



Amazon FSx File Gateway 使用者指南

# AWS Storage Gateway



API 版本 2021-03-31

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# AWS Storage Gateway: Amazon FSx File Gateway 使用者指南

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

# Table of Contents

.....	x
什麼是 Amazon FSx 檔案閘道 .....	1
FSx 檔案閘道的運作方式 .....	1
入門 AWS Storage Gateway .....	3
註冊 Amazon Web Services .....	3
建立具有管理員權限的 IAM 使用者 .....	4
存取 AWS Storage Gateway .....	5
AWS 區域 支援 Storage Gateway .....	5
檔案閘道設定需求 .....	7
先決條件 .....	7
硬體及儲存體需求 .....	7
內部部署 VM 的硬體需求 .....	8
Amazon EC2 執行個體類型的需求 .....	8
儲存需求 .....	9
網路與防火牆需求 .....	9
連接埠需求 .....	10
硬體設備的網路與防火牆需求 .....	20
允許透過防火牆和路由器的閘道存取 .....	23
設定安全群組 .....	24
支援的 Hypervisor 與主機需求 .....	25
檔案閘道支援的 SMB 用戶端 .....	26
支援的檔案系統操作 .....	26
管理本機磁碟 .....	26
決定本機磁碟儲存體的數量 .....	27
新增快取儲存體 .....	27
搭配 EC2 閘道使用暫時性儲存 .....	28
使用硬體設備 .....	30
設定您的硬體設備 .....	31
實際安裝您的硬體設備 .....	32
存取硬體設備主控台 .....	34
設定硬體設備網路參數 .....	35
啟動您的硬體設備 .....	36
在硬體設備上建立閘道 .....	37
在硬體設備上設定閘道 IP 地址 .....	38

從硬體設備移除閘道軟體 .....	40
刪除您的硬體設備 .....	41
建立閘道 .....	43
概觀：閘道啟動 .....	43
設定閘道 .....	43
連線至 AWS .....	43
檢閱並啟用 .....	44
概觀：閘道組態 .....	44
概觀：儲存資源 .....	44
建立 Amazon FSx for Windows File Server 檔案系統 .....	44
建立並啟動 Amazon FSx File Gateway .....	45
設定 Amazon FSx File Gateway .....	45
將您的 Amazon FSx 檔案閘道連線至 AWS .....	46
檢閱設定並啟用 Amazon FSx 檔案閘道 .....	47
設定您的 Amazon FSx File Gateway .....	48
在 VPC 中啟用閘道 .....	50
建立 Storage Gateway 的 VPC 端點 .....	51
設定 Microsoft Active Directory 網域存取設定 .....	52
連接 Amazon FSx 檔案系統 .....	54
掛載和使用您的 Amazon FSx 檔案共享 .....	57
在用戶端上掛載 SMB 檔案共享 .....	57
測試您的 FSx 檔案閘道 .....	58
管理您的 Amazon FSx File Gateway 資源 .....	60
閘道狀態 .....	60
了解檔案系統狀態 .....	61
編輯基本閘道資訊 .....	61
設定閘道安全層級 .....	62
編輯 n FSx 檔案閘道的 Active Directory 設定 .....	63
編輯 Amazon FSx 檔案系統的設定 .....	65
分離 Amazon FSx 檔案系統 .....	66
監控 Storage Gateway .....	67
了解 CloudWatch 警示 .....	67
建立建議的 CloudWatch 警示 .....	69
建立自訂 CloudWatch 警示 .....	69
監控 FSx 檔案閘道 .....	71
取得 FSx File Gateway 運作狀態日誌 .....	71

使用 Amazon CloudWatch 指標 .....	72
了解閘道指標 .....	73
了解檔案系統指標 .....	78
了解 FSx File Gateway 稽核日誌 .....	80
維護您的閘道 .....	85
管理閘道更新 .....	85
更新頻率和預期行為 .....	86
開啟或關閉維護更新 .....	86
修改閘道維護時段排程 .....	87
手動套用更新 .....	88
使用本機主控台執行維護任務 .....	89
存取閘道本機主控台 .....	89
在虛擬機器本機主控台上執行任務 .....	92
在 EC2 本機主控台上執行任務 .....	104
關閉您的閘道 VM .....	110
將現有的 FSx 檔案閘道取代為新的執行個體 .....	110
刪除您的閘道並移除資源 .....	112
使用 Storage Gateway 主控台刪除閘道 .....	112
效能和最佳化 .....	114
FSx File Gateway 的基本效能指引 .....	114
Windows 用戶端上的 FSx File Gateway 效能 .....	115
最佳化閘道效能 .....	115
新增資源至您的閘道 .....	115
新增資源到您的應用程式環境 .....	117
最大化 S3 檔案閘道輸送量 .....	117
在與用戶端相同的位置部署閘道 .....	118
減少因磁碟緩慢所造成的瓶頸 .....	118
調整 CPU、RAM 和快取磁碟的虛擬機器資源配置 .....	119
調整 SMB 安全層級 .....	120
使用多個執行緒和用戶端來平行化寫入操作 .....	121
關閉自動快取重新整理 .....	123
增加 Amazon S3 上傳程式執行緒的數量 .....	123
增加 SMB 逾時設定 .....	124
為相容應用程式開啟機會鎖定 .....	124
根據工作檔案集的大小調整閘道容量 .....	124
為更大的工作負載部署多個閘道 .....	125

最佳化 SQL Server 資料庫備份的 S3 檔案閘道 .....	126
在與 SQL Server 相同的位置部署閘道 .....	126
減少因磁碟緩慢所造成的瓶頸 .....	126
調整 CPU、RAM 和快取磁碟的 S3 檔案閘道虛擬機器資源配置 .....	127
透過調整 S3 檔案閘道的安全層級來改善 SMB 用戶端輸送量 .....	128
將 SQL 備份分割成多個檔案，以改善 SMB 用戶端輸送量 .....	129
增加 SMB 逾時設定，防止大型檔案複製失敗 .....	130
增加 Amazon S3 上傳程式執行緒的數量 .....	130
關閉自動快取重新整理 .....	130
部署多個閘道以支援工作負載 .....	131
資料庫備份工作負載的其他資源 .....	131
安全 .....	132
資料保護 .....	132
資料加密 .....	133
身分與存取管理 .....	134
目標對象 .....	134
使用身分驗證 .....	134
使用政策管理存取權 .....	135
How AWS Storage Gateway 可與 IAM 搭配使用 .....	137
身分型政策範例 .....	141
疑難排解 .....	144
使用標籤來控制對 資源的存取 .....	145
法規遵循驗證 .....	148
恢復能力 .....	148
基礎設施安全性 .....	149
AWS 安全最佳實務 .....	150
日誌記錄和監控 .....	150
CloudTrail 中的 Storage Gateway 資訊 .....	150
了解 Storage Gateway 日誌檔案項目 .....	151
疑難排解 .....	154
故障診斷：閘道離線問題 .....	154
檢查相關聯的防火牆或代理 .....	155
檢查閘道流量的持續 SSL 或深度封包檢查 .....	155
在重新啟動或軟體更新後檢查 IOWaitPercent 指標 .....	155
檢查 Hypervisor 主機上是否有電源中斷或硬體故障 .....	155
檢查相關聯的快取磁碟是否有問題 .....	155

故障診斷：Active Directory 問題 .....	156
透過執行 nping 測試，確認閘道可以到達網域控制站 .....	156
檢查為 Amazon EC2 閘道執行個體的 VPC 設定的 DHCP 選項 .....	157
確認閘道可以透過執行 dig 查詢來解析網域 .....	157
檢查網域控制站設定和角色 .....	158
檢查閘道是否已加入最近的網域控制站 .....	158
確認 Active Directory 在預設組織單位 (OU) 中建立新的電腦物件 .....	159
檢查您的網域控制站事件日誌 .....	159
故障診斷：閘道啟用問題 .....	159
解決使用公有端點啟用閘道時的錯誤 .....	160
解決使用 Amazon VPC 端點啟用閘道時的錯誤 .....	162
解決使用公有端點啟用閘道，且相同 VPC 中有 Storage Gateway VPC 端點時的錯誤 .....	166
故障診斷：內部部署閘道問題 .....	167
開啟 支援 存取權以協助對閘道進行故障診斷 .....	170
故障診斷：Microsoft Hyper-V 設定問題 .....	171
故障診斷：Amazon EC2 閘道問題 .....	173
閘道在一段時間後仍未啟用 .....	173
執行個體清單中找不到 EC2 閘道執行個體 .....	174
使用序列主控台連接到您的 Amazon EC2 閘道 .....	174
開啟 支援 存取權以協助對閘道進行故障診斷 .....	174
故障診斷：硬體設備問題 .....	176
如何確定服務 IP 地址 .....	176
如何執行重設成出廠預設值？ .....	176
如何執行遠端重新啟動 .....	176
如何取得 Dell iDRAC 支援 .....	177
如何找到硬體設備序號 .....	177
如何取得硬體設備支援 .....	177
故障診斷：檔案閘道問題 .....	178
錯誤：FileMissing .....	178
錯誤：FsxFileSystemAuthenticationFailure .....	179
錯誤：FsxFileSystemConnectionFailure .....	179
錯誤：FsxFileSystemFull .....	179
錯誤：GatewayClockOutOfSync .....	179
錯誤：InvalidFileState .....	180
錯誤：ObjectMissing .....	180
錯誤：DroppedNotifications .....	180

通知：HardReboot .....	181
通知：重新啟動 .....	181
故障診斷 Active Directory 網域問題 .....	181
使用 CloudWatch 指標進行故障診斷 .....	183
高可用性運作狀態通知 .....	185
故障診斷：高可用性問題 .....	185
運作狀態通知 .....	185
指標 .....	187
最佳實務 .....	188
復原您的資料 .....	188
從非預期的 VM 關機復原 .....	188
從故障的快取磁碟復原資料 .....	188
從無法存取的資料中心復原資料 .....	189
在 Amazon FSx 上還原資料 .....	189
清除不必要的資源 .....	190
其他資源 .....	191
主機設定 .....	191
部署檔案閘道的預設 Amazon EC2 主機 .....	192
部署適用於 File Gateway 的自訂 Amazon EC2 主機 .....	194
修改 Amazon EC2 執行個體中繼資料選項 .....	197
同步 VM 時間與 Hyper-V 或 Linux KVM 主機時間 .....	197
同步 VM 時間與 VMware 主機時間 .....	198
為您的閘道設定網路轉接器 .....	200
搭配 VMware HA 使用 Storage Gateway .....	202
取得啟用金鑰 .....	205
Linux (curl) .....	206
Linux (bash/zsh) .....	207
Microsoft Windows PowerShell .....	208
使用本機主控台 .....	208
使用 Direct Connect .....	209
Active Directory 許可 .....	209
取得閘道 IP 地址 .....	210
從 Amazon EC2 主機取得 IP 地址 .....	210
了解資源和資源 IDs .....	211
使用資源 ID .....	211
標記您的 資源 .....	212

使用標籤 .....	212
開放原始碼元件 .....	213
Storage Gateway 的開放原始碼元件 .....	214
Amazon FSx 檔案閘道的開放原始碼元件 .....	214
配額 .....	214
Amazon FSx 檔案系統的配額 .....	214
適用於您閘道的建議本機磁碟大小 .....	215
API 參考 .....	216
必要請求標頭 .....	216
簽署請求 .....	218
簽章計算範例 .....	219
錯誤回應 .....	220
例外狀況 .....	221
操作錯誤代碼 .....	223
錯誤回應 .....	242
動作 .....	244
文件歷史紀錄 .....	245
舊版更新 .....	252

Amazon FSx File Gateway 不再提供給新客戶。FSx File Gateway 的現有客戶可以繼續正常使用服務。如需類似 FSx File Gateway 的功能，請造訪[此部落格文章](#)。

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。

# 什麼是 Amazon FSx 檔案閘道

Amazon FSx File Gateway (FSx File Gateway) 是一種新的檔案閘道類型，可讓您從內部部署設施存取雲端 FSx for Windows File Server 檔案共用時，享有低延遲和高效率的存取。如果您因為延遲或頻寬需求而維護內部部署檔案儲存，您可以改為使用 FSx File Gateway，無縫存取 FSx for Windows File Server 在 AWS Cloud 中提供的全受管、高度可靠且幾乎無限制的 Windows 檔案共用。

使用 Amazon FSx File Gateway 的優勢

FSx File Gateway 提供下列優點：

- 有助於消除內部部署檔案伺服器，並將所有資料合併到 AWS 中，以利用雲端儲存的規模和經濟效益。
- 提供可用於所有檔案工作負載的選項，包括需要現場部署雲端資料存取權的選項。
- 需要留在內部部署的應用程式現在可以體驗到與其中相同的低延遲和高效能 AWS，而不會對您的網路課稅或影響最嚴苛的應用程式所經歷的延遲。

## Amazon FSx 檔案閘道的運作方式

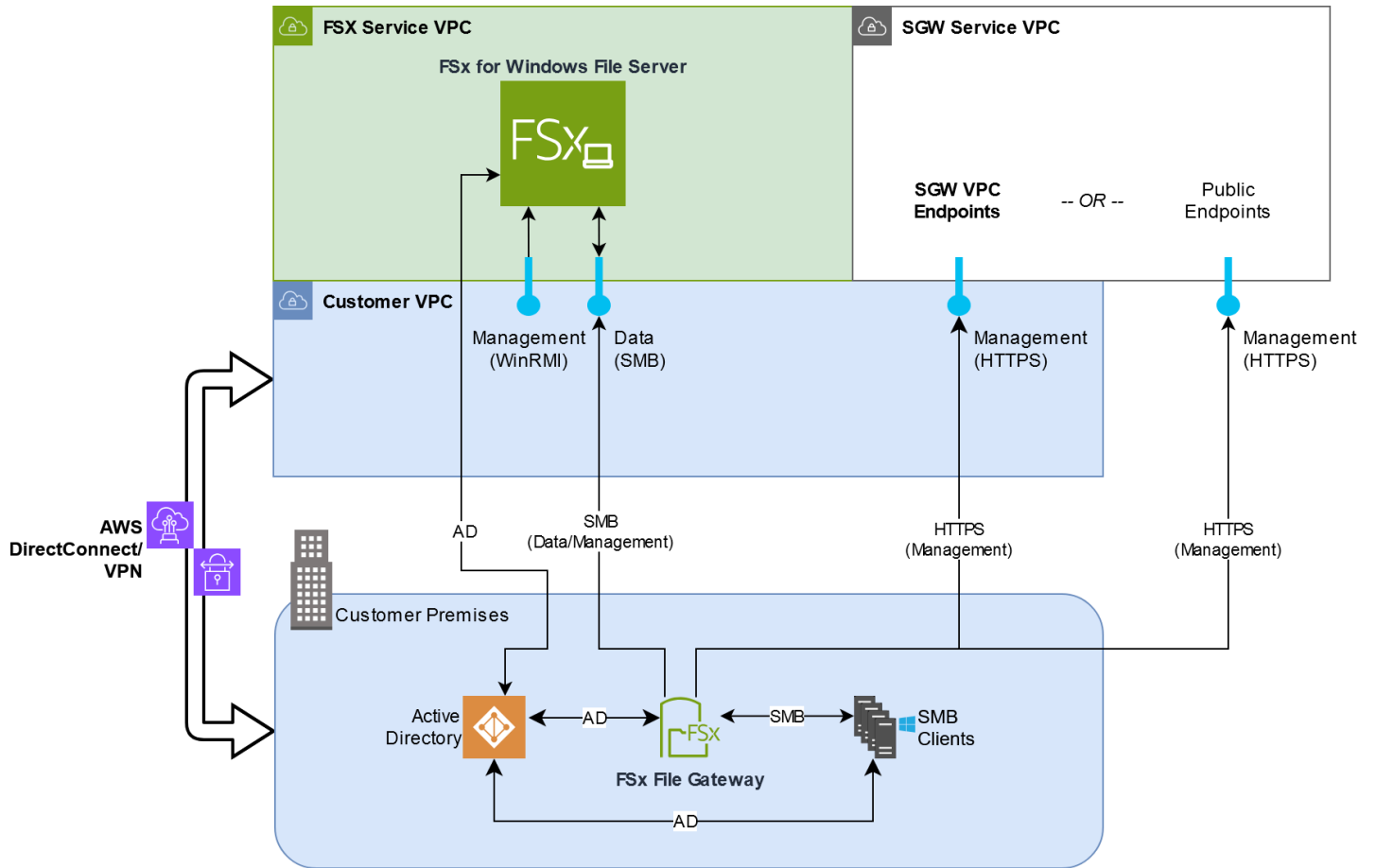
若要使用 Amazon FSx File Gateway (FSx File Gateway)，您必須至少有一個 Amazon FSx for Windows File Server 檔案系統。您也必須透過 VPN 或 Direct Connect 連線，擁有 FSx for Windows File Server 的內部部署存取權。如需使用 Amazon FSx 檔案系統的詳細資訊，請參閱[什麼是 Amazon FSx for Windows File Server ?](#)

您可以將閘道部署到內部部署環境，做為在 VMware ESXi、Microsoft Hyper-V 或 Linux 核心型虛擬機器 (KVM) 上執行的虛擬機器 (VM)，或是您從偏好的經銷商訂購的硬體設備。您也可以在 VMware Cloud on 中部署 Storage Gateway VM AWS，或在 Amazon EC2 中部署為 AMI。部署設備之後，您可以從 Storage Gateway 主控台或透過 Storage Gateway API 啟用 FSx 檔案閘道。

啟用 Amazon FSx File Gateway 並可存取 FSx for Windows File Server 之後，請使用 Storage Gateway 主控台將其加入您的 Microsoft Active Directory 網域。閘道成功加入網域後，您可以使用 Storage Gateway 主控台將閘道連接至現有的 FSx for Windows File Server。FSx for Windows File Server 可讓伺服器上的所有共用成為 Amazon FSx 檔案閘道上的共用。然後，您可以使用用戶端瀏覽並連線至 FSx File Gateway 上對應至所選 FSx File Gateway 的檔案共用。

連接檔案共享時，您可以在本機讀取和寫入檔案，同時受益於 FSx for Windows File Server 上提供的所有功能。FSx File Gateway 會將本機檔案共用及其內容映射至遠端存放在 FSx for Windows File Server 中的檔案共用。遠端檔案和本機可見檔案及其共用之間有 1 : 1 的通訊。

下圖提供 Storage Gateway 的檔案儲存部署概觀。



請注意下圖中的以下內容：

- Direct Connect 或 VPN，以允許 FSx 檔案閘道使用 SMB 存取 Amazon FSx 檔案共享，並允許 FSx for Windows File Server 加入您的內部部署 Active Directory 網域。
- 需要 Amazon Virtual Private Cloud (Amazon VPC) 才能使用私有端點連線至 FSx for Windows File Server 服務 VPC 和 Storage Gateway 服務 VPC。FSx 檔案閘道也可以連接到公有端點。

# 入門 AWS Storage Gateway

本節提供開始使用的指示 AWS。您需要有 AWS 帳戶才能開始使用 AWS Storage Gateway。您可以使用現有的 AWS 帳戶，或註冊新帳戶。您也需要 AWS 帳戶中屬於群組的 IAM 使用者，具有執行 Storage Gateway 任務所需的管理許可。具有適當權限的使用者可以存取 Storage Gateway 主控台和 Storage Gateway API，以執行閘道部署、組態和維護任務。如果您是第一次使用，建議您先檢閱[支援的 AWS 區域](#)和[檔案閘道設定需求](#)區段，再使用 Storage Gateway。

本節包含下列主題，提供有關 入門的其他資訊 AWS Storage Gateway：

## 主題

- [註冊 Amazon Web Services](#) - 了解如何註冊 AWS 和建立 AWS 帳戶。
- [建立具有管理員權限的 IAM 使用者](#) - 了解如何為您的帳戶 AWS 建立具有管理權限的 IAM 使用者。
- [存取 AWS Storage Gateway](#) - 了解如何 AWS Storage Gateway 透過 Storage Gateway 主控台或以程式設計方式使用 AWS SDKs 存取。
- [AWS 區域 支援 Storage Gateway](#) - 了解在 Storage Gateway 中啟用閘道時，您可以使用哪些 AWS 區域來存放資料。

## 註冊 Amazon Web Services

AWS 帳戶是存取 AWS 服務的基本需求。您的 AWS 帳戶是您以使用者身分 AWS 建立之所有 AWS 資源的基本容器。您的 AWS 帳戶也是 AWS 資源的基本安全界限。您在帳戶中建立的任何資源都可供擁有帳戶登入資料的使用者使用。您必須先註冊 AWS Storage Gateway，才能開始使用 AWS 帳戶。

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

### 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或簡訊，並在電話鍵盤輸入驗證碼。

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

我們也建議您要求使用者在存取時使用暫時登入資料 AWS。若要提供臨時登入資料，您可以使用聯合身分和身分提供者，例如 AWS IAM Identity Center。如果您的公司已經使用身分提供者，您可以搭配聯合使用它，以簡化您提供 AWS 帳戶中資源存取權的方式。

## 建立具有管理員權限的 IAM 使用者

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

若要建立管理員使用者，請選擇下列其中一個選項。

選擇一種管理管理員的方式	到	根據	您也可以
在 IAM Identity Center (建議)	使用短期憑證存取 AWS。 這與安全性最佳實務一致。有關最佳實務的資訊，請參閱 IAM 使用者指南中的 <a href="#">IAM 安全最佳實務</a> 。	請遵循 AWS IAM Identity Center 使用者指南的 <a href="#">入門</a> 中的說明。	在 AWS Command Line Interface 使用者指南中設定 <a href="#">AWS CLI 以使用來設定 AWS IAM Identity Center</a> 程式設計存取。
在 IAM 中 (不建議使用)	使用長期憑證存取 AWS。	請遵循《IAM 使用者指南》中 <a href="#">建立 IAM 使用者以進行緊急存取</a> 的指示。	請依照《IAM 使用者指南》中的 <a href="#">管理 IAM 使用者的存取金鑰</a> 設定以程式設計方式存取。

### Warning

IAM 使用者具有存在安全風險的長期登入資料。為了協助降低此風險，建議您只為這些使用者提供執行任務所需的許可，並在不再需要這些使用者時將其移除。

## 存取 AWS Storage Gateway

您可以使用 [AWS Storage Gateway 主控台](#) 來執行各種閘道組態和維護任務，包括從部署中啟用或停用 Storage Gateway 硬體設備、建立、管理和刪除不同類型的閘道、連接、管理和檔案檔案系統，以及監控 Storage Gateway 服務各種元素的運作狀態和狀態。為了簡單易用，本指南著重於使用 Storage Gateway 主控台 Web 介面執行任務。您可以透過網頁瀏覽器存取 Storage Gateway 主控台，網址為：<https://console.aws.amazon.com/storagegateway/home/>。

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

您也可以使用 AWS SDKs 來開發與 Storage Gateway 互動的應用程式。適用於 Java、.NET 和 PHP 的 AWS SDK 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 程式庫的資訊，請參閱 [AWS 開發人員中心](#)。

如需定價的詳細資訊，請參閱 [AWS Storage Gateway 定價](#)。

## AWS 區域 支援 Storage Gateway

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

Amazon FSx File Gateway 會將檔案資料存放在 Amazon FSx 檔案系統所在的 AWS 區域中。開始部署閘道之前，請選擇 Storage Gateway 主控台右上角的區域。

- Amazon FSx 檔案閘道 — 如需可搭配 Amazon FSx 檔案閘道使用的支援 AWS 區域和服務 AWS 端點清單，請參閱 中的 [Amazon FSx 檔案閘道端點和配額](#) AWS 一般參考。
- Storage Gateway — 如需可搭配 Storage Gateway 使用的支援 AWS 區域和服務 AWS 端點清單，請參閱 中的 [AWS Storage Gateway 端點和配額](#) AWS 一般參考。

- Storage Gateway 硬體設備 — 如需可與硬體設備搭配使用的支援區域，請參閱《》中的 [AWS Storage Gateway 硬體設備區域](#) AWS 一般參考。

# 檔案閘道設定需求

除非另有說明，否則以下要求適用於所有 檔案閘道類型 AWS Storage Gateway。您的設定必須符合本節的要求。在部署閘道之前，請先檢閱適用於閘道設定的需求。

## 主題

- [先決條件](#)
- [硬體及儲存體需求](#)
- [網路與防火牆需求](#)
- [支援的 Hypervisor 與主機需求](#)
- [檔案閘道支援的 SMB 用戶端](#)
- [檔案閘道支援的檔案系統操作](#)
- [管理閘道的本機磁碟](#)

## 先決條件

設定 Amazon FSx 檔案閘道 (FSx 檔案閘道) 之前，您必須符合下列先決條件：

- 建立和設定 FSx for Windows File Server 檔案系統。如需說明，請參閱《[Amazon FSx for Windows File Server 使用者指南](#)》中的 [步驟 1：建立您的檔案系統](#)。FSx
- 設定 Microsoft Active Directory (AD) 並建立具備必要許可的 Active Directory 服務帳戶。如需詳細資訊，請參閱 [Active Directory 服務帳戶許可要求](#)。
- 確保閘道和 之間有足夠的網路頻寬 AWS。成功下載、啟用和更新閘道至少需要 100 Mbps。
- 設定您要用於部署閘道之內部部署環境 AWS 與 之間網路流量的連線。您可以使用公有網際網路、私有聯網、VPN 或 進行連線 Direct Connect。如果您希望閘道 AWS 透過私有連線與 Amazon Virtual Private Cloud 通訊，請在設定閘道之前設定 Amazon VPC。
- 確保您的閘道可以解析 Active Directory 網域控制站的名稱。您可以在 Active Directory 網域中使用 DHCP 來處理解析度，或從閘道本機主控台的網路組態設定選單手動指定 DNS 伺服器。

## 硬體及儲存體需求

下列各節提供有關閘道所需的硬體和儲存組態下限，以及為所需儲存配置的磁碟空間下限的資訊。

## 內部部署 VM 的硬體需求

在內部部署閘道時，請確定您部署閘道虛擬機器 (VM) 的基礎硬體可以專用於下列最低資源：

- 指派給 VM 的四個虛擬處理器
- 16 GiB 保留 RAM，適用於檔案閘道
- 80 GiB 的磁碟空間，用於安裝 VM 映像和系統資料

## Amazon EC2 執行個體類型的需求

在 Amazon Elastic Compute Cloud (Amazon EC2) 上部署閘道時，執行個體大小必須至少 **xlarge** 為，閘道才能運作。不過，對於運算最佳化執行個體系列，大小必須至少為 **2xlarge**。

### Note

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

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。

### 建議用於檔案閘道類型

- 一般用途執行個體系列 – m5、m6 或 m7 執行個體類型。選擇 xlarge 執行個體大小或更高，以符合 Storage Gateway 處理器和 RAM 需求。
- 運算最佳化執行個體系列 – c5、c6 或 c7 執行個體類型。選擇 2xlarge 或更高的執行個體大小，以符合 Storage Gateway 處理器和 RAM 需求。
- 記憶體最佳化執行個體系列 – r5、r6 或 r7 執行個體類型。選擇 xlarge 執行個體大小或更高，以符合 Storage Gateway 處理器和 RAM 需求。
- 儲存體最佳化執行個體系列 – i3、i4 或 i7 執行個體類型。選擇 xlarge 執行個體大小或更高，以符合 Storage Gateway 處理器和 RAM 需求。

### Note

當您在 Amazon EC2 中啟動閘道，且您選擇的執行個體類型支援暫時性儲存時，系統會自動列出磁碟。如需 Amazon EC2 執行個體儲存體的詳細資訊，請參閱《Amazon EC2 使用者指南》中的 [執行個體儲存體](#)。Amazon EC2

## 儲存需求

除了 VM 的 80 GiB 磁碟空間之外，您的閘道還需要額外的磁碟。

閘道類型	快取 (最低)	快取 (最大值)			
File Gateway :	150 GiB	64 TiB			

### Note

您可以為快取設定一或多個本機磁碟機，最大容量為。將快取新增至現有閘道時，請務必在主機 (Hypervisor 或 Amazon EC2 執行個體) 中建立新的磁碟。如果磁碟先前已配置為快取，請勿變更現有磁碟的大小。

## 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。

網路頻寬要求會根據閘道上傳及下載的資料數量而有所不同。至少需要 100Mbps 才能成功下載、啟用和更新閘道。您的資料傳輸模式將決定支援工作負載所需的頻寬。

您可以在以下內容找到必要連接埠及如何允許透過防火牆及路由器進行存取的相關資訊。

### Note

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

## 主題

- [連接埠需求](#)

- [Storage Gateway 硬體設備的網路與防火牆要求](#)
- [允許透過防火牆和路由器 AWS Storage Gateway 存取](#)
- [設定 Amazon EC2 閘道執行個體的安全群組](#)

## 連接埠需求

FSx File Gateway 需要透過網路安全允許特定連接埠，才能成功部署和操作。所有閘道都需要某些連接埠，而其他連接埠只需要特定組態，例如連線至 VPC 端點時。

對於 FSx 檔案閘道，您必須使用 Microsoft Active Directory 來允許網域使用者存取伺服器訊息區塊 (SMB) 檔案共享。您可以將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 Directory Service 在 Amazon Web Services Cloud [AWS Managed Microsoft AD](#) 中建立。對於大多數 AWS Managed Microsoft AD 部署，您需要為 VPC 設定動態主機組態協定 (DHCP) 服務。如需有關建立 DHCP 選項集的資訊，請參閱《AWS Directory Service 管理指南》中的[建立 DHCP 選項集](#)。

下表列出必要的連接埠，並說明備註欄中的條件需求。


### FSx File Gateway 的連接埠需求

網路元素	從	到	通訊協定	站點	傳入	傳出	必要	備註
Web 瀏覽器	您的 Web 瀏覽器	Storage Gateway VM	TCP HTTP	80	✓	✓	✓	供本機系統用來取得 Storage Gateway 啟用金鑰。只有在啟用 Storage Gateway 裝置時，才

網路元素	從	到	通訊協定	站點	傳入	傳出	必要	備註
								會使用連接埠 80。Storage Gateway VM 不需要讓連接埠 80 可公開存取。連接埠 80 所需的存取權限級別取決於您的網路設定。如果您從 Storage Gateway 管理主控台啟用閘道，您連線至主控台的主機必須能夠存取閘道的連

網路元素	從	到	通訊協定	站點	傳入	傳出	必要	備註
								埠 80。
Web 瀏覽器	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓	AWS 管理主控台 ( 所有其他操作 )
DNS	Storage Gateway VM	網域名稱服務 (DNS) 伺服器	TCP 和 UDP DNS	53	✓	✓	✓	用於 Storage Gateway VM 與 DNS 伺服器之間的通訊，以進行 IP 名稱解析。

網路元素	從	到	通訊協定	站點	傳入	傳出	必要	備註
NTP	Storage Gateway VM	網路時間協定 (NTP) 伺服器	TCP 和 UDP NTP	123	✓	✓	✓	<p>內部部署系統用來將 VM 時間與主機時間同步。</p> <p>Storage Gateway VM 會設定為使用下列 NTP 伺服器：</p> <ul style="list-style-type: none"> <li>• 0.amazon.pool.ntp.org</li> <li>• 1.amazon.pool.ntp.org</li> <li>• 2.amazon.pool.ntp.org</li> <li>• 3.amazon.pool.ntp.org</li> </ul>

 Note  
Amazon EC2

網路元素	從	到	通訊協定	站點	傳入	傳出	必要	備註
								上託管的閘道不需要。

網路元素	從	到	通訊協定	站點	傳入	傳出	必要	備註
Storage Gateway	Storage Gateway VM	支援端點	TCP SSH	22	✓	✓	✓	允許支援存取您的閘道，以協助您疑難排解閘道問題。不需要將此埠開放給閘道的正常操作使用，但進行疑難排解時需要用到。如需支援端點的清單，請參閱 <a href="#">支援端點</a> 。
Storage Gateway	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓	管理主控台
Amazon CloudFront	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓	用於啟用

網路元素	從	到	通訊協定	站點	傳入	傳出	必要	備註
VPC	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓*	管理主控台  *只有在使用 VPC 端點時才需要
VPC	Storage Gateway VM	AWS	TCP HTTPS	1026		✓	✓*	控制平面端點  *只有在使用 VPC 端點時才需要
VPC	Storage Gateway VM	AWS	TCP HTTPS	1027		✓	✓*	Anon 控制平面 (用於啟用)  *只有在使用 VPC 端點時才需要

網路元素	從	到	通訊協定	站點	傳入	傳出	必要	備註
VPC	Storage Gateway VM	AWS	TCP HTTPS	1028		✓	✓*	Proxy 端點  *只有在 在使用 VPC 端 點時才 需要
VPC	Storage Gateway VM	AWS	TCP HTTPS	1031		✓	✓*	資料平 面  *只有 在使用 VPC 端 點時才 需要
VPC	Storage Gateway VM	AWS	TCP HTTPS	2222		✓	✓*	VPCe 的 SSH 支援管 道  *僅在使 用 VPC 端點時 開啟支 援管道 時才需 要

網路元素	從	到	通訊協定	站點	傳入	傳出	必要	備註
VPC	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓*	管理主控台  *只有在使用 VPC 端點時才需要
檔案共享用戶端	SMB 用戶端	Storage Gateway VM	TCP 或 UDP SMBv3	445	✓	✓	✓	檔案共用資料傳輸工作階段服務。  取代 Microsoft Windows NT 和更新版本的連接埠 137–139。
Microsoft Active Directory	Storage Gateway VM	Active Directory 伺服器	UDP NetBIOS	137	✓	✓	✓	名稱服務
Microsoft Active Directory	Storage Gateway VM	Active Directory 伺服器	UDP NetBIOS	138	✓	✓	✓	資料包服務

網路元素	從	到	通訊協定	站點	傳入	傳出	必要	備註
Microsoft Active Directory	Storage Gateway VM	Active Directory 伺服器	TCP 和 UDP LDAP	389	✓	✓	✓	Directory System Agent (DSA) 用戶端連線
Microsoft Active Directory	Storage Gateway VM	Active Directory 伺服器	TCP 和 UDP Kerberos	88	✓	✓	✓	Kerberos
Microsoft Active Directory	Storage Gateway VM	Active Directory 伺服器	TCP 分散式運算環境/端點映射器 (DCE/EMAP)	135	✓	✓	✓	RPC
Microsoft Active Directory	Storage Gateway VM	Active Directory 伺服器	TCP 分散式運算環境/端點映射器 (DCE/EMAP)	49152-65535	✓	✓	✓	RPC 或者，如果您的 AD 網域控制器使用專用 RPC 連接埠，請改為開啟這些連接埠。

網路元素	從	到	通訊協定	站點	傳入	傳出	必要	備註
Amazon FSx 連線	Storage Gateway VM	FSx for Windows File Server	TCP 或 UDP SMBv3	445	✓	✓	✓	檔案共用資料傳輸工作階段服務

## Storage Gateway 硬體設備的網路與防火牆要求

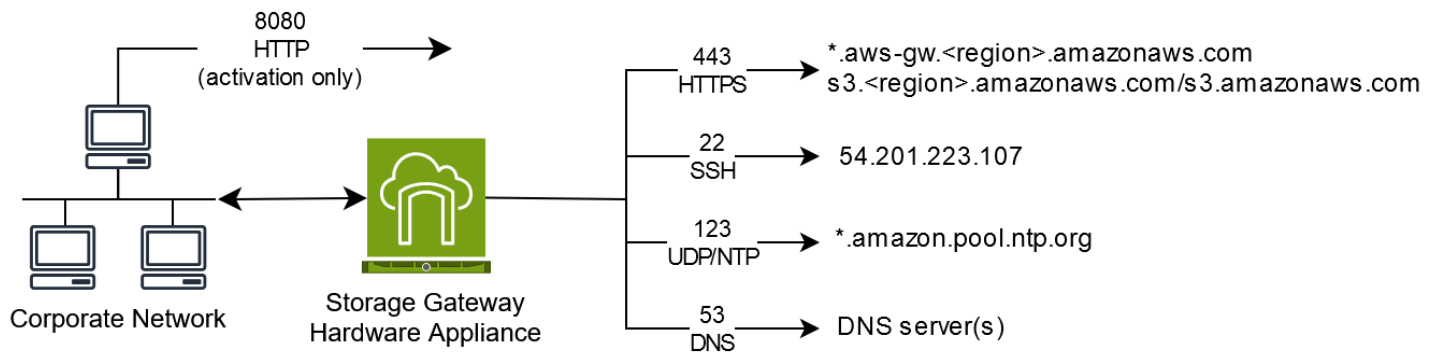
每個 Storage Gateway 硬體設備都需要下列網路服務：

- 網際網路存取：透過任何伺服器上的網路介面，全年無休的連線到網際網路。
- DNS 服務：用於在硬體設備和 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	站點	Direction	來源	目標	Usage
SSH	22	傳出	硬體設備	54.201.223.107	支援通道
DNS	53	傳出	硬體設備	DNS 伺服器	名稱解析
UDP/NTP	123	傳出	硬體設備	*.amazon.pool.ntp.org	時間同步
HTTPS	443	傳出	硬體設備	*.amazonaws.com	資料傳輸
HTTP	8080	傳入	AWS	硬體設備	啟用 (只需短暫時間)

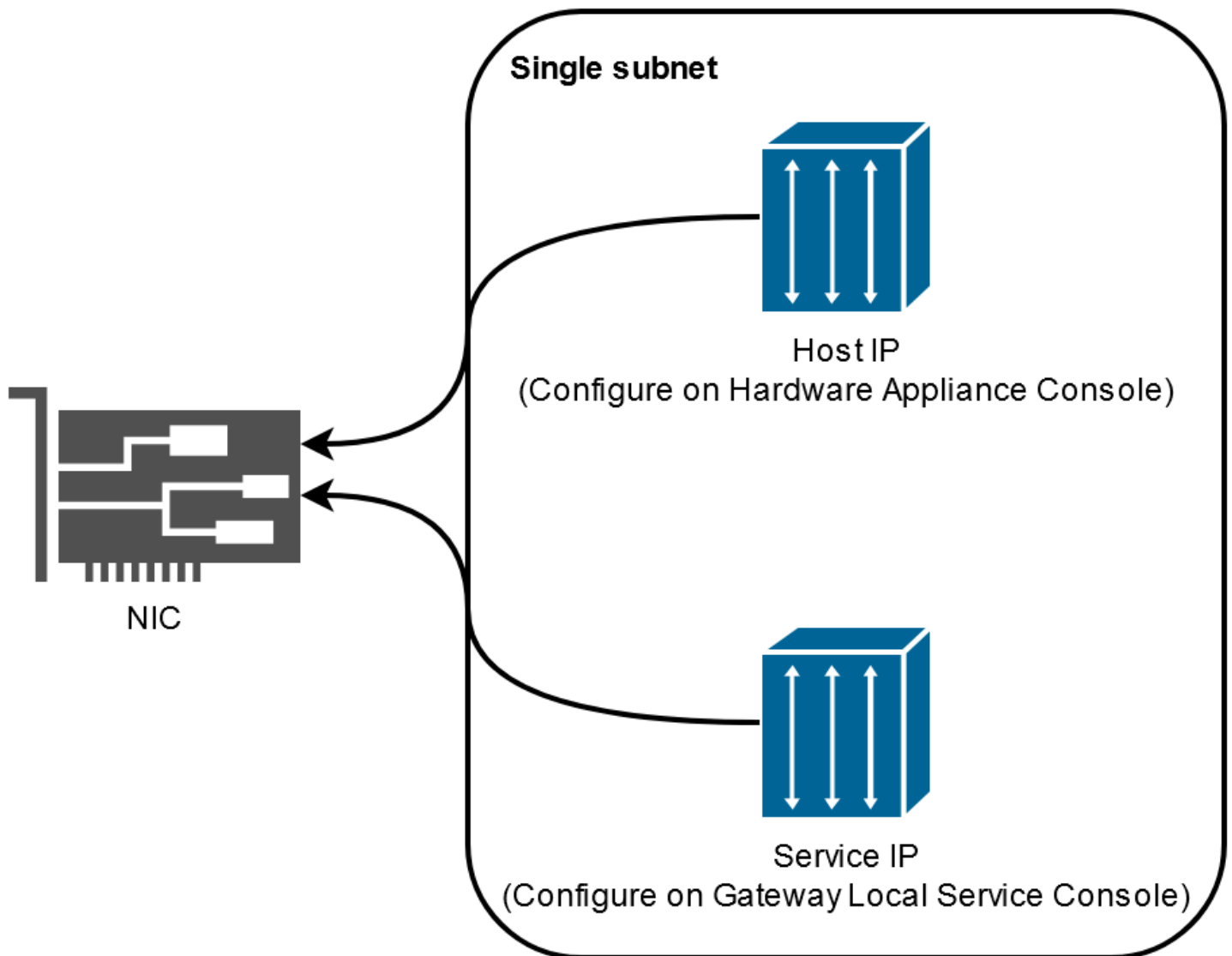
若要依設計方式執行，硬體設備需要如下所示的網路和防火牆設定：

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

**Note**

如需顯示伺服器後端及其連接埠的圖例，請參閱 [實際安裝您的硬體設備](#)。

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，請參閱 [使用 AWS Storage Gateway 硬體設備](#)。

## 允許透過防火牆和路由器 AWS Storage Gateway 存取

您的閘道需要存取下列 Storage Gateway 服務端點才能與之通訊 AWS。在閘道設定期間，根據您的網路環境選取閘道的端點類型。若您使用防火牆或路由器來篩選或限制網路流量，則必須設定防火牆和路由器，以允許這些服務端點可與 AWS 進行傳出通訊。

### Note

如果您將 Storage Gateway 的私有 VPC 端點設定為用於往返連線和資料傳輸 AWS，則閘道不需要存取公有網際網路。如需詳細資訊，請參閱[在虛擬私有雲端中啟用閘道](#)。

### Important

將下列端點範例中###取代為閘道的正確 AWS 區域字串，例如 us-west-2。

將 *amzn-s3-demo-bucket* 取代為部署中 Amazon S3 儲存貯體的實際名稱。您也可以使用星號 (\*) 取代 *amzn-s3-demo-bucket*，在防火牆規則中建立萬用字元項目，這會允許列出所有儲存貯體名稱的服務端點。

如果您的閘道部署 AWS 區域在美國或加拿大的中，且需要符合聯邦資訊處理標準 (FIPS) 的端點連線，請將 *s3* 取代為 *s3-fips*。

## 端點類型

### 標準端點

這些端點支援閘道設備與之間的 IPv4 流量 AWS。

所有閘道都需要下列服務端點，才能進行頭部儲存貯體的操作。

```
bucket-name.s3.region.amazonaws.com:443
```

控制路徑 (anon-cp、client-cp、proxy-app) 和資料路徑 (dp-1) 操作的所有閘道都需要下列服務端點。

```
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) 中的閘道服務端點。

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

除了 Storage Gateway 和 Amazon S3 服務端點之外，Storage Gateway VMs 還需要網路存取下列 NTP 伺服器：

```
time.aws.com  
0.amazon.pool.ntp.org  
1.amazon.pool.ntp.org  
2.amazon.pool.ntp.org  
3.amazon.pool.ntp.org
```

如需支援 AWS 區域 和服務端點的詳細資訊，請參閱《》中的 [Storage Gateway](#) AWS 一般參考。

## 設定 Amazon EC2 閘道執行個體的安全群組

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

- 安全群組不應該允許來自外部網際網路的傳入連線。它只應該允許閘道安全群組內的執行個體與閘道通訊。

如果您需要允許執行個體從其安全群組外部連線至閘道，建議您僅允許連接埠 80（用於啟用）上的連線。

- 如果您要從閘道安全群組外部的 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。
- 只有在您使用 [支援](#) 進行故障診斷時，才允許連接埠 22 存取。如需詳細資訊，請參閱 [支援 您想要協助疑難排解 Amazon EC2 閘道](#)。

## 支援的 Hypervisor 與主機需求

您可以將 Storage Gateway 內部部署作為虛擬機器 (VM) 設備或實體硬體設備執行，或在 AWS 中作為 Amazon EC2 執行個體執行。

### Note

檔案閘道 2.x、磁碟區閘道 3.x 和磁帶閘道 3.x 需要停用安全開機的 UEFI 開機模式 (loader\_secure=no)。每個 qcow 下載都會提供 xml 檔案，做為快速設定組態。

Storage Gateway 支援下列 Hypervisor 版本與主機：

- VMware ESXi Hypervisor (7.0 或 8.0 版) – 在此設定中，您也需要 VMware vSphere 用戶端來連線至主機。
- Microsoft Hyper-V Hypervisor (2019、2022 或 2025) – 在此設定中，您需要 Microsoft Windows 用戶端電腦上的 Microsoft Hyper-V Manager 才能連線至主機。
- Linux 核心基礎虛擬機器 (KVM)：免費的開放原始碼虛擬化技術。KVM 包含於所有版本的 Linux 2.6.20 及更新版本中。Storage Gateway 已針對 CentOS/RHEL 7.7、RHEL 8.6 Ubuntu 16.04 LTS 和 Ubuntu 18.04 LTS 分佈進行測試和支援。任何其他現代 Linux 發行版都可以運作，但不保證功能或性能。如果您已經啟動並執行 KVM 環境，而且您已經熟悉 KVM 的運作方式，建議您使用此選項。如需建議的開機組態，請參閱提供的 aws-storage-gateway.xml 檔案。檔案閘道 2.x、磁碟區閘道 3.x 和磁帶閘道 3.x 需要停用安全開機的 UEFI 開機模式 (loader\_secure=no)。
- 從版本 10.0.1.1 開始的 Nutanix AHV (Acropolis Hypervisor) – 以 KVM 為基礎的虛擬化平台，整合到 Nutanix 超融合基礎設施 (HCI) 解決方案。
- Amazon EC2 執行個體：Storage Gateway 提供包含閘道 VM 映像檔的 Amazon Machine Image (AMI)。如需如何在 Amazon EC2 上部署閘道的資訊，請參閱 [部署 FSx 檔案閘道的預設 Amazon EC2 主機](#)。
- Storage Gateway 硬體設備 – Storage Gateway 為虛擬機器基礎設施有限的位置提供實體硬體設備做為內部部署選項。

### Note

Storage Gateway 不支援透過從快照、另一個閘道 VM 的複製項目，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 [從非預期的虛擬機器關機復原](#)。

Storage Gateway 不支援動態記憶體和虛擬記憶體佔用。

## 檔案閘道支援的 SMB 用戶端

File Gateway 支援下列服務訊息區塊 (SMB) 用戶端：

- Microsoft Windows Server 2008 R2 及更新版本
- Windows 桌面版本：10、8 及 7。
- 在 Windows Server 2008 及更新版本上執行的 Windows 終端機伺服器

### Note

伺服器訊息區塊加密需要支援 SMB v3.x 方言的用戶端。

## 檔案閘道支援的檔案系統操作

您的 SMB 用戶端可以寫入、讀取、刪除和截斷檔案。當用戶端將寫入傳送至 Storage Gateway 時，它會同步寫入本機快取。然後，它會透過最佳化傳輸以非同步方式寫入 Amazon FSx。讀取會先透過本機快取提供。如果資料不可用，則會透過 Amazon FSx 擷取資料做為讀取快取。

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。刪除從 Amazon FSx 移除檔案。

## 管理閘道的本機磁碟

閘道虛擬機器 (VM) 使用您內部部署的本機磁碟來進行緩衝及儲存。您在 Amazon EC2 執行個體上建立的檔案閘道將使用 Amazon EBS 磁碟區做為本機磁碟。您希望為閘道配置的磁碟數目及大小皆由您決定。閘道會使用您配置的快取儲存體，提供最近存取資料的低延遲存取。快取儲存可做為現場部署的耐用存放區，用於待上傳到 Amazon FSx 的資料。檔案閘道至少需要一個 150 GiB 磁碟才能用作快取。在閘道的初始組態和部署之後，您可以隨著工作負載需求增加，為快取儲存新增更多磁碟。本節包含下列主題，說明與管理本機磁碟相關的概念和程序。

### 主題

- [決定本機磁碟儲存體的數量](#) - 了解如何判斷要為您的檔案閘道配置的本機快取磁碟數量和大小。

- [設定其他快取儲存](#) - 了解如何隨著應用程式需求變更，增加檔案閘道的快取儲存容量。
- [搭配 EC2 閘道使用暫時性儲存](#) - 了解如何在搭配 File Gateway 使用暫時性磁碟儲存時防止資料遺失。

## 決定本機磁碟儲存體的數量

部署 FSx File Gateway 時，請考慮要配置多少快取磁碟。FSx File Gateway 使用最近最少使用的演算法，自動從快取移出資料。FSx File Gateway 上的快取會在該閘道上的所有檔案共用之間共用。如果您有多個作用中共享，請務必注意，一個共享的大量使用率可能會影響另一個共享可存取的快取資源量，進而可能影響效能。

判斷特定工作負載所需的快取磁碟數量時，請務必注意，您一律可以將快取磁碟新增至閘道（最高可達 FSx File Gateway 上的目前配額），但無法減少特定閘道的快取。您可以對資料集執行基本分析，以判斷正確的快取磁碟數量，但無法確切判斷要儲存在本機的資料量「熱」和「冷」，而且可以分層至雲端。工作負載會隨著時間而變更，FSx File Gateway 提供與可耗用資源量相關的彈性和彈性。快取數量隨時可以增加，因此從小開始，並視需要增加通常是最具成本效益的方法。

您可以使用 150 GiB 的初始近似值，在閘道設定期間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[效能和最佳化](#)。

### 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，使用做為快取儲存）時，您可以選擇將虛擬磁碟存放在與 VM 相同的資料存放區或不同的資料存放區中。

如果您有多個資料存放區，強烈建議您為快取儲存選擇一個資料存放區。在某些情況下，只有一個基礎實體磁碟支援的資料存放區可能會在用來備份快取儲存體時導致效能不佳。這在備份為效能較差的 RAID 組態（例如 RAID1）時也相同。

## 設定其他快取儲存

隨著應用程式需求變更，您可以增加閘道的快取儲存容量。您可以為閘道增加儲存容量，而不會中斷功能或造成停機。在您新增更多儲存空間時，您的閘道 VM 會同時維持開啟狀態。

**⚠ Important**

將快取新增至現有閘道時，您必須在閘道主機 Hypervisor 或 Amazon EC2 執行個體上建立新的磁碟。請勿移除或變更已配置為快取的現有磁碟大小。

### 設定閘道的其他快取儲存

1. 在閘道主機 Hypervisor 或 Amazon EC2 執行個體上佈建一或多個新磁碟。如需如何在 Hypervisor 中佈建磁碟的資訊，請參閱 Hypervisor 文件。如需為 Amazon EC2 執行個體佈建 Amazon EBS 磁碟區的相關資訊，請參閱《適用於 Linux 執行個體的 Amazon Elastic Compute Cloud 使用者指南》中的 [Amazon EBS 磁碟區](#)。在下列步驟中，您將將此磁碟設定為快取儲存。
2. 前往 <https://console.aws.amazon.com/storagegateway/home> 開啟 Storage Gateway 主控台。
3. 在導覽窗格中，選擇 Gateways (網際網路閘道)。
4. 從清單中搜尋您的閘道，並選取它。
5. 從動作功能表中，選擇設定快取儲存。
6. 在設定快取儲存區段中，識別您佈建的磁碟。如果您沒有看到您的磁碟，請選擇重新整理圖示重新整理清單。對於每個磁碟，從配置到下拉式功能表中選擇快取。

**i Note**

快取是在檔案閘道上配置磁碟的唯一可用選項。

7. 選擇儲存變更以儲存您的組態設定。

## 搭配 EC2 閘道使用暫時性儲存

我們不建議在 FSx 檔案閘道上使用暫時性磁碟進行快取儲存。

暫時性磁碟為您的 Amazon EC2 執行個體提供暫時性區塊層級儲存。當您使用 Amazon EC2 Amazon Machine Image 啟動閘道，且您選取的執行個體類型支援暫時性儲存時，系統會自動列出暫時性磁碟。您可以選擇其中一個磁碟來存放閘道的快取資料。如需詳細資訊，請參閱 [《Amazon EC2 使用者指南》](#) 中的 [Amazon EC2 執行個體存放區](#)。Amazon EC2

應用程式寫入閘道的資料會同步存放在暫時性磁碟的快取中，然後非同步上傳至 FSx for Windows File Server 中的耐用儲存體。如果 Amazon EC2 執行個體在資料寫入暫時性儲存體後停止，但在非同步上傳發生之前，任何尚未上傳至 FSx for Windows File Server 的資料都可能遺失。

**⚠ Important**

如果您正使用暫時性儲存，且停止然後啟動 Amazon EC2 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。沒有解決此問題的解決方法。唯一的解決方法是刪除閘道並在新 EC2 執行個體上啟用一個新的閘道。

# 使用 AWS Storage Gateway 硬體設備

## Note

可用性終止通知：自 2025 年 5 月 12 日起，將不再提供 AWS Storage Gateway 硬體設備。硬體 AWS Storage Gateway 設備的現有客戶可以繼續使用和獲得支援，直到 2028 年 5 月為止。或者，您可以使用 AWS Storage Gateway 服務為應用程式提供現場部署和雲端存取幾乎無限制的雲端儲存。

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

每個硬體設備都是高效能的 1U 伺服器，您可以部署在您的資料中心內或內部部署在公司防火牆內。當您購買並啟用硬體設備時，啟用程序會將硬體設備與您的 建立關聯 AWS 帳戶。啟用後，您的硬體設備會出現在硬體設備概觀頁面上的 主控台中。您可以將硬體設備設定為 S3 檔案閘道、FSx 檔案閘道、磁帶閘道或磁碟區閘道類型。您在硬體設備上部署這些閘道類型的程序與虛擬平台上的程序相同。

如需支援 AWS 區域 使用 AWS Storage Gateway 硬體設備的清單，請參閱 中的 [AWS Storage Gateway 硬體設備區域](#) AWS 一般參考。

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

## 主題

- [設定 your AWS Storage Gateway 硬體設備](#)
- [實際安裝您的硬體設備](#)
- [存取硬體設備主控台](#)
- [設定硬體設備網路參數](#)
- [啟用 your AWS Storage Gateway 硬體設備](#)
- [在硬體設備上建立閘道](#)
- [在硬體設備上設定閘道 IP 地址](#)
- [從硬體設備移除閘道軟體](#)
- [刪除 your AWS Storage Gateway 硬體設備](#)

# 設定 your AWS Storage Gateway 硬體設備

## Note

可用性終止通知：自 2025 年 5 月 12 日起，將不再提供 AWS Storage Gateway 硬體設備。硬體 AWS Storage Gateway 設備的現有客戶可以繼續使用和獲得支援，直到 2028 年 5 月為止。或者，您可以使用 AWS Storage Gateway 服務為應用程式提供現場部署和雲端存取幾乎無限制的雲端儲存。

收到 Storage Gateway 硬體設備後，您可以使用硬體設備本機主控台來設定聯網，以提供與的永遠連線 AWS，並啟用您的設備。啟用會將您的設備與啟用程序期間使用的 AWS 帳戶建立關聯。啟用設備後，您可以從 Storage Gateway 主控台啟動 S3 檔案閘道、FSx 檔案閘道、磁帶閘道或磁碟區閘道。

若要安裝並設定硬體設備，請執行下列步驟：

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

您可以使用與在 VMware ESXi、Microsoft Hyper-V、Linux 核心基礎虛擬機器 (KVM) 或 Amazon EC2 上設定閘道的相同方式來設定您硬體設備上的閘道。

## 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。這樣做可提供更大的快取，以低延遲存取中的資料 AWS。如果您訂購了 5 TB 型號，則可以購買五個 1.92 TB SSD (固態硬碟)，將可用儲存空間增加到 12 TB。

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

1. 將硬體設備重設為出廠設定。如需如何執行此操作的說明，請聯絡 AWS Support。
2. 將五個 1.92 TB SSD 新增到裝置。

## NIC 選項

根據您訂購的設備模型，它可能隨附 10G-Base-T RJ45 銅線或 10G DA/SFP+ 網路卡。

- 10G-Base-T 的 NIC 組態：
  - 將 6 號線用於 10G 或 CAT5 (e)，適用於 1G
- 10G DA/SFP+ NIC 組態：
  - 使用長達 5 公尺的雙軸銅直接連接纜線
  - 戴爾/英特爾兼容的 SFP+ 光學模區塊 (SR 或 LR)
  - 適用於 1G-Base-T 或 10G-Base-T 的 SFP/SFP+ 銅線收發器

## 實際安裝您的硬體設備

### Note

可用性終止通知：自 2025 年 5 月 12 日起，將不再提供 AWS Storage Gateway 硬體設備。硬體 AWS Storage Gateway 設備的現有客戶可以繼續使用和獲得支援，直到 2028 年 5 月為止。或者，您可以使用 AWS Storage Gateway 服務為應用程式提供現場部署和雲端存取幾乎無限制的雲端儲存。

您的裝置具有 1U 機型，適用於符合標準國際電工委員會 (IEC) 的 19 英吋機架。

### 先決條件

若要安裝硬體設備，您需要下列元件：

- 電源線：一條為必要、建議兩條。
- 支援的網路佈線 (視硬體設備中包含的網路介面卡 (NIC) 而定)。雙軸銅 DAC，SFP+ 光學模區塊 (英特爾兼容) 或 SFP 到 Base-T 銅線收發器。
- 鍵盤和顯示器，或鍵盤、視訊和滑鼠 (KVM) 切換解決方案。

### Note

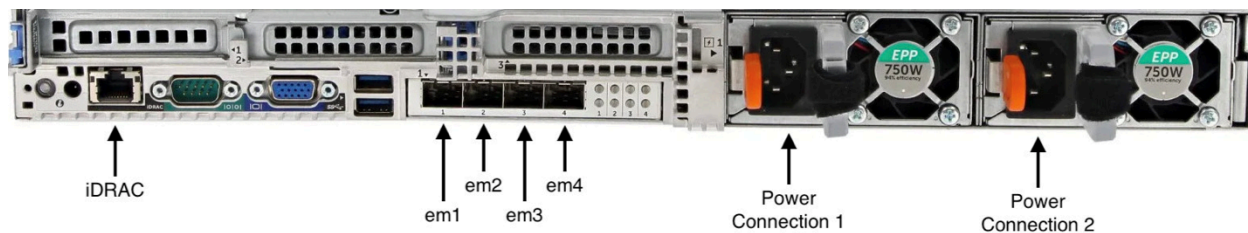
執行下列程序之前，請確定您符合 [Storage Gateway 硬體設備的網路與防火牆要求](#) 中所述的所有 Storage Gateway 硬體設備要求。

## 實際安裝您的硬體設備

1. 解壓縮您的硬體設備，並依照方塊中的指示掛載伺服器。

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

硬體設備後方有網路和電源連接器標籤。



硬體設備後方有網路和電源連接器標籤。

2. 將電源線插入兩個電源供應器。您可以僅將 插入一個電源連接，但我們建議將電源連接到兩個電源以進行備援。
3. 將乙太網路纜線插入 em1 連接埠，以提供全年無休的網際網路連線。em1 連接埠是背面四個實體網路連接埠 (從左到右) 中的第一個。

### Note

硬體設備不支援 VLAN 中繼。將您要連接硬體設備的交換連接埠設定為非中繼 VLAN 連接埠。

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

硬件裝置正面帶有電源按鈕標籤。

下一步驟

[存取硬體設備主控台](#)

# 存取硬體設備主控台

## Note

可用性終止通知：自 2025 年 5 月 12 日起，將不再提供 AWS Storage Gateway 硬體設備。硬體 AWS Storage Gateway 設備的現有客戶可以繼續使用和獲得支援，直到 2028 年 5 月為止。或者，您可以使用 AWS Storage Gateway 服務為應用程式提供現場部署和雲端存取幾乎無限制的雲端儲存。

當您開啟硬體設備的電源時，硬體設備主控台會顯示在監視器上。硬體設備主控台提供特定於的使用者介面 AWS，您可以用來設定管理員密碼、設定初始網路參數，以及開啟支援管道 AWS。

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

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

## 設定管理員密碼

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

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

- 設定網路
- 開啟服務主控台
- 變更密碼
- 登出
- 開啟支援主控台

## 下一步驟

## 設定硬體設備網路參數

# 設定硬體設備網路參數

### Note

可用性終止通知：自 2025 年 5 月 12 日起，將不再提供 AWS Storage Gateway 硬體設備。硬體 AWS Storage Gateway 設備的現有客戶可以繼續使用和獲得支援，直到 2028 年 5 月為止。或者，您可以使用 AWS Storage Gateway 服務為應用程式提供現場部署和雲端存取幾乎無限制的雲端儲存。

在硬體設備開機並在硬體主控台中設定管理員使用者密碼後[存取硬體設備主控台](#)，請使用下列程序來設定網路參數，以便您的硬體設備可以連線 AWS。

### 若要設定網路地址

1. 在首頁中，選擇設定網路，然後按 Enter。設定網路頁面隨即出現。設定網路頁面顯示硬體設備上 4 個網路介面中每個介面的 IP 和 DNS 資訊，並包含為每個介面設定 DHCP 或靜態地址的功能表選項。
2. 針對 em1 介面，執行下列其中一項操作：
  - 選擇 DHCP，然後按 Enter 以使用動態主機組態通訊協定 (DHCP) 伺服器指派給實體網路連接埠的 IPv4 地址。

請注意此地址，以供稍後在啟用步驟中使用。

- 選擇靜態，然後按 Enter 設定靜態 IPv4 地址。

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

完成後，選擇儲存，然後按 Enter 儲存組態。

### Note

除了 em1 之外，您還可以使用此程序來設定其他網路介面。如果您設定其他介面，則必須提供與需求中所列 AWS 端點相同的全年無休連線。  
硬體設備或 Storage Gateway 不支援網路連結和連結彙總控制通訊協定 (LACP)。

我們不建議在同一個子網路上設定多個網路介面，因為這有時可能會導致路由問題。

若要登出硬體主控台

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

下一步驟

[啟用 your AWS Storage Gateway 硬體設備](#)

## 啟用 your AWS Storage Gateway 硬體設備

### Note

可用性終止通知：自 2025 年 5 月 12 日起，將不再提供 AWS Storage Gateway 硬體設備。硬體 AWS Storage Gateway 設備的現有客戶可以繼續使用和獲得支援，直到 2028 年 5 月為止。或者，您可以使用 AWS Storage Gateway 服務為應用程式提供現場部署和雲端存取幾乎無限制的雲端儲存。

設定 IP 地址後，您可以在 AWS Storage Gateway 主控台的硬體頁面上輸入此 IP 地址，以啟用您的硬體設備。啟用程序會將設備註冊到您的帳戶 AWS。

您可以選擇在任何支援的 [中](#) 啟用您的硬體設備 AWS 區域。如需支援的清單 AWS 區域，請參閱《》中的 [Storage Gateway 硬體設備區域](#) AWS 一般參考。

啟用 your AWS Storage Gateway 硬體設備

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

### Note

僅限啟用，必須符合下列條件：

- 您的瀏覽器必須位於硬體設備的同一個網路上。
- 您的防火牆必須允許連接埠 8080 上對裝置的輸入流量 HTTP 存取。

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

如需有關設定 IP 地址的詳細資訊，請參閱來[設定網路參數](#)。

5. 為硬體設備輸入名稱。名稱最多可包含 255 個字元，不可包含斜線字元。
6. 針對硬體應用裝置時區，輸入要產生閘道大部分工作負載的本機時區。然後選擇下一步。

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

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

硬體設備概況頁面會顯示橫幅，指出硬體設備已成功啟用。

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

下一步驟

[在硬體設備上建立閘道](#)

## 在硬體設備上建立閘道

### Note

可用性終止通知：自 2025 年 5 月 12 日起，將不再提供 AWS Storage Gateway 硬體設備。硬體 AWS Storage Gateway 設備的現有客戶可以繼續使用和獲得支援，直到 2028 年 5 月為止。或者，您可以使用 AWS Storage Gateway 服務為應用程式提供現場部署和雲端存取幾乎無限制的雲端儲存。

您可以在部署中的任何 Storage Gateway 硬體設備上建立 S3 檔案閘道、FSx 檔案閘道、磁帶閘道或磁碟區閘道。AWS Storage Gateway

## 若要在硬體設備上建立閘道

1. 登入 AWS 管理主控台，並在 <https://console.aws.amazon.com/storagegateway/home> 開啟 Storage Gateway 主控台。
2. 遵循[建立閘道](#)中所述的程序來設定、連線和設定您要部署的 Storage Gateway 類型。

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

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

### 下一步驟

#### [在硬體設備上設定閘道 IP 地址](#)

## 在硬體設備上設定閘道 IP 地址

### Note

可用性終止通知：自 2025 年 5 月 12 日起，將不再提供 AWS Storage Gateway 硬體設備。硬體 AWS Storage Gateway 設備的現有客戶可以繼續使用和獲得支援，直到 2028 年 5 月為止。或者，您可以使用 AWS Storage Gateway 服務為應用程式提供現場部署和雲端存取幾乎無限制的雲端儲存。

在啟動硬體設備之前，您已為其實體網路介面指派 IP 地址。現在您已啟動裝置並在其上啟動 Storage Gateway，您需要將另一個 IP 地址指派給在硬體設備上執行的 Storage Gateway VM。若要將靜態 IP 地址指派給硬體設備上安裝的閘道，請從該閘道的閘道本機主控台設定 IP 地址。您的應用程式（例如 NFS 或 SMB 用戶端）會連線至此 IP 地址。您可以使用 Open Service Console 選項，從硬體設備主控台存取閘道本機主控台。

### 若要在裝置上設定 IP 地址以使用應用程式

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

預設帳戶是 admin，預設密碼是 password。

**Note**

建議您從 AWS 設備啟用 - 組態主功能表中輸入閘道主控台的對應數字，然後執行 `passwd` 指令，以變更預設密碼。如需如何執行命令的資訊，請參閱 [在本機主控台上執行 Storage Gateway 命令](#)。您也可以從 Storage Gateway 主控台設定密碼。如需詳細資訊，請參閱 [從 Storage Gateway 主控台設定本機主控台密碼](#)。

**3. AWS 設備啟用 - 組態頁面包含下列功能表選項：**

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

**Note**

有些選項只會針對特定閘道類型或主機平台顯示。

輸入對應的數字以導覽至網路組態頁面。

**4. 執行下列其中一項操作來設定閘道 IP 地址：**

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

**Note**

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

## 結束閘道本機主控台

- 按 **Crtl+] (右括號) 按鍵**。硬體主控台會顯示。

### Note

前述按鍵是結束閘道本機主控台的唯一方式。

啟用並設定硬體設備後，您的裝置會顯示在主控台中。現在，您可以在 Storage Gateway 主控台中繼續閘道的設定和組態程序。如需說明，請參閱[設定您的 Amazon FSx File Gateway](#)。

## 從硬體設備移除閘道軟體

### Note

可用性終止通知：自 2025 年 5 月 12 日起，將不再提供 AWS Storage Gateway 硬體設備。硬體 AWS Storage Gateway 設備的現有客戶可以繼續使用和獲得支援，直到 2028 年 5 月為止。或者，您可以使用 AWS Storage Gateway 服務為應用程式提供現場部署和雲端存取幾乎無限制的雲端儲存。

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

### 若要從硬體設備移除閘道

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

出現確認對話方塊。

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

**Note**

移除閘道軟體後，就無法復原動作。對於特定的閘道類型，刪除後可能會遺失資料，特別是快取的資料。如需刪除閘道的詳細資訊，請參閱 [刪除您的閘道並移除相關聯的資源](#)。

移除閘道並不會從主控台刪除硬體設備。硬體設備會保留以供日後閘道部署。

## 刪除 your AWS Storage Gateway 硬體設備

**Note**

可用性終止通知：自 2025 年 5 月 12 日起，將不再提供 AWS Storage Gateway 硬體設備。硬體 AWS Storage Gateway 設備的現有客戶可以繼續使用和獲得支援，直到 2028 年 5 月為止。或者，您可以使用 AWS Storage Gateway 服務為應用程式提供現場部署和雲端存取幾乎無限制的雲端儲存。

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

**Note**

若要將設備移至不同的 AWS 帳戶 AWS 區域，或者，您必須先使用下列程序將其刪除，然後開啟閘道的支援管道並聯絡 支援 以執行軟重設。如需詳細資訊，請參閱診斷 [開啟 支援 存取以協助對內部部署託管的閘道進行故障診斷](#)。

### 刪除您的硬體設備

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

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

## 建立閘道

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

- [建立並啟動 Amazon S3 File Gateway](#)
- [建立並啟動 Amazon FSx File Gateway](#)
- [建立和啟用磁帶閘道](#)
- [建立和啟用磁碟區閘道](#)

### Important

Amazon FSx File Gateway 不再提供給新客戶。FSx File Gateway 的現有客戶可以繼續正常使用服務。如需類似 FSx File Gateway 的功能，請造訪[此部落格文章](#)。

## 概觀：閘道啟動

閘道啟用包括設定閘道、將其連線至 AWS，然後檢閱您的設定並啟用它。

### 設定閘道

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

### 連線至 AWS

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

## 檢閱並啟用

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

## 概觀：閘道組態

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

## 概觀：儲存資源

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

## 建立 Amazon FSx for Windows File Server 檔案系統

若要在 中建立 Amazon FSx 檔案閘道 AWS Storage Gateway，第一個步驟是建立 Amazon FSx for Windows File Server 檔案系統。如果您已建立 Amazon FSx 檔案系統，請前往下一個步驟：[建立並啟動 Amazon FSx File Gateway](#)。

### Note

從 FSx 檔案閘道寫入 Amazon FSx 檔案系統時，適用下列限制：

- 您的 Amazon FSx 檔案系統和您的 FSx 檔案閘道必須由相同 AWS 帳戶擁有，且位於相同 AWS 區域。
- 每個閘道都可以支援五個連接的檔案系統。連接檔案系統時，Storage Gateway 主控台會在選取的閘道處於容量時通知您。在這種情況下，您必須先選擇不同的閘道或分離檔案系統，才能連接另一個閘道。
- FSx File Gateway 支援軟儲存配額（當使用者超過資料限制時發出警告），但不支援硬配額（透過拒絕寫入存取強制執行資料限制）。除了 Amazon FSx 管理員使用者之外，所有使用者都支援軟配額。如需設定儲存配額的詳細資訊，請參閱《Amazon FSx for Windows File Server 使用者指南》中的[儲存配額](#)。

- 我們不建議使用 Microsoft 分散式檔案系統 (DFS) 透過 FSx 檔案閘道將使用者重新導向到您的 Amazon FSx 檔案系統。反之，請設定 DFS 直接重新導向至中的 Amazon FSx 檔案系統 AWS 雲端，如《Amazon FSx for Windows File Server 使用者指南》[中的使用 DFS 命名空間分組多個檔案系統](#)所述。
- FSx File Gateway 上的某些檔案操作，例如頂層資料夾重新命名或許可變更，可能會導致多個檔案操作，導致 FSx for Windows File Server 檔案系統具有高 I/O 負載。如果您的檔案系統沒有足夠的效能資源來處理工作負載，檔案系統可能會刪除[影子複本](#)，因為它會將持續 I/O 的可用性優先於歷史影子複本保留。

在 Amazon FSx 主控台中，檢查監控和效能頁面，查看您的檔案系統是否佈建不足。如果是，您可以切換到 SSD 儲存、增加輸送量容量或增加 SSD IOPS 來處理工作負載。

## 建立 FSx for Windows File Server 檔案系統

1. AWS 管理主控台 在 <https://console.aws.amazon.com/fsx/home/> 開啟，然後選擇您要在其中建立閘道的區域。
2. 請遵循 [《Amazon FSx for Windows File Server 使用者指南》](#) 中的 Amazon FSx 入門中的指示。

## 建立並啟動 Amazon FSx File Gateway

在本節中，您可以找到如何在其中建立、部署和啟用檔案閘道的指示 AWS Storage Gateway。

### 主題

- [設定 Amazon FSx File Gateway](#)
- [將您的 Amazon FSx 檔案閘道連線至 AWS](#)
- [檢閱設定並啟用 Amazon FSx 檔案閘道](#)
- [設定您的 Amazon FSx File Gateway](#)

## 設定 Amazon FSx File Gateway

### 設定新的 FSx 檔案閘道

1. 在 AWS 管理主控台 <https://console.aws.amazon.com/storagegateway/home/> 開啟，然後選擇您要建立閘道 AWS 區域的。
2. 選擇建立閘道以開啟設定閘道頁面。

3. 在閘道設定區段中，執行下列操作：
  - a. 為 Gateway name (閘道名稱) 輸入閘道的名稱。建立閘道之後，您可以搜尋此名稱，在 主控台的清單頁面上 AWS Storage Gateway 尋找閘道。
  - b. 針對閘道時區，請選擇您要部署閘道的全球當地時區。
4. 在閘道選項區段中，針對閘道類型選擇 Amazon FSx 檔案閘道。
5. 在平台選項區段中，執行下列操作：
  - a. 針對主機平台，選擇您要部署閘道的平台。然後，遵循 Storage Gateway 主控台頁面上顯示的平台特定指示來設定您的主機平台。您可從下列選項擇一使用：
    - VMware ESXi – 使用 VMware ESXi 下載、部署和設定閘道虛擬機器。
    - Microsoft Hyper-V – 使用 Microsoft Hyper-V 下載、部署和設定閘道虛擬機器。
    - Linux KVM – 使用 Linux 核心型虛擬機器 (KVM) 下載、部署和設定閘道虛擬機器。如需建議的開機組態，請參閱提供的 `aws-storage-gateway.xml` 檔案。檔案閘道 2.x、磁碟區閘道 3.x 和磁帶閘道 3.x 需要停用安全開機的 UEFI 開機模式 (`loader_secure=no`)。
    - Amazon EC2 – 設定並啟動 Amazon EC2 執行個體來託管您的閘道。
    - 硬體設備 – 從 訂購專用實體硬體設備 AWS ，以託管您的閘道。
  - b. 在確認設定閘道中，選取核取方塊以確認您已針對所選主機平台執行部署步驟。此步驟不適用於硬體設備主機平台。
6. 現在您的閘道已設定完成，您必須選擇其連線和通訊的方式 AWS。選擇下一步繼續進行。

## 將您的 Amazon FSx 檔案閘道連線至 AWS

### 將新的 FSx 檔案閘道連線至 AWS

1. 如果您尚未這麼做，請完成[設定 Amazon FSx 檔案閘道](#)中所述的程序。完成後，選擇下一步以在 AWS Storage Gateway 主控台中開啟連線至 AWS 頁面。
2. 在端點選項區段中，針對服務端點，選擇閘道將用於通訊的端點類型 AWS。您可從下列選項擇一使用：
  - 可公開存取 – 您的閘道 AWS 會透過公有網際網路與 通訊。如果您選取此選項，請使用啟用 FIPS 的端點核取方塊來指定連線是否符合聯邦資訊處理標準 (FIPS)。

**Note**

如果您在 AWS 透過命令列界面或 API 存取時需要 FIPS 140-2 驗證的密碼編譯模組，請使用符合 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 服務端點僅適用於某些 AWS 區域。如需詳細資訊，請參閱 AWS 一般參考中的[AWS Storage Gateway 端點和配額](#)。

- VPC 託管 – 閘道 AWS 會透過與虛擬私有雲端 (VPC) 的私有連線與通訊，讓您控制網路設定。如果您選取此選項，則必須從下拉式清單中選擇其 VPC 端點 ID，以指定現有的 VPC 端點。您也可以提供其 VPC 端點網域名稱系統 (DNS) 名稱或 IP 地址。
3. 在閘道連線選項區段中，針對連線選項，選擇如何識別連線至 AWS 的閘道。您可從下列選項擇一使用：
- IP 地址 – 在對應的欄位中提供閘道的 IP 地址。此 IP 地址必須是公開的，或可從您目前的網路存取，而且您必須能夠從 Web 瀏覽器連線到該 IP 地址。
- 您可以從 Hypervisor 用戶端登入閘道的本機主控台，或從 Amazon EC2 執行個體詳細資訊頁面複製來取得閘道 IP 地址。
- 啟用金鑰 – 在對應的欄位中提供閘道的啟用金鑰。您可以使用閘道的本機主控台產生啟用金鑰。如果您閘道的 IP 地址無法使用，請選擇此選項。
4. 現在您已選擇閘道的連線方式 AWS，您必須啟用閘道。選擇下一步繼續進行。

## 檢閱設定並啟用 Amazon FSx 檔案閘道

### 啟用新的 FSx 檔案閘道

1. 如果您尚未這麼做，請完成下列主題中所述的程序：
  - [設定 Amazon FSx File Gateway](#)
  - [將您的 Amazon FSx 檔案閘道連線至 AWS](#)

完成後，選擇下一步以在主控台中 AWS Storage Gateway 開啟檢閱並啟用頁面。

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

**⚠ Important**

啟動閘道後，您無法修改閘道選項或連線設定。

- 現在您已啟用閘道，您必須執行第一次組態來配置本機儲存磁碟並設定記錄。選擇下一步繼續進行。

## 設定您的 Amazon FSx File Gateway

在新的 FSx 檔案閘道上執行第一次組態

- 如果您尚未這麼做，請完成下列主題中所述的程序：

- [設定 Amazon FSx File Gateway](#)
- [將您的 Amazon FSx 檔案閘道連線至 AWS](#)
- [檢閱設定並啟用 Amazon FSx 檔案閘道](#)

完成後，選擇下一步以在主控台中 AWS Storage Gateway 開啟設定閘道頁面。

- 在設定儲存區段中，使用下拉式清單配置至少一個具有至少 150 GB (GiB) 容量的本機磁碟來快取。本節中列出的本機磁碟對應於您在主機平台上佈建的實體儲存體。
- 在 CloudWatch 日誌群組區段中，選擇如何設定 Amazon CloudWatch Logs 以監控閘道的運作狀態。您可從下列選項擇一使用：
  - 建立新的日誌群組 – 設定新的日誌群組來監控您的閘道。
  - 使用現有的日誌群組 – 從對應的下拉式清單中選擇現有的日誌群組。
  - 停用記錄 – 請勿使用 Amazon CloudWatch Logs 監控您的閘道。

**i Note**

若要接收 Storage Gateway 運作狀態日誌，您的日誌群組資源政策中必須存在下列許可。將#####取代為部署的特定日誌群組 resourceArn 資訊。

```
"Sid": "AWSLogDeliveryWrite20150319",
  "Effect": "Allow",
  "Principal": {
```

```
"Service": [
  "delivery.logs.amazonaws.com"
],
"Action": [
  "logs:CreateLogStream",
  "logs:PutLogEvents"
],
"Resource": "arn:aws:logs:eu-west-1:1234567890:log-group:/foo/bar:log-stream:*"
```

只有在您希望許可明確套用至個別日誌群組時，才需要「資源」元素。

4. 在 CloudWatch 警示區段中，選擇如何設定 Amazon CloudWatch 警示，以便在閘道的指標偏離定義的限制時通知您。您可從下列選項擇一使用：
  - 建立儲存閘道的建議警示：建立閘道時，自動建立所有建議的 CloudWatch 警示。如需建議警示的詳細資訊，請參閱[了解 CloudWatch 警示](#)。

#### Note

此功能需要 CloudWatch 政策許可，這些許可不會在預先設定的 Storage Gateway 完整存取政策中自動授予。在嘗試建立建議的 CloudWatch 警示之前，請確定您的安全性原則授與下列許可：

- `cloudwatch:PutMetricAlarm`：建立警示
  - `cloudwatch:DisableAlarmActions`：關閉警示動作
  - `cloudwatch:EnableAlarmActions`：開啟警示動作
  - `cloudwatch>DeleteAlarms`：刪除警示
- 建立自訂警示 – 設定新的 CloudWatch 警示，以接收閘道指標的通知。選擇建立警示以在 Amazon CloudWatch 主控台中定義指標並指定警示動作。如需詳細指引，請參閱《Amazon CloudWatch 使用者指南》中的[使用 Amazon CloudWatch 警示](#)。
  - 無警示 – 請勿使用 CloudWatch 警示來接收閘道指標的通知。
5. (選用) 在標籤區段中，選擇新增標籤，然後輸入區分大小寫的鍵值對，協助您在主控台的 AWS Storage Gateway 清單頁面上搜尋和篩選閘道。重複此步驟，視需要新增任意數量的標籤。
  6. (選用) 在驗證 VMware 高可用性組態區段中，如果您的閘道部署在屬於 VMware 高可用性 (HA) 叢集的 VMware 主機上，請選擇驗證 VMware HA 以測試 HA 組態是否正常運作。

**Note**

本節僅適用於在 VMware 主機平台上執行的閘道。  
完成閘道組態程序不需要此步驟。您可以隨時測試閘道的 HA 組態。驗證需要幾分鐘的時間，並重新啟動 Storage Gateway 虛擬機器 (VM)。

**7. 選擇設定以完成建立閘道。**

若要檢查新閘道的狀態，請在 主控台的 AWS Storage Gateway 閘道概觀頁面上搜尋它。

現在您已建立閘道，您必須連接檔案系統以供其使用。如需說明，請參閱[連接 Amazon FSx for Windows File Server 檔案系統](#)。

如果您沒有要連接的現有 Amazon FSx 檔案系統，則必須建立一個。如需說明，請參閱[Amazon FSx 入門](#)。

## 在虛擬私有雲端中啟用閘道

您可以在內部部署閘道裝置以及雲端儲存基礎設施之間建立私有連線。您可以使用此連線來啟用閘道，並將其設定為將資料傳輸至 AWS 儲存服務，而無需透過公有網際網路進行通訊。使用 Amazon VPC 服務，您可以在自訂虛擬私有雲端 (VPC) 中啟動 AWS 資源，包括私有網路介面端點。您可利用 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。如需有關 VPC 的詳細資訊，請參閱《Amazon VPC 使用者指南》中的[什麼是 Amazon VPC ?](#)。

若要在 VPC 中啟用閘道，請使用 Amazon VPC 主控台為 [Storage Gateway 建立 VPC 端點](#) 並取得 VPC 端點 ID，然後在建立和啟用閘道時指定此 VPC 端點 ID。如需詳細資訊，請參閱[連接至您的 Amazon FSx 檔案閘道 AWS](#)。

若要設定 FSx 檔案閘道透過 VPC 傳輸資料，您必須在 Amazon FSx for Windows File Server VPC 與部署閘道的網路之間建立 VPN 或 AWS DirectConnect 連結。

**Note**

您必須在為 Storage Gateway 建立 VPC 端點的相同區域中啟用閘道。

## 建立 Storage Gateway 的 VPC 端點

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

### 建立 Storage Gateway 的 VPC 端點

1. 登入 AWS 管理主控台，並在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇端點，然後選擇建立端點。
3. 在建立端點頁面上，針對服務類別選擇 AWS 服務。
4. 在 Service Name (服務名稱) 中，選擇 `com.amazonaws.region.storagegateway`。例如 `com.amazonaws.us-east-2.storagegateway`。
5. 針對 VPC，選擇您的 VPC，並記下其可用區域和子網路。
6. 確認未選取啟用 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. 在所選儲存區閘道端點的詳細資訊標籤的 DNS 名稱下，使用未指定可用區域的第一個 DNS 名稱。您的 DNS 名稱看起來應該類似下列範例：  
`vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

現在您已擁有 VPC 端點，您可以建立和啟用閘道。如需詳細資訊，請參閱[建立和啟用 Amazon FSx 檔案閘道](#)。

如需有關取得啟用金鑰的資訊，請參閱[取得閘道的啟用金鑰](#)。

## 設定 Microsoft Active Directory 網域存取設定

在此步驟中，您可以設定存取設定，將 Amazon FSx 檔案閘道加入 Microsoft Active Directory 網域。

### 設定 Active Directory 設定

1. 在 Storage Gateway 主控台中，從導覽功能表中選擇 FSx 檔案系統。
2. 選擇連接 FSx 檔案系統。
3. 在確認閘道頁面上，從下拉式選單中選擇您要加入 Active Directory 網域的閘道。

如果您沒有閘道，則必須建立一個閘道。確保您的閘道可以解析 Active Directory 網域控制站的名稱。如需相關資訊，請參閱[先決條件](#)。

4. 輸入 Active Directory 設定的值：

#### Note

如果您的閘道已加入網域，則不需要再次加入。前往下一個步驟。

- 針對網域名稱，輸入您要使用的 Active Directory 網域名稱。
- 對於網域使用者，輸入您要用來將閘道加入網域的 Active Directory 使用者的使用者名稱。此使用者必須具有必要的許可。如需詳細資訊，請參閱[Active Directory 服務帳戶許可要求](#)。
- 針對網域密碼，輸入使用者的密碼。
- 對於組織單位 - 選用，您可以指定 Active Directory 所屬的組織單位。

#### Note

如果您將此欄位保留空白，加入網域會使用閘道的閘道 ID 做為帳戶名稱（例如，SGW-1234ADE），在預設電腦容器（非 OU）中建立 Active Directory 電腦帳戶。您無法自訂此帳戶的名稱。

如果您的 Active Directory 環境要求您預先設定帳戶以促進加入網域程序，您將需要事先建立此帳戶。

如果您的 Active Directory 環境具有新電腦物件的指定 OU，您必須在加入網域時指定該 OU。

- 輸入網域控制站的值（選用）。

5. 選擇下一步以開啟連接 FSx 檔案系統頁面。

下一步驟

[連接 Amazon FSx for Windows File Server 檔案系統](#)

## 連接 Amazon FSx for Windows File Server 檔案系統

您必須先擁有 FSx for Windows File Server 檔案系統，才能將其連接至 FSx 檔案閘道。如果您沒有檔案系統，則必須建立一個。如需說明，請參閱《Amazon FSx for Windows [File Server 使用者指南](#)》中的 [步驟 1：建立您的檔案系統](#)。

下一個步驟是將 Amazon FSx 檔案系統連接至閘道。當您連接 Amazon FSx 檔案系統時，檔案系統上的所有檔案共用都會提供給 Amazon FSx 檔案閘道 (FSx 檔案閘道) 供您掛載。

### Note

從 Amazon FSx 檔案閘道寫入 Amazon FSx 檔案系統時，適用下列限制：

- 您的 Amazon FSx 檔案系統和 FSx 檔案閘道必須由相同擁有 AWS 帳戶，且位於相同 AWS 區域。
- 每個閘道最多可支援五個連接的檔案系統。當您連接檔案系統時，Storage Gateway 主控台會在選取的閘道容量不足時通知您。在這種情況下，您必須先選擇不同的閘道或分離檔案系統，才能連接另一個閘道。
- FSx File Gateway 支援軟儲存配額（當使用者超過資料限制時警告您），但不支援硬配額（透過拒絕寫入存取強制執行資料限制）。除了 Amazon FSx 管理員使用者之外，所有使用者都支援軟配額。如需設定儲存配額的詳細資訊，請參閱《Amazon FSx 使用者指南》中的 [儲存配額](#)。
- 我們不建議使用 Microsoft 分散式檔案系統 (DFS) 透過 FSx 檔案閘道將使用者重新導向到您的 Amazon FSx 檔案系統。反之，請設定 DFS 直接重新導向至中的 Amazon FSx 檔案系統 AWS 雲端，如《Amazon FSx for Windows File Server 使用者指南》中的 [使用 DFS 命名空間分組多個檔案系統](#) 所述。FSx

### 連接 Amazon FSx 檔案系統

1. 在 Storage Gateway 主控台的 FSx 檔案系統 > 連接 FSx 檔案系統頁面上，完成 FSx 檔案系統設定區段中的下列欄位：
  - 對於 FSx 檔案系統名稱，從下拉式清單中選擇您要連接的檔案系統。
  - 針對本機端點 IP 地址，輸入用戶端用來瀏覽 FSx 檔案系統上檔案共用的閘道 IP 地址。

**Note**

- 您必須為連接到閘道的每個檔案系統指定 IP 地址。
- 對於 Amazon EC2 閘道，您可以指定 EC2 執行個體的私有 IP 地址，除非它已由不同的檔案系統使用，在這種情況下，您必須將新的私有地址新增至閘道，然後重新啟動它。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[多個 IP 地址](#)。
- 對於內部部署閘道，您可以指定主要網路介面（靜態或 DHCP）的 IP 地址，除非它已由不同的檔案系統使用，在這種情況下，您必須提供與主要介面相同的子網路不同的 IP 地址，這將作為虛擬 IP 提供。請勿使用指派給主要介面以外的任何網路介面的 IP 地址。

2. 在服務帳戶設定區段中，提供與 Amazon FSx 檔案系統相關聯的服務帳戶登入憑證。

**Note**

此服務帳戶必須具有與 Amazon FSx 檔案系統相關聯的 Active Directory 服務的 Backup Operators 權限，或具有同等許可。

**Important**

為了確保檔案、資料夾和檔案中繼資料的足夠許可，建議您將服務帳戶設為檔案系統管理員群組的成員。

如果您使用 AWS Directory Service for Microsoft Active Directory 搭配 Amazon FSx for Windows File Server，則服務帳戶必須是 AWS 委派 FSx 管理員群組的成員。

如果您使用自我管理 Active Directory 搭配 Amazon FSx for Windows File Server，我們建議您的服務帳戶是您在建立 Amazon FSx 檔案系統時為檔案系統管理指定的自訂委派檔案系統管理員群組的成員。

如果您在建立 Amazon FSx 檔案系統時選擇不建立自訂委派檔案系統管理員群組，則預設群組為網域管理員。雖然您可以改為讓服務帳戶成為此群組的成員，但不建議將其視為最佳實務。

如需詳細資訊，請參閱 [《Amazon FSx for Windows File Server 使用者指南》中的將權限委派給 Amazon FSx 服務帳戶](#)。 FSx

3. 在稽核日誌區段中，選擇現有日誌群組，然後選擇您要用來監控 Amazon FSx 檔案系統存取的日誌。您可以建立新的。如果您不想監控系統，請選擇停用記錄。

4. 對於自動快取重新整理設定，如果您希望快取自動重新整理，請選擇設定重新整理間隔，並指定介於 5 分鐘到 30 天的間隔。
5. （選用）在標籤區段中，選擇新增標籤以新增一或多個金鑰和值來標記您的設定。
6. 選擇下一步並檢閱設定。若要變更設定，您可以在每個區段中選擇編輯。
7. 完成時請選擇 Finish (完成)。

下一步驟

[掛載和使用您的 Amazon FSx 檔案共享](#)

# 掛載和使用您的 Amazon FSx 檔案共享

在用戶端上掛載檔案共享之前，請等待 Amazon FSx 檔案系統的狀態變更為可用。掛載檔案共享之後，您可以開始使用 Amazon FSx 檔案閘道 (FSx 檔案閘道)。

## 主題

- [在用戶端上掛載 SMB 檔案共享](#)
- [測試您的 FSx 檔案閘道](#)

## 在用戶端上掛載 SMB 檔案共享

在此步驟中，您會掛載 SMB 檔案共用，並映射至用戶端可存取的磁碟機。主控台的檔案閘道區段顯示您可以用於 SMB 用戶端的支援掛載命令。以下是一些可嘗試的其他選項。

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：

- net use 命令 – 除非您使用/persistent:(yes:no)切換，否則不會在系統重新啟動期間保留。
- CmdKey 命令列公用程式 – 建立對掛載 SMB 檔案共用的持久性連線，該共用會在重新啟動後保留。
- 在 File Explorer 中映射的網路磁碟機 – 將掛載的檔案共用設定為在登入時重新連線，並要求您輸入網路憑證。
- PowerShell 指令碼 – 可以是持久性，且掛載時作業系統可以可見或不可見。

### Note

如果您是 Microsoft Active Directory 使用者，請先向您的管理員確認您有權存取 SMB 檔案共享，再將檔案共享掛載到本機系統。

Amazon FSx File Gateway 不支援 SMB 鎖定或 SMB 延伸屬性。

使用 net use 命令掛載 Active Directory 使用者的 SMB 檔案共享

1. 請確定您有權存取 SMB 檔案共享，再將檔案共享掛載到本機系統。
2. 對於 Microsoft Active Directory 用戶端，請在命令提示中輸入下列命令：

```
net use [WindowsDriveLetter]: \\[Gateway IP Address]\[Name of the share on the FSx file system]
```

## 使用 CmdKey 在 Windows 上掛載 SMB 檔案共享

1. 按 Windows 鍵並輸入 **cmd** 以檢視命令提示功能表項目。
2. 開啟命令提示字元的內容（按一下滑鼠右鍵）選單，然後選擇以管理員身分執行。
3. 輸入以下命令：

```
C:\>cmdkey /add:[Gateway VM IP address] /user:[DomainName]\[UserName] /pass:[Password]
```

### Note

掛載檔案共享時，您可能需要在重新啟動用戶端後重新掛載檔案共享。

## 使用 Windows 檔案總管掛載 SMB 檔案共享


1. 按 Windows 鍵，然後在搜尋 Windows **File Explorer** 方塊中輸入 **，** 或按 **Win+E**。
2. 在導覽窗格中，選擇此 PC。然後，在電腦索引標籤上，選擇映射網路磁碟機。
3. 在映射網路磁碟機對話方塊中，選擇磁碟機的磁碟機代號。
4. 針對資料夾，輸入 **\\[File Gateway IP]\[SMB File Share Name]**，或選擇瀏覽，從對話方塊中選取您的 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) 如果您希望使用者輸入 Active Directory 登入或訪客帳戶使用者密碼，請選取使用不同登入資料進行連線。
7. 選擇 Finish (完成) 完成您的掛載點。

## 測試您的 FSx 檔案閘道

您可以將檔案和目錄複製到映射的磁碟機。檔案會自動上傳至 FSx for Windows File Server 檔案系統。

### 將檔案從 Windows 用戶端上傳至 Amazon FSx

1. 在 Windows 用戶端上，導覽至您掛載檔案系統的磁碟機。磁碟機的名稱前面是檔案系統的名稱。
2. 將檔案或目錄複製到磁碟機。

 Note

檔案閘道不支援在檔案共享上建立硬連結或符號連結。

# 管理您的 Amazon FSx File Gateway 資源

下列各節提供如何管理 Amazon FSx 檔案閘道 (FSx 檔案閘道) 資源的相關資訊，包括連接和分離 Amazon FSx 檔案系統，以及設定 Microsoft Active Directory 設定。

## 主題

- [了解閘道狀態](#)
- [了解檔案系統狀態](#)
- [編輯 FSx 檔案閘道的基本資訊](#)
- [設定閘道的安全層級](#)
- [編輯 n FSx 檔案閘道的 Active Directory 設定](#)
- [編輯 Amazon FSx 檔案系統的設定](#)
- [分離 Amazon FSx 檔案系統](#)

## 了解閘道狀態

your AWS Storage Gateway 部署中的每個閘道都有相關聯的狀態，可讓您快速了解閘道的運作狀態。大多數情況下，狀態表示閘道正常運作，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 主控台的閘道頁面上查看部署中每個閘道的狀態。閘道狀態會出現在閘道名稱旁的狀態欄中。正常運作的閘道狀態為 RUNNING。

在下表中，您可以找到每個閘道狀態的描述，以及您是否應該根據狀態採取行動。閘道在全部或大部分時間都應該處於 RUNNING 狀態。

狀態	意義
RUNNING	閘道已正確設定且可供使用。
OFFLINE	由於以下一個或多個原因，您的閘道可能處於 OFFLINE 狀態： <ul style="list-style-type: none"><li>• 閘道無法連線到 Storage Gateway 服務端點。</li><li>• 閘道發生未預期的關閉。</li><li>• 閘道具有已中斷連線、已修改或已失敗的相關聯快取磁碟。</li></ul>

## 了解檔案系統狀態

您可以查看檔案系統的狀態，一目了然地檢視其運作狀態。如果狀態指出檔案系統正常運作，您不需要採取任何動作。如果狀態指出發生問題，您可以進行調查，以判斷是否需要採取動作。

您可以在狀態欄的 Storage Gateway 主控台上檢視檔案系統的狀態。正常運作的檔案系統會顯示可用狀態。這應該是大多數時間的狀態。

下表說明檔案共用狀態、其意義，以及是否需要採取動作。

狀態	意義
AVAILABLE	檔案系統已正確設定且可供使用。這是正常運作之檔案系統的標準狀態。
CREATING	檔案系統尚未完全建立，且尚未準備好可供使用。CREATING (正在建立) 狀態是過渡的。無需採取任何動作。如果檔案系統卡在此狀態，可能是因為閘道 VM 失去連線 AWS。
UPDATING	檔案系統組態目前正在更新。UPDATING 狀態為轉換狀態。無需採取任何動作。如果檔案系統卡在此狀態，可能是因為閘道 VM 失去連線 AWS。
DELETING	正在刪除檔案系統。在上傳所有資料之前，不會刪除檔案系統 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)	正在強制刪除檔案系統。檔案系統會立即刪除，且資料不會上傳到其中 AWS。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。
ERROR	檔案系統處於運作狀態不佳的狀態。動作為必要項目。有些可能的原因包括存取憑證或權限的問題、連線問題，或檔案系統的儲存空間不足。解決造成運作狀態不佳的問題時，檔案系統會回到可用狀態。

## 編輯 FSx 檔案閘道的基本資訊

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

## 編輯現有閘道的基本資訊

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

### Note

閘道名稱必須介於 2 到 255 個字元之間，且不能包含斜線 (\ 或 /)。  
變更閘道名稱將中斷設定為監控閘道的任何 CloudWatch 警示。若要重新連線警示，請在 CloudWatch 主控台中更新每個警示的 GatewayName。

5. 針對閘道時區，請選擇您要部署閘道的全球當地時區。
6. 針對選擇如何設定日誌群組，選擇如何設定 Amazon CloudWatch Logs 來監控閘道的運作狀態。您可從下列選項擇一使用：
  - 建立新的日誌群組 – 設定新的日誌群組來監控您的閘道。
  - 使用現有的日誌群組 – 從對應的下拉式清單中選擇現有的日誌群組。
  - 停用記錄 – 請勿使用 Amazon CloudWatch Logs 監控您的閘道。
7. 當您完成修改您要變更的設定時，請選擇儲存變更。

## 設定閘道的安全層級

您可以設定 FSx 檔案閘道的 SMB 安全層級，以指定閘道是否需要伺服器訊息區塊 (SMB) 簽署或 SMB 加密。

### 設定安全層級

1. 前往 <https://console.aws.amazon.com/storagegateway/home> 開啟 Storage Gateway 主控台。
2. 選擇閘道，然後選擇您要為其編輯 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 SMB 安全設定。
4. 對於 Security level (安全層級)，請選擇以下其中一項：

**Note**

如需有關使用 AWS API 設定此設定的資訊，請參閱 AWS Storage Gateway API 參考中的 [UpdateSMBSecurityStrategy](#)。  
更高的安全層級可能會影響閘道的效能。

- 強制性加密 – 如果您選擇此選項，FSx File Gateway 僅允許使用 256 位元 AES 加密演算法的 SMBv3 用戶端進行連線。不允許使用 128 位元演算法。對於處理敏感資料的環境，建議使用此選項。它適用於 Microsoft Windows 8、Windows Server 2012 或更新版本的 SMB 用戶端。
- 強制加密 – 如果您選擇此選項，FSx File Gateway 僅允許來自己開啟加密之 SMBv3 用戶端的連線。允許 256 位元和 128 位元演算法。對於處理敏感資料的環境，建議使用此選項。它適用於 Microsoft Windows 8、Windows Server 2012 或更新版本的 SMB 用戶端。
- 強制簽署 – 如果您選擇此選項，FSx File Gateway 僅允許來自己開啟簽署之 SMBv2 或 SMBv3 用戶端的連線。此選項適用於 Microsoft Windows Vista、Windows Server 2008 或更新版本上的 SMB 用戶端。

**Note**

FSx File Gateway 的預設安全層級是強制加密。

## 5. 選擇儲存。

## 編輯 n FSx 檔案閘道的 Active Directory 設定

若要使用公司 Microsoft Active Directory 或 AWS Managed Microsoft AD 進行使用者驗證存取 Amazon FSx 檔案系統，請編輯閘道的 SMB 設定並提供您的 Active Directory 網域憑證。這樣做可讓您的閘道加入 Active Directory 網域，並允許網域成員存取檔案系統。

**Note**

您可以使用 Directory Service 在 中建立託管 Active Directory 網域服務 AWS 雲端。  
若要 AWS Managed Microsoft AD 搭配 Amazon EC2 閘道使用，您必須在與 相同的 VPC 中建立 Amazon EC2 執行個體 AWS Managed Microsoft AD，將 `_workspaceMembers` 安全群

組新增至 Amazon EC2 執行個體，並使用來自的 Admin 憑證加入 AD 網域 AWS Managed Microsoft AD。

如需的詳細資訊 AWS Managed Microsoft AD，請參閱 [AWS Directory Service 管理指南](#)。

如需 Amazon EC2 的詳細資訊，請參閱 [Amazon Elastic Compute Cloud 文件](#)。

## 開啟 Active Directory 身分驗證

1. 前往 <https://console.aws.amazon.com/storagegateway/home> 開啟 Storage Gateway 主控台。
2. 選擇閘道，然後選擇您要為其編輯 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. 針對網域名稱，輸入您希望閘道加入的 Active Directory 網域名稱。

### Note

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

您的 Active Directory 服務帳戶必須具有必要的許可。如需詳細資訊，請參閱 [Active Directory 服務帳戶許可要求](#)。

加入網域會使用閘道的閘道 ID 做為帳戶名稱 (例如，SGW-1234ADE)，在預設的電腦容器 (不是 OU) 中建立 Active Directory 電腦帳戶。您無法自訂此帳戶的名稱。

如果您的 Active Directory 環境要求您預先設定帳戶以促進加入網域程序，您將需要事先建立此帳戶。

如果您的 Active Directory 環境具有新電腦物件的指定 OU，您必須在加入網域時指定該 OU。

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。

5. 對於網域使用者和網域密碼，輸入閘道將用於加入網域的 Active Directory 服務帳戶的登入資料。
6. (選用) 針對組織單位 (OU)，輸入 Active Directory 用於新電腦物件的指定 OU。
7. (選用) 對於網域控制器 (DC)，輸入閘道將透過其中連線到 Active Directory 的一或多個 DCs 的名稱。您可以輸入多個 DCs 做為逗號分隔清單。您可以保留此欄位空白，以允許 DNS 自動選取 DC。
8. 選擇儲存變更。

## 編輯 Amazon FSx 檔案系統的設定

建立 Amazon FSx for Windows File Server 檔案系統之後，您可以編輯 CloudWatch 日誌、自動快取重新整理和 Amazon FSx 服務帳戶憑證的設定。

### 編輯 Amazon FSx 檔案系統設定

1. 前往 <https://console.aws.amazon.com/storagegateway/home> 開啟 Storage Gateway 主控台。
2. 在導覽窗格中，選擇檔案系統，然後選擇您要編輯其設定的檔案系統。
3. 針對動作，選擇編輯檔案系統設定。
4. 在檔案系統設定區段中，驗證閘道、Amazon FSx 位置和 IP 地址資訊。

#### Note

您無法在檔案系統的 IP 地址連接到閘道後編輯該檔案系統的 IP 地址。若要變更 IP 地址，您必須分離並重新連接檔案系統。

5. 在稽核日誌區段中，選擇選項以使用 CloudWatch 日誌群組來監控對 Amazon FSx 檔案系統的存取。您可以使用現有的日誌群組。
6. 針對自動快取重新整理設定，選擇  選項。如果您選擇設定重新整理間隔，請設定以天、小時和分鐘為單位的時間，以使用存留時間 (TTL) 重新整理檔案系統的快取。

TTL 是自上次重新整理以來的時間長度。當目錄在該時間長度之後存取時，檔案閘道會從 Amazon FSx 檔案系統重新整理該目錄的內容。

#### Note

有效的重新整理間隔值介於 5 分鐘到 30 天之間。

7. 在服務帳戶設定 - 選用區段中，輸入使用者名稱和密碼。這些登入資料適用於具有來自與您的 Amazon FSx 檔案系統相關聯之 Active Directory 服務的 Backup Administrator 角色的使用者。
8. 選擇儲存變更。

## 分離 Amazon FSx 檔案系統

分離檔案系統不會刪除 FSx for Windows File Server 中的資料。在您分離之前寫入這些檔案系統的資料，仍會上傳至 FSx for Windows File Server。

### 分離 Amazon FSx 檔案系統

1. 前往 <https://console.aws.amazon.com/storagegateway/home> 開啟 Storage Gateway 主控台。
2. 選擇 FSx 檔案系統，然後選擇一或多個要分離的檔案系統。
3. 針對動作，選擇分離檔案系統。出現確認對話方塊。
4. 確認您想要分離指定的檔案系統，然後在確認方塊中輸入分離一詞，然後選擇分離。

# 監控 Storage Gateway

本節中的主題說明如何使用 Amazon CloudWatch 監控閘道，包括監控快取儲存體和與閘道相關聯的其他資源。您可以使用 Storage Gateway 主控台檢視閘道的指標和警示。例如，您可以檢視讀取和寫入操作中使用的位元組數、讀取和寫入操作所花費的時間，以及從 AWS 雲端擷取資料所花費的時間。使用指標，您可以追蹤閘道的運作狀態，並設定警示，在一或多個指標落在定義閾值以外時通知您。

Storage Gateway 提供 CloudWatch 指標，無需支付額外費用。會記錄兩週期間的 Storage Gateway 指標。透過使用這些指標，您可以存取歷史資訊，並更好地了解閘道的效能。Storage Gateway 也提供 CloudWatch 警示 (高解析度警示除外)，無須額外付費。如需 CloudWatch 定價的詳細資訊，請參閱 [Amazon CloudWatch 定價](#)。如需有關 CloudWatch 的詳細資訊，請參閱《[Amazon CloudWatch 使用者指南](#)》。

## 主題

- [了解 CloudWatch 警示](#) - 了解 CloudWatch 警示的基本資訊，包括警示狀態和建議的組態。
- [建立建議的 CloudWatch 警示](#) - 了解如何在初始檔案閘道設定程序中快速自動設定所有建議的 CloudWatch 警示。
- [建立自訂 CloudWatch 警示](#) - 了解如何建立自訂 CloudWatch 警示，以使用特定評估條件來觸發警示狀態和傳送通知來監控特定指標。
- [監控 FSx 檔案閘道](#) - 了解如何檢視 CloudWatch 日誌和稽核日誌，並尋找閘道報告的特定閘道和檔案 sharefile 系統指標的相關資訊。

## 了解 CloudWatch 警示

CloudWatch 警示會根據指標和運算式監控閘道的相關資訊。您可以為閘道新增 CloudWatch 警示，並在 Storage Gateway 主控台中檢視其狀態。如需用於監控 FSx File Gateway 之指標的詳細資訊，請參閱 [了解閘道指標](#) 和 [了解檔案系統指標](#)。對於每個警示，您指定將啟用其 ALARM 狀態的條件。Storage Gateway 主控台內的警示狀態指示燈處於警示狀態時會變成紅色，讓您更輕鬆地主動監控狀態。您可以將警示設定為根據持續的狀態變更自動調用動作。如需有關 CloudWatch 警示的詳細資訊，請參閱《[Amazon CloudWatch 使用者指南](#)》中的 [使用 Amazon CloudWatch 警示](#)。

### Note

如果您沒有檢視 CloudWatch 的許可，您將無法檢視這些警示。

使用每個已啟用的閘道時，建議您建立下列 CloudWatch 警示：

- 高 IO 等候：IoWaitpercent  $\geq$  20，15 分鐘內 3 個資料點
- 快取變更百分比：CachePercentDirty  $>$  80，20 分鐘內 4 個資料點
- 檔案上傳失敗：FilesFailingUpload  $\geq$  5 分鐘內 1 個資料點
- 檔案系統錯誤：FileSystem-ERROR  $\geq$  1 表示 5 分鐘內 1 個資料點
- 運作狀態通知：HealthNotifications  $\geq$  1 表示 5 分鐘內 1 個資料點。設定此警示時，請將遺失資料處理設定為 notBreaching。

#### Note

只有在閘道在 CloudWatch 中有先前的健康狀況通知，您才能設定健康狀況通知警示。

對於屬於 VMware 高可用性叢集的 VMware 主機平台上的閘道，我們也建議使用此額外的 CloudWatch 警示：

- 可用性通知：AvailabilityNotifications  $\geq$  1 代表 5 分鐘內的 1 個資料點。設定此警示時，請將遺失資料處理設定為 notBreaching。

下表說明 CloudWatch 警示狀態。

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

## 建立閘道的 CloudWatch 警示

使用 Storage Gateway 主控台建立新閘道時，您可以選擇在初始設定程序中自動建立所有建議的 CloudWatch 警示。如需詳細資訊，請參閱[設定 Amazon FSx 檔案閘道](#)。如果您想要在完成第一次設定後，為現有閘道新增或更新建議的 CloudWatch 警示，請使用下列程序。

若要為現有閘道新增或更新建議的 CloudWatch 警示

### Note

此功能需要 CloudWatch 政策許可，這些許可不會在預先設定的 Storage Gateway 完整存取政策中自動授與。在嘗試建立建議的 CloudWatch 警示之前，請確定您的安全性原則授與下列許可：

- `cloudwatch:PutMetricAlarm`：建立警示
- `cloudwatch:DisableAlarmActions`：關閉警示動作
- `cloudwatch:EnableAlarmActions`：開啟警示動作
- `cloudwatch>DeleteAlarms`：刪除警示

1. 前往 <https://console.aws.amazon.com/storagegateway/home> 開啟 Storage Gateway 主控台。
2. 在頁面左側的導覽窗格中，選擇閘道，然後選擇您要為其建立建議 CloudWatch 警示的閘道。
3. 在閘道的詳細資訊頁面上，選擇監控索引標籤。
4. 在警示下，選擇建議的警示。建議的警示會自動建立。

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

## 為您的閘道建立自訂 CloudWatch 警示

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

## 为 Storage Gateway 主控台建立 CloudWatch 警示

1. 前往 <https://console.aws.amazon.com/storagegateway/home> 開啟 Storage Gateway 主控台。
2. 在導覽窗格中，選擇閘道，然後選擇您要管理的閘道。
3. 在閘道詳細資訊頁面上，選擇監控標籤。
4. 在警示下方，選擇建立警示以開啟 CloudWatch 主控台。
5. 使用 CloudWatch 主控台建立所需的警示類型。您可以建立以下類型的警示：

- 靜態閾值警示：根據所選指標之設定閾值的警示。當指標在指定的評估期間數違反閾值時，警示會進入 ALARM 狀態。

若要建立靜態閾值警示，請參閱《Amazon CloudWatch 使用者指南》中的[建立以靜態閾值為基礎的 CloudWatch 警示](#)。

- 異常偵測警示：異常偵測會探勘過去的指標資料，並建立預期值的模型。您可以設定異常偵測臨界值，CloudWatch 會使用此臨界值搭配模型，以決定指標的「正常」範圍。較高的臨界值會產生較厚的「正常」值範圍。您可以選擇警示觸發時機是在指標值超過預期值範圍、低於範圍，或者兩者擇一。

若要建立異常偵測警示，請參閱《Amazon CloudWatch 使用者指南》中的[建立以異常偵測為基礎的 CloudWatch 警示](#)。

- 指標數學運算式警示：以數學運算式中使用的一或多個指標為基礎的警示。您要指定表達式、閾值和評估期間。

若要建立指標數學表達式警示，請參閱《Amazon CloudWatch 使用者指南》中的[建立以指標數學表達式為基礎的 CloudWatch 警示](#)。

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

若要建立複合警示，請參閱《Amazon CloudWatch 使用者指南》中的[建立複合警示](#)。

6. 在 CloudWatch 主控台中建立警示後，傳回 Storage Gateway 主控台。您可以執行下列其中一個操作來檢視警示：
  - 在導覽窗格中，選擇閘道，然後選擇您要檢視的閘道。在詳細資訊標籤上，為警示選擇 CloudWatch 警示。
  - 在瀏覽窗格中，選擇閘道，選擇要檢視警示的閘道，然後選擇監控標籤頁。

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

- 在導覽窗格中，選擇閘道，然後選擇您要檢視其警示之閘道的警示狀態。

如需如何編輯或刪除警示的相關資訊，請參閱[編輯或刪除 CloudWatch 警示](#)。

#### Note

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

## 監控 FSx 檔案閘道

您可以使用 Amazon CloudWatch 指標和稽核日誌 AWS Storage Gateway，在中監控 FSx 檔案閘道和相關聯的資源。您也可以使用 CloudWatch Events 在檔案操作完成時收到通知。

### 主題

- [使用 CloudWatch 日誌群組取得 FSx File Gateway 運作狀態日誌](#)
- [使用 Amazon CloudWatch 指標](#)
- [了解閘道指標](#)
- [了解檔案系統指標](#)
- [了解 FSx File Gateway 稽核日誌](#)

## 使用 CloudWatch 日誌群組取得 FSx File Gateway 運作狀態日誌

您可以使用 Amazon CloudWatch Logs 來取得 FSx 檔案閘道和相關資源運作狀態的相關資訊。您可以使用日誌來監控閘道所遇到的錯誤。此外，您可以使用 Amazon CloudWatch 訂閱篩選條件，自動即時處理日誌資訊。如需更多資訊，請參閱《Amazon CloudWatch 使用者指南》中的[使用訂閱即時處理日誌資料](#)。

例如，您可以設定 CloudWatch 日誌群組來監控閘道，並在 FSx 檔案閘道無法將檔案上傳至 Amazon FSx 檔案系統時收到通知。您可以在啟用閘道時或在啟用閘道並啟動和執行之後設定群組。如需有關如何在啟用閘道時設定 CloudWatch 日誌群組的資訊，請參閱[設定您的 Amazon FSx File Gateway](#)。

如需 CloudWatch 日誌群組的一般資訊，請參閱《Amazon CloudWatch 使用者指南》中的[使用日誌群組和日誌串流](#)。Amazon CloudWatch

如需如何對 FSx File Gateway 可能報告的錯誤進行故障診斷的資訊，請參閱[故障診斷：檔案閘道問題](#)。

## 啟用閘道後設定 CloudWatch 日誌群組

下列程序說明如何在閘道啟用後設定 CloudWatch Log Group。

設定 CloudWatch 日誌群組以搭配 FSx File Gateway 使用

1. 登入 AWS 管理主控台，並在 <https://console.aws.amazon.com/storagegateway/home> 開啟 Storage Gateway 主控台。
2. 在導覽窗格中，選擇閘道，然後選擇您要設定 CloudWatch 日誌群組的閘道。
3. 針對動作，選擇編輯閘道資訊。
4. 針對選擇如何設定日誌群組，選擇下列其中一項：
  - 建立新的日誌群組會建立新的 CloudWatch 日誌群組。
  - 使用現有的日誌群組來使用已存在的 CloudWatch 日誌群組。  
從現有的日誌群組清單中選擇日誌群組。
  - 如果您不想使用 CloudWatch 日誌群組監控閘道，請停用記錄。
5. 選擇儲存變更。
6. 若要查看閘道的運作狀態日誌，請依下列步驟執行：
  1. 在導覽窗格中，選擇閘道，然後選擇您設定 CloudWatch 日誌群組的閘道。
  2. 選擇詳細資訊標籤，然後在運作狀況日誌下選擇 CloudWatch Logs。在 CloudWatch 主控台中，開啟日誌群組頁面。

## 使用 Amazon CloudWatch 指標

您可以使用 AWS 管理主控台 或 CloudWatch API，取得 FSx File Gateway 的監控資料。主控台會根據 CloudWatch API 的原始資料顯示一系列圖形。CloudWatch API 也可以透過其中一個[AWS SDKs](#) 或 [Amazon CloudWatch API](#) 工具使用。根據需求，您可能偏好使用顯示於主控台內的圖形或自 API 擷取的圖形。

無論您使用哪種方法來使用指標，都必須指定下列資訊：

- 要使用的指標維度。維度是一組用來單獨辨識指標的名稱值組。Storage Gateway 的維度為 GatewayId 和 GatewayName。在 CloudWatch 主控台中，您可以使用 Gateway Metrics 檢視來選取閘道特定的維度。如需維度的詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的[維度](#)。
- 指標名稱，例如 ReadBytes。

下表摘要說明可供您使用之 Storage Gateway 指標資料的類型。

Amazon CloudWatch 命名空間	維度	Description
AWS/StorageGateway	GatewayId , GatewayName	<p>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 FSx 檔案閘道。</p> <p>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。</p> <p>每隔 5 分鐘免費自動提供資料。</p>

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](#)
- [取得指標的統計資料](#)
- [建立 CloudWatch 警示](#)

## 了解閘道指標

下表說明涵蓋 FSx 檔案閘道的指標。每個閘道都有一組與其相關聯的指標。有些閘道特定指標與特定 file-system-specific 指標的名稱相同。這些指標代表相同的測量類型，但範圍是閘道而非檔案系統。

使用特定指標時，請務必指定要使用閘道或檔案系統。具體而言，在使用閘道指標時，您必須 Gateway Name 為要檢視其指標資料的閘道指定。如需詳細資訊，請參閱[使用 Amazon CloudWatch 指標](#)。

**Note**

某些指標只有在最近的監視期間產生新資料時，才會傳回資料點。

下表說明可用來取得 FSx File Gateway 相關資訊的指標。

指標	Description
AvailabilityNotifications	<p>此指標會報告閘道在報告期間所產生的可用性相關運作狀態通知數目。</p> <p>單位：Count</p>
CacheDirectorySize	<p>此指標會追蹤閘道快取中資料夾的大小。資料夾大小取決於其第一層中的檔案和子資料夾數量，這不會遞迴計入子資料夾。</p> <p>將此指標與 Average 統計資料搭配使用，以測量閘道快取中資料夾的平均大小。將此指標與 Max 統計資料搭配使用，以測量閘道快取中資料夾的大小上限。</p> <p>單位：Count</p>
CacheFileSize	<p>此指標會追蹤閘道快取中檔案的大小。</p> <p>將此指標與 Average 統計資料搭配使用，以測量閘道快取中檔案的平均大小。將此指標與 Max 統計資料搭配使用，以測量閘道快取中檔案的大小上限。</p> <p>單位：位元組</p>
CacheFree	<p>此指標會報告閘道快取中可用位元組的數量。</p> <p>單位：位元組</p>
CacheHitPercent	<p>從快取提供的應用程式讀取操作百分比。報告期間結束時會取樣。</p>

指標	Description
	<p>當沒有來自閘道的應用程式讀取操作時，此指標會報告 100%。</p> <p>單位：百分比</p>
CachePercentDirty	<p>尚未保留的閘道快取整體百分比 AWS。報告期間結束時會取樣。</p> <p>單位：百分比</p>
CachePercentUsed	<p>使用的閘道快取儲存體的整體百分比。報告期間結束時會取樣。</p> <p>單位：百分比</p>
CacheUsed	<p>此指標會報告閘道快取中已使用位元組的數量。</p> <p>單位：位元組</p>
CloudBytesDownloaded	<p>在報告期間，閘道從 下載 AWS 的位元組總數。</p> <p>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。</p> <p>單位：位元組</p>
CloudBytesUploaded	<p>在 AWS 報告期間，閘道上傳到的位元組總數。</p> <p>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)。</p> <p>單位：位元組</p>

指標	Description
FilesFailingUpload	<p>此指標會追蹤無法上傳到的檔案數量 AWS。這些檔案會產生運作狀態通知，其中包含有關問題的詳細資訊。</p> <p>使用此指標搭配 Sum 統計資料，以顯示目前上傳失敗的檔案數量 AWS。</p> <p>單位：Count</p>
FileShares	<p>此指標會報告閘道上的檔案共用數目。</p> <p>單位：Count</p>
FileSystem-ERROR	<p>此指標提供此閘道上處於 ERROR 狀態的檔案系統關聯數目。</p> <p>如果此指標報告任何檔案系統關聯處於 ERROR 狀態，則閘道可能有問題，這可能會導致工作流程中斷。建議在此指標報告非零值時建立警示。</p> <p>單位：Count</p>
HealthNotifications	<p>此指標會報告此閘道在報告期間所產生的運作狀態通知數目。</p> <p>單位：Count</p>
IndexEvictions	<p>此指標會報告從檔案中繼資料的快取索引中移出其中繼資料的檔案數量，以便為新項目騰出空間。閘道會維護此中繼資料索引，該索引會從隨需 AWS 雲端填入。</p> <p>單位：Count</p>

指標	Description
IndexFetches	<p>此指標會報告擷取中繼資料的檔案數量。閘道會維護檔案中繼資料的快取索引，這會從隨需 AWS 雲端填入。</p> <p>單位：Count</p>
IoWaitPercent	<p>此指標會報告 CPU 從本機磁碟等待回應的時間百分比。</p> <p>單位：百分比</p>
MemTotalBytes	<p>此指標會報告閘道上的記憶體總量。</p> <p>單位：位元組</p>
MemUsedBytes	<p>此指標會報告閘道上已使用記憶體的數量。</p> <p>單位：位元組</p>
RootDiskFreeBytes	<p>此指標會報告閘道根磁碟上可用的位元組數。</p> <p>如果此指標回報少於 20 GB 是免費的，您應該增加根磁碟的大小。</p> <p>若要增加根磁碟大小，您可以增加 VM 上現有根磁碟的大小。重新啟動 VM 時，閘道會辨識根磁碟上增加的大小。</p> <p>單位：位元組</p>
SmbV2Sessions	<p>此指標會報告閘道上作用中的 SMBv2 工作階段數目。此指標會針對與閘道相關聯的每個檔案系統發出一個。使用 SUM 統計資料來計算所有檔案系統中作用中 SMBv2 工作階段的總數。</p> <p>單位：Count</p>

指標	Description
SmbV3Sessions	此指標會報告閘道上作用中的 SMBv3 工作階段數目。此指標會針對與閘道相關聯的每個檔案系統發出一次。使用 SUM 統計資料來計算所有檔案系統中作用中 SMBv3 工作階段的總數。  單位：Count
TotalCacheSize	此指標會報告快取的總大小。  單位：位元組
UserCpuPercent	此指標會報告閘道處理所花費的時間百分比。  單位：百分比

## 了解檔案系統指標

您可以在下面找到涵蓋檔案系統的 Storage Gateway 指標的相關資訊。每個檔案系統都有一組與其相關聯的指標。有些檔案系統特定指標與特定閘道特定指標的名稱相同。這些指標代表相同類型的測量，但範圍改為檔案系統。

在使用指標之前，請務必指定您要使用閘道或檔案系統指標。具體而言，使用檔案系統指標時，您必須指定 File system ID 可識別您有興趣檢視指標之檔案系統的。如需詳細資訊，請參閱 [使用 Amazon CloudWatch 指標](#)。

### Note

某些指標只有在最近的監視期間產生新資料時，才會傳回資料點。

下表說明可用來取得檔案共享相關資訊的 Storage Gateway 指標。

指標	Description
CacheHitPercent	從快取提供的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。

指標	Description
	<p>當檔案共享中沒有應用程式讀取操作時，此指標會報告 100%。</p> <p>單位：百分比</p>
CachePercentDirty	<p>檔案共享對尚未保留之閘道快取整體百分比的貢獻 AWS。報告期間結束時會取樣。</p> <p>使用此指標搭配 Sum 統計資料。</p> <p>理想情況下，此指標應保持低。</p> <div data-bbox="829 703 1507 968"><p> Note</p><p>使用閘道的 CachePercentDirty 指標來檢視尚未保留的閘道快取整體百分比 AWS。</p></div> <p>單位：百分比</p>
CachePercentUsed	<p>在整個閘道中使用的資料快取百分比。報告期間結束時會取樣。此檔案共享特定指標會報告與對應閘道特定指標相同的值。</p> <p>單位：百分比</p>
CloudBytesUploaded	<p>在 AWS 報告期間，閘道上傳到的位元組總數。</p> <p>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。</p> <p>單位：位元組</p>

指標	Description
CloudBytesDownloaded	<p>在報告期間，閘道從下載 AWS 的位元組總數。</p> <p>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)。</p> <p>單位：位元組</p>
FilesFailingUpload	<p>此指標會追蹤無法上傳到的檔案數量 AWS。這些檔案會產生運作狀態通知，其中包含有關問題的詳細資訊。</p> <p>使用此指標搭配 Sum 統計資料，以顯示目前上傳失敗的檔案數量 AWS。</p> <p>單位：Count</p>
ReadBytes	<p>檔案共享報告期間從您內部部署應用程式讀取的位元組總數。</p> <p>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。</p> <p>單位：位元組</p>
WriteBytes	<p>報告期間寫入至您內部部署應用程式的位元組總數。</p> <p>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。</p> <p>單位：位元組</p>

## 了解 FSx File Gateway 稽核日誌

Amazon FSx File Gateway (FSx File Gateway) 稽核日誌為您提供有關使用者存取檔案系統關聯內檔案和資料夾的詳細資訊。您可以使用稽核日誌來監控使用者活動，並在發現不適當的活動模式時採取行

動。日誌的格式類似於 Windows Server 安全日誌事件，以支援與 Windows 安全事件的現有日誌處理工具的相容性。

## 操作

下表說明 FSx File Gateway 稽核日誌檔案存取操作。

操作名稱	定義
讀取資料	讀取檔案的內容。
寫入資料	變更檔案的內容。
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。
刪除	刪除檔案或資料夾。
寫入屬性	更新檔案或資料夾中繼資料 (ACL、擁有者、群組、許可)。

## Attributes

下表說明 FSx File Gateway 稽核日誌檔案存取屬性。

屬性	定義
securityDescriptor	以 SDDL 格式顯示物件上設定的判別式存取控制清單 (DACL)。
sourceAddress	檔案共享用用戶端機器的 IP 地址。
SubjectDomainName	用戶端帳戶所屬的 Active Directory (AD) 網域。
SubjectUserName	用戶端的 Active Directory 使用者名稱。
source	正在FileSystemAssociation 稽核的 Storage Gateway ID。

屬性	定義
mtime	由用戶端設定修改物件內容的時間。
version	稽核日誌格式的版本。
ObjectType	定義物件是檔案還是資料夾。
locationDnsName	FSx 檔案閘道系統 DNS 名稱。
objectName	物件的完整路徑。
ctime	由用戶端設定修改物件內容或中繼資料的時間。
shareName	正在存取的共用名稱。
operation	物件存取操作的名稱。
newObjectName	新物件重新命名後的完整路徑。
gateway	Storage Gateway ID。
status	操作的狀態。只會記錄成功（會記錄失敗，但因許可遭拒而產生的失敗除外）。
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）。

## 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 FSx File Gateway 稽核日誌屬性。

	讀取資料	寫入資料	建立資料夾	建立檔案	重新命名檔案/資料夾	刪除檔案/資料夾	寫入屬性 (變更 ACL)	寫入屬性 (chown)	寫入屬性 (chmod)	寫入屬性 (chgrp)
securi escrip							X			
source ress	X	X	X	X	X	X	X	X	X	X
Subjec mainNa	X	X	X	X	X	X	X	X	X	X
Subjec erName	X	X	X	X	X	X	X	X	X	X
source	X	X	X	X	X	X	X	X	X	X
mtime			X	X						
versic	X	X	X	X	X	X	X	X	X	X
object e	X	X	X	X	X	X	X	X	X	X
locati nsName	X	X	X	X	X	X	X	X	X	X
object e	X	X	X	X	X	X	X	X	X	X
ctime			X	X						
shareN	X	X	X	X	X	X	X	X	X	X

	讀取 資料	寫入 資料	建 立資 料夾	建立 檔案	重新 命名 檔 案/資 料夾	刪 除檔 案/資 料夾	寫入 屬性 (變 更 ACL)	寫入 屬性 (chown)	寫入 屬性 (chmod)	寫入 屬性 (chgrp)
operat	X	X	X	X	X	X	X	X	X	X
newObj Name					X					
gatewa	X	X	X	X	X	X	X	X	X	X
status	X	X	X	X	X	X	X	X	X	X
fileSi nBytes				X						

## 維護您的閘道

維護 Amazon FSx File Gateway 需要執行一般維護，以最佳化閘道的效能。這些任務對於所有閘道類型而言非常常見。

本節包含下列主題，說明與維護 Amazon FSx File Gateway 相關的概念和程序：

### 主題

- [管理閘道更新](#) – 了解如何開啟或關閉維護更新，並修改檔案閘道的維護時段排程。
- [使用本機主控台執行維護任務](#) – 了解如何使用閘道本機主控台執行維護任務。
- [關閉您的閘道 VM](#) – 了解如果您需要關閉或重新啟動閘道虛擬機器以進行維護時該怎麼做，例如將修補程式套用至 Hypervisor 時。
- [將現有的 FSx 檔案閘道取代為新的執行個體](#) – 了解如何在想要改善效能或回應通知以遷移閘道時，以新的執行個體取代 FSx File Gateway。
- [刪除您的閘道並移除相關聯的資源](#) – 了解如何使用 AWS Storage Gateway 主控台刪除閘道，並清除相關聯的資源，以避免因繼續使用而產生費用。

## 管理閘道更新

Storage Gateway 包含受管雲端服務元件，以及您在內部部署或 AWS 雲端 Amazon EC2 執行個體上部署的閘道設備元件。這兩個元件都會定期收到更新。本節中的主題說明這些更新的節奏、如何套用更新，以及如何在部署中的閘道上設定更新相關設定。

### Important

您應該將 Storage Gateway 設備視為受管虛擬機器，且不應嘗試以任何方式存取或修改其安裝或內容。嘗試使用一般 AWS 閘道更新機制（例如 SSM 或 Hypervisor 工具）以外的方法安裝或更新任何軟體套件，可能會導致閘道故障。

Storage Gateway 會自動並定期修補設備，以維護安全性和穩定性。Storage Gateway 設備使用 Amazon Linux 作為其基本作業系統。您可以在 [Amazon Linux 安全中心](#) 檢查偵測到的常見漏洞與暴露 (CVE) 問題的狀態。CVE 修補程式會在發行後 30 天內自動套用，如 Amazon Linux 安全中心所示。修補程式會在閘道維護排程期間安裝，前提是您的閘道已上線。

Storage Gateway 不支援使用 cloud-init 指令手動更新 Amazon EC2 閘道。如果您使用此方法更新閘道，您可能遇到互通性問題，使您無法啟用或使用閘道設備。

## 更新頻率和預期行為

AWS 會視需要更新雲端服務元件，而不會造成已部署閘道的中斷。您部署的閘道設備會收到以下類型的更新：

- 維護 - 定期更新，可能包括作業系統和軟體升級、解決穩定性、效能和安全性的修正，以及新功能的存取。
- 緊急 - 包括立即影響閘道安全性、效能或耐久性之問題的必要修正的關鍵更新。緊急更新可隨時在每月維護和功能更新的正常節奏之外發佈。

所有更新都是累積的，在套用時會將閘道升級為目前版本。如需有關每次更新中包含的特定變更的資訊，請參閱。

所有閘道設備更新都可能導致服務短暫中斷。閘道的 VM 主機不需要在更新期間重新啟動，但在閘道設備更新和重新啟動時，閘道將短暫無法使用。

當您部署和啟用閘道時，會設定預設的維護時段排程。您可以隨時[修改維護時段排程](#)。您也可以關閉維護更新，但我們建議將其保持開啟狀態。

### Note

即使定期維護更新已關閉，也會根據維護時段排程套用緊急更新。

將任何更新套用至閘道之前，AWS 會在 Storage Gateway 主控台和上通知您訊息 AWS Health 儀板表。如需詳細資訊，請參閱[AWS Health 儀板表](#)。若要修改傳送軟體更新通知的電子郵件地址，請參閱[AWS 《帳戶管理參考指南》中的更新帳戶的替代聯絡人](#)。AWS

有更新可用時，閘道詳細資訊索引標籤會顯示維護訊息。您也可以在詳細資訊索引標籤上查看套用上次成功更新的日期和時間。

## 開啟或關閉維護更新

開啟維護更新作業時，您的閘道會根據設定的維護時段排程自動套用這些更新。如需詳細資訊，請參閱[修改閘道維護時段排程](#)。

如果關閉維護更新，閘道不會自動套用這些更新，但您可以隨時使用 Storage Gateway 主控台、API 或 CLI 手動套用這些更新。緊急更新有時會在您設定的維護時段期間套用，無論此設定為何。

**Note**

下列程序說明如何使用 Storage Gateway 主控台開啟或關閉閘道更新。若要使用 API 以程式設計方式變更此設定，請參閱 Storage Gateway API 參考中的 [UpdateMaintenanceStartTime](#)。

若要使用 Storage Gateway 主控台開啟或關閉維護更新：

1. 前往 <https://console.aws.amazon.com/storagegateway/home> 開啟 Storage Gateway 主控台。
2. 在導覽窗格中，選擇閘道，然後選擇您要設定維護更新的閘道。
3. 選擇動作，然後選擇編輯維護設定。
4. 針對維護更新，選取開啟或關閉。
5. 完成後，請選擇儲存變更。

您可以在 Storage Gateway 主控台中，驗證所選閘道的詳細資訊索引標籤上的更新設定。

## 修改閘道維護時段排程

如果開啟維護更新，閘道會根據維護時段排程自動套用這些更新。緊急更新有時會在您設定的維護時段期間套用，無論維護更新設定為何。

**Note**

下列程序說明如何使用 Storage Gateway 主控台修改維護時段排程。若要使用 API 以程式設計方式變更此設定，請參閱 Storage Gateway API 參考中的 [UpdateMaintenanceStartTime](#)。

若要使用 Storage Gateway 主控台修改維護時段排程：

1. 前往 <https://console.aws.amazon.com/storagegateway/home> 開啟 Storage Gateway 主控台。
2. 在導覽窗格中，選擇閘道，然後選擇您要設定維護更新的閘道。
3. 選擇動作，然後選擇編輯維護設定。
4. 在維護時段開始時間下，執行下列動作：
  - a. 針對排程，選擇每週或每月以設定維護時段節奏。
  - b. 如果您選擇每週，請修改星期幾和時間的值，以在每週開始維護時段期間設定特定點。

如果您選擇每月，請修改每月日期和時間的值，以在每個月開始維護時段期間設定特定點。

#### Note

可以為月份中的日期設定的最大值為 28。維護排程無法設定為在 29 至 31 天之間的任何一天開始。

如果您在設定此設定時收到錯誤，可能表示您的閘道軟體已過時。考慮先手動更新您的閘道，然後嘗試再次設定維護時段排程。

5. 完成後，請選擇儲存變更。

您可以在 Storage Gateway 主控台中驗證所選閘道的詳細資訊索引標籤上的更新設定。

## 手動套用更新

如果您的閘道有可用的軟體更新，您可以依照下列程序手動套用。即使維護更新已關閉，此手動更新程序仍會忽略維護時段排程並立即套用更新。

#### Note

下列程序說明如何使用 Storage Gateway 主控台手動套用更新。若要使用 API 以程式設計方式執行此動作，請參閱 Storage Gateway API 參考中的 [UpdateGatewaySoftwareNow](#)。

若要使用 Storage Gateway 主控台手動套用閘道軟體更新：

1. 前往 <https://console.aws.amazon.com/storagegateway/home> 開啟 Storage Gateway 主控台。
2. 在導覽窗格中，選擇閘道，然後選擇您要更新的閘道。

如果更新可用，主控台會在閘道詳細資訊索引標籤上顯示藍色通知橫幅，其中包含套用更新的選項。

3. 選擇立即套用更新以立即更新閘道。

**Note**

此操作會在更新安裝時暫時中斷閘道功能。在此期間，閘道狀態會在 Storage Gateway 主控台中顯示為 OFFLINE。更新完成安裝後，閘道會繼續正常操作，且其狀態會變更為 RUNNING。

您可以在 Storage Gateway 主控台中檢查所選閘道的詳細資訊索引標籤，以確認閘道軟體已更新至最新版本。

## 使用本機主控台執行維護任務

本節包含下列主題，提供如何使用閘道設備本機主控台執行維護任務的相關資訊。您可以透過內部部署虛擬機器或託管閘道設備的 Amazon EC2 執行個體，存取本機主控台來執行這些任務。大多數任務在不同的主機平台上都是常見的，但也有一些差異。

### 主題

- [存取閘道本機主控台](#) - 了解如何登入本機主控台，以便在 Linux 核心型虛擬機器 (KVM)、VMware ESXi 或 Microsoft Hyper-V Manager 平台上託管的內部部署閘道。
- [在虛擬機器本機主控台上執行任務](#) - 了解如何使用本機主控台執行內部部署閘道的基本設定和進階組態任務，例如設定 HTTP 代理、檢視系統資源狀態或執行終端機命令。
- [在 Amazon EC2 閘道本機主控台上執行任務](#) - 了解如何登入本機主控台，以執行 Amazon EC2 閘道的基本設定和進階組態任務，例如設定 HTTP 代理、檢視系統資源狀態或執行終端機命令。

## 存取閘道本機主控台

如何存取您的 VM 的本機主控台，取決於您的閘道 VM 部署所在的 Hypervisor 類型。在本節中，您可以找到如何使用 Linux 核心型虛擬機器 (KVM)、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
```

命令會傳回每個 VMs 的 ID、名稱和狀態資訊清單。請注意您要為其啟動閘道本機主控台 Id 的 VM 的。

2. 使用下列命令來存取本機主控台。

```
# virsh console Id
```

將 *Id* 取代之為您在上一個步驟中記下的 VM ID。

AWS 設備閘道本機主控台會提示您登入以變更網路組態和其他設定。

3. 輸入您的使用者名稱和密碼以登入閘道本機主控台。如需詳細資訊，請參閱[登入檔案閘道本機主控台](#)。

登入後，會顯示 AWS 設備啟用 - 組態功能表。您可以從選單選項中選取來執行閘道組態任務。如需詳細資訊，請參閱[在虛擬機器本機主控台上執行任務](#)。

## 使用 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. 確定閘道 VM 已開啟。

**Note**

如果您的閘道 VM 已開啟，應用程式視窗左側的 VM 瀏覽器面板中會出現綠色箭頭圖示與 VM 圖示。如果您的閘道 VM 未開啟，您可以選擇應用程式視窗頂端工具列上的綠色開啟電源圖示來開啟。

3. 選擇應用程式視窗右側主要資訊面板中的主控台索引標籤。

幾分鐘後，AWS 設備閘道本機主控台會提示您登入以變更網路組態和其他設定。

**Note**

若要從主控台視窗釋出該游標，請按Ctrl+Alt。

4. 輸入您的使用者名稱和密碼以登入閘道本機主控台。如需詳細資訊，請參閱[登入檔案閘道本機主控台](#)。

登入後，會顯示AWS 設備啟用 - 組態功能表。您可以從選單選項中選取來執行閘道組態任務。如需詳細資訊，請參閱[在虛擬機器本機主控台上執行任務](#)。

## 使用 Microsoft Hyper-V 存取閘道本機主控台

### 存取您閘道的本機主控台 (Microsoft Hyper-V)

1. 從 Microsoft Hyper-V Manager 應用程式視窗左側的虛擬機器面板中選取您的閘道設備虛擬機器。
2. 確定已開啟閘道。

**Note**

如果您的閘道 VM 已開啟，Running 會顯示在應用程式視窗左側虛擬機器面板中 VM 的狀態欄中。如果您的閘道 VM 未開啟，您可以在應用程式視窗右側的動作面板中選擇開始來開啟它。

3. 從動作面板選擇連線。

Virtual Machine Connection (虛擬機器連線) 視窗即會顯示。若出現身分驗證視窗，請輸入虛擬化管理程序管理員提供給您的登入憑證。

幾分鐘後，AWS 設備閘道本機主控台會提示您登入以變更網路組態和其他設定。

4. 輸入您的使用者名稱和密碼以登入閘道本機主控台。如需詳細資訊，請參閱[登入檔案閘道本機主控台](#)。

登入後，會顯示AWS 設備啟用 - 組態功能表。您可以從選單選項中選取 來執行閘道組態任務。如需詳細資訊，請參閱[在虛擬機器本機主控台上執行任務](#)。

## 在虛擬機器本機主控台上執行任務

對於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 File Gateway 本機主控台](#) - 了解如何登入本機主控台，您可以在其中設定閘道網路設定和變更預設密碼。
- [設定 HTTP 代理](#) - 了解如何設定 Storage Gateway 透過代理伺服器路由所有 AWS 端點流量。
- [設定您的閘道網路設定](#) - 了解如何將閘道設定為使用 DHCP 或靜態 IP 地址。
- [測試閘道的網路連線](#) - 了解如何使用閘道本機主控台來測試網路連線。
- [檢視閘道系統資源狀態](#) - 了解如何檢查閘道的虛擬 CPU 核心、根磁碟區大小和 RAM。
- [為您的閘道設定網路時間通訊協定 \(NTP\) 伺服器](#) - 了解如何檢視和編輯網路時間通訊協定 (NTP) 伺服器組態，並將閘道上的時間與 Hypervisor 主機同步。
- [在本機主控台上執行 Storage Gateway 命令](#) - 了解如何執行本機主控台命令來執行任務，例如儲存路由表 支援、連線至 等。

## 登入 File Gateway 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 VM 本機主控台，您可以使用暫時登入憑證登入。這些臨時登入資料可讓您存取功能表，您可以在其中設定閘道網路設定，並從本機主控台變更密碼。初始使用者名稱為 admin，臨時密碼為 password。您必須在第一次登入時變更密碼。

### 變更臨時密碼

1. 在AWS 設備啟用 - 組態主功能表上，輸入閘道主控台的對應數字。
2. 執行 passwd 命令。如需如何執行命令的資訊，請參閱 [在本機主控台上執行 Storage Gateway 命令](#)。

## 從 Storage Gateway 主控台設定本機主控台密碼

您也可以從 Storage Gateway Web 型主控台管理本機主控台的密碼。使用 Web 主控台進行的任何成功密碼更新都會覆寫閘道 VM 本機主控台所使用的密碼，如果您從未在本機登入，包括臨時密碼。如果目前無法透過網路存取閘道，密碼更新程序將會失敗。

### 在 Storage Gateway 主控台中設定本機主控台密碼

1. 前往 <https://console.aws.amazon.com/storagegateway/home> 開啟 Storage Gateway 主控台。
2. 在導覽窗格中，選擇閘道，然後選取您要為其設定新密碼的閘道。
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)。

您的新密碼會取代目前的密碼。Storage Gateway 服務不會儲存、存放或記錄密碼，而是安全地透過加密頻道將其傳輸到安全存放的 VM。

#### Note

密碼可以由鍵盤上的任何字元組成，長度可以是 1-512 個字元。

## 設定 HTTP 代理

檔案閘道支援 HTTP 代理的組態。

#### Note

File Gateways 支援的唯一代理組態是 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。這麼做之後，Storage Gateway 會透過代理伺服器路由所有 AWS 端點流量。即便使用 HTTP 代理，閘道與端點之間的通訊也會加密。如需閘道之網路需求的資訊，請參閱[網路與防火牆需求](#)。

### 設定檔案閘道的 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. 從 AWS 裝置啟用 - 組態主功能表中，輸入對應的數字以選取設定 HTTP 代理。
  3. 從 AWS 裝置啟用 HTTP 代理組態功能表中，輸入您要執行之任務的對應數字：
    - 設定 HTTP 代理：您需要提供主機名稱和連接埠才能完成設定。
    - 檢視目前的 HTTP 代理組態：如未設定 HTTP 代理，即會顯示訊息：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：即會顯示訊息：HTTP Proxy Configuration Removed。
  4. 重新啟動您的 VM 以套用您的 HTTP 組態設定。

## 設定您的閘道網路設定

閘道的預設網路組態為動態主機組態協定 (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. 從 AWS 設備啟用 - 組態主功能表中，輸入對應的數字以選取網路組態。
3. 從網路組態功能表中，執行下列其中一個任務：

執行此任務	執行此作業
取得網路轉接器的相關資訊	

執行此任務	執行此作業
	<p>輸入對應的數字以選取描述介面卡。</p> <p>隨即出現轉接器名稱清單，並提示您輸入轉接器名稱，例如 <b>eth0</b>。若您指定的轉接器為使用中，將顯示轉接器的下列資訊：</p> <ul style="list-style-type: none"><li>• 媒體存取控制 (MAC) 地址</li><li>• IP 地址</li><li>• 網路遮罩</li><li>• 閘道 IP 地址</li><li>• DHCP 已啟用狀態</li></ul> <p>您可以在設定靜態 IP 地址或設定閘道的預設轉接器時，使用此處列出的轉接器名稱。</p>
設定 DHCP 路由	<p>輸入對應的數字以選取設定 DHCP。</p> <p>系統會提示您設定網路界面使用 DHCP。</p>

執行此任務	執行此作業
為閘道設定靜態 IP 地址	<p>輸入對應的數字以選取設定靜態 IP。</p> <p>系統會提示您輸入下列資訊來設定靜態 IP：</p> <ul style="list-style-type: none"><li>• 網路轉接器名稱</li><li>• IP 地址</li><li>• 網路遮罩</li><li>• 預設閘道地址</li><li>• 主要網域名稱服務 (DNS) 地址</li><li>• 輔助 DNS 地址</li></ul> <div data-bbox="829 1066 1507 1381" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> <b>Important</b></p><p>如果您的閘道已啟用，您必須將其關閉並在 Storage Gateway 主控台重新啟動，設定才能生效。如需詳細資訊，請參閱<a href="#">關閉您的閘道 VM</a>。</p></div> <p>如果您的閘道使用多個網路介面，您必須將所有作用中介面設定為使用 DHCP 或靜態 IP 地址。</p> <p>例如，假設您的閘道 VM 使用兩個設定為 DHCP 的介面。如果您稍後將一個介面設定為靜態 IP，另一個介面將停用。在此情況下，若要啟用介面，您必須將其設定為靜態 IP。</p>

執行此任務	執行此作業
設定閘道的主機名稱	<p>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。</p> <p>輸入對應的數字以選取設定主機名稱。</p> <p>系統會提示您選擇閘道要使用您指定的靜態主機名稱，還是透過 DHCP 或 rDNS 自動取得主機名稱。</p> <p>如果您選取靜態，系統會提示您提供靜態主機名稱，例如 <code>testgateway.example.com</code>。輸入 <code>y</code> 以套用組態。</p> <div data-bbox="829 814 1507 1178" style="border: 1px solid #add8e6; border-radius: 15px; padding: 10px;"><p> <b>Note</b></p><p>如果您為閘道設定靜態主機名稱，請確定提供的主機名稱位於閘道加入的網域中。您還必須在 DNS 系統中建立 A 記錄，將閘道的 IP 地址指向其靜態主機名稱。</p></div>
檢視閘道的主機名稱組態	<p>輸入對應的數字以選取檢視主機名稱組態。</p> <p>隨即顯示閘道的主機名稱、查詢模式、網域和 Active Directory 領域。</p>

執行此任務	執行此作業
重設所有閘道的網路組態為 DHCP	<p>輸入對應的數字以選取全部重設為 DHCP。</p> <p>所有的網路界面皆設定為使用 DHCP。</p> <div data-bbox="829 415 1507 730" style="border: 1px solid #f08080; padding: 10px;"><p> <b>Important</b></p><p>如果您的閘道已啟用，您必須將其關閉並在 Storage Gateway 主控台重新啟動您的閘道，設定才能生效。如需詳細資訊，請參閱<a href="#">關閉您的閘道 VM</a>。</p></div>
設定閘道的預設路由轉接器	<p>輸入對應的數字以選取設定預設介面卡。</p> <p>會顯示閘道的可用轉接器，並提示您選擇其中一個轉接器，例如 <b>eth0</b>。</p>
編輯閘道的 DNS 組態	<p>輸入對應的數字以選取編輯 DNS 組態。</p> <p>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。</p>
檢視閘道的 DNS 組態	<p>輸入對應的數字以選取檢視 DNS 組態。</p> <p>隨即顯示主要和次要 DNS 名稱伺服器的可用轉接器。</p> <div data-bbox="829 1549 1507 1766" style="border: 1px solid #add8e6; padding: 10px;"><p> <b>Note</b></p><p>對於有些版本的 VMware Hypervisor，您可以在此選單中編輯轉接器組態。</p></div>

執行此任務	執行此作業
檢視路由表	<p>輸入對應的數字以選擇檢視路線。</p> <p>隨即顯示閘道的預設路由。</p>

## 測試閘道的網路連線

您可使用閘道的本機主控台測試網路連線。此測試在您故障診斷閘道的網路問題時，很有幫助。

### 測試閘道的網路連線

#### 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 裝置啟用 - 組態主功能表中，輸入對應的數字以選取測試網路連線。

如果您的閘道已經啟動，連線測試會立即開始。對於尚未啟用的閘道，您必須指定端點類型和 AWS 區域，如下列步驟所述。

- 如果您的閘道尚未啟動，請輸入對應的數字以選取閘道的端點類型。
- 如果您選取公有端點類型，請輸入對應的數字來選取您要測試 AWS 區域的。如需可與 Storage Gateway 搭配使用的支援 AWS 和服務端點 AWS 區域清單，請參閱中的[AWS Storage Gateway 端點和配額](#) AWS 一般參考。

隨著測試的進行，每個端點都會顯示 [通過] 或 [失敗]，指示連線的狀態，如下所示：

訊息	Description
[通過]	Storage Gateway 具有網路連線能力。
[失敗]	Storage Gateway 沒有網路連線能力。

## 檢視閘道系統資源狀態

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. 從 AWS 設備啟用 - 組態主功能表中，輸入相應數字以選取檢視系統資源檢查的結果。

每個資源都會顯示 [確定]、[警告] 或 [失敗]，以指示資源的狀態，如下所示：

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

## 為您的閘道設定網路時間通訊協定 (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. 從AWS 設備啟用 - 組態主功能表中，輸入對應的數字以選取系統時間管理。

### 3. 從系統時間管理功能表中，輸入對應的數字來執行下列其中一個任務。

執行此任務	執行此作業
檢視並同步 VM 時間與 NTP 伺服器時間。	<p>輸入對應的數字以選取檢視和同步系統時間。</p> <p>即顯示 VM 上目前的時間。檔案閘道會決定與閘道 VM 之間的時間差異，而 NTP 伺服器時間會提示您同步 VM 時間與 NTP 時間。</p> <p>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。</p> <p>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<a href="#">同步 VM 時間與 VMware 主機時間</a>。</p> <p>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<a href="#">同步 VM 時間與 Hyper-V 或 Linux KVM 主機時間</a>。</p>

執行此任務	執行此作業
編輯 NTP 伺服器組態	<p>對於在 KVM 上部署的閘道，您可以使用 KVM 的 <code>virsh</code> 命令列界面來檢查並同步虛擬機器時間。</p> <p>輸入對應的數字以選取編輯 NTP 組態。</p> <p>系統會提示您提供偏好的和次要的 NTP 伺服器。</p>
檢視 NTP 伺服器組態	<p>輸入對應的數字以選取檢視 NTP 組態。</p> <p>隨即顯示您的 NTP 伺服器組態。</p>


## 在本機主控台上執行 Storage Gateway 命令

Storage Gateway 中的 VM 本機主控台可協助提供用於設定和診斷閘道問題的安全環境。使用本機主控台命令，您可以執行維護任務，例如儲存路由表 支援、連線至 等。

### 執行組態或診斷命令

- 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](#)。
- 從 AWS 設備啟用 - 設定主功能表中，輸入對應的數字以選取閘道主控台。
- 在閘道主控台命令提示字元中，輸入 **h**。

該主控台會顯示可用命令功能表與可用的命令。

命令	函式
dig	從挖掘中收集輸出以進行 DNS 疑難排解。
exit	傳回組態功能表。
h	顯示可用的命令清單。
ifconfig	檢視或設定網路介面。  <div data-bbox="834 569 1507 890" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p> <b>Note</b> 建議您使用 Storage Gateway 主控台或專用的本機主控台功能表選項來設定網路或 IP 設定。如需說明，請參閱<a href="#">設定閘道網路設定</a>。</p> </div>
ip	顯示/操作路由、裝置和通道。  <div data-bbox="834 999 1507 1320" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p> <b>Note</b> 建議您使用 Storage Gateway 主控台或專用的本機主控台功能表選項來設定網路或 IP 設定。如需說明，請參閱<a href="#">設定閘道網路設定</a>。</p> </div>
iptables	IPv4 封包篩選和 NAT 的管理工具。
ncport	測試網路上特定 TCP 連接埠的連線。
nping	從 nping 收集輸出以進行網路疑難排解。
開放式支援通道	連線至 AWS Support。如需如何開啟 AWS 支援存取的指示，請參閱診斷 <a href="#">您希望 AWS Support 協助對 EC2 閘道進行故障診斷</a> 。
passwd	更新身份驗證令牌。

命令	函式
save-iptables	持續存取 IP 資料表。
save-routing-table	儲存新增的路由表項目。
tcptraceroute	將 TCP 流量上的追蹤路由輸出收集到目的地。
sslcheck	使用憑證發行者傳回輸出

**Note**

Storage Gateway 使用憑證發行者驗證，不支援 ssl 檢查。如果此命令傳回 aws-appliance@amazon.com 以外的發行者，則應用程式可能會執行 ssl 檢查。在這種情況下，我們建議略過 Storage Gateway 設備的 ssl 檢查。

4. 在閘道主控台命令提示字元中，輸入您要使用之功能的對應指令，然後依照指示進行。

若要了解命令，請在命令提示字元中提示輸入 **man + #####**。

## 在 Amazon EC2 閘道本機主控台上執行任務

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。本節說明如何登入本機主控台以及執行維護任務。

### 主題

- [登入 Amazon EC2 閘道本機主控台](#) - 了解如何使用 Secure Shell (SSH) 用戶端來連接和登入 Amazon EC2 執行個體的閘道本機主控台。
- [透過 HTTP 代理路由部署在 Amazon EC2 上的閘道](#) - 了解如何在 AWS 與部署在 Amazon EC2 執行個體上的閘道之間設定 Socket Secure 第 5 版 (SOCKS5) 代理。
- [測試閘道的網路連線](#) - 了解如何使用閘道本機主控台來測試閘道與各種網路資源之間的網路連線。
- [檢視閘道系統資源狀態](#) - 了解如何使用閘道本機主控台來檢查閘道的虛擬 CPU 核心、根磁碟區大小和 RAM。

- [在本機主控台上執行 Amazon EC2 閘道的 Storage Gateway 命令](#) - 了解如何執行本機主控台命令來執行任務，例如儲存路由表 支援、連線至 等。
- [設定 Amazon EC2 閘道網路設定](#) - 了解如何使用本機主控台來檢視和設定網路設定，例如 Amazon EC2 執行個體上閘道的 DNS 和主機名稱。

## 登入 Amazon EC2 閘道本機主控台

您可以使用 Secure Shell (SSH) 用戶端登入 Amazon EC2 執行個體上的閘道本機主控台。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[連線至您的執行個體](#)。若要以這種方式連線，您需要在啟動執行個體時指定的 SSH 金鑰對。如需 Amazon EC2 金鑰對的詳細資訊，請參閱《[Amazon EC2 使用者指南](#)》中的 [Amazon EC2 金鑰對](#)。Amazon EC2

### 登入至閘道本機主控台

1. 使用 SSH 連線至 Amazon EC2 執行個體，並以管理員使用者身分登入。
2. 登入後，您會看到AWS 設備啟用 - 組態主功能表，您可以從中執行各種任務。

若要了解此項	請參閱此主題
為您的閘道設定 HTTP 代理	<a href="#">透過 HTTP 代理路由部署在 Amazon EC2 上的閘道</a>
為您的閘道設定網路設定	<a href="#">設定 Amazon EC2 閘道網路設定</a>
測試網路連線	<a href="#">測試閘道的網路連線</a>
檢視系統資源檢查	<a href="#">檢視閘道系統資源狀態</a>
執行 Storage Gateway 主控台命令	<a href="#">在本機主控台上執行 Amazon EC2 閘道的 Storage Gateway 命令</a>

若要關閉閘道，請輸入 **0**。

若要結束組態工作階段，請輸入 **X**。

## 透過 HTTP 代理路由部署在 Amazon EC2 上的閘道

Storage Gateway 支援部署在 Amazon EC2 和 AWS 之閘道間的 Socket Secure 5 版 (SOCKS5) 代理組態。

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。這麼做之後，Storage Gateway 會透過代理伺服器路由所有 AWS 端點流量。即便使用 HTTP 代理，閘道與端點之間的通訊也會加密。

### 透過本機代理伺服器路由您的閘道網際網路流量

1. 登入您閘道的本機主控台。如需說明，請參閱[登入 Amazon EC2 閘道本機主控台](#)。
2. 從 AWS 裝置啟用 - 組態主功能表中，輸入對應的數字以選取設定 HTTP 代理。
3. 從 AWS 裝置啟用 HTTP 代理組態功能表中，輸入您要執行之任務的對應數字：
  - 設定 HTTP 代理：您需要提供主機名稱和連接埠才能完成設定。
  - 檢視目前的 HTTP 代理組態：如未設定 HTTP 代理，即會顯示訊息：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：即會顯示訊息：HTTP Proxy Configuration Removed。

## 測試閘道的網路連線

您可使用閘道的本機主控台測試網路連線。此測試在您故障診斷閘道的網路問題時，很有幫助。

### 測試閘道的連線

1. 登入您閘道的本機主控台。如需說明，請參閱[登入 Amazon EC2 閘道本機主控台](#)。
2. 從 AWS 裝置啟用 - 組態主功能表中，輸入對應的數字以選取測試網路連線。

如果您的閘道已經啟動，連線測試會立即開始。對於尚未啟用的閘道，您必須指定端點類型和 AWS 區域，如下列步驟所述。

3. 如果您的閘道尚未啟動，請輸入對應的數字以選取閘道的端點類型。
4. 如果您選取公有端點類型，請輸入對應的數字來選取您要測試 AWS 區域的。如需可與 Storage Gateway 搭配使用的支援 AWS 和服務端點 AWS 區域清單，請參閱中的[AWS Storage Gateway 端點和配額](#) AWS 一般參考。

隨著測試的進行，每個端點都會顯示 [通過] 或 [失敗]，指示連線的狀態，如下所示：

訊息	Description
[通過]	Storage Gateway 具有網路連線能力。
[失敗]	Storage Gateway 沒有網路連線能力。

## 檢視閘道系統資源狀態

檔案閘道啟動時，它會檢查其虛擬 CPU 核心、根磁碟區大小和 RAM。然後，它會判斷可用的系統資源是否足以讓您的閘道正常運作。您可以使用閘道本機主控台檢視系統資源檢查的結果。

### 檢視系統資源檢查的狀態

1. 登入 Amazon EC2 檔案閘道上的本機主控台。如需說明，請參閱[登入 Amazon EC2 閘道本機主控台](#)。
2. 從 AWS 設備啟用 - 組態主功能表中，輸入相應數字以選取檢視系統資源檢查的結果。

閘道本機主控台會顯示 **【OK】**、**【WARNING】** 或 **【FAIL】**，以指出資源的狀態，如下所示：

訊息	Description
[OK]	此資源已通過系統資源檢查。
[警告]	資源不符合建議的需求，但您的閘道可以繼續運作。閘道本機主控台會顯示說明資源檢查結果的訊息。
[失敗]	此資源未符合最低要求。您的閘道可能無法正常運作。閘道本機主控台會顯示說明資源檢查結果的訊息。

本機主控台也會在資源檢查功能表選項旁顯示錯誤和警告的數量。

## 在本機主控台上執行 Amazon EC2 閘道的 Storage Gateway 命令

AWS Storage Gateway 主控台有助於提供安全的環境，以設定和診斷閘道的問題。使用主控台命令，您可以執行維護任務，例如儲存路由表或連線到支援。

## 執行組態或診斷命令

1. 登入您閘道的本機主控台。如需說明，請參閱[登入 Amazon EC2 閘道本機主控台](#)。
2. 從 AWS 設備啟用 - 設定主功能表中，輸入對應的數字以選取閘道主控台。
3. 在閘道主控台命令提示字元中，輸入 **h**。

該主控台會顯示可用命令功能表與可用的命令。

命令	函式
dig	從挖掘中收集輸出以進行 DNS 疑難排解。
exit	傳回組態功能表。
h	顯示可用的命令清單。
ifconfig	檢視或設定網路介面。  <div data-bbox="834 947 1510 1262" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p><b>Note</b> 建議您使用 Storage Gateway 主控台或專用的本機主控台功能表選項來設定網路或 IP 設定。如需說明，請參閱<a href="#">設定閘道網路設定</a>。</p> </div>
ip	顯示/操作路由、裝置和通道。  <div data-bbox="834 1373 1510 1688" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p><b>Note</b> 建議您使用 Storage Gateway 主控台或專用的本機主控台功能表選項來設定網路或 IP 設定。如需說明，請參閱<a href="#">設定閘道網路設定</a>。</p> </div>
iptables	IPv4 封包篩選和 NAT 的管理工具。
ncport	測試網路上特定 TCP 連接埠的連線。

命令	函式
nping	從 nping 收集輸出以進行網路疑難排解。
開放式支援通道	連線至 AWS Support。
save-iptables	持續存取 IP 資料表。
save-routing-table	儲存新增的路由表項目。
tcptraceroute	將 TCP 流量上的追蹤路由輸出收集到目的地。

4. 在閘道主控台命令提示字元中，輸入您要使用之功能的對應指令，然後依照指示進行。

若要了解命令，請在命令提示字元中提示輸入 `man + #####`。

## 設定 Amazon EC2 閘道網路設定

您可以使用閘道本機主控台檢視和設定 Amazon EC2 檔案閘道的網路設定。

### 設定您的網路設定

1. 登入 Amazon EC2 檔案閘道上的本機主控台。如需說明，請參閱 [登入 Amazon EC2 閘道本機主控台](#)。
2. 從 AWS 設備啟用 - 組態主功能表中，輸入對應的數字以選取網路組態。
3. 從 AWS 設備啟用 - 網路組態功能表中，輸入您要執行之任務的對應數字：
  - 編輯 DNS 組態 - 閘道本機主控台會顯示主要和次要 DNS 伺服器的可用轉接器。然後，主控台會提示您提供新的 IP 地址。
  - 檢視 DNS 組態 - 閘道本機主控台會顯示主要和次要 DNS 伺服器的可用轉接器。
  - 設定主機名稱 - 閘道本機主控台會提示您選擇閘道是否將使用您指定的靜態主機名稱，或者是否將透過 DHCP 或 rDNS 自動查詢主機名稱。

#### Note

如果您選擇為閘道設定靜態主機名稱，則必須在 DNS 系統中建立 A 記錄，將閘道的 IP 地址指向其靜態主機名稱。

- 檢視主機名稱組態 - 閘道本機主控台會顯示 Amazon EC2 檔案閘道的主機名稱、擷取模式、網域和 Active Directory 領域。

## 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。您可以使用 Hypervisor 介面關閉內部部署閘道 VMs，並使用 Amazon EC2 主控台關閉 Amazon EC2 執行個體。

### Important

如果您正使用暫時性儲存，且停止然後啟動 Amazon EC2 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。沒有解決此問題的解決方法。唯一的解決方法是刪除閘道並在新 EC2 執行個體上啟用一個新的閘道。

## 將現有的 FSx 檔案閘道取代為新的執行個體

隨著資料和效能需求增加，或者您收到遷移閘道的 AWS 通知，您可以將現有的 FSx File Gateway 取代為新的執行個體。如果您想要將閘道移至更好的主機平台或更新的 Amazon EC2 執行個體，或重新整理基礎伺服器硬體，您可能需要執行此操作。

### Important

僅將這些說明用於遷移執行 1.x 版的閘道設備。您無法使用它們來遷移執行較低版本的閘道設備。

### Note

遷移只能在相同類型的閘道之間執行。例如，您無法將設定或資料從 FSx 檔案閘道遷移至 S3 檔案閘道。

若要將 FSx File Gateway 閘道取代為具有空快取磁碟和新閘道 ID 的新執行個體：

1. 停止寫入現有 FSx File Gateway 的任何應用程式。在新閘道上設定檔案系統關聯之前，請確認監控標籤上的 CachePercentDirty 指標。

2. 執行下列動作，使用 AWS Command Line Interface (AWS CLI) 收集並儲存現有 FSx 檔案閘道和相關聯檔案系統的組態資訊：

- a. 儲存 FSx File Gateway 的閘道組態資訊。

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

此命令會輸出包含閘道相關中繼資料的 JSON 區塊，例如其名稱、網路介面、設定的時區及其狀態（閘道是否正在執行）。

- b. 儲存 FSx File Gateway 的伺服器訊息區塊 (SMB) 設定。

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

此命令會輸出 JSON 區塊，其中包含閘道加入的 Microsoft Active Directory 網域名稱。

- c. 儲存與 FSx File Gateway 相關聯之每個檔案系統的檔案共用資訊：

針對每個相關聯的檔案系統使用以下命令。

```
aws storagegateway describe-file-system-associations --file-system-  
association-arn-list "arn:aws:storagegateway:us-east-2:123456789012:fs-  
association/fsa-987A654B"
```

此命令會輸出包含檔案系統中繼資料的 JSON 區塊，例如其位置 ARN、稽核日誌目的地、快取重新整理屬性、設定的 IP 地址和標籤。

3. 使用與舊閘道相同的設定和組態建立新的 FSx 檔案閘道。如有必要，請參閱您在步驟 2 中儲存的資訊。
4. 使用與舊閘道上設定的檔案系統相同的設定和組態，為新閘道建立新的檔案系統關聯。如有必要，請參閱您在步驟 2 中儲存的資訊。
5. 確認您的新閘道正常運作，然後以最適合您環境的方式，將用戶端從舊檔案系統重新映射/切換到新的檔案系統。
6. 確認您的新閘道正常運作，然後從 Storage Gateway 主控台刪除舊閘道。

**⚠ Important**

刪除 FSx File Gateway 之前，請確定目前沒有應用程式寫入該閘道的快取。如果您刪除使用中的閘道，則資料可能會遺失。

**⚠ Warning**

閘道一旦刪除，就無法還原。

## 7. 刪除舊閘道 VM 或 Amazon EC2 執行個體。

## 刪除您的閘道並移除相關聯的資源

如果您不打算繼續使用閘道，請考慮刪除閘道和其相關聯資源。移除資源可避免產生您不打算繼續使用之資源的費用，並協助降低每月帳單。

當您刪除閘道時，它不會再出現在 AWS Storage Gateway 管理主控台上，而且其系統連線會關閉。所有閘道類型的閘道刪除程序都會相同；不過，根據您要刪除的閘道類型以及在其上部署它的主機，您會遵循特定說明來移除相關聯資源。

您可以使用 Storage Gateway 主控台或以程式設計方式來刪除閘道。您可以在以下內容中找到如何使用 Storage Gateway 主控台刪除閘道的相關資訊。如果您要以程式設計方式刪除閘道，請參閱 [AWS Storage Gateway API 參考資料](#)。

## 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。

**ℹ Note**

針對 Amazon EC2 執行個體上部署的閘道，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. 前往 <https://console.aws.amazon.com/storagegateway/home> 開啟 Storage Gateway 主控台。
2. 選擇閘道，然後選取要刪除的一個或多個閘道。
3. 針對 Actions (動作)，選擇 Delete gateway (刪除閘道)。出現確認對話方塊。

### Warning

執行此步驟之前，請確定目前沒有應用程式寫入至閘道的磁碟區。如果您刪除使用中的閘道，則資料可能會遺失。閘道一旦刪除，就沒有方法可以取回。

4. 確認您要刪除指定的閘道，然後在確認方塊中輸入刪除一詞，然後選擇刪除。
5. (選用) 如果您想要提供有關已刪除閘道的意見回饋，請完成意見回饋對話方塊，然後選擇提交。否則，請選擇略過。

### Important

刪除閘道後，您不再需要支付軟體費用，但 Amazon S3 儲存貯體和 Amazon EC2 執行個體等資源仍會保留。您可以在移除檔案閘道之後移除閘道 Amazon EC2 執行個體。

# 效能和最佳化

本節說明最佳化 File Gateway 效能的指引和最佳實務。

## 主題

- [FSx File Gateway 的基本效能指引](#)
- [最佳化閘道效能](#)
- [最大化 S3 檔案閘道輸送量](#)
- [最佳化 SQL Server 資料庫備份的 S3 檔案閘道](#)

## FSx File Gateway 的基本效能指引

在本節中，您可以找到為 FSx 檔案閘道 VM 佈建硬體的指引。資料表中列出的執行個體組態是範例，並提供參考。

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。

### 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[搭配 EC2 閘道使用暫時性儲存](#)。

您連線到檔案閘道檔案系統中個別目錄的建議大小限制為每個目錄 10,000 個檔案。您可以使用檔案閘道搭配超過 10,000 個檔案的目錄，但效能可能會受到影響。

在下表中，快取命中讀取操作是從快取提供的檔案資料讀取。快取遺漏讀取操作是從 Amazon FSx for Windows File Server 提供的檔案資料進行讀取。

下表顯示 FSx File Gateway 組態範例。

## Windows 用戶端上的 FSx File Gateway 效能

範例組態	通訊協定	寫入輸送量 (檔案大小 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、4000 IOPS  快取磁碟：2 x 2 TiB NVME  最低網路效能： 10 Gbps  CPU：32 vCPU   RAM：244 GB	SMBv3 - 1 個執行緒	162 MiB/秒 (1.4 Gbps)	403 MiB/秒 (3.4 Gbps)	288 MiB/秒 (2.4 Gbps)
	SMBv3 - 8 個執行緒	511 MiB/秒 (4.3 Gbps)	571 MiB/秒 (4.8 Gbps)	567 MiB/秒 (4.8 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。寫入輸送量效能會隨著檔案大小而降低，小型檔案（小於 32MiB）可達到的最高輸送量為每秒 16 個檔案。

## 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)。如需新增磁碟的詳細資訊，請參閱 [設定其他快取儲存](#)。

若要測量輸送量，請使用 ReadBytes 和 WriteBytes 指標搭配 Samples Amazon CloudWatch 統計資料。例如，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 指標不適用於所有閘道。有关网关指标的資訊，請參閱 [監控 FSx 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並行處理從應用程式將資料儲存到本機儲存，以及將此資料上傳至 FSx for Windows File Server。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 支援在閘道主機伺服器中使用 24 CPUs。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 保留 RAM，適用於檔案閘道
  - 16 GiB 保留 RAM，適用於快取大小高達 16 TiB 的閘道
  - 32 GiB RAM，適用於快取大小為 16 TiB 至 32 TiB 的閘道
  - 48 GiB 保留 RAM，適用於快取大小為 32 TiB 至 64 TiB 的閘道
- 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。
- 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

當您佈建閘道磁碟時，強烈建議您不要為使用相同基礎實體儲存磁碟的本機儲存佈建本機磁碟。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與閘道之間的頻寬

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。您可以使用閘道的 ReadBytes 和 WriteBytes 指標來測量總資料輸送量。

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。

FSx File Gateway 上的某些檔案操作，例如頂層資料夾重新命名或許可變更，可能會導致多個檔案操作，導致 FSx for Windows File Server 檔案系統具有高 I/O 負載。如果您的檔案系統沒有足夠的工作負載效能資源，檔案系統可能會刪除[影子複本](#)，因為它會將持續 I/O 的可用性優先於歷史影子複本保留。

在 Amazon FSx 主控台中，檢查監控和效能頁面，查看您的檔案系統是否佈建不足。如果是，您可以切換到 SSD 儲存體、增加輸送量容量或增加 SSD IOPS 來處理工作負載。

## 最大化 S3 檔案閘道輸送量

下列各節說明將 NFS 和 SMB 用戶端、S3 檔案閘道和 Amazon S3 之間的輸送量最大化的最佳實務。每個區段中提供的指引會逐步提升整體輸送量。雖然這些建議都不需要，而且不是相互依存的，但它

們是以支援用來測試和調整 S3 File Gateway 實作的邏輯方式選取和排序。當您實作和測試這些建議時，請記住每個 S3 File Gateway 部署都是唯一的，因此您的結果可能會有所不同。

S3 File Gateway 提供檔案界面，使用業界標準的 NFS 或 SMB 檔案通訊協定來存放和擷取 Amazon S3 物件，並在檔案和物件之間進行原生的 1:1 映射。您可以將 S3 檔案閘道部署為 VMware、Microsoft Hyper-V 或 Linux KVM 環境中的內部部署虛擬機器，或將 AWS 雲端部署為 Amazon EC2 執行個體。S3 File Gateway 並非設計做為完整的企業 NAS 替換。S3 File Gateway 會模擬檔案系統，但不是檔案系統。使用 Amazon S3 作為耐用的後端儲存會為每個 I/O 操作產生額外的額外負荷，因此針對現有的 NAS 或檔案伺服器評估 S3 File Gateway 效能不是同等的比較。

## 在與用戶端相同的位置部署閘道

建議您將 S3 File Gateway 虛擬設備部署到實體位置，並在其與 NFS 或 SMB 用戶端之間盡可能減少網路延遲。選擇閘道的位置時，請考慮下列事項：

- 降低閘道的網路延遲有助於改善 NFS 或 SMB 用戶端的效能。
- S3 檔案閘道旨在容忍閘道與 Amazon S3 之間的網路延遲高於閘道與用戶端之間的網路延遲。
- 對於在 Amazon EC2 中部署的 S3 檔案閘道執行個體，我們建議將閘道和 NFS 或 SMB 用戶端保留在相同的置放群組中。如需詳細資訊，請參閱 [《Amazon Elastic Compute Cloud 使用者指南》中的 Amazon EC2 執行個體的置放群組](#)。

## 減少因磁碟緩慢所造成的瓶頸

我們建議您監控 `IoWaitPercent` CloudWatch 指標，以識別由於 S3 檔案閘道上的儲存磁碟緩慢而導致的效能瓶頸。嘗試最佳化磁碟相關的效能問題時，請考慮下列事項：

- `IoWaitPercent` 報告 CPU 從根磁碟或快取磁碟等待回應的時間百分比。
- 當 `IoWaitPercent` 大於 5-10% 時，這通常表示由於磁碟效能不佳而導致閘道效能瓶頸。此指標應盡可能接近 0%，這表示閘道永遠不會在磁碟上等待，這有助於最佳化 CPU 資源。
- 您可以檢查 Storage Gateway 主控台的 `IoWaitPercent` 監控索引標籤，或設定建議的 CloudWatch 警示，以便在指標峰值超過特定閾值時自動通知您。如需詳細資訊，請參閱 [為您的閘道建立建議的 CloudWatch 警示](#)。
- 我們建議將 NVMe 或 SSD 用於閘道的根磁碟和快取磁碟，以將降至最低 `IoWaitPercent`。

## 調整 CPU、RAM 和快取磁碟的虛擬機器資源配置

嘗試最佳化 S3 檔案閘道的輸送量時，請務必將足夠的資源配置給閘道 VM，包括 CPU、RAM 和快取磁碟。4 個 CPUs、16GB RAM 和 150GB 快取儲存體的最低虛擬資源需求通常僅適用於較小的工作負載。為較大的工作負載配置虛擬資源時，我們建議下列事項：

- 根據 S3 檔案閘道產生的典型 CPUs 使用量，將配置的 CPU 數量增加到 16 到 48 之間。您可以使用 UserCpuPercent 指標監控 CPU 用量。如需詳細資訊，請參閱[了解閘道指標](#)。
- 將配置的 RAM 增加到 32 到 64 GB 之間。

### Note

S3 檔案閘道無法使用超過 64 GB 的 RAM。

- 針對根磁碟和快取磁碟使用 NVMe 或 SSD，並調整快取磁碟的大小，以符合您計劃寫入閘道的尖峰工作資料集。如需詳細資訊，請參閱官方 Amazon Web Services YouTube 頻道上的[S3 File Gateway 快取大小調整最佳實務](#)。
- 將至少 4 個虛擬快取磁碟新增至閘道，而不是使用單一大型磁碟。即使多個虛擬磁碟共用相同的基礎實體磁碟，也可以改善效能，但當虛擬磁碟位於不同的基礎實體磁碟時，改善通常會更大。

例如，如果您想要部署 12TB 的快取，您可以使用下列其中一個組態：

- 4 x 3 TB 快取磁碟
- 8 x 1.5 TB 快取磁碟
- 12 x 1 TB 快取磁碟

除了效能之外，這還允許在一段時間內更有效率地管理虛擬機器。隨著工作負載變更，您可以逐步增加快取磁碟的數量和整體快取容量，同時維持每個個別虛擬磁碟的原始大小，以保持閘道完整性。

如需詳細資訊，請參閱[決定本機磁碟儲存量](#)。

將 S3 檔案閘道部署為 Amazon EC2 執行個體時，請考慮下列事項：

- 您選擇的執行個體類型可能會大幅影響閘道效能。Amazon EC2 提供調整 S3 File Gateway 執行個體資源配置的廣泛彈性。
- 如需 S3 檔案閘道的建議 Amazon EC2 執行個體類型，請參閱[Amazon EC2 執行個體類型的需求](#)。

- 您可以變更託管作用中 S3 檔案閘道的 Amazon EC2 執行個體類型。這可讓您輕鬆調整 Amazon EC2 硬體的產生和資源配置，以找到理想的price-to-performance比率。若要變更執行個體類型，請在 Amazon EC2 主控台中使用下列程序：
  1. 停止 Amazon EC2 執行個體。
  2. 變更 Amazon EC2 執行個體類型。
  3. 開啟 Amazon EC2 執行個體的電源。

#### Note

停止託管 S3 檔案閘道的執行個體將暫時中斷檔案共用存取。如有必要，請務必排定維護時段。

- Amazon EC2 執行個體price-to-performance比是指您支付的價格獲得的運算能力。一般而言，較新一代的 Amazon EC2 執行個體提供最佳price-to-performance比，與較舊世代相比，硬體和效能提升的成本相對較低。執行個體類型、區域和用量模式等因素會影響此比率，因此請務必為特定工作負載選取正確的執行個體，以最佳化成本效益。

## 調整 SMB 安全層級

SMBv3 通訊協定允許 SMB 簽署和 SMB 加密，這在效能和安全性方面有一些取捨。若要最佳化輸送量，您可以調整閘道的 SMB 安全層級，以指定要針對用戶端連線強制執行哪些安全功能。如需詳細資訊，請參閱[設定閘道的安全層級](#)。

調整 SMB 安全層級時，請考慮下列事項：

- S3 File Gateway 的預設安全層級是強制加密。此設定會對閘道檔案共享的 SMB 用戶端連線強制執行加密和簽署，這表示從用戶端到閘道的所有流量都會加密。此設定不會影響從閘道到 AWS 的流量，其一律會加密。

閘道會將每個加密用戶端連線限制為單一 vCPU。例如，如果您只有 1 個加密用戶端，則該用戶端將限制為只有 1 個 vCPU，即使有 4 個以上的 vCPUs 配置給閘道。因此，從單一用戶端到 S3 File Gateway 的加密連線輸送量通常會遇到 40-60 MB/s 之間的瓶頸。

- 如果您的安全需求允許更寬鬆的姿勢，您可以將安全層級變更為用戶端交涉，這會停用 SMB 加密並僅強制執行 SMB 簽署。透過此設定，閘道的用戶端連線可以使用多個 vCPUs，這通常會導致輸送量效能提高。

**Note**

變更 S3 檔案閘道的 SMB 安全層級後，您必須等待檔案共用狀態從 Storage Gateway 主控台更新變更為可用，然後中斷連線並重新連接 SMB 用戶端，新設定才會生效。

## 使用多個執行緒和用戶端來平行化寫入操作

使用僅使用一個 NFS 或 SMB 用戶端一次寫入一個檔案的 S3 檔案閘道，很難達到最大輸送量效能，因為從單一用戶端循序寫入是單執行緒操作。反之，我們建議您使用每個 NFS 或 SMB 用戶端的多個執行緒來平行寫入多個檔案，並同時使用多個 NFS 或 SMB 用戶端到您的 S3 檔案閘道，以最大化閘道輸送量。

使用多個執行緒可以大幅提升效能。不過，使用更多執行緒需要更多系統資源，如果閘道的大小不符合增加的負載，可能會對效能產生負面影響。在一般部署中，您可以預期在新增更多執行緒和用戶端時達到更好的輸送量效能，直到您達到閘道的最大硬體和頻寬限制為止。建議您實驗不同的執行緒計數，以找出特定硬體和網路組態的速度和系統資源使用量之間的最佳平衡。

請考慮下列有關可協助您測試執行緒和用戶端組態之常見工具的資訊：

- 您可以使用 robocopy 等工具，將一組檔案複製到閘道上的檔案共享，以測試多執行緒寫入效能。根據預設，robocopy 在複製檔案時使用 8 個執行緒，但您最多可以指定 128 個執行緒。

若要搭配 Robocopy 使用多個執行緒，請將 /MT:n 交換器新增至命令，其中 n 是您要使用的執行緒數目。例如：

```
robocopy C:\source D:\destination /MT:64
```

此命令將使用 64 個執行緒進行複製操作。

**Note**

我們不建議使用 Windows Explorer 在測試最大輸送量時拖放檔案，因為此方法僅限於單一執行緒並依序複製檔案。

如需詳細資訊，請參閱 Microsoft Learn 網站上的 [robocopy](#)。

- 您也可以使用常見的儲存基準工具進行測試，例如 DISKSPD 或 FIO。這些工具可以選擇調整執行緒數量、I/O 深度和其他參數，以符合您的特定工作負載需求。

DiskSpd 可讓您使用 `-t` 參數控制執行緒的數量。例如：

```
diskspd -c10G -d300 -r -w50 -t64 -o32 -b1M -h -L C:\testfile.dat
```

此範例命令會執行下列動作：

- 建立 10GB 測試檔案 (`-c1G`)
- 執行 300 秒 (`-d300`)
- 使用 50% 讀取 50% 寫入執行隨機 I/O 測試 (`-r -w50`)
- 使用 64 個執行緒 (`-t64`)
- 將佇列深度設定為每個執行緒 32 個 (`-o32`)
- 使用 1MB 區塊大小 (`-b1M`)
- 停用硬體和軟體快取 (`-h -L`)

如需詳細資訊，請參閱 Microsoft Learn 網站上的[使用 DISKSPD 測試工作負載儲存效能](#)。

- FIO 使用 `numjobs` 參數來控制平行執行緒的數量。例如：

```
fio --name=mixed_test --rw=randrw --rwmixread=70 --bs=1M -- iodepth=64  
--size=10G --runtime=300 --numjobs=64 --ioengine=libaio --direct=1 --  
group_reporting
```

此範例命令會執行下列動作：

- 執行隨機 I/O 測試 (`--rw=randrw`)
- 執行 70% 的讀取和 30% 的寫入 (`--rwmixread=70`)
- 使用 1MB 區塊大小 (`--bs=1M`)
- 將 I/O 深度設定為 64 (`--iodepth=64`)
- 在 10 GB 檔案上進行測試 (`--size=10G`)
- 執行 5 分鐘 (`--runtime=300`)
- 建立 64 個平行任務 (執行緒) (`--numjobs=64`)
- 使用非同步 I/O 引擎 (`--ioengine=libaio`)
- 分組結果以更輕鬆地分析 (`--group_reporting`)

## 關閉自動快取重新整理

自動化快取重新整理功能可讓您的 S3 檔案閘道自動重新整理其中繼資料，這有助於擷取使用者或應用程式對檔案集所做的任何變更，方法是直接寫入 Amazon S3 儲存貯體，而不是透過閘道。如需詳細資訊，請參閱[重新整理 Amazon S3 儲存貯體物件快取](#)。

若要最佳化閘道輸送量，建議您在部署中關閉此功能，其中所有讀取和寫入 Amazon S3 儲存貯體的作業都會透過 S3 檔案閘道執行。

設定自動快取重新整理時，請考慮下列事項：

- 如果您需要使用自動快取重新整理，因為部署中的使用者或應用程式偶爾會直接寫入 Amazon S3，則建議您設定重新整理之間的最長時間間隔，這仍然適合您業務需求。較長的快取重新整理間隔有助於減少閘道在瀏覽目錄或修改檔案時需要執行的中繼資料操作數目。

例如：如果工作負載可容忍，請將自動快取重新整理設定為 24 小時，而不是 5 分鐘。

- 最短時間間隔為 5 分鐘。間隔上限為 30 天。
- 如果您選擇設定非常短的快取重新整理間隔，建議您測試 NFS 和 SMB 用戶端的目錄瀏覽體驗。重新整理閘道快取所需的時間可能會大幅增加，具體取決於 Amazon S3 儲存貯體中的檔案和子目錄數量。

## 增加 Amazon S3 上傳程式執行緒的數量

根據預設，S3 File Gateway 會為 Amazon S3 資料上傳開啟 8 個執行緒，這可為大多數典型部署提供足夠的上傳容量。不過，閘道可能會以高於標準 8 執行緒容量上傳至 Amazon S3 的速率從 NFS 和 SMB 用戶端接收資料，這可能會導致本機快取達到其儲存限制。

在特定情況下，支援可以將閘道的 Amazon S3 上傳執行緒集區計數從 8 增加到 40，這允許平行上傳更多資料。根據頻寬和部署特有的其他因素，這可以大幅提高上傳效能，並有助於減少支援工作負載所需的快取儲存量。

建議使用 CachePercentDirty CloudWatch 指標來監控儲存在本機閘道快取磁碟上尚未上傳至 Amazon S3 的資料量，並聯絡支援以協助判斷增加上傳執行緒集區計數是否可能改善 S3 檔案閘道的輸送量。如需詳細資訊，請參閱[了解閘道指標](#)。

**Note**

此設定會使用其他閘道 CPU 資源。我們建議您監控閘道 CPU 用量，並視需要增加配置的 CPU 資源。

## 增加 SMB 逾時設定

當 S3 File Gateway 將大型檔案複製到 SMB 檔案共享時，SMB 用戶端連線可能會在長時間後逾時。

我們建議您將 SMB 用戶端的 SMB 工作階段逾時設定延長至 20 分鐘或以上，具體取決於檔案大小和閘道的寫入速度。預設值為 300 秒或 5 分鐘。如需詳細資訊，請參閱[您的閘道備份任務失敗，或寫入閘道時發生錯誤](#)。

## 為相容應用程式開啟機會鎖定

預設會為每個新的 S3 檔案閘道啟用伺機鎖定或「oplocks」。搭配相容的應用程式使用 oplock 時，用戶端會將多個較小的操作批次處理為較大的操作，這對於用戶端、閘道和網路更有效率。如果您使用利用用戶端本機快取的應用程式，例如 Microsoft Office、Adobe Suite 等，我們建議您保持開啟機會鎖定，因為它可以大幅改善效能。

如果您關閉機會鎖定，支援封鎖的應用程式通常會更慢地開啟大型檔案 (50 MB 或更大)。發生此延遲是因為閘道以 4 KB 部分傳送資料，這會導致高 I/O 和低輸送量。

## 根據工作檔案集的大小調整閘道容量

閘道容量參數會指定閘道在其本機快取中存放中繼資料的檔案數目上限。根據預設，閘道容量會設定為小型，這表示閘道最多可存放 500 萬個檔案的中繼資料。預設設定適用於大多數工作負載，即使 Amazon S3 中有數億或甚至數十億個物件，因為在一般部署中的指定時間只會主動存取一小部分的檔案。此檔案群組稱為「工作集」。

如果您的工作負載定期存取一組大於 500 萬的工作檔案，則閘道將需要頻繁執行快取移出，這是存放在 RAM 中並保留在根磁碟上的小型 I/O 操作。這可能會對閘道效能產生負面影響，因為閘道會從 Amazon S3 擷取新資料。

您可以監控 IndexEvictions 指標，以判斷從快取移出中繼資料的檔案數量，為新項目騰出空間。如需詳細資訊，請參閱[了解閘道指標](#)。

我們建議您使用 UpdateGatewayInformation API 動作來增加閘道容量，以對應一般工作集中的檔案數量。如需詳細資訊，請參閱[UpdateGatewayInformation](#)。

**Note**

增加閘道容量需要額外的 RAM 和根磁碟容量。

- 小型 (500 萬個檔案) 需要至少 16 GB 的 RAM 和 80 GB 的根磁碟。
- 中型 (1,000 萬個檔案) 需要至少 32 GB 的 RAM 和 160 GB 的根磁碟。
- 大型 (2,000 萬個檔案) 需要 64 GB 的 RAM 和 240 GB 的根磁碟。

**Important**

無法減少閘道容量。

## 為更大的工作負載部署多個閘道

我們建議您盡可能將工作負載分割到多個閘道，而不是在單一大型閘道上合併多個檔案共用。例如，您可以在一個閘道上隔離一個重度使用的檔案共享，同時將較不常用的檔案共享分組到另一個閘道上。

規劃具有多個閘道和檔案共享的部署時，請考慮下列事項：

- 單一閘道上的檔案共用數目上限為 50，但閘道管理的檔案共用數目可能會影響閘道的效能。如需詳細資訊，請參閱[具有多個檔案共享之閘道的效能指引](#)。
- 每個 S3 檔案閘道上的資源會跨所有檔案共用共用，無需分割。
- 具有大量用量的單一檔案共享可能會影響閘道上其他檔案共享的效能。

**Note**

我們不建議從多個閘道建立多個映射至相同 Amazon S3 位置的檔案共用，除非其中至少一個是唯讀的。

從多個閘道同時寫入相同的檔案會被視為多寫入器案例，這可能會導致資料完整性問題。

## 最佳化 SQL Server 資料庫備份的 S3 檔案閘道

資料庫備份是 S3 File Gateway 的常見建議使用案例，它透過將資料庫備份儲存在 Amazon S3 中來提供經濟實惠的短期和長期保留，並能夠根據需要生命週期以降低成本儲存層。透過此解決方案，您可以使用 SQL Server Management Studio 和 Oracle RMAN 等內建工具，減少企業備份應用程式的需求。

下列各節說明調整 S3 File Gateway 部署的最佳實務，以最佳化效能，並為數百 TB 的 SQL 資料庫備份提供符合成本效益的支援。每個區段中提供的指引會逐步提升整體輸送量。雖然這些建議都不需要，而且不是相互依存的，但它們是以支援用來測試和調整 S3 File Gateway 實作的邏輯方式選取和排序。當您實作和測試這些建議時，請記住每個 S3 File Gateway 部署都是唯一的，因此您的結果可能會有所不同。

S3 File Gateway 提供檔案界面，使用業界標準的 NFS 或 SMB 檔案通訊協定來存放和擷取 Amazon S3 物件，並在檔案和物件之間進行原生的 1:1 映射。您可以將 S3 檔案閘道部署為 VMware、Microsoft Hyper-V 或 Linux KVM 環境中的內部部署虛擬機器，或將 AWS 雲端部署為 Amazon EC2 執行個體。S3 File Gateway 並非設計做為完整的企業 NAS 替換。S3 File Gateway 會模擬檔案系統，但不是檔案系統。使用 Amazon S3 作為耐用的後端儲存會為每個 I/O 操作產生額外的額外負荷，因此針對現有的 NAS 或檔案伺服器評估 S3 File Gateway 效能不是同等的比較。

### 在與 SQL Server 相同的位置部署閘道

建議您將 S3 File Gateway 虛擬設備部署在實體位置，並在其與 SQL 伺服器之間盡可能減少網路延遲。選擇閘道的位置時，請考慮下列事項：

- 降低閘道的網路延遲有助於改善 SMB 用戶端的效能，例如 SQL 伺服器。
- S3 檔案閘道旨在容忍閘道與 Amazon S3 之間的網路延遲高於閘道與用戶端之間的網路延遲。
- 對於在 Amazon EC2 中部署的 S3 檔案閘道執行個體，我們建議將閘道和 SQL 伺服器保留在相同的置放群組中。如需詳細資訊，請參閱 [《Amazon Elastic Compute Cloud 使用者指南》中的 Amazon EC2 執行個體的置放群組](#)。

### 減少因磁碟緩慢所造成的瓶頸

我們建議您監控 IoWaitPercent CloudWatch 指標，以識別由於 S3 檔案閘道上的儲存磁碟緩慢而導致的效能瓶頸。嘗試最佳化磁碟相關的效能問題時，請考慮下列事項：

- IoWaitPercent 報告 CPU 從根磁碟或快取磁碟等待回應的時間百分比。
- 當 IoWaitPercent 大於 5-10% 時，這通常表示由於磁碟效能不佳而導致閘道效能瓶頸。此指標應盡可能接近 0%，這表示閘道永遠不會在磁碟上等待，這有助於最佳化 CPU 資源。

- 您可以檢查 Storage Gateway 主控台的 IoWaitPercent 監控索引標籤，或設定建議的 CloudWatch 警示，以便在指標峰值超過特定閾值時自動通知您。如需詳細資訊，請參閱[為您的閘道建立建議的 CloudWatch 警示](#)。
- 我們建議將 NVMe 或 SSD 用於閘道的根磁碟和快取磁碟，以將降至最低 IoWaitPercent。

## 調整 CPU、RAM 和快取磁碟的 S3 檔案閘道虛擬機器資源配置

嘗試最佳化 S3 檔案閘道的輸送量時，請務必將足夠的資源配置給閘道 VM，包括 CPU、RAM 和快取磁碟。4 個 CPUs、16GB RAM 和 150GB 快取儲存體的最低虛擬資源需求通常僅適用於較小的工作負載。為較大的工作負載配置虛擬資源時，我們建議下列事項：

- 根據 S3 檔案閘道產生的典型 CPUs 使用量，將配置的 CPU 數量增加到 16 到 48 之間。您可以使用 UserCpuPercent 指標監控 CPU 用量。如需詳細資訊，請參閱[了解閘道指標](#)。
- 將配置的 RAM 增加到 32 到 64 GB 之間。

### Note

S3 檔案閘道無法使用超過 64 GB 的 RAM。

- 針對根磁碟和快取磁碟使用 NVMe 或 SSD，並調整快取磁碟的大小，以符合您計劃寫入閘道的尖峰工作資料集。如需詳細資訊，請參閱官方 Amazon Web Services YouTube 頻道上的[S3 File Gateway 快取大小調整最佳實務](#)。
- 將至少 4 個虛擬快取磁碟新增至閘道，而不是使用單一大型磁碟。即使多個虛擬磁碟共用相同的基礎實體磁碟，也可以改善效能，但當虛擬磁碟位於不同的基礎實體磁碟時，改善通常會更大。

例如，如果您想要部署 12TB 的快取，您可以使用下列其中一個組態：

- 4 x 3 TB 快取磁碟
- 8 x 1.5 TB 快取磁碟
- 12 x 1 TB 快取磁碟

除了效能之外，這還允許在一段時間內更有效率地管理虛擬機器。隨著工作負載變更，您可以逐步增加快取磁碟的數量和整體快取容量，同時維持每個個別虛擬磁碟的原始大小，以保持閘道完整性。

如需詳細資訊，請參閱[決定本機磁碟儲存量](#)。

將 S3 檔案閘道部署為 Amazon EC2 執行個體時，請考慮下列事項：

- 您選擇的執行個體類型可能會大幅影響閘道效能。Amazon EC2 提供調整 S3 File Gateway 執行個體資源配置的廣泛彈性。
- 如需 S3 檔案閘道的建議 Amazon EC2 執行個體類型，請參閱 [Amazon EC2 執行個體類型的需求](#)。
- 您可以變更託管作用中 S3 檔案閘道的 Amazon EC2 執行個體類型。這可讓您輕鬆調整 Amazon EC2 硬體的產生和資源配置，以找到理想的price-to-performance比率。若要變更執行個體類型，請在 Amazon EC2 主控台中使用下列程序：
  1. 停止 Amazon EC2 執行個體。
  2. 變更 Amazon EC2 執行個體類型。
  3. 開啟 Amazon EC2 執行個體的電源。

#### Note

停止託管 S3 檔案閘道的執行個體將暫時中斷檔案共用存取。如有必要，請務必排定維護時段。

- Amazon EC2 執行個體price-to-performance比是指您支付的價格獲得的運算能力。一般而言，較新一代的 Amazon EC2 執行個體提供最佳price-to-performance比，與較舊世代相比，硬體和效能提升的成本相對較低。執行個體類型、區域和使用模式等因素會影響此比率，因此請務必為特定工作負載選取正確的執行個體，以最佳化成本效益。

## 透過調整 S3 檔案閘道的安全層級來改善 SMB 用戶端輸送量

SMBv3 通訊協定允許 SMB 簽署和 SMB 加密，這在效能和安全性方面有一些取捨。若要最佳化輸送量，您可以調整閘道的 SMB 安全層級，以指定要針對用戶端連線強制執行哪些安全功能。如需詳細資訊，請參閱[設定閘道的安全層級](#)。

調整 SMB 安全層級時，請考慮下列事項：

- S3 File Gateway 的預設安全層級是強制加密。此設定會對閘道檔案共享的 SMB 用戶端連線強制執行加密和簽署，這表示從用戶端到閘道的所有流量都會加密。此設定不會影響從閘道到 AWS 的流量，其一律會加密。

閘道會將每個加密用戶端連線限制為單一 vCPU。例如，如果您只有 1 個加密用戶端，則該用戶端將限制為只有 1 個 vCPU，即使有 4 個以上的 vCPUs 配置給閘道。因此，從單一用戶端到 S3 File Gateway 的加密連線輸送量通常會遇到 40-60 MB/s 之間的瓶頸。

- 如果您的安全需求允許更輕鬆的姿勢，您可以將安全層級變更為用戶端交涉，這會停用 SMB 加密並僅強制執行 SMB 簽署。透過此設定，開道的用戶端連線可以使用多個 vCPUs，這通常會導致輸送量效能提高。

#### Note

變更 S3 檔案開道的 SMB 安全層級後，您必須等待檔案共用狀態從 Storage Gateway 主控台更新變更為可用，然後中斷連線並重新連接 SMB 用戶端，新設定才會生效。

## 將 SQL 備份分割成多個檔案，以改善 SMB 用戶端輸送量

- 使用一次只寫入一個檔案的 S3 檔案開道，很難達到最大輸送量效能，因為從單一 SQL 伺服器循序寫入是單執行緒操作。反之，我們建議您使用每個 SQL 伺服器的多個執行緒來平行寫入多個檔案，並同時使用多個 SQL 伺服器到您的 S3 檔案開道，以最大化開道輸送量。使用 SQL 備份時，將備份分割成多個檔案可讓每個檔案使用單獨的執行緒，這會同時將多個檔案寫入 S3 檔案開道檔案共享。執行緒越多，可達到的輸送量就越多，最高可達開道的限制。
- SQL Server 支援在單一備份操作期間同時寫入多個檔案。例如，您可以使用 T-SQL 命令或 SQL Server Management Studio (SSMS) 指定多個檔案目的地。每個檔案使用單獨的執行緒，將資料從 SQL 伺服器傳送至開道檔案共享。此方法可提高 I/O 輸送量，大幅改善備份速度和效率。

設定 SQL 伺服器備份時，請考慮下列事項：

- 透過將備份分割為多個檔案，SQL Server 管理員可以最佳化備份時間，並更有效地管理大型資料庫備份。
- 使用的檔案數量取決於伺服器的儲存組態和效能需求。對於大型資料庫，我們建議將備份分成數個較小的檔案，每個檔案介於 10 GB 到 20 GB 之間。
- SQL Server 在備份期間可以寫入多少檔案沒有嚴格的限制，但儲存架構和網路頻寬等實際考量應該會引導此選項。

如需詳細資訊，請參閱：

- [寫入多個檔案以加快 SQL Server 備份速度 43-67%](#)
- [使用檔案開道在 Amazon S3 中輕鬆存放 SQL Server 備份](#)

## 增加 SMB 逾時設定，防止大型檔案複製失敗

當 S3 File Gateway 將大型 SQL 備份檔案複製到 SMB 檔案共享時，SMB 用戶端連線可能會在長時間後逾時。我們建議您將 SQL Server SMB 用戶端的 SMB 工作階段逾時設定延長至 20 分鐘或更久，具體取決於檔案大小和閘道的寫入速度。預設值為 300 秒或 5 分鐘。如需詳細資訊，請參閱[您的閘道備份任務失敗，或寫入閘道時發生錯誤](#)。

## 增加 Amazon S3 上傳程式執行緒的數量

根據預設，S3 File Gateway 會為 Amazon S3 資料上傳開啟 8 個執行緒，這可為大多數典型部署提供足夠的上傳容量。不過，閘道可能會以高於標準 Amazon S3 執行緒容量的速率從 SQL 伺服器接收資料，這可能會導致本機快取達到其儲存限制。

在特定情況下，支援 可以將閘道的 Amazon S3 上傳執行緒集區計數從 8 增加到 40，這允許平行上傳更多資料。根據頻寬和部署特有的其他因素，這可以大幅提高上傳效能，並有助於減少支援工作負載所需的快取儲存量。

建議使用 CachePercentDirty CloudWatch 指標來監控儲存在本機閘道快取磁碟上尚未上傳至 Amazon S3 的資料量，並聯絡 支援 以協助判斷增加上傳執行緒集區計數是否可能改善 S3 檔案閘道的輸送量。如需詳細資訊，請參閱[了解閘道指標](#)。

### Note

此設定會使用其他閘道 CPU 資源。我們建議您監控閘道 CPU 用量，並視需要增加配置的 CPU 資源。

## 關閉自動快取重新整理

自動化快取重新整理功能可讓您的 S3 檔案閘道自動重新整理其中繼資料，這有助於擷取使用者或應用程式對檔案集所做的任何變更，方法是直接寫入 Amazon S3 儲存貯體，而不是透過閘道。如需詳細資訊，請參閱[重新整理 Amazon S3 儲存貯體物件快取](#)。

若要最佳化閘道輸送量，建議您在部署中關閉此功能，其中所有讀取和寫入 Amazon S3 儲存貯體的作業都會透過 S3 檔案閘道執行。

設定自動快取重新整理時，請考慮下列事項：

- 如果您需要使用自動快取重新整理，因為部署中的使用者或應用程式偶爾會直接寫入 Amazon S3，則建議您設定重新整理之間的最長時間間隔，這仍然適合您業務需求。較長的快取重新整理間隔有助於減少閘道在瀏覽目錄或修改檔案時需要執行的中繼資料操作數目。

例如：如果工作負載可容忍，請將自動快取重新整理設定為 24 小時，而不是 5 分鐘。

- 最短時間間隔為 5 分鐘。間隔上限為 30 天。
- 如果您選擇設定非常短的快取重新整理間隔，建議您測試 SQL 伺服器的目錄瀏覽體驗。重新整理閘道快取所需的時間可能會大幅增加，具體取決於 Amazon S3 儲存貯體中的檔案和子目錄數量。

## 部署多個閘道以支援工作負載

Storage Gateway 可以透過跨多個閘道分割工作負載，為具有數百個 SQL 資料庫、多個 SQL Server 和數百 TB 備份資料的大型環境支援 SQL 備份。

規劃具有多個閘道和 SQL 伺服器的部署時，請考慮下列事項：

- 單一閘道通常每天最多可以上傳 20 TB，具有足夠的硬體資源和頻寬。您可以增加 [Amazon S3 上傳程式執行緒的數量](#)，將此限制提高到每天 40 TB。
- 我們建議您進行proof-of-concept測試，以測量效能並考慮部署中的所有變數。確定 SQL 備份工作負載的最高輸送量之後，您可以擴展閘道數量以符合您的需求。
- 我們建議您以成長為考量來設計解決方案，因為資料庫數量和資料庫大小可能會隨著時間增加。若要繼續擴展和支援不斷增加的工作負載，您可以視需要部署其他閘道。

## 資料庫備份工作負載的其他資源

- [使用在 Amazon S3 中存放 SQL Server 備份 AWS Storage Gateway](#)
- [使用檔案閘道在 Amazon S3 中輕鬆存放 SQL Server 備份](#)
- [使用 AWS Storage Gateway 在 Amazon S3 中存放 Oracle 資料庫備份](#)
- [大規模將 Oracle 資料庫備份至 Amazon S3](#)
- [使用將 SAP ASE 資料庫整合到 Amazon S3 AWS Storage Gateway](#)
- [一個 AWS Hero 如何使用 AWS Storage Gateway 進行雲端內備份](#)
- [S3 File Gateway 快取調整大小最佳實務](#)

# 安全 in AWS Storage Gateway

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構專為滿足最安全敏感組織的需求而建置。

安全性是 AWS 與您之間共同責任。[共同責任模式](#)將其描述為雲端的安全性，和雲端中的安全性：

- 雲端的安全性 – AWS 負責保護在 Cloud AWS 中執行 AWS 服務的基礎設施。AWS 也為您提供可安全使用的服務。在[AWS 合規計畫](#)中，第三方稽核人員會定期測試和驗證我們安全的有效性。若要了解適用於 AWS Storage Gateway 的合規計畫，請參閱[AWS 合規計畫的服務範圍](#)。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您的公司的要求和適用法律和法規。

本文件有助於您了解如何在使用 Storage Gateway 時套用共同責任模型。下列各主題將說明如何設定 Storage Gateway，以達成您的安全性與合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 Storage Gateway 資源。

## in AWS Storage Gateway 的資料保護

AWS [共同責任模型](#)適用於 in AWS Storage Gateway 的資料保護。如此模型所述，AWS 負責保護執行所有的全域基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱[資料隱私權常見問答集](#)。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 共同責任模型和 GDPR](#) 部落格文章。

基於資料保護目的，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《使用者指南》中的[使用 CloudTrail 追蹤](#)。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。

- 如果您在 AWS 透過命令列界面或 API 存取時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱[聯邦資訊處理標準 \(FIPS\) 140-3](#)。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 Storage Gateway 或使用主控台、API AWS CLI 或其他 AWS 服務 AWS SDKs 時。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 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 進行資料加密 AWS KMS

Amazon FSx File Gateway 支援 SMB 加密，最高可達最新的 SMB v3.1.1 規格，包括 AES 128 CCM 和 AES 128 GCM。相容用戶端會自動使用加密進行連線。此外，FSx File Gateway 會在與 FSx for Windows File Server 通訊時使用 SMB 加密 AWS。您必須設定 Direct Connect 的連結 AWS，並設定適當的政策，以允許 SMB 流量和管理流量傳遞至 AWS。

### 加密檔案系統

如需詳細資訊，請參閱 [《Amazon FSx for Windows File Server 使用者指南》](#) 中的 [Amazon FSx 中的資料加密](#)。FSx

使用 AWS KMS 加密您的資料時，請記住下列事項：

- 您的資料是在雲端中的靜態狀態下加密。也就是說，資料會在 Amazon FSx 中加密。
- IAM 使用者必須擁有呼叫 AWS KMS API 操作所需的許可。如需詳細資訊，請參閱 [《AWS Key Management Service 開發人員指南》](#) 中的 [AWS KMS 使用 IAM 政策](#)。

#### Important

當您使用 AWS KMS 金鑰進行伺服器端加密時，您必須選擇對稱金鑰。Storage Gateway 不支援非對稱金鑰。如需詳細資訊，請參閱 AWS Key Management Service 開發人員指南中的 [使用對稱和非對稱金鑰](#)。

如需詳細資訊 AWS KMS，請參閱 [什麼是 AWS Key Management Service ?](#)

# AWS Storage Gateway的身分和存取管理

AWS Identity and Access Management (IAM) 是 AWS 服務，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證（登入）和授權（具有許可）來使用 AWS SGW 資源。IAM 是您可以免費使用 AWS 服務的。

## 主題

- [目標對象](#)
- [使用身分驗證](#)
- [使用政策管理存取權](#)
- [How AWS Storage Gateway 可與 IAM 搭配使用](#)
- [AWS Storage Gateway的身分型政策範例](#)
- [故障診斷 AWS Storage Gateway 身分和存取](#)
- [使用標籤來控制對閘道和資源的存取](#)

## 目標對象

使用方式 AWS Identity and Access Management (IAM) 會根據您的角色而有所不同：

- 服務使用者 — 若無法存取某些功能，請向管理員申請所需許可 (請參閱 [故障診斷 AWS Storage Gateway 身分和存取](#))
- 服務管理員 — 負責設定使用者存取權並提交相關許可請求 (請參閱 [How AWS Storage Gateway 可與 IAM 搭配使用](#))
- IAM 管理員 — 撰寫政策以管理存取控制 (請參閱 [AWS Storage Gateway的身分型政策範例](#))

## 使用身分驗證

身分驗證是您 AWS 使用身分憑證登入的方式。您必須以 AWS 帳戶根使用者、IAM 使用者或擔任 IAM 角色身分進行身分驗證。

您可以使用身分來源的登入資料，例如 AWS IAM Identity Center (IAM Identity Center)、單一登入身分驗證或 Google/Facebook 登入資料，以聯合身分的形式登入。如需有關登入的詳細資訊，請參閱《AWS 登入 使用者指南》中的[如何登入您的 AWS 帳戶](#)。

對於程式設計存取，AWS 提供 SDK 和 CLI 以密碼編譯方式簽署請求。如需詳細資訊，請參閱《IAM 使用者指南》中的[API 請求的AWS 第 4 版簽署程序](#)。

## AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個名為 AWS 帳戶 theroot 使用者的登入身分開始，該身分可完整存取所有 AWS 服務和資源。強烈建議不要使用根使用者來執行日常任務。有關需要根使用者憑證的任務，請參閱《IAM 使用者指南》中的[需要根使用者憑證的任務](#)。

## 聯合身分

最佳實務是要求人類使用者使用聯合身分提供者，以 AWS 服務使用臨時憑證存取。

聯合身分是您企業目錄、Web 身分提供者的使用者，或使用身分來源的 AWS 服務憑證存取 Directory Service。聯合身分會擔任角色，而該角色會提供臨時憑證。

若需集中化管理存取權限，建議使用 AWS IAM Identity Center。如需詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的[什麼是 IAM Identity Center?](#)。

## IAM 使用者和群組

IAM 使用者[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_users.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html)是一種身分具備單人或應用程式的特定許可權。建議以臨時憑證取代具備長期憑證的 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的[要求人類使用者使用聯合身分提供者來 AWS 使用臨時憑證存取](#)。

[IAM 群組](#)會指定 IAM 使用者集合，使管理大量使用者的許可權更加輕鬆。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 使用者的使用案例](#)。

## IAM 角色

IAM 角色[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html)的身分具有特定許可權，其可以提供臨時憑證。您可以透過[從使用者切換到 IAM 角色（主控台）](#)或呼叫 AWS CLI 或 AWS API 操作來擔任角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[擔任角色的方法](#)。

IAM 角色適用於聯合身分使用者存取、臨時 IAM 使用者許可、跨帳戶存取權與跨服務存取，以及在 Amazon EC2 執行的應用程式。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 中的快帳戶資源存取](#)。

## 使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策定義與身分或資源相關聯的許可。當委託人提出請求時 AWS，會評估這些政策。大多數政策會以 JSON 文件 AWS 形式存放在中。如需進一步了解 JSON 政策文件，請參閱《IAM 使用者指南》中的[JSON 政策概觀](#)。

管理員會使用政策，透過定義哪些主體可在哪些條件下對哪些資源執行動作，以指定可存取的範圍。

預設情況下，使用者和角色沒有許可。IAM 管理員會建立 IAM 政策並將其新增至角色，供使用者後續擔任。IAM 政策定義動作的許可，無論採用何種方式執行。

## 身分型政策

身分型政策是附加至身分 (使用者、使用者群組或角色) 的 JSON 許可政策文件。這類政策控制身分可對哪些資源執行哪些動作，以及適用的條件。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的[透過客戶管理政策定義自訂 IAM 許可](#)。

身分型政策可分為內嵌政策 (直接內嵌於單一身分) 與受管政策 (可附加至多個身分的獨立政策)。如需了解如何在受管政策及內嵌政策之間做選擇，請參閱《IAM 使用者指南》中的[在受管政策與內嵌政策之間選擇](#)。

## 資源型政策

資源型政策是附加到資源的 JSON 政策文件。範例包括 IAM 角色信任政策與 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。您必須在資源型政策中[指定主體](#)。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

## 其他政策類型

AWS 支援其他政策類型，可設定更多常見政策類型授予的最大許可：

- 許可界限 — 設定身分型政策可授與 IAM 實體的最大許可。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 實體許可界限](#)。
- 服務控制政策 (SCP) — 為 AWS Organizations 中的組織或組織單位指定最大許可。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的[服務控制政策](#)。
- 資源控制政策 (RCP) — 設定您帳戶中資源可用許可的上限。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的[資源控制政策 \(RCP\)](#)。
- 工作階段政策 — 在以程式設計方式為角色或聯合身分使用者建立臨時工作階段時，以參數形式傳遞的進階政策。如需詳細資訊，請參閱《IAM 使用者指南》中的[工作階段政策](#)。

## 多種政策類型

當多種類型的政策適用於請求時，產生的許可會更複雜而無法理解。若要了解如何 AWS 在涉及多個政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的[政策評估邏輯](#)。

## How AWS Storage Gateway 可與 IAM 搭配使用

在您使用 IAM 管理 SGW AWS 的存取權之前，請先了解哪些 IAM 功能可與 SGW AWS 搭配使用。

您可以搭配 AWS Storage Gateway 使用的 IAM 功能

IAM 功能	AWS SGW 支援
<a href="#">身分型政策</a>	是
<a href="#">資源型政策</a>	否
<a href="#">政策動作</a>	是
<a href="#">政策資源</a>	是
<a href="#">政策條件索引鍵 (服務特定)</a>	是
<a href="#">ACL</a>	否
<a href="#">ABAC(政策中的標籤)</a>	部分
<a href="#">臨時憑證</a>	是
<a href="#">轉送存取工作階段 (FAS)</a>	是
<a href="#">服務角色</a>	是
<a href="#">服務連結角色</a>	是

若要全面了解 AWS SGW 和其他 AWS 服務如何與大多數 IAM 功能搭配使用，請參閱 [《AWS IAM 使用者指南》](#) 中的 [與 IAM 搭配使用的服務](#)。

### SGW AWS 的身分型政策

支援身分型政策：是

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。如需了解如何建立身分型政策，請參閱 [《IAM 使用者指南》](#) 中的 [透過客戶管理政策定義自訂 IAM 許可](#)。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 [IAM JSON 政策元素參考](#)。

## SGW AWS 的身分型政策範例

若要檢視 AWS SGW 身分型政策的範例，請參閱 [AWS Storage Gateway 的身分型政策範例](#)。

## SGW AWS 內的資源型政策

支援資源型政策：否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中 [指定主體](#)。委託人可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

如需啟用跨帳戶存取權，您可以在其他帳戶內指定所有帳戶或 IAM 實體作為資源型政策的主體。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM 中的快帳戶資源存取](#)。

## SGW AWS 的政策動作

支援政策動作：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 Action 元素描述您可以用來允許或拒絕政策中存取的動作。政策會使用動作來授予執行相關聯動作的許可。

若要查看 AWS SGW 動作清單，請參閱服務授權參考中的 [AWS Storage Gateway 定義的動作](#)。

SGW AWS 中的政策動作在動作之前使用下列字首：

sgw

若要在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [  
  "sgw:action1",  
  "sgw:action2"  
]
```

若要檢視 AWS SGW 身分型政策的範例，請參閱 [AWS Storage Gateway 的身分型政策範例](#)。

## SGW AWS 的政策資源

支援政策資源：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素可指定要套用動作的物件。最佳實務是使用其 [Amazon Resource Name \(ARN\)](#) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (\*) 表示該陳述式適用於所有資源。

```
"Resource": "*"
```

若要查看 AWS SGW 資源類型及其 ARNs，請參閱《服務授權參考》中的 [AWS Storage Gateway 定義的資源](#)。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 [AWS Storage Gateway 定義的動作](#)。

若要檢視 AWS SGW 身分型政策的範例，請參閱 [AWS Storage Gateway 的身分型政策範例](#)。

## SGW AWS 的政策條件索引鍵

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素會根據定義的條件，指定陳述式的執行時機。您可以建立使用 [條件運算子](#) 的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的 [AWS 全域條件內容索引鍵](#)。

若要查看 AWS SGW 條件金鑰清單，請參閱服務授權參考中的[AWS Storage Gateway的條件金鑰](#)。若要了解您可以使用條件金鑰的動作和資源，請參閱[AWS Storage Gateway定義的動作](#)。

若要檢視 AWS SGW 身分型政策的範例，請參閱 [AWS Storage Gateway的身分型政策範例](#)。

## SGW AWS 中的 ACLs

支援 ACL：否

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

## ABAC 搭配 AWS SGW

支援 ABAC (政策中的標籤)：部分

屬性型存取控制 (ABAC) 是一種授權策略，根據稱為標籤的屬性定義許可權。您可以將標籤連接至 IAM 實體 AWS 和資源，然後設計 ABAC 政策，以便在委託人的標籤符合資源上的標籤時允許操作。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的[條件元素](#)中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的[使用 ABAC 授權定義許可](#)。如要查看含有設定 ABAC 步驟的教學課程，請參閱《IAM 使用者指南》中的[使用屬性型存取控制 \(ABAC\)](#)。

## 搭配 SGW AWS 使用臨時登入資料

支援臨時憑證：是

臨時登入資料提供對 AWS 資源的短期存取，並在您使用聯合或切換角色時自動建立。AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 中的臨時安全憑證與可與 IAM 搭配運作的AWS 服務](#)。

## 轉送 SGW AWS 的存取工作階段

支援轉寄存取工作階段 (FAS)：是

轉送存取工作階段 (FAS) 使用呼叫的委託人許可 AWS 服務，結合 AWS 服務請求向下游服務提出請求。如需提出 FAS 請求時的政策詳細資訊，請參閱[轉發存取工作階段](#)。

## SGW AWS 的服務角色

支援服務角色：是

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](#)。

### Warning

變更服務角色的許可可能會中斷 AWS SGW 功能。只有在 AWS SGW 提供指引時，才能編輯服務角色。

## SGW AWS 的服務連結角色

支援服務連結角色：是

服務連結角色是連結至的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 [中 AWS 帳戶](#)，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理服務連結角色的詳細資訊，請參閱[可搭配 IAM 運作的 AWS 服務](#)。在資料表中尋找服務，其中包含服務連結角色欄中的 Yes。選擇是連結，以檢視該服務的服務連結角色文件。

## AWS Storage Gateway的身分型政策範例

根據預設，使用者和角色沒有建立或修改 AWS SGW 資源的許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。

如需了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的[建立 IAM 政策 \(主控台\)](#)。

如需 SGW AWS 定義的動作和資源類型的詳細資訊，包括每種資源類型的 ARNs 格式，請參閱服務授權參考中的[適用於 AWS Storage Gateway的動作、資源和條件金鑰](#)。

主題

- [政策最佳實務](#)
- [使用 AWS SGW 主控台](#)

- [允許使用者檢視他們自己的許可](#)

## 政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 AWS SGW 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需更多資訊，請參閱《IAM 使用者指南》中的 [AWS 受管政策](#) 或 [任務職能的 AWS 受管政策](#)。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱《IAM 使用者指南》中的 [IAM 中的政策和許可](#)。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 例如 使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 CloudFormation。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM JSON 政策元素：條件](#)。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 [使用 IAM Access Analyzer 驗證政策](#)。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 [透過 MFA 的安全 API 存取](#)。

如需 IAM 中最佳實務的相關資訊，請參閱《IAM 使用者指南》中的 [IAM 安全最佳實務](#)。

## 使用 AWS SGW 主控台

若要存取 AWS Storage Gateway 主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視中 AWS SGW 資源的詳細資訊 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許最低主控台許可。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

為了確保使用者和角色仍然可以使用 AWS SGW 主控台，請將 AWS SGW *ConsoleAccess* 或 *ReadOnly* AWS 受管政策連接到實體。如需詳細資訊，請參閱《IAM 使用者指南》中的 [新增許可到使用者](#)。

## 允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視連接到他們使用者身分的內嵌及受管政策。此政策包含在主控台或使用 或 AWS CLI AWS API 以程式設計方式完成此動作的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}
```

## 故障診斷 AWS Storage Gateway 身分和存取

使用以下資訊來協助您診斷和修正使用 SGW AWS 和 IAM 時可能遇到的常見問題。

### 主題

- [我無權在 SGW AWS 中執行動作](#)
- [我未獲得執行 iam:PassRole 的授權](#)
- [我想要允許 外的人員 AWS 帳戶 存取我的 AWS SGW 資源](#)

### 我無權在 SGW AWS 中執行動作

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在 mateojackson IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 `sgw:GetWidget` 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
sgw:GetWidget on resource: my-example-widget
```

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 `sgw:GetWidget` 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

### 我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，告知您無權執行 `iam:PassRole` 動作，您的政策必須更新，以允許您將角色傳遞給 AWS SGW。

有些 AWS 服務可讓您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為 marymajor 的 IAM 使用者嘗試使用主控台在 AWS SGW 中執行動作時，發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞給服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 `iam:PassRole` 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

### Important

Storage Gateway 可以擔任使用 `iam:PassRole` 政策動作傳遞的現有服務角色，但不支援使用 `iam:PassedToService` 內容索引鍵將動作限制為特定服務的 IAM 政策。

如需詳細資訊，請參閱《AWS Identity and Access Management 使用者指南》中的以下主題：

- [IAM：將 IAM 角色傳遞至特定 AWS 服務](#)
- [授予使用者將角色傳遞至 AWS 服務的許可](#)
- [IAM 的可用金鑰](#)

## 我想要允許 外的人員 AWS 帳戶 存取我的 AWS SGW 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 AWS SGW 是否支援這些功能，請參閱 [How AWS Storage Gateway 可與 IAM 搭配使用](#)。
- 若要了解如何 AWS 帳戶 在您擁有的 資源之間提供存取權，請參閱《[IAM 使用者指南](#)》中的 [在您擁有 AWS 帳戶 的另一個 中提供存取權給 IAM 使用者](#)。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的 [將存取權提供給第三方 AWS 帳戶 擁有](#)。
- 如需了解如何透過聯合身分提供存取權，請參閱《IAM 使用者指南》中的 [將存取權提供給在外部進行身分驗證的使用者 \(聯合身分\)](#)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 [IAM 中的跨帳戶資源存取](#)。

## 使用標籤來控制對閘道和資源的存取

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](#)。

## 根據資源的標籤控制存取

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。

### JSON

```
{
  "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:us-east-1:111122223333:*/*"
    }
  ]
}
```

```
}
```

## 根據 IAM 請求中的標籤控制存取

若要控制使用者可以對閘道資源執行的動作，您可以根據標籤在 IAM 政策中使用條件。例如，您可以撰寫政策，以根據使用者在建立資源時提供的標籤，允許或拒絕使用者執行特定 API 操作。

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校道上的標籤金鑰值組符合 **Department** 和 **Finance** 時，允許使用者在校道上建立網路檔案系統 (NFS) 或伺服器訊息區塊 (SMB) 檔案共用。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，因此使用者無法在校道或檔案共用上執行這些操作。

## JSON

```
{
  "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"
  }
}
```

## AWS Storage Gateway的合規驗證

在多個合規計畫中，第三方稽核人員會評估 AWS Storage Gateway 的安全性和 AWS 合規性。其中包括 SOC、PCI、ISO、FedRAMP、HIPAA、MTCS、C5、K-ISMS、ENS High、OSPAR 和 HITRUST CSF。

如需特定合規計畫範圍內 AWS 的服務清單，請參閱[AWS 合規計畫範圍內的服務](#)。如需一般資訊，請參閱 [AWS Compliance Programs](#)。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱在 [中下載報告 AWS Artifact](#)。

您在使用 Storage Gateway 時的合規責任，取決於資料的敏感性、您公司的合規目標，以及適用的法律和法規。AWS 會提供以下資源協助您處理合規事宜：

- [安全與合規快速入門指南](#) – 這些部署指南討論架構考量，並提供部署以安全與合規為中心之基準環境的步驟 AWS。
- [HIPAA 安全與合規架構白皮書](#) – 此白皮書說明公司如何使用 AWS 來建立符合 HIPAA 規範的應用程式。
- [AWS 合規資源](#) – 此工作手冊和指南的集合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符合內部實務、產業準則和法規的程度。
- [AWS Security Hub CSPM](#) – AWS 此服務提供 內安全狀態的完整檢視 AWS ，協助您檢查是否符合安全產業標準和最佳實務。

## in AWS Storage Gateway 的復原能力

AWS 全球基礎設施是以 AWS 區域 和可用區域為基礎建置。

AWS 區域 是全球資料中心叢集所在的實體位置。每個邏輯資料中心群組稱為可用區域 (AZ)。每個 AWS 區域 都包含一個地理區域內至少三個隔離且實際隔離AZs。與通常將區域定義為單一資料中心的其他雲端供應商不同，每個的多個可用區域設計 AWS 區域 都具有不同的優勢。每個 AZ 都有獨立的電源、冷卻和實體安全性，並透過備援ultra-low-latency的網路連接。如果您的部署需要專注於高可用性，您可以在多個 AZs 中將 服務和資源設定為 ，以實現更高的容錯能力。

AWS 區域 符合最高層級的基礎設施安全性、合規性和資料保護。AZ 之間的所有流量都會加密。網路效能足以完成 AZs 之間的不同步複寫。AZs可讓分割服務和資源變得簡單，以實現高可用性。如果您的部署跨AZs分割，您的資源會受到更好的隔離和保護，免於停電、閃電、龍捲風、地震等問題。AZs實際上與任何其他 AZ 相隔一段有意義的距離，但彼此距離都在 100 公里 (60 英里 ) 內。

如需 AWS 區域 和可用區域的詳細資訊，請參閱 [AWS 全球基礎設施](#)。

除了 AWS 全球基礎設施之外，Storage Gateway 還支援 VMware vSphere 高可用性 (VMware HA)，以協助保護儲存工作負載免於硬體、Hypervisor 或網路故障。如需詳細資訊，請參閱[搭配使用 VMware vSphere 高可用性與 Storage Gateway](#)。

## 基礎設施安全 in AWS Storage Gateway

作為受管服務，AWS Storage Gateway 受到 [Security Pillar - AWS Well-Architected Framework](#) 中所述的 AWS 全球網路安全程序的保護。

您可以使用 AWS 發佈的 API 呼叫，透過網路存取 Storage Gateway。用戶端必須支援 Transport Layer Security (TLS) 1.2。用戶端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 主體相關聯的私密存取金鑰來簽署。或者，您可以透過 [AWS Security Token Service](#) (AWS STS) 來產生暫時安全憑證來簽署請求。

### Note

您應該將 AWS Storage Gateway設備視為受管虛擬機器，且不應嘗試以任何方式存取或修改其安裝。嘗試使用一般閘道更新機制以外的方法安裝掃描軟體或更新任何軟體套件，可能會導致閘道故障，並可能影響我們支援或修正閘道的能力。

AWS 會定期檢閱、分析和修復 CVEs。我們會在正常的軟體版本週期中，將這些問題的修正納入 Storage Gateway。這些修正通常會在排定的維護時段內，做為正常閘道更新程序的一部分套用。如需閘道更新的詳細資訊，請參閱[使用 AWS Storage Gateway 主控台管理閘道更新](#)。

# AWS 安全最佳實務

AWS 在您開發和實作自己的安全政策時，提供多種要考慮的安全功能。這些最佳實務為一般準則，並不代表完整的安全解決方案。這些實務可能不適用或無法滿足您的環境需求，因此請將其視為實用建議就好，而不要當作是指示。如需詳細資訊，請參閱 [AWS 安全最佳實務](#)。

## 在中記錄和監控 AWS Storage Gateway

Storage Gateway 已與服務整合 AWS CloudTrail，此服務提供由使用者、角色或 Storage Gateway 中的 AWS 服務所採取之動作的記錄。CloudTrail 會將 Storage Gateway 的所有 API 呼叫擷取為事件。擷取的呼叫包括從 Storage Gateway 主控台進行的呼叫，以及針對 Storage Gateway API 操作的程式碼呼叫。如果您建立追蹤，您可以開啟 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 Storage Gateway 的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台的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》<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/>。

## CloudTrail 中的 Storage Gateway 資訊

當您建立 AWS 帳戶時，會在您的帳戶上啟用 CloudTrail。在 Storage Gateway 中發生活動時，該活動將與事件歷史中的其他 AWS 服務事件一起記錄在 CloudTrail 事件中。您可以在 AWS 帳戶中檢視、搜尋和下載最近的事件。如需詳細資訊，請參閱《使用 CloudTrail 事件歷史記錄檢視事件》<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/view-cloudtrail-events.html>。

若要持續記錄您 AWS 帳戶中的事件，包括 Storage Gateway 的事件，請建立追蹤。追蹤可讓 CloudTrail 將日誌檔案傳送至 Amazon S3 儲存貯體。根據預設，當您在主控台中建立線索時，線索會套用至所有 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中收集的事件資料。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 Storage Gateway 動作都會記錄並記載在 [動作](#) 主題中。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。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 是否使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出請求。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱 [CloudTrail userIdentity 元素](#)。

## 了解 Storage Gateway 日誌檔案項目

追蹤是一種組態，允許事件以日誌檔案的形式交付至您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。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": "AIDAI5AUPEBH2M7JTNCV",
      "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",
```

```

DHK88",
    "gatewayRegion": "us-east-2",
    "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
    "gatewayType": "VTL"
  },
  "responseElements": {
    "gatewayARN":
    "arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayv1"
  },
  "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": "AIDAI15AUEPBH2M7JTNVC",
      "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 ":"  
6U2N42CU37KA08BG6V1I23FRSJ1Q8GLLE1QEU3KPGG6F0KSTAUU0 ",  
        " eventID ":" f76e5919 - 9362 - 48ff - a7c4 -  
d203a189ec8d ",  
        " eventType ":" AwsApiCall ",  
        " apiVersion ":" 20130630 ",  
        " recipientAccountId ":" 444455556666"  
    ]]  
}
```

# 針對 Storage Gateway 部署的問題進行故障診斷

您可以在下面找到與閘道、主機平台、檔案系統、高可用性、資料復原和快照相關的最佳實務和疑難排解問題的相關資訊。內部部署閘道疑難排解資訊涵蓋部署在支援的虛擬化平台上的閘道。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

- [故障診斷：閘道離線問題](#) - 了解如何診斷可能導致您的閘道在 Storage Gateway 主控台中離線顯示的問題。
- [故障診斷：Active Directory 問題](#) - 了解如何在嘗試將檔案閘道加入 Microsoft Active Directory 網域 ACCESS\_DENIED 時收到錯誤訊息，例如 TIMEOUT、NETWORK\_ERROR 或。
- [故障診斷：閘道啟用問題](#) - 了解如何在嘗試啟用 Storage Gateway 時收到內部錯誤訊息。
- [故障診斷：內部部署閘道問題](#) - 了解使用內部部署閘道時可能遇到的典型問題，以及如何允許支援連接到閘道以協助故障診斷。
- [故障診斷：Microsoft Hyper-V 設定問題](#) - 了解在 Microsoft Hyper-V 平台上部署 Storage Gateway 時可能遇到的典型問題。
- [故障診斷：Amazon EC2 閘道問題](#) - 尋找您在使用 Amazon EC2 上部署的閘道時可能遇到的典型問題的相關資訊。
- [故障診斷：硬體設備問題](#) - 了解如何解決使用 AWS Storage Gateway 硬體設備時可能遇到的問題。
- [故障診斷：檔案閘道問題](#) - 尋找可協助您了解檔案閘道 CloudWatch 日誌中出現錯誤和運作狀態通知的原因的資訊。
- [故障診斷：高可用性問題](#) - 了解如果您在 VMware HA 環境中部署的閘道遇到問題，該怎麼辦。

## 故障診斷：Storage Gateway 主控台內的閘道離線

如果主控台顯示您的閘道離線，AWS Storage Gateway 請使用下列疑難排解資訊來判斷該怎麼做。

由於以下一個或多個原因，您的閘道可能顯示為離線：

- 閘道無法連線到 Storage Gateway 服務端點。
- 閘道意外關閉。
- 與閘道相關聯的快取磁碟已中斷連線或修改，或已失敗。

若要讓閘道重新上線，請識別並解決導致閘道離線的問題。

## 檢查相關聯的防火牆或代理

如果您將閘道設定為使用代理，或將閘道放置在防火牆後方，請檢閱代理或防火牆的存取規則。代理或防火牆必須允許進出 Storage Gateway 所需網路連接埠和服務端點的流量。如需詳細資訊，請參閱[網路和防火牆需求](#)。

## 檢查閘道流量的持續 SSL 或深度封包檢查

如果目前對閘道和之間的網路流量執行 SSL 或深度封包檢查 AWS，則閘道可能無法與所需的服務端點通訊。若要讓閘道重新上線，您必須停用檢查。

## 在重新啟動或軟體更新後檢查 IOWaitPercent 指標

重新啟動或軟體更新後，請檢查檔案閘道的 IOWaitPercent 指標是否為 10 或更高。這可能會導致閘道在重建索引快取至 RAM 時回應速度變慢。如需詳細資訊，請參閱[故障診斷：使用 CloudWatch 指標](#)。

## 檢查 Hypervisor 主機上是否有電源中斷或硬體故障

閘道 Hypervisor 主機上的電源中斷或硬體故障可能會導致閘道意外關閉且無法連線。還原電源和網路連線後，您的閘道將可再次連線。

閘道恢復上線後，請務必採取步驟來復原資料。如需詳細資訊，請參閱[最佳實務：復原資料](#)。

## 檢查相關聯的快取磁碟是否有問題

如果至少有一個與閘道相關聯的快取磁碟遭到移除、變更或調整大小，或者已損毀，您的閘道可能會離線。

如果從 Hypervisor 主機移除工作快取磁碟：

1. 關機閘道。
2. 重新新增磁碟。

### Note

請務必將磁碟新增至相同的磁碟節點。

3. 重新啟動閘道。

如果快取磁碟損毀、已取代或已調整大小：

- 遵循將[現有 S3 檔案閘道取代為新執行個體](#)中所述的方法 2 程序，以設定新的閘道，並從雲端重新下載快取磁碟資訊 AWS。

## 故障診斷：將閘道加入 Active Directory 時發生問題

使用以下疑難排解資訊，判斷當您嘗試將檔案閘道加入 Microsoft Active Directory 網域 ACCESS\_DENIED 時，收到錯誤訊息時該怎麼做 NETWORK\_ERROR，例如 TIMEOUT、或。

若要解決這些錯誤，請執行下列檢查和組態。

### 透過執行 nping 測試，確認閘道可以到達網域控制站

若要執行 nping 測試：

1. 使用 Hypervisor 管理軟體 (VMware、Hyper-V 或 KVM) 連接內部部署閘道的閘道本機主控台，或使用 ssh 連接 Amazon EC2 閘道。
2. 輸入對應的數字以選取閘道主控台，然後輸入 h 以列出所有可用的命令。若要測試 Storage Gateway 虛擬機器與網域之間的連線，請執行下列命令：

```
nping -d corp.domain.com -p 389 -c 1 -t tcp
```

#### Note

*corp.domain.com* 將取代為您的 Active Directory 網域 DNS 名稱，並將取代 389 為您環境的 LDAP 連接埠。

確認您已在防火牆中開啟必要的連接埠。

以下是閘道能夠到達網域控制站的成功 nping 測試範例：

```
nping -d corp.domain.com -p 389 -c 1 -t tcp
```

```
Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2022-06-30 16:24 UTC
SENT (0.0553s) TCP 10.10.10.21:9783 > 10.10.10.10:389 S ttl=64 id=730 iplen=40
  seq=2597195024 win=1480
RCVD (0.0556s) TCP 10.10.10.10:389 > 10.10.10.21:9783 SA ttl=128 id=22332 iplen=44
  seq=4170716243 win=8192 <mss 8961>
```

```
Max rtt: 0.310ms | Min rtt: 0.310ms | Avg rtt: 0.310ms  
Raw packets sent: 1 (40B) | Rcvd: 1 (44B) | Lost: 0 (0.00%)  
Nping done: 1 IP address pinged in 1.09 seconds<br>
```

以下是 nping 測試的範例，其中沒有 corp.domain.com 目的地的連線或回應：

```
nping -d corp.domain.com -p 389 -c 1 -t tcp  
  
Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2022-06-30 16:26 UTC  
SENT (0.0421s) TCP 10.10.10.21:47196 > 10.10.10.10:389 S ttl=64 id=30318 iplen=40  
seq=1762671338 win=1480  
  
Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A  
Raw packets sent: 1 (40B) | Rcvd: 0 (0B) | Lost: 1 (100.00%)  
Nping done: 1 IP address pinged in 1.07 seconds
```

## 檢查為 Amazon EC2 閘道執行個體的 VPC 設定的 DHCP 選項

如果檔案閘道是在 Amazon EC2 執行個體上執行，則您必須確保 DHCP 選項集已正確設定並連接到包含閘道執行個體的 Amazon Virtual Private Cloud (VPC)。如需詳細資訊，請參閱 [Amazon VPC 中的 DHCP 選項集](#)。

## 確認閘道可以透過執行 dig 查詢來解析網域

如果閘道無法解析網域，則閘道無法加入網域。

若要執行 dig 查詢：

1. 使用 Hypervisor 管理軟體 (VMware、Hyper-V 或 KVM) 連接內部部署閘道的閘道本機主控台，或使用 ssh 連接 Amazon EC2 閘道。
2. 輸入對應的數字以選取閘道主控台，然後輸入 h 以列出所有可用的命令。若要測試閘道是否可以解析網域，請執行下列命令：

```
dig -d corp.domain.com
```

### Note

corp.domain.com 將取代為您的 Active Directory 網域 DNS 名稱。

以下是成功回應的範例：

```
; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.amzn2.5.2 <<>> corp.domain.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24817
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;corp.domain.com.      IN      A

;; ANSWER SECTION:
corp.domain.com.      600     IN      A      10.10.10.10
corp.domain.com.      600     IN      A      10.10.20.10

;; Query time: 0 msec
;; SERVER: 10.10.20.228#53(10.10.20.228)
;; WHEN: Thu Jun 30 16:36:32 UTC 2022
;; MSG SIZE rcvd: 78
```

## 檢查網域控制站設定和角色

確認網域控制站未設定為唯讀，且網域控制站有足夠的角色可供電腦加入。若要測試這一點，請嘗試將閘道 VM 所在相同 VPC 子網路的其他伺服器加入網域。

## 檢查閘道是否已加入最近的網域控制站

最佳實務是，建議您將閘道加入地理上靠近閘道設備的網域控制站。如果閘道設備因為網路延遲無法在 20 秒內與網域控制器通訊，則網域連結程序可能會逾時。例如，如果閘道設備位於美國東部（維吉尼亞北部），AWS 區域且網域控制站位於亞太區域（新加坡），則程序可能會逾時。AWS 區域

### Note

若要增加預設逾時值 20 秒，您可以在 AWS Command Line Interface (AWS CLI) 中執行 [join-domain 命令](#)，並包含增加時間 `--timeout-in-seconds` 的選項。您也可以使用 [JoinDomain API 呼叫](#) 並包含 `TimeoutInSeconds` 參數來增加時間。逾時值上限為 3,600 秒。如果您在執行 AWS CLI 命令時收到錯誤，請確定您使用的是最新版本 AWS CLI。

## 確認 Active Directory 在預設組織單位 (OU) 中建立新的電腦物件

請確定 Microsoft Active Directory 沒有任何群組政策物件，可在預設 OU 以外的任何位置建立新的電腦物件。您必須先在預設的 OU 中存在新的電腦物件，才能將閘道加入 Active Directory 網域。有些 Active Directory 環境會自訂為針對新建立的物件具有不同的 OUs。若要保證閘道 VM 的新電腦物件存在於預設 OU 中，請先嘗試在網域控制器上手動建立電腦物件，再將閘道加入網域。您也可以使用執行 [join-domain 命令](#) AWS CLI。然後，指定的選項 `--organizational-unit`。

### Note

建立電腦物件的程序稱為預備。

## 檢查您的網域控制站事件日誌

如果您在嘗試前幾節所述的所有其他檢查和組態後，無法將閘道加入網域，建議您檢查網域控制站事件日誌。檢查網域控制站的事件檢視器中是否有任何錯誤。確認閘道查詢已到達網域控制站。

## 故障診斷：閘道啟用期間的內部錯誤

Storage Gateway 啟用請求會周遊兩個網路路徑。用戶端傳送的傳入啟用請求會透過連接埠 80 連線至閘道的虛擬機器 (VM) 或 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。如果閘道成功接收啟用請求，閘道會與 Storage Gateway 端點通訊，以接收啟用金鑰。如果閘道無法連線到 Storage Gateway 端點，閘道會以內部錯誤訊息回應用戶端。

使用以下疑難排解資訊，判斷在嘗試啟用時，如果收到內部錯誤訊息該怎麼辦 AWS Storage Gateway。

### Note

- 請務必使用最新的虛擬機器映像檔案或 Amazon Machine Image (AMI) 版本部署新的閘道。如果您嘗試啟用使用過期 AMI 的閘道，將會收到內部錯誤。
- 下載 AMI 之前，請務必選取您要部署的正確閘道類型。每個閘道類型的 .ova 檔案和 AMIs 不同，且不可互換。

## 解決使用公有端點啟用閘道時的錯誤

若要解決使用公有端點啟用閘道時的啟用錯誤，請執行下列檢查和組態。

### 檢查所需的連接埠

對於內部部署的閘道，請檢查本機防火牆上的連接埠是否已開啟。對於部署在 Amazon EC2 執行個體上的閘道，請檢查連接埠是否在執行個體的安全群組上開啟。若要確認連接埠已開啟，請從伺服器對公有端點執行 telnet 命令。此伺服器必須與閘道位於相同的子網路中。例如，下列 telnet 命令會測試連接埠 443 的連線：

```
telnet d4kdq0yaxexbo.cloudfront.net 443
telnet storagegateway.region.amazonaws.com 443
telnet dp-1.storagegateway.region.amazonaws.com 443
telnet proxy-app.storagegateway.region.amazonaws.com 443
telnet client-cp.storagegateway.region.amazonaws.com 443
telnet anon-cp.storagegateway.region.amazonaws.com 443
```

若要確認閘道本身可以到達端點，請存取閘道的本機 VM 主控台（適用於內部部署的閘道）。或者，您可以 SSH 到閘道的執行個體（適用於部署在 Amazon EC2 上的閘道）。然後，執行網路連線測試。確認測試傳回 [PASSED]。如需詳細資訊，請參閱[測試閘道的網路連線](#)。

#### Note

閘道主控台的預設登入使用者名稱為 admin，預設密碼為 password。

### 確保防火牆安全不會修改從閘道傳送至公有端點的封包

SSL 檢查、深度封包檢查或其他形式的防火牆安全可能會干擾從閘道傳送的封包。如果從啟用端點預期修改 SSL 憑證，則 SSL 交握會失敗。若要確認沒有進行中的 SSL 檢查，請在連接埠 443 的主要啟用端點 (anon-cp.storagegateway.region.amazonaws.com) 上執行 OpenSSL 命令。您必須從與閘道位於相同子網路的機器執行此命令：

```
$ openssl s_client -connect anon-cp.storagegateway.region.amazonaws.com:443 -
servername anon-cp.storagegateway.region.amazonaws.com
```

**Note**

將##取代為您的 AWS 區域。

如果沒有進行中的 SSL 檢查，則命令會傳回類似如下的回應：

```
$ openssl s_client -connect anon-cp.storagegateway.us-east-2.amazonaws.com:443 -
servername anon-cp.storagegateway.us-east-2.amazonaws.com
CONNECTED(00000003)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-2.amazonaws.com
verify return:1
---
Certificate chain
 0 s:/CN=anon-cp.storagegateway.us-east-2.amazonaws.com
  i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
 1 s:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
  i:/C=US/O=Amazon/CN=Amazon Root CA 1
 2 s:/C=US/O=Amazon/CN=Amazon Root CA 1
  i:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
  Root Certificate Authority - G2
 3 s:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
  Root Certificate Authority - G2
  i:/C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority
---
```

如果有持續的 SSL 檢查，回應會顯示已變更的憑證鏈，如下所示：

```
$ openssl s_client -connect anon-cp.storagegateway.ap-southeast-1.amazonaws.com:443 -
servername anon-cp.storagegateway.ap-southeast-1.amazonaws.com
CONNECTED(00000003)
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
```

```
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.ap-southeast-1.amazonaws.com
  i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

啟用端點只有在識別 SSL 憑證時，才會接受 SSL 交握。這表示閘道對端點的傳出流量必須不受網路中防火牆執行的檢查。這些檢查可能是 SSL 檢查或深度封包檢查。

## 檢查閘道時間同步

時間過長可能會導致 SSL 交握錯誤。對於內部部署閘道，您可以使用閘道的本機 VM 主控台來檢查閘道的時間同步。時間扭曲不應大於 60 秒。如需詳細資訊，請參閱 [your Gateway VM TimeSynchronizing](#)。

系統時間管理選項不適用於在 Amazon EC2 執行個體上託管的閘道。為了確保 Amazon EC2 閘道可以正確同步時間，請確認 Amazon EC2 執行個體可以透過連接埠 UDP 和 TCP 123 連線至下列 NTP 伺服器集區清單：

- time.aws.com
- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org
- 2.amazon.pool.ntp.org
- 3.amazon.pool.ntp.org

## 解決使用 Amazon VPC 端點啟用閘道時的錯誤

若要解決使用 Amazon Virtual Private Cloud (Amazon VPC) 端點啟用閘道時的啟用錯誤，請執行下列檢查和組態。

### 檢查所需的連接埠

確定本機防火牆（適用於內部部署部署的閘道）或安全群組（適用於 Amazon EC2 中部署的閘道）內的必要連接埠已開啟。將閘道連線至 Storage Gateway VPC 端點所需的連接埠，與將閘道連線至公有端點時所需的連接埠不同。連線至 Storage Gateway VPC 端點需要下列連接埠：

- TCP 443
- TCP 1026

- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

如需詳細資訊，請參閱 [為 Storage Gateway 建立 VPC 端點](#) 為 Storage Gateway。

此外，請檢查連接至 Storage Gateway VPC 端點的安全群組。連接至端點的預設安全群組可能不允許必要的連接埠。建立新的安全群組，允許來自閘道 IP 地址範圍的流量通過所需的連接埠。然後，將該安全群組連接到 VPC 端點。

#### Note

使用 [Amazon VPC 主控台](#) 來驗證連接到 VPC 端點的安全群組。從主控台檢視 Storage Gateway VPC 端點，然後選擇安全群組索引標籤。

若要確認所需的連接埠已開啟，您可以在 Storage Gateway VPC 端點上執行 telnet 命令。您必須從與閘道位於相同子網路中的伺服器執行這些命令。您可以在未指定可用區域的第一個 DNS 名稱上執行測試。例如，下列 telnet 命令會使用 DNS 名稱 `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com` 測試所需的連接埠連線：

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 443
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1026
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1027
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1028
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1031
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 2222
```

## 確保防火牆安全不會修改從閘道傳送至 Storage Gateway Amazon VPC 端點的封包

SSL 檢查、深度封包檢查或其他形式的防火牆安全可能會干擾從閘道傳送的封包。如果從啟用端點預期修改 SSL 憑證，則 SSL 交握會失敗。若要確認沒有進行中的 SSL 檢查，請在 Storage Gateway VPC 端點上執行 OpenSSL 命令。您必須從與閘道位於相同子網路的機器執行此命令。為每個必要的連接埠執行命令：

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:443 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1026 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1028 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1031 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:2222 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

如果沒有進行中的 SSL 檢查，則命令會傳回類似如下的回應：

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-1.amazonaws.com
verify return:1
---
Certificate chain
 0 s:CN = anon-cp.storagegateway.us-east-1.amazonaws.com
  i:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
 1 s:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
  i:C = US, O = Amazon, CN = Amazon Root CA 1
 2 s:C = US, O = Amazon, CN = Amazon Root CA 1
  i:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
Starfield Services Root Certificate Authority - G2
```

```

3 s:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
Starfield Services Root Certificate Authority - G2
  i:C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification
Authority
---
```

如果有持續的 SSL 檢查，回應會顯示已變更的憑證鏈，如下所示：

```

openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.us-
east-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
```

Certificate chain

```

0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.us-east-1.amazonaws.com
  i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

啟用端點只有在識別 SSL 憑證時，才會接受 SSL 交握。這表示閘道透過所需連接埠傳出至 VPC 端點的流量不受網路防火牆執行的檢查影響。這些檢查可能是 SSL 檢查或深度封包檢查。

## 檢查閘道時間同步

時間過長可能會導致 SSL 交握錯誤。對於內部部署閘道，您可以使用閘道的本機 VM 主控台來檢查閘道的時間同步。時間扭曲不應大於 60 秒。如需詳細資訊，請參閱 [your Gateway VM TimeSynchronizing](#)。

系統時間管理選項不適用於在 Amazon EC2 執行個體上託管的閘道。為了確保 Amazon EC2 閘道可以正確同步時間，請確認 Amazon EC2 執行個體可以透過連接埠 UDP 和 TCP 123 連線至下列 NTP 伺服器集區清單：

- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org

- 2.amazon.pool.ntp.org
- 3.amazon.pool.ntp.org

## 檢查 HTTP 代理並確認相關聯的安全群組設定

啟用之前，請檢查 Amazon EC2 上的 HTTP 代理是否已在內部部署閘道 VM 上設定為連接埠 3128 上的 Squid 代理。在此情況下，請確認下列事項：

- 連接至 Amazon EC2 上 HTTP 代理的安全群組必須具有傳入規則。此傳入規則必須允許來自閘道 VM IP 地址之連接埠 3128 上的 Squid 代理流量。
- 連接至 Amazon EC2 VPC 端點的安全群組必須具有傳入規則。這些傳入規則必須允許連接埠 1026-1028、1031、2222 和 443 上來自 Amazon EC2 上 HTTP 代理的 IP 地址的流量。

## 解決使用公有端點啟用閘道，且相同 VPC 中有 Storage Gateway VPC 端點時的錯誤

若要解決在相同 VPC 中有 Amazon Virtual Private Cloud (Amazon VPC) 點時，使用公有端點啟用閘道時的錯誤，請執行下列檢查和組態。

### 確認 Storage Gateway VPC 端點上未啟用啟用私有 DNS 名稱設定

如果啟用私有 DNS 名稱已啟用，您就無法啟用從該 VPC 到公有端點的任何閘道。

若要停用私有 DNS 名稱選項：

1. 開啟 [Amazon VPC 主控台](#)。
2. 在導覽窗格中選擇端點。
3. 選擇 Storage Gateway VPC 端點。
4. 選擇動作。
5. 選擇管理私有 DNS 名稱。
6. 針對啟用私有 DNS 名稱，清除此端點的啟用。
7. 選擇修改私有 DNS 名稱以儲存設定。

## 故障診斷：內部部署閘道問題

您可以在下面找到有關使用現場部署閘道時可能遇到的典型問題的資訊，以及如何允許 支援 連接到您的閘道以協助故障診斷。

下表列出使用內部部署閘道時一般可能遇到的問題。

問題	採取動作
您找不到閘道的 IP 地址。	<p>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。</p> <ul style="list-style-type: none"> <li>• 若為 VMware ESXi，VM 的 IP 地址可在 Summary (摘要) 標籤的 vSphere 用戶端中找到。</li> <li>• 若為 Microsoft Hyper-V，登入本機主控台即可找到 VM 的 IP 地址。</li> </ul> <p>如果仍找不到閘道 IP 地址：</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul>
您有網路或防火牆的問題。	<ul style="list-style-type: none"> <li>• 允許閘道使用適當的連接埠。</li> <li>• 若您使用防火牆或路由器來篩選或限制網路流量，則必須設定防火牆和路由器，以允許這些服務端點可與 AWS 進行傳出通訊。如需網路和防火牆需求的詳細資訊，請參閱 <a href="#">網路與防火牆需求</a>。</li> </ul>
當您在 Storage Gateway 管理主控台中按一下繼續啟用按鈕時，您的閘道啟用會失敗。	<ul style="list-style-type: none"> <li>• 從您的用戶端 ping VM，檢查是否可存取閘道 VM。</li> <li>• 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 <a href="#">測試閘道的網路連線</a>。</li> <li>• 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 <a href="#">為您的閘道設定網路時間通訊協定 (NTP) 伺服器</a>。</li> </ul>

問題	採取動作
	<ul style="list-style-type: none"><li>• 執行完這些步驟後，您可以使用 Storage Gateway 主控台和設定與啟用閘道精靈，重試閘道部署。</li><li>• 檢查您的 VM 至少有 16 GB 的 RAM。如果 RAM 少於 16 GB，閘道配置會失敗。如需詳細資訊，請參閱<a href="#">檔案閘道設定需求</a>。</li></ul>
您需要改善閘道與 AWS 之間的頻寬。	<p>您可以在與連接應用程式和閘道 VM 分開的網路轉接器 (NIC) AWS 上設定的網際網路連線，AWS 以改善從閘道到的頻寬。如果您與有高頻寬連線，AWS 而且想要避免頻寬爭用，尤其是在快照還原期間，採取此方法非常有用。對於高輸送量工作負載的需求，您可以使用 <a href="#">Direct Connect</a> 在內部部署閘道和 AWS 之間建立專用網路連線。若要測量閘道連線的頻寬 AWS，請使用閘道的 CloudBytesDownloaded 和 CloudBytesUploaded 指標。如需此主題的詳細資訊，請參閱<a href="#">效能和最佳化</a>。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。</p>

問題	採取動作
<p>閘道的出入輸送量降到零。</p>	<ul style="list-style-type: none"> <li>• 在 Storage Gateway 主控台的閘道標籤上，驗證您閘道 VM 的 IP 地址是否和您看到使用您的虛擬化管理程序用戶端軟體 (也就是 VMware vSphere 用戶端或 Microsoft Hyper-V Manager) 的 IP 地址相同。如果您發現不相符，請從 Storage Gateway 主控台重新啟動您的閘道，如 <a href="#">關閉您的閘道 VM</a> 所述。重新啟動後，Storage Gateway 主控台之閘道標籤中的 IP 地址清單中的地址，應該符合您從虛擬化管理程序用戶端決定的閘道 IP 地址。</li> <li>• 若為 VMware ESXi，VM 的 IP 地址可在 Summary (摘要) 標籤的 vSphere 用戶端中找到。</li> <li>• 若為 Microsoft Hyper-V，登入本機主控台即可找到 VM 的 IP 地址。</li> <li>• 檢查閘道對的連線 AWS，如 <a href="#">中所述測試閘道的網路連線</a>。</li> <li>• 檢查 Hypervisor 管理用戶端中閘道的網路轉接器組態，並確保您打算用於閘道的所有介面都已啟用。</li> <li>• 在閘道本機主控台中檢查閘道的網路轉接器組態。如需說明，請參閱 <a href="#">設定您的閘道網路設定</a>。</li> </ul> <p>您可以從 Amazon CloudWatch 主控台檢視在您閘道出入的輸送量。如需測量閘道與之間傳輸量的詳細資訊 AWS，請參閱 <a href="#">效能和最佳化</a>。</p>
<p>您無法在 Microsoft Hyper-V 匯入 (部署) Storage Gateway。</p> <p>您會收到以下訊息：「The data that has been written to the volume in your gateway isn't securely stored at AWS」。</p>	<p>請參閱 <a href="#">故障診斷：Microsoft Hyper-V 設定</a>，以了解在 Microsoft Hyper-V 部署閘道的常見問題。</p> <p>如果您的閘道 VM 是從另一個閘道 VM 的複製或快照所建立，就會收到此訊息。如果不是這種情況，請聯絡 支援。</p>

## 開啟 支援 存取權，以協助對內部部署託管的閘道進行故障診斷

Storage Gateway 提供本機主控台，您可以用來執行數個維護任務，包括允許 支援 存取您的閘道，以協助您疑難排解閘道問題。根據預設，對閘道的 支援 存取會關閉。您可以透過主機的本機主控台開啟此存取權。若要允許 支援 存取您的閘道，請先登入主機的本機主控台，導覽至 Storage Gateway 的主控台，然後連線至支援伺服器。

### 開啟對閘道的 支援 存取

1. 登入您主機的本機主控台。
    - VMware ESXi：如需詳細資訊，請參閱 [使用 VMware ESXi 存取閘道本機主控台](#)。
    - Microsoft Hyper-V：如需詳細資訊，請參閱 [使用 Microsoft Hyper-V 存取閘道本機主控台](#)。
  2. 出現提示時，輸入對應的數字以選取閘道組態。
  3. 輸入 **h** 以開啟可用命令視窗。
  4. 執行以下任意一項：
    - 如果您的閘道使用公有端點，請在可用命令視窗中輸入 **open-support-channel** 來連線到 Storage Gateway 的客戶支援。允許 TCP 連接埠 22，即可開啟 AWS 的支援管道。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 地址以連線到 Storage Gateway 的客戶支援。允許 TCP 連接埠 22，即可開啟 AWS 的支援管道。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. 建立支援管道之後，請將支援服務號碼提供給 `support`，以便 `support` 可以提供故障診斷協助。
  6. 當支援工作階段完成時，請輸入 **q** 將其結束。在 Amazon Web Services Support 通知您支援工作階段完成之前，請勿關閉工作階段。
  7. 輸入 **exit** 以登出 Storage Gateway 主控台。
  8. 依照提示結束本機主控台。

## 故障診斷：Microsoft Hyper-V 設定

在 Microsoft Hyper-V 平台上部署 Storage Gateway 時通常可能會遇到的問題如下表所列。

問題	採取動作
<p>您嘗試匯入閘道並收到下列錯誤訊息：</p> <p>「嘗試匯入虛擬機器時發生伺服器錯誤。匯入失敗。在位置 【...】 下找不到虛擬機器匯入檔案。只有在在使用 Hyper-V 建立和匯出虛擬機器時，才能匯入虛擬機器。」</p>	<p>此錯誤的發生原因如下：</p> <ul style="list-style-type: none"> <li>如果您不是指向解壓縮閘道來源檔案的根目錄。您在匯入虛擬機器對話方塊中指定的最後一個部分應為 <code>AWS-Storage-Gateway</code>。例如： <code>C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\</code>。</li> <li>如已部署閘道，但未選取複製虛擬機器選項及勾選匯入虛擬機器對話方塊中的複製所有檔案選項，則 VM 會建立在您解壓縮閘道檔案的位置，而您無法再次由此位置匯入檔案。為修正此問題，請取得原始的解壓縮閘道來源檔案，然後複製到新的位置。使用新的位置做為匯入來源。</li> </ul> <p>如果您打算從一個解壓縮的來源檔案位置建立多個閘道，則必須選取複製虛擬機器，並勾選匯入虛擬機器對話方塊中的複製所有檔案方塊。</p>
<p>您嘗試匯入閘道並收到下列錯誤訊息：</p> <p>「嘗試匯入虛擬機器時發生伺服器錯誤。匯入失敗。匯入任務無法從 【...】 複製檔案：檔案存在。(0x80070050)''</p>	<p>如已部署閘道，而您嘗試重複使用存放虛擬硬碟檔案和虛擬機器組態檔案的預設資料夾，則會發生此錯誤。若要修正此問題，請在 Hyper-V 設定對話方塊左側面板的伺服器下指定新位置。</p>
<p>您嘗試匯入閘道並收到下列錯誤訊息：</p> <p>「嘗試匯入虛擬機器時發生伺服器錯誤。匯入失敗。Import failed because</p>	<p>當您匯入閘道時，請務必選取複製虛擬機器，並勾選匯入虛擬機器對話方塊中的複製所有檔案方塊，為虛擬機器建立新的唯一 ID。</p>

問題	採取動作
the virtual machine must have a new identifier. Select a new identifier and try the import again."	
您嘗試啟動閘道 VM 並收到下列錯誤訊息：  「嘗試啟動選取的虛擬機器（多個）時發生錯誤。子分割區處理器設定與父分割區不相容。'AWS-Storage-Gateway' 無法初始化。（虛擬機器 ID 【...】）」	此錯誤可能是因為閘道所需 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。  如需關於 Storage Gateway 需求的詳細資訊，請參閱 <a href="#">檔案閘道設定需求</a> 。
您嘗試啟動閘道 VM 並收到下列錯誤訊息：  「嘗試啟動選取的虛擬機器（多個）時發生錯誤。'AWS-Storage-Gateway' 無法初始化。（虛擬機器 ID 【...】）無法建立分割區：系統資源不足，無法完成請求的服務。(0x800705AA)''	此錯誤可能是因為閘道所需 RAM 和主機可用 RAM 之間的 RAM 差異所造成。  如需關於 Storage Gateway 需求的詳細資訊，請參閱 <a href="#">檔案閘道設定需求</a> 。
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 <a href="#">為您的閘道設定網路時間通訊協定 (NTP) 伺服器</a> 。
您需要將解壓縮的 Microsoft Hyper-V Storage Gateway 檔案放在主機的檔案系統。	像您對一般 Microsoft Windows 伺服器所做的一樣，存取主機。例如，如果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。

問題	採取動作
連線到虛擬化管理程序時，系統會提示您提供登入資料。	使用 Sconfig.cmd 工具新增您的使用者登入資料，做為虛擬化管理程序主機的本機管理員。
如果您為使用 Broadcom 網路轉接器的 Hyper-V 主機開啟虛擬機器佇列 (VMQ)，您可能會注意到網路效能不佳。	如需解決方法的資訊，請參閱 Microsoft 文件，請參閱 <a href="#">開啟 VMQ 時 Windows Server 2012 Hyper-V 主機上虛擬機器的網路效能不佳</a> 。

## 故障診斷：Amazon EC2 閘道問題

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。如需內部部署閘道和部署在 Amazon EC2 閘道兩者間之差異的詳細資訊，請參閱 [部署 FSx 檔案閘道的預設 Amazon EC2 主機](#)。

### 主題

- [您的閘道在一段時間後仍未啟用](#)
- [執行個體清單中找不到您的 EC2 閘道執行個體](#)
- [使用 Amazon EC2 序列主控台連接到您的閘道執行個體](#)
- [支援 您想要協助疑難排解 Amazon EC2 閘道](#)

## 您的閘道在一段時間後仍未啟用

在 Amazon EC2 主控台中，檢查以下項目：

- 連接埠 80 會在您與該執行個體相關聯的安全群組中開啟。如需新增安全群組規則的詳細資訊，請參閱《Amazon EC2 使用者指南》中的[新增安全群組規則](#)。
- 閘道執行個體標示為執行中。在 Amazon EC2 主控台中，執行個體的狀態值應為執行中。
- 請確保您的 Amazon EC2 執行個體類型符合最低要求，如 [儲存需求](#) 所述。

更正問題後，請嘗試再次啟動閘道。若要執行此操作，請開啟 Storage Gateway 主控台，選擇在 Amazon EC2 上部署新的閘道，然後重新輸入執行個體的 IP 地址。

## 執行個體清單中找不到您的 EC2 閘道執行個體

如果您並未建立執行個體的資源標籤，又有許多執行個體正在執行，要分辨您啟動了哪些執行個體會十分困難。在這種情況下，您可以執行以下動作，尋找閘道執行個體：

- 在執行個體的描述標籤上檢查 Amazon Machine Image (AMI) 的名稱。以 Storage Gateway AMI 為基礎的執行個體的開頭文字應為 **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。

## 使用 Amazon EC2 序列主控台連接到您的閘道執行個體

您可以使用 Amazon EC2 序列主控台來疑難排解開機、網路設定和其他問題。如需指示和疑難排解秘訣，請參閱《Amazon 彈性運算雲端使用者指南》中的 [Amazon EC2 序列主控台](#)。

## 支援 您想要協助疑難排解 Amazon EC2 閘道

Storage Gateway 提供本機主控台，您可以用來執行數個維護任務，包括允許 支援 存取您的閘道，以協助您疑難排解閘道問題。根據預設，對閘道的 支援 存取會關閉。您可以透過 Amazon EC2 本機主控台開啟此存取權。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。如需安全群組以及如何新增安全群組規則的詳細資訊，請參閱《Amazon EC2 使用者指南》中的 [Amazon EC2 安全群組](#)。

若要讓 支援 連線至您的閘道，請先登入 Amazon EC2 執行個體的本機主控台，導覽至 Storage Gateway 的主控台，然後提供存取權。

開啟在 Amazon EC2 執行個體上部署之閘道的 支援 存取

1. 登入 Amazon EC2 執行個體的本機主控台。如需說明，請參閱《Amazon EC2 使用者指南》中的 [連線到您的執行個體](#)。

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

*PRIVATE-KEY* 是 .pem 檔案，其中包含 EC2 金鑰對的私有憑證，您可用來啟動 Amazon EC2 執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[擷取金鑰對的公有金鑰](#)。

*INSTANCE-PUBLIC-DNS-NAME* 是用於執行閘道之 Amazon EC2 執行個體的公有網域名稱系統 (DNS) 名稱。您可以在 EC2 主控台中選取 Amazon EC2 執行個體，然後按一下描述標籤以取得此公有 DNS 名稱。

2. 出現提示時，輸入 **6 - Command Prompt** 以開啟 支援 管道主控台。
3. 輸入 **h** 以開啟可用命令視窗。
4. 執行以下任意一項：
  - 如果您的閘道使用公有端點，請在可用命令視窗中輸入 **open-support-channel** 來連線到 Storage Gateway 的客戶支援。允許 TCP 連接埠 22，即可開啟 AWS 的支援管道。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 地址以連線到 Storage Gateway 的客戶支援。允許 TCP 連接埠 22，即可開啟 AWS 的支援管道。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. 建立支援管道之後，請將支援服務號碼提供給 `support`，以便 `support` 可以提供故障診斷協助。
6. 當支援工作階段完成時，請輸入 **q** 將其結束。在 Amazon Web Services Support 通知您支援工作階段完成之前，請勿關閉工作階段。
7. 輸入 **exit** 以結束 Storage Gateway 主控台。
8. 依照主控台選單操作登出 Storage Gateway 執行個體。

## 故障診斷：硬體設備問題

### Note

可用性終止通知：自 2025 年 5 月 12 日起，將不再提供 AWS Storage Gateway 硬體設備。硬體 AWS Storage Gateway 設備的現有客戶可以繼續使用和接收支援，直到 2028 年 5 月為止。或者，您可以使用 AWS Storage Gateway 服務為應用程式提供現場部署和雲端存取幾乎無限制的雲端儲存。

下列主題討論您使用 AWS Storage Gateway 硬體設備時可能遇到的問題，以及疑難排解這些問題的建議。

### 主題

- [您無法確定服務 IP 地址](#)
- [如何執行重設成出廠預設值？](#)
- [如何執行遠端重新啟動？](#)
- [哪裡可以取得 Dell iDRAC 支援？](#)
- [您找不到硬體設備序號](#)
- [在何處取得硬體設備支援](#)

## 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前往服務主控台，請選擇 Open Service Console (開啟服務主控台)。

## 如何執行重設成出廠預設值？

如果您需要在設備上執行原廠重設，請聯絡 AWS Storage Gateway 硬體設備團隊以取得支援，如以下支援一節所述。

## 如何執行遠端重新啟動？

如果您需要執行裝置的遠端重新啟動，可以使用 Dell iDRAC 管理介面來執行此作業。如需詳細資訊，請參閱 Dell Technologies InfoHub 網站上的 [iDRAC9 虛擬電源重啟：遠端重啟 Dell EMC PowerEdge 伺服器電源](#)。

## 哪裡可以取得 Dell iDRAC 支援？

Dell PowerEdge 伺服器隨附 Dell iDRAC 管理介面。我們建議下列作法：

- 如果您使用 iDRAC 管理介面，則應變更預設密碼。如需關於 iDRAC 認證的詳細資訊，請參閱 [Dell PowerEdge - 什麼是 iDRAC 的預設登入憑證？](#)
- 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裝置正常運作。

## 您找不到硬體設備序號

您可以使用 AWS Storage Gateway 主控台找到 Storage Gateway 閘道硬體設備的序號。

若要尋找硬體設備序號：

1. 前往 <https://console.aws.amazon.com/storagegateway/home> 開啟 Storage Gateway 主控台。
2. 在頁面左側的導覽窗格選擇硬體。
3. 從清單中選取您的硬體設備。
4. 在設備的詳細資訊索引標籤上尋找序號欄位。

## 在何處取得硬體設備支援

若要聯絡 AWS 以取得硬體設備的技術支援，請參閱 [支援](#)。

支援 團隊可能會要求您啟用支援管道，以遠端疑難排解您的閘道問題。不需要將此連接埠開放給閘道的正常操作使用，但進行疑難排解時需要用到。您可以從硬體主控台啟用支援管道，如以下程序所示。

開啟 的支援管道 AWS

1. 開啟硬體主控台。
2. 選擇硬體主控台主頁面底部的開啟支援管道，然後按 Enter。

如果沒有網路連線或防火牆問題，指派的連接埠號碼應該會在 30 秒內顯示。例如：

狀態：在連接埠 19599 上開啟

3. 請記下連接埠號碼並將其提供給 支援。

## 故障診斷：檔案閘道問題

您可以設定檔案閘道，將日誌項目寫入 Amazon CloudWatch 日誌群組。如果您這樣做，您會收到有關閘道運作狀態和閘道遇到之任何錯誤的通知。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：FileMissing](#)
- [錯誤：FsxFileSystemAuthenticationFailure](#)
- [錯誤：FsxFileSystemConnectionFailure](#)
- [錯誤：FsxFileSystemFull](#)
- [錯誤：GatewayClockOutOfSync](#)
- [錯誤：InvalidFileState](#)
- [錯誤：ObjectMissing](#)
- [錯誤：DroppedNotifications](#)
- [通知：HardReboot](#)
- [通知：重新啟動](#)
- [故障診斷：Active Directory 網域問題](#)
- [故障診斷：使用 CloudWatch 指標](#)

## 錯誤：FileMissing

FileMissing 錯誤類似於ObjectMissing錯誤，解決錯誤的步驟相同。當指定檔案閘道以外的寫入器從 Amazon FSx 刪除指定的檔案時，您可能會收到FileMissing錯誤。任何後續上傳至 Amazon FSx 或從 Amazon FSx 擷取物件都會失敗。

### 解決 FileMissing 錯誤

1. 將檔案的最新副本儲存至 SMB 用戶端的本機檔案系統（您需要在步驟 3 中使用此檔案副本）。
2. 使用 SMB 用戶端從檔案閘道刪除檔案。
3. 使用 SMB 用戶端複製您在步驟 1 Amazon FSx 中儲存的最新版本檔案。透過您的檔案閘道執行此操作。

## 錯誤：FsxFileSystemAuthenticationFailure

當附加檔案系統時提供的登入資料過期，或其權限已撤銷時，您可能會收到FsxFileSystemAuthenticationFailure錯誤。

解決 FsxFileSystemAuthenticationFailure 錯誤

1. 確定連接 Amazon FSx 檔案系統時提供的登入資料仍然有效。
2. 確定使用者擁有所有必要的許可，如[連接 Amazon FSx for Windows File Server 檔案系統](#)所述。

## 錯誤：FsxFileSystemConnectionFailure

當無法從閘道機器存取 Amazon FSx 伺服器時，您可能會收到FsxFileSystemConnectionFailure錯誤。

解決 FsxFileSystemConnectionFailure 錯誤

1. 確保所有防火牆和 VPC 規則允許閘道機器和 Amazon FSx 伺服器之間的連線。
2. 確定 Amazon FSx 伺服器正在執行。

## 錯誤：FsxFileSystemFull

當 Amazon FSx 檔案系統中沒有足夠的可用磁碟空間時，您可能會收到FsxFileSystemFull錯誤。

解決 FsxFileSystemFull 錯誤

- 增加 Amazon FSx 檔案系統的儲存空間。

## 錯誤：GatewayClockOutOfSync

當閘道偵測到本機系統時間和 AWS Storage Gateway伺服器報告的時間之間有 5 分鐘或更多的差異時，您可能會收到GatewayClockOutOfSync錯誤。時鐘同步問題可能會對閘道與之間的連線產生負面影響 AWS。如果閘道時鐘不同步，NFS 和 SMB 連線可能會發生 I/O 錯誤，而 SMB 使用者可能會發生身分驗證錯誤。

## 解決 GatewayClockOutOfSync 錯誤

- 檢查閘道和 NTP 伺服器之間的網路組態。如需同步閘道 VM 時間和更新 NTP 伺服器組態的詳細資訊，請參閱[為您的閘道設定網路時間協定 \(NTP\) 伺服器](#)。

## 錯誤：InvalidFileState

當指定閘道以外的寫入器修改指定檔案共享中的指定檔案時，您可能會收到InvalidFileState錯誤。因此，閘道上檔案的狀態與 Amazon FSx 中的狀態不相符。後續從 Amazon FSx 上傳或擷取檔案可能會失敗。

### 解決 InvalidFileState 錯誤

1. 將檔案的最新副本儲存至 SMB 用戶端的本機檔案系統（您需要此檔案才能在步驟 4 中複製）。如果 Amazon FSx 中的檔案版本是最新版本，請下載該版本。您可以使用任何 SMB 用戶端直接存取 Amazon FSx 共用來執行此操作。
2. 直接刪除 Amazon FSx 中的檔案。
3. 使用 SMB 用戶端從閘道刪除檔案。
4. 使用您的 SMB 用戶端，透過檔案閘道將您在步驟 1 中儲存的最新版本檔案複製到 Amazon FSx。

## 錯誤：ObjectMissing

當指定檔案閘道以外的寫入器從 Amazon FSx 刪除指定的檔案時，您可能會收到ObjectMissing錯誤。任何後續上傳至 Amazon FSx 或從 Amazon FSx 擷取物件都會失敗。

### 解決 ObjectMissing 錯誤

1. 將檔案的最新副本儲存至 SMB 用戶端的本機檔案系統（您需要在步驟 3 中使用此檔案副本）。
2. 使用 SMB 用戶端從檔案閘道刪除檔案。
3. 使用 SMB 用戶端複製您在步驟 1 Amazon FSx 中儲存的最新版本檔案。透過您的檔案閘道執行此操作。

## 錯誤：DroppedNotifications

當閘道根磁碟上的可用儲存空間小於 1 GB，或在 1 分鐘內產生超過 100 個運作狀態通知時，您可能會看到DroppedNotifications錯誤，而不是其他預期的 CloudWatch 日誌項目類型。在這些情況下，閘道會停止產生詳細的 CloudWatch 日誌通知做為預防措施。

## 解決 DroppedNotifications 錯誤

1. 檢查 Storage Gateway Root Disk Usage 主控台中閘道的監控索引標籤上的指標，以判斷可用的根磁碟空間是否不足。
2. 如果可用空間小於 1 GB，請增加閘道根儲存磁碟的大小。如需說明，請參閱虛擬機器 Hypervisor 的文件。

若要增加 Amazon EC2 閘道的根磁碟大小，請參閱《Amazon Elastic Compute Cloud 使用者指南》中的[請求修改 EBS 磁碟區](#)。

### Note

無法增加 AWS Storage Gateway 硬體設備的根磁碟大小。

3. 重新啟動您的閘道。

## 通知：HardReboot

當閘道 VM 意外重新啟動時，您可能會收到 HardReboot 通知。這種重新啟動可能是因為電源中斷、硬體故障或其他事件。對於 VMware 閘道，vSphere 高可用性應用程式監控重設可能會導致此事件。

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。

## 通知：重新啟動

當閘道 VM 重新啟動時，您可能會收到重新啟動通知。您可以使用 VM Hypervisor Management 主控台或 Storage Gateway 主控台來重新啟動閘道 VM。您也可以在此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。

## 故障診斷：Active Directory 網域問題

FSx File Gateway 不會為 Active Directory 網域問題產生特定日誌訊息。如果您在將閘道加入 Active Directory 網域時遇到問題，請執行下列動作：

- 確認閘道並未嘗試使用唯讀網域控制站 (RODC) 加入網域。

- 確認閘道已設定為使用正確的 DNS 伺服器。

例如，如果您嘗試將 Amazon EC2 閘道執行個體加入 AWS 受管 Active Directory，請確認 EC2 VPC 的 DHCP 選項集指定受 AWS 管 Active Directory DNS 伺服器。

您透過 VPC DHCP 選項集設定的 DNS 伺服器會提供給 VPC 中的所有 EC2 執行個體。如果您想要為個別閘道指定 DNS 伺服器，您可以使用該閘道的 EC2 本機主控台來執行此操作。

對於內部部署閘道，您可以使用 VM 本機主控台指定 DNS 伺服器。

- 從閘道本機主控台的命令提示字元執行下列命令，以確認閘道網路連線。將反白顯示的變數取代為部署中的實際網域名稱和 IP 地址。

```
dig -d ExampleDomainName  
ncport -d ExampleDomainControllerIPAddress -p 445  
ncport -d ExampleDomainControllerIPAddress -p 389
```

- 確認您的 Active Directory 服務帳戶具有必要的許可。如需詳細資訊，請參閱 [Active Directory 服務帳戶許可要求](#)。
- 確認閘道加入正確的組織單位 (OU)。

加入網域會使用閘道的閘道 ID 做為帳戶名稱（例如，SGW-1234ADE），在預設的電腦容器（非 OU）中建立 Active Directory 電腦帳戶。您無法自訂此帳戶的名稱。

如果您的 Active Directory 環境具有新電腦物件的指定 OU，您必須在加入網域時指定該 OU。

如果您在嘗試加入指定的 OU 時遇到存取遭拒錯誤，請洽詢 Active Directory 網域管理員。管理員可能需要預先設定閘道的電腦帳戶，才能加入網域。如需詳細資訊，請參閱 [如何疑難排解將 Storage Gateway 檔案閘道加入網域以進行 Microsoft Active Directory 身分驗證的問題？](#)。

- 從閘道本機主控台的命令提示字元執行下列命令，確認閘道的主機名稱可在 DNS 中解析。將反白顯示的變數取代為閘道的實際主機名稱。

```
dig -d ExampleHostName -r A
```

如果您已為閘道設定自訂主機名稱，則必須手動新增指向其 IP 地址的 DNS A 記錄。

- 確認閘道與網域控制器之間的網路延遲相當低。如果閘道未在 20 秒內收到來自網域控制器的回應，則加入網域的查詢可能會逾時。

如果您使用 [JoinDomain](#) CLI 命令將閘道加入網域，您可以新增 `--timeout-in-seconds` 旗標，將逾時增加到最多 3,600 秒。

- 確認您用來將閘道加入網域的 Active Directory 使用者具有執行此作業所需的權限。

## 故障診斷：使用 CloudWatch 指標

您可以在下面找到使用 Amazon CloudWatch 指標搭配 Storage Gateway 處理問題之動作的相關資訊。

### 主題

- [瀏覽目錄時，您的閘道反應緩慢](#)
- [您的閘道未回應](#)
- [您在 Amazon FSx 檔案系統中看不到檔案](#)
- [您在 Amazon FSx 檔案系統中看不到較舊的快照](#)
- [您的閘道傳輸資料到 Amazon FSx 的速度緩慢](#)
- [您的閘道備份任務失敗，或寫入閘道時發生錯誤](#)

### 瀏覽目錄時，您的閘道反應緩慢

如果您的檔案閘道在執行ls命令或瀏覽目錄時反應緩慢，請檢查 IndexFetch和 IndexEviction CloudWatch 指標：

- 當您執行ls命令或瀏覽目錄時，如果IndexFetch指標大於 0，您的 File Gateway 會啟動，但不提供有關受影響目錄內容的資訊，且必須存取 FSx for Windows File Server。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，表示您的檔案閘道已達到當時可在其快取中管理的限制。在這種情況下，您的檔案閘道必須從最近最少存取的目錄中釋放一些儲存空間，以列出新的目錄。如果經常發生這種情況且效能受到影響，請聯絡 支援。

與相關 Amazon FSx 檔案系統 支援 的內容和建議討論，以根據您的使用案例改善效能。

### 您的閘道未回應

如果您的檔案閘道沒有回應，請執行下列動作：

- 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，檔案閘道可能會在重建索引快取至 RAM 時，因為根磁碟緩慢而遇到瓶頸。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指標與MemTotalBytes指標等於或幾乎相同，則檔案閘道會用盡可用的 RAM。請確定您的檔案閘道至少具有所需的最低 RAM。如果已經這麼做，請考慮根據您的工作負載和使用案例，將更多 RAM 新增至您的檔案閘道。

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。如果連接了許多用戶端，您可能需要將更多 RAM 新增至檔案閘道。

## 您在 Amazon FSx 檔案系統中看不到檔案

如果您注意到閘道上的檔案未反映在 Amazon FSx 檔案系統中，請檢查 FilesFailingUpload 指標。如果指標報告某些檔案上傳失敗，請檢查您的運作狀態通知。當檔案上傳失敗時，閘道會產生運作狀態通知，其中包含問題的詳細資訊。

## 您在 Amazon FSx 檔案系統中看不到較舊的快照

FSx File Gateway 上的某些檔案操作，例如頂層資料夾重新命名或許可變更，可能會導致多個檔案操作，導致 FSx for Windows File Server 檔案系統具有高 I/O 負載。如果您的檔案系統沒有足夠的工作負載效能資源，檔案系統可能會刪除[影子複本](#)，因為它會將持續 I/O 的可用性優先於歷史影子複本保留。

在 Amazon FSx 主控台中，檢查監控和效能頁面，查看您的檔案系統是否佈建不足。如果是，您可以切換到 SSD 儲存體、增加輸送量容量或增加 SSD IOPS 來處理工作負載。

## 您的閘道傳輸資料到 Amazon FSx 的速度緩慢

如果您的檔案閘道將資料傳輸到 Amazon FSx for Windows File Server，請執行下列動作：

- 如果CachePercentDirty指標為 80 或更高，您的檔案閘道將資料寫入磁碟的速度會比將資料上傳至 Amazon FSx for Windows File Server 的速度更快。考慮增加從檔案閘道上傳的頻寬、新增一或多個快取磁碟，或減慢用戶端寫入速度，或增加相關聯 Amazon FSx for Windows File Server 的輸送量容量。
- 如果CachePercentDirty指標很低，請檢查IoWaitPercent指標。如果 IoWaitPercent 大於 10，您的檔案閘道可能會因為本機快取磁碟的速度而遇到瓶頸。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。

## 您的閘道備份任務失敗，或寫入閘道時發生錯誤

如果您的檔案閘道備份任務失敗，或寫入檔案閘道時發生錯誤，請執行下列動作：

- 如果CachePercentDirty指標為 90% 或更高，您的檔案閘道就無法接受對磁碟的新寫入，因為快取磁碟上沒有足夠的可用空間。若要查看您的檔案閘道上傳到 FSx for Windows File Server 的速度，請檢視 CloudBytesUploaded 指標。將該指標與 WriteBytes 指標進行比較，該指標顯示用戶端將檔案寫入檔案閘道的速度。如果 SMB 用戶端寫入檔案閘道的速度比上傳至 FSx for Windows File Server 的速度快，請新增更多快取磁碟，以至少涵蓋備份任務的大小。或者，增加上傳頻寬。
- 如果備份任務等大型檔案副本失敗，但CachePercentDirty指標低於 80%，您的檔案閘道可能會命中用戶端工作階段逾時。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。

## 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

- [運作狀態通知](#)
- [指標](#)

## 運作狀態通知

在 VMware vSphere HA 上執行閘道時，所有閘道都會對您設定的 Amazon CloudWatch 日誌群組產生下列運作狀態通知。這些通知會進入名為 AvailabilityMonitor 的日誌串流。

主題

- [通知：重新啟動](#)
- [通知：HardReboot](#)

- [通知 : HealthCheckFailure](#)
- [通知 : AvailabilityMonitorTest](#)

## 通知 : 重新啟動

當閘道 VM 重新啟動時，您可能會收到重新啟動通知。您可以使用 VM Hypervisor Management 主控台或 Storage Gateway 主控台來重新啟動閘道 VM。您也可以在此期間使用閘道軟體來重新啟動。

### 採取動作

如果重新啟動的時間在閘道所設定之[維護開始時間](#)的 10 分鐘以內，這可能是正常的情況，而不是任何問題的徵兆。如果重新啟動很常在維護時段外發生，請檢查閘道是否已手動重新啟動。

## 通知 : HardReboot

當閘道 VM 意外重新啟動時，您可能會收到 HardReboot 通知。這種重新啟動可能是因為電源中斷、硬體故障或其他事件。對於 VMware 閘道，vSphere 高可用性應用程式監控重設可能會導致此事件。

### 採取動作

當閘道在這種環境中執行時，請檢查 HealthCheckFailure 通知是否存在，並參閱 VM 的 VMware 事件記錄。

## 通知 : HealthCheckFailure

若是 VMware vSphere HA 上的閘道，當運作狀態檢查失敗且請求 VM 重新啟動時，您可能會收到 HealthCheckFailure 通知。此事件也會在監控可用性的測試期間發生，並顯示於 AvailabilityMonitorTest 通知中。在此情況下，則預期會收到 HealthCheckFailure 通知。

### Note

此通知僅適用於 VMware 閘道。

### 採取動作

如果此事件在沒有 AvailabilityMonitorTest 通知的情況下重複發生，請檢查您的 VM 基礎設施是否有問題 (儲存空間、記憶體等)。如果您需要其他協助，請聯絡支援。

## 通知：AvailabilityMonitorTest

對於 VMware vSphere HA 上的閘道，您可以在 VMware 中[執行可用性和應用程式監控](#)系統的測試時收到 AvailabilityMonitorTest 通知。

## 指標

AvailabilityNotifications 指標可在所有閘道上使用。此指標會計算閘道產生的可用相關運作狀態通知數目。使用 Sum 統計資料，即可觀察閘道是否發生任何可用性相關事件。如需事件的詳細資訊，請參閱您設定的 CloudWatch 日誌群組。

# 檔案閘道的最佳實務

本節包含下列主題，提供使用閘道、檔案共用、儲存貯體和資料之最佳實務的相關資訊。我們建議您熟悉本節中概述的資訊，並嘗試遵循這些準則，以避免您的發生問題 AWS Storage Gateway。如需診斷和解決部署可能遇到之常見問題的其他指導，請參閱 [針對 Storage Gateway 部署的問題進行故障診斷](#)。

## 主題

- [最佳實務：復原您的資料](#)
- [直接從 Amazon FSx 上的備份或快照還原](#)
- [清除不必要的資源](#)

## 最佳實務：復原您的資料

雖然這種情況極少發生，但您的閘道可能遇到無法復原的故障。這種故障可能發生在您的虛擬機器 (VM)、閘道本身、本機儲存體或其他地方。如果發生故障，我們建議您按照下列合適各節中的指示來復原資料。

### Important

Storage Gateway 不支援從 Hypervisor 或 Amazon EC2 Amazon Machine Image (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。

## 從非預期的虛擬機器關機復原

如果您的 VM 因非預期原因關閉 (例如停電)，您的閘道就會無法連接。當電力和網路連線還原後，您的閘道就可以連接並開始正常運作。下列是您可在此時採取的步驟，有利於復原您的資料：

- 如果中斷導致網路連線問題，您可以故障診斷此問題。如需如何測試網路連線的資訊，請參閱 [測試閘道的網路連線](#)。

## 從故障的快取磁碟復原資料

如果您的快取磁碟發生故障，我們建議根據您的情況，使用下列步驟復原您的資料：

- 如果發生故障的原因是快取磁碟已從您的主機移除，請關閉閘道、重新新增磁碟並重新啟動閘道。

## 從無法存取的資料中心復原資料

如果您的閘道或資料中心因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。

### 從無法存取的資料中心中的檔案閘道復原資料

對於檔案閘道，您可以將新的系統映射至 FSx for Windows File Server，其中包含您要復原的資料。

1. 在 Amazon EC2 主機上建立新的檔案閘道。如需詳細資訊，請參閱[部署 FSx 檔案閘道的預設 Amazon EC2 主機](#)。
2. 在您建立的 EC2 閘道上建立新的系統。如需詳細資訊，請參閱[建立 FSx for Windows File Server 檔案系統](#)。
3. 在用戶端上掛載系統，並將其映射至 SFSx for Windows File Server，其中包含您要復原的資料。如需詳細資訊，請參閱[和使用您的檔案共用](#)。

## 直接從 Amazon FSx 上的備份或快照還原

在某些情況下，您可能需要使用先前時間點的備份或快照，直接還原 Amazon FSx 檔案系統上的資料。在這些執行個體中，備份應用程式和 FSx 檔案閘道之間存在建立雙寫入器案例的風險，這可能會導致檔案卡住或不相符。若要避免從備份或快照還原 Amazon FSx 檔案系統時發生問題，請使用下列程序。

### Note

在您使用此程序從備份或快照還原 Amazon FSx 檔案系統之後，目前存放在 FSx 檔案閘道中的任何快取資料都將無效。

### 避免從備份或快照還原 Amazon FSx 檔案系統時發生問題

1. 使用 Storage Gateway 主控台從 FSx 檔案閘道分離 Amazon FSx 檔案系統。FSx
2. 直接在您的 Amazon FSx 檔案系統上還原備份或快照。
3. 使用 Storage Gateway 主控台將 Amazon FSx 檔案系統重新連接至 FSx 檔案閘道。

## 清除不必要的資源

最佳實務是建議清除 Storage Gateway 資源，以避免意外或不必要的費用。例如，如果您建立閘道做為示範練習或測試，請考慮將其及其虛擬設備從部署中刪除。使用下列程序來清理資源。

### 清除不需要的資源

1. 如果您不再打算繼續使用閘道，請將其刪除。如需詳細資訊，請參閱[刪除您的閘道並移除相關聯的資源](#)。
2. 從內部部署主機刪除 Storage Gateway VM。如果您已在 Amazon EC2 執行個體上建立閘道，請終止執行個體。

## 其他 Storage Gateway 資源

本節包含下列主題，提供與設定和使用 相關的其他資訊和資源 AWS Storage Gateway：

### 主題

- [主機設定](#) - 了解如何為您的閘道部署和設定虛擬機器主機。
- [搭配 VMware HA 使用 Storage Gateway](#) - 了解如何設定 Storage Gateway 以使用 VMware vSphere 高可用性功能。
- [取得啟用金鑰](#) - 了解在部署新閘道時，在何處尋找您需要提供的啟用金鑰。
- [使用 Direct Connect](#) - 了解如何在內部部署閘道和 AWS 雲端之間建立專用網路連線。
- [Active Directory 許可](#) - 了解您的服務帳戶必須具備哪些許可，才能將閘道加入 Active Directory 網域。
- [取得閘道設備的 IP 地址](#) - 了解如何尋找閘道的虛擬機器主機 IP 地址，您在部署新閘道時需要提供這些地址。
- [了解資源和資源 IDs](#) - 了解如何 AWS 識別 Storage Gateway 建立的資源和子資源。
- [標記您的 資源](#) - 了解如何使用中繼資料標籤來分類您的資源，並讓它們更容易管理。
- [開放原始碼元件](#) - 了解用於提供 Storage Gateway 功能的第三方工具和授權。
- [配額](#) - 了解檔案閘道的限制和配額，包括檔案共用和本機快取磁碟的最小和最大限制。

## 部署和設定閘道 VM 主機

下列主題提供有關為您的閘道設定虛擬機器主機平台的資訊。

### 主題

- [部署 FSx 檔案閘道的預設 Amazon EC2 主機](#)
- [部署 FSx 檔案閘道的自訂 Amazon EC2 主機](#)
- [修改 Amazon EC2 執行個體中繼資料選項](#)
- [同步 VM 時間與 Hyper-V 或 Linux KVM 主機時間](#)
- [同步 VM 時間與 VMware 主機時間](#)
- [為您的閘道設定網路轉接器](#)
- [將 VMware vSphere High Availability 與 Storage Gateway 搭配使用](#)

## 部署 FSx 檔案閘道的預設 Amazon EC2 主機

本主題列出使用預設規格部署 Amazon EC2 主機的步驟。

您可以在 FSx File Gateway。Amazon EC2 AWS Storage Gateway Amazon Machine Image (AMI) 提供為社群 AMI。

### Note

Storage Gateway 社群 AMI 已發佈且完整支援 AWS。您可以看到發佈者是經過驗證 AWS 的提供者。

- 若要設定 Amazon EC2 執行個體，請在工作流程的平台選項區段中選擇 Amazon EC2 作為主機平台。如需設定 Amazon EC2 執行個體的指示，請參閱[部署 Amazon EC2 執行個體以託管您的 Amazon FSx 檔案閘道](#)。
- 選取啟動執行個體以在 Amazon EC2 主控台中開啟 AWS Storage Gateway AMI 範本，並自訂其他設定，例如執行個體類型、網路設定和設定儲存。
- 或者，您可以選取 Storage Gateway 主控台的使用預設設定，以使用預設組態部署 Amazon EC2 執行個體。

使用預設設定建立的 Amazon EC2 執行個體具有下列預設規格：

- 執行個體類型：m5.xlarge
- 網路設定
  - 針對 VPC，選擇您要執行 EC2 執行個體的 VPC。
  - 對於子網路，指定 EC2 執行個體應在其中啟動的子網路。

### Note

只有從 VPC 管理主控台啟用自動指派公有 IP 地址設定時，VPC 子網路才會出現在下拉式清單中。

- 自動分配公用 IP：已啟動
- EC2 安全群組已建立並與 EC2 執行個體建立關聯。安全群組具有下列傳入連接埠規則：

**Note**

在閘道啟動期間，您需要開啟連接埠 80。啟動後，連接埠會立即關閉。之後，您的 EC2 執行個體只能透過所選 VPC 的其他連接埠存取。

閘道上的檔案共享只能從與閘道位於相同 VPC 的主機存取。如果需要從 VPC 外部的主機存取檔案共享，您應該更新適當的安全群組規則。

您可以隨時編輯安全群組，方法是導覽至 Amazon EC2 執行個體詳細資訊頁面、選取安全性、導覽至安全群組詳細資訊，然後選擇安全群組 ID。

連接埠	通訊協定	檔案系統協定				
80	TCP	用於啟用的 HTTP 存取				
137	UDP	NetBIOS				
138	UDP	NetBIOS				
139	TCP、UDP	SMB				
389	TCP	LDAP				
445	TCP	SMB				

- 設定儲存

預設設定	AMI 根磁碟區	磁碟區 2 快取				
裝置名稱		'/dev/sdb'				
大小	80 GiB	165 GiB				

預設設定	AMI 根磁碟區	磁碟區 2 快取				
磁碟區類型	gp3	gp3				
IOPS	3000	3000				
在終止時刪除	是	是				
加密	否	否				
輸送量	125	125				

## 部署 FSx 檔案閘道的自訂 Amazon EC2 主機

您可以在 FSx File Gateway。Amazon EC2 AWS Storage Gateway Amazon Machine Image (AMI) 提供為社群 AMI。

### Note

Storage Gateway 社群 AMI 已發佈且完整支援 AWS。您可以看到發佈者是經過驗證 AWS 的提供者。

FSx File Gateway AMIs 使用以下命名慣例。附加至 AMI 名稱的版本編號會隨每個版本版本而變更。

`aws-storage-gateway-FILE_FSX_SMB-2.2.3`

### 部署 Amazon EC2 執行個體以託管您的 Amazon FSx 檔案閘道

1. 使用 Storage Gateway 主控台開始設定新閘道。如需說明，請參閱[設定 Amazon FSx 檔案閘道](#)。當您到達平台選項區段時，請選擇 Amazon EC2 作為主機平台，然後使用下列步驟啟動將託管檔案閘道的 Amazon EC2 執行個體。
2. 選擇啟動執行個體以在 Amazon EC2 主控台中開啟 AWS Storage Gateway AMI 範本，您可以在其中設定其他設定。

使用快速啟動以預設設定啟動 Amazon EC2 執行個體。如需 Amazon EC2 Quicklaunch 預設規格的詳細資訊，請參閱 [Quicklaunch Configuration Specifications for Amazon EC2](#)。

- 對於名稱，輸入 Amazon EC2 執行個體的名稱。部署執行個體後，您可以搜尋此名稱，在 Amazon EC2 主控台的清單頁面上尋找您的執行個體。
- 在執行個體類型區段中，從執行個體類型清單中，為執行個體選擇硬體組態。硬體組態必須符合特定的最低需求，才能支援閘道。建議您從 m5.xlarge 執行個體類型開始，它符合您閘道正常運作的最低硬體要求。如需詳細資訊，請參閱 [Amazon EC2 執行個體類型的需求](#)。

必要時，您可以在啟動執行個體之後調整執行個體的大小。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的 [調整執行個體的大小](#)。

#### Note

有些執行個體類型，特別是 i3 EC2，會使用 NVMe SSD 磁碟。當您啟動或停止檔案閘道時，這些可能會導致問題；例如，您可能會遺失快取中的資料。監控 CachePercentDirty Amazon CloudWatch 指標，而且僅在參數為 0 時啟動或停止您的系統。若要深入了解閘道的監控指標，請參閱 CloudWatch 文件中的 [Storage Gateway 指標和維度](#)。

- 在金鑰對 (登入) 區段中，針對金鑰對名稱(必要)，選取您要用來安全連線至執行個體的金鑰對。如有必要，您可以建立新的金鑰對。如需詳細資訊，請參閱《適用於 Linux 執行個體的 Amazon Elastic Compute Cloud 使用者指南》中的 [建立金鑰對](#)。
- 在網路設定區段中，檢閱預先設定的設定值，然後選擇編輯以變更下列欄位：
  - 對於 VPC：必要項目，請選擇您要啟動 Amazon EC2 執行個體的 VPC。如需詳細資訊，請參閱《Amazon Virtual Private Cloud 使用者指南》中的 [VPC 如何運作](#)。
  - (選用) 對於子網路，請選擇要在其中啟動 Amazon EC2 執行個體子網路。
  - 在 Auto-assign Public IP (自動指派公有 IP) 中，選擇 Enable (啟用)。
- 在防火牆 (安全群組) 子區段中，檢閱預先設定的設定值。您可以視需要變更要為 Amazon EC2 執行個體建立的新安全群組的預設名稱和說明，或選擇從現有安全群組套用防火牆規則。
- 在傳入安全群組規則子區段中，新增防火牆規則，以開啟用戶端將用來連線至執行個體的連接埠。如需 FSx File Gateway 所需連接埠的詳細資訊，請參閱 [連接埠需求](#)。如需詳細資訊，請參閱《適用於 Linux 執行個體的 Amazon Elastic Compute Cloud 使用者指南》中的 [安全群組規則](#)。

**Note**

Amazon FSx File Gateway 需要為傳入流量開啟 TCP 連接埠 80，並在閘道啟用期間開啟一次性 HTTP 存取。啟用後，您可以關閉此連接埠。

此外，您必須為 SMB 存取開啟 TCP 連接埠 445、為 NetBIOS 存取開啟 UDP 連接埠 137、為 NetBIOS 存取開啟 UDP 連接埠 138，以及為 LDAP 存取開啟 TCP 連接埠 389。

9. 在進階網路組態子區段中，檢閱預先設定的設定，並視需要進行變更。
10. 在新增儲存體頁面上，選擇新增新的磁碟區將儲存體新增到您的閘道執行個體。

**Important**

除了預先設定的根磁碟區之外，您還必須為快取儲存新增至少一個具有至少 150 GiB 容量的 Amazon EBS 磁碟區。為了提高效率，我們建議為每個至少 150 GiB 的快取儲存配置多個 EBS 磁碟區。

11. 在進階詳細資訊區段中，檢閱預先設定的設定值，並視需要進行變更。
12. 選擇啟動執行個體以使用已設定的設定值來啟動新的 Amazon EC2 閘道執行個體。
13. 若要驗證新執行個體是否已成功啟動，請導覽至 Amazon EC2 主控台內的執行個體頁面，然後按名稱搜尋新執行個體。確定執行個體狀態顯示為執行中以及具有綠色核取記號，且狀態核取方塊已完成，並顯示綠色核取記號。
14. 從詳細資訊頁面選取執行個體。從執行個體摘要區段複製公有 IP 地址，然後返回 Storage Gateway 主控台內的設定閘道頁面，以繼續設定您的 Amazon FSx 檔案閘道。

您可以使用 Storage Gateway 主控台或查詢 AWS Systems Manager 參數存放區，判斷用於啟動檔案閘道的 AMI ID。

若要判定 AMI ID，請執行以下操作之一：

- 使用 Storage Gateway 主控台開始設定新閘道。如需說明，請參閱[設定 Amazon FSx 檔案閘道](#)。當您到達平台選項區段時，請選擇 Amazon EC2 作為主機平台，然後選擇啟動執行個體以在 Amazon EC2 主控台中開啟 AWS Storage Gateway AMI 範本。

系統會將您重新導向至 EC2 社群 AMI 頁面，您可以在 URL 中查看 AWS 區域的 AMI ID。

- 查詢 Systems Manager 參數存放區。您可以使用 AWS CLI 或 Storage Gateway API 來查詢命名空間下的 Systems Manager 公有參數 `/aws/service/storagegateway/ami/FILE_FSX_SMB/latest`。例如，使用下列 CLI 命令會在 AWS 區域 您指定的 中傳回目前 AMI 的 ID。

```
aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/FILE_FSX_SMB/latest
```

CLI 命令會傳回類似以下的輸出。

```
{
  "Parameter": {
    "Type": "String",
    "LastModifiedDate": 1561054105.083,
    "Version": 18,
    "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/FILE_FSX_SMB/latest",
    "Name": "/aws/service/storagegateway/ami/FILE_FSX_SMB/latest",
    "Value": "ami-033d1edba5606cffb"
  }
}
```

## 修改 Amazon EC2 執行個體中繼資料選項

執行個體中繼資料服務 (IMDS) 是一種執行個體元件，可提供對 Amazon EC2 執行個體中繼資料的安全存取。執行個體可設定為接受使用 IMDS 第 1 版 (IMDSv1) 的傳入中繼資料請求，或要求所有中繼資料請求使用 IMDS 第 2 版 (IMDSv2)。IMDSv2 會使用工作階段導向的請求，並減緩可能用來嘗試存取 IMDS 的幾種漏洞類型。如需 IMDSv2 的相關資訊，請參閱《Amazon Elastic Compute Cloud 使用者指南》中的[執行個體中繼資料服務第 2 版的運作方式](#)。

對於託管 Storage Gateway 的所有 Amazon EC2 執行個體，我們建議您需要 IMDSv2。Amazon EC2 根據預設，所有新啟動的閘道執行個體都需要 IMDSv2。如果您現有的執行個體仍設定為接受 IMDSv1 中繼資料請求，請參閱《Amazon Elastic Compute Cloud 使用者指南》中的[需要使用 IMDSv2](#)，以取得修改執行個體中繼資料選項以需要使用 IMDSv2 的說明。套用此變更不需要重新啟動執行個體。

## 同步 VM 時間與 Hyper-V 或 Linux KVM 主機時間

對於部署在 VMware ESXi 上的閘道，設定 Hypervisor 主機時間並將虛擬機器時間同步到主機就足以避免時間偏離。如需詳細資訊，請參閱[同步 VM 時間與 VMware 主機時間](#)。對於部署在 Microsoft Hyper-V 或 Linux KVM 上的閘道，我們建議您使用下列程序定期檢查虛擬機器時間。

檢視 Hypervisor 閘道虛擬機器的時間，並將其同步至網路時間通訊協定 (NTP) 伺服器

1. 登入您閘道的本機主控台：

- 如需登入 Microsoft Hyper-V 本機主控台的詳細資訊，請參閱[使用 Microsoft Hyper-V 存取閘道本機主控台](#)。
- 如需登入 Linux 核心型虛擬機器 (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 Storage Gateway 組態主功能表畫面上，輸入對應的數字以選取系統時間管理。

3. 在系統時間管理功能表畫面上，輸入對應的數字以選取檢視和同步系統時間。

閘道本機主控台會顯示目前的系統時間，並將其與 NTP 伺服器報告的時間進行比較，然後報告兩次之間的确切差異，以秒為單位。

4. 如果時間差異大於 60 秒，請輸入 **y** 以同步系統時間與 NTP 時間。否則，輸入 **n**。

時間同步可能需要一些時間。

## 同步 VM 時間與 VMware 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，在應用程式視窗左側面板中的閘道 VM 名稱上按一下滑鼠右鍵，開啟 VM 的內容選單，然後選擇編輯設定。

Virtual Machine Properties (虛擬機器屬性) 對話方塊隨即開啟。

- b. 選擇選項索引標籤，然後從選項清單中選擇 VMware 工具。

- c. 在虛擬機器屬性對話方塊右側的進階區段中，檢查使用主機同步訪客時間選項，然後選擇確定。

VM 會同步其時間與主機。

## 2. 設定主機時間。

請務必確定您的主機時鐘設定為正確時間。如果您尚未設定主機時鐘，請執行下列步驟來設定和同步它與 NTP 伺服器。

- a. 在 VMware vSphere 用戶端中，選取左側面板中的 vSphere 主機節點，然後選擇組態索引標籤。
- b. 選取 Software (軟體) 面板中的 Time Configuration (時間組態)，然後選擇 Properties (屬性) 連結。

Time Configuration (時間組態) 對話方塊隨即出現。

- c. 在日期和時間下，設定 vSphere 主機的日期和時間。
- d. 設定主機自動同步其時間與 NTP 伺服器。
  - i. 在時間組態對話方塊中選擇選項，然後在 NTP 協助程式 (ntpd) 選項對話方塊中，選擇左側面板中的 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 做為網域名稱。

- iv. 在 NTP 協助程式 (ntpd) 選項對話方塊中，選擇左側面板中的一般。
- v. 在服務命令下，選擇開始以啟動服務。

請注意，如果您變更此 NTP 伺服器參考，或稍後新增另一個參考，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。

## 為您的閘道設定網路轉接器

Storage Gateway 預設使用單一 VMXNET3 (10 GbE) 網路轉接器，但您可以將閘道設定為使用多個網路轉接器，以便多個 IP 地址存取。建議您在下列其中一種狀況中執行此作業：

- 最大化輸送量 – 當網路轉接器存在瓶頸時，您可能想要最大化閘道的輸送量。
- 分隔應用程式：您可能需要區隔應用程式寫入閘道磁碟區的方式。例如，您可以選擇只讓關鍵儲存應用程式使用一種為您閘道定義的特定轉接器。
- 網路限制 – 您的應用程式環境可能需要您將檔案共用和連接到它們的啟動器保留在隔離的網路中。此網路與閘道與 AWS 通訊用的網路不同。

在典型的多轉接器使用案例中，會將一個轉接器設定為閘道通訊的路由 AWS（即預設閘道）。除了這個轉接器之外，啟動者必須與包含其連線之檔案共用的轉接器位於相同的子網路中。否則，可能無法與預定目標通訊。如果在用於與通訊的相同轉接器上設定目標 AWS，則檔案共用該目標的流量和 AWS 流量會流經相同的轉接器。

在某些情況下，您可以設定一個轉接器連接到 Storage Gateway 主控台，然後新增第二個轉接器。在這種情況下，Storage Gateway 會自動將路由表設定為使用第二個轉接器作為偏好的路由。如需如何設定多個轉接器的指示，請參閱下列主題：

### 主題

- [在 VMware ESXi 主機上設定多個 NICs 的閘道](#)
- [在 Microsoft Hyper-V 主機中為多張 NIC 設定您的閘道](#)

## 在 VMware ESXi 主機上設定多個 NICs 的閘道

下列程序假設您的閘道 VM 已定義一個 NIC，而且說明如何新增 VMware ESXi 的一個介面卡。

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. 在網路類型窗格中，確定已針對類型選取在開機時連線，然後選擇 下一步。

建議您搭配使用 VMXNET3 NIC 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 VM 的摘要 標籤，然後選擇 IP 地址方塊旁的檢視全部。虛擬機器 IP 地址視窗會顯示您可用來存取閘道的所有 IP 地址。確認針對閘道列出第二個 IP 地址。

 Note

可能需要一些時間，轉接器變更才會生效並重新整理 VM 摘要資訊。

7. 在 Storage Gateway 主控台中，開啟閘道。
8. 在 Storage Gateway 主控台的導覽窗格中，選擇閘道，然後選擇您已新增介面卡的閘道。確認在 Details (詳細資訊) 標籤中列出第二個 IP 地址。

如需 VMware、Hyper-V 和 KVM 主機之本機主控台常見任務的詳細資訊，請參閱 [在虛擬機器本機主控台上執行任務](#)

## 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 Manager 中，從虛擬機器面板選取閘道 VM。
3. 如果閘道 VM 尚未關閉，請在 VM 名稱上按一下滑鼠右鍵以開啟內容選單，然後選擇關閉。
4. 在閘道 VM 名稱上按一下滑鼠右鍵以開啟內容功能表，然後選擇設定。
5. 在設定對話方塊中的硬體下，選擇新增硬體。
6. 在設定對話方塊右側的新增硬體面板中，選擇網路轉接器，然後選擇新增以新增裝置。
7. 設定網路轉接器，然後選擇 Apply (套用) 以套用設定。

- 在設定對話方塊的硬體下，確認新的網路轉接器已新增至硬體清單，然後選擇確定。
- 使用 Storage Gateway 主控台開啟閘道。
- 在 Storage Gateway 主控台的導覽面板中，選擇閘道，然後選取您新增轉接器的閘道。確認第二個 IP 地址已列在詳細資訊索引標籤中。

如需 VMware、Hyper-V 和 KVM 主機之本機主控台常見任務的詳細資訊，請參閱[在虛擬機器本機主控台上執行任務](#)

## 將 VMware vSphere High Availability 與 Storage Gateway 搭配使用

Storage Gateway 透過與 VMware vSphere High Availability (VMware HA) 整合的一組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。

透過此整合，部署在 VMware 環境內部部署或 VMware Cloud on 中的閘道 AWS 會自動從大多數服務中斷中復原。此操作通常會在 60 秒以內完成，而且不會遺失資料。

### Note

如果您在 VMware HA 叢集中部署 Storage Gateway，建議您執行下列動作：

- 在叢集中僅一個主機上部署包含 Storage Gateway VM 的 VMware ESX .ova 可下載套件。
- 部署 .ova 套件時，請選取不是本機主機的資料存放區。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。
- 使用叢集時，如果您將 .ova 套件部署到叢集，請在出現提示時選取主機。或者，您可以直接部署至叢集中的主機。

下列主題說明如何在 VMware HA 叢集中部署 Storage Gateway：

### 主題

- [設定 vSphere VMware HA 叢集](#)
- [設定您的閘道類型](#)
- [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 叢集設定為與 Storage Gateway 搭配運作。

### 設定 VMware 叢集

1. 在 VMware vSphere 的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。若要這樣做，請為每個選項設定下列值：
  - Host Failure Response (主機故障回應)：Restart VMs (重新啟動 VM)
  - Response for Host Isolation (主機隔離回應)：Shut down and restart VMs (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
2. 調整下列的值以微調叢集敏感度：
  - 失敗間隔：在此間隔後，如果沒有收到 VM 訊號，則會重新啟動 VM。
  - 最短執行時間：在 VM 啟動以開始監控 VM 工具的訊號後，叢集會等待這段指定的時間。
  - 每個 VM 的最大重設：在最大重設時間範圍內，叢集會重新啟動 VM 的最大次數。
  - 最大重設時間範圍：計算每個 VM 重設的最大重設次數的時間範圍。

如果您不確定要設定哪些值，請使用這些設定範例：

- 失敗間隔：**30** 秒
- 最短執行時間：**120** 秒
- 每個 VM 的最大重設次數：**3**
- 最大重設時間範圍：**1** 小時

如果您在叢集上有其他正在執行的 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](#)。

## 設定您的閘道類型

使用下列程序來設定閘道

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 – [建立並啟動 Amazon FSx File Gateway](#)

## 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。如需說明，請參閱 VMware vSphere 線上文件中的[部署 OVF 或 OVA 範本](#)。

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。如需說明，請參閱 VMware vSphere 線上文件中的[自訂個別虛擬機器](#)。

為叢集上的其他 VM 新增覆寫選項

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

在 vSphere HA - VM 監控下為每個選項設定下列值：

- VM 監控：覆寫已啟用 - VM 和應用程式監控
- VM 監控敏感度：覆寫已啟用 - VM 和應用程式監控
- VM 監控：自訂
- 失敗間隔：**30**秒
- 最短執行時間：**120** 秒

- 每個 VM 的最大重設次數：5
- 重設時間範圍上限：1小時以內

## 啟用閘道

在 VMware 環境中部署 .ova 之後，請使用 Storage Gateway 主控台啟用閘道。如需說明，請參閱[檢閱設定](#)，以及啟用 [Amazon FSx File Gateway](#)。

## 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. 前往 <https://console.aws.amazon.com/storagegateway/home> 開啟 Storage Gateway 主控台。
2. 在導覽窗格中，選擇 閘道，然後選擇您要測試 VMware HA 的閘道。
3. 針對 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訊標籤中。

5. 選擇 退出。

您可以在 Amazon CloudWatch 日誌群組中找到有關 VMware HA 事件的資訊。如需詳細資訊，請參閱[使用 CloudWatch 日誌群組取得 FSx File Gateway 運作狀態日誌](#)。

## 取得閘道的啟用金鑰

若要接收閘道的啟用金鑰，請向閘道虛擬機器 (VM) 發出網頁請求。虛擬機器會傳回包含啟用金鑰的重新導向，該重新導向會當做 ActivateGateway API 動作的其中一個參數傳遞，以指定閘道的組態。如需詳細資訊，請參閱 Storage Gateway API 參考資料中的 [ActivateGateway](#)。

**Note**

如果未使用，閘道啟用金鑰會在 30 分鐘內過期。

您對閘道 VM 提出的請求包含進行啟用 AWS 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`。此查詢的輸出傳回啟用區域和金鑰。

此 URL 也包含 `vpcEndpoint` 使用 VPC 端點類型連線之閘道的 VPC 端點識別碼。

**Note**

AWS Storage Gateway 硬體設備、VM 映像範本和 Amazon EC2 Amazon Machine Image (AMI) 已預先設定 HTTP 服務，以接收和回應此頁面所述的 Web 請求。您不需要或建議您在閘道上安裝任何其他服務。

**主題**

- [Linux \(curl\)](#)
- [Linux \(bash/zsh\)](#)
- [Microsoft Windows PowerShell](#)
- [使用本機主控台](#)

**Linux (curl)**

以下範例顯示如何使用 Linux (curl) 取得啟用金鑰。

**Note**

將反白顯示的變數取代為閘道的實際值。可接受的值如下：

- `gateway_ip_address`：例如，閘道器的 IPV4 地址 172.31.29.201
- `gateway_type` - 您要啟用的閘道類型，例如 STORED、CACHED、FILE\_S3、VTL 或 FILE\_FSX\_SMB。

- *region\_code* : 您要啟用閘道的區域。請參閱《AWS 一般參考指南》中的[區域端點](#)。如果未指定此參數，或提供的值拼字錯誤或不符合有效區域，則命令會預設為us-east-1區域。
- *vpc\_endpoint* : 例如，閘道的 VPC 端點名稱 vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com。

若要取得公用端點的啟用金鑰：

```
curl "http://gateway_ip_address?activationRegion=region_code&no_redirect"
```

若要取得 VPC 端點的啟用金鑰：

```
curl "http://gateway_ip_address?  
activationRegion=region_code&vpcEndpoint=vpc_endpoint&no_redirect"
```

## Linux (bash/zsh)

下列範例顯示如何使用 Linux (bash/zsh) 擷取 HTTP 回應、剖析 HTTP 標頭及取得啟用金鑰的方式。

```
function get-activation-key() {  
    local ip_address=$1  
    local activation_region=$2  
    if [[ -z "$ip_address" || -z "$activation_region" || -z "$gateway_type" ]]; then  
        echo "Usage: get-activation-key ip_address activation_region gateway_type"  
        return 1  
    fi  
  
    if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?  
activationRegion=$activation_region&gatewayType=$gateway_type"); then  
        activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')  
        echo "$activation_key_param" | cut -f2 -d=  
    else  
        return 1  
    fi  
}
```

## Microsoft 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,
        [parameter(Mandatory=$true)][string]$GatewayType
    )
    PROCESS {
        $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion&gatewayType=$GatewayType" -MaximumRedirection 0 -
ErrorAction SilentlyContinue
        if ($request) {
            $activationKeyParam = $request.Headers.Location | Select-String -Pattern
"activationKey=([A-Z0-9-]+)"
            $activationKeyParam.Matches.Value.Split("=")[1]
        }
    }
}
```

## 使用本機主控台

下列如何使用本機主控台來產生和顯示啟用金鑰。

從本機主控台取得閘道的啟用金鑰

1. 以管理員身分登入您的本機主控台。
2. 登入並查看 AWS 設備啟用 - 設定主功能表後，選取 0 以選擇取得啟用金鑰。
3. 為閘道系列選項選取 Storage Gateway。
4. 出現提示時，輸入您要啟用閘道 AWS 區域的。
5. 輸入 1 公用端點或 2 VPC 端點做為網路類型。
6. 輸入 1 標準或 2 美國聯邦資訊處理標準 (FIPS) 做為端點類型。

## Direct Connect 搭配 Storage Gateway 使用

Direct Connect 會將您的內部網路連結至 Amazon Web Services Cloud。透過使用 Direct Connect 搭配 Storage Gateway，您可以建立高輸送量工作負載需求的連線，在內部部署閘道與之間提供專用的網路連線 AWS。

Storage Gateway 使用公用端點。建立 Direct Connect 連線後，您可以建立公有虛擬介面，以允許流量路由至 Storage Gateway 端點。公有虛擬界面會略過您網路路徑中的網際網路服務提供者。Storage Gateway 服務公有 Direct Connect 端點可以與位置位於相同的 AWS 區域，也可以位於不同的 AWS 區域。

下圖顯示 如何使用 Direct Connect Storage Gateway 的範例。  
網路架構顯示使用 AWS 直接連線連線至雲端的 Storage Gateway。

下列程序假設您已建立正常運作的閘道。

### Direct Connect 搭配 Storage Gateway 使用

1. 建立並建立內部部署資料中心與 Storage Gateway 端點之間的 AWS Direct Connect 連線。如需關於如何建立連線的詳細資訊，請參閱《Direct Connect 使用者指南》中的[Direct Connect 入門指南](#)。
2. 將您的內部部署 Storage Gateway 設備連接到 Direct Connect 路由器。
3. 建立公有虛擬界面，然後以同樣方式設定您的內部部署路由器。如需詳細資訊，請參閱《Direct Connect 使用者指南》中的[建立虛擬介面](#)。

如需的詳細資訊 Direct Connect，請參閱[什麼是 Direct Connect ?](#) Direct Connect 《使用者指南》中的。

## Active Directory 服務帳戶許可要求

如果您計劃使用 Microsoft Active Directory 為使用者提供對上的系統進行身分驗證的存取權 AWS Storage Gateway，您需要確定您擁有 Active Directory 服務帳戶，且該服務帳戶已委派許可將電腦加入您的網域。服務帳戶是 Active Directory 使用者帳戶，已委派執行特定任務的許可。當您將 Storage Gateway 加入 Active Directory 網域時，請提供此帳戶的使用者名稱和密碼登入資料。

Active Directory 服務帳戶必須在您要加入閘道的 OU 中委派下列許可：

- 能夠建立和刪除電腦物件

- 能夠重設密碼
- 修改許可的能力
- 限制帳戶讀取和寫入資料的能力
- 驗證讀取和寫入帳戶限制的能力
- 已驗證能夠寫入服務主體名稱
- 已驗證能夠寫入 DNS 主機名稱

這些代表將電腦物件加入 Active Directory 所需的最低許可集。如需詳細資訊，請參閱 Microsoft Windows Server 文件主題 [錯誤：當被委派控制的非管理員使用者嘗試將電腦加入網域控制站時，存取遭拒](#)。

## 取得閘道設備的 IP 地址

在您選擇主機以及部署閘道 VM 之後，即可連線和啟用閘道。若要執行此作業，您需要閘道 VM 的 IP 地址。您可以從閘道的本機主控台取得 IP 地址。您登入本機主控台，並從主控台頁面頂端取得 IP 地址。

針對在內部部署所部署的閘道，您也可以從虛擬化管理程序取得 IP 地址。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，傳回 Storage Gateway 主控台，並在主控台中輸入 IP 地址。

## 從 Amazon EC2 主機取得 IP 地址

若要取得閘道部署所在之 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。如需說明，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. 前往 <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。傳回 Storage Gateway 主控台，並輸入 IP 地址。

如果您要使用彈性 IP 地址予以啟用，請使用下列程序。

## 程序 2：使用彈性 IP 地址連線至閘道

1. 前往 <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。傳回 Storage Gateway 主控台，並輸入彈性 IP 地址。

## 了解 Storage Gateway 資源和資源 IDs

在 Storage Gateway 中，主要資源是閘道，但其他資源類型是檔案共享。檔案共用稱為子資源，除非它們與閘道相關聯，否則不存在。

這些資源和子資源具有與其相關聯的唯一 Amazon Resource Name (ARNs)，如下表所示。

資源類型	ARN 格式
閘道 ARN	arn:aws:storagegateway: <i>region:account-id</i> :gateway/ <i>gateway-id</i>
檔案共享 ARN	arn:aws:storagegateway: <i>region:account-id</i> :share/ <i>share-id</i>

## 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。

Storage Gateway 資源 ID 為大寫。不過，如果您將這些資源 IDs 與 Amazon EC2 API 搭配使用，Amazon EC2 會預期資源 IDs 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，閘道的 ID 可能是 `sgw-12A3456B`。如果您將此 ID 與 EC2 API 搭配使用，則必須將其變更為 `sgw-12a3456b`。否則，EC2 API 可能無法如預期運作。

## 標記 Storage Gateway 資源

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。

對於檔案閘道，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[使用標籤來控制對閘道和資源的存取](#)。

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:`。此字首已保留供 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 `@`。

## 使用標籤

您可以使用 Storage Gateway 主控台、Storage Gateway API，或是[Storage Gateway 命令列界 \(CLI\)](#) 來使用標籤。以下程序顯示在主控台上新增、編輯及刪除標籤的方式。

### 新增標籤

1. 前往 <https://console.aws.amazon.com/storagegateway/home> 開啟 Storage Gateway 主控台。

2. 在導覽窗格中，選擇您希望新增標籤的資源。

例如，若要為閘道新增標籤，請選擇 閘道，然後從閘道清單中選擇您希望新增標籤的閘道。

3. 選擇 Tags (標籤)，然後選擇 Add/edit tags (新增/編輯標籤)。
4. 在 Add/edit tags (新增/編輯標籤) 對話方塊中，選擇 Create tag (建立標籤)。
5. 針對 金鑰 輸入金鑰，並針對 值 輸入值。例如，您可以針對金鑰輸入 **Department**，並針對值輸入 **Accounting**。

#### Note

您可以將 Value (值) 方塊保留空白。

6. 選擇 建立標籤 以新增更多標籤。您可以為單一資源新增多個標籤。
7. 完成新增標籤後，請選擇 儲存。

### 編輯標籤

1. 前往 <https://console.aws.amazon.com/storagegateway/home> 開啟 Storage Gateway 主控台。
2. 選擇您要編輯標籤的資源。
3. 選擇 Tags (標籤) 以開啟 Add/edit tags (新增/編輯標籤) 對話方塊。
4. 選擇您要編輯之標籤旁的鉛筆圖示，然後編輯標籤。
5. 完成編輯標籤後，選擇儲存。

### 若要刪除標籤

1. 前往 <https://console.aws.amazon.com/storagegateway/home> 開啟 Storage Gateway 主控台。
2. 選擇您要刪除標籤的資源。
3. 選擇 Tags (標籤)，然後選擇 Add/edit tags (新增/編輯標籤) 以開啟 Add/edit tags (新增/編輯標籤) 對話方塊。
4. 選擇您要刪除之標籤旁的 X 圖示，然後選擇 儲存。

## 使用的開放原始碼元件 AWS Storage Gateway

本節說明我們交付 AWS Storage Gateway 功能所依賴的第三方工具和授權。

## 主題

- [Storage Gateway 的開放原始碼元件](#)
- [Amazon FSx 檔案閘道的開放原始碼元件](#)

## Storage Gateway 的開放原始碼元件

數個第三方工具和授權用於提供磁碟區閘道、磁帶閘道和 Amazon S3 檔案閘道的功能。

使用以下連結下載 AWS Storage Gateway 軟體隨附的特定開放原始碼軟體元件的原始程式碼：

- 針對部署在 VMware ESXi 上的 Storage Gateway 設備：[source.tar](#)
- 對於部署在 Microsoft Hyper-V 上的 Storage Gateway 設備：[source\\_hyperv.tar](#)
- 針對部署在 Linux 核心型虛擬機器 (KVM) 上的 Storage Gateway 設備：[source\\_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，請參閱《[第三方授權](#)》。

## Amazon FSx 檔案閘道的開放原始碼元件

數個第三方工具和授權用於提供 Amazon FSx 檔案閘道 (FSx 檔案閘道) 功能。

使用以下連結下載 FSx File Gateway 軟體隨附的特定開放原始碼軟體元件的原始程式碼：

- 對於 Amazon FSx File Gateway 2021-07-07 版本：[sgw-file-fsx-smb-open-source.tgz](#)
- 對於 Amazon FSx File Gateway 2021-04-06 版本：[sgw-file-fsx-smb-20210406-open-source.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，請參閱下列連結：

- 對於 Amazon FSx File Gateway 2021-07-07 版本：[第三方授權](#)。
- 對於 Amazon FSx File Gateway 2021-04-06 版本：[第三方授權](#)。

## FSx File Gateway的限制和配額

### Amazon FSx 檔案系統配額

下表列出 Amazon FSx 檔案系統的下限和上限限制和配額。

資源	每個 Amazon FSx 檔案系統的限制
標籤數量上限	50 個標籤
自動備份的最長保留期間	90 天
每個帳戶的單一目的地區域正在進行的備份複製請求數目上限。	5 個請求
SSD 檔案系統的最小儲存容量	32 GiB
HDD 檔案系統的最小儲存容量	2,000 GiB
SSD 和 HDD 檔案系統的儲存容量上限	64 TiB
輸送量容量下限	8 MBps
最大輸送量容量	2,048 MBps
Amazon FSx 檔案共用數量上限	100,000

## 適用於您閘道的建議本機磁碟大小

下表建議部署 AWS Storage Gateway 中每個的本機磁碟儲存體大小。

閘道類型	快取 (最小值)	快取 (最大值)
FSx File Gateway	150 GiB	64 TiB

### Note

您可以為快取設定一或多個本機磁碟機，最大容量為。  
將快取新增至現有的 FSx 檔案閘道時，請務必在虛擬主機 (Hypervisor 或 Amazon EC2 執行個體) 上建立新的磁碟。如果磁碟先前已配置為快取，請勿變更現有磁碟的大小。

# Storage Gateway 的 API 參考

除了使用主控台之外，您還可以使用 AWS Storage Gateway API 以程式設計方式設定和管理閘道。本節說明 AWS Storage Gateway 操作、身分驗證的請求簽署和錯誤處理。如需 Storage Gateway 可用區域和端點的詳細資訊，請參閱 AWS 一般參考中的 [AWS Storage Gateway 端點與配額](#)。

## Note

使用 Storage Gateway 開發應用程式時，您也可以使用 AWS SDKs。適用於 Java、.NET 和 PHP SDKs AWS 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 必要的請求標頭](#)
- [簽署請求](#)
- [錯誤回應](#)
- [Storage Gateway API 動作](#)

## AWS Storage Gateway 必要的請求標頭

本節說明您必須隨每個 POST 請求傳送至的必要標頭 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
```

以下是您必須在 POST 請求中包含的標頭 AWS Storage Gateway。以下以 "x-amz" AWS 開頭的標頭是特定的標頭。所有其他列出的標頭都是 HTTP 交易中使用的常見標頭。

標頭	Description
Authorization	<p>授權標頭包含有關請求的數個資訊片段，AWS Storage Gateway 允許判斷請求是否為請求者的有效動作。此標頭的格式如下 (為求可讀性已新增分行)：</p> <pre>Authorization: AWS4-HMAC_SHA456 Credentials= <i>YourAccessKey</i> /<i>yyyymmdd</i>/<i>region</i>/storagegateway/aw s4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-targ et, Signature= <i>CalculatedSignature</i></pre> <p>在前述語法中，您指定 <i>YourAccessKey</i>、年、月、日 (<i>yyyymmdd</i>)、<i>region</i>，以及 <i>CalculatedSignature</i>。授權標頭的格式取決於 AWS V4 簽署程序的要求。簽章的詳細資訊會在<a href="#">簽署請求</a>主題中討論。</p>
Content-Type	<p>使用 <code>application/x-amz-json-1.1</code> 作為所有請求的內容類型 AWS Storage Gateway。</p> <pre>Content-Type: application/x-amz-json-1.1</pre>
Host	<p>使用主機標頭來指定您傳送請求的 AWS Storage Gateway 端點。舉例來說，<code>storagegateway.us-east-2.amazonaws.com</code> 代表美國東部 (俄亥俄) 區域的端點。如需 可用端點的詳細資訊 AWS Storage Gateway，請參閱《<a href="#">AWS Storage Gateway</a>》中的<a href="#">端點和配額</a>。AWS 一般參考。</p> <pre>Host: storagegateway. <i>region</i>.amazonaws.com</pre>
x-amz-date	<p>您必須在 HTTP Date 標頭或 AWS <code>x-amz-date</code> 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。) 當 <code>x-amz-date</code> 標頭存在時，會在請求身分驗證期間 AWS Storage Gateway 忽略任</p>

標頭	Description
	<p>何Date標頭。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。</p> <pre>x-amz-date: YYYYMMDD'T'HHMMSS'Z'</pre>
x-amz-target	<p>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。</p> <pre>x-amz-target: StorageGateway_ APIVersion .operationName</pre> <p>operationName 值 (例如："ActivateGateway") 可從 API 清單 (<a href="#">Storage Gateway 的 API 參考</a>) 中找到。</p>

## 簽署請求

Storage Gateway 會要求您簽署請求，對您發送的每個請求進行身分驗證。若要簽署請求，請使用加密雜湊函數來計算數位簽章。加密雜湊是一個函數，其根據輸入傳回一個唯一的雜湊值。此雜湊函數的輸入包含請求和私密存取金鑰的文字。雜湊函數會傳回一個雜湊值，您將此值包含在請求中做為簽章。該簽章是請求 Authorization 標頭中的一部分。

收到請求後，Storage Gateway 會使用您原先用以簽署請求的相同雜湊函數與輸入，重新計算簽章。如果產生的簽章符合請求中的簽章，Storage Gateway 將處理請求。否則，請求會遭到拒絕。

Storage Gateway 支援使用 [AWS Signature 第 4 版](#) 進行身分驗證。計算簽章的程序可以分成三個任務：

- [任務 1：建立正式請求](#)

將 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分驗證碼 (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。

該範例假設如下：

- 請求的時間戳記為 "Mon, 10 Sep 2012 00:00:00" GMT。
- 端點是美國東部 (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，則計算簽章是：

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

最後步驟是建立 Authorization 標頭。對於示範存取金鑰 AKIAIOSFODNN7EXAMPLE，標頭 (為了可讀性而新增了換行) 是：

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120910/us-east-2/
storagegateway/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

## 錯誤回應

### 主題

- [例外狀況](#)
- [操作錯誤代碼](#)
- [錯誤回應](#)

本節提供有關 AWS Storage Gateway 錯誤的參考資訊。這些錯誤會以錯誤異常及操作錯誤代碼表示。例如，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。

## 例外狀況

下表列出 AWS Storage Gateway API 例外狀況。當 AWS Storage Gateway 操作傳回錯誤回應時，回應內文會包含其中一個例外狀況。`InternalServerError` 和 `InvalidGatewayRequestException` 會傳回 [操作錯誤代碼](#) 訊息代碼中的其中一項操作錯誤代碼，提供特定操作錯誤代碼。

異常情形	訊息	HTTP 狀態碼
<code>IncompleteSignatureException</code>	指定的簽章不完整。	400 錯誤的請求
<code>InternalFailure</code>	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
<code>InternalServerError</code>	<a href="#">操作錯誤代碼</a> 的其中一項操作錯誤代碼訊息。	500 內部伺服器錯誤
<code>InvalidAction</code>	無效的請求動作或操作。	400 錯誤的請求
<code>InvalidClientTokenId</code>	提供的 X.509 憑證或 AWS 存取金鑰 ID 不存在於我們的記錄中。	403 禁止
<code>InvalidGatewayRequestException</code>	<a href="#">操作錯誤代碼</a> 中的其中一項操作錯誤代碼訊息。	400 錯誤的請求

異常情形	訊息	HTTP 狀態碼
InvalidSignatureException	我們計算的請求簽章不符合您提供的簽章。檢查您的 AWS 存取金鑰和簽署方法。	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	請求必須包含有效的 (已註冊) AWS 存取金鑰 ID 或 X.509 憑證。	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	AWS 存取金鑰 ID 需要訂閱服務。	400 錯誤的請求
ThrottlingException	超過費率。	400 錯誤的請求
TooManyRequests	請求過多。	429 太多請求
UnknownOperationException	指定的操作不明。有效操作會在 <a href="#">Storage Gateway API 動作</a> 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 操作錯誤代碼與可傳回代碼APIs 之間的映射。所有的操作錯誤代碼都會使用InternalServerError中所說明之兩種一般異常 (InvalidGatewayRequestException 和 [例外狀況](#)) 中的其中一種傳回。

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
ActivationKeyExpired	指定的啟用金鑰已過期。	<a href="#">ActivateGateway</a>
ActivationKeyInvalid	指定的啟用金鑰無效。	<a href="#">ActivateGateway</a>
ActivationKeyNotFound	找不到指定的啟用金鑰。	<a href="#">ActivateGateway</a>
BandwidthThrottleScheduleNotFound	找不到指定的頻寬調節。	<a href="#">DeleteBandwidthRateLimit</a>
CannotExportSnapshot	無法匯出指定的快照。	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a>
InitiatorNotFound	找不到指定的啟動器。	<a href="#">DeleteChapCredentials</a>
DiskAlreadyAllocated	指定的磁碟已配置。	<a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateStorediSCSIVolume</a>
DiskDoesNotExist	指定的磁碟不存在。	<a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateStorediSCSIVolume</a>

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
DiskSizeNotGigAligned	指定的磁碟未調整為 GB。	<a href="#">CreateStorediSCSIVolume</a>
DiskSizeGreaterThanVolumeMaxSize	指定的磁碟大小大於磁碟區大小上限。	<a href="#">CreateStorediSCSIVolume</a>
DiskSizeLessThanVolumeSize	指定的磁碟大小小於磁碟區大小。	<a href="#">CreateStorediSCSIVolume</a>
DuplicateCertificateInfo	指定的憑證資訊重複。	<a href="#">ActivateGateway</a>
FileSystemAssociationEndpointConfigurationConflict	現有的檔案系統關聯端點組態與指定的組態衝突。	<a href="#">AssociateFileSystem</a>
FileSystemAssociationEndpointIpAddressAlreadyInUse	指定的端點 IP 地址已在使用中。	<a href="#">AssociateFileSystem</a>
FileSystemAssociationEndpointIpAddressMissing	檔案系統關聯端點 IP 地址遺失。	<a href="#">AssociateFileSystem</a>
FileSystemAssociationNotFound	找不到指定的檔案系統關聯。	<a href="#">UpdateFileSystemAssociation</a> <a href="#">DisassociateFileSystem</a> <a href="#">DescribeFileSystemAssociations</a>
FileSystemNotFound	找不到指定的檔案系統。	<a href="#">AssociateFileSystem</a>

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
GatewayInternalError	發生閘道內部錯誤。	<a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateSnapshot</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">DeleteBandwidthRateLimit</a> <a href="#">DeleteChapCredentials</a> <a href="#">DeleteVolume</a> <a href="#">DescribeBandwidthRateLimit</a> <a href="#">DescribeCache</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeChapCredentials</a> <a href="#">DescribeGatewayInformation</a> <a href="#">DescribeMaintenanceStartTime</a> <a href="#">DescribeSnapshotSchedule</a> <a href="#">DescribeStorediSCSIVolumes</a> <a href="#">DescribeWorkingStorage</a> <a href="#">ListLocalDisks</a>

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
		<a href="#">ListVolumes</a> <a href="#">ListVolumeRecoveryPoints</a> <a href="#">ShutdownGateway</a> <a href="#">StartGateway</a> <a href="#">UpdateBandwidthRateLimit</a> <a href="#">UpdateChapCredentials</a> <a href="#">UpdateMaintenanceStartTime</a> <a href="#">UpdateGatewaySoftwareNow</a> <a href="#">UpdateSnapshotSchedule</a>

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
GatewayNotConnected	指定的閘道並未連線。	<a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateSnapshot</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">DeleteBandwidthRateLimit</a> <a href="#">DeleteChapCredentials</a> <a href="#">DeleteVolume</a> <a href="#">DescribeBandwidthRateLimit</a> <a href="#">DescribeCache</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeChapCredentials</a> <a href="#">DescribeGatewayInformation</a> <a href="#">DescribeMaintenanceStartTime</a> <a href="#">DescribeSnapshotSchedule</a> <a href="#">DescribeStorediSCSIVolumes</a> <a href="#">DescribeWorkingStorage</a> <a href="#">ListLocalDisks</a>

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
		<a href="#">ListVolumes</a> <a href="#">ListVolumeRecoveryPoints</a> <a href="#">ShutdownGateway</a> <a href="#">StartGateway</a> <a href="#">UpdateBandwidthRateLimit</a> <a href="#">UpdateChapCredentials</a> <a href="#">UpdateMaintenanceStartTime</a> <a href="#">UpdateGatewaySoftwareNow</a> <a href="#">UpdateSnapshotSchedule</a>

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
GatewayNotFound	找不到指定的閘道。	<a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateSnapshot</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteBandwidthRateLimit</a> <a href="#">DeleteChapCredentials</a> <a href="#">DeleteGateway</a> <a href="#">DeleteVolume</a> <a href="#">DescribeBandwidthRateLimit</a> <a href="#">DescribeCache</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeChapCredentials</a> <a href="#">DescribeGatewayInformation</a> <a href="#">DescribeMaintenanceStartTime</a> <a href="#">DescribeSnapshotSchedule</a> <a href="#">DescribeStorediSCSIVolumes</a> <a href="#">DescribeWorkingStorage</a>

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
		<a href="#">ListLocalDisks</a> <a href="#">ListVolumes</a> <a href="#">ListVolumeRecoveryPoints</a> <a href="#">ShutdownGateway</a> <a href="#">StartGateway</a> <a href="#">UpdateBandwidthRateLimit</a> <a href="#">UpdateChapCredentials</a> <a href="#">UpdateMaintenanceStartTime</a> <a href="#">UpdateGatewaySoftwareNow</a> <a href="#">UpdateSnapshotSchedule</a>

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
GatewayProxyNetworkConnectionBusy	指定的閘道代理網路連線忙碌中。	<a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateSnapshot</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteBandwidthRateLimit</a> <a href="#">DeleteChapCredentials</a> <a href="#">DeleteVolume</a> <a href="#">DescribeBandwidthRateLimit</a> <a href="#">DescribeCache</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeChapCredentials</a> <a href="#">DescribeGatewayInformation</a> <a href="#">DescribeMaintenanceStartTime</a> <a href="#">DescribeSnapshotSchedule</a> <a href="#">DescribeStorediSCSIVolumes</a> <a href="#">DescribeWorkingStorage</a> <a href="#">ListLocalDisks</a>

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
		<a href="#">ListVolumes</a> <a href="#">ListVolumeRecoveryPoints</a> <a href="#">ShutdownGateway</a> <a href="#">StartGateway</a> <a href="#">UpdateBandwidthRateLimit</a> <a href="#">UpdateChapCredentials</a> <a href="#">UpdateMaintenanceStartTime</a> <a href="#">UpdateGatewaySoftwareNow</a> <a href="#">UpdateSnapshotSchedule</a>

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
InternalError	發生內部錯誤。	<a href="#">ActivateGateway</a> <a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateSnapshot</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteBandwidthRateLimit</a> <a href="#">DeleteChapCredentials</a> <a href="#">DeleteGateway</a> <a href="#">DeleteVolume</a> <a href="#">DescribeBandwidthRateLimit</a> <a href="#">DescribeCache</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeChapCredentials</a> <a href="#">DescribeGatewayInformation</a> <a href="#">DescribeMaintenanceStartTime</a> <a href="#">DescribeSnapshotSchedule</a> <a href="#">DescribeStorediSCSIVolumes</a>

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
		<a href="#">DescribeWorkingStorage</a> <a href="#">ListLocalDisks</a> <a href="#">ListGateways</a> <a href="#">ListVolumes</a> <a href="#">ListVolumeRecoveryPoints</a> <a href="#">ShutdownGateway</a> <a href="#">StartGateway</a> <a href="#">UpdateBandwidthRateLimit</a> <a href="#">UpdateChapCredentials</a> <a href="#">UpdateMaintenanceStartTime</a> <a href="#">UpdateGatewayInformation</a> <a href="#">UpdateGatewaySoftwareNow</a> <a href="#">UpdateSnapshotSchedule</a>

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
InvalidParameters	指定的請求包含無效的參數。	<a href="#">ActivateGateway</a> <a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateSnapshot</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteBandwidthRateLimit</a> <a href="#">DeleteChapCredentials</a> <a href="#">DeleteGateway</a> <a href="#">DeleteVolume</a> <a href="#">DescribeBandwidthRateLimit</a> <a href="#">DescribeCache</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeChapCredentials</a> <a href="#">DescribeGatewayInformation</a> <a href="#">DescribeMaintenanceStartTime</a> <a href="#">DescribeSnapshotSchedule</a> <a href="#">DescribeStorediSCSIVolumes</a>

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
		<a href="#">DescribeWorkingStorage</a> <a href="#">ListLocalDisks</a> <a href="#">ListGateways</a> <a href="#">ListVolumes</a> <a href="#">ListVolumeRecoveryPoints</a> <a href="#">ShutdownGateway</a> <a href="#">StartGateway</a> <a href="#">UpdateBandwidthRateLimit</a> <a href="#">UpdateChapCredentials</a> <a href="#">UpdateMaintenanceStartTime</a> <a href="#">UpdateGatewayInformation</a> <a href="#">UpdateGatewaySoftwareNow</a> <a href="#">UpdateSnapshotSchedule</a>
LocalStorageLimitExceeded	超過本機儲存限制。	<a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a>
LunInvalid	指定的 LUN 無效。	<a href="#">CreateStorediSCSIVolume</a>
MaximumVolumeCountExceeded	超過磁碟區計數上限。	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeStorediSCSIVolumes</a>

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
NetworkConfigurationChanged	閘道網路組態已變更。	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a>

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
NotSupported	不支援指定的操作。	<a href="#">ActivateGateway</a> <a href="#">AddCache</a> <a href="#">AddUploadBuffer</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateSnapshot</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteBandwidthRateLimit</a> <a href="#">DeleteChapCredentials</a> <a href="#">DeleteGateway</a> <a href="#">DeleteVolume</a> <a href="#">DescribeBandwidthRateLimit</a> <a href="#">DescribeCache</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeChapCredentials</a> <a href="#">DescribeGatewayInformation</a> <a href="#">DescribeMaintenanceStartTime</a> <a href="#">DescribeSnapshotSchedule</a> <a href="#">DescribeStorediSCSIVolumes</a>

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
		<a href="#">DescribeWorkingStorage</a> <a href="#">ListLocalDisks</a> <a href="#">ListGateways</a> <a href="#">ListVolumes</a> <a href="#">ListVolumeRecoveryPoints</a> <a href="#">ShutdownGateway</a> <a href="#">StartGateway</a> <a href="#">UpdateBandwidthRateLimit</a> <a href="#">UpdateChapCredentials</a> <a href="#">UpdateMaintenanceStartTime</a> <a href="#">UpdateGatewayInformation</a> <a href="#">UpdateGatewaySoftwareNow</a> <a href="#">UpdateSnapshotSchedule</a>
OutdatedGateway	指定的閘道已過期。	<a href="#">ActivateGateway</a>
SnapshotInProgressException	指定的快照正在進行。	<a href="#">DeleteVolume</a>
SnapshotIdInvalid	指定的快照無效。	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a>
StagingAreaFull	預備區域已滿。	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a>

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
TargetAlreadyExists	指定的目標已存在。	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a>
TargetInvalid	指定的目標無效。	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteChapCredentials</a> <a href="#">DescribeChapCredentials</a> <a href="#">UpdateChapCredentials</a>
TargetNotFound	找不到指定的目標。	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteChapCredentials</a> <a href="#">DescribeChapCredentials</a> <a href="#">DeleteVolume</a> <a href="#">UpdateChapCredentials</a>

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
UnsupportedOperationForGatewayType	指定的操作對於閘道類型無效。	<a href="#">AddCache</a> <a href="#">AddWorkingStorage</a> <a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">CreateStorediSCSIVolume</a> <a href="#">DeleteSnapshotSchedule</a> <a href="#">DescribeCache</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeStorediSCSIVolumes</a> <a href="#">DescribeUploadBuffer</a> <a href="#">DescribeWorkingStorage</a> <a href="#">ListVolumeRecoveryPoints</a>
VolumeAlreadyExists	指定的磁碟區已存在。	<a href="#">CreateCachediSCSIVolume</a> <a href="#">CreateStorediSCSIVolume</a>
VolumeIdInvalid	指定的磁碟區無效。	<a href="#">DeleteVolume</a>
VolumeInUse	指定的磁碟區已在使用。	<a href="#">DeleteVolume</a>

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
VolumeNotFound	找不到指定的磁碟區。	<a href="#">CreateSnapshot</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a> <a href="#">DeleteVolume</a> <a href="#">DescribeCachediSCSIVolumes</a> <a href="#">DescribeSnapshotSchedule</a> <a href="#">DescribeStorediSCSIVolumes</a> <a href="#">UpdateSnapshotSchedule</a>
VolumeNotReady	指定的磁碟區尚未準備就緒。	<a href="#">CreateSnapshot</a> <a href="#">CreateSnapshotFromVolumeRecoveryPoint</a>

## 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[例外狀況](#)的異常。

類型：字串

#### `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：集合

#### `errorCode`

其中一項操作錯誤代碼。

類型：字串

#### `errorDetails`

目前的 API 版本未使用此欄位。

類型：字串

#### `message`

的其中一項操作錯誤代碼訊息。

類型：字串

## 錯誤回應範例

如果您使用 `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"
  }
}
```

```
}
```

若 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 API 動作

如需 Storage Gateway 操作的清單，請參閱 AWS Storage Gateway API 參考中的[動作](#)。

# Amazon FSx File Gateway 使用者指南的文件歷史記錄

下表說明 2018 年 4 月之後本使用者指南每個版本的重要變更。如需有關此文件更新的通知，您可以訂閱 RSS 訂閱源。

變更	描述	日期
<a href="#">FSx File Gateway 可用性變更通知</a>	Amazon FSx File Gateway 不再提供給新客戶。FSx File Gateway 的現有客戶可以繼續正常使用服務。如需類似 FSx File Gateway 的功能，請造訪 <a href="#">此部落格文章</a> 。	2024 年 10 月 28 日
<a href="#">FSx File Gateway 可用性變更通知</a>	AWS Storage Gateway 從 10/28/24 開始，新客戶將無法再使用的 FSx 檔案閘道。若要使用服務，您必須在該日期之前註冊。FSx File Gateway 的現有客戶可以繼續正常使用服務。如需類似 FSx File Gateway 的功能，請造訪 <a href="#">此部落格文章</a> 。	2024 年 9 月 26 日
<a href="#">新增開啟或關閉維護更新的選項</a>	Storage Gateway 會收到定期維護更新，其中包括作業系統和軟體升級、解決穩定性、效能和安全性的修正，以及新功能的存取。您現在可以設定設定，為部署中的每個個別閘道開啟或關閉這些更新。如需詳細資訊，請參閱 <a href="#">使用 AWS Storage Gateway 主控台管理閘道更新</a> 。	2024 年 6 月 6 日
<a href="#">更新建議 CloudWatch 警示</a>	CloudWatch HealthNotifications 警示現在適	2023 年 10 月 2 日

用於所有閘道類型和主機平台，並建議您使用此警示。建議的組態設定也已針對 HealthNotifications 和 AvailabilityNotifications 更新。如需詳細資訊，請參閱[了解 CloudWatch 警示](#)。

### [新增 GatewayClockOutOfSync 疑難排解秘訣](#)

故障診斷：檔案閘道問題區段現在包含故障診斷準則，以協助診斷閘道系統時鐘未與 AWS Storage Gateway 伺服器時間同步時可能遇到的問題。如需詳細資訊，請參閱[錯誤：GatewayClockOutOfSync](#)。

2022 年 10 月 19 日

### [新增 Active Directory 加入網域疑難排解秘訣](#)

故障診斷：檔案閘道問題區段現在包含故障診斷準則，以協助診斷您在嘗試將閘道加入 Active Directory 網域時可能遇到的問題。如需詳細資訊，請參閱[故障診斷：Active Directory 網域問題](#)。

2022 年 10 月 19 日

### [更新的閘道建立程序](#)

建立新閘道的程序已更新，以反映 Storage Gateway 主控台中的變更。如需詳細資訊，請參閱[建立和啟用 Amazon S3 檔案閘道](#)。

2021 年 10 月 12 日

### [多個檔案系統支援](#)

Amazon FSx File Gateway 現在支援最多五個連接的 Amazon FSx 檔案系統。如需詳細資訊，請參閱[連接 Amazon FSx for Windows File Server 檔案系統](#)。

2021 年 7 月 7 日

## [Amazon FSx 軟儲存配額支援](#)

Amazon FSx File Gateway 現在支援軟儲存配額（當使用者超過其資料限制時提醒您），當寫入已設定儲存配額的連接 Amazon FSx 檔案系統時。不支援硬性配額（透過拒絕寫入存取強制執行資料限制）。除 Amazon FSx 管理員使用者外，軟配額適用於所有使用者。如需設定儲存配額的詳細資訊，請參閱《Amazon FSx for Windows File Server 使用者指南》中的[儲存配額](#)。

2021 年 7 月 7 日

## [新的指南](#)

除了原始檔案閘道（現在稱為 Amazon S3 檔案閘道）之外，Storage Gateway 還提供 Amazon FSx 檔案閘道 (FSx 檔案閘道)。FSx File Gateway 提供從內部部署設施存取雲端 FSx for Windows File Server 檔案共享的低延遲和高效率。如需詳細資訊，請參閱[什麼是 Amazon FSx 檔案閘道？](#)

2021 年 4 月 27 日

## [FedRAMP 合規](#)

Storage Gateway 現在符合 FedRAMP 標準。如需詳細資訊，請參閱 [Storage Gateway 的合規驗證](#)。

2020 年 11 月 24 日

## [檔案閘道遷移](#)

File Gateway 現在提供以新檔案閘道取代現有檔案閘道的記錄程序。如需詳細資訊，請參閱[將檔案閘道取代為新的檔案閘道](#)。

2020 年 10 月 30 日

### [檔案閘道冷快取讀取效能提高 4 倍](#)

Storage Gateway 已將冷快取讀取效能提高 4 倍。如需詳細資訊，請參閱[檔案閘道的效能指引](#)。

2020 年 8 月 31 日

### [透過主控台訂購硬體設備](#)

您現在可以透過 AWS Storage Gateway 主控台訂購硬體設備。如需詳細資訊，請參閱[使用 AWS Storage Gateway 硬體設備](#)。

2020 年 8 月 12 日

### [支援新 AWS 區域中的聯邦資訊處理標準 \(FIPS\) 端點](#)

您現在可在美國東部 (俄亥俄)、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 (奧勒岡)、以及加拿大 (中部) 地區啟用具有 FIPS 端點的閘道。如需詳細資訊，請參閱 AWS 一般參考中的 [AWS Storage Gateway 端點和配額](#)。

2020 年 7 月 31 日

### [檔案閘道本機快取儲存增加 4 倍](#)

Storage Gateway 現在支援檔案閘道高達 64 TB 的本機快取，藉由提供對大型工作資料集的低延遲存取，提升內部部署應用程式的效能。如需詳細資訊，請參閱《Storage Gateway 使用者指南》中的[閘道的建議本機磁碟大小](#)。

2020 年 7 月 7 日

### [在 Storage Gateway 主控台中檢視 Amazon CloudWatch 警示](#)

您現在可在 Storage Gateway 主控台中檢視 CloudWatch 警示。如需詳細資訊，請參閱[了解 CloudWatch 警示](#)。

2020 年 5 月 29 日

<a href="#">支援聯邦資訊處理標準 (FIPS) 端點</a>	您現在可以在 AWS GovCloud (US) 區域中啟用具有 FIPS 端點的閘道。若要選擇檔案閘道的 FIPS 端點，請參閱 <a href="#">選擇服務端點</a> 。	2020 年 5 月 22 日
<a href="#">新 AWS 區域</a>	Storage Gateway 現已在非洲 (開普敦) 和歐洲 (米蘭) 區域提供。如需詳細資訊，請參閱 AWS 一般參考中的 <a href="#">AWS Storage Gateway 端點和配額</a> 。	2020 年 5 月 7 日
<a href="#">S3 Intelligent-Tiering 儲存體方案的支援</a>	Storage Gateway 現支援 S3 Intelligent-Tiering 儲存體方案。S3 Intelligent-Tiering 儲存體方案旨在透過自動將資料移動到最具成本效益的儲存體存取層，將儲存成本最佳化，且不會影響效能或帶來額外負荷。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的 <a href="#">自動最佳化經常存取物件與不常存取物件的儲存體方案</a> 。	2020 年 4 月 30 日
<a href="#">新 AWS 區域</a>	Storage Gateway 現已在 AWS GovCloud (美國東部) 區域提供。如需詳細資訊，請參閱 AWS 一般參考中的 <a href="#">AWS Storage Gateway 端點和配額</a> 。	2020 年 3 月 12 日

### [支援 Linux 核心基礎虛擬機器 \(KVM\) Hypervisor](#)

Storage Gateway 現在能夠讓您在 KVM 虛擬化平台上部署內部部署閘道。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《Storage Gateway 使用者指南》中的[支援的 Hypervisor 和主機需求](#)。

2020 年 2 月 4 日

### [支援 VMware vSphere 高可用性](#)

Storage Gateway 現可在 VMware 上提供高可用性支援，協助防範儲存工作負載出現硬體、Hypervisor 或網路故障。如需詳細資訊，請參閱《Storage Gateway 使用者指南》中的[將 VMware vSphere 高可用性與 Storage Gateway 搭配](#)。此版本也包含了效能改善。如需詳細資訊，請參閱《Storage Gateway 使用者指南》中的[效能](#)。

2019 年 11 月 20 日

### [新增對 Amazon CloudWatch Logs 的支援](#)

您現在可以使用 Amazon CloudWatch 日誌群組設定檔案閘道，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《Storage Gateway 使用者指南》中的[接收有關 Amazon CloudWatch 日誌群組的閘道運作狀態和錯誤的通知](#)。

2019 年 9 月 4 日

### [New \(新增\) AWS 區域](#)

Storage Gateway 現已在亞太區域 (香港) 提供。如需詳細資訊，請參閱 AWS 一般參考中的[AWS Storage Gateway 端點和配額](#)。

2019 年 8 月 14 日

## [New \(新增\) AWS 區域](#)

Storage Gateway 現已在中東 (巴林) 區域提供。如需詳細資訊，請參閱 AWS 一般參考 中的 [AWS Storage Gateway 端點和配額](#)。

2019 年 7 月 29 日

## [支援在虛擬私有雲端 \(VPC\) 中啟用閘道](#)

您現在可以在 VPC 中啟用閘道。您可以在內部部署軟體裝置以及雲端儲存基礎設施之間建立私有連線。如需詳細資訊，請參閱 [在 VPC 中啟用閘道](#)。

2019 年 6 月 20 日

## [檔案閘道支援標籤型授權](#)

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上的標籤來控制對 File Gateway 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

## [歐洲儲存 AWS Storage Gateway 硬體設備的可用性](#)

The AWS Storage Gateway 硬體設備現已在歐洲提供。如需詳細資訊，請參閱 AWS 一般參考 中的 [AWS Storage Gateway 硬體設備區域](#)。此外，您現在可以將 AWS Storage Gateway 硬體設備上的可用儲存體從 5 TB 增加到 12 TB，並以 10 GB 光纖網路卡取代已安裝的銅網路卡。如需詳細資訊，請參閱 [設定您的硬體設備](#)。

2019 年 2 月 25 日

## [支援 AWS Storage Gateway 硬體設備](#)

The AWS Storage Gateway 硬體設備包含第三方伺服器上預先安裝的 Storage Gateway 軟體。您可以從 AWS 管理主控台管理裝置。設備可以託管檔案、磁帶和磁碟區。如需詳細資訊，請參閱[使用 Storage Gateway 硬體設備](#)。

2018 年 9 月 18 日

## 舊版更新

下表說明 2018 年 5 月前每個《AWS Storage Gateway 使用者指南》版本的重要變更。

變更	描述	變更日期
新的 AWS 區域	磁帶閘道現已在亞太區域 (新加坡) 提供。如需詳細資訊，請參閱 <a href="#">AWS 區域 支援 Storage Gateway</a> 。	2018 年 4 月 3 日
新的 AWS 區域	Storage Gateway 現已在歐洲 (巴黎) 區域提供。如需詳細資訊，請參閱 <a href="#">AWS 區域 支援 Storage Gateway</a> 。	2017 年 12 月 18 日
支援 VMware ESXi 虛擬化管理程序 6.5 版	AWS Storage Gateway 現在支援 VMware ESXi Hypervisor 6.5 版。這是 4.1、5.0、5.1、5.5 和 6.0 版以外的支援。如需詳細資訊，請參閱 <a href="#">支援的 Hypervisor 與主機需求</a> 。	2017 年 9 月 13 日
檔案閘道支援 Microsoft Hyper-V Hypervisor	您現在可以將檔案閘道部署在 Microsoft Hyper-V Hypervisor。如需相關資訊，請參閱 <a href="#">支援的 Hypervisor 與主機需求</a> 。	2017 年 6 月 22 日
新的 AWS 區域	Storage Gateway 現已在亞太區域 (孟買) 提供。如需詳細資訊，請參閱 <a href="#">AWS 區域 支援 Storage Gateway</a> 。	2017 年 5 月 02 日
支援 Amazon EC2 的檔案閘道	AWS Storage Gateway 現在提供在 Amazon EC2 中部署檔案閘道的功能。您可以使用現可當成社群 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	2017 年 2 月 08 日

變更	描述	變更日期
	<p>立檔案閘道並將其部署到 EC2 執行個體的詳細資訊，請參閱 <a href="#">建立並啟動 Amazon FSx File Gateway</a>。如需如何啟動檔案閘道 AMI 的詳細資訊，請參閱 <a href="#">部署 FSx 檔案閘道的預設 Amazon EC2 主機</a>。</p> <p>此外，檔案閘道現在支援 HTTP 代理組態。如需詳細資訊，請參閱 <a href="#">透過 HTTP 代理路由部署在 Amazon EC2 上的閘道</a>。</p>	
新的 AWS 區域	Storage Gateway 現已在歐洲（倫敦）區域提供。如需詳細資訊，請參閱 <a href="#">AWS 區域 支援 Storage Gateway</a> 。	2016 年 12 月 13 日
新的 AWS 區域	Storage Gateway 現已在加拿大（中部）區域提供。如需詳細資訊，請參閱 <a href="#">AWS 區域 支援 Storage Gateway</a> 。	2016 年 12 月 08 日
支援檔案閘道	除了磁碟區閘道和磁帶閘道之外，Storage Gateway 道現在還提供檔案閘道。檔案閘道結合了服務和虛擬軟體裝置，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 中存放和擷取物件。閘道可讓您存取 Amazon S3 中的物件，就像存取 NFS 掛載點的檔案。	2016 年 11 月 29 日