Notification 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 執行的重設可能會觸發此事件。

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。

：Notification 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。

：Notification AvailabilityMonitorTest

如果是 VMware vSphere HA 上的閘道，您可以獲取`AvailabilityMonitorTest`當您運行測試的可用性和應用程序監控系統。

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。如需事件的詳細資訊，請參您配置的 CloudWatch 日誌組。

恢復您的數據最佳實務

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 道不支援從虛擬化管理程序或 Amazon EC2 Amazon 機器映像 (AMI) 所建立的快照復原閘道 VM。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

- 從意外的虛擬機關閉中恢復
- 從出現故障的緩存磁盤恢復數據
- 從無法存取之資料中心的復原資料

從意外的虛擬機關閉中恢復

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，請參閱測試網關的網絡連接。

- 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。

從出現故障的緩存磁盤恢復數據

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 從出現故障的緩存磁盤恢復數據。

從無法存取之資料中心的復原資料

如果您的閘道或資料中心因為某些原因而無法存取，您可以將資料復原到不同資料中心的另一個閘道，或復原到 Amazon EC2 執行個體託管的閘道。如果您無法存取另一個資料中心，我們建議您在 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檔案閘道復原資料

針對檔案閘道，您要將新的檔案共享映射到包含要復原資料的 Amazon S3 儲存貯體。

1. 在 Amazon EC2 主機上建立和啟用新的檔案閘道。如需詳細資訊，請參閱 在 Amazon EC2 主機上部署檔案閘道。
2. 在您建立的 EC2 閘道上建立新的檔案共享。如需詳細資訊，請參閱「」建立檔案共享。
3. 將您的檔案共享掛載在您的用户端，將它映射到包含您要復原資料的 S3 儲存貯體。如需詳細資訊，請參閱「」裝載並使用您的文件共享。

其他 Storage Gateway 資源

在本區段中，您可以找到關於AWS和第三方軟體、工具和資源，以及幫助您設定或管理閘道之 Storage Gateway 額的資訊。

主題

主機設定

主題

設定 VMware of Storage Gateway

配置 VMware to Storage Gateway 時，請務必同步 VM 時間與主機時間、設定 VM 以在佈建儲存時使用全虛擬化磁碟控制器，以及提供保護免於支援閘道 VM 之基礎設施層的故障。

主題

同步 VM 時間與主機時間

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，您檢查主機時間，並在需要時設定主機時間，以及設定主機自動同步其時間與網路時間協定 (NTP) 伺服器。

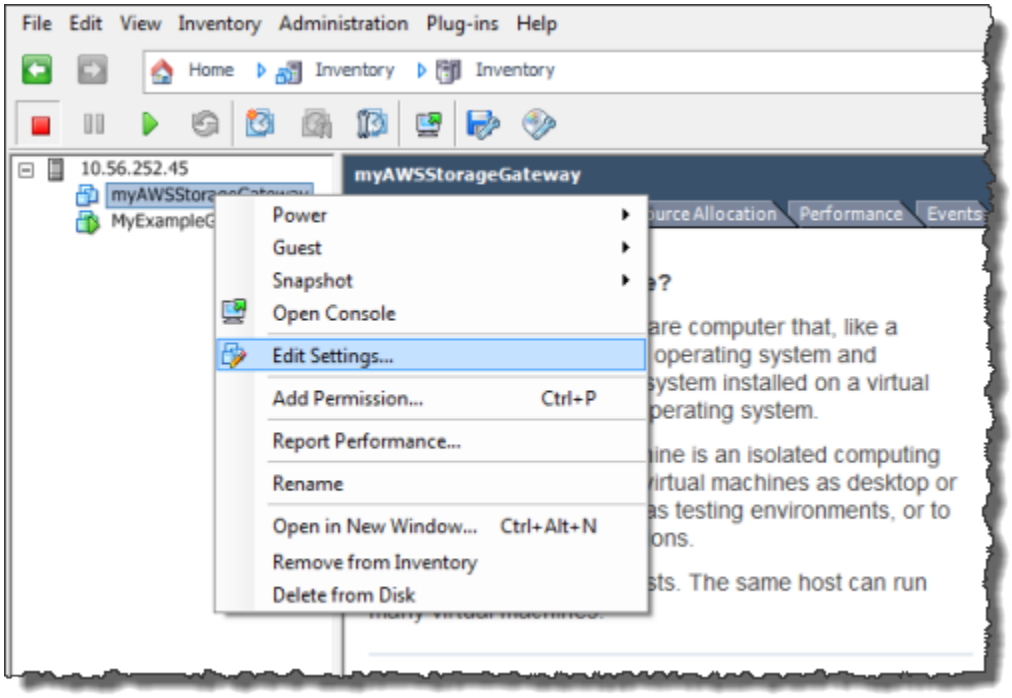
> **Important**
>
> 需要同步 VM 時間與主機時間，才能成功啟用閘道。

同步 VM 時間與主機時間

1. 設定 VM 時間。

   a. 在 vSphere 用戶端中，開啟閘道 VM 的內容 (按右鍵) 選單，然後選擇 Edit Settings (編輯設定)。

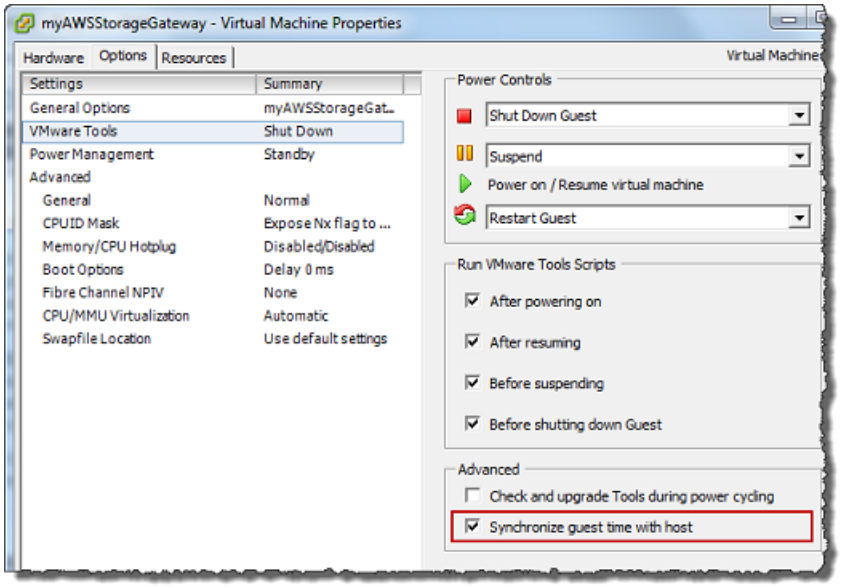
      Virtual Machine Properties (虛擬機器屬性) 對話方塊隨即開啟。



   b. 選擇 Options (選項) 標籤，然後選擇選項清單中的 VMware Tools。

   c. 核取 Synchronize guest time with host (同步訪客時間與主機) 選項，然後選擇 OK (確定)。

VM 會同步其時間與主機。



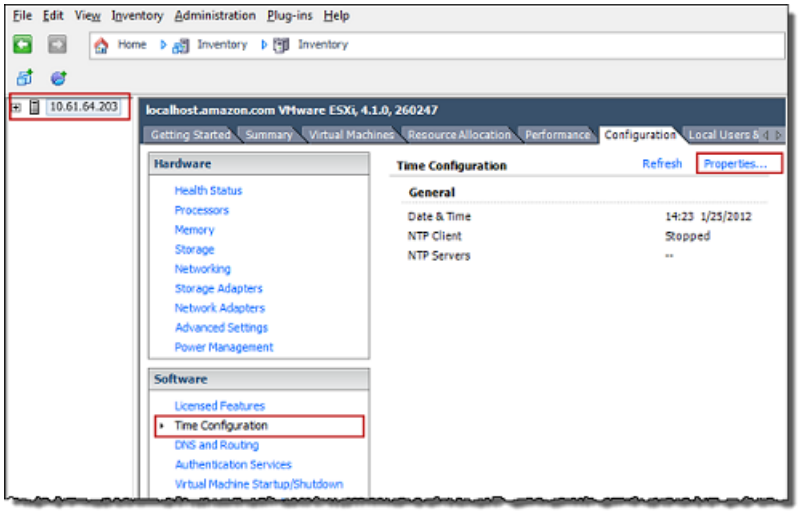
2. 設定主機時間。

   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，請執行下列步驟來設定和同步它與 NTP 伺服器。

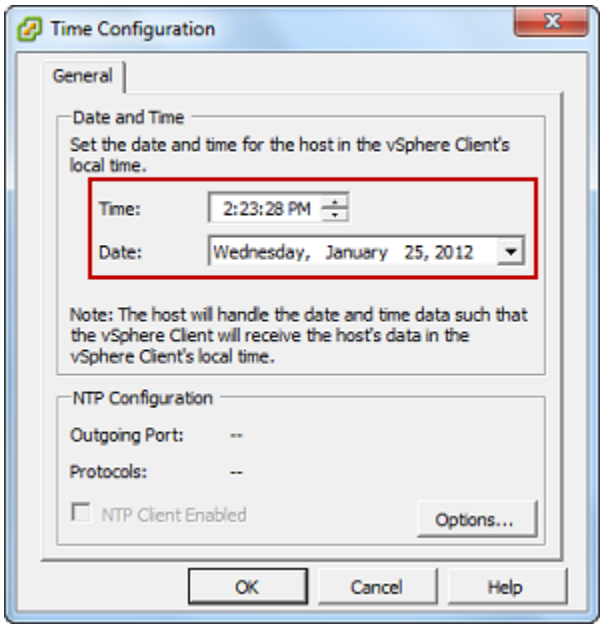
   a. 在 VMware vSphere 用戶端中，於左窗格中選取 vSphere 主機節點，然後選擇 Configuration (組態) 標籤。

   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。

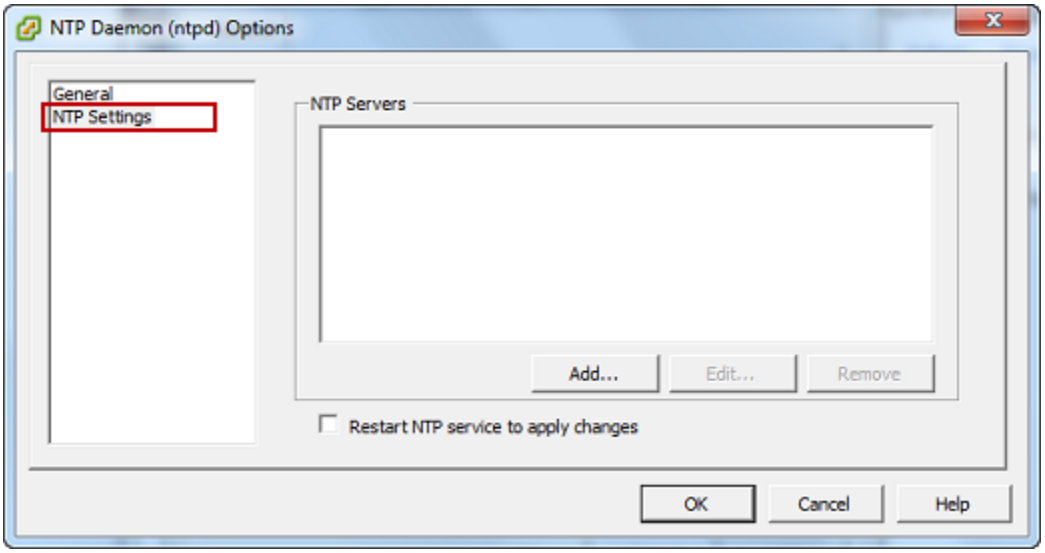


c. 在 Date and Time (日期和時間) 面板中，設定日期和時間。



d. 設定主機自動同步其時間與 NTP 伺服器。

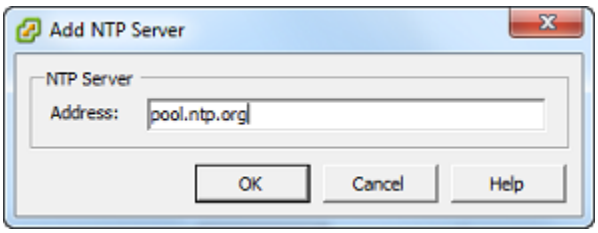
i. 選擇 Time Configuration (時間組態) 對話方塊中的 Options (選項)，然後在 NTP Daemon (ntpd) Options (NTP 協助程式 (ntpd) 選項) 對話方塊的左窗格中選擇 NTP Settings (NTP 設定)。



ii. 選擇 Add (新增) 以新增 NTP 伺服器。

iii. 在 Add NTP Server (新增 NTP 伺服器) 對話方塊中，輸入 NTP 伺服器之完整網域名稱的 IP 地址，然後選擇 OK (確定)。

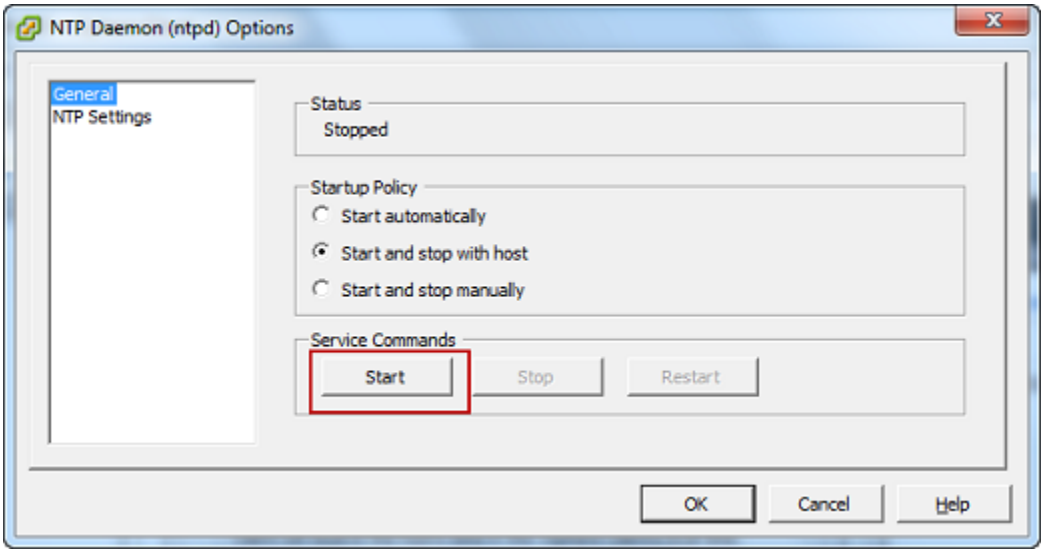
您可以使用 `pool.ntp.org`，如下列範例所示。



iv. 在 NTP Daemon (ntpd) Options (NTP 協助程式 (ntpd) 選項) 對話方塊中，選擇左窗格中的 General (一般)。

v. 在 Service Commands (服務命令) 窗格中，選擇 Start (啟動) 以啟動服務。

請注意，如果您變更此 NTP 伺服器參考，或稍後新增另一個參考，則需要重新啟動服務，以使用新的伺服器。



e. 選擇 OK (確定) 以關閉 NTP Daemon (ntpd) Options (NTP 協助程式 (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。

搭配使用 Storage Gateway 及 VMware 高可用性

VMware 高可用性 (HA) 是一種 vSphere 元件，可提供保護免於支援閘道 VM 之基礎設施層的故障。VMware HA 的做法是使用多個設定為叢集的主機，因此，如果執行閘道 VM 的主機故障，則可以在叢集的另一個主機上自動重新啟動閘道 VM。如需 VMware HA 的詳細資訊，請參VMware HA：概念和最佳實務在 VMware 官方網站上。

若要搭配使用 Storage Gateway 與 VMware HA，建議執行下列事項：

- 部署 VMware ESX.ova只在叢集的一個主機上包含 Storage Gateway 道 VM 的可下載套件。
- 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。
- 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。

同步閘道的 VM 時間

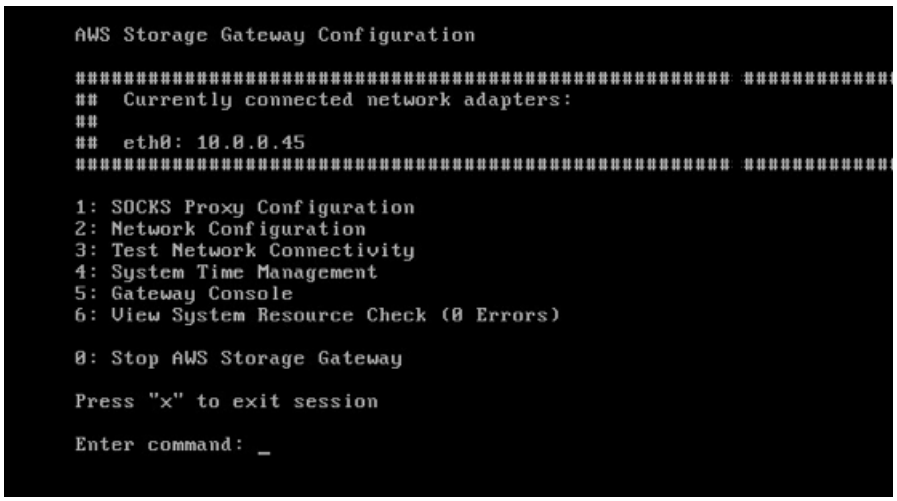
針對部署在 VMware ESXi 上的閘道，設定虛擬化管理程序主機時間並讓 VM 時間與主機同步便足以避免時間產生差異。如需詳細資訊，請參閱 同步 VM 時間與主機時間。針對在 Microsoft Hyper-V 上部署的閘道，建議您使用以下說明的程序定期檢查您 VM 的時間。

檢視並將 Hypervisor 閘道虛擬機器的時間與網路時間協定 (NTP) 伺服器同步

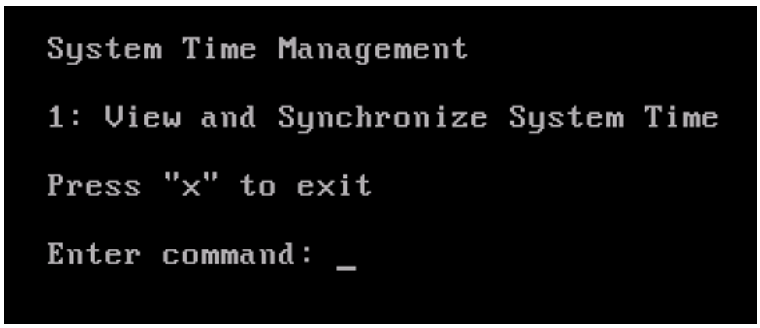
1. 登入您閘道的本機主控台：

   - 如需登入 VMware ESXi 本機主控台的詳細資訊，請參閱使用 VMware ESXi 存取閘道本機主控台。
   - 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 (KVM) 的本機主控台的詳細資訊，請參閱使用 Linux KVM 存取閘道本機主控台。

2. 在Storage Gateway 組態主選單中，輸入**4**為了系統時間管理。



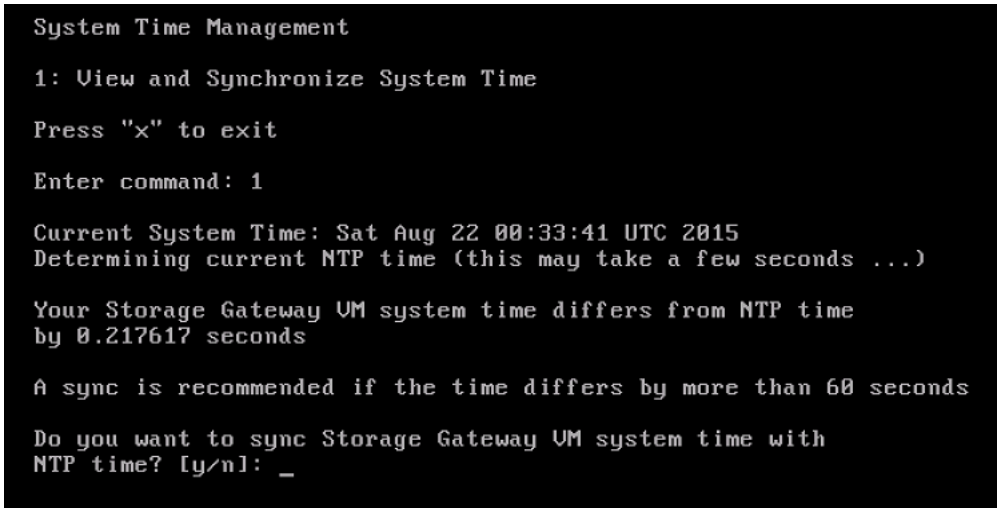
3. 在系統時間管理選單中，輸入**1**為了查看和同步系統時間。



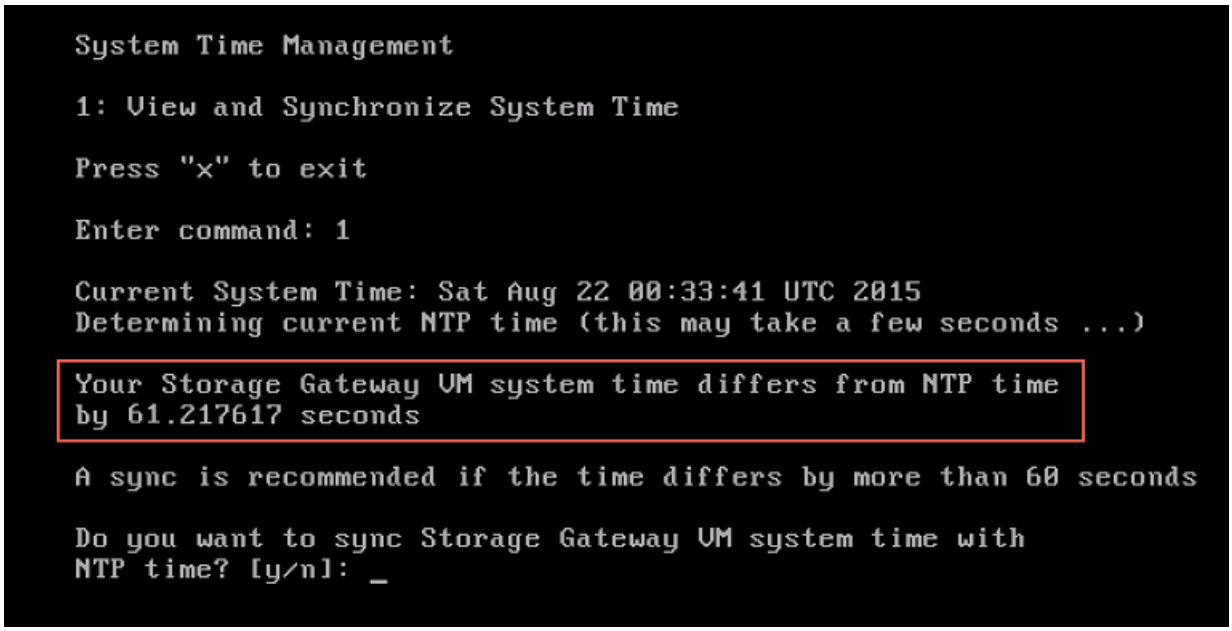
4. 若結果指出您應將您 VM 的時間與 NTP 時間同步，請輸入 **y**。否則，輸入 **n**。

   若您輸入 **y** 以進行同步，同步可能需要一些時間。

   以下螢幕擷取畫面顯示不需要進行時間同步的 VM。



以下螢幕擷取畫面顯示需要進行時間同步的 VM。



在 Amazon EC2 主機上部署檔案閘道

您可在 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體上部署和啟用檔案閘道。檔案閘道 Amazon Machine Image (AMI) 可提供做為社群 AMI。

在 Amazon EC2 執行個體上部署閘道

1. 在 Select host platform (選取託管平台) 頁面上，選擇 Amazon EC2。

2. 選擇 Launch instance (啟動執行個體) 啟動 Storage Gateway EC2 AMI。系統會將您重新導向到 Amazon EC2 主控台，在此可以選擇執行個體類型。
3. 在步驟 2：選擇執行個體類型頁面上，選擇您執行個體的硬體組態。符合特定最低需求的執行個體類型都支援 Storage Gateway。建議您從 m4.xlarge 執行個體類型開始，它符合您閘道正常運作的最低要求。如需詳細資訊，請參閱 現場部署 VM 的硬體需求。

   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「」調整實例大小中的Amazon EC2 Linux 執行個體使用者指南。

   > **Note**
   >
   > 有些執行個體類型，特別是 i3 EC2，會使用 NVMe SSD 磁碟。它們會在您啟動或停止檔案閘道時產生問題；例如，讓您遺失快取的資料。監控`CachePercentDirty`Amazon CloudWatch 指標，而且只在參數為`0`。若要進一步了解閘道的監控指標，請參Storage Gateway 指標與維度在 CloudWatch 文檔中。如需 Amazon EC2 執行個體類型需求的詳細資訊，請參the section called “Amazon EC2 執行個體類型的要求”。
4. 選擇 Next: (下一步：) 設定執行個體詳細資訊。
5. 在步驟 3：設定執行個體詳細資訊頁面中，選擇自動指派公有 IP。如果您的執行個體應從公有網際網路存取，請確認 Auto-assign Public IP (自動指派公有 IP) 設為 Enable (啟用)。如果您的執行個體不應從網際網路存取，請為 Auto-assign Public IP (自動指派公有 IP) 選擇 Disable (停用)。
6. 適用於IAM 角色中，選擇AWS Identity and Access Management(IAM) 角色，您想要為閘道使用。
7. 選擇 Next: (下一步：) 新增儲存。
8. 在步驟 4：新增儲存頁面上，選擇新增新卷將儲存體新增到您的檔案閘道執行個體。您至少需要設定一個 Amazon EBS 磁碟區供快取儲存使用。

   建議的磁盤大小：高速緩存（最小值）150 GiB 和高速緩存（最大值）64 TiB
9. 在步驟 5：新增標籤頁面上，您可將選用標籤新增到您的執行個體。然後選擇 Next (下一步)：設定安全群組。
10. 在步驟 6：設定安全群組頁面上，針對傳送至我們執行個體的特定流量新增防火牆規則。您可以建立新的安全群組，或選擇現有的安全群組。

> **Important**
>
> 除了 Storage Gateway 啟用和 Secure Shell (SSH) 存取端口外，NFS 用户端還需要存取其他連接口。如需詳細資訊，請參閱 網路與防火牆需求。

11. 選擇 Review and Launch (檢閱和啟動) 以檢閱您的組態。
12. 在步驟 7：檢閱執行個體的啟動頁面上，選擇啟動。
13. 在 Select an existing key pair or create a new key pair (選取現有金鑰對或建立新金鑰對) 對話方塊中，選擇 Choose an existing key pair (選擇現有金鑰對)，然後選取您在設定時建立的金鑰對。準備就緒後，請選擇 acknowledgment (確認) 方塊，然後選擇 Launch Instances (啟動執行個體)。

    此時會出現確認頁面，指出您的執行個體正在啟動。
14. 選擇 View Instances (檢視執行個體) 關閉確認頁面並返回主控台。您可以在 Instances (執行個體) 畫面中檢視您的執行個體狀態。啟動執行個體無須費時。當您啟動執行個體時，其初始狀態為 pending (待定)。在執行個體啟動後，其狀態會變更為 running (正在執行)，並收到公有的 DNS 名稱
15. 選擇您的執行個體，記下描述標籤，然後返回連線到AWS頁面，以繼續您的網關設置。

您可以使用 Storage Gateway 主控台或查詢AWS Systems Manager參數儲存。

若要判定 AMI ID

1. 登入AWS Management Console，然後打開 Storage Gateway 控制台https://console.aws.amazon.com/storagegateway/home。
2. 選擇 Create gateway (建立閘道)、選擇 File gateway (檔案閘道)，然後選擇 Next (下一步)。
3. 在 Choose host platform (選擇託管平台) 頁面上，選擇 Amazon EC2。
4. 選擇啟動執行個體啟動 Storage Gateway EC2 AMI。系統會將您重新導向到 EC2 社羣 AMI 頁面，您可以在此查看AWSURL 中的區域。

   或者您可以查詢 Systems Manager 參數存放區。您可以使用AWS CLI或 Storage Gateway API 查詢命名空間下方的 Systems Manager 公用參數`/aws/service/storagegateway/ami/FILE_S3/latest`。例如，使用下列 CLI 命令，返回目前 AMI 的 ID，而AWS區域。

```
aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/
FILE_S3/latest
```

CLI 命令會傳回類似以下的輸出。

```
{
    "Parameter": {
        "Type": "String",
        "LastModifiedDate": 1561054105.083,
        "Version": 4,
        "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/
FILE_S3/latest",
        "Name": "/aws/service/storagegateway/ami/FILE_S3/latest",
        "Value": "ami-123c45dd67d891000"
    }
}
```

取得您閘道的啟用金鑰

若要取得您閘道的啟用金鑰，您必須向閘道 VM 傳送 Web 請求，便會傳回包含啟用金鑰的重新導向。此啟用金鑰會做為其中一項參數傳遞到 ActivateGateway API 動作，指定您閘道的組態。如需詳細資訊，請參閱「」ActivateGateway中的Storage Gateway API 參考。

您對閘道 VM 發送的請求包含AWS激活發生的區域。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*。

主題

- AWS CLI
- Linux (bash/zsh)
- Microsoft Windows PowerShell

AWS CLI

若您尚未執行此作業，您必須安裝及設定 AWS CLI。若要執行此作業，請遵循AWS Command Line Interface 使用者指南中的這些說明：

- 安裝AWS Command Line Interface
- 設定AWS Command Line Interface

以下範例顯示如何使用AWS CLI取得 HTTP 回應，剖析 HTTP 標頭及取得啟用金鑰。

```
wget 'ec2_instance_ip_address/?activationRegion=eu-west-2' 2>&1 | \
grep -i location | \
grep -i key | \
cut -d'=' -f2 |\
cut -d'&' -f1
```

Linux (bash/zsh)

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 "$activation_region" ]]; then
    echo "Usage: get-activation-key ip_address activation_region"
    return 1
  fi
  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region"); then
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
    echo "$activation_key_param" | cut -f2 -d=
  else
    return 1
  fi
}
```

Microsoft Windows PowerShell

下列範例顯示如何使用 Microsoft Windows PowerShell 擷取 HTTP 回應、剖析 HTTP 標頭及取得啟用金鑰的方式。

```
function Get-ActivationKey {
  [CmdletBinding()]
  Param(
```

```
    [parameter(Mandatory=$true)][string]$IpAddress,
    [parameter(Mandatory=$true)][string]$ActivationRegion
  )
  PROCESS {
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion" -MaximumRedirection 0 -ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

使用AWS Direct Connect使用 Storage Gateway

AWS Direct Connect會將您的內部網路連結到 Amazon Web Services vice 雲端。使用AWS Direct Connect，您可以為高輸送量工作負載的需求建立連線，在您的現場部署閘道和AWS。

Storage Gateway 使用公有端點。使用AWS Direct Connect連線，您可以建立公有虛擬界面，允許流量路由至 Storage Gateway 道端點。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 服務公共終端節點可以位於同一AWS區域作為AWS Direct Connect位置，也可以在不同的AWS區域。

下圖顯示了AWS Direct Connect與 Storage Gateway 配合使用。

下列程序假設您已建立正常運作的閘道。

使用AWS Direct Connect使用 Storage Gateway

1. 創建並建立AWS Direct Connect現場部署資料中心與 Storage Gateway 終端節點之間的連線。如需如何建立連線的詳細資訊，請參入門AWS Direct Connect中的AWS Direct Connect使用者指南。
2. Connect 您的本地 Storage Gateway 設備連線到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現場部署路由器。如需詳細資訊，請參閱「」建立虛擬介面中的AWS Direct Connect使用者指南。

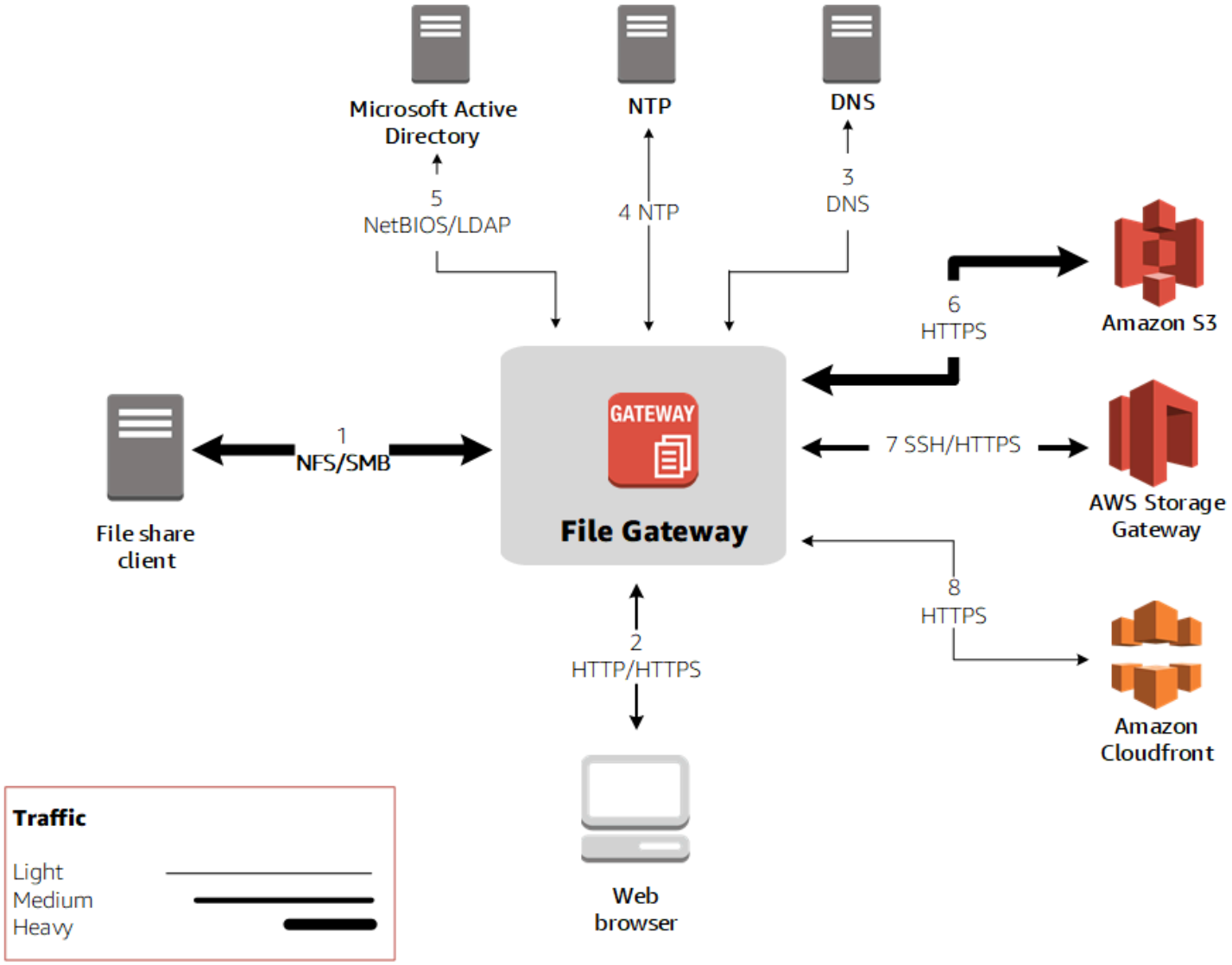
有關詳細資訊AWS Direct Connect，請參什麼是AWS Direct Connect?中的AWS Direct Connect使用者指南。

連接埠需求

Storage Gateway 需要下列連接埠才能進行操作。有些是所有閘道類型常見，也是所有閘道類型均需使用的連接埠。有些則是特定閘道類型需要的連接埠。在本節中，您可以找到所需連接埠的圖例以及每個閘道類型所需連接埠的清單。

檔案閘道

下圖顯示要為檔案閘道操作開啟的連接埠。



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。

從	若要	通訊協定	連接埠	使用方式	
Storage Gateway VM	Amazon Web Services	傳輸控制通訊協定 (TCP)	443 (HTTPS)	用於 Storage Gateway VM 至AWS服務端點。如需服務端點的資訊，請參閱 允許透過防火牆和路由器的 AWS Storage 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。 存放閘道 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。如果您是以儲存閘道管理主控台啟動閘道，則您連線至主控台	

從	若要	通訊協定	連接埠	使用方式	
				的主機必須擁有閘道連接閘道端口 80 的存取權限。	
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	Amazon Web Services	TCP	22 (支援通道)	允許 Amazon Web Services vice Support 存取您的閘道，以協助疑難排解閘道的問題。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	若要	通訊協定	連接埠	使用方式	
Storage Gateway VM	網路時間協定 (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。存放閘道 VM 會設定為使用下列 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	Hypertext Transfer Protocol (HTTP) 代理	TCP	8080 (HTTP)	短暫需要啟用。	

下表列出使用網路檔案系統 (NFS) 或伺服器訊息區塊 (SMB) 通訊協定針對檔案閘道必須開啓的所需連接埠。這些連接埠規則是安全群組定義的一部分。

規則	網路元素	檔案共享類型	通訊協定	連接埠	傳入	傳出	是否為必要？	備註
1	檔案共享用戶端	NFS	TCP/UDP 資料	111	✓	✓	✓	檔案共享資料傳輸 (僅限 NFS)
			TCP/UDP NFS	2049	✓	✓	✓	檔案共享資料傳輸 (僅限 NFS)
			TCP/UDP NFSv3	2004	✓	✓	✓	檔案共享資料傳輸 (僅限 NFS)
		SMB	TCP/UDP SMBv2	139	✓	✓	✓	檔案共享資料傳輸工作階段服務 (僅限 SMB)；針對 Microsoft Windows NT 和更高版本取代連接埠 137 —139
			TCP/UDP SMBv3	445	✓	✓	✓	檔案共享資料傳輸工作階段服務 (僅限 SMB)；針對 Microsoft Windows NT 和更高版本取代連接埠 137 —139
2	Web 瀏覽器	NFS 和 SMB	TCP HTTP	80	✓	✓	✓	Amazon Storage Manage Manage 主控台 (僅啟用)
			TCP HTTPS	443	✓	✓	✓	Amazon Web Services 管理主控台 (所有其他操作)
3	DNS	NFS 和 SMB	TCP/UDP DNS	53	✓	✓	✓	IP 名稱解析

規則	網路元素	檔案共享類型	通訊協定	連接埠	傳入	傳出	是否為必要？	備註
4	NTP	NFS 和 SMB	UDP NTP	123	✓	✓	✓	時間同步服務
5	Microsoft Active Directory	SMB	UDP NetBIOS	137	✓	✓	✓	名稱服務 (不是用於 NFS)
			UDP NetBIOS	138	✓	✓	✓	資料包服務
			TCP LDAP	389	✓	✓		Directory System Agent (DSA)；用戶端連線
			TCP LDAPS	636	✓	✓		LDAP-安全套接字層 (SSL) 上的輕量型目錄存取協定 (LDAP)
6	Amazon S3	NFS 和 SMB	HTTPS 資料	443	✓	✓	✓	儲存資料傳輸
7	Storage Gateway	NFS 和 SMB	TCP SSH	22	✓	✓	✓	支援通道
			TCP HTTPS	443	✓	✓	✓	管理主控台
8	Amazon CloudFront	NFS 和 SMB	TCP HTTPS	443	✓	✓	✓	用於啟用

連線至閘道

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。

針對在現場部署所部署的閘道，您也可以從虛擬化管理程序取得 IP 地址。針對 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 VMware ESXi 存取閘道本機主控台
- 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 KVM 存取閘道本機主控台
- 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，返回 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

若要取得閘道部署所在之 Amazon EC2 執行個體的 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。如需指示，請參閱 。

您也可以從 Amazon EC2 管理主控台取得 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 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格中，選擇 Instances (執行個體)，然後選取您閘道部署所在的 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。返回存放閘道主控台，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 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。

2. 在導覽窗格中，選擇 Instances (執行個體)，然後選取您閘道部署所在的 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。返回 Storage Gateway 主控台，並輸入彈性 IP 地址。
4. 在啟用您的閘道之後，請選擇您剛剛啟用的閘道，然後選擇底部面板中的 VTL devices (VTL 裝置) 標籤。
5. 取得您所有 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
   ```

   您的閘道現在可以使用 EC2 執行個體的彈性 IP 地址予以連線。

了解 Storage Gateway 資源和資源 ID

在 Storage Gateway 中，主要資源是閘道但其他資源類型包括：體積、虛擬磁帶、iSCSI target (iSCSI 目標)，以及VTL 設備。它們稱為子資源，必須與閘道相關聯才能存在。

這些資源和子資源都有獨一無二的 Amazon Resource Name (ARN) 與其相關聯，如下表所示。

資源類型	ARN 格式
閘道 ARN	arn:aws:storagegateway: *region*:*account-id* :gateway/ *gateway-id*
檔案共享 ARN	arn:aws:storagegateway: *region*:*account-id* :share/*share-id*
磁碟區 ARN	arn:aws:storagegateway: *region*:*account-id* :gateway/ *gateway-id* /volume/*volume-id*
磁帶 ARN	arn:aws:storagegateway: *region*:*account-id* :tape/*tapebarcode*
目標 ARN (iSCSI 目標)	arn:aws:storagegateway: *region*:*account-id* :gateway/ *gateway-id* /target/*iSCSItarget*

資源類型	ARN 格式
VTL 裝置 ARN	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`* `/device/`*`vtldevice`*

Storage Gateway 也支援使用 EC2 執行個體以及 EBS 磁碟區和快照。這些資源是 Amazon EC2 資源，用於 Storage Gateway。

使用資源 ID

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 ARN 的一部分。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 資源 ID 為大寫。不過，當您搭配使用這些資源 ID 與 Amazon EC2 API 時，Amazon EC2 預期資源 ID 為小寫。您必須將資源 ID 變更為小寫，才能將它與 EC2 API 搭配使用。例如，在 Storage Gateway 中，磁碟區的 ID 可能是 `vol-1122AABB`。但當您使用此 ID 配合 EC2 API 時，您必須將它變更為 `vol-1122aabb`。否則，EC2 API 可能無法如預期運作。

> **Important**
>
> Storage Gateway 磁碟區的 ID 以及從閘道磁碟區建立的 Amazon EBS 快照 ID 將會變更為較長的格式。從 2016 年 12 月開始，將會使用 17 個字元的字串建立所有新的磁碟區和快照。從 2016 年 4 月開始，您將可以使用這些較長的 ID，讓您可以使用新的格式來測試系統。如需詳細資訊，請參閱較長 EC2 和 EBS 資源 ID。
>
> 例如，使用較長磁碟區 ID 格式的磁碟區 ARN 將如下：`arn:aws:storagegateway:us-west-2:111122223333:gateway/sgw-12A3456B/volume/vol-1122AABBCCDDEEFFG`.
>
> 使用較長 ID 格式的快照 ID 將如下：`snap-78e226633445566ee`。
>
> 如需詳細資訊，請參閱「」公告：更長的 Storage Gateway 磁碟區和快照 ID 將於 2016 年推出。

為儲存體閘道資源加上標籤

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。

針對檔案閘道，您可以使用標籤來控制對資源的存取。如需如何進行該服務的詳細資訊，請參閱使用標籤來控制對您的 Gateway 和資源的存取。

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:`。此字首保留供AWS使用。
- 金鑰屬性的有效字元為 UTF-8 字母和數字、空格及特殊字元 + - = . _ : / 和 @。

處理標籤

您可以使用 Storage Gateway 主控台、Storage Gateway API 或Storage Gateway 命令列界面 (CLI)。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. 打開 Storage Gateway 主控台，位於https://console.aws.amazon.com/storagegateway/home。
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 Gateways (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 Key (金鑰) 輸入金鑰，並針對 Value (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 Create Tag (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 Save (儲存)。

編輯標籤

1. 打開 Storage Gateway 主控台，位於https://console.aws.amazon.com/storagegateway/home。
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 Save (儲存)。

若要刪除標籤

1. 打開 Storage Gateway 主控台，位於https://console.aws.amazon.com/storagegateway/home。
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 Save (儲存)。

另請參閱

使用標籤來控制對您的 Gateway 和資源的存取

使用開源組件AWS Storage Gateway

在本節中，您可以找到有關我們依賴用於交付 Storage Gateway 功能的第三方工具和授權的資訊。

主題

用於 Storage Gateway 的開源組件

多種第三方工具和許可證用於為卷網關、磁帶網關和 Amazon S3 文件網關提供功能。

使用下列鏈接，下載所隨附之特定開放原始碼軟體元件的源碼。AWS Storage Gateway軟體：

- 針對部署至 VMware ESXi 的閘道：sources.tar
- 對於部署至 Microsoft Hyper-V 的閘道：sources_hyperv.tar
- 對於部署在 Linux 核心架構虛擬機器 (KVM) 上的閘道：sources_KVM.tar

此產品包含 OpenSSL Project 所開發以用於 OpenSSL Toolkit 的軟體 (http://www.openssl.org/。如需所有相依第三方工具的相關授權，請參第三方授權。

適用於 Amazon S3 文件網關的開源組件

多種第三方工具和許可證用於提供 Amazon S3 文件網關（S3 文件網關）功能。

使用以下鏈接，下載 S3 File Gateway 軟體所隨附之特定開放原始碼軟體元件的來源碼：

- 對於 Amazon S3 文件網關：SGW 文件-s3 開源 .tgz

此產品包含 OpenSSL Project 所開發以用於 OpenSSL Toolkit 的軟體 (http://www.openssl.org/。如需所有相依第三方工具的相關授權，請參第三方授權。

配額

檔案共享的配額

下表列出檔案共享的配額。

描述	檔案閘道
每個 Amazon S3 儲存貯體的檔案共享數目上限。檔案共享和 S3 儲存貯體間具有一對一的映射。	1
每個閘道的檔案共享數目上限	10
個別檔案的大小上限，即 Amazon S3 中個別物件的大小上限 **Note** 若您寫入的檔案大小超過 5 TB，您會收到 "file too large" (檔案過大) 的錯誤訊息，並且只會上傳檔案的前 5 TB。	5 TB
最大路徑長度 **Note** 不允許用戶端建立超過此長度的路徑，這樣會導致錯誤。此限制適用於檔案閘道支援的兩種通訊協定：NFS 和 SMB。	1024 位元組

建議的網關本地磁盤大小

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	高速緩存（最小值）	高速緩存（最大值）	其他所需本機磁碟
S3 檔案閘道	150 GiB	64 TiB	—

> **Note**
>
> 您可以在最大容量下為快取設定一或多個本機驅動器。
> 新增快取至現有的閘道時，請務必在您的主機 (虛擬化管理程序或 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，請勿變更現有磁碟的大小。

使用儲存體方案

Storage Gateway 道支持 Amazon S3 標準、Amazon S3 標準 — 不經常存取、Amazon S3 單區域不頻繁存取、Amazon S3 智慧型分層和 S3 Glacier 儲存類別。如需儲存體方案的詳細資訊，請參Amazon S3 儲存類別中的Amazon Simple Storage Service 用户指南。

主題

- 將存儲類與文件網關結合使用
- 將 GLACIER 存儲類與文件網關結合使用

將存儲類與文件網關結合使用

當您建立或更新檔案共用時，可以選擇物件的儲存類別。您可以選擇 Amazon S3 標準儲存類別或 S3 標準 — IA、S3 單區域 — IA 或 S3 智慧型分層儲存類別。存放在這些儲存類別中的物件可以使用生命週期政策轉換至 GLACIER

Amazon S3 儲存體方案	考量
標準	選擇 Standard (標準)，透過備援方式在多個可用區域 (不同地理位置) 存放經常存取的檔案。這是默認儲存體方案。如需更多詳細資訊，請參 Amazon S3 定價。
S3 Intelligent-Tiering	選擇 Intelligent-Tiering (智慧型分層)，自動將資料移至最經濟實惠的儲存存取層，以最佳化儲存成本。 存放在 Intelligent-Tiering (智慧型分層) 儲存方案中的物件，可能會因 30 天內覆寫、刪除、請求或轉換物件而產生額外的費用。最少存儲持續

Amazon S3 儲存體方案	考量
	時間為 30 天，在 30 天之前刪除的對象將產生相當於剩餘天數的存儲費用按比例計算的費用。考慮這些物件變更的頻率、計劃保留這些物件的時間長度，以及需要存取這些物件的頻率。小於 128 KB 的物件不符合智慧分層儲存方案中的自動分層資格。這些對象按頻繁訪問層費率收費，並且需支付提前刪除費用。 S3 智能分層現在支持存檔訪問層和深度歸檔訪問層。S3 Intelligent-Tiering 會自動將 90 天未存取過的物件移至存取層，然後在 180 天未存取後移至 Deep Archive 存取層。無論何時還原其中一個存檔訪問層中的對象，該對象都會在幾小時內移動到「頻繁訪問」層，並準備好進行檢索。如果對象僅存在於兩個存檔層中的一個，則這會為嘗試通過文件共享訪問文件的用户或應用程序創建超時錯誤。如果您的應用程序通過文件網關提供的文件共享訪問文件，請勿將存檔層與 S3 智能分層結合使用。 對文件網關管理的文件執行更新元數據的文件操作（如所有者、時間戳、權限和 ACL）時，將刪除現有數據元，並在此 Amazon S3 存儲類中創建新版本的數據元。在生產中使用此存儲類之前，您應先驗證文件操作如何影響對象創建，因為需要支付提前刪除費用。如需更多詳細資訊，請參 Amazon S3 定價。

Amazon S3 儲存體方案	考量
S3 標準 – IA	選擇 Standard-IA (標準 - IA)，將不經常存取的檔案透過備援方式存放在地理位置不同的多個可用區域。 存放在 Standard-IA (標準-IA) 儲存方案中的物件，可能會因覆寫、刪除、請求、檢索或在存儲類別間轉換物件而產生額外的費用。存儲時間最短為 30 天。在 30 天之前刪除的對象將產生相當於剩餘天數的存儲費用按比例計算的費用。考慮這些物件變更的頻率、計劃保留這些物件的時間長度，以及需要存取這些物件的頻率。小於 128 KB 的對象需支付 128 KB 的費用，並收取提前刪除費用。 對文件網關管理的文件執行更新元數據的文件操作（如所有者、時間戳、權限和 ACL）時，將刪除現有數據元，並在此 Amazon S3 存儲類中創建新版本的數據元。在生產中使用此存儲類之前，您應先驗證文件操作如何影響對象創建，因為需要支付提前刪除費用。如需更多詳細資訊，請參 Amazon S3 定價。

Amazon S3 儲存體方案	考量
S3 單區域 – IA	選擇 One Zone IA (One Zone IA)，將不常存取的檔案存放在單一可用區域中。 存放在 One Zone-IA (單區域-IA) 儲存方案中的物件，可能會因 30 天內覆寫、刪除、請求、檢索或轉換物件而產生額外的費用。最少存儲持續時間為 30 天，在 30 天之前刪除的對象將產生相當於剩餘天數的存儲費用按比例計算的費用。考慮這些物件變更的頻率、計劃保留這些物件的時間長度，以及需要存取這些物件的頻率。小於 128 KB 的對象需支付 128 KB 的費用，並收取提前刪除費用。 對文件網關管理的文件執行更新元數據的文件操作（如所有者、時間戳、權限和 ACL）時，將刪除現有數據元，並在此 Amazon S3 存儲類中創建新版本的數據元。在生產中使用此存儲類之前，您應先驗證文件操作如何影響對象創建，因為需要支付提前刪除費用。如需更多詳細資訊，請參 Amazon S3 定價。

雖然您可以直接從檔案共用寫入物件到 S3-Standard-IA、S3-One Zone-IA 或 S3 Intelligent-Tiering 儲存類別，但仍建議您使用生命週期政策來轉換物件，而不是直接從檔案共用寫入，尤其是如果您預期會更新或刪除對象進行存檔後的 30 天內。如需生命週期政策的資訊，請參物件生命週期管理。

將 GLACIER 存儲類與文件網關結合使用

如果您是以 Amazon S3 生命週期政策將檔案轉換至 S3 Glacier，而檔案共用用用戶端可以透過緩存看到檔案，則會在您更新檔案時會看到 I/O 錯誤。我們建議您設定 CloudWatch Event，以在發生 I/O 錯誤時接收通知，然後使用通知來採取動作。例如，您可以採取動作來將存檔物件還原到 Amazon S3。物件還原到 S3 後，您的檔案共用用戶端就能透過檔案共用來存取和更新物件。

如需如何還原存檔物件的詳細資訊，請參還原存檔物件中的Amazon Simple Storage Service 用户指南。

Storage Gateway 的 API 參考

除了使用主控台之外，您可以使用 AWS Storage Gateway API 來以程式設計方式設定及管理您的閘道。本節說明 AWS Storage Gateway 操作、身份驗證的請求簽章，以及錯誤處理。如需 Storage Gateway 可用區域及端點的資訊，請參「」AWS Storage Gateway端點和配額中的AWS一般參考。

> **Note**
>
> 您也可以使用AWS使用 Storage Gateway 開發應用程式時，會使用 SDK。所以此AWS適用於 Java、.NET、PHP 的開發套件都會包裝基礎 Storage Gateway API，簡化您的程式設計任務。如需下載軟體開發套件程式庫的詳細資訊，請參閱範本程式碼程式庫。

主題

AWS Storage Gateway必要請求標頭

本節介紹您必須在每個 POST 請求中傳送到AWS Storage Gateway。您會透過包含 HTTP 標頭，來識別關於請求的關鍵資訊，包含您希望呼叫的操作、請求的日期，以及表示授權您做為請求寄件者的資訊。標頭不區分大小寫，並且標頭的順序也不重要。

以下範例會顯示在 ActivateGateway 操作中使用的標頭。

```
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
```

以下是必須包含在您的 POST 請求中的標頭AWS Storage Gateway。下面顯示的標頭中，以「x-amz」開頭為AWS-特定標頭。所有其他列出的標頭都是 HTTP 交易中使用的常見標頭。

標頭	描述
`Authorization`	授權標頭包含幾段請求的資訊，這些資訊都會啟用AWS Storage Gateway以確定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` 在前述語法中，您指定 YourAccessKey、年、月、日 (yyyymmdd)、region，以及 CalculatedSignature。授權標頭的格式由 AWSV4 簽名過程。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` 作為所有請求的內容類型AWS Storage Gateway。 `Content-Type: application/x-amz-json-1.1`
`Host`	使用主機標頭可指定AWS Storage Gateway終端節點，您可以在其中發送請求。例如：`storagegateway.us-east-2.amazonaws.com` 是美國東部 (俄亥俄) 區域的端點。如需端點的詳細資訊，請參AWS Storage Gateway，請參。AWS Storage Gateway端點和配額中的AWS一般參考。 `Host: storagegateway. region.amazonaws.com`
`x-amz-date`	您必須在 HTTP `Date` 標頭或 AWS `x-amz-date` 標頭提供時間戳記。(有些 HTTP 用戶端程式庫不讓您設定 `Date` 標頭。) 如果`x-amz-date` 標頭存在時，AWS Storage Gateway忽略任何`Date`頭部在請求身份

標頭	描述
	驗證過程中。x-amz-date 格式必須符合 ISO8601 Basic，其格式為 YYYYMMDD'T'HHMMSS'Z'。若同時使用 Date 和 x-amz-date 標頭，則 Date 標頭的格式便不需要是 ISO8601。 `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
x-amz-target	此標頭會指定 API 的版本，以及您請求的操作。目標標頭值是透過串連 API 版本及 API 名稱構成，且其格式如下。 `x-amz-target: StorageGateway_ APIversion .operationName` operationName 值 (例如："ActivateGateway") 可從 API 清單 (Storage Gateway 的 API 參考) 中找到。

簽署請求

Storage Gateway 需要您驗證透過簽署請求傳送的每個請求。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AWSSignature 第 4 版。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 HTTP 請求重新編排為正式格式。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」的計算方式是從私密存取金鑰開始，並使用「登入資料範圍」字串來建立一系列雜湊類型訊息身份驗證碼 (HMAC)。

簽章計算範例

下列範例會逐步解說如何建立 ListGateways 簽章的詳細資訊。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：

- 請求的時間戳記為 "Mon, 10 Sep 2012 00:00:00" GMT。
- 端點為美國東部 (俄亥俄) 區域。

一般請求語法 (包括 JSON 內文) 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。這是因為此 API (或任何 Storage Gateway API) 沒有查詢參數。

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)，則計算的簽章為：

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

最後步驟是建立 Authorization 標頭。對於演示存取金鑰 AKIAIOSFODNN7EXAMPLE，標頭 (為了可讀性而新增換行) 為：AKIAIOSFODNN7EXAMPLE

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120910/us-east-2/
storagegateway/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

錯誤回應

主題

- 異常情形
- 操作錯誤代碼
- 錯誤回應

本節提供 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，若請求簽章發生問題，任意 API 回應會傳回 `InvalidSignatureException` 錯誤異常。但是，操作錯誤代碼 `ActivationKeyInvalid` 僅會由 ActivateGateway API 傳回。

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。

異常情形

下表列出 AWS Storage Gateway API 異常。當 AWS Storage Gateway 操作傳回錯誤回應時，回應內文會包含以下任一項異常。`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	Message	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`	無效的請求動作或操作。	400 錯誤的請求
`InvalidClientTokenId`	X.509 憑證或AWS提供的存取金鑰 ID 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	Message	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存取金鑰及簽章方法。	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	請求必須包含有效 (已註冊)AWS存取金鑰 ID 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。確認您的 JSON 承載格式正確。	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	所以此AWS存取金鑰 ID 需要訂服務。	400 錯誤的請求
ThrottlingException	超過費率。	400 錯誤的請求
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	包含在要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 AWS Storage Gateway 操作錯誤代碼與傳回代碼之 API 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` 和異常情形) 中的其中一種傳回。

操作錯誤代碼	Message	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	Message	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
文件系統關聯終端點配置衝突	現有文件系統關聯端點配置與指定配置衝突。	關聯文件系統
文件系統關聯終端點地址現有使用	指定的終端 IP 地址已在使用中。	關聯文件系統
文件系統關聯終端點地址丟失	缺少文件系統關聯終端節點 IP 地址。	關聯文件系統
未找到文件系統關聯	找不到指定的文件系統關聯。	更新文件系統關聯 解除文件系統的關聯 描述文件系統關聯
未找到文件系統	找不到指定的文件系統。	關聯文件系統

操作錯誤代碼	Message	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	Message	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	Message	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	Message	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	Message	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	Message	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	Message	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	Message	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	Message	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	Message	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	Message	傳回此錯誤代碼的操作
InvalidParameters	指定的請求包含無效的參數。	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	Message	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 LUN 無效。	CreateStorediSCSIVolume
MaximumVolumeCountExceeded	超過磁碟區計數上限。	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes

操作錯誤代碼	Message	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	Message	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	Message	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	Message	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	Message	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	Message	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：

- Content-Type: application/x-amz-json-1.1
- 適當的 4xx 或 5xx HTTP 狀態代碼

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"
        }
```

```
}
```

下表說明在上述語法中顯示的 JSON 錯誤回應欄位。

__type

其中一個來自異常情形的異常。

類型：String

error

包含特定 API 的錯誤詳細資訊。在一般錯誤 (即不限定於任何 API) 中，不會顯示這項錯誤資訊。

類型：收集

errorCode

其中一項操作錯誤代碼 。

類型：String

errorDetails

目前的 API 版本未使用此欄位。

類型：String

message

的其中一項操作錯誤代碼訊息。

類型：String

錯誤回應範例

如果您使用 DescribeStorediSCSIVolumes API 並指定不存在的閘道 ARN 要求輸入，則會傳回下列 JSON 內文。

```
{
  "__type": "InvalidGatewayRequestException",
  "message": "The specified volume was not found.",
  "error": {
    "errorCode": "VolumeNotFound"
  }
```

```
}
```

如果 Storage Gateway 計算出的簽章不符合與請求一同傳送的簽章，便會傳回以下 JSON 內文。

```
{
  "__type": "InvalidSignatureException",
  "message": "The request signature we calculated does not match the signature you
 provided."
}
```

Storage Gateway 中的操作

如需存 Storage Gateway 操作的清單，請參「」動作中的AWS Storage GatewayAPI 參考。

的文件歷程記錄AWSStorage Gateway

- API 版本：2013-06-30
- 最新文件更新時間：2021 年 10 月 12 日

下表說明每個版本的重要變更。AWSStorage Gateway 者指南2018 年 4 月之後。如需有關此文件更新的通知，您可以訂閱 RSS 摘要。

update-history-change	update-history-description	update-history-date
更新閘道建立過程	已更新新閘道的步驟，以反映 Storage Gateway 控制台中的變更。如需詳細資訊，請參閱「」創建和激活 Amazon S3 檔案閘道。	2021 年 10 月 12 日
Support 強制關閉 SMB 文件共享上的文件	您現在可以使用本地組設置來分配網關管理員權限。網關管理員可以使用共享文件夾 Microsoft 管理控制台管理單元強制關閉 SMB 文件共享上打開和鎖定的文件。如需詳細資訊，請參閱「」為您的閘道配置本地組。	2021 年 10 月 12 日
對 NFS 文件共享的審核日誌支持	您現在可以將 NFS 檔案共享配置為生成稽核日誌，提供有關使用者存取檔案共享內的檔案和資料夾的詳細資訊。您可以使用這些日誌來監視用户活動，並在識別不當的活動模式時採取行動。如需詳細資訊，請參閱「」瞭解文件網關審核日誌。	2021 年 10 月 12 日

支持存取點別名	文件網關文件共享現在可以使用存儲桶式接入點別名連接到 Amazon S3 存儲。如需詳細資訊，請參閱「」建立檔案共享。	2021 年 10 月 12 日
VPC 終端節點和接入點支持	文件網關文件共享現在可以通過由AWS PrivateLink。如需詳細資訊，請參閱「」建立檔案共享。	2021 年 7 月 7 日
機會鎖定支援	文件網關文件共享現在可以使用機會鎖定來優化其文件緩衝策略，這在大多數情況下可以提高性能，特別是在 Windows 上下文菜單方面。如需詳細資訊，請參閱「」建立 SMB 檔案共享。	2021 年 7 月 7 日
FedRAMP 合規	Storage Gateway 現在符合 FedRAMP 要求。如需詳細資訊，請參閱「」的合規驗證。	2020 年 11 月 24 日
基於計劃的帶寬限制	Storage Gateway 現在支援磁帶和磁碟區閘道的基於排程的帶寬限制。如需詳細資訊，請參閱「」使用 Storage Gateway 控制台計劃帶寬限制。	2020 年 11 月 9 日
文件網關的文件上傳通知	文件網關現在提供文件上傳通知，當文件網關完全將文件上傳到 Amazon S3 時通知您。如需詳細資訊，請參閱「」獲取文件上傳通知。	2020 年 11 月 9 日

文件網關的基於訪問的枚舉	文件網關現在提供基於訪問的枚舉，它根據共享的 ACL 過濾 SMB 文件共享上的文件和文件夾枚舉。如需詳細資訊，請參閱「」建立 SMB 檔案共享。	2020 年 11 月 9 日
檔案閘道遷移	文件網關現在提供了一個有記錄的過程，用於用新的文件網關替換現有文件網關。如需詳細資訊，請參閱「」用新的文件網關替換文件網關。	2020 年 10 月 30 日
文件網關冷緩存讀取性能提高 4 倍	Storage Gateway 將冷緩存讀取性能提高了 4 倍。如需詳細資訊，請參閱「」檔案閘道的性能指南。	2020 年 8 月 31 日
通過控制台訂購硬件設備	現在，您可以通過AWSStorage Gateway 控制台。如需詳細資訊，請參閱「」使用 Storage Gateway 硬體設備。	2020 年 8 月 12 日
Support 新的聯邦資訊處理標準 (FIPS) 端點AWS區域	您現在可以在美國東部 (奧亥俄)、美國東部 (維吉尼亞北部)、美國西部 (加利佛尼亞北部)、美國西部 (加利佛尼亞北部)、美國西部 (奧勒岡) 和加拿大 (中部) 等區域激活 FIPS 終端節點。如需詳細資訊，請參閱「」AWSStorage Gateway 端點和配額中的AWS一般參考。	2020 年 7 月 31 日

Support 附加到單個 Amazon S3 存儲桶的多個文件共享	文件網關現在支持為單個 S3 存儲桶創建多個文件共享，並根據目錄訪問頻率將文件網關的本地緩存與存儲桶同步。您可以限制管理在文件網關上創建的文件共享所需的存儲桶數。您可以為 S3 存儲桶定義多個 S3 前綴，並將單個 S3 前綴映射到單個網關文件共享。您還可以將網關文件共享名稱定義為獨立於存儲桶名稱，以適應本地文件共享命名約定。如需詳細資訊，請參閱「」建立 NFS 檔案共享或者建立 SMB 檔案共享。	2020 年 7 月 7 日
文件網關本地緩存存儲增加 4 倍	Storage Gateway 現在支持文件網關高達 64 TB 的本地緩存，通過提供對較大工作數據集的低延遲訪問來提高本地應用程序的性能。如需詳細資訊，請參閱「」建議的網關本地磁盤大小中的Storage Gateway 者指南。	2020 年 7 月 7 日
在 Storage Gateway 控制台中查看亞馬遜雲手錶警報	您現在可以在 Storage Gateway 控制台中檢視 CloudWatch 警示。如需詳細資訊，請參閱「」瞭解 CloudWatch 示。	2020 年 5 月 29 日

支援聯邦資訊處理標準 (FIPS) 端點	您現在可以在 AWS GovCloud (US) 區域中啟用具有 FIPS 端點的閘道。若要為檔案閘道選擇 FIPS 端點，請參閱選擇服務端點。若要為磁碟區閘道選擇 FIPS 端點，請參閱選擇服務端點。若要選擇磁帶閘道的 FIPS 端點，請參閱選擇服務端點。	2020 年 5 月 22 日
新的AWS區域	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「」AWSStorage Gateway 端點和配額中的AWS一般參考。	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「」自動最佳化經常存取物件與不常存取物件的儲存體方案中的Amazon Simple Simple Storage Service 用户。	2020 年 4 月 30 日
新的AWSRegion (區域)	現可於使用AWSGovCloud (美國東部) 區域。如需詳細資訊，請參閱「」AWSStorage Gateway 端點和配額中的AWS一般參考。	2020 年 3 月 12 日

支援 Linux 核心型虛擬機器 (KVM) Hypervisor	Storage Gateway 現在能夠讓您在 KVM 虛擬化平台上部署現場部署閘道。在 KVM 上部署的閘道具有與現有內部部署閘道相同的機能和功能。如需詳細資訊，請參閱「」支援的虛擬化管理程序與主機需求中的Storage Gateway 者指南。	2020 年 2 月 4 日
支援 VMware vSphere High Availability	現可在 VMware 上提供高可用性支援，協助防範儲存工作負載出現硬體、虛擬層或網路故障。如需詳細資訊，請參閱「」將 VMware vSphere AvSphere 與 Storage Gateway 搭配使用中的Storage Gateway 者指南。此版本也包含了效能改善。如需詳細資訊，請參閱「」效能中的Storage Gateway 者指南。	2019 年 11 月 20 日
新的AWS 區域對於磁帶閘道	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「」AWSStorage Gateway 端點和配額中的AWS 一般參考。	2019 年 9 月 24 日
Support Amazon CloudWatch Logs 的支援	您現在可以使用 Amazon CloudWatch 日誌組配置檔案閘道，以取得閘道及其資源的錯誤和運作狀態的通知。如需詳細資訊，請參閱「」獲取有關 Amazon CloudWatch 日誌組網關 Health 和錯誤的通知中的Storage Gateway 使用者指南。	2019 年 9 月 4 日

新的AWS 區域	亞太區域 (香港) 區域現在可以使用 Storage Gateway。如需詳細資訊，請參閱「」AWSStorage Gateway 端點和配額中的AWS一般參考。	2019 年 8 月 14 日
新的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「」AWSStorage Gateway 端點和配額中的AWS一般參考。	2019 年 7 月 29 日
支援在虛擬私有雲端 (VPC) 中啟用閘道	您現在可以在 VPC 中啟用閘道。您可以在現場部署軟體設備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 Virtual Private Cloud 中啟用閘道。	2019 年 6 月 20 日
SMB 檔案共享支援 Microsoft Windows ACL	對於檔案閘道，您現在可以使用 Microsoft Windows 存取控制清單 (ACL) 來控制伺服器訊息區塊 (SMB) 檔案共享的存取。如需詳細資訊，請參閱使用 Microsoft Windows ACL 來控制 SMB 檔案共享的存取。	2019 年 5 月 8 日
檔案閘道支援以標籤為基礎的授權	檔案閘道現在支援以標籤為基礎的授權。您可以根據這些資源的標籤來控制對檔案閘道資源的存取。您也可以根據可在 IAM 請求條件中傳遞的標籤來控制存取。如需詳細資訊，請參閱控制對檔案閘道資源的存取。	2019 年 3 月 4 日

歐洲區域的 Storage Gateway 硬體設備	現已在歐洲區域提供。如需詳細資訊，請參閱「」AWSStorage Gateway 硬體設備區域中的AWS一般參考。此外，您現在可以將儲存閘道硬體設備上的可使用儲存體從 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
Support 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上的 Storage Gateway 軟體。您可以從AWS Management Console管理設備。設備可以裝載檔案、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
支援伺服器訊息區塊 (SMB) 通訊協定	檔案閘道新增檔案共享的伺服器訊息區塊 (SMB) 通訊協定支援。如需詳細資訊，請參閱建立檔案共享。	2018 年 6 月 20 日

舊版更新

下表說明每個版本的重要變更。AWSStorage Gateway 者指南2018 年 5 月之前。

變更	描述	變更日期
Support S3 單區域 — IA 儲存類別	您現在可以使用檔案閘道選擇 S3 One Zone Zone IA 作為檔案共享的默認儲存類別。使用此儲存類別，您可	2018 年 4 月 4 日

變更	描述	變更日期
	以將您的物件數據存放在 Amazon S3 的單個可用區域中。如需詳細資訊，請參閱 建立檔案共享。	
新的 AWS 區域	磁帶閘道正式於亞太區域 (新加坡) 區域推出 如需詳細資訊，請參閱 支援的 AWS 區域。	2018 年 4 月 3 日
Amazon S3 儲存貯體的刷新緩存通知、申請者付款和固定 ACL 的 Support 援	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「」RefreshCache.html中的Storage Gateway API 參考。 對於檔案閘道，您現在可以指定申請者或讀者支付訪問費用，而不是儲存貯體擁有者付款。 您現在可以使用檔案閘道啟用將完整控制權授予映射至 NFS 檔案共享的 S3 儲存貯體擁有者。 如需詳細資訊，請參閱 建立檔案共享。	2018 年 3 月 1 日
新的 AWS 區域	現已在歐洲 (巴黎) 區域提供。如需詳細資訊，請參閱 支援的 AWS 區域。	2017 年 12 月 18 日
支援 MIME 類型的檔案上傳通知和猜想	當所有寫入您 NFS 檔案共享的檔案皆已上傳到 Amazon S3 時，檔案閘道現在可讓您收到通知。如需詳細資訊，請參閱「」NotifyWhenUploaded中的Storage Gateway API 參考。 檔案閘道現在可對以副檔名為基礎的上傳物件使用 MIME 類型的猜想。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 虛擬化管理程序 6.5 版	AWSStorage Gateway 現在支援 VMware ESXi 虛擬化管理程序 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

變更	描述	變更日期
檔案閘道支援 Microsoft Hyper-V 虛擬化管理程序	您現在可以將檔案閘道部署在 Microsoft Hyper-V 虛擬化管理程序。如需相關資訊，請參閱 支援的 Hypervisor 與主機需求。	2017 年 6 月 22 日
新的 AWS 區域	亞太區域 (孟買) 區域現在可以使用 Storage Gateway。如需詳細資訊，請參閱 支援的 AWS 區域。	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 參考中的 RefreshCache。	2017 年 3 月 28 日
支援 Amazon EC2 的檔案閘道	AWSStorage Gateway 現在能夠在 Amazon EC2 中部署檔案閘道。您可以使用現可當成社羣 AMI 使用之 Storage Gateway Amazon Machine Image (AMI)，在 Amazon EC2 中啟動檔案閘道。如需如何建立檔案閘道以及在 EC2 執行個體部署它的資訊，請參閱建立和激活 Amazon S3 檔案閘道。如需如何啟動檔案閘道 AMI 的資訊，請參閱 在 Amazon EC2 主機上部署檔案閘道。 此外，檔案閘道現在支援 HTTP 代理組態。如需詳細資訊，請參閱 通過 HTTP 代理路由部署在 EC2 上的網關。	2017 年 2 月 08 日
新的 AWS 區域	現已在歐洲 (倫敦) 區域提供。如需詳細資訊，請參閱 支援的 AWS 區域。	2016 年 12 月 13 日
新的 AWS 區域	加拿大 (中部) 區域現在可以使用 Storage Gateway。如需詳細資訊，請參閱 支援的 AWS 區域。	2016 年 12 月 08 日

變更	描述	變更日期
支援檔案閘道	除卷閘道和磁帶閘道外，Storage Gateway 現在還提供檔案閘道。檔案閘道結合了服務和虛擬軟體設備，讓您使用網路檔案系統 (NFS) 等業界標準的檔案通訊協定，在 Amazon S3 中存放和提取物件。閘道讓您存取 Amazon S3 中的物件，就像存取 NFS 掛載點的檔案。	2016 年 11 月 29 日

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。