《磁碟區閘道使用者指南》

AWS Storage Gateway

API 版本 2013-06-30

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

AWS Storage Gateway: 《磁碟區閘道使用者指南》

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

什麼是磁碟區閘道？ 1
磁碟區閘道的運作方式 2
磁碟區閘道 2
入門 AWS Storage Gateway 6
註冊 AWS 帳戶 6
存取 AWS Storage Gateway 6
AWS 區域 支援 Storage Gateway 7
磁碟區閘道設定需求 8
硬體及儲存體需求 8
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 10
連接埠需求 11
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 25
支援的 Hypervisor 與主機需求 26
支援的 iSCSI 啟動器 27
使用硬體設備 28
設定您的硬體設備 29
實際安裝您的硬體設備 30
存取硬體設備主控台 32
設定硬體設備網路參數 33
啟動您的硬體設備 34
在硬體設備上建立閘道 35
在硬體設備上設定閘道 IP 地址 36
從硬體設備移除閘道軟體 38
刪除您的硬體設備 39
建立閘道 40
概觀：閘道啟動 40
設定閘道 40
連線至 AWS 40
檢閱並啟用 41

概觀：閘道組態 41
概觀：儲存資源 41
建立磁碟區端點 41
設定磁碟區閘道 41
將您的磁碟區閘道連線至 AWS 43
檢閱設定並啟用磁碟區閘道 44
設定磁碟區閘道 44
建立磁碟區 46
設定磁碟區的 CHAP 身分驗證 48
將磁碟區連接到用戶端 49
連線至 Microsoft Windows 用戶端 49
連線至 Red Hat Enterprise Linux 用戶端 50
初始化和格式化您的磁碟區 51
在 Windows 上初始化和格式化 51
在 RHEL 上初始化和格式化 53
測試您的閘道 54
備份您的磁碟區 55
使用 Storage Gateway 備份磁碟區 55
使用 AWS Backup 來備份您的磁碟區 55
接下來做些什麼？ 58
針對實際工作負載調整您磁碟區閘道的儲存體大小 58
在 VPC 中啟用閘道 59
建立針對 Storage Gateway 的 VPC 端點 60
管理磁碟區閘道 62
編輯閘道資訊 63
新增和擴展磁碟區 64
複製磁碟區 64
檢視磁碟區用量 66
刪除儲存磁碟區 66
將您的磁碟區移至不同的閘道 67
建立復原快照 69
編輯快照排程 69
刪除快照 70
使用適用於 Java 的 AWS 開發套件 70
使用適用於 .NET 的 AWS 開發套件 74
使用 AWS Tools for Windows PowerShell 80

了解磁碟區狀態和轉換 82
了解磁碟區狀態 83
了解磁碟區狀態 87
了解快取磁碟區狀態轉換 87
了解存放磁碟區狀態轉換 89
將資料移至新的閘道執行個體 92
將儲存的磁碟區移至新的儲存磁碟區閘道 92
將快取磁碟區移至新的閘道虛擬機器 94
監控 Storage Gateway 98
了解閘道指標 98
Storage Gateway 指標的維度 103
監控上傳緩衝區 103
監控快取儲存 105
了解 CloudWatch 警示 107
建立建議的 CloudWatch 警示 108
建立自訂 CloudWatch 警示 109
監控您的磁碟區閘道 110
取得磁碟區閘道運作狀態日誌 111
使用 Amazon CloudWatch 指標 112
測量您應用程式和閘道之間的效能 113
測量閘道與 之間的效能 AWS 115
了解磁碟區指標 118
維護您的閘道 123
管理本機磁碟 123
決定本機磁碟儲存體的數量 123
新增上傳緩衝或快取儲存體 126
管理頻寬 127
使用 Storage Gateway 主控台變更頻寬限流 128
排程頻寬限流 128
使用 適用於 Java 的 AWS SDK 129
使用 適用於 .NET 的 AWS SDK 131
使用 AWS Tools for Windows PowerShell 133
管理閘道更新 134
更新頻率和預期行為 135
開啟或關閉維護更新 135
修改閘道維護時段排程 136

手動套用更新 137
關閉閘道 VM 138
啟動和停止磁碟區閘道 138
刪除您的閘道並移除資源 139
使用 Storage Gateway 主控台刪除閘道 139
從內部部署的閘道移除資源 140
從 Amazon EC2 執行個體上所部署的閘道移除資源 141
使用本機主控台執行維護任務 142
存取閘道本機主控台 142
使用 Linux KVM 存取閘道本機主控台 142
使用 VMware ESXi 存取閘道本機主控台 143
使用 Microsoft Hyper-V 存取閘道本機主控台 144
在 VM 本機主控台上執行任務 145
登入磁碟區閘道本機主控台 145
為您的內部部署閘道設定 SOCKS5 代理 146
設定您的閘道網路 147
測試閘道與網際網路的連線 151
在本機主控台中為內部部署閘道執行儲存閘道命令 152
檢視閘道系統資源狀態 154
在 EC2 本機主控台上執行任務 155
登入至您的 EC2 閘道本機主控台 156
設定 HTTP 代理 156
測試閘道網路連線 157
檢視閘道系統資源狀態 157
在本機主控台上執行 Storage Gateway 命令 158
磁碟區閘道的效能和最佳化 161
最佳化閘道效能 161
建議組態 161
新增資源至您的閘道 161
最佳化 iSCSI 設定 164
新增資源到您的應用程式環境 164
安全 166
資料保護 166
資料加密 167
設定 CHAP 身分驗證 169
身分和存取權管理 170

目標對象 170
使用身分驗證 171
使用政策管理存取權 172
How AWS Storage Gateway 可與 IAM 搭配使用 173
身分型政策範例 177
疑難排解 180
法規遵循驗證 181
恢復能力 182
基礎設施安全性 183
AWS 安全最佳實務 183
記錄和監控 183
CloudTrail 中的 Storage Gateway 資訊 184
了解 Storage Gateway 日誌檔案項目 185
疑難排解閘道問題 187
故障診斷：閘道離線問題 187
檢查相關聯的防火牆或代理 188
檢查閘道流量的持續 SSL 或深度封包檢查 188
檢查 Hypervisor 主機上是否有電源中斷或硬體故障 188
檢查相關聯的快取磁碟是否有問題 188
故障診斷：閘道啟用問題 189
解決使用公有端點啟用閘道時的錯誤 189
解決使用 Amazon VPC 端點啟用閘道時的錯誤 192
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 195
對內部部署閘道問題進行疑難排解 196
啟用 支援 以協助疑難排解您的閘道 199
為 Microsoft Hyper-V 設定問題進行疑難排解 200
為 Amazon EC2 閘道問題進行疑難排解 202
閘道在一段時間後仍未啟用 203
執行個體清單中找不到 EC2 閘道執行個體 203
無法將 Amazon EBS 磁碟區連接到 EC2 閘道執行個體 204
您無法將啟動器連接到您 EC2 閘道的磁碟區目標 204
當您嘗試新增儲存磁碟區訊息時，無磁碟可用 204
如何移除配置為上傳緩衝空間的磁碟，以減少上傳緩衝空間 204
您的 EC2 閘道出入輸送量降到零 204
啟用 支援 以協助對閘道進行故障診斷 204
使用序列主控台連接到您的 Amazon EC2 閘道 206

為硬體設備問題進行疑難排解 206
如何確定服務 IP 地址 206
如何執行重設成出廠預設值？ 206
如何執行遠端重新啟動 207
如何取得 Dell iDRAC 支援 207
如何找到硬體設備序號 207
如何取得硬體設備支援 207
對磁碟區問題進行疑難排解 208
主控台指出您的磁碟區尚未設定 208
主控台指出您的磁碟區無法還原 208
您的快取閘道無法連接，而您想要復原資料 209
主控台指出您的磁碟區狀態為 PASS THROUGH (傳遞) 209
您想要驗證磁碟區完整性並修復可能的錯誤 210
您磁碟區的 iSCSI 目標未出現在 Windows 磁碟管理主控台 210
您想要變更您磁碟區的 iSCSI 目標名稱 210
您的排程磁碟區快照未出現 210
您需要移除或取代故障的磁碟 210
從您應用程式到磁碟區的輸送量降到零 211
您閘道的快取磁碟發生故障 211
磁碟區快照的 PENDING (擱置) 狀態比預期久 212
高可用性運作狀態通知 212
對高可用性問題進行疑難排解 212
運作狀態通知 212
指標 214
最佳實務 215
最佳實務：復原您的資料 215
從非預期的 VM 關機復原 216
從故障的閘道或 VM 復原資料 216
從無法復原的磁碟區復原資料 216
從故障的快取磁碟復原資料 217
從損毀的檔案系統復原資料 217
從無法存取的資料中心復原資料 218
清除不必要的資源 219
減少磁碟區上的計費儲存量 219
其他資源 220
主機設定 220

部署磁碟區閘道的預設 Amazon EC2 主機 221
部署磁碟區閘道的自訂 Amazon EC2 執行個體 223
修改 Amazon EC2 執行個體中繼資料選項 226
同步 VM 時間與 Hyper-V 或 Linux KVM 主機時間 227
同步 VM 時間與 VMware 主機時間 227
設定半虛擬化磁碟控制器 229
為您的閘道設定網路轉接器 229
搭配使用 VMware 高可用性與 Storage Gateway 232
使用磁碟區閘道儲存資源 236
從閘道移除磁碟 236
EC2 閘道的 EBS 磁碟區 238
取得啟用金鑰 239
Linux (curl) 240
Linux (bash/zsh) 241
Microsoft Windows PowerShell 242
使用本機主控台 243
連線 iSCSI 啟動器 244
從 Windows 用戶端連線至您的磁碟區 245
將 volumes連接到 Linux 用戶端 248
自訂 iSCSI 設定 249
設定 CHAP 身分驗證 255
Direct Connect 搭配 Storage Gateway 使用 259
取得閘道 IP 地址 260
從 Amazon EC2 主機取得 IP 地址 261
IPv6 支援 262
了解資源和資源 ID 262
使用資源 ID 262
為您的資源建立標籤 263
處理標籤 263
開放原始碼元件 265
配額 265
磁碟區的配額 265
適用於您閘道的建議本機磁碟大小 266
API 參考 267
必要請求標頭 267
簽署請求 269

簽章計算範例 270
錯誤回應 271
例外狀況 272
操作錯誤代碼 274
錯誤回應 293
操作 295
文件歷史紀錄 296
舊版更新 307
AL2 到 AL2023 遷移 321
快速連結和資源 321
閘道版本遷移參考 321
遷移時間軸 322
遷移前檢查清單 322
遷移指南 322
支援和監控 323
常見問答集 323
版本備註 324
..... cccxxxii

什麼是磁碟區閘道？

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

您可以將 Storage Gateway 部署為現場部署為在 VMware ESXi、KVM 或 Microsoft Hyper-V Hypervisor 上執行的 VM 設備、部署為硬體設備，或在 中 AWS 部署為 Amazon EC2 執行個體。您可以將 EC2 執行個體上所託管的閘道用於災難復原、資料鏡像，以及提供 Amazon EC2 上所託管應用程式的儲存。

若要查看 AWS Storage Gateway 各種有助於實現目標的使用案例，請參閱 AWS Storage Gateway。如需目前定價資訊，請參閱 詳細資訊頁面上的定價 AWS Storage Gateway 。

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

本使用者指南提供磁碟區閘道的相關資訊。

磁碟區閘道提供雲端支援的儲存磁碟區，您可以從內部部署應用程式伺服器以網際網路小型電腦系統界面 (iSCSI) 裝置的形式掛載。

磁碟區閘道支援下列磁碟區組態：

- 快取磁碟區：您將資料存放至 Amazon Simple Storage Service (Amazon S3)，並將經常存取的資料子集複本保留在本機。快取磁碟區可大幅節省主要儲存上的成本，並以內部部署方式將擴展儲存的需求降到最低。您也可以保留對經常存取資料的低延遲存取。
- 存放磁碟區：如果您需要整個資料集的低延遲存取，則請先將內部部署閘道設定為在本機存放所有資料。然後，將此資料的時間點快照非同步備份至 Amazon S3。此組態提供耐久又便宜的離站備份，而您可以將離站備份復原到本機資料中心或 Amazon Elastic Compute Cloud (Amazon EC2)。例如，如果您因災難復原而需要替代容量，則可以將備份復原到 Amazon EC2。

如需架構概觀，請參閱 磁碟區閘道的運作方式。

在本使用者指南中，您可以找到涵蓋所有閘道類型常見設定資訊的入門章節。您也可以找到磁碟區閘道設定需求，以及描述如何部署、啟用、設定和管理磁碟區閘道的章節。

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

磁碟區閘道的運作方式

接下來，您可以尋找磁碟區閘道解決方案的架構概觀。

磁碟區閘道

針對磁碟區閘道，您可以使用快取磁碟區或存放磁碟區。

主題

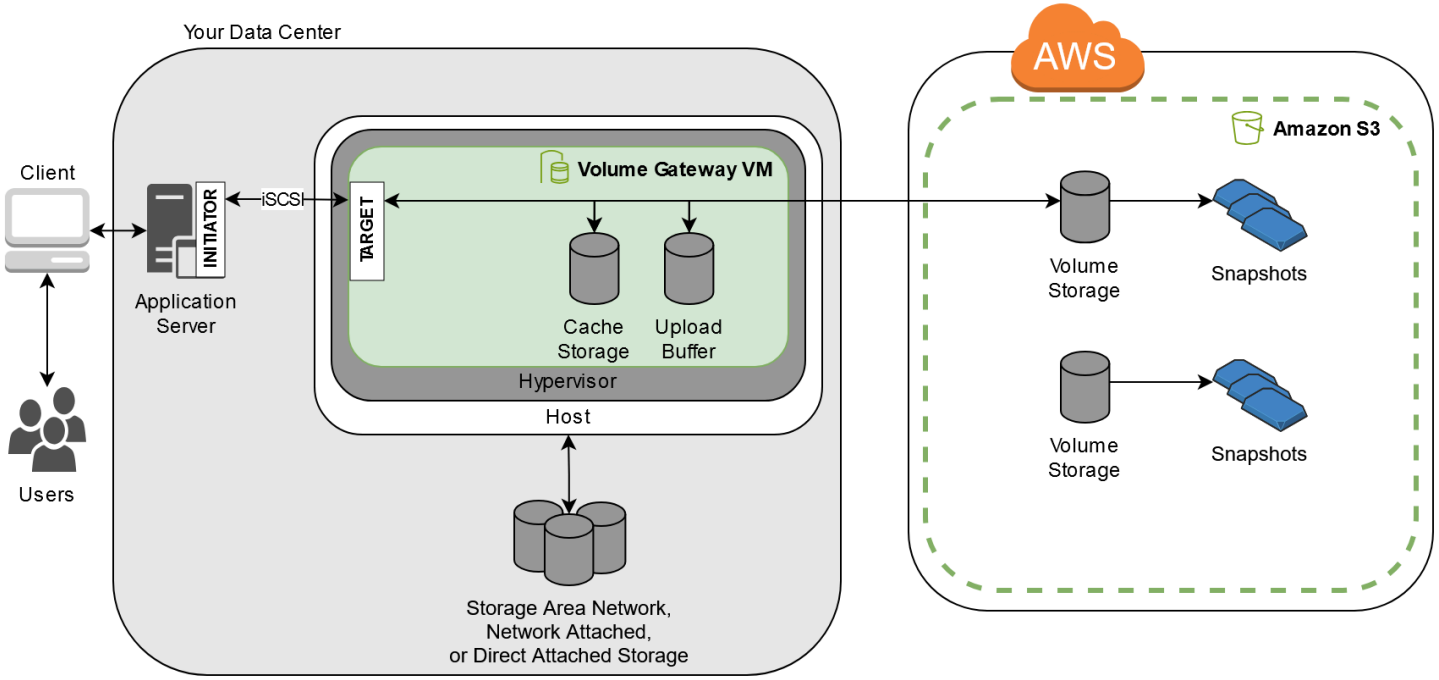
- 快取磁碟區架構
- 存放磁碟區架構

快取磁碟區架構

透過使用快取磁碟區，您可以使用 Amazon S3 做為您的主要資料儲存體，同時將經常存取的資料保留在 Storage Gateway 本機。快取磁碟區可將擴展內部部署儲存基礎設施的需求減到最低，同時讓應用程式以低延遲方式存取其經常存取的資料。您可以建立最高 32 TiB 的儲存磁碟區，並透過內部部署應用程式伺服器，將這些磁碟區連接至 iSCSI 裝置。您的閘道會將寫入至這些磁碟區的資料存放至 Amazon S3，並將最近讀取的資料保留在內部部署 Storage Gateway 快取中，並上傳緩衝區儲存。

快取磁碟區大小範圍可以從 1 GiB 到 32 TiB，而且必須四捨五入到最接近的 GiB。針對快取磁碟區所設定的每個閘道最多可以支援 32 個磁碟區，其總最大儲存磁碟區為 1,024 TiB (1 PiB)。

在快取磁碟區解決方案中，Storage Gateway 會將所有內部部署應用程式資料存放至 Amazon S3 中的儲存磁碟區。下圖概述快取磁碟區部署。



在資料中心的主機上安裝 Storage Gateway 軟體設備 - VM 並啟用後，您可以使用 AWS 管理主控台佈建 Amazon S3 支援的儲存磁碟區。您也可以使用 Storage Gateway API 或 AWS SDK 程式庫，以程式設計方式佈建儲存磁碟區。您接著會將這些儲存磁碟區掛載至內部部署應用程式伺服器做為 iSCSI 裝置。

您也可以在內部部署配置 VM 的磁碟。這些內部部署磁碟提供下列目的：

- 閘道用作快取儲存體的磁碟 – 當應用程式將資料寫入儲存磁碟區時 AWS，閘道會先將資料存放在用於快取儲存體的內部部署磁碟上。接著，閘道會將資料上傳至 Amazon S3。快取儲存做為內部部署耐久存放區來存放等待從上傳緩衝區上傳至 Amazon S3 的資料。

  快取儲存也可讓閘道存放應用程式近期存取的內部部署資料，以維持低延遲存取。如果您的應用程式請求資料，則閘道會先檢查資料的快取儲存，再檢查 Amazon S3。

  您可以使用下列準則，以判斷要配置做為快取儲存的磁碟空間量。一般而言，您應該配置至少 20% 的現有檔案存放區大小做為快取儲存。快取儲存也應該大於上傳緩衝區。此準則可協助確保快取儲存的大小足夠將所有資料保留在尚未上傳至 Amazon S3 的上傳緩衝區中。
- 閘道用來做為上傳緩衝區的磁碟：若要準備上傳至 Amazon S3，您的閘道也會將傳入資料存放至暫存區域 (稱為上傳緩衝區)。您的閘道會透過加密 Secure Sockets Layer (SSL) 連線上傳此緩衝區資料至 AWS，該連線會加密存放在 Amazon S3 中。

您可以建立儲存磁碟區的增量備份 (稱為快照)。這些時間點快照也會存放至 Amazon S3，以做為 Amazon EBS 快照。當您建立新的快照時，只會存放自最後一個快照以來所變更的資料。拍攝快照時，閘道會將變更上傳到快照點，然後使用 Amazon EBS 建立新快照。您可以依排程或一次性地初始化快照。單一磁碟區支援快速連續將多個快照排入佇列，但每個快照都必須先完成建立，才能擷取下一個快照。當您刪除快照時，只會移除任何其他快照不需要的資料。如需關於 Amazon EBS 快照的資訊，請參閱 Amazon EBS 快照。

如果您需要復原資料備份，則可以將 Amazon EBS 快照還原至閘道儲存磁碟區。或者，針對大小高達 16 TiB 的快照，您可以使用快照做為新 Amazon EBS 磁碟區的起點。您接著可以將這個新的 Amazon EBS 磁碟區連接至 Amazon EC2 執行個體。

快取磁碟區的所有閘道資料和快照資料都會存放至 Amazon S3，並使用伺服器端加密 (SSE) 靜態加密。不過，您無法使用 Amazon S3 API 或其他工具 (例如 Amazon S3 管理主控台) 來存取此資料。

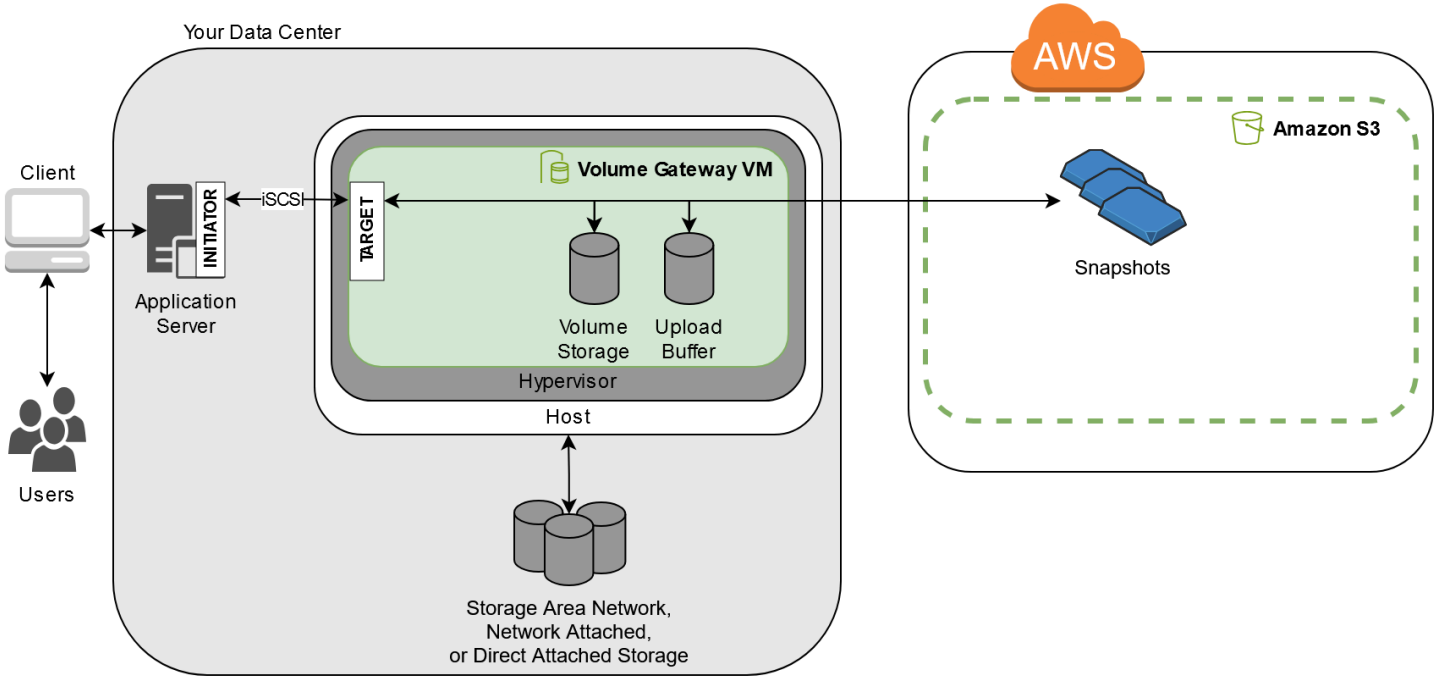
存放磁碟區架構

透過使用儲存的磁碟區，您可以在本機存放主要資料，同時非同步備份該資料 AWS。存放磁碟區可讓內部部署應用程式低延遲存取其整個資料集。它們同時也提供耐久的離站備份。您可以建立儲存磁碟區，並透過內部部署應用程式伺服器，將這些磁碟區掛載為 iSCSI 裝置。寫入至存放磁碟區的資料存放至內部部署儲存硬體。以 Amazon Elastic Block Store (Amazon EBS) 快照的形式將該資料非同步備份至 Amazon S3。

存放磁碟區大小範圍可以從 1 GiB 到 16 TiB，而且必須四捨五入到最接近的 GiB。針對存放磁碟區所設定的每個閘道最多可以支援 32 個磁碟區，且總磁碟區儲存為 512 TiB (0.5 PiB)。

使用存放磁碟區，您可以在資料中心內以內部部署維護磁碟區儲存。也就是說，您將所有應用程式資料存放至內部部署儲存硬體。然後，使用各種功能協助保持資料安全，閘道會將資料上傳至 Amazon Web Services 雲端，以取得具有經濟效益的備份和快速災難復原。如果您想要以內部部署方式將資料保留在本機，則此解決方案十分理解，因為您需要低延遲存取所有資料，也需要在 AWS中維護備份。

下圖概述存放磁碟區部署。



在您於資料中心的主機上安裝並啟用 Storage Gateway 軟體裝置 (VM) 之後，可以建立閘道儲存磁碟區。您接著可以將它們映射至內部部署直接連接儲存裝置 (DAS) 或儲存區域網路 (SAN) 磁碟。您可以開始使用新磁碟或已保留資料的磁碟。您接著可以將這些儲存磁碟區掛載至內部部署應用程式伺服器做為 iSCSI 裝置。內部部署應用程式在閘道儲存磁碟區中寫入和讀取資料時，這項資料是存放並擷取自磁碟區的已指派磁碟。

若要準備要上傳至 Amazon S3 的資料，閘道也會將傳入資料存放至暫存區域，稱為上傳緩衝區。您可以使用內部部署 DAS 或 SAN 磁碟來處理儲存。您的閘道透過加密 Secure Sockets Layer (SSL) 連線，將資料從上傳緩衝區上傳至在 Amazon Web Services 雲端中執行的 Storage Gateway 服務。此服務接著會存放 Amazon S3 中所加密的資料。

您可以建立儲存磁碟區的增量備份 (稱為快照)。閘道會將這些快照存放至 Amazon S3，做為 Amazon EBS 快照。當您建立新的快照時，只會存放自最後一個快照以來所變更的資料。拍攝快照時，閘道會將變更上傳到快照點，然後使用 Amazon EBS 建立新快照。您可以依排程或一次性地初始化快照。單一磁碟區支援快速連續將多個快照排入佇列，但每個快照都必須先完成建立，才能擷取下一個快照。刪除快照時，只會移除其他快照都不需要的資料。

如果您需要復原資料備份，則可以將 Amazon EBS 快照還原至內部部署閘道儲存磁碟區。您也可以使用快照做為新 Amazon EBS 磁碟區的起點，之後可以這個新磁碟區連接至 Amazon EC2 執行個體。

入門 AWS Storage Gateway

本節提供開始使用 的說明 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 帳戶中屬於具有執行 Storage Gateway 任務所需管理許可之群組的 IAM 使用者。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 區域和磁碟區閘道設定需求區段，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 AWS 帳戶 - 了解如何註冊 AWS 和建立 AWS 帳戶。
- 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 SDKs存取 AWS 。
- 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 AWS 帳戶

若要開始使用 AWS，您需要 AWS 帳戶。如需建立 的相關資訊 AWS 帳戶，請參閱《 AWS 帳戶管理參考指南》中的 入門 AWS 帳戶。

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、建立、管理和刪除，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 Web 瀏覽器存取 Storage Gateway 主控台，網址為：https://console.aws.amazon.com/storagegateway/home/。

如果您偏好程式設計方法，則可以使用 AWS Storage Gateway 應用程式設計界面 (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 AWS SDKs 會包裝基礎 Storage Gateway API，以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，且與其他區域無關。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 AWS Identity and Access Management，例如 ，沒有區域資源。您可以在符合您業務需求的位置啟動 AWS 資源。例如，您可能想要啟動 Amazon EC2 執行個體，以 AWS 區域 在歐洲的 中託管您的 AWS Storage Gateway 設備，以便更接近您的歐洲使用者，或符合法律要求。您的 會 AWS 帳戶 決定特定服務支援哪些區域可供您使用。

- Storage Gateway - 如需支援 AWS 的區域和服務 AWS 端點清單 Storage Gateway ，請參閱《AWS Storage Gateway 》中的端點和配額AWS 一般參考。
- Storage Gateway 硬體設備 - 如需可搭配硬體設備使用的支援 AWS 區域，請參閱《》中的AWS Storage Gateway 硬體設備區域AWS 一般參考。

設定磁碟區閘道的需求

除非另有說明，否則以下需求皆為所有閘道組態的常見需求。

主題

- 硬體及儲存體需求
- 網路與防火牆需求
- 支援的 Hypervisor 與主機需求
- 支援的 iSCSI 啟動器

硬體及儲存體需求

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

VM 的硬體需求。

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

- 指派給 VM 的四個虛擬處理器。
- 對於磁碟區閘道，您的硬體應該專用以下數量的 RAM：
  - 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
- 安裝 VM 映像和系統資料的 80 GiB 磁碟空間。

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

Amazon EC2 執行個體類型的需求

將閘道部署於 Amazon Elastic Compute Cloud (Amazon EC2) 時，執行個體的大小必須至少為 xlarge，您的閘道才能正常運作。但是，針對運算最佳化的執行個體系列，大小必須至少為 2xlarge。

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

> **Note**
>
> Storage Gateway AMI 需要支援 UEFI 開機模式的 Amazon EC2 執行個體類型。如果您選擇僅支援舊版 BIOS 開機的執行個體類型，則執行個體無法啟動，也不會通過其運作狀態檢查。啟動閘道之前，請確認您選擇的執行個體類型支援 UEFI 開機。若要檢查執行個體類型支援的開機模式，請呼叫 DescribeInstanceTypes Amazon EC2 API 操作。然後檢閱回應中的 `SupportedBootModes` 欄位。UEFI 開機支援也可能因可用區域而有所不同。

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

- 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

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。

建議用於快取磁碟區

- 一般用途執行個體系列 – m5 或 m6 執行個體類型。
- 運算最佳化執行個體系列 – c5、c6 或 c7 執行個體類型。選取 2xlarge 或更高的執行個體大小來符合必要的 RAM 需求。
- 記憶體最佳化執行個體系列 – r5、r6 或 r7 執行個體類型。
- 儲存體最佳化執行個體系列 – i4 或 i7 執行個體類型。

儲存需求

除了 VM 的 80 GiB 磁碟空間之外，您的閘道也需要額外的磁碟。

下表針對您所部署的閘道建議本機磁碟儲存體大小。

閘道類型	快取 (最小值)	快取 (最大值)	上傳緩衝區 (最小值)	上傳緩衝區 (最大值)	其他必要的本機磁碟
快取磁碟區閘道	150 GiB	64 TiB	150 GiB	2 TiB	—
儲存的磁碟區閘道	—	—	150 GiB	2 TiB	1 個或以上的儲存磁碟區

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

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

網路與防火牆需求

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

> **Note**
>
> 在某些情況下，您可以在 Amazon EC2 上部署 Storage Gateway，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，您的閘道可能會遇到服務連線問題。您需要使用的 AWS IP 地址範圍值位於您啟用閘道所在 AWS 區域的 Amazon 服務子集中。如需有關目前 IP 範圍值的資訊，請參閱 AWS 一般參考 中的 AWS IP 地址範圍。

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

主題

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

連接埠需求

磁碟區閘道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。

磁碟區閘道的連接埠需求

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，您從中連線到主控台的主機必須能夠存取閘道

網路元素	從	到	通訊協定	站點	傳入	傳出	必要	備註
								的連接埠 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	✓	✓	✓	內部部署系統用來將 VM 時間與主機時間同步。Storage Gateway VM 會設定為使用下列 NTP 伺服器： • 0.amazon.pool.ntp.org • 1.amazon.pool.ntp.org • 2.amazon.pool.ntp.org • 3.amazon.pool.ntp.org 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。

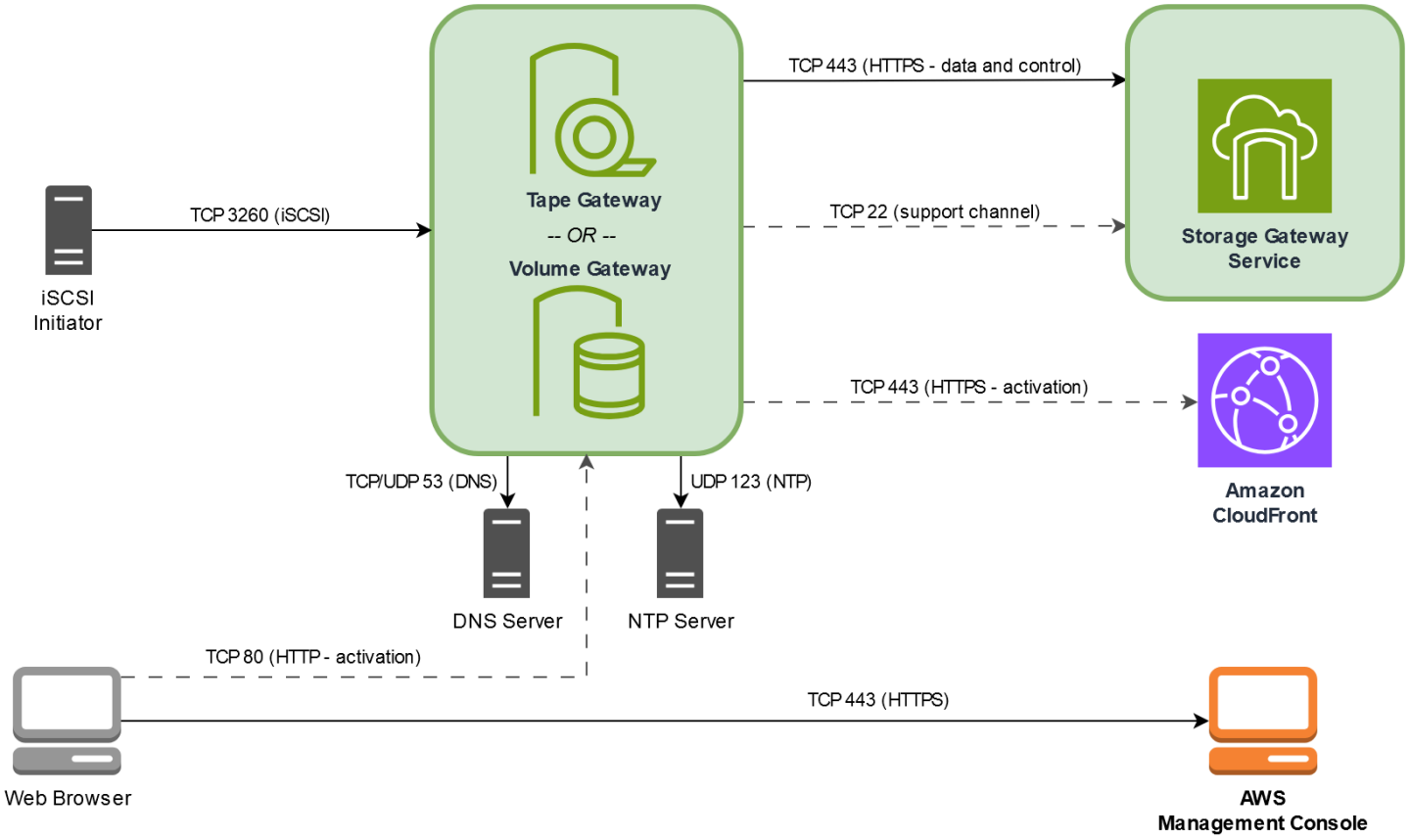
網路元素	從	到	通訊協定	站點	傳入	傳出	必要	備註
Storage Gateway	Storage Gateway VM	支援 端點	TCP SSH	22	✓	✓	✓	允許 支援 存取您的閘道，以協助您疑難排解閘道問題。不需要將此埠開放給閘道的正常操作使用，但進行疑難排解時需要用到。如需支援端點的清單，請參閱支援 端點。
Storage Gateway	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓	管理主控台
Amazon CloudFront	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓	用於啟用

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
iSCSI 用戶端	iSCSI 用戶端	Storage Gateway VM	TCP	3260	✓	✓	✓	讓本機系統連線到閘道公開的 iSCSI 目標。

下圖顯示基本 Volume Gateway 部署的網路流量流程。



Storage Gateway 硬體設備的網路與防火牆要求

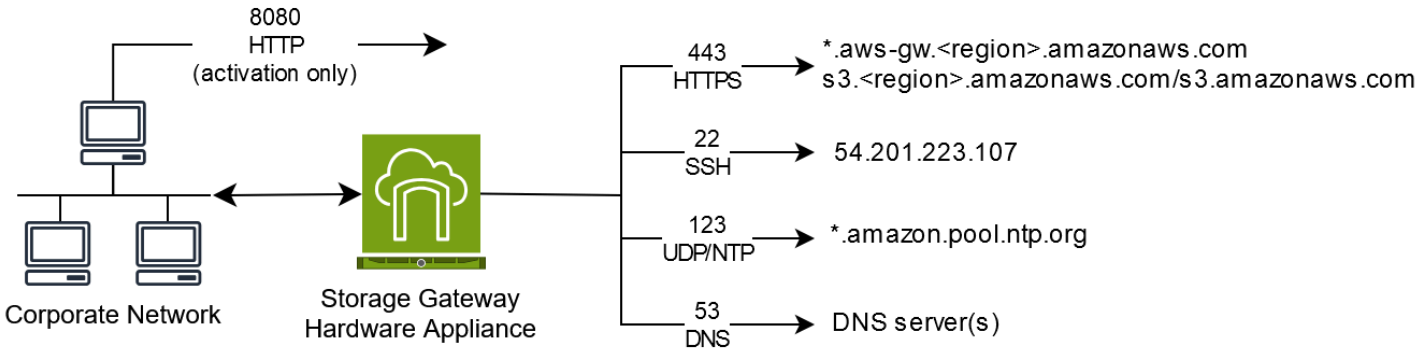
每個 Storage Gateway 硬體設備都需要下列網路服務：

- 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。

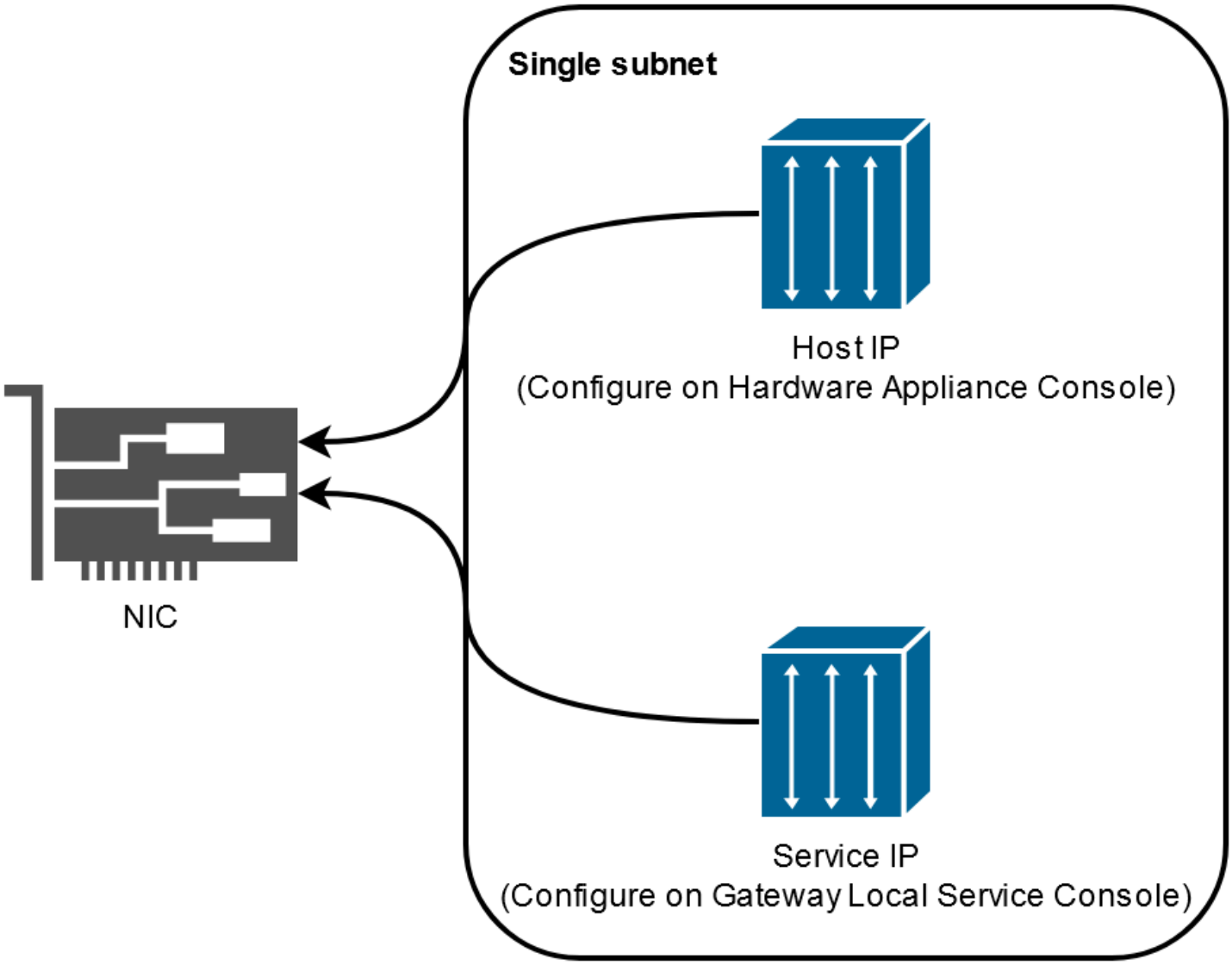
通訊協定	站點	Direction	來源	目標	使用方式
SSH	22	傳出	硬體設備	54.201.223.107	支援通道
DNS	53	傳出	硬體設備	DNS 伺服器	名稱解析
UDP/NTP	123	傳出	硬體設備	*.amazon.pool.ntp.org	時間同步
HTTPS	443	傳出	硬體設備	*.amazonaws.com	資料傳輸
HTTP	8080	傳入	AWS	硬體設備	啟用 (只需短暫時間)

若要依設計方式執行，硬體設備需要如下所示的網路和防火牆設定：

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

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

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。



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

允許透過防火牆和路由器 AWS Storage Gateway 存取

您的閘道需要存取 Storage Gateway 服務端點，才能與 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**
>
> 根據您閘道 AWS 的區域，以正確的*##*字串取代服務端點中的區域。

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。

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
```

雙堆疊端點

這些端點支援閘道設備與 之間的 IPv4 和 IPv6 流量 AWS。

控制路徑 （ 啟用、控制平面、代理 ） 和資料路徑 （ 資料平面 ） 操作的所有閘道都需要下列雙堆疊服務端點。

```
activation-storagegateway.region.api.aws:443
controlplane-storagegateway.region.api.aws:443
proxy-storagegateway.region.api.aws:443
dataplane-storagegateway.region.api.aws:443
```

需要下列閘道雙堆疊服務端點才能進行 API 呼叫。

```
storagegateway.region.api.aws:443
```

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

```
storagegateway.us-west-2.api.aws:443
```

FIPS 端點

這些端點支援閘道設備與 之間的 IPv4 流量 AWS，並符合聯邦資訊處理標準 (FIPS)。

FIPS 閘道需要下列服務端點，才能進行控制路徑 (anon-cp、client-cp、proxy-app) 和資料路徑 (dp-1) 操作。

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

使用下列閘道服務端點進行 API 呼叫。

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

雙堆疊 FIPS 端點

這些端點支援閘道設備與 之間的 IPv4 和 IPv6 流量 AWS，並符合 FIPS。

FIPS 閘道需要下列雙堆疊服務端點，才能進行控制路徑 （ 啟用、控制平面、代理 ） 和資料路徑 （ 資料平面 ） 操作。

```
activation-storagegateway-fips.region.api.aws:443
controlplane-storagegateway-fips.region.api.aws:443
proxy-storagegateway-fips.region.api.aws:443
dataplane-storagegateway-fips.region.api.aws:443
```

使用下列閘道雙堆疊服務端點進行 API 呼叫。

```
storagegateway-fips.region.api.aws:443
```

> **Note**
>
> FIPS 端點僅適用於某些 AWS 區域。如需詳細資訊，請參閱 AWS 一般參考 中的 Storage Gateway 端點和配額。

NTP 伺服器

Storage Gateway VM 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 和服務端點的完整清單，請參閱《》中的 Storage GatewayAWS 一般參考。

設定 Amazon EC2 閘道執行個體的安全群組

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

- 安全群組不應該允許來自外部網際網路的傳入連線。它只應該允許閘道安全群組內的執行個體與閘道通訊。如果您需要允許執行個體從其安全群組外部連線至閘道，則建議您只允許連接埠 3260 (適用於 iSCSI 連線) 和 80 (適用於啟用) 上的連線。
- 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 您想要協助對 EC2 閘道進行故障診斷。

在某些情況下，您可能會使用 Amazon EC2 執行個體作為啟動器 (也就是說，連線至 Amazon EC2 上所部署閘道上的 iSCSI 目標)。在這種情況下，建議使用兩個步驟的方法：

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

如需要針對閘道所開啟之連接埠的資訊，請參閱連接埠需求。

支援的 Hypervisor 與主機需求

您可以將 Storage Gateway 內部部署以虛擬機器 (VM) 設備或實體硬體設備的形式執行，或在 中以 Amazon EC2 執行個體 AWS 的形式執行。

> **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。

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

Storage Gateway 支援下列 Hypervisor 版本與主機：

- VMware ESXi Hypervisor (7.0 或 8.0 版） – 在此設定中，您也需要 VMware vSphere 用戶端來連線至主機。
- Microsoft Hyper-V Hypervisor (2019、2022 或 2025 版） – 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 經過 CentOS/RHEL 7.7、Ubuntu 16.04 LTS 和 Ubuntu 18.04 LTS 發行版本的測試，並受其支援。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 10.0.1.1 版開始的 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) 解決方案中。
- Amazon EC2 執行個體：Storage Gateway 提供包含閘道 VM 映像檔的 Amazon Machine Image (AMI)。僅有檔案、快取磁碟區和磁帶閘道類型才能在 Amazon EC2 上部署。如需如何在 Amazon EC2 上部署閘道的資訊，請參閱 部署磁碟區閘道的自訂 Amazon EC2 執行個體。
- Storage Gateway 硬體設備：Storage Gateway 以內部部署選項形式，為具有有限虛擬機器基礎設施的位置提供實體硬體設備。

> **Note**
>
> Storage Gateway 不支援透過從快照、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。

支援的 iSCSI 啟動器

當部署快取磁碟區或儲存的磁碟區閘道時，您可以在閘道上建立 iSCSI 儲存磁碟區。

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

- Microsoft Windows Server 2022
- Red Hat Enterprise Linux 8
- Red Hat Enterprise Linux 9
- VMware ESX 啟動器，提供使用您 VM 之 Guest 作業系統中的啟動器之外的替代方案。

> **Important**
>
> Storage Gateway 不支援來自 Windows 用戶端的 Microsoft Multipath I/O (MPIO)。
> 如果主機使用 Windows Server 容錯移轉叢集 (WSFC) 協調存取，Storage Gateway 可支援將多個主機連線到相同的磁碟區。但是，您無法在不使用 WSFC 的情況下將多個主機連線至同個磁碟區 (例如：共享一個非叢集 NTFS/ext4 檔案系統)。

使用 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。

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

每個硬體設備都是高效能的 1U 伺服器，您可以部署在您的資料中心內或內部部署在公司防火牆內。當您購買並啟用硬體設備時，啟用程序會將硬體設備與您的 建立關聯 AWS 帳戶。啟用後，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。您用來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 AWS 區域 Storage Gateway 硬體設備可供啟用和使用的支援清單，請參閱 中的 Storage Gateway 硬體設備區域AWS 一般參考。

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

主題

- 設定 Storage Gateway 硬體設備
- 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 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 Storage Gateway 硬體設備

設定 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。

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 Storage Gateway 硬體設備。
4. 在硬體設備上建立閘道。如需詳細資訊，請參閱建立磁碟區端點。

   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。

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：

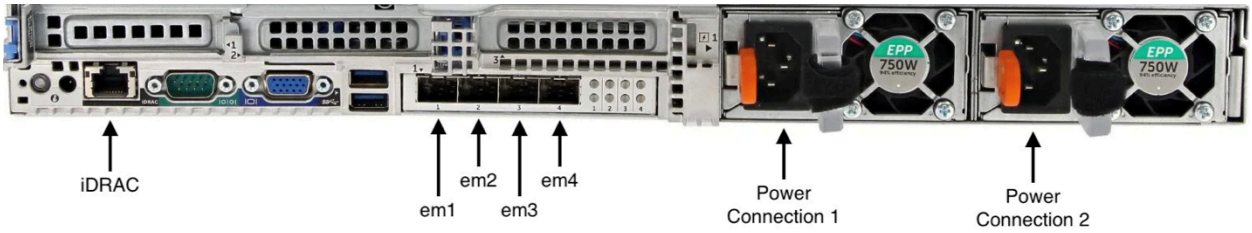
- 電源線：一條為必要、建議兩條。
- 支援的網路佈線 (視硬體設備中包含的網路介面卡 (NIC) 而定)。雙軸銅 DAC，SFP+ 光學模區塊 (英特爾兼容) 或 SFP 到 Base-T 銅線收發器。
- 鍵盤和顯示器，或鍵盤、視訊和滑鼠 (KVM) 切換解決方案。

> **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. 將硬體設備拆箱，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。

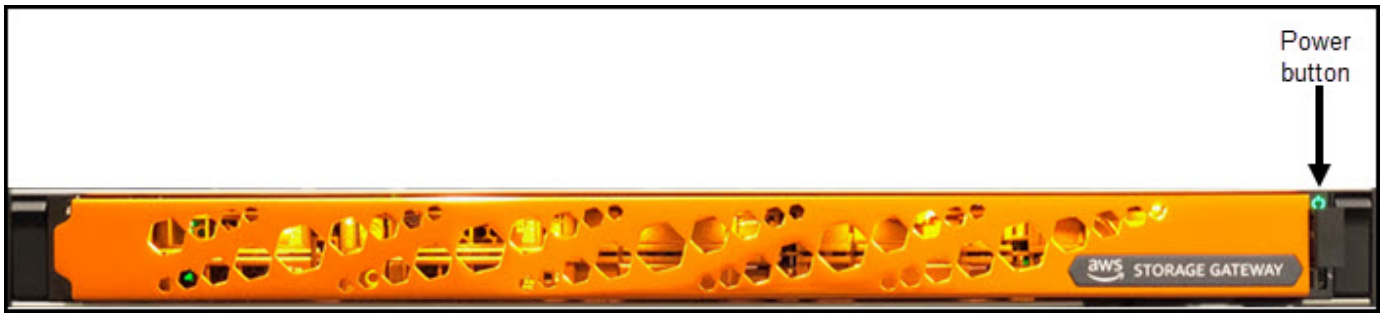
2. 將電源線插入兩個電源供應器。您可以只將 插入一個電源連接，但我們建議將電源連接到兩個電源以進行備援。

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。

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。設定網路頁面會顯示硬體設備上 4 個網路介面中每個介面的 IP 和 DNS 資訊，並包含用於設定每個介面 DHCP 或靜態地址的功能表選項。
2. 針對 em1 界面，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 網路界面的有效 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 端點相同的永遠連線。

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 Storage Gateway 硬體設備

啟用 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。

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。

如要啟用您的儲存閘道硬體設備。

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

> **Note**
>
> 僅限啟用，必須符合下列條件：
>
> - 您的瀏覽器必須位於硬體設備的同一個網路上。

- 您的防火牆必須允許連接埠 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。

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。 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：//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 地址指派給安裝在硬體設備上的閘道，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 在本機主控台中為內部部署閘道執行儲存閘道命令。您也可以從 Storage Gateway 主控台設定密碼。如需詳細資訊，請參閱從 Storage Gateway 主控台設定本機主控台密碼。

3. AWS 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. 執行下列其中一項來設定閘道 IP 地址：

   - 若要使用動態主機組態協定 (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，請輸入對應的數字來設定靜態 IP，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。

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

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

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

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

建立磁碟區端點

在本節中，您可以找到如何下載、部署和啟用磁碟區閘道的說明。

主題

- 設定磁碟區閘道
- 將您的磁碟區閘道連線至 AWS
- 檢閱設定並啟用磁碟區閘道
- 設定磁碟區閘道

設定磁碟區閘道

設定新的磁碟區閘道

1. 在 AWS 管理主控台 https：//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。您可以搜尋此名稱，在 Storage Gateway 主控台的清單頁面上尋找閘道。
   b. 針對閘道時區，請選擇您要部署閘道的全球當地時區。
4. 在閘道選項區段中，針對閘道類型選擇磁碟區閘道，然後選擇閘道將使用的磁碟區類型。您可從下列選項擇一使用：
   - 快取磁碟區：將您的主要資料存放在 Amazon S3，並將經常存取的資料保留在本機快取中，以加快存取速度。
   - 存放磁碟區：將所有資料存放在本機，同時以非同步方式備份到 Amazon S3。使用此磁碟區類型的閘道無法部署在 Amazon EC2 上。
5. 在平台選項區段中，執行下列操作：
   a. 對於主機平台，請選擇要在其上部署閘道的平台，然後依照 Storage Gateway 主控台頁面上顯示的平台特定指示來設定主機平台。您可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、部署和配置閘道虛擬機。
      - Linux KVM：使用 Linux KVM 下載、部署和設定閘道器虛擬機器。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：配置和啟動一個 Amazon EC2 執行個體來託管您的閘道。此選項不適用於儲存磁碟區閘道。
      - 硬體設備 - 從 訂購專用實體硬體設備 AWS ，以託管您的閘道。
   b. 在確認設定閘道中，選取核取方塊以確認您已針對所選主機平台執行部署步驟。此步驟不適用於硬體設備主機平台。
6. 選擇下一步繼續進行。

現在您的閘道已設定完成，您需要選擇連線和通訊的方式 AWS。如需說明，請參閱將磁碟區閘道連接至 AWS 。

將您的磁碟區閘道連線至 AWS

將新的磁碟區閘道連線至 AWS

1. 如果您尚未完成設定磁碟區閘道中所述的程序，請完成該程序。完成時，請選擇下一步，在 Storage Gateway 主控台中開啟連接到 AWS 頁面。
2. 在端點選項區段中，針對服務端點，選擇閘道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。如果選取此選項，請使用已啟用 FIPS 的端點核取方塊來指定連線是否應符合聯邦資訊處理標準 (FIPS)。

     > **Note**
     >
     > 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 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) 140-3。
     > FIPS 服務端點僅適用於 AWS 區域。如需詳細資訊，請參閱 AWS 一般參考 中的 Storage Gateway 端點和配額。

   - VPC 託管：您的閘道透過 VPC 的私人連線與 AWS 進行通訊，可讓您控制網路設定。如果選取此選項，則必須從下拉式功能表中選擇其 VPC 端點識別碼，或提供其 VPC 端點 DNS 名稱或 IP 地址，以指定現有的 VPC 端點。與可公開存取的端點類似，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)。如需詳細資訊，請參閱在虛擬私有雲端中啟用閘道。

     > **Note**
     >
     > 如果您在 AWS 透過 VPC 端點存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用符合 FIPS 標準的 VPC 端點。如需詳細資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。
     > FIPS 服務端點僅適用於 AWS 區域。如需詳細資訊，請參閱 AWS 一般參考 中的 Storage Gateway 端點和配額。

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

4. 選擇下一步繼續進行。

現在您已選擇閘道的連線方式 AWS，您需要啟用閘道。如需指示，請參閱檢閱設定並啟用磁碟區閘道。

檢閱設定並啟用磁碟區閘道

部署並啟用新的磁碟區閘道。

1. 如果您尚未這麼做，請完成下列主題中所述的程序：

   - 設定磁碟區閘道
   - 將您的磁碟區閘道連線至 AWS

   完成時，請選擇下一步，在 Storage Gateway 主控台中開啟檢閱並啟用頁面。
2. 檢閱頁面上每個區段的初始閘道詳細資訊。
3. 如果區段包含錯誤，請選擇編輯以傳回對應的設定頁面並進行變更。

> **Note**
>
> 建立閘道後，您無法修改閘道選項或連線設定。

4. 選擇啟動閘道以繼續。

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

設定磁碟區閘道

在新的磁碟區閘道上執行第一次設定

1. 如果您尚未這麼做，請完成下列主題中所述的程序：

- 設定磁碟區閘道
- 將您的磁碟區閘道連線至 AWS
- 檢閱設定並啟用磁碟區閘道

完成時，請選擇下一步，在 Storage Gateway 主控台中開啟設定閘道頁面。

2. 在設定儲存區段中，使用下拉式功能表至少配置一個具有 165 GiB 容量的磁碟供快取儲存使用，以及至少一個具有 150 GiB 容量的磁碟以供上傳緩衝區使用。本節中列出的本機磁碟對應於您在主機平台上佈建的實體儲存體。
3. 在 CloudWatch 日誌群組區段中，選擇如何設定 Amazon CloudWatch Logs 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：設定新的日誌群組以監控閘道。
   - 使用現有的日誌群組：從對應的下拉式功能表中選擇現有的日誌群組。
   - 停用記錄：請勿使用 Amazon CloudWatch Logs 來監控您的閘道。

   > **Note**
   >
   > 若要接收 Storage Gateway 運作狀態日誌，您的日誌群組資源政策中必須存在下列許可。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

   - 建立自訂警示：設定新的 CloudWatch 警示以通知您閘道的指標。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：不會收到有關閘道指標的 CloudWatch 通知。

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

6. 選擇設定以完成建立閘道。

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

現在您已經建立閘道，您必須建立要使用的磁碟區。如需說明，請參閱建立磁碟區。

建立儲存磁碟區

先前，您已配置已新增至 VM 快取儲存和上傳緩衝的本機磁碟。現在，您可以建立應用程式讀取和寫入資料的儲存磁碟區。閘道會將磁碟區的最近存取資料保留在快取儲存本機，並且將資料非同步傳輸至 Amazon S3。針對儲存的磁碟區，您已配置新增至 VM 上傳緩衝區和應用程式資料的本機磁碟。

> **Note**
>
> 您可以使用 AWS Key Management Service (AWS KMS) 加密寫入 Amazon S3 中存放之快取磁碟區的資料。您現可使用 AWS Storage Gateway API 參考資料執行此作業。如需詳細資訊，請參閱 CreateCachediSCSIVolume 或 create-cached-iscsi-volume。

建立 磁碟區

1. 前往 https://console.aws.amazon.com/storagegateway/home 開啟 Storage Gateway 主控台。
2. 在 Storage Gateway 主控台上，選擇建立磁碟區。
3. 在 Create volume (建立磁碟區) 對話方塊中，針對 Gateway (閘道) 選擇閘道。
4. 針對快取磁碟區，在容量中輸入容量。

   針對存放磁碟區，從清單選擇 Disk ID (磁碟 ID) 值。
5. 針對磁碟區內容，您的選項取決於您為其建立磁碟區的閘道類型。

   針對快取磁碟區，您有下列選項：

   - Create a new empty volume (建立新的且空白的磁碟區)。
   - 根據 Amazon EBS 快照建立磁碟區。如果您選擇此選項，則請提供 EBS snapshot ID (EBS 快照 ID) 的值。

     > **Note**
     >
     > Storage Gateway 不支援從 AWS Marketplace 磁碟區的快照建立快取磁碟區。

   - Clone from last volume recovery point (從上次磁碟區復原點複製)。如果您選擇此選項，則請針對 Source volume (來源磁碟區) 選擇磁碟區 ID。如果區域中沒有磁碟區，則不會出現此選項。

   針對存放磁碟區，您有下列選項：

   - Create a new empty volume (建立新的且空白的磁碟區)。
   - Create a volume based on a snapshot (根據快照建立磁碟區)。如果您選擇此選項，則請提供 EBS snapshot ID (EBS 快照 ID) 的值。
   - Preserve existing data on the disk (保留磁碟上的現有資料)
6. 針對 iSCSI 目標名稱，輸入名稱。

目標名稱可以包含小寫字母、數字、句號 (.) 和連字號 (-)。在探索之後，此目標名稱會顯示為 iSCSI Microsoft 啟動器 UI 之目標標籤中的 iSCSI 目標節點名稱。例如，`target1` 名稱會顯示為 `iqn.1007-05.com.amazon:target1`。請確定目標名稱在儲存區域網路 (SAN) 內為全域唯一的。

7. 確認 Network interface (網路界面) 設定已選取 IP 地址，或針對 Network interface (網路界面) 選擇 IP 地址。針對 Network interface (網路界面)，會針對閘道 VM 所設定的每個轉接器顯示一個 IP 地址。如果只針對一個網路轉接器設定閘道 VM，則不會顯示 Network interface (網路界面) 清單，因為只有一個 IP 地址。

   您的 iSCSI 目標將可在您選擇的網路轉接器上使用。

   如果您已定義閘道使用多個網路轉接器，則請選擇您儲存應用程式應該用來存取磁碟區的 IP 地址。如需設定多個網路轉接器的資訊，請參閱為多個 NIC 設定閘道。

   > **Note**
   >
   > 在您選擇網路轉接器之後，就無法變更此設定。

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

   如果您之前已在此區域中建立磁碟區，則可以看到它們列在 Storage Gateway 主控台中。

   Configure CHAP Authentication (設定 CHAP 身分驗證) 對話方塊隨即出現。您目前可以設定磁碟區的挑戰交握驗證協定 (CHAP)，也可以選擇取消並稍後設定 CHAP。如需 CHAP 設定的詳細資訊，請參閱 設定磁碟區的 CHAP 身分驗證。

如果您不想要設定 CHAP，則請開始使用磁碟區。如需詳細資訊，請參閱將磁碟區連接到用戶端。

設定磁碟區的 CHAP 身分驗證

CHAP 會要求通過驗證方可存取儲存磁碟區目標，藉此防範重送攻擊。請在 Configure CHAP Authentication (設定 CHAP 驗證) 對話方塊中，提供磁碟區 CHAP 設定時所需的資訊。

設定 CHAP

1. 選擇要用來設定 CHAP 的磁碟區。

2. 針對 Actions (動作)，選擇 Configure CHAP authentication (設定 CHAP 身分驗證)。
3. 針對啟動器名稱，輸入您啟動器的名稱。
4. 針對啟動器秘密，輸入您用來驗證您 iSCSI 啟動器的秘密短語。
5. 針對目標秘密，輸入用來驗證您的雙向 CHAP 目標的秘密短語。
6. 選擇 Save (儲存) 儲存各個項目。

   如需設定與使用 CHAP 驗證方面的詳細資訊，請參閱 設定 iSCSI 目標的 CHAP 身分驗證。

下一步驟

將磁碟區連接到用戶端

將磁碟區連接到用戶端

您可以在用戶端中使用 iSCSI 啟動器，以連線至磁碟區。在下列程序結束時，磁碟區在您的用戶端上會當成本機裝置使用。

> **Important**
>
> 如果主機使用 Windows Server 容錯移轉叢集 (WSFC) 協調存取，則您可以使用 Storage Gateway 將多個主機連線至相同的磁碟區。您無法在不使用 WSFC 的情況下將多個主機連線至相同的磁碟區 (例如，共享一個非叢集 NTFS/ext4 檔案系統)。

主題

- 連線至 Microsoft Windows 用戶端
- 連線至 Red Hat Enterprise Linux 用戶端

連線至 Microsoft Windows 用戶端

下列程序概略說明您連線至 Windows 用戶端所遵循的步驟。如需詳細資訊，請參閱連線 iSCSI 啟動器。

連線至 Windows 用戶端

1. 啟動 iscsicpl.exe。

2. 在 iSCSI Initiator Properties (iSCSI 啟動器屬性) 對話方塊中，選擇 Discovery (搜索) 標籤，然後選擇 Discovery Portal (搜索入口網站)。
3. 在 Discover Target Portal (搜索目標入口網站) 對話方塊中，輸入 iSCSI 目標的 IP 地址做為 IP 地址或 DNS 名稱。
4. 將新的目標入口網站連線至閘道上的儲存磁碟區目標。
5. 選擇目標，然後選擇 Connect (連線)。
6. 在 Targets (目標) 標籤中，確定目標狀態的值為 Connected (已連線) (這指出已連線目標)，然後選擇 OK (確定)。

連線至 Red Hat Enterprise Linux 用戶端

下列程序顯示您可遵循以連線至 Red Hat Enterprise Linux (RHEL) 用戶端之步驟的摘要。如需詳細資訊，請參閱連線 iSCSI 啟動器。

將 Linux 用戶端連線至 iSCSI 目標

1. 安裝 iscsi-initiator-utils RPM 套件。

   您可以使用下列命令來安裝套件。

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

2. 確定 iSCSI 協助程式正在執行。

   針對 RHEL 5 或 6，使用下列命令。

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

   對於 RHEL 7、8 或 9，請使用下列命令。

   ```
   sudo service iscsid status
   ```

3. 搜索針對閘道所定義的磁碟區或 VTL 裝置目標。請使用下列搜索命令。

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

   搜索命令的輸出看起來應該像下列範例輸出。

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

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

4. 連線至目標

   確認您在連線命令中指定正確的 *[GATEWAY_IP]* 及 IQN。

   使用下列 命令。

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

5. 確認磁碟區已連接至用戶端機器 (啟動器)。為此，請使用下列命令。

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

   命令的輸出看起來應該像下列範例輸出。

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

   強烈建議您在設定啟動器之後，依照自訂您的 Linux iSCSI 設定中討論的內容自訂 iSCSI 設定。

初始化和格式化您的磁碟區

當您使用 iSCSI 啟動器在用戶端連線到您的磁碟區之後，您即可初始化和格式化您的磁碟區。

主題

- 在 Microsoft Windows 上初始化和格式化您的磁碟區
- 在 Red Hat Enterprise Linux 上初始化和格式化您的磁碟區

在 Microsoft Windows 上初始化和格式化您的磁碟區

請使用下列步驟在 Windows 初始化和格式化您的磁碟區。

初始化和格式化您的儲存磁碟區

1. 啟動 **diskmgmt.msc** 以開啟 Disk Management (磁碟管理) 主控台。

2. 在 Initialize Disk (初始化磁碟) 對話方塊中，將磁碟區初始化為 MBR (Master Boot Record) (MBR (主開機記錄)) 分割區。選取分割區樣式時，您應該考慮要連線的磁碟區類型 (快取或存放)，如下表所示。

分割區樣式	在下列條件中使用
MBR (主開機記錄)	• 如果您的閘道是存放磁碟區，且儲存磁碟區的大小限制為 1 TiB。 • 如果您的閘道是快取磁碟區，且儲存磁碟區的大小小於 2 TiB。
GPT (GUID 分割區表)	如果您的閘道儲存磁碟區大小為 2 TiB 或更大。

3. 建立簡易磁碟區：

   a. 將磁碟區上線並初始化。所有可用的磁碟區都會顯示在磁碟管理主控台中。

   b. 開啟內容 (按右鍵) 選單取得磁碟，然後選擇 New Simple Volume (新增簡易磁碟區)。

   > **Important**
   >
   > 請小心勿錯誤的磁碟格式化。檢查以確認您格式化的磁碟符合您配置給閘道 VM 的本機磁碟大小，而且狀態為 Unallocated (未配置)。

   c. 指定磁碟大小上限。

   d. 將某個磁碟機字母或路徑指派給您的磁碟區，然後選擇 Perform a quick format (執行快速格式化) 格式化磁碟區。

   > **Important**
   >
   > 快取磁碟區強烈建議使用 Perform a quick format (執行快速格式化)。這樣可得到較少的初始化 I/O、較小的初始快照大小，以及最快可用的磁碟區。還可避免使用快取磁碟區空間處理完整的格式化程序。

   > **Note**
   >
   > 格式化磁碟區所需的時間取決於磁碟區的大小。此程序可能需要幾分鐘才能完成。

在 Red Hat Enterprise Linux 上初始化和格式化您的磁碟區

請使用下列步驟在 Red Hat Enterprise Linux (RHEL) 上初始化和格式化您的磁碟區。

初始化和格式化您的儲存磁碟區

1. 將目錄變更到 /dev 資料夾。
2. 執行 sudo cfdisk 命令。
3. 使用下列命令，找出您的新磁碟區。若要尋找新的磁碟區，您可以列出您磁碟區的分割區配置。

   ```
   $ lsblk
   ```

   新的未分割磁碟區會顯示「無法辨識磁碟區標籤」錯誤。
4. 初始化您新的磁碟區。選取分割區樣式時，您應該考慮要連線的磁碟區大小和類型 (快取或存放)，如下表所示。

分割區樣式	在下列條件中使用
MBR (主開機記錄)	• 如果您的閘道是存放磁碟區，且儲存磁碟區的大小限制為 1 TiB。 • 如果您的閘道是快取磁碟區，且儲存磁碟區的大小小於 2 TiB。
GPT (GUID 分割區表)	如果您的閘道儲存磁碟區大小為 2 TiB 或更大。

   針對 MBR 分割區，請使用下列命令：sudo parted /dev/*your volume* mklabel msdos

   針對 GPT 分割區，請使用下列命令：sudo parted /dev/*your volume* mklabel gpt
5. 使用下列命令建立分割區。

   ```
   sudo parted -a opt /dev/your volume mkpart primary file system 0% 100%
   ```
6. 將某個磁碟機字母指派給分割區，並使用下列命令建立檔案系統。

   ```
   sudo mkfs -L datapartition /dev/your volume
   ```
7. 使用下列命令掛載檔案系統。

   ```
   sudo mount -o defaults /dev/your volume /mnt/your directory
   ```

測試您的閘道

執行下列任務，以測試磁碟區閘道設定：

1. 將資料寫入至磁碟區。
2. 建立快照。
3. 將快照還原到另一個磁碟區。

您可以透過建立磁碟區的快照備份並將快照存放在其中，來驗證閘道的設定 AWS。您接著會將快照還原到新的磁碟區。您的閘道會將資料從 中指定的快照複製到 AWS 新的磁碟區。

> **Note**
>
> 不支援從加密的 Amazon Elastic Block Store (Amazon EBS) 磁碟區還原資料。

在 Microsoft Windows 上建立儲存磁碟區的 Amazon EBS 快照

1. 在 Windows 電腦上，將一些資料複製至映射儲存磁碟區。

   在本示範中，複製的資料量不重要。小型檔案就足以示範還原處理程序。
2. 在 Storage Gateway 主控台的導覽窗格中，選擇磁碟區。
3. 選擇您為閘道所建立的儲存磁碟區。

   此閘道應該只有一個儲存磁碟區。選擇磁碟區以顯示其屬性。
4. 針對 Actions (動作)，選擇 Create EBS snapshot (建立 EBS 快照) 以建立磁碟區的快照。

   根據磁碟上的資料量和上傳頻寬，可能需要幾秒鐘的時間才能完成快照。請記下從中建立快照之磁碟區的磁碟區 ID。您可以使用 ID 來尋找快照。
5. 在 Create EBS Snapshot (建立 EBS 快照) 對話方塊中，提供快照的描述。
6. (選用) 針對 Tags (標籤)，輸入索引鍵和值以將標籤新增至快照。標籤為區分大小寫的索引鍵值組，可協助您管理、篩選和搜尋快照。
7. 選擇 Create Snapshot (建立快照)。您的快照會存放為 Amazon EBS 快照。記下您的快照 ID。為您的磁碟區所建立的快照數目會顯示在快照欄中。
8. 在 EBS 快照欄中，選擇您為其建立快照之磁碟區的連結，以查看 Amazon EC2 主控台上的 EBS 快照。

將快照還原到另一個磁碟區

請參閱建立儲存磁碟區。

備份您的磁碟區

您可以使用 Storage Gateway，協助保護將 Storage Gateway 磁碟區用於雲端備份儲存裝置的內部部署商業應用程式。您可以使用 Storage Gateway 或 AWS Backup中的原生快照排程器，備份您的內部部署 Storage Gateway 磁碟區。在這兩種情況下，Storage Gateway 磁碟區備份都會以 Amazon EBS 快照形式存放在 Amazon Web Services 中。

主題

- 使用 Storage Gateway 備份磁碟區
- 使用 AWS Backup 來備份您的磁碟區

使用 Storage Gateway 備份磁碟區

您可以使用 Storage Gateway 管理主控台建立 Amazon EBS 快照並將快照儲存於 Amazon Web Services，來備份您的磁碟區。您可以建立一次性快照，或設定由 Storage Gateway 管理的快照排程。您稍後可以使用 Storage Gateway 主控台，將快照還原到新的磁碟區。如需如何從 Storage Gateway 備份和管理備份的資訊，請參閱下列主題：

- 測試您的閘道
- 建立復原快照
- 從復原點複製快取磁碟區

使用 AWS Backup 來備份您的磁碟區

AWS Backup 是一種集中式備份服務，可讓您在 Amazon Web Services Cloud 和內部部署 AWS 的服務之間輕鬆且經濟實惠地備份應用程式資料。這樣做可協助您滿足業務和法規備份合規要求。 提供集中位置，讓您輕鬆地 AWS Backup 保護 AWS 儲存磁碟區、資料庫和檔案系統，以便執行下列動作：

- 設定和稽核您要備份 AWS 的資源。
- 自動化備份排程。
- 設定保留政策。

- 監控所有最近的備份與還原活動。

由於 Storage Gateway 與 整合 AWS Backup，因此可讓客戶使用 AWS Backup 來備份使用 Storage Gateway 磁碟區進行雲端後端儲存的內部部署商業應用程式。 AWS Backup 支援快取和存放磁碟區的備份和還原。如需 的詳細資訊 AWS Backup，請參閱 AWS Backup 文件。如需 的資訊 AWS Backup，請參閱AWS Backup 《 使用者指南》中的什麼是 AWS Backup？。

您可以使用 AWS Backup 管理 Storage Gateway 磁碟區的備份和復原操作，而不必建立自訂指令碼，或手動管理時間點備份。使用 AWS Backup，您也可以從單一 AWS Backup 儀表板監控內部部署磁碟區備份與雲端 AWS 資源。您可以使用 AWS Backup 建立一次性隨需備份或定義 管理的備份計劃 AWS Backup。

從 取得的 Storage Gateway 磁碟區備份 AWS Backup 會以 Amazon EBS 快照的形式儲存在 Amazon S3 中。您可以從 AWS Backup 主控台或 Amazon EBS 主控台查看 Storage Gateway 磁碟區備份。

您可以輕鬆將透過 管理的 Storage Gateway 磁碟區還原 AWS Backup 至任何內部部署閘道或雲端閘道。您也可以將此類磁碟區還原至您可以搭配 Amazon EC2 執行個體使用的 Amazon EBS 磁碟區。

使用 AWS Backup 備份Storage Gateway磁碟區的優點

使用 AWS Backup 備份 Storage Gateway 磁碟區的優點是您可以滿足合規要求、避免操作負擔，以及集中備份管理。 AWS Backup 可讓您執行下列動作：

- 設定符合您備份需求的可自訂排程備份政策。
- 設定備份保留和過期規則，因此您不再需要開發自訂指令碼，或手動管理您磁碟區的時間點備份。
- 從中央檢視管理和監控跨多個閘道和其他 AWS 資源的備份。

使用 AWS Backup 建立磁碟區的備份

> **Note**
>
> AWS Backup 要求您選擇 AWS Backup 取用的 AWS Identity and Access Management (IAM) 角色。您需要建立此角色，因為 AWS Backup 不會為您建立。您也需要在 AWS Backup 和此 IAM 角色之間建立信任關係。如需如何執行此作業的資訊，請參閱《AWS Backup 使用者指南》。如需如何執行此作業的資訊，請參閱《AWS Backup 使用者指南》中的建立備份計劃。

1. 開啟 Storage Gateway 主控台，然後從左側的導覽窗格選擇磁碟區。

2. 針對動作，選擇使用 建立隨需備份 AWS Backup 或建立 AWS 備份計劃。

   如果您想要建立 Storage Gateway 磁碟區的隨需備份，請選擇使用 建立隨需備份 AWS Backup。系統會將您導向至 AWS Backup 主控台。

   如果您想要建立新的 AWS Backup 計劃，請選擇建立 AWS 備份計劃。系統會將您導向至 AWS Backup 主控台。

   在 AWS Backup 主控台上，您可以建立備份計畫、將 Storage Gateway 磁碟區指派給備份計畫，以及建立備份。您也可以進行持續的備份管理任務。

從 尋找和還原您的磁碟區 AWS Backup

您可以從 AWS Backup 主控台尋找和還原備份 Storage Gateway 磁碟區。如需詳細資訊，請參閱《AWS Backup 使用者指南》。如需詳細資訊，請參閱《AWS Backup 使用者指南》中的復原點。

尋找和還原您的磁碟區

1. 開啟 AWS Backup 主控台並尋找您要還原的 Storage Gateway 磁碟區備份。您可以將 Storage Gateway 磁碟區備份還原到 Amazon EBS 磁碟區或 Storage Gateway 磁碟區。選擇適合您還原需求的選項。
2. 針對還原類型，選擇要還原的存放或快取 Storage Gateway 磁碟區並提供所需資訊：
   - 若是存放磁碟區，請提供 Gateway name (閘道名稱)、Disk ID (磁碟 ID) 和 iSCSI target name (iSCSI 目標名稱) 的資訊。
   - 若是快取磁碟區，請提供 Gateway name (閘道名稱)、Capacity (容量) 和 iSCSI target name (iSCSI 目標名稱) 的資訊。
3. 選擇 還原資源來還原您的磁碟區。

> **Note**
>
> 您無法使用 Amazon EBS 主控台來刪除由 建立的快照 AWS Backup。

接下來做些什麼？

在先前的章節中，您已建立及佈建閘道，並將您的主機連線到閘道的儲存體磁碟區。您將資料新增到閘道的 iSCSI 磁碟區、擷取磁碟區的快照，並將其還原至新的磁碟區、連線到新的磁碟區，然後確認資料在其中出現。

在您完成練習後，請考慮以下事項：

- 若您計劃繼續使用您的閘道，請閱讀針對實際的工作負載調整更適當的上傳緩衝大小的相關內容。如需詳細資訊，請參閱針對實際工作負載調整您磁碟區閘道的儲存體大小。

本指南的其他章節包含如何執行下列作業的相關資訊：

- 若要進一步了解儲存體磁碟區及管理方式，請參閱管理磁碟區閘道。
- 如果您不打算繼續使用您的閘道，請考慮刪除閘道，以免產生任何費用。如需詳細資訊，請參閱清除不必要的資源。
- 若要為閘道問題進行故障診斷，請參閱 為您的閘道進行疑難排解。
- 若要最佳化您的閘道，請參閱最佳化閘道效能。
- 若要了解 Storage Gateway 指標及監控您閘道執行狀況的方式，請參閱 監控 Storage Gateway。
- 若要進一步了解設定您閘道的 iSCSI 目標以存放資料，請參閱從 Windows 用戶端連線至您的磁碟區。

若要了解針對實際工作負載調整您磁碟區閘道的儲存體大小，以及清理您不需要的資源，請參閱下列各節。

針對實際工作負載調整您磁碟區閘道的儲存體大小

此時，您擁有一個簡易、可運作的閘道。但是，用來建立此閘道的假設並不適合用於實際的工作負載。若您希望此閘道適合實際的工作負載，您需要執行兩項作業：

1. 適當調整您的上傳緩衝。
2. 設定您上傳緩衝的監控 (若您尚未設定)。

您可於下述找到執行這兩項任務的方式。若您為快取磁碟區啟用閘道，您也需要針對實際的工作負載調整您的快取儲存體大小。

為閘道快取設定調整您的上傳緩衝及快取儲存體大小

- 使用在判斷要配置的上傳緩衝大小中顯示的公式來調整上傳緩衝的大小。我們強烈建議您為上傳緩衝配置至少 150 GiB。若上傳緩衝公式得出的值低於 150 GiB，請使用 150 GiB 做為您的配置上傳緩衝。

  上傳緩衝公式會考慮從應用程式到閘道的輸送量與從閘道到 的輸送量之間的差異 AWS，乘以您預期寫入資料的時間長度。例如，假設您的應用程式將文字資料寫入閘道的速率為每秒 40 MB，每天 12 小時，而您的網路輸送量為每秒 12 MB。假設文字資料的壓縮因數為 2:1，公式便會指定您需要配置大約 675 GiB 的上傳緩衝空間。

為存放設定調整您的上傳緩衝大小

- 使用在判斷要配置的上傳緩衝大小中討論的公式。我們強烈建議您為您的上傳緩衝配置至少 150 GiB。若上傳緩衝公式得出的值低於 150 GiB，請使用 150 GiB 做為您的配置上傳緩衝。

  上傳緩衝公式會考慮從應用程式到閘道的輸送量與從閘道到 的輸送量之間的差異 AWS，乘以您預期寫入資料的時間長度。例如，假設您的應用程式將文字資料寫入閘道的速率為每秒 40 MB，每天 12 小時，而您的網路輸送量為每秒 12 MB。假設文字資料的壓縮因數為 2:1，公式便會指定您需要配置大約 675 GiB 的上傳緩衝空間。

監控您的上傳緩衝

1. 前往 https://console.aws.amazon.com/storagegateway/home 開啟 Storage Gateway 主控台。
2. 選擇 Gateway (閘道) 標籤，選擇 Details (詳細資訊) 標籤，然後尋找 Upload Buffer Used (使用的上傳緩衝) 欄位來檢視您閘道目前的上傳緩衝。
3. 設定一或多個警示來通知您上傳緩衝的使用。

   我們強烈建議您在 Amazon CloudWatch 主控台中建立一或多個上傳緩衝警示。例如，您可以針對要收到警告的使用量層級設定警示，和針對在超出時引發以採取動作的使用量層級設定警示。動作可能會是新增更多上傳緩衝空間。如需詳細資訊，請參閱設定閘道上傳緩衝區的閾值警示上限。

在 VPC 中啟用閘道

您可以在內部部署閘道裝置以及雲端儲存基礎設施之間建立私有連線。您可以使用此連線來啟用閘道，並允許它將資料傳輸到 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，請參閱連接磁碟區閘道。 AWS

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

主題

- 建立針對 Storage Gateway 的 VPC 端點

建立針對 Storage Gateway 的 VPC 端點

按照這些指示來建立 VPC 端點。如果您已經有適用於 Storage Gateway 的 VPC 端點，則可以使用它來啟動閘道。

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`。針對 FIPS 相容的端點，選擇 `com.amazonaws.region.storagegateway-fips`，例如 `com.amazonaws.us-east-2.storagegateway-fips`。

   > **Note**
   >
   > FIPS 端點僅適用於某些 AWS 區域。如需詳細資訊，請參閱 AWS 一般參考 中的 Storage Gateway 端點和配額。

5. 針對 VPC，選擇您的 VPC，並記下其可用區域和子網路。

6. 確認未選取 Enable Private DNS Name (啟用私有 DNS 名稱)。
7. 針對 Security group (安全群組)，選擇要用於您的 VPC 的安全群組。您可以接受預設的安全群組。驗證您的安全群組中已允許所有下列 TCP 連接埠：

   - TCP 443
   - TCP 1026
   - TCP 1027
   - TCP 1028
   - TCP 1031
   - TCP 2222
8. 選擇建立端點。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 名稱看起來會像這樣：`vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

    如果您在具有 FIPS 可用性的區域中使用 FIPS 端點，您的 DNS 名稱看起來與此範例類似： `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway-fips.us-east-1.vpce.amazonaws.com`

現在您有一個 VPC 端點，您可以建立您的閘道。如需詳細資訊，請參閱建立閘道。

管理磁碟區閘道

管理閘道包括設定快取儲存和上傳緩衝空間、使用磁碟區，以及執行一般維護等任務。若您尚未建立閘道，請參閱入門 AWS Storage Gateway。

快取磁碟區是 Amazon Simple Storage Service (Amazon S3) 中的磁碟區，會公開為您可在其上存放應用程式資料的 iSCSI 目標。您可以在以下找到有關如何新增和刪除您快取設定之磁碟區的資訊。您也可以了解如何在 Amazon EC2 閘道中新增和移除 Amazon Elastic Block Store (Amazon EBS) 磁碟區。

> **Important**
>
> 如果快取磁碟區將主要資料保存在 Amazon S3 中，則您應該避免讀取或寫入整個磁碟區上所有資料的程序。例如，不建議使用病毒掃描軟體來掃描整個快取磁碟區。不論是根據需求或依排定完成，這類掃描都會將 Amazon S3 中存放的所有資料下載至本機來掃描，但這會導致高頻寬用量。您可以使用即時病毒掃描 (即在讀取或寫入快取磁碟區時掃描資料)，而不是執行完整磁碟掃描。

不支援調整磁碟區大小。若要變更磁碟區大小，請建立磁碟區的快照，然後使用該快照建立新的快取磁碟區。新的磁碟區可能會大於從中建立快照的磁碟區。如需說明如何移除磁碟區的步驟，請參閱刪除磁碟區。如需說明如何新增磁碟區以及保留現有資料的步驟，請參閱刪除儲存磁碟區。

所有快取磁碟區資料和快照資料都會存放至 Amazon S3，並使用伺服器端加密 (SSE) 靜態加密。不過，您無法使用 Amazon S3 API 或其他工具 (例如 Amazon S3 管理主控台) 來存取此資料。

您可以在下面找到如何管理 Volume Gateway 資源的相關資訊。

主題

- 編輯基本閘道資訊 - 了解如何使用 Storage Gateway 主控台編輯現有閘道的基本資訊，包括閘道名稱、時區和 CloudWatch 日誌群組。
- 新增和擴展磁碟區 - 了解如何將更多磁碟區新增至閘道，或隨著應用程式需求的增長擴展現有磁碟區的大小。
- 從復原點複製快取磁碟區 - 了解如何從現有磁碟區的復原點建立新的磁碟區，這是磁碟區上所有資料一致時儲存的時間點。
- 檢視磁碟區用量 - 了解如何使用 Storage Gateway 主控台檢視磁碟區上存放的資料量。

- 刪除儲存磁碟區 - 了解如何在應用程式需要變更時刪除磁碟區，例如遷移應用程式以使用較大的儲存磁碟區。
- 將您的磁碟區移至不同的閘道 - 了解如何分離並重新連接磁碟區，如果您需要隨著效能需求變更將磁碟區移至不同的磁碟區閘道，這會很有用。
- 建立復原快照 - 了解如何從閘道的磁碟區復原點建立復原快照，以及建立快照後可在 Storage Gateway 主控台中找到該快照的位置。
- 編輯快照排程 - 了解如何透過變更快照每天發生的時間或拍攝快照的頻率來自訂快照排程。
- 刪除儲存磁碟區的快照 - 了解如何在不再需要不必要的快照時將其刪除。
- 了解磁碟區狀態和轉換 - 了解 Storage Gateway 報告的各種磁碟區狀態值，以協助判斷磁碟區是否正常運作，或是否存在可能需要您採取動作的問題。
- 將資料移至新的閘道執行個體 - 了解如何隨著資料和效能需求的增長，或是在您收到遷移閘道的 AWS 通知時，在閘道之間移動資料。

編輯基本閘道資訊

您可以使用 Storage Gateway 主控台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。您可以從下列選項來選擇：

- 建立新的日誌群組 – 設定新的日誌群組來監控您的閘道。
- 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. 當您完成修改要變更的設定時，請選擇儲存變更。

新增和擴展磁碟區

隨著應用程式需求的增長，您可能需要將更多磁碟區新增至閘道，或擴展現有磁碟區的大小。當您新增或展開磁碟區時，必須考慮您配置給閘道的快取儲存體和上傳緩衝區的大小。閘道必須要有足夠的緩衝區和快取空間，以供新磁碟區使用。如需詳細資訊，請參閱判斷要配置的上傳緩衝大小。

您可以使用 Storage Gateway 主控台或 Storage Gateway API 新增磁碟區。如需如何使用 Storage Gateway 主控台新增磁碟區的說明，請參閱 建立儲存磁碟區。如需使用 Storage Gateway API 新增磁碟區的資訊，請參閱 CreateCachediSCSIVolume。

您可以使用下列其中一種方法擴展現有磁碟區的大小：

- 建立您要擴充之磁碟區的快照，然後使用該快照建立大小更大的新磁碟區。如需如何建立快照的資訊，請參閱建立復原快照。如需如何使用快照建立新磁碟區的資訊，請參閱建立儲存磁碟區。
- 使用您要擴充的快取磁碟區，以複製大小較大的新磁碟區。如需如何複製磁碟區的資訊，請參閱從復原點複製快取磁碟區。如需如何建立磁碟區的資訊，請參閱建立儲存磁碟區。

從復原點複製快取磁碟區

您可以從相同 AWS 區域中的任何現有快取磁碟區建立新的磁碟區。使用所選取磁碟區的最新復原點來建立新的磁碟區。磁碟區復原點是磁碟區的所有資料都一致的時間點。若要複製磁碟區，您可以選擇建立磁碟區對話方塊中的從上次復原點複製選項，然後選取磁碟區作為來源使用。

從現有磁碟區複製比建立 Amazon EBS 快照更快且更經濟實惠。使用來源磁碟區的最新復原點，複製會以位元組對位元組的方式將資料從來源磁碟區複製至新的磁碟區。Storage Gateway 會自動為您的快取磁碟區建立復原點。若要查看建立上次復原點的時間，請檢查 Amazon CloudWatch 中的 `TimeSinceLastRecoveryPoint` 指標。

複製的磁碟區與來源磁碟區無關。也就是說，複製後對任一磁碟區的變更都不會影響彼此。例如，如果您刪除來源磁碟區，則不會影響複製的磁碟區。您可以複製來源磁碟區，同時啟動器處於連線狀態並為

作用中使用。這樣做並不會影響來源磁碟區的效能。如需如何複製磁碟區的資訊，請參閱建立儲存磁碟區。

您也可以在復原藍本中使用複製程序。如需詳細資訊，請參閱您的快取閘道無法連接，而您想要復原資料。

下列程序顯示如何從磁碟區復原點複製磁碟區，以及使用該磁碟區。

從無法存取的閘道複製和使用磁碟區

1. 前往 https://console.aws.amazon.com/storagegateway/home 開啟 Storage Gateway 主控台。
2. 在 Storage Gateway 主控台上，選擇建立磁碟區。
3. 在 Create volume (建立磁碟區) 對話方塊中，針對 Gateway (閘道) 選擇閘道。
4. 針對 Capacity (容量)，輸入您磁碟區的容量。容量的大小必須至少與來源磁碟區相同。
5. 選擇 Clone from last recovery point (從上次復原點複製)，然後針對 Source volume (來源磁碟區) 選取磁碟區 ID。來源磁碟區可以是所選區域中的任何快取磁碟 AWS 區。
6. 針對 iSCSI target name (iSCSI 目標名稱)，輸入名稱。

   目標名稱可以包含小寫字母、數字、句號 (.) 和連字號 (-)。在探索之後，此目標名稱會顯示為 iSCSI Microsoft 啟動器 UI 之目標標籤中的 iSCSI 目標節點名稱。例如，`target1` 名稱會顯示為 `iqn.1007-05.com.amazon:target1`。請確定目標名稱在儲存區域網路 (SAN) 內為全域唯一的。
7. 確認 Network interface (網路界面) 設定是您閘道的 IP 地址，或針對 Network interface (網路界面) 選擇 IP 地址。

   如果您已定義閘道使用多個網路轉接器，則請選擇您儲存應用程式用來存取磁碟區的 IP 地址。針對閘道所定義的每個網路轉接器都代表您可以選擇的一個 IP 地址。

   如果為多個網路轉接器設定閘道 VM，則 Create volume (建立磁碟區) 對話方塊會顯示 Network interface (網路界面) 的清單。在此清單中，會針對閘道 VM 所設定的每個轉接器顯示一個 IP 地址。如果只針對一個網路轉接器設定閘道 VM，則不會顯示清單，因為只有一個 IP 地址。
8. 選擇建立磁碟區。Configure CHAP Authentication (設定 CHAP 身分驗證) 對話方塊隨即出現。您稍後可以設定 CHAP。如需相關資訊，請參閱 設定 iSCSI 目標的 CHAP 身分驗證。

下一個步驟是將磁碟區連線至用戶端。如需詳細資訊，請參閱將磁碟區連接到用戶端。

檢視磁碟區用量

當您將資料寫入磁碟區時，可以在 Storage Gateway 管理主控台中檢視存放在磁碟區上的資料量。每個磁碟區的 詳細資訊 標籤會顯示磁碟區用量資訊。

檢視寫入磁碟區的資料量

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 磁碟區，然後選擇您感興趣的磁碟區。
3. 選擇詳細資訊索引標籤。

   下列欄位提供磁碟區的相關資訊：

   - 大小：所選取磁碟區的總容量。
   - 已使用：磁碟區上所存放資料的大小。

   > **Note**
   >
   > 除非您將資料存放在 2015 年 5 月 13 日之前建立的磁碟區，否則這些值不適用於該磁碟區。

刪除儲存磁碟區

您可能需要在應用程式需求變更時刪除磁碟區，例如，如果您遷移應用程式以使用較大的儲存磁碟區。刪除磁碟區之前，請確定目前沒有應用程式寫入至磁碟區。此外，請確定磁碟區沒有進行中的快照。如果針對磁碟區定義快照排程，則您可以在 Storage Gateway 主控台的快照排程標籤上檢查它。如需詳細資訊，請參閱編輯快照排程。

您可以使用 Storage Gateway 主控台或 Storage Gateway API 刪除磁碟區。如需使用 Storage Gateway API 移除磁碟區的資訊，請參閱刪除磁碟區。下列程序示範如何使用主控台。

在您刪除磁碟區之前，請備份資料，或建立重要資料的快照。針對存放磁碟區，不會刪除您的本機磁碟。在您刪除磁碟區之後，就無法復原。

刪除磁碟區

1. 前往 https://console.aws.amazon.com/storagegateway/home 開啟 Storage Gateway 主控台。
2. 選擇磁碟區，然後選取一或多個要刪除的磁碟區。

3. 對於動作，請選擇刪除。出現確認對話方塊。
4. 確認您要刪除指定的磁碟區，然後在確認方塊中輸入刪除一詞，然後選擇刪除。

將您的磁碟區移至不同的閘道

隨著您的資料和效能需求成長，您可能想要將您的磁碟區移至不同的磁碟區閘道。方法是使用 Storage Gateway 主控台或 API 分離和連接磁碟區。

分離和連接磁碟區後，您可以執行下列操作：

- 將您的磁碟區移至更好的主機平台或更新的 Amazon EC2 執行個體。
- 重新整理您伺服器的底層硬體。
- 請在 Hypervisor 類型之間移動您的磁碟區。

分離磁碟區時，您的閘道會上傳並將磁碟區資料和中繼資料存放於 AWS中的 Storage Gateway 服務。您稍後可以將已分離磁碟區連接至任何支援之主機平台上的閘道。

> **Note**
>
> 已分離的磁碟區會以標準磁碟區儲存費率計費，直到您刪除此磁碟區為止。如需減少帳單費用的相關資訊，請參閱減少磁碟區上的計費儲存量。

> **Note**
>
> 磁碟區連接和分離有些限制：
>
> - 磁碟區分離相當耗時。當您分離磁碟區時，閘道會在分離磁碟區 AWS 之前，將磁碟區上的所有資料上傳至 。完成上傳的時間取決於需要上傳的資料量和您網路與 AWS的連線能力。
> - 如果您分離快取磁碟區，您無法將此磁碟區做為存放磁碟區重新連接。
> - 如果您分離存放磁碟區，您無法將此磁碟區做為快取磁碟區重新連接。
> - 已分離的磁碟區在連接至閘道前，都無法使用。
> - 當您連接存放磁碟區時，需要完全還原此磁碟區，才能再將此磁碟區連接至閘道。
> - 當您開始連接或分離磁碟區時，您需要等候至此操作完成，才能使用此磁碟區。
> - 目前僅支援在 API 中強制刪除磁碟區。

- 如果您在從該閘道分離您的磁碟區時刪除閘道，則會造成資料遺失。刪除閘道前，請等候磁碟區分離操作完成。
- 如果存放閘道處於還原狀態，您無法從該閘道分離磁碟區。

下列步驟說明您如何使用 Storage Gateway 主控台分離和連接磁碟區。有關使用 API 執行此操作的更多資訊，請參閱 AWS Storage Gateway API 參考中的 DetachVolume 或 AttachVolume。

從閘道分離磁碟區

1. 前往 https://console.aws.amazon.com/storagegateway/home 開啟 Storage Gateway 主控台。
2. 選擇磁碟區，選取一或多個要分離的磁碟區。
3. 針對 Actions (動作)，選擇 Detach volume (分離磁碟區)。出現確認對話方塊。
4. 確認您要分離指定的磁碟區，然後在確認方塊中輸入分離一詞，然後選擇分離。

> **Note**
>
> 如果您分離的磁碟區有許多資料，此磁碟區的狀態會從 Attached (已連接) 轉換成 Detaching (正在分離)，直到所有資料上傳完成為止。狀態稍後會變更為 Detached (已分離)。如果只有少量資料，您可能看不到 Detaching (正在卸離) 狀態。如果磁碟區上面沒有資料，狀態則會從 Attached (已連接) 變更為 Detached (已分離)。

您現在可以將磁碟區連接至不同的閘道。

將磁碟區連接至閘道

1. 前往 https://console.aws.amazon.com/storagegateway/home 開啟 Storage Gateway 主控台。
2. 在導覽窗格上，選擇 Volumes (磁碟區)。各個已分離的磁碟區會顯示 Detached (已分離) 的狀態。
3. 從已分離的磁碟區清單，選擇您要連接的磁碟區。您一次只能連接一個磁碟區。
4. 針對 Actions (動作)，Attach Volume (連接磁碟區)。
5. 在 Attach Volume (連接磁碟區) 對話方塊中，選擇您要連接磁碟區的閘道，然後輸入您要連接磁碟區的 iSCSI 目標。

   如果您正在連接存放磁碟區，請為 Disk ID (磁碟 ID) 輸入其磁碟識別符。
6. 選擇 Attach volume (連接磁碟區)。如果您附加的磁碟區上有大量資料，則在 `AttachVolume` 操作成功時，它會從已分離轉換為已連接。

7. 在出現的 Configure CHAP (設定 CHAP) 身分驗證精靈中，請輸入 Initiator name (啟動器名稱)、Initiator secret (啟動器秘密) 和 Target secret (目標秘密)，然後選擇 Save (儲存)。如需使用挑戰交握驗證協定 (Challenge-Handshake Authentication Protocol, CHAP) 身分驗證的詳細資訊，請參閱 設定 iSCSI 目標的 CHAP 身分驗證。

建立復原快照

下列程序說明如何從閘道的磁碟區復原點建立復原快照，以及在建立快照之後，可在 Storage Gateway 主控台中找到該快照的位置。您可以臨時擷取復原快照一次，也可以設定快照排程，以定期擷取您指定的磁碟區的重複快照。

從現有閘道建立並使用磁碟區的復原快照

1. 前往 https://console.aws.amazon.com/storagegateway/home 開啟 Storage Gateway 主控台。
2. 在主控台頁面左側的導覽窗格中，選擇閘道。
3. 選擇您要為其建立快照的閘道，然後選擇詳細資訊索引標籤。

   詳細資訊索引標籤會顯示所選閘道的復原快照訊息。
4. 選擇 Create recovery snapshot (建立復原快照) 以開啟 Create recovery snapshot (建立復原快照) 對話方塊。
5. 從顯示的磁碟區清單中，選擇您要復原的磁碟區，然後選擇建立快照。

   Storage Gateway 會啟動指定磁碟區的快照程序。當快照程序完成時，您可以在 Storage Gateway 主控台的磁碟區頁面上檢視磁碟區時，在快照欄中找到列出的快照。

編輯快照排程

對於儲存的磁碟區， AWS Storage Gateway 會建立預設快照排程，一天一次。

> **Note**
>
> 您無法移除預設快照排程。存放磁碟區需要至少一個快照排程。不過，您可以指定快照每天發生的時間或頻率 (每 1、2、4、8、12 或 24 小時) 或者兩者，來變更快照排程。

對於快取磁碟區， AWS Storage Gateway 不會建立預設快照排程。因為您的資料存放至 Amazon S3，所以不會建立預設排程，因此您不需要快照或快照排程即可進行災難復原。不過，需要時，您隨時可以設定快照排程。建立快取磁碟區的快照可提供額外的方式在需要時復原資料。

使用下列步驟，即可編輯磁碟區的快照排程。

編輯磁碟區的快照排程

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 Volumes (磁碟區)，然後選擇從中建立快照的磁碟區。
3. 在 Actions (動作) 選擇 Edit snapshot schedule (編輯快照排程)。
4. 在 Edit snapshot schedule (編輯快照排程) 對話方塊中，修改排程，然後選擇 Save (儲存)。

刪除儲存磁碟區的快照

您可以刪除儲存磁碟區的快照。例如，如果您已在一段時間後建立儲存磁碟區的多個快照，而且不需要較舊的快照，則建議您執行這項操作。因為快照是增量備份，所以如果您刪除快照，則只會刪除其他快照中不需要的資料。

主題

- 使用適用於 Java 的 AWS 開發套件刪除快照
- 使用適用於 .NET 的 AWS SDK 刪除快照
- 使用 刪除快照 AWS Tools for Windows PowerShell

在 Amazon EBS 主控台上，您一次可以刪除一個快照。如需如何使用 Amazon EBS 主控台刪除快照的資訊，請參閱《Amazon EC2 使用者指南》中的刪除 Amazon EBS 快照。

若要一次刪除多個快照，您可以使用其中一個支援 Storage Gateway 操作 AWS SDKs。如需範例，請參閱 使用適用於 Java 的 AWS 開發套件刪除快照、使用適用於 .NET 的 AWS SDK 刪除快照和使用 刪除快照 AWS Tools for Windows PowerShell。

使用適用於 Java 的 AWS 開發套件刪除快照

若要刪除與某個磁碟區建立關聯的多個快照，您可以使用程式設計方式。下列範例示範如何使用適用於 Java 的 AWS 軟體開發套件來刪除快照。若要使用範例程式碼，您應該熟悉如何執行 Java 主控台應用程式。如需詳細資訊，請參閱《適用於 Java 的AWS 軟體開發套件開發人員指南》中的入門。如果您只需要刪除一些快照，請使用主控台，如刪除儲存磁碟區的快照所述。

Example：使用適用於 Java 的 AWS 開發套件刪除快照

下列 Java 程式碼範例列出閘道之每個磁碟區的快照，以及快照開始時間早於還是晚於指定的日期。它使用適用於 Storage Gateway 和 Amazon EC2 的適用於 Java 的 AWS SDK API。Amazon EC2 API 包含使用快照的操作。

更新程式碼以提供服務端點、閘道 Amazon Resource Name (ARN)，以及您要儲存快照的天數。會刪除此截止時間之前所建立的快照。您也需要指定布林值 `viewOnly`，指出要檢視要刪除的快照，還是實際執行快照刪除。首先，僅使用檢視選項來執行程式碼 (即，將 `viewOnly` 設定為 `true`)，以查看程式碼所刪除的內容。如需可與 Storage Gateway 搭配使用 AWS 的服務端點清單，請參閱《AWS Storage Gateway 》中的端點和配額AWS 一般參考。

```
import java.io.IOException;
import java.util.ArrayList;
import java.util.Calendar;
import java.util.Collection;
import java.util.Date;
import java.util.GregorianCalendar;
import java.util.List;

import com.amazonaws.auth.PropertiesCredentials;
import com.amazonaws.services.ec2.AmazonEC2Client;
import com.amazonaws.services.ec2.model.DeleteSnapshotRequest;
import com.amazonaws.services.ec2.model.DescribeSnapshotsRequest;
import com.amazonaws.services.ec2.model.DescribeSnapshotsResult;
import com.amazonaws.services.ec2.model.Filter;
import com.amazonaws.services.ec2.model.Snapshot;
import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
import com.amazonaws.services.storagegateway.model.ListVolumesRequest;
import com.amazonaws.services.storagegateway.model.ListVolumesResult;
import com.amazonaws.services.storagegateway.model.VolumeInfo;

public class ListDeleteVolumeSnapshotsExample {

    public static AWSStorageGatewayClient sgClient;
    public static AmazonEC2Client ec2Client;
    static String serviceURLSG = "https://storagegateway.us-east-1.amazonaws.com";
    static String serviceURLEC2 = "https://ec2.us-east-1.amazonaws.com";

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

```
   // The number of days back you want to save snapshots. Snapshots before this cutoff
are deleted
   // if viewOnly = false.
   public static int daysBack = 10;

   // true = show what will be deleted; false = actually delete snapshots that meet
the daysBack criteria
   public static boolean viewOnly = true;

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

       // Create a Storage Gateway and amazon ec2 client
       sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(

ListDeleteVolumeSnapshotsExample.class.getResourceAsStream("AwsCredentials.properties")));

       sgClient.setEndpoint(serviceURLSG);

       ec2Client = new AmazonEC2Client(new PropertiesCredentials(

ListDeleteVolumeSnapshotsExample.class.getResourceAsStream("AwsCredentials.properties")));
       ec2Client.setEndpoint(serviceURLEC2);

       List<VolumeInfo> volumes = ListVolumesForGateway();
       DeleteSnapshotsForVolumes(volumes, daysBack);

   }
   public static List<VolumeInfo> ListVolumesForGateway()
   {
       List<VolumeInfo> volumes = new ArrayList<VolumeInfo>();

       String marker = null;
       do {
           ListVolumesRequest request = new
ListVolumesRequest().withGatewayARN(gatewayARN);
           ListVolumesResult result = sgClient.listVolumes(request);
           marker = result.getMarker();

           for (VolumeInfo vi : result.getVolumeInfos())
           {
               volumes.add(vi);
               System.out.println(OutputVolumeInfo(vi));
           }
       } while (marker != null);
```

```
        return volumes;
    }
    private static void DeleteSnapshotsForVolumes(List<VolumeInfo> volumes,
            int daysBack2) {

        // Find snapshots and delete for each volume
        for (VolumeInfo vi : volumes) {

            String volumeARN = vi.getVolumeARN();
            String volumeId =
volumeARN.substring(volumeARN.lastIndexOf("/")+1).toLowerCase();
            Collection<Filter> filters = new ArrayList<Filter>();
            Filter filter = new Filter().withName("volume-id").withValues(volumeId);
            filters.add(filter);

            DescribeSnapshotsRequest describeSnapshotsRequest =
                new DescribeSnapshotsRequest().withFilters(filters);
            DescribeSnapshotsResult describeSnapshotsResult =
                ec2Client.describeSnapshots(describeSnapshotsRequest);

            List<Snapshot> snapshots = describeSnapshotsResult.getSnapshots();
            System.out.println("volume-id = " + volumeId);
            for (Snapshot s : snapshots){
                StringBuilder sb = new StringBuilder();
                boolean meetsCriteria = !CompareDates(daysBack, s.getStartTime());
                sb.append(s.getSnapshotId() + ", " + s.getStartTime().toString());

                sb.append(", meets criteria for delete? " + meetsCriteria);
                sb.append(", deleted? ");
                if (!viewOnly & meetsCriteria) {
                    sb.append("yes");
                    DeleteSnapshotRequest deleteSnapshotRequest =
                        new DeleteSnapshotRequest().withSnapshotId(s.getSnapshotId());
                    ec2Client.deleteSnapshot(deleteSnapshotRequest);
                }
                else {
                    sb.append("no");
                }
                System.out.println(sb.toString());
            }
        }
    }
```

```
    private static String OutputVolumeInfo(VolumeInfo vi) {

        String volumeInfo = String.format(
                "Volume Info:\n" +
                "  ARN: %s\n" +
                "  Type: %s\n",
                vi.getVolumeARN(),
                vi.getVolumeType());
        return volumeInfo;
     }

    // Returns the date in two formats as a list
    public static boolean CompareDates(int daysBack, Date snapshotDate) {
        Date today = new Date();
        Calendar cal = new GregorianCalendar();
        cal.setTime(today);
        cal.add(Calendar.DAY_OF_MONTH, -daysBack);
        Date cutoffDate = cal.getTime();
        return (snapshotDate.compareTo(cutoffDate) > 0) ? true : false;
    }

}
```

使用適用於 .NET 的 AWS SDK 刪除快照

若要刪除與某個磁碟區建立關聯的多個快照，您可以使用程式設計方式。下列範例示範如何使用適用於 .NET 的 AWS 軟體開發套件第 2 版和第 3 版來刪除快照。若要使用範例程式碼，您應該熟悉如何執行 .NET 主控台應用程式。如需詳細資訊，請參閱《適用於 .NET 的AWS 軟體開發套件開發人員指南》中的入門。如果您只需要刪除一些快照，請使用主控台，如刪除儲存磁碟區的快照所述。

Example：使用適用於 .NET 的 AWS SDK 刪除快照

在下列 C# 程式碼範例中， AWS Identity and Access Management 使用者可以列出閘道每個磁碟區的快照。使用者接著可以判斷快照開始時間早於還是晚於指定的日期 (保留期)，以及刪除已過保留期的快照。此範例使用適用於 Storage Gateway 和 Amazon EC2 的 AWS .NET API 開發套件。Amazon EC2 API 包含使用快照的操作。

下列程式碼範例使用適用於 .NET 的 AWS SDK 第 2 版和第 3 版。您可以將較舊版本的 .NET 遷移至較新版本。如需詳細資訊，請參閱遷移適用於 .NET 的 AWS SDK 專案。

更新程式碼以提供服務端點、閘道 Amazon Resource Name (ARN)，以及您要儲存快照的天數。會刪除此截止時間之前所建立的快照。您也需要指定布林值 `viewOnly`，指出要檢視要刪除的快照，還

是實際執行快照刪除。首先，僅使用檢視選項來執行程式碼 (即，將 `viewOnly` 設定為 `true`)，以查看程式碼所刪除的內容。如需可與 Storage Gateway 搭配使用 AWS 的服務端點清單，請參閱《AWS Storage Gateway 》中的端點和配額AWS 一般參考。

首先，您建立使用者，並將最小 IAM 政策連接至使用者。然後，您排定閘道的自動化快照。

下列程式碼會建立允許使用者刪除快照的最小政策。在此範例中，政策命名為 **`sgw-delete-snapshot`**。

JSON

```
{
      "Version":"2012-10-17",
      "Statement": [
          {
              "Sid": "StmtEC2Snapshots",
              "Effect": "Allow",
              "Action": [
                  "ec2:DeleteSnapshot",
                  "ec2:DescribeSnapshots"
              ],
              "Resource": [
                  "*"
              ]
          },
          {
              "Sid": "StmtSgwListVolumes",
              "Effect": "Allow",
              "Action": [
                  "storagegateway:ListVolumes"
              ],
              "Resource": [
                  "*"
              ]
          }
      ]
  }
```

下列 C# 程式碼會找出指定閘道中符合磁碟區和指定截止期間的所有快照，然後予以刪除。

```
using System;
```

```
using System.Collections.Generic;
using System.Text;
using Amazon.EC2;
using Amazon.EC2.Model;
using Amazon.StorageGateway.Model;
using Amazon.StorageGateway;

namespace DeleteStorageGatewaySnapshotNS
{
    class Program
    {
        /*
         * Replace the variables below to match your environment.
         */

         /* IAM AccessKey */
        static String AwsAccessKey = "AKIA...............";

        /* IAM SecretKey */
        static String AwsSecretKey = "******************************";

        /* Account number, 12 digits, no hyphen */
        static String OwnerID = "123456789012";

        /* Your Gateway ARN. Use a Storage Gateway ID, sgw-XXXXXXXX* */
        static String GatewayARN = "arn:aws:storagegateway:ap-
southeast-2:123456789012:gateway/sgw-XXXXXXXX";

        /* Snapshot status: "completed", "pending", "error" */

        static String SnapshotStatus = "completed";

        /* Region where your gateway is activated */
        static String AwsRegion = "ap-southeast-2";

        /* Minimum age of snapshots before they are deleted (retention policy) */
        static int daysBack = 30;

        /*
         * Do not modify the four lines below.
         */
        static AmazonEC2Config ec2Config;
        static AmazonEC2Client ec2Client;
        static AmazonStorageGatewayClient sgClient;
```

```
        static AmazonStorageGatewayConfig sgConfig;

        static void Main(string[] args)
        {
            // Create an EC2 client.
            ec2Config = new AmazonEC2Config();
            ec2Config.ServiceURL = "https://ec2." + AwsRegion + ".amazonaws.com";
            ec2Client = new AmazonEC2Client(AwsAccessKey, AwsSecretKey, ec2Config);

            // Create a Storage Gateway client.
            sgConfig = new AmazonStorageGatewayConfig();
            sgConfig.ServiceURL = "https://storagegateway." + AwsRegion +
".amazonaws.com";
            sgClient = new AmazonStorageGatewayClient(AwsAccessKey, AwsSecretKey,
sgConfig);

            List<VolumeInfo> StorageGatewayVolumes = ListVolumesForGateway();
            List<Snapshot> StorageGatewaySnapshots =
ListSnapshotsForVolumes(StorageGatewayVolumes,
                                                    daysBack);
            DeleteSnapshots(StorageGatewaySnapshots);
        }

        /*
         * List all volumes for your gateway
         * returns: A list of VolumeInfos, or null.
         */
        private static List<VolumeInfo> ListVolumesForGateway()
        {
            ListVolumesResponse response = new ListVolumesResponse();
            try
            {
                ListVolumesRequest request = new ListVolumesRequest();
                request.GatewayARN = GatewayARN;
                response = sgClient.ListVolumes(request);

                foreach (VolumeInfo vi in response.VolumeInfos)
                {
                    Console.WriteLine(OutputVolumeInfo(vi));
                }
            }
            catch (AmazonStorageGatewayException ex)
            {
                Console.WriteLine(ex.Message);
```

```
            }
            return response.VolumeInfos;
        }

        /*
         * Gets the list of snapshots that match the requested volumes
         * and cutoff period.
         */
        private static List<Snapshot> ListSnapshotsForVolumes(List<VolumeInfo> volumes,
int snapshotAge)
        {
            List<Snapshot> SelectedSnapshots = new List<Snapshot>();
            try
            {
                foreach (VolumeInfo vi in volumes)
                {
                    String volumeARN = vi.VolumeARN;
                    String volumeID = volumeARN.Substring(volumeARN.LastIndexOf("/") +
1).ToLower();

                    DescribeSnapshotsRequest describeSnapshotsRequest = new
DescribeSnapshotsRequest();

                    Filter ownerFilter = new Filter();
                    List<String> ownerValues = new List<String>();
                    ownerValues.Add(OwnerID);
                    ownerFilter.Name = "owner-id";
                    ownerFilter.Values = ownerValues;
                    describeSnapshotsRequest.Filters.Add(ownerFilter);

                    Filter statusFilter = new Filter();
                    List<String> statusValues = new List<String>();
                    statusValues.Add(SnapshotStatus);
                    statusFilter.Name = "status";
                    statusFilter.Values = statusValues;
                    describeSnapshotsRequest.Filters.Add(statusFilter);

                    Filter volumeFilter = new Filter();
                    List<String> volumeValues = new List<String>();
                    volumeValues.Add(volumeID);
                    volumeFilter.Name = "volume-id";
                    volumeFilter.Values = volumeValues;
                    describeSnapshotsRequest.Filters.Add(volumeFilter);
```

```
                    DescribeSnapshotsResponse describeSnapshotsResponse =
                      ec2Client.DescribeSnapshots(describeSnapshotsRequest);

                    List<Snapshot> snapshots = describeSnapshotsResponse.Snapshots;
                    Console.WriteLine("volume-id = " + volumeID);
                    foreach (Snapshot s in snapshots)
                    {
                        if (IsSnapshotPastRetentionPeriod(snapshotAge, s.StartTime))
                        {
                            Console.WriteLine(s.SnapshotId + ", " + s.VolumeId + ",
                               " + s.StartTime + ", " + s.Description);
                            SelectedSnapshots.Add(s);
                        }
                    }
                }
            }
            catch (AmazonEC2Exception ex)
            {
                Console.WriteLine(ex.Message);
            }
            return SelectedSnapshots;
        }

        /*
         * Deletes a list of snapshots.
         */
        private static void DeleteSnapshots(List<Snapshot> snapshots)
        {
            try
            {
                foreach (Snapshot s in snapshots)
                {

                    DeleteSnapshotRequest deleteSnapshotRequest = new
DeleteSnapshotRequest(s.SnapshotId);
                    DeleteSnapshotResponse response =
ec2Client.DeleteSnapshot(deleteSnapshotRequest);
                    Console.WriteLine("Volume: " +
                              s.VolumeId +
                              " => Snapshot: " +
                              s.SnapshotId +
                              " Response: "
                              + response.HttpStatusCode.ToString());
                }
```

```
            }
            catch (AmazonEC2Exception ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /*
         * Checks if the snapshot creation date is past the retention period.
         */
        private static Boolean IsSnapshotPastRetentionPeriod(int daysBack, DateTime
 snapshotDate)
        {
            DateTime cutoffDate = DateTime.Now.Add(new TimeSpan(-daysBack, 0, 0, 0));
            return (DateTime.Compare(snapshotDate, cutoffDate) < 0) ? true : false;
        }

        /*
         * Displays information related to a volume.
         */
        private static String OutputVolumeInfo(VolumeInfo vi)
        {
            String volumeInfo = String.Format(
                "Volume Info:\n" +
                "  ARN: {0}\n" +
                "  Type: {1}\n",
                vi.VolumeARN,
                vi.VolumeType);
            return volumeInfo;
        }
    }
}
```

使用 刪除快照 AWS Tools for Windows PowerShell

若要刪除與某個磁碟區建立關聯的多個快照，您可以使用程式設計方式。下列範例示範如何使用 AWS Tools for Windows PowerShell來刪除快照。若要使用範例指令碼，您應該熟悉如何執行 PowerShell 指令碼。如需詳細資訊，請參閱《》中的AWS Tools for Windows PowerShell入門。如果您只需要刪除一些快照，請使用主控台，如刪除儲存磁碟區的快照所述。

Example：使用 刪除快照 AWS Tools for Windows PowerShell

下列 PowerShell 指令碼範例列出閘道之每個磁碟區的快照，以及快照開始時間早於還是晚於指定的日期。它使用適用於 Storage Gateway 和 Amazon EC2 的 AWS Tools for Windows PowerShell cmdlet。Amazon EC2 API 包含使用快照的操作。

您需要更新指令碼，並提供閘道 Amazon Resource Name (ARN) 和您要儲存快照的天數。會刪除此截止時間之前所建立的快照。您也需要指定布林值 `viewOnly`，指出要檢視要刪除的快照，還是實際執行快照刪除。首先，僅使用檢視選項來執行程式碼 (即，將 `viewOnly` 設定為 `true`)，以查看程式碼所刪除的內容。

```
<#
.DESCRIPTION
    Delete snapshots of a specified volume that match given criteria.

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

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

# Criteria to use to filter the results returned.
$daysBack = 18
$gatewayARN = "*** provide gateway ARN ***"
$viewOnly = $true;

#ListVolumes
$volumesResult = Get-SGVolume -GatewayARN $gatewayARN
$volumes = $volumesResult.VolumeInfos
Write-Output("`nVolume List")
foreach ($volumes in $volumesResult)
  { Write-Output("`nVolume Info:")
    Write-Output("ARN:  " + $volumes.VolumeARN)
    write-Output("Type: " + $volumes.VolumeType)
  }

Write-Output("`nWhich snapshots meet the criteria?")
foreach ($volume in $volumesResult)
```

```
  {
    $volumeARN = $volume.VolumeARN

    $volumeId = ($volumeARN-split"/")[3].ToLower()

    $filter = New-Object Amazon.EC2.Model.Filter
    $filter.Name = "volume-id"
    $filter.Value.Add($volumeId)

    $snapshots = get-EC2Snapshot -Filter $filter
    Write-Output("`nFor volume-id = " + $volumeId)
    foreach ($s in $snapshots)
    {
       $d = ([DateTime]::Now).AddDays(-$daysBack)
       $meetsCriteria = $false
       if ([DateTime]::Compare($d, $s.StartTime) -gt 0)
       {
            $meetsCriteria = $true
       }

       $sb = $s.SnapshotId + ", " + $s.StartTime + ", meets criteria for delete? " +
$meetsCriteria
       if (!$viewOnly -AND $meetsCriteria)
       {
           $resp = Remove-EC2Snapshot -SnapshotId $s.SnapshotId
           #Can get RequestId from response for troubleshooting.
           $sb = $sb + ", deleted? yes"
       }
       else {
           $sb = $sb + ", deleted? no"
       }
       Write-Output($sb)
    }
  }
```

了解磁碟區狀態和轉換

每個磁碟區都有一個相關聯的狀態，可讓您一眼得知磁碟區的運作狀態。大多數時間，該狀態指出磁碟區正常運作，而且您不需要採取任何動作。在某些情況下，該狀態指出的磁碟區問題，可能需要或可能不需要您採取動作。您可以找到下列資訊，協助您決定何時需要採取操作。您可以在 Storage Gateway 主控台或使用其中一個 Storage Gateway API 操作來查看磁碟區狀態，例如 DescribeCachediSCSIVolumes 或 DescribeStorediSCSIVolumes。

主題

- 了解磁碟區狀態
- 了解連接狀態
- 了解快取磁碟區狀態轉換
- 了解存放磁碟區狀態轉換

了解磁碟區狀態

下表顯示 Storage Gateway 主控台中的磁碟區狀態。您閘道中每個儲存磁碟區的磁碟區狀態都會出現在 Status (狀態) 欄。正常運作之磁碟區的狀態為 Available (可用)。

在下表中，您可以找到每個儲存磁碟區狀態的描述，而且是您應該根據每個狀態採取操作時。Available (可用) 狀態是磁碟區的正常狀態。磁碟區在使用中時，所有或大部分時間都應該具有此狀態。

狀態	意義
可用性	磁碟區可供使用。此狀態是磁碟區正常執行的狀態。 當 Bootstrapping (引導) 階段完成後，磁碟區會回復為 Available (可用) 狀態。也就是說，在磁碟區第一次進入 Pass Through (傳遞) 狀態後，閘道即已同步磁碟區所做的任何變更。
引導	閘道正在本機同步資料與存放於 中的資料副本 AWS。您通常不需要針對此狀態採取動作，因為儲存磁碟區在大部分情況下會自動查看 Available (可用) 狀態。 下列是磁碟區狀態為 Bootstrapping (引導) 的案例： • 閘道因非預期原因關閉。 • 閘道已超過上傳緩衝。在本案例中，當您的磁碟區狀態為 Pass Through (傳遞) 且增加足夠的免費上傳緩衝量時，引導即會出現。您可提供額外的上傳緩衝空間，做為提高免費上傳緩衝空間百分比的一個方式。在此特別的案例中，儲存磁碟區的狀態會從 Pass Through (傳遞) 變成 Bootstrapping (引導) 再到 Available (可用)。您可在此引導期間繼續使用此磁碟區。不過，此時無法拍攝磁碟區的快照。

狀態	意義
	• 您要建立存放磁碟區閘道，並保留現有的本機磁碟資料。在此案例中，您的閘道會開始上傳所有資料至 AWS。磁碟區具有引導狀態，直到本機磁碟中的所有資料都複製到其中為止 AWS。您在此引導期間可以使用磁碟區。不過，此時無法拍攝磁碟區的快照。
正在建立	目前正在建立磁碟區，尚無法使用。Creating (正在建立) 狀態是過渡的。無需採取任何動作。
正在刪除	目前正在刪除磁碟區。Deleting (正在刪除) 是過渡狀態。無需採取任何動作。
無法還原	磁碟區發生無法復原的錯誤。如需如何處理此狀況的資訊，請參閱對磁碟區問題進行疑難排解。

狀態	意義
傳遞	本機維護的資料與存放於 的資料不同步 AWS。寫入狀態為 Pass Through (傳遞) 之磁碟區的資料會留在快取中，直到磁碟區的狀態變成 Bootstrapping (引導)。當引導狀態開始時 AWS ，此資料會開始上傳至 。 發生 Pass Through (傳遞) 狀態的原因很多，如下所列： • 如果您的閘道已用盡上傳緩衝空間，即會出現 Pass Through (傳遞) 狀態。在磁碟區狀態為 Pass Through (傳遞) 時，您的應用程式仍可持續在您的儲存磁碟區讀寫資料。但是閘道不會將任何磁碟區資料寫入其上傳緩衝，也不會將此資料的任何內容上傳到 AWS。 閘道會在磁碟區進入 Pass Through (傳遞) 狀態之前，持續上傳已寫入磁碟區的所有資料。當磁碟區的狀態為 Pass Through (傳遞) 時，任何等待中或排程的儲存磁碟區快照都會失敗。如需如何處理儲存磁碟區因為超過上傳緩衝以致狀態成為 Pass Through (傳遞) 的資訊，請參閱對磁碟區問題進行疑難排解。 狀態為 Pass Through (傳遞) 的磁碟區必須完成 Bootstrapping (引導) 階段，才會回復為 ACTIVE (作用中) 狀態。在引導期間，磁碟區會在內重新建立同步 AWS，以便恢復磁碟區的變更記錄 （ 日誌 ），並啟用`CreateSnapshot` 功能。在 Bootstrapping (引導) 期間，磁碟區寫入作業會記錄在上傳緩衝中。 • 一次出現多個儲存磁碟區引導時，會發生 Pass Through (傳遞) 狀態。一次只能引導一個閘道儲存磁碟區。例如，假設您建立兩個儲存磁碟區，然後選擇使用它們兩個來留存現有的資料。在這種狀況下，第二個儲存磁碟區的狀態會保持 Pass Through (傳遞)，直到第一個儲存磁碟區完成引導。在此案例中，您不需要採取任何操作。每個儲存磁碟區建立完成後，都會自動變成 Available (可用) 狀態。您可以讀寫儲存狀態為 Pass Through (傳遞) 或 Bootstrapping (引導) 的磁碟區。 • Pass Through (傳遞) 狀態不常指示用於上傳緩衝的配置磁碟已失敗。如需本案例應採取動作的資訊，請參閱對磁碟區問題進行疑難排解。 •

狀態	意義
	當磁碟區狀態為作用中或引導時，就會出現傳遞狀態。在這種情況下，磁碟區會收到寫入，但上傳緩衝容量不足，無法記錄該寫入 (日誌)。 • 當磁碟區處於任何狀態，且閘道未徹底關閉時，就會出現 Pass Through (傳遞) 狀態。這類的關機是因為軟體損毀或 VM 關機而發生。在這種情況下，任何狀態的磁碟區都會轉換到 Pass Through (傳遞) 狀態。
Restoring (正在還原)	正從現有的快照還原磁碟區。此狀態只適用於存放磁碟區。如需詳細資訊，請參閱磁碟區閘道的運作方式。 如果您要同時還原兩個儲存磁碟區，這兩個儲存磁碟區的狀態會顯示為 Restoring (正在還原)。每個儲存磁碟區建立完成後，都會自動變成 Available (可用) 狀態。當磁碟區狀態為 Restoring (正在還原) 時，您可以讀寫儲存磁碟區並拍攝其快照。
還原傳遞	正從現有的快照還原磁碟區，發生上傳緩衝問題。此狀態只適用於存放磁碟區。如需詳細資訊，請參閱磁碟區閘道的運作方式。 如果您的閘道已用盡上傳緩衝空間，這也是造成 Restoring Pass Through (正在還原傳遞) 狀態的原因之一。在磁碟區狀態為 Restoring Pass Through (正在還原傳遞) 時，您的應用程式仍可持續在您的儲存磁碟區讀寫資料。不過，在狀態為 Restoring Pass Through (正在還原傳遞) 期間，您無法拍攝儲存磁碟區的快照。如需如何處理儲存磁碟區因為超過上傳緩衝容量以致狀態成為 Restoring Pass Through (正在還原傳遞) 的資訊，請參閱對磁碟區問題進行疑難排解。 Restoring Pass Through (正在還原傳遞) 狀態不常指示上傳緩衝的配置磁碟已失敗。如需本案例應採取動作的資訊，請參閱對磁碟區問題進行疑難排解。
Upload Buffer Not Configured (未設定上傳緩衝)	您無法建立或使用磁碟區，因為閘道未設定上傳緩衝。如需如何在快取磁碟區設定中為磁碟區新增上傳緩衝容量的資訊，請參閱判斷要配置的上傳緩衝大小。如需如何在存放磁碟區設定中為磁碟區新增上傳緩衝容量的資訊，請參閱判斷要配置的上傳緩衝大小。

了解連接狀態

您可以使用 Storage Gateway 主控台或 API，從閘道分離磁碟區，或連接磁碟區至閘道。下表顯示 Storage Gateway 主控台中的磁碟區連接狀態。您閘道中每個儲存磁碟區的磁碟區連接狀態都會出現在 Attachment status (連接狀態) 欄。例如，從閘道分離的磁碟區會有 Detached (已分離) 的狀態。如需如何分離和連接磁碟區的資訊，請參閱將您的磁碟區移至不同的閘道。

狀態	意義
Attached	磁碟區已連接至閘道。
Detached	磁碟區已從閘道分離。
正在卸離	磁碟區正在從閘道分離。您正在分離磁碟區，且磁碟區其中無資料時，您可能看不見此狀態。

了解快取磁碟區狀態轉換

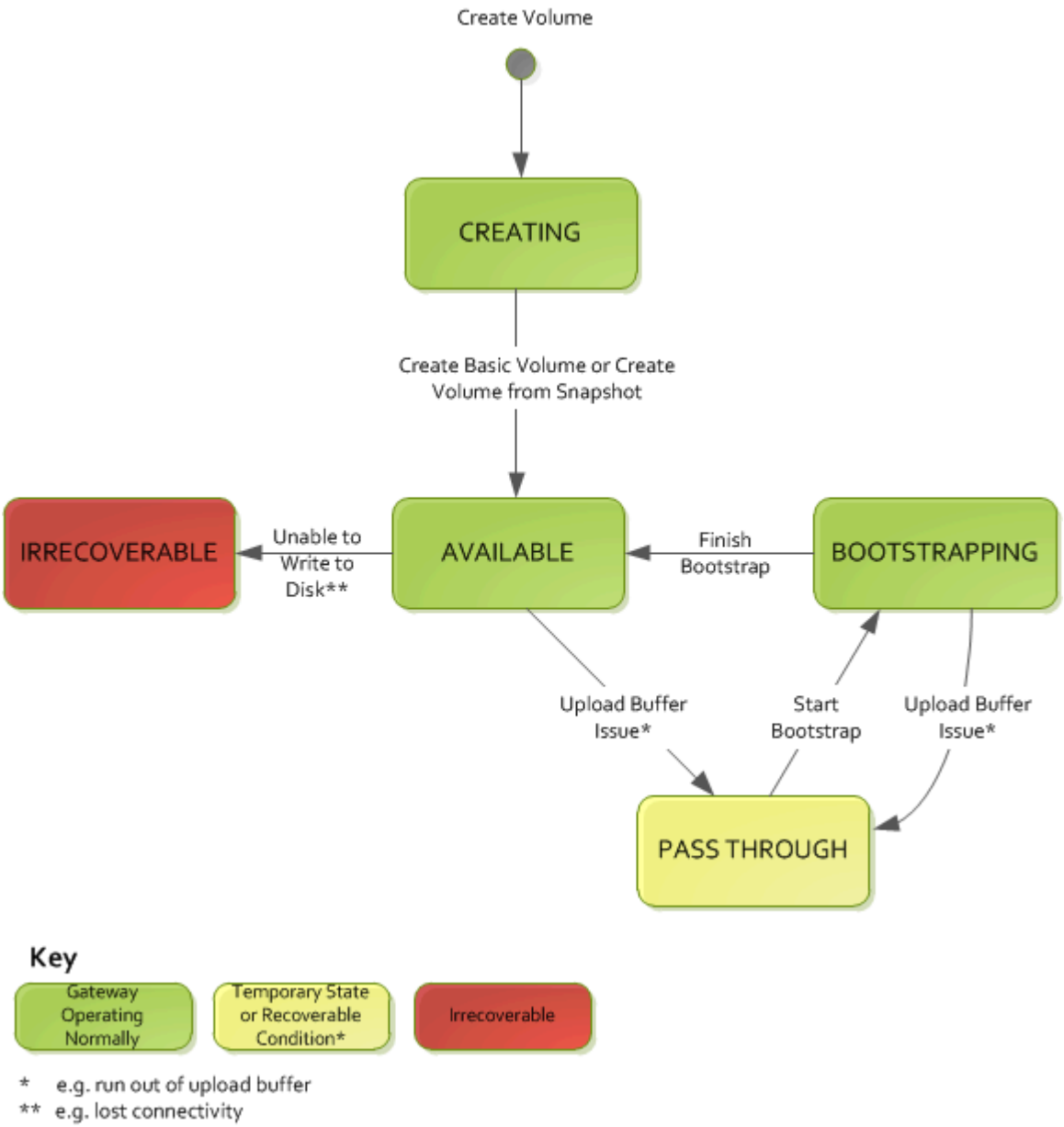
使用下列狀態圖，了解快取閘道之磁碟區最常見的狀態轉換。您不需要詳細了解此圖，也能有效使用閘道。而是，如果您有興趣了解更多磁碟區閘道的運作方式，此圖可提供詳細資訊。

此圖不顯示 Upload Buffer Not Configured (未設定上傳緩衝) 狀態或 Deleting (正在刪除) 狀態。圖中的磁碟區狀態會顯示為綠色、黃色和紅色方塊。您可以如下所述解釋這些顏色。

顏色	磁碟區狀態
綠色	此閘道運作正常。磁碟區狀態為 Available (可用) 或最終成為 Available (可用)。
黃色	磁碟區狀態為 Pass Through (傳遞) 時，表示儲存磁碟區可能有問題。如果此狀態是因為上傳緩衝空間已滿而出現，則在某些情況下，緩衝空間可再次使用。此時，儲存磁碟區會自我修正到 Available (可用) 狀態。在其他情況下，您可能必須在閘道新增更多的上傳緩衝空間，讓儲存磁碟區狀態變成 Available (可用)。如需如何故障診斷超過上傳緩衝容量狀況的資訊，請參閱對磁碟區問題進行疑難排

顏色	磁碟區狀態
	解。如需如何新增上傳緩衝容量的資訊，請參閱判斷要配置的上傳緩衝大小。
紅色	儲存磁碟區的狀態為 Irrecoverable (無法還原)。在這種情況下，您應該刪除磁碟區。如需如何執行此作業的資訊，請參閱 刪除磁碟區。

在本圖中，兩個狀態間的轉換以標籤線繪製。例如，從 Creating (正在建立) 狀態轉換到 Available (可用) 狀態會標籤為 Create Basic Volume or Create Volume from Snapshot (建立基本磁碟區或從快照建立磁碟區)。此轉換代表正在建立快取磁碟區。如需建立儲存磁碟區的詳細資訊，請參閱新增和擴展磁碟區。



> **Note**
>
> 磁碟區狀態為 Pass Through (傳遞) 在圖中顯示為黃色。但這不符合 Storage Gateway 主控台之狀態方塊中的狀態圖示顏色。

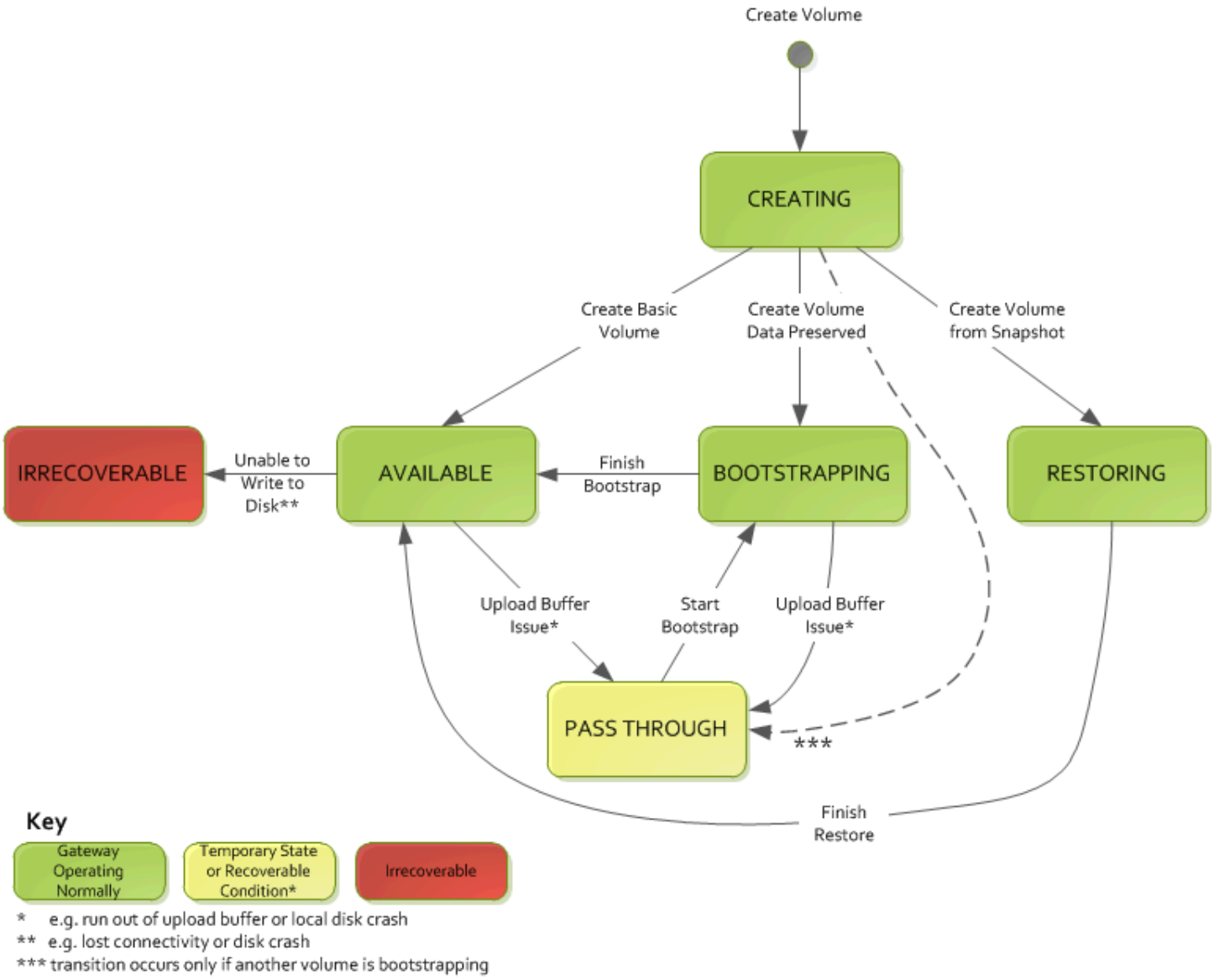
了解存放磁碟區狀態轉換

使用下列的狀態圖，了解存放閘道之磁碟區最常見的狀態轉換。您不需要詳細了解此圖，也能有效使用閘道。而是，如果您有興趣了解更多磁碟區閘道的運作方式，此圖可提供詳細資訊。

此圖不顯示 Upload Buffer Not Configured (未設定上傳緩衝) 狀態或 Deleting (正在刪除) 狀態。圖中的磁碟區狀態會顯示為綠色、黃色和紅色方塊。您可以如下所述解釋這些顏色。

顏色	磁碟區狀態
綠色	此閘道運作正常。磁碟區狀態為 Available (可用) 或最終成為 Available (可用)。
黃色	當您要建立儲存磁碟區並保留資料時，如果另一個磁碟區正在引導，路徑就會從 Creating (正在建立) 狀態通往 Pass Through (傳遞) 狀態。在本例中，狀態為 Pass Through (傳遞) 的磁碟區變成 Bootstrapping (引導) 狀態，然後在第一個磁碟區完成引導後變成 Available (可用) 狀態。除特定案例所提及者外，黃色 (Pass Through (傳遞) 狀態) 指出儲存磁碟區可能有問題，最常見的是上傳緩衝問題。如果超過上傳緩衝容量，則在某些情況下緩衝空間可再次使用。此時，儲存磁碟區會自我修正到 Available (可用) 狀態。在其他情況下，您可能必須在閘道新增更多的上傳緩衝容量，讓儲存磁碟區狀態回復成 Available (可用)。如需如何故障診斷超過上傳緩衝容量狀況的資訊，請參閱對磁碟區問題進行疑難排解。如需如何新增上傳緩衝容量的資訊，請參閱判斷要配置的上傳緩衝大小。
紅色	儲存磁碟區的狀態為 Irrecoverable (無法還原)。在這種情況下，您應該刪除磁碟區。如需如何執行此作業的資訊，請參閱 刪除儲存磁碟區。

在下圖中，兩個狀態間的轉換以標籤線繪製。例如，從 Creating (正在建立) 狀態轉換到 Available (可用) 狀態會標籤為 Create Basic Volume (建立基本磁碟區)。此轉換代表建立儲存磁碟區，而不保留資料或從快照建立磁碟區。



> **Note**
>
> 磁碟區狀態為 Pass Through (傳遞) 在圖中顯示為黃色。但這不符合 Storage Gateway 主控台之狀態方塊中的狀態圖示顏色。

將資料移至新的閘道執行個體

> **Note**
>
> 如果您正在執行 Storage Gateway AL2 到 AL2023 遷移，在開始之前，請確定您已完成 Storage Gateway AL2 到 AL2023 遷移行銷活動 中遷移前檢查清單中的所有項目。

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

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

> **Important**
>
> 資料只能在相同的閘道類型之間移動。
> 下列遷移說明僅適用於執行 2.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。

遷移程序會根據您使用的儲存磁碟區或快取磁碟區而有所不同。這兩種閘道類型需要不同的遷移步驟。選擇符合您閘道類型的程序：

主題

- 將儲存的磁碟區移至新的儲存磁碟區閘道
- 將快取磁碟區移至新的閘道虛擬機器

將儲存的磁碟區移至新的儲存磁碟區閘道

將儲存的磁碟區移至新的儲存磁碟區閘道

1. 停止任何寫入舊儲存的磁碟區閘道的應用程式。
2. 使用下列步驟來建立磁碟區的快照，然後等待快照完成。

a. 前往 https://console.aws.amazon.com/storagegateway/home 開啟 Storage Gateway 主控台。
b. 在導覽窗格中，選擇磁碟區，然後選擇您要從中建立快照的磁碟區。
c. 針對 Actions (動作)，選擇 Create snapshot (建立快照)。
d. 在建立快照對話方塊中，輸入快照描述，然後選擇建立快照。

   您可以確認快照是使用主控台所建立。如果資料仍在上傳至磁碟區，請等待上傳完成後，即可前往下一個步驟。若要查看快照狀態並驗證沒有快照處於擱置中，請選取磁碟區上的快照連結。

3. 請使用下列步驟停止舊儲存的磁碟區閘道：

   a. 在導覽窗格中，選擇閘道，然後選擇您要停止的舊儲存的磁碟區閘道。閘道的狀態為 Running (正在執行)。
   b. 對於動作，選擇停止閘道。從對話方塊確認閘道 ID，然後選擇停止閘道。

      閘道停止時，您可能會看到訊息，指出閘道的狀態。閘道關閉時，訊息和啟動閘道按鈕會出現在詳細資訊標籤中。閘道關閉時，閘道的狀態為關閉。
   c. 使用 Hypervisor 主控台關閉 VM。

   如需如何關閉閘道的詳細資訊，請參閱 啟動和停止磁碟區閘道。
4. 將與儲存磁碟區關聯的儲存磁碟從閘道 VM 中分離。這會排除 VM 的根磁碟。
5. 使用可從 Storage Gateway 主控台 (https://console.aws.amazon.com/storagegateway/home) 取得的新 Hypervisor VM 映像，啟動新儲存的磁碟區閘道。
6. 連接在步驟 5 中您從舊儲存的磁碟區閘道 VM 中分離的實體儲存磁碟。
7. 若要保留磁碟上的現有資料，請使用下列步驟建立儲存的磁碟區。

   a. 在 Storage Gateway 主控台上，選擇建立磁碟區。
   b. 在建立磁碟區對話方塊中，選取您在步驟 5 中建立的儲存的磁碟區閘道。
   c. 從清單中選擇磁碟 ID 值。
   d. 針對磁碟區內容，選取保留磁碟上現有的資料選項。

   如需建立磁碟區的詳細資訊，請參閱 建立儲存磁碟區。
8. (選用) 在出現的設定 CHAP 身分驗證精靈中，請輸入啟動器名稱、啟動器秘密和目標秘密，然後選擇儲存。

如需使用挑戰交握驗證協定 (Challenge-Handshake Authentication Protocol, CHAP) 身分驗證的詳細資訊，請參閱 設定 iSCSI 目標的 CHAP 身分驗證。

9. 啟動寫入儲存的磁碟區的應用程式。
10. 確認新儲存的磁碟區閘道正常運作後，您可以刪除舊儲存的磁碟區閘道。

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

請使用下列步驟來刪除舊儲存的磁碟區閘道：

> **Warning**
>
> 閘道一旦刪除，就無法還原。

a. 在導覽窗格中，選擇閘道，然後選擇您要刪除的舊儲存的磁碟區閘道。
b. 針對 Actions (動作)，選擇 Delete gateway (刪除閘道)。
c. 在出現的確認對話方塊中，選取核取方塊以確認刪除。請確定列出的閘道 ID 指定您要刪除的舊儲存的磁碟區閘道，然後選擇刪除。

11. 刪除舊的閘道 VM。如需刪除 VM 的資訊，請參閱 Hypervisor 文件。

將快取磁碟區移至新的閘道虛擬機器

要將快取磁碟區移至新的快取磁碟區閘道虛擬機器 (VM)

1. 停止任何寫入舊快取磁碟區閘道的應用程式。
2. 使用下列步驟將閘道更新至最新版本

a. 前往 https://console.aws.amazon.com/storagegateway/home 開啟 Storage Gateway 主控台。
b. 在導覽窗格中，選擇閘道，然後選擇您要遷移的舊快取磁碟區閘道。
c. 如果可用，請按一下立即更新。如果沒有，表示您的閘道已在最新版本上。

3. 確認現有快取閘道的監控索引標籤上的CachePercentDirty指標為 0。
4. 從任何使用 iSCSI 磁碟區的用戶端卸載或中斷連線。如此可防止用戶端變更或新增資料至這些磁碟區，以協助保持這些磁碟區上的資料一致。
5. 使用下列步驟來建立磁碟區的快照，然後等待快照完成。

   a. 前往 https://console.aws.amazon.com/storagegateway/home 開啟 Storage Gateway 主控台。

   b. 在導覽窗格中，選擇磁碟區，然後選擇您要從中建立快照的磁碟區。

   c. 針對動作，選擇建立 EBS 快照。

   d. 在建立快照對話方塊中，輸入快照描述，然後選擇建立快照。

      您可以確認快照是使用主控台所建立。如果資料仍在上傳至磁碟區，請等待上傳完成後，即可前往下一個步驟。若要查看快照狀態並驗證沒有快照處於擱置中，請選取磁碟區上的快照連結。

      如需有關在主控台中檢查磁碟區狀態的詳細資訊，請參閱 了解磁碟區狀態和轉換。如需快取磁碟區狀態的資訊，請參閱 了解快取磁碟區狀態轉換。
6. 請使用下列步驟停止舊快取磁碟區閘道：

   a. 在導覽窗格中，選擇閘道，然後選擇您要停止的舊快取磁碟區閘道。

   b. 對於動作，選擇停止閘道。從對話方塊確認閘道 ID，然後選擇停止閘道。記下閘道 ID，因為需要在稍後的步驟中使用。

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

   c. 使用 Hypervisor 主控台關閉舊 VM。如需關閉 Amazon EC2 執行個體的詳細資訊，請參閱《Amazon EC2 使用者指南》中的停止和啟動執行個體。如需關閉 KVM、VMware 或 Hyper-V 虛擬機器的詳細資訊，請參閱您的 Hypervisor 文件。

   如需如何關閉閘道的詳細資訊，請參閱 啟動和停止磁碟區閘道。
7. 從舊閘道虛擬機器中分離所有磁碟，包括根磁碟、快取磁碟和上傳緩衝磁碟。

> **Note**
>
> 記下根磁碟的磁碟區 ID，以及與該根磁碟相關聯的閘道 ID。您可以在後續步驟中使用此磁碟。

如果您使用 Amazon EC2 執行個體做為快取磁碟區閘道的 VM，請參閱《Amazon EC2 使用者指南》中的從 Linux 執行個體分離 Amazon EBS 磁碟區。 Amazon EC2 如需有關從 KVM、VMware 或 Hyper-V VM 分離磁碟的詳細資訊，請參閱您的 Hypervisor 文件。

8. 建立新的 Storage Gateway Hypervisor VM 執行個體，但不要將其啟用為閘道。如需有關建立新 Storage Gateway Hypervisor VM 的詳細資訊，請參閱 設定磁碟區閘道。這個新閘道將採用舊閘道的身分識別。

   > **Note**
   >
   > 請勿向新 VM 中新增快取或上傳緩衝磁碟。您的新 VM 將使用舊 VM 使用的相同快取磁碟和上傳緩衝磁碟。

9. 新的 Storage Gateway Hypervisor VM 執行個體應使用與舊 VM 相同的網路組態。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。

   如果您需要手動設定新 VM 的靜態 IP 地址，請參閱 設定您的閘道網路 以取得更多詳細資訊。如果您的閘道必須使用 Socket Secure 第 5 版 (SOCKS5) 代理連線到網際網路，請參閱 為您的內部部署閘道設定 SOCKS5 代理 以取得更多詳細資訊。

10. 啟動新的 VM。

11. 將您在步驟 7 中從舊快取磁碟區閘道 VM 分離的磁碟連接到新的快取磁碟區閘道。按照與舊閘道 VM 上相同的順序將它們連結至新閘道虛 VM。

    所有磁碟都必須使轉換不變。請勿變更磁碟區大小，因為這會導致中繼資料變得不一致。

12. 透過連線至新閘道 VM 的本機主控台，或向新閘道 VM 的 IP 地址提出 Web 請求 （ 如下所述 ） 來啟動閘道遷移程序。

    a. 若要使用本機主控台，請選取 Migrate Gateway 的選項，並在出現提示時提供現有的閘道 ID。系統會提示您將先前在舊閘道上套用的設定複製到新閘道。您可以選擇套用它們，或稍後手動設定它們。請參閱存取閘道本機主控台。

    b. 或者，您可以使用下列格式的 URL 連接到新的 VM，以啟動閘道遷移程序。

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

    您可以為新閘道 VM 重複使用與舊閘道 VM 所用相同的 IP 地址。您的 URL 看起來應該如下列範例：

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

從瀏覽器或從使用 `curl` 的命令列使用此 URL 來啟動移轉程序。

當閘道遷移程序成功完成時，您會看到確認成功遷移的訊息。

13. 分離舊閘道的根磁碟，您在步驟 7 中記下其磁碟區 ID。
14. 啟動閘道。

    請使用下列步驟來啟動新快取磁碟區閘道：

    a. 前往 https://console.aws.amazon.com/storagegateway/home 開啟 Storage Gateway 主控台。
    b. 在導覽窗格中，選擇閘道，然後選擇要啟動的新閘道。閘道的狀態為 Shutdown (關機)。
    c. 選擇詳細資訊，然後選擇啟動閘道。

    如需啟動閘道的詳細資訊，請參閱 啟動和停止磁碟區閘道。
15. 您的磁碟區現在應可透過新的閘道 VM 網路界面供應用程式使用。遷移成功訊息包含每個磁碟區與新閘道網路介面之間更新映射的詳細資訊。如需與每個網路介面相關聯之 IP 地址的詳細資訊，請造訪閘道本機主控台的主頁面。請參閱存取閘道本機主控台。
16. 確認您的磁碟區可用，並刪除舊閘道 VM。如需刪除 VM 的資訊，請參閱 Hypervisor 文件。

監控 Storage Gateway

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

Storage Gateway 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，並更加了解閘道和磁碟區的執行狀況。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。

如需監控磁碟區閘道及其相關資源的特定資訊，請參閱監控磁碟區閘道。

主題

- 了解閘道指標
- 監控上傳緩衝區
- 監控快取儲存
- 了解 CloudWatch 警示
- 建立閘道的 CloudWatch 警示
- 為您的閘道建立自訂 CloudWatch 警示
- 監控您的磁碟區閘道

了解閘道指標

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

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

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

指標	Description
AvailabilityNotifications	閘道產生的可用相關運作狀態通知數目。 使用此指標搭配 Sum 統計資料，即可觀察閘道是否發生任何可用性相關事件。如需事件的詳細資訊，請查看您設定的 CloudWatch 日誌群組。 單位：數字
CacheHitPercent	從快取服務的應用程式讀取百分比。報告期間結束時會取樣。 單位：百分比
CachePercentDirty	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。 使用此指標搭配 Sum 統計資料。 理想情況下，此指標應保持低。 單位：百分比
CacheUsed	閘道快取儲存體中已使用的位元組總數。報告期間結束時會取樣。

指標	Description
	單位：位元組
IoWaitPercent	閘道等候本機磁碟回應的時間百分比。 單位：百分比
MemTotalBytes	佈建至閘道 VM 的 RAM 數量，以位元組為單位。 單位：位元組
MemUsedBytes	閘道 VM 目前使用中的 RAM 數量，以位元組為單位。 單位：位元組
QueuedWrites	一般而言，此值代表等待寫入的本機儲存位元組數目 AWS，但也會反映本機資料和雲端資料在「引導」期間發生的同步程序，每次閘道重新啟動時都會發生。 單位：位元組
ReadBytes	報告期間針對閘道中的所有磁碟區，從您的內部部署應用程式讀取的位元組總數。 使用此指標搭配 Sum 統計資料可測量輸送量，搭配 Samples 統計資料可測量 IOPS。 單位：位元組

指標	Description
ReadTime	報告期間針對閘道中的所有磁碟區，從您的內部部署應用程式執行讀取操作所花費的總毫秒數。 使用此指標搭配 Average 統計資料可測量延遲。 單位：毫秒
TimeSinceLastRecoveryPoint	距上一個可用復原點的時間。如需詳細資訊，請參閱您的快取閘道無法連接，而您想要復原資料。 單位：秒
TotalCacheSize	快取大小總計 (位元組)。報告期間結束時會取樣。 單位：位元組
UploadBufferPercentUsed	閘道上傳緩衝區的使用百分比。報告期間結束時會取樣。 單位：百分比
UploadBufferUsed	閘道上傳緩衝區中已使用的位元組總數。報告期間結束時會取樣。 單位：位元組
UserCpuPercent	閘道處理所花費的 CPU 時間百分比，此為所有核心的平均值。 單位：百分比

指標	Description
WorkingStorageFree	閘道工作儲存體中未使用的總空間量。報告期間結束時會取樣。 單位：位元組
WorkingStoragePercentUsed	閘道上傳緩衝區的使用百分比。報告期間結束時會取樣。 單位：百分比
WorkingStorageUsed	閘道上傳緩衝區中已使用的位元組總數。報告期間結束時會取樣。 單位：位元組
WriteBytes	報告期間針對閘道中的所有磁碟區，寫入至您內部部署應用程式的位元組總數。 使用此指標搭配 Sum 統計資料可測量輸送量，搭配 Samples 統計資料可測量 IOPS。 單位：位元組
WriteTime	報告期間針對閘道中的所有磁碟區，從您的內部部署應用程式執行寫入操作所花費的總毫秒數。 使用此指標搭配 Average 統計資料可測量延遲。 單位：毫秒

Storage Gateway 指標的維度

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

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

監控上傳緩衝區

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

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

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

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

測量已使用的上傳緩衝區百分比

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

其結果之依照時間排序的資料點集合包含上傳緩衝區使用百分比。

使用下列程序，即可使用 CloudWatch 主控台建立警示。如需有關警示和閾值的詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的建立 Amazon CloudWatch 警示。

設定閘道上傳緩衝區的閾值警示上限

1. 透過 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 選擇 Create Alarm (建立警示) 以啟動 [Create Alarm] (建立警示) 精靈。
3. 指定警示的指標：
   a. 在「建立警示」精靈的選取指標頁面上，選擇 AWS/StorageGateway:GatewayId，GatewayName 維度，然後找到您要使用的閘道。
   b. 選擇 UploadBufferPercentUsed 指標。使用 Average 統計資料和 5 分鐘的期間。
   c. 選擇繼續。
4. 定義警示名稱、描述和閾值：

a. 在 [Create Alarm] (建立警示) 精靈的 Define Alarm (定義警示) 頁面上，透過在 Name (名稱) 和 Description (描述) 方塊中提供警示的名稱和描述來識別警示。

b. 定義警示閾值。

c. 選擇繼續。

5. 設定警示的電子郵件動作：

a. 在建立警示精靈的設定動作頁面中，針對警示狀態選擇警示。

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

建立電子郵件主題，表示您設定 Amazon SNS 主題。如需詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的設定 Amazon SNS 通知。

c. 針對 Topic (主題)，輸入主題的描述性名稱。

d. 選擇 Add Action (新增動作)。

e. 選擇繼續。

6. 檢閱警示設定，然後建立警示：

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

b. 在檢閱警示摘要之後，請選擇 Save Alarm (儲存警示)。

7. 確認警示主題的訂閱：

a. 開啟 Amazon SNS 已傳送至您在建立主題時所指定之電子郵件地址的電子郵件。

b. 按一下電子郵件中的連結，以確認訂閱。

訂閱確認隨即出現。

監控快取儲存

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

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

感興趣的項目	測量方式
總快取用量	搭配使用 CachePercentUsed 和 TotalCacheSize 指標與 Average 統計資料。例如，搭配使用 CachePercentUsed 與 Average 統計資料，以分析一段時間的快取用量。 只有在您將快取新增至閘道時，TotalCacheSize 指標才會變更。
由快取提供服務的讀取請求百分比	搭配 CacheHitPercent 統計資料使用 Average 指標。 一般而言，您想要將 CacheHitPercent 保留為高。
骯髒的快取百分比 - 也就是說，它包含尚未上傳至 的內容 AWS	搭配使用 CachePercentDirty 指標與 Average 統計資料。 一般而言，您想要將 CachePercentDirty 保留為低。

測量閘道及其所有磁碟區的快取已變更百分比

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

其結果之依照時間排序的資料點集合包含超過 5 分鐘的快取已變更百分比。

測量磁碟區的快取已變更百分比

1. 透過 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 選擇 StorageGateway: Volume Metrics (StorageGateway：磁碟區指標) 維度，然後尋找您希望使用的磁碟區。
3. 選擇 CachePercentDirty 指標。
4. 針對 Time Range (時間範圍)，選擇一個值。

5. 選擇 Average 統計資料。
6. 針對 Period (期間)，選擇 5 分鐘的值以符合預設報告時間。

其結果之依照時間排序的資料點集合包含超過 5 分鐘的快取已變更百分比。

了解 CloudWatch 警示

CloudWatch 警示會根據指標和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。如需用來監督磁碟區閘道之測量結果的相關資訊，請參閱了解閘道指標和了解磁碟區指標。對於每個警示，您可以指定將啟動其 ALARM 狀態的條件。Storage Gateway 主控台中的警示狀態指示燈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` >= 20，15 分鐘內 3 個資料點
- 快取變更百分比：`CachePercentDirty` > 80，20 分鐘內 4 個資料點
- 健康狀況通知：`HealthNotifications` >= 1，5 分鐘內 1 個資料點。設定此警示時，請將遺失資料處理設定為 notBreaching。

> **Note**
>
> 只有在閘道在 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。

對於已啟動 HA 模式的 VMware 主機平台上的閘道，我們也建議您使用下列額外的 CloudWatch 警示：

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

下表說明警示的狀態。

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

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，請參閱設定磁碟區閘道。如果您要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. 在導覽窗格中，選擇閘道，然後選擇您要建立 CloudWatch 警示的閘道。
3. 在閘道詳細資訊頁面上，選擇監控標籤。
4. 在警示下，選擇建議的警示。建議的警示會自動建立。

   警示區段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？

為 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。當指標超過閾值達到指定的評估期間數，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。

監控您的磁碟區閘道

本節中的主題說明如何在快取磁碟區或儲存磁碟區設定中監控磁碟區閘道，包括監控與閘道相關聯的磁碟區和監控上傳緩衝區。您可以使用 AWS 管理主控台 來檢視閘道的指標。例如，您可以檢視用於讀取和寫入操作的位元組數目、讀取和寫入操作所花的時間，以及從 Amazon Web Services 雲端擷取資料所花的時間。使用指標，您可以追蹤閘道的運作狀態，並設定警示，在一或多個指標落在定義閾值以外時通知您。

Storage Gateway 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，並更加了解閘道和磁碟區的執行狀況。如需有關 CloudWatch 的詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

主題

- 使用 Amazon CloudWatch Logs 取得磁碟區閘道運作狀態日誌 - 了解如何使用 Amazon CloudWatch Logs 取得磁碟區閘道和相關資源運作狀態的相關資訊。
- 使用 Amazon CloudWatch 指標 - 了解如何使用 AWS 管理主控台 或 CloudWatch API 取得閘道的監控資料。
- 測量您應用程式和閘道之間的效能 - 了解如何測量資料輸送量、資料延遲和每秒操作，以了解應用程式和閘道之間的效能。
- 測量閘道與 之間的效能 AWS - 了解如何測量資料輸送量、資料延遲和每秒操作，以了解閘道和 AWS 雲端之間的效能。
- 了解磁碟區指標 - 了解如何測量提供與閘道相關聯磁碟區相關資料的指標。

使用 Amazon CloudWatch Logs 取得磁碟區閘道運作狀態日誌

您可以使用 Amazon CloudWatch Logs 取得有關磁碟區閘道運作狀態和相關資源的資訊。您可以使用這些日誌來監控閘道遇到的錯誤。此外，您可以使用 Amazon CloudWatch 訂閱篩選條件，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，假設您的閘道是部署於已啟用 VMware 高可用性 (HA) 的叢集中，而且您需要知道是否有任何錯誤。您可以將 CloudWatch 日誌群組設定為監控閘道，並在閘道發生錯誤時收到通知。您可以在啟用閘道時或在啟用並啟動及執行閘道之後，設定群組。如需有關如何在啟用閘道時設定 CloudWatch 日誌群組的資訊，請參閱 設定磁碟區閘道。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。

如需有關如何疑難排解和修正這些類型錯誤的詳細資訊，請參閱對磁碟區問題進行疑難排解。

下列程序說明如何在啟用閘道之後設定 CloudWatch 日誌群組。

將 CloudWatch 日誌群組設定為使用您的閘道

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/storagegateway/home 開啟 Storage Gateway 主控台。
2. 在左側導覽窗格中，選擇閘道，然後選擇您為其設定 CloudWatch 日誌群組的閘道。
3. 針對動作，選擇編輯閘道資訊，或在詳細資訊標籤上的運作狀態日誌和未啟用下，選擇設定日誌群組以開啟編輯 ***CustomerGatewayName*** 對話方塊。
4. 針對閘道運作狀態日誌群組，選擇下列其中一項：

- 如果您不想使用 CloudWatch 日誌群組監控閘道，請停用記錄。
- 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。

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. 在左側導覽窗格中，選擇閘道，然後選擇您為其設定 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 Amazon CloudWatch 主控台中，開啟日誌群組詳細資訊頁面。

使用 Amazon CloudWatch 指標

您可以使用 AWS 管理主控台 或 CloudWatch API 取得閘道的監控資料。主控台會根據 CloudWatch API 的原始資料顯示一系列圖形。您也可以透過其中一個 AWS 軟體開發套件 (SDK) 或 Amazon CloudWatch API 工具使用 CloudWatch API。根據需求，您可能偏好使用顯示於主控台中的圖形或自 API 擷取的圖形。

無論您選擇使用指標的方法為何，您都必須指定下列資訊：

- 要使用的指標維度。維度是一組用來單獨辨識指標的名稱值組。Storage Gateway 的維度為 `GatewayId`、`GatewayName` 和 `VolumeId`。在 CloudWatch 主控台中，您可以使用 `Gateway Metrics` 和 `Volume Metrics` 檢視，輕鬆選取閘道專屬和磁碟區專屬的維度。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`。

下表摘要說明您可以使用的 Storage Gateway 指標資料類型。

CloudWatch 命名空間	維度	描述
`AWS/StorageGateway`	`GatewayId`，`GatewayName`	這些維度會篩選描述閘道各層面的指標資料。您可以透過同時指定 `GatewayId` 和 `GatewayName` 維度，來識別要使用的閘道。

CloudWatch 命名空間	維度	描述
		閘道的輸送量和延遲資料是以閘道中的所有磁碟區為基礎。 每隔 5 分鐘免費自動提供資料。
	VolumeId	此維度會篩選磁碟區專屬的指標資料。使用其 VolumeId 維度識別要使用的磁碟區。 每隔 5 分鐘免費自動提供資料。

閘道和磁碟區指標的使用類似於其他服務指標的使用。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

測量您應用程式和閘道之間的效能

資料輸送量、資料延遲和每秒操作數這三種測量，可讓您了解使用您閘道之應用程式儲存體的執行狀況。當您使用正確的彙整統計資料時，您可以使用 Storage Gateway 指標來測量這些值。

「統計資料」是在一段指定期間內的指標彙整。當您在 CloudWatch 中檢視指標的值時，請針對資料延遲 (毫秒) 使用 Average 統計資料，針對資料輸送量(每秒位元組數)使用 Sum 統計資料，並針對每秒讀/寫次數 (IOPS) 使用 Samples 統計資料。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的統計資料。

下表摘要您可以用來測量您應用程式和閘道間輸送量、延遲和 IOPS 的指標及其對應的統計資料。

感興趣的項目	測量方式
輸送量	搭配使用 ReadBytes 和 WriteBytes 指標與 Sum CloudWatch 統計資料。例如，在 5 分鐘範例期間內的 Sum 指標之 ReadBytes 值，除以 300 秒，便可得到以每秒位元組速率方式表示的輸送量。

感興趣的項目	測量方式
延遲	搭配使用 ReadTime 和 WriteTime 指標與 Average CloudWatch 統計資料。例如，Average 指標的 ReadTime 值可讓您了解在範例期間內每個操作的延遲。
IOPS	搭配使用 ReadBytes 和 WriteBytes 指標與 Samples CloudWatch 統計資料。例如，將 5 分鐘範例期間內 Samples 指標的 ReadBytes 值除以 300 秒，便可取得 IOPS。

若是平均延遲圖形和平均大小圖形，平均值是依據在此期間完成的操作 (依圖形適用的讀取或寫入而定) 總數來計算。

測量從應用程式到磁碟區的資料輸送量

1. 透過 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 選擇 Metrics (指標)，然後選擇 All metrics (所有指標) 標籤，然後選擇 Storage Gateway (儲存體閘道)。
3. 選擇 Volume metrics (磁碟區指標) 維度，然後尋找您希望使用的磁碟區。
4. 選擇 ReadBytes 和 WriteBytes 指標。
5. 針對 Time Range (時間範圍)，選擇一個值。
6. 選擇 Sum 統計資料。
7. 針對 Period (期間)，選擇 5 分鐘或更高的值。
8. 在結果依照時間排序的資料點集合中 (其中一個是 ReadBytes，另一個則為 WriteBytes)，將每個資料點除以期間 (單位為秒)，便可取得範例點的輸送量。總輸送量是所有輸送量的加總。

例如，如果讀取輸送量在 300 秒期間內為 2，384，199，680 個位元組，則該資料點的近似輸送量速率為每秒 7.9 MB。

測量從應用程式到磁碟區的每秒資料輸入/輸出操作數

1. 透過 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 選擇 Metrics (指標)，然後選擇 All metrics (所有指標) 標籤，然後選擇 Storage Gateway (儲存體閘道)。
3. 選擇 Volume metrics (磁碟區指標) 維度，然後尋找您希望使用的磁碟區。

4. 選擇 ReadBytes 和 WriteBytes 指標。
5. 針對 Time Range (時間範圍)，選擇一個值。
6. 選擇 Samples 統計資料。
7. 針對 Period (期間)，選擇 5 分鐘或更高的值。
8. 在結果依照時間排序的資料點集合中 (其中一個是 ReadBytes，另一個則為 WriteBytes)，將每個資料點除以期間 (單位為秒)，便可取得 IOPS。

例如，如果寫入操作的數量在 300 秒的期間內為 24，373，則該資料點的 IOPS 為每秒 81 個寫入操作。

測量閘道與 之間的效能 AWS

資料輸送量、資料延遲和每秒操作數這三個測量，可讓您了解使用 Storage Gateway 之應用程式儲存體的執行狀況。當您使用正確的彙整統計資料時，便可做為您提供的 Storage Gateway 指標測量這三個值。下表摘要說明您可以用來測量您閘道和 AWS間輸送量、延遲和每秒讀/寫次數 (IOPS) 的指標及其對應的統計資料。

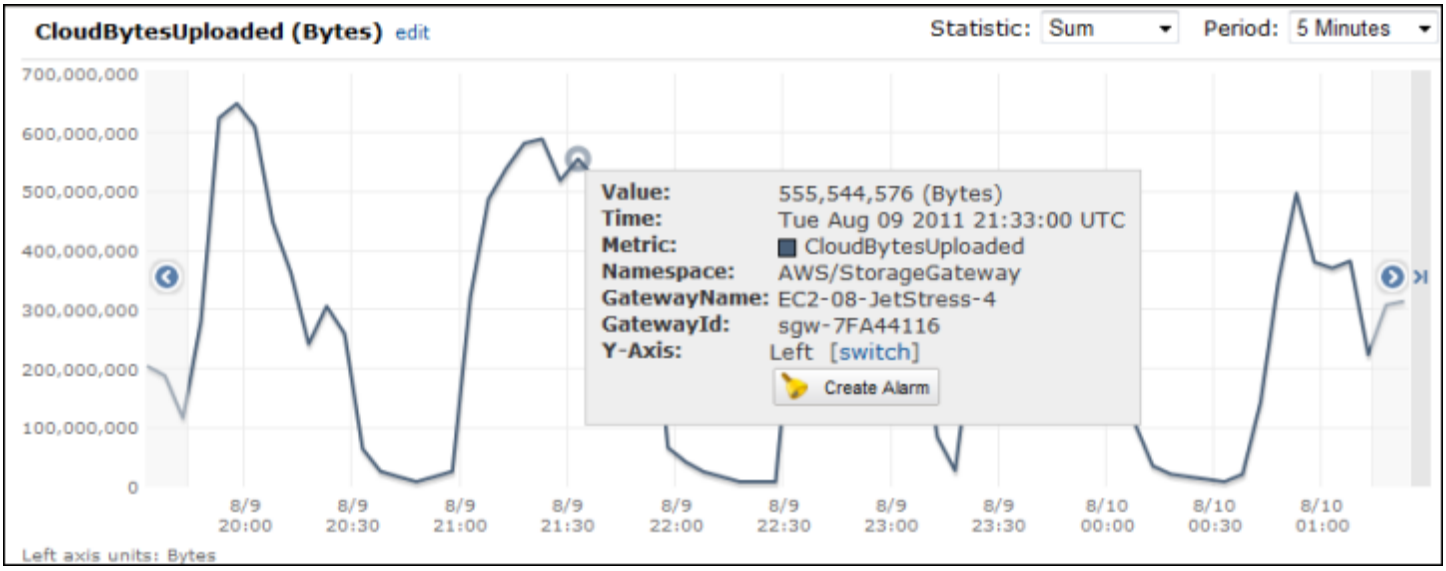
感興趣的項目	測量方式
輸送量	搭配使用 ReadBytes 和 WriteBytes 指標與 Sum CloudWatch 統計資料。例如，在 5 分鐘範例期間內的 Sum 指標之 ReadBytes 值，除以 300 秒，便可得到以每秒位元組速率方式表示的輸送量。
延遲	搭配使用 ReadTime 和 WriteTime 指標與 Average CloudWatch 統計資料。例如，Average 指標的 ReadTime 值可讓您了解在範例期間內每個操作的延遲。
IOPS	搭配使用 ReadBytes 和 WriteBytes 指標與 Samples CloudWatch 統計資料。例如，將 5 分鐘範例期間內 Samples 指標的 ReadBytes 值除以 300 秒，便可取得 IOPS。
對 的輸送量 AWS	搭配使用 CloudBytesDownloaded 和 CloudBytesUploaded 指標與 Sum CloudWatch 統計資料。例如，在 5 分鐘的取樣期間， CloudBytesDownloaded 指標Sum的值除以 300 秒，可讓您以每秒位元組為單位從 AWS 到閘道的輸送量。

感興趣的項目	測量方式
資料的延遲 AWS	搭配 CloudDownloadLatency 統計資料使用 Average 指標。例如，Average 指標的 CloudDownloadLatency 統計資料可讓您了解在範例期間內每個操作的延遲。

測量從閘道到 的上傳資料輸送量 AWS

1. 透過 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 選擇 Metrics (指標)，然後選擇 All metrics (所有指標) 標籤，然後選擇 Storage Gateway (儲存體閘道)。
3. 選擇 Gateway metrics (閘道指標) 維度，然後尋找您希望使用的磁碟區。
4. 選擇 CloudBytesUploaded 指標。
5. 針對 Time Range (時間範圍)，選擇一個值。
6. 選擇 Sum 統計資料。
7. 針對 Period (期間)，選擇 5 分鐘或更高的值。
8. 在結果依照時間排序的資料點集合中，將每個資料點除以期間 (單位為秒)，便可取得範例期間的輸送量。

將游標移至資料點上會顯示資料點的相關資訊，包括其值和上傳的位元組。將此值除以 Period (期間) 值 (5 分鐘)，便可取得該範例點的輸送量。例如，如果閘道到 的輸送量在 300 秒期間內 AWS 為 555，544，576 位元組，則每秒的大約輸送量為 1.85 MB。



測量閘道每個操作的延遲

1. 透過 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 選擇 Metrics (指標)，然後選擇 All metrics (所有指標) 標籤，然後選擇 Storage Gateway (儲存體閘道)。
3. 選擇 Gateway metrics (閘道指標) 維度，然後尋找您希望使用的磁碟區。
4. 選擇 `ReadTime` 和 `WriteTime` 指標。
5. 針對 Time Range (時間範圍)，選擇一個值。
6. 選擇 `Average` 統計資料。
7. 針對 Period (期間)，選擇 5 分鐘的值以符合預設報告時間。
8. 在結果依照時間排序的點集合中 (其中一個是 `ReadTime`，另一個則為 `WriteTime`)，將相同時間範例的資料點相加，便可取得總延遲 (單位為毫秒)。

測量從閘道到 的資料延遲 AWS

1. 透過 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 選擇 Metrics (指標)，然後選擇 All metrics (所有指標) 標籤，然後選擇 Storage Gateway (儲存體閘道)。
3. 選擇 Gateway metrics (閘道指標) 維度，然後尋找您希望使用的磁碟區。
4. 選擇 `CloudDownloadLatency` 指標。
5. 針對 Time Range (時間範圍)，選擇一個值。
6. 選擇 `Average` 統計資料。
7. 針對 Period (期間)，選擇 5 分鐘的值以符合預設報告時間。

其結果之依照時間排序的資料點集合便包含延遲 (單位為毫秒)。

將閘道輸送量的閾值上限警示設定為 AWS

1. 透過 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 選擇 Alarms (警示)。
3. 選擇 Create Alarm (建立警示) 以啟動 [Create Alarm] (建立警示) 精靈。
4. 選擇 Storage Gateway (儲存體閘道) 維度，然後尋找您希望使用的閘道。
5. 選擇 `CloudBytesUploaded` 指標。

6. 若要定義警示，請定義當 CloudBytesUploaded 指標大於等於指定值且持續指定時間之後的警示狀態。例如，您可以定義當 CloudBytesUploaded 指標大於 10 MB 長達 60 分鐘時的警示狀態。
7. 設定要針對警示狀態採取的動作。例如，您可以設定要傳送一封電子郵件通知給您。
8. 選擇建立警示 。

設定從 讀取資料的閾值上限警示 AWS

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

了解磁碟區指標

您可以在以下內容中找到涵蓋閘道磁碟區之 Storage Gateway 指標的相關資訊。每個閘道的磁碟區都有一組與其關聯的指標。

有些磁碟區專屬的指標與特定閘道專屬的指標名稱相同。這些指標代表相同類型的測量，但其範圍為磁碟區而非閘道。開始工作前，請指定您要使用閘道指標還是磁碟區指標。具體而言，使用磁碟區指標時，請指定您要檢視指標之儲存體磁碟區的磁碟區 ID。如需詳細資訊，請參閱使用 Amazon CloudWatch 指標。

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

下表說明您可以用來取得儲存體磁碟區資訊的 Storage Gateway 指標。

指標	描述	快取磁碟區	存放的磁碟區
AvailabilityNotification	磁碟區已傳送的可用性通知數目。 單位：計數	是	是
CacheHitPercent	來自由快取提供服務之磁碟區的應用程式讀取操作百分比。報告期間結束時會取樣。 當沒有來自磁碟區的應用程式讀取操作時，此指標會回報 100%。 單位：百分比	是	否
CachePercentDirty	未保存到 AWS的閘道快取整體百分比中磁碟區的比重。報告期間結束時會取樣。 使用閘道的 CachePercentDirty 指標可檢視未保存到 AWS的閘道快取整體百分比。如需詳細資訊，請參閱了解閘道指標。 單位：百分比	是	是
CachePercentUsed	閘道快取儲存體整體使用百分比中磁碟區的比重。報告期間結束時會取樣。	是	否

指標	描述	快取磁碟區	存放的磁碟區
	使用 CachePercentUsed 指標可檢視閘道快取儲存體的整體使用百分比。如需詳細資訊，請參閱了解閘道指標。 單位：百分比		
CloudBytesDownloaded	已從雲端下載到磁碟區的位元組數量。 單位：位元組	是	是
CloudBytesUploaded	已從雲端上傳到磁碟區的位元組數量。 單位：位元組	是	是
HealthNotification	磁碟區已傳送的運作狀態通知數目。 單位：計數	是	是
IoWaitPercent	磁碟區目前正在使用的 IoWaitPercent 百分比。 單位：百分比	是	是
MemTotalBytes	磁碟區目前使用的總記憶體百分比。 單位：百分比	是	否
MemoryUsage	磁碟區目前使用的記憶體百分比。 單位：百分比	是	否

指標	描述	快取磁碟區	存放的磁碟區
ReadBytes	報告期間從您內部部署應用程式讀取的位元組總數。 使用此指標搭配 Sum 統計資料可測量輸送量，搭配 Samples 統計資料可測量 IOPS。 單位：位元組	是	是
ReadTime	報告期間您的內部部署應用程式在讀取操作上所花費的總毫秒數。 使用此指標搭配 Average 統計資料可測量延遲。 單位：毫秒	是	是
UserCpuPercent	磁碟區目前正在使用的已配置 CPU 運算單位百分比。 單位：百分比	是	是

指標	描述	快取磁碟區	存放的磁碟區
WriteBytes	報告期間寫入至您內部部署應用程式的位元組總數。 使用此指標搭配 Sum 統計資料可測量輸送量，搭配 Samples 統計資料可測量 IOPS。 單位：位元組	是	是
WriteTime	報告期間您的內部部署應用程式在寫入操作上所花費的總毫秒數。 使用此指標搭配 Average 統計資料可測量延遲。 單位：毫秒	是	是
QueuedWrites	等待寫入的位元組數 AWS，在報告期間結束時取樣。 單位：位元組	是	是

維護您的閘道

維護您的磁碟區閘道包括調整快取儲存體和上傳緩衝空間的本機磁碟大小和設定、管理更新和設定更新排程、管理頻寬用量，以及在必要時關閉或刪除閘道和相關資源等任務。這些任務對於所有閘道類型而言非常常見。若您尚未建立閘道，請參閱建立閘道。

主題

- 管理 Storage Gateway 的本機磁碟 - 了解如何評估磁碟大小需求、新增快取容量，以及管理您配置給磁碟區閘道以進行緩衝和儲存的本機磁碟。
- 管理磁碟區閘道的頻寬 - 了解如何限制從閘道到 的上傳輸送量 AWS ，以控制閘道使用的網路頻寬量。
- 管理閘道更新 - 了解如何開啟或關閉維護更新，並修改磁碟區閘道的維護時段排程。
- 關閉閘道 VM - 了解如果您需要關閉或重新啟動閘道虛擬機器以進行維護時該怎麼做，例如將修補程式套用至 Hypervisor 時。
- 刪除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 Storage Gateway 的本機磁碟

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

主題

- 決定本機磁碟儲存體的數量
- 設定額外的上傳緩衝和快取儲存體

決定本機磁碟儲存體的數量

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

- 磁碟區閘道：
  - 存放的閘道需要至少一個磁碟，做為上傳緩衝使用。
  - 快取的閘道需要至少兩個磁碟。一個做為快取使用，另一個則做為上傳緩衝使用。

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

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

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

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

判斷要配置的上傳緩衝大小

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

> **Note**
>
> 針對磁碟區閘道，當上傳緩衝到達其容量時，您的磁碟區便會進入傳遞狀態。在此狀態中，您應用程式寫入的新資料會在本機持久保存，但不會立即上傳至 AWS 。因此，您無法擷取新的快照。當上傳緩衝容量釋出時，磁碟區便會進入 BOOTSTRAPPING (引導) 狀態。在此狀態下，任何在本機保留的新資料都會上傳到 AWS。最後，磁碟區會回到作用中狀態。然後，Storage Gateway 會恢復與存放在 中的複本一起儲存在本機的資料正常同步 AWS，您可以開始拍攝新的快照。如需磁碟區狀態的詳細資訊，請參閱了解磁碟區狀態和轉換。

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

傳入資料的速率

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

傳出資料的速率

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

若為下列任一情形，強烈建議您配置至少 150 GiB 的上傳緩衝區空間：

- 您的傳入率高於傳出率。
- 該公式傳回小於 150 GiB 的值。

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

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

Example

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

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

判斷要配置的快取儲存體大小

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

您可以先使用概略值來佈建快取儲存體的磁碟。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，請參閱監控快取儲存。

設定額外的上傳緩衝和快取儲存體

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

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

為您的閘道設定額外的上傳緩衝或快取儲存體

1. 在閘道主機 Hypervisor 或 Amazon EC2 執行個體上佈建一或多個新磁碟。如需如何在 Hypervisor 中佈建磁碟的資訊，請參閱 Hypervisor 文件。如需為 Amazon EC2 執行個體佈建 Amazon EBS 磁碟區的相關資訊，請參閱《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。在以下步驟中，您將設定此磁碟為上傳緩衝或快取儲存體。
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，選擇設定儲存體。
6. 在設定儲存體區段中，識別您佈建的磁碟。如果您沒有看到您的磁碟，請選擇重新整理圖示重新整理清單。針對每個磁碟，從配置給下拉式功能表中選擇上傳緩衝或快取儲存體。

> **Note**
>
> 上傳緩衝是在儲存的磁碟區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。

管理磁碟區閘道的頻寬

您可以限制（或調節）從閘道到 的上傳輸送量， AWS 或從 AWS 到閘道的下載輸送量。使用頻寬限流可協助您控制閘道使用的網路頻寬量。根據預設，啟用的閘道在上傳或下載時沒有速率限制。

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

您也可以為閘道定義以排程為基礎的頻寬限流。您可以透過定義一或多個頻寬速率限制間隔來排程頻寬限流。如需詳細資訊，請參閱使用 Storage Gateway 主控台進行排程的頻寬限流。

設定頻寬限流的單一設定，相當於定義排程時將單一頻寬速率限制間隔設定為每天，且開始時間為 `00:00`，結束時間為 `23:59`。

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

主題

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

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

使用 Storage Gateway 主控台變更頻寬限流

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

使用主控台變更閘道的頻寬調節

1. 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. 在動作中，選擇編輯頻寬限制。
4. 在編輯速率限制對話方塊中，輸入新的限制值，然後選擇儲存。您的變更會出現在閘道的 Details (詳細資訊) 標籤中。

使用 Storage Gateway 主控台進行排程的頻寬限流

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

新增或修改閘道頻寬限流的排程

1. 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. 在動作中，選擇編輯頻寬速率限制排程。

   閘道的頻寬-速率限制排程會顯示在編輯頻寬速率限制排程對話方塊中。根據預設，新的閘道頻寬-速率限制排程為空白。
4. 在編輯頻寬速率限制排程對話方塊中，選擇新增項目以新增頻寬-速率限制間隔。為每個頻寬-速率限制間隔輸入下列資訊：

   - 星期幾：您可以針對工作日 (星期一至星期五)、週末 (星期六和星期日)、一週中的每一天或一週中的一或多天建立頻寬速率限制間隔。
   - 開始時間：輸入閘道本機時區中頻寬間隔的開始時間 (使用 HH: MM 格式)。

   > **Note**
   >
   > 頻寬速率限制間隔會從您在此處指定的分鐘開始時開始。

- 結束時間：輸入閘道本地時區中頻寬-速率限制間隔的結束時間 (使用 HH: MM 格式)。

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

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

若要修改頻寬-速率限制間隔，您可以輸入間隔參數的修訂值。

若要移除頻寬-速率限制間隔，您可以選擇要刪除之間隔右側的移除。

完成變更後，選擇儲存。

5. 選擇新增項目並輸入日期、開始和結束時間，以及下載和上傳速率限制，繼續新增頻寬速率限制間隔。

   > **Important**
   >
   > 頻寬速率限制間隔不能重疊。間隔的開始時間必須在前一個間隔的結束時間之後，以及在下列間隔的開始時間之前發生。

6. 輸入所有頻寬速率限制間隔後，請選擇儲存變更以儲存頻寬-速率限制排程。

成功更新頻寬速率限制排程後，您可以在閘道的詳細資訊面板中查看目前的下載和上傳速率限制。

使用 更新閘道頻寬速率限制 適用於 Java 的 AWS SDK

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

Example：使用 更新閘道頻寬速率限制 適用於 Java 的 AWS SDK

下列 Java 程式碼範例會更新閘道的頻寬速率限制。如需使用此範例程式碼，您需要提供服務端點、閘道 Amazon Resource Name (ARN)，以及上傳及下載限制。如需可與 Storage Gateway 搭配使用 AWS 的服務端點清單，請參閱《AWS Storage Gateway 》中的端點和配額AWS 一般參考。

```
import java.io.IOException;

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


public class UpdateBandwidthExample {

    public static AWSStorageGatewayClient sgClient;

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

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

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

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

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

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

        UpdateBandwidth(gatewayARN, uploadRate, downloadRate);

    }

    private static void UpdateBandwidth(String gatewayARN2, long uploadRate2,
            long downloadRate2) {
```

```
        try
        {
            UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
                new UpdateBandwidthRateLimitRequest()
                .withGatewayARN(gatewayARN)
                .withAverageDownloadRateLimitInBitsPerSec(downloadRate)
                .withAverageUploadRateLimitInBitsPerSec(uploadRate);

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

使用 更新閘道頻寬速率限制 適用於 .NET 的 AWS SDK

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

Example：使用 更新閘道頻寬速率限制 適用於 .NET 的 AWS SDK

下列 C# 程式碼範例會更新閘道的頻寬速率限制。如需使用此範例程式碼，您需要提供服務端點、閘道 Amazon Resource Name (ARN)，以及上傳及下載限制。如需可與 Storage Gateway 搭配使用 AWS 的服務端點清單，請參閱《AWS Storage Gateway 》中的端點和配額AWS 一般參考。

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
```

```
using Amazon.StorageGateway;
using Amazon.StorageGateway.Model;

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

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

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

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

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

            UpdateBandwidth(gatewayARN, uploadRate, downloadRate);

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

        public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
 downloadRate)
        {
            try
            {
                UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
                    new UpdateBandwidthRateLimitRequest()
                    .WithGatewayARN(gatewayARN)
                    .WithAverageDownloadRateLimitInBitsPerSec(downloadRate)
                    .WithAverageUploadRateLimitInBitsPerSec(uploadRate);
```

```
                UpdateBandwidthRateLimitResponse updateBandwidthRateLimitResponse =
 sgClient.UpdateBandwidthRateLimit(updateBandwidthRateLimitRequest);
                String returnGatewayARN =
 updateBandwidthRateLimitResponse.UpdateBandwidthRateLimitResult.GatewayARN;
                Console.WriteLine("Updated the bandwidth rate limits of " +
 returnGatewayARN);
                Console.WriteLine("Upload bandwidth limit = " + uploadRate + " bits per
 second");
                Console.WriteLine("Download bandwidth limit = " + downloadRate + " bits
 per second");
            }
            catch (AmazonStorageGatewayException ex)
            {
                Console.WriteLine("Error updating gateway bandwith.\n" +
 ex.ToString());
            }
        }
    }
}
```

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

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

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

下列 PowerShell 指令碼範例會更新閘道的頻寬速率限制。如需使用此範例指令碼，您需要提供服務端點、閘道 Amazon Resource Name (ARN)，以及上傳及下載限制。

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

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

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

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

#Update Bandwidth Rate Limits
Update-SGBandwidthRateLimit -GatewayARN $gatewayARN `
                            -AverageUploadRateLimitInBitsPerSec $UploadBandwidthRate `
                            -AverageDownloadRateLimitInBitsPerSec
 $DownloadBandwidthRate

$limits =  Get-SGBandwidthRateLimit -GatewayARN $gatewayARN

Write-Output("`nGateway: " + $gatewayARN);
Write-Output("`nNew Upload Rate: " + $limits.AverageUploadRateLimitInBitsPerSec)
Write-Output("`nNew Download Rate: " + $limits.AverageDownloadRateLimitInBitsPerSec)
```

管理閘道更新

Storage Gateway 包含受管雲端服務元件和閘道設備元件，您可以在內部部署或在 AWS 雲端的 Amazon EC2 執行個體上部署。這兩個元件都會定期收到更新。本節中的主題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，您可能會遇到互通性問題，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每月維護更新。每月維護更新可能包括作業系統和軟體升級、解決穩定性、效能和安全性的修正，以及新功能的存取。所有更新都是累積的，並在套用時將閘道升級到目前版本。如需有關每次更新中包含的特定變更的資訊，請參閱磁碟區閘道設備軟體的版本備註。

每月維護更新可能會導致服務短暫中斷。閘道的 VM 主機不需要在更新期間重新啟動，但在閘道設備更新和重新啟動時，閘道將短暫無法使用。因為透過增加您 iSCSI 啟動器的逾時來重新啟動閘道，您可以將任何應用程式中斷的機率降到最低。如需增加 Windows 和 Linux 之 iSCSI 啟動器逾時的詳細資訊，請參閱自訂您的 Windows iSCSI 設定和自訂您的 Linux iSCSI 設定。

當您部署和啟用閘道時，會設定預設的每週維護時段排程。您可以隨時修改維護時段排程。您也可以關閉每月維護更新，但我們建議您將其保持開啟狀態。

> **Note**
>
> 即使定期維護更新已關閉，緊急更新有時會根據維護時段排程套用。

將任何更新套用至閘道之前， 會在 Storage Gateway 主控台和 上 AWS 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

開啟維護更新時，閘道會根據設定的維護時段排程自動套用這些更新。如需詳細資訊，請參閱。

如果維護更新已關閉，閘道將不會自動套用這些更新，但您一律可以使用 Storage Gateway 主控台、API 或 CLI 手動套用這些更新。無論此設定為何，緊急更新有時會在您設定的維護時段期間套用。

> **Note**
>
> 下列程序說明如何使用 Storage Gateway 主控台開啟或關閉閘道更新。若要使用 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，選擇儲存變更。

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

修改閘道維護時段排程

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

> **Note**
>
> 下列程序說明如何使用 Storage Gateway 主控台修改維護時段排程。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。考慮先手動更新閘道，然後嘗試再次設定維護時段排程。

5. 完成後，選擇儲存變更。

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

手動套用更新

如果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。

關閉閘道 VM

您可能需要基於維護而關機或重新啟動 VM，例如將修補程式套用至虛擬化管理程序時。關機 VM 之前，必須先停止閘道。雖然本節著重於使用 Storage Gateway 管理主控台啟動和停止閘道，但您也可以使用 VM 本機主控台或 Storage Gateway API 啟動和停止閘道。當您開啟 VM 的電源時，請記得重新啟動閘道。

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。

Note

如果您在備份軟體寫入或讀取磁帶時停止閘道，則寫入或讀取任務可能不會成功。停止閘道之前，應該檢查備份軟體以及任何進行中任務的備份排程。

- 閘道 VM 本機主控台：請參閱 登入磁碟區閘道本機主控台。
- Storage Gateway API：請參閱 ShutdownGateway

啟動和停止磁碟區閘道

停止磁碟區閘道

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 Gateways (閘道)，然後選擇要停止的閘道。閘道的狀態為 Running (正在執行)。
3. 在 Actions (動作) 選單上，選擇 Stop gateway (停止閘道)，並從對話方塊確認閘道 ID，然後選擇 Stop gateway (停止閘道)。

   閘道停止時，您可能會看到訊息，指出閘道的狀態。閘道關閉時，訊息和 Start gateway (啟動閘道) 按鈕會出現在 Details (詳細資訊) 標籤中。

當您停止閘道時，除非您啟動儲存，否則將無法存取儲存資源。如果閘道在停止時正在上傳資料，則會在您啟動閘道時繼續上傳。

啟動磁碟區閘道

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 Gateways (閘道)，然後選擇要啟動的閘道。閘道的狀態為 Shutdown (關機)。
3. 選擇詳細資訊，然後選擇啟動閘道。

刪除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，而且其與啟動器的 iSCSI 連線已關閉。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。

主題

- 使用 Storage Gateway 主控台刪除閘道
- 從內部部署的閘道移除資源
- 從 Amazon EC2 執行個體上所部署的閘道移除資源

使用 Storage Gateway 主控台刪除閘道

所有閘道類型的閘道刪除程序都相同。不過，根據您要刪除的閘道類型以及在其上部署閘道的主機，您可能需要執行額外任務才能移除與閘道建立關聯的資源。移除這些資源可協助您避免支付不打算使用之資源的費用。

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

從內部部署的閘道移除資源

您可以使用下列說明，從內部部署的閘道移除資源。

從 VM 上所部署的磁碟區閘道移除資源

如果您要刪除的閘道部署在虛擬機器 (VM) 上，則建議您採取下列動作來清除資源：

- 刪除閘道。如需說明，請參閱使用 Storage Gateway 主控台刪除閘道。
- 刪除所有您不需要的 Amazon EBS 快照。如需說明，請參閱《Amazon EC2 使用者指南》中的刪除 Amazon EBS 快照。 Amazon EC2

從 Amazon EC2 執行個體上所部署的閘道移除資源

如果您想要刪除在 Amazon EC2 執行個體上部署的閘道，我們建議您清除與閘道搭配使用 AWS 的資源，特別是部署磁帶閘道時的 Amazon EC2 執行個體、任何 Amazon EBS 磁碟區，以及磁帶。這樣做有助於避免意外的使用費。

從 Amazon EC2 上所部署的快取磁碟區移除資源

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

1. 在 Storage Gateway 主控台中，刪除閘道，如 使用 Storage Gateway 主控台刪除閘道 中所示。
2. 在 Amazon EC2 主控台中，如果您打算再次使用執行個體，則請停止 EC2 執行個體。否則，請終止執行個體。如果您打算刪除磁碟區，則請先記下連接至執行個體的區塊型儲存裝置以及儲存裝置的識別符，再終止執行個體。您需要這些項目才能識別您要刪除的磁碟區。
3. 在 Amazon EC2 主控台中，如果您不打算再次使用所有連接至執行個體的 Amazon EBS 磁碟區，則請予以移除。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的清除執行個體和磁碟區。

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。本機主控台會直接在託管閘道設備的虛擬化主機平台上執行。對於內部部署閘道，您可以透過 VMware、Hyper-v 或 Linux KVM 虛擬化主機存取本機主控台。對於 Amazon EC2 閘道，您可以使用 SSH 連線至 Amazon EC2 執行個體來存取主控台。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 VM 本機主控台上執行任務 - 了解如何使用本機主控台執行內部部署閘道的基本設定和進階組態任務，例如設定 HTTP 代理、檢視系統資源狀態或執行終端機命令。
- 在 Amazon EC2 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，請參閱登入磁碟區閘道本機主控台。

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，請參閱登入磁碟區閘道本機主控台。

   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，請參閱登入磁碟區閘道本機主控台。

   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 VM 本機主控台上執行任務

對於您部署現場部署的磁碟區閘道，您可以使用從虛擬機器主機平台存取的閘道本機主控台來執行下列維護任務。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

- 登入磁碟區閘道本機主控台 - 了解如何登入閘道本機主控台，您可以在其中設定閘道網路設定並變更預設密碼。
- 為您的內部部署閘道設定 SOCKS5 代理 - 了解如何設定 Storage Gateway 以透過 Socket Secure 第 5 版 (SOCKS5) 代理伺服器路由所有 AWS 端點流量。
- 設定您的閘道網路 - 了解如何設定閘道以使用 DHCP 或指派靜態 IP 地址。
- 測試閘道與網際網路的連線 - 了解如何使用閘道本機主控台來測試閘道與網際網路之間的連線。
- 在本機主控台中為內部部署閘道執行儲存閘道命令 - 了解如何執行本機主控台命令，讓您執行其他任務，例如儲存路由表、連線至 支援等。
- 檢視閘道系統資源狀態 - 了解如何檢查閘道設備可用的虛擬 CPU 核心、根磁碟區大小和 RAM。

登入磁碟區閘道本機主控台

當 VM 可供您登入時，將顯示登入畫面。如果這是您第一次登入 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 在本機主控台中為內部部署閘道執行儲存閘道命令。

> **Important**
>
> 對於磁碟區閘道或磁帶閘道的較舊版本，使用者名稱為 `sguser`，密碼為 `sgpassword`。如果您重設密碼，且閘道已更新至較新版本，使用者名稱將變更為 admin，但密碼將保持不變。

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 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。

為您的內部部署閘道設定 SOCKS5 代理

磁碟區閘道和磁帶閘道支援您的內部部署閘道和 AWS之間的 Socket Secure 5 版 (SOCKS5) 代理組態。

> **Note**
>
> 支援的唯一代理組態是 SOCKS5。

如果您的閘道必須使用代理伺服器與網際網路通訊，您即需要為閘道設定 SOCKS 代理設定。您透過指定 IP 地址和執行代理的主機連接埠號碼，來完成此作業。完成此作業後，Storage Gateway 會透過您的代理伺服器路由所有流量。如需閘道之網路需求的資訊，請參閱網路與防火牆需求。

下列程序說明如何設定磁碟區閘道和磁帶閘道的 SOCKS 代理。

設定磁碟區和磁帶閘道的 SOCKS5 代理

1. 登入您閘道的本機主控台。

   - VMware ESXi：如需詳細資訊，請參閱 使用 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。

- 如需 KVM 的詳細資訊，請參閱 使用 Linux KVM 存取閘道本機主控台。

2. 從 AWS Storage Gateway - 組態主功能表中，輸入對應的數字以選取 SOCKS 代理伺服器組態。
3. 從 AWS Storage Gateway SOCKS 代理組態功能表中，輸入對應的數字，以執行下列其中一項工作：

執行此任務	執行此作業
設定 SOCKS 代理	輸入對應的數字以選取設定 SOCKS 代理伺服器。 您需要提供主機名稱和連接埠才能完成設定。
檢視目前的 SOCKS 代理組態	輸入對應的數字以選取檢視目前的 SOCKS 代理組態。 如果未設定 SOCKS 代理，會顯示訊息 `SOCKS Proxy not configured` 。如已設定 SOCKS 代理，即會顯示主機名稱和代理的連接埠。
移除 SOCKS 代理組態	輸入對應的數字以選取移除 SOCKS 代理組態。 會顯示訊息 `SOCKS Proxy Configuration Removed` 。

4. 重新啟動您的 VM 以套用您的 HTTP 組態。

設定您的閘道網路

閘道的預設網路組態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。

- 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。
- 如需 KVM 的詳細資訊，請參閱 使用 Linux KVM 存取閘道本機主控台。

2. 從 AWS Storage Gateway - 組態主功能表中，輸入對應的數字以選取網路組態。
3. 從 AWS Storage Gateway 網路組態功能表中，執行下列其中一項工作：

執行此任務	執行此作業
說明網路轉接器	輸入對應的數字以選取描述介面卡。 隨即顯示介面卡名稱的清單，系統會提示您輸入介面卡名稱例如 **`eth0`**。若您指定的轉接器為使用中，將顯示轉接器的下列資訊： • 媒體存取控制 (MAC) 地址 • IP 地址 • 網路遮罩 • 閘道 IP 地址 • DHCP 啟動狀態 當您設定靜態 IP 地址或設定閘道的預設介面卡時，可以使用此處列出的介面卡名稱。
設定 DHCP	輸入對應的數字以選取設定 DHCP。 系統會提示您設定網路界面使用 DHCP。
為閘道設定靜態 IP 地址	輸入對應的數字以選取設定靜態 IP。 系統會提示您輸入下列資訊來設定靜態 IP： •

執行此任務	執行此作業
	網路轉接器名稱 • IP 地址 • 網路遮罩 • 預設閘道地址 • 主要網域名稱服務 (DNS) 地址 • 輔助 DNS 地址 **Important** 如果您的閘道已啟用，您必須將其關閉並在 Storage Gateway 主控台重新啟動，設定才能生效。如需詳細資訊，請參閱關閉閘道 VM。 如果您的閘道使用一個以上的網路界面，您必須將所有已啟用的界面設定為使用 DHCP 或靜態 IP 地址。 例如，假設您的閘道 VM 使用兩個設定為 DHCP 的界面。如果您稍後將一個界面設定為靜態 IP，另一個界面將停用。在此情況下，若要啟用界面，您必須將其設定為靜態 IP。 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。

執行此任務	執行此作業
設定閘道的主機名稱	輸入對應的數字以選取設定主機名稱。 系統會提示您選擇閘道要使用您指定的靜態主機名稱，還是透過 DCHP 或 rDNS 自動取得主機名稱。 如果您選取靜態，系統會提示您提供靜態主機名稱，例如 `testgateway.example.com` 。輸入 y以套用組態。 **Note** 如果您為閘道設定靜態主機名稱，請確定提供的主機名稱位於閘道加入的網域中。您還必須在 DNS 系統中建立 A 記錄，將閘道的 IP 地址指向其靜態主機名稱。
重設所有閘道的網路組態為 DHCP	輸入對應的數字以選取全部重設為 DHCP。 所有的網路界面皆設定為使用 DHCP。 **Important** 如果您的閘道已啟用，您必須將其關閉並在 Storage Gateway 主控台重新啟動您的閘道，設定才能生效。如需詳細資訊，請參閱關閉閘道 VM。

執行此任務	執行此作業
設定閘道的預設路由轉接器	輸入對應的數字以選取設定預設介面卡。 隨即顯示閘道可用的介面卡，系統會提示您選取其中一個介面卡例如 **`eth0`**。
檢視閘道的 DNS 組態	輸入對應的數字以選取檢視 DNS 組態。 隨即顯示主要和次要 DNS 名稱伺服器的 IP 地址。
檢視路由表	輸入對應的數字以選擇檢視路線。 隨即顯示閘道的預設路由。

測試閘道與網際網路的連線

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

測試閘道的網際網路連線

1. 登入您閘道的本機主控台。
   - VMware ESXi：如需詳細資訊，請參閱 使用 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。
   - 如需 KVM 的詳細資訊，請參閱 使用 Linux KVM 存取閘道本機主控台。
2. 從 AWS Storage Gateway - 組態主功能表中，輸入對應的數字以選取測試網路連線。

   如果您的閘道已經啟動，連線測試會立即開始。對於尚未啟用的閘道，您必須指定端點類型 和 AWS 區域 ，如下列步驟所述。
3. 如果您的閘道尚未啟動，請輸入對應的數字以選取閘道的端點類型。
4. 如果您選取公有端點類型，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。

在本機主控台中為內部部署閘道執行儲存閘道命令

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

執行組態或診斷命令

1. 登入您閘道的本機主控台：
   - 如需登入 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 - 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。

命令	函式
	Note 建議您使用 Storage Gateway 主控台或專用的本機主控台功能表選項來設定網路或 IP 設定。如需指示，請參閱設定閘道網路。
ip	顯示/操作路由、裝置和通道。 **Note** 建議您使用 Storage Gateway 主控台或專用的本機主控台功能表選項來設定網路或 IP 設定。如需指示，請參閱設定閘道網路。
iptables	IPv4 封包篩選和 NAT 的管理工具。
ip6tables	IPv6 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。
passwd	更新身份驗證令牌。
save-iptables	持續存取 IP 資料表。
save-routing-table	儲存新增的路由表項目。

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

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。

在 Amazon EC2 本機主控台上執行任務

有些 Storage Gateway 維護任務需要您登入閘道本機主控台，以取得已部署在 Amazon EC2 執行個體上的閘道。您可以使用 Secure Shell (SSH) 用戶端存取 Amazon EC2 執行個體上的閘道本機主控台。本節中的主題說明如何登入閘道本機主控台並執行維護任務。

主題

- 登入至您的 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 代理路由您部署在 EC2 的閘道 - 了解如何設定 Storage Gateway，將所有 enpoint 流量透過 Socket Secure 第 AWS 5 版 (SOCKS5) 代理伺服器路由到 Amazon EC2 閘道執行個體。
- 測試閘道網路連線 - 了解如何使用閘道本機主控台來測試閘道與各種網路資源之間的網路連線。
- 檢視閘道系統資源狀態 - 了解如何使用閘道本機主控台來檢查閘道設備可用的虛擬 CPU 核心、根磁碟區大小和 RAM。
- 在本機主控台上執行 Storage Gateway 命令 - 了解如何執行本機主控台命令，讓您執行其他任務，例如儲存路由表、連線至 支援等。

登入至您的 Amazon EC2 閘道本機主控台

您可以使用 Secure Shell (SSH) 用戶端連線到您的 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。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 金鑰對的資訊，請參閱《Amazon EC2 使用者指南》中的 Amazon EC2 金鑰對。

登入至閘道本機主控台

1. 登入您的本機主控台。如果您是從 Windows 電腦連線到您的 EC2 執行個體，請以 admin 身分登入。
2. 登入之後，您會看到 AWS Storage Gateway - 組態主功能表，您可以從中執行各種工作。

若要了解此項	請參閱此主題
為您的閘道設定 SOCKS 代理	透過 HTTP 代理路由您部署在 EC2 的閘道
測試網路連線	測試閘道網路連線
執行 Storage Gateway 主控台命令	在本機主控台上執行 Storage Gateway 命令
檢視系統資源檢查	檢視閘道系統資源狀態.

若要關閉閘道，請輸入 **0**。

若要結束組態工作階段，請輸入 **x**。

透過 HTTP 代理路由您部署在 EC2 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，請參閱登入至您的 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，請參閱登入至您的 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

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。如需說明，請參閱登入至您的 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。

   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。

在本機主控台上執行 Storage Gateway 命令

AWS Storage Gateway 主控台可協助提供安全的環境，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，請參閱登入至您的 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。

命令	函式
exit	傳回組態功能表。
h	顯示可用的命令清單。
ifconfig	檢視或設定網路介面。 **Note** 建議您使用 Storage Gateway 主控台或專用的本機主控台功能表選項來設定網路或 IP 設定。
ip	顯示/操作路由、裝置和通道。 **Note** 建議您使用 Storage Gateway 主控台或專用的本機主控台功能表選項來設定網路或 IP 設定。
iptables	IPv4 封包篩選和 NAT 的管理工具。
ip6tables	IPv6 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。
save-iptables	持續存取 IP 資料表。
save-routing-table	儲存新增的路由表項目。
sslcheck	檢查 SSL 有效性以進行網路疑難排解
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。

若要瞭解某個指令，請輸入指令名稱，然後輸入 -h 選項，如：`sslcheck -h`。

磁碟區閘道的效能和最佳化

本節說明 Storage Gateway 效能。

主題

- 最佳化閘道效能

最佳化閘道效能

建議閘道伺服器組態

若要取得閘道的最佳效能，Storage Gateway 建議您為閘道的主機伺服器採用下列閘道組態：

- 至少 24 個專屬實體 CPU 核心
- 針對磁碟區閘道，您的硬體應該專用以下數量的 RAM：
  - 至少 16 GiB 的保留 RAM，適用於快取大小高達 16 TiB 的閘道
  - 至少 32 GiB 的保留 RAM，適用於快取大小為 16 TiB 至 32 TiB 的閘道
  - 至少 48 GiB 的保留 RAM，適用於快取大小為 32 TiB 至 64 TiB 的閘道
- 磁碟 1，用作閘道快取，如下所示：
  - 使用 NVMe 控制器的 SSD。
- 磁碟 2，用作閘道上傳緩衝，如下所示：
  - 使用 NVMe 控制器的 SSD。
- 磁碟 3，用作閘道上傳緩衝，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)。

新增資源至您的閘道

下列瓶頸可將磁碟區閘道的效能降低到低於理論上持續輸送量上限 （ 您的頻寬到 AWS 雲端 ）：

- CPU 核心数
- 快取/上傳緩衝磁碟輸送量
- RAM 總容量
- 的網路頻寬 AWS
- 從啟動器到閘道的網路頻寬

本節包含最佳化閘道效能時可採取的步驟。本指南是以將資源新增至您的閘道或至您的應用程式伺服器為基礎。

您可以利用下列其中一或多個方法，將資源新增到您的閘道，以將閘道效能最佳化。

使用高效能磁碟

快取和上傳緩衝磁碟輸送量可能會限制閘道的上傳和下載效能。如果閘道的效能大幅低於預期效能，請考慮改善快取和上傳緩衝磁碟輸送量，方法如下：

- 使用諸如 RAID 10 之類的條紋化 RAID 來提高磁碟輸送量，最好是使用硬件 RAID 控制器。

  > **Note**
  >
  > RAID (獨立磁碟冗餘陣列) 或特別是磁碟條紋化 RAID 組態 (如 RAID 10) 是將資料主體劃分為區塊並將資料區塊分散到多個儲存裝置的程序。您使用的 RAID 層級會影響您可達到的確切速度和容錯能力。藉由跨多個磁碟分割 IO 工作負載，RAID 裝置的整體輸送量遠高於任何單一成員磁碟的整體輸送量。

- 使用直接連接的高效能磁碟

  若要最佳化閘道效能，您可以新增高效能磁碟，例如固態硬碟 (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)。

  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。如需閘道指標的資訊，請參閱 監控 Storage Gateway。

新增更多上傳緩衝磁碟

若要達到更高的寫入輸送量，請至少新增兩個上傳緩衝磁碟。將資料寫入閘道時，資料會寫入並儲存在本機的上傳緩衝磁碟。之後，儲存的本機資料會以非同步方式在要處理的磁碟上讀取，並上傳至 AWS。新增更多上傳緩衝磁碟，可能會減少對每個磁碟執行的並行 I/O 作業數量。這可能會增加閘道的寫入輸送量。

具備個別實體磁碟的後端閘道虛擬磁碟

佈建閘道磁碟時，強烈建議您不要為使用相同基礎實體儲存體磁碟的上傳緩衝及快取儲存體佈建本機磁碟。例如，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 或 RAID 6) 支援的資料存放區，可能導致效能不佳。

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 的每個虛擬處理器受到專屬 CPU 核心的支援。此外，確認您沒有過度訂閱主機伺服器的 CPU。

將額外的 CPU 新增到閘道主機伺服器時，您會提高閘道的處理容量。這樣做可讓您的閘道平行處理將資料從您的應用程式存放到本機儲存以及將此資料上傳至 Amazon S3。額外的 CPU 也可協助確保您的閘道在主機與其他 VM 共享時，也能取得足夠的 CPU 資源。提供足夠的 CPU 資源對於改善輸送量具有一般性的效果。

增加閘道與 AWS 雲端之間的頻寬

增加往返 的頻寬 AWS 將增加傳入閘道和傳出 AWS 雲端的最大資料速率。如果網路速度是閘道組態中的限制因素，而不是其他因素 (例如磁碟速度緩慢或閘道 - 啟動器連線頻寬不佳)，這樣可以改善閘道效能。

> **Note**
>
> 由於此處列出的其他限制因素 (例如快取/上傳緩衝磁碟輸送量、CPU 核心數、RAM 總容量，或啟動器與閘道之間的頻寬)，觀察到的閘道效能可能會低於網路頻寬。此外，閘道的正常操作包含許多為保護資料而採取的動作，這可能會導致觀察到的效能低於網路頻寬。

變更磁碟區組態

針對磁碟區閘道，若您發現新增更多磁碟區至閘道會減少閘道的輸送量，請考慮將磁碟區新增至不同的閘道。尤其是當磁碟區用於高輸送量的應用程式時，請考慮為高輸送量應用程式建立不同的閘道。但是，一般而言，您不應將一個閘道供所有的高輸送量應用程式使用，然後將另一個閘道供所有的低輸送量應用程式使用。若要測量您的磁碟區輸送量，請使用 `ReadBytes` 和 `WriteBytes` 指標。

如需這些指標的詳細資訊，請參閱 測量您應用程式和閘道之間的效能。

最佳化 iSCSI 設定

您可在 iSCSI 啟動器上將 iSCSI 設定最佳化，以提升 I/O 效能。建議您在 `MaxReceiveDataSegmentLength` 和 `FirstBurstLength` 選擇 256 KiB，在 `MaxBurstLength` 選擇 1 MiB。如需關於配置 iSCSI 設定的詳細資訊，請參閱自訂 iSCSI 設定。

> **Note**
>
> 這些建議設定可提升整體效能。但最佳化效能需要的特定 iSCSI 設定，則取決於您使用的備份軟體。如需詳細資訊，請參閱備份軟體的文件。

新增資源到您的應用程式環境

增加您應用程式伺服器和閘道之間的頻寬

iSCSI 啟動器與閘道之間的連線可能會限制您的上傳和下載效能。如果閘道的效能明顯差於預期，而且您已經改善了 CPU 核心數和磁碟輸送量，請考慮：

- 升級您的網路纜線，使其在啟動器和閘道之間擁有更高的頻寬。

若要最佳化閘道效能，請確認您應用程式和閘道之間的頻寬足以供給您應用程式的需求。您可以使用閘道的 `ReadBytes` 和 `WriteBytes` 指標測量總資料輸送量。

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。

安全 in AWS Storage Gateway

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

安全是 AWS 與您之間的共同責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 – AWS 負責保護在 Amazon Web Services Cloud 中執行 AWS 服務的基礎設施。AWS 也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的合規計劃，請參閱AWS 合規計劃的 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。

主題

- in AWS Storage Gateway 的資料保護
- Identity and Access Management for AWS Storage Gateway
- AWS Storage Gateway的合規驗證
- in AWS Storage Gateway 的彈性
- 基礎設施安全 in AWS Storage Gateway
- AWS 安全最佳實務
- 在 中記錄和監控 AWS Storage Gateway

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。 如需歐洲資料保護的詳細資訊，請參閱一般資料保護規則 (GDPR) 中心。

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 的資料加密 AWS KMS

Storage Gateway 使用 SSL/TLS (Secure Socket Layers/Transport Layer Security) 來加密閘道設備與 AWS 儲存之間傳輸的資料。在預設情況下，Storage Gateway 使用 Amazon S3 受管加密金鑰 (SSE-S3) 在伺服器端加密存放在 Amazon S3 中的所有資料。您可以選擇使用 Storage Gateway API 來設定閘道，使用伺服器端加密搭配 AWS Key Management Service (SSE-KMS) 金鑰來加密存放在雲端的資料。

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

加密檔案共享

對於檔案共用，您可以將閘道設定為使用 SSE-KMS，以使用 AWS KMS的管理金鑰來加密物件。如需使用 Storage Gateway API 加密寫入檔案共用的資料的詳細資訊，請參閱 AWS Storage Gateway API 參考中的 CreateNFSFileShare。

加密磁碟區

對於快取和儲存的磁碟區，您可以使用 Storage Gateway API，設定閘道以使用 AWS KMS受管金鑰加密存放在雲端中的磁碟區資料。您可以將一個受管金鑰指定為 KMS 金鑰。您用來加密磁碟區的金輪在磁碟區建立之後就無法變更。若要使用 Storage Gateway API 來加密寫入快取或存放磁碟區的資料，請參閱 AWS Storage Gateway API 參考中的 CreateCachediSCSIVolume 或 CreateStorediSCSIVolume。

加密磁帶

對於虛擬磁帶，您可以使用 Storage Gateway API 設定閘道，以加密存放在雲端的磁帶資料與 AWS KMS受管金鑰。您可以將一個受管金鑰指定為 KMS 金鑰。您用來加密磁帶資料的金輪在磁帶建立之後就無法變更。如需使用 Storage Gateway API 加密寫入虛擬磁帶的資料的相關資訊，請參閱 AWS Storage Gateway API 參考中的 CreateTapes。

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。意即資料會在 Amazon S3 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。
- 如果您刪除或停用 AWS AWS KMS 金鑰或撤銷授予字符，則無法存取磁碟區或磁帶上的資料。如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的刪除 KMS 金鑰。
- 若您從 KMS 加密的磁碟區建立快照，快照也會處於加密狀態。快照會繼承磁碟區的 KMS 金鑰。
- 若您從 KMS 加密的快照建立新的磁碟區，那麼磁碟區也會處於加密狀態。您可以為新的磁碟區指定不同的 KMS 金鑰。

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

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

設定磁碟區的 CHAP 身分驗證

在 Storage Gateway 中，iSCSI 啟動器會連線至您的磁碟區，以做為 iSCSI 目標。Storage Gateway 使用挑戰交握驗證協定 (CHAP) 來驗證 iSCSI 和啟動器連線。CHAP 會要求通過身分驗證方可存取儲存磁碟區目標，藉此防範重送攻擊。針對每個磁碟區目標，您可以定義一或多個 CHAP 登入資料。您可以在 Configure CHAP credentials (設定 CHAP 登入資料) 對話方塊中，針對不同的啟動器檢視和編輯這些登入資料。

設定 CHAP 登入資料

1. 在 Storage Gateway 主控台中，選擇磁碟區，然後選取您要設定 CHAP 憑證的磁碟區。
2. 針對 Actions (動作)，選擇 Configure CHAP authentication (設定 CHAP 身分驗證)。
3. 針對 Initiator name (啟動器名稱)，輸入您啟動器的名稱。名稱的長度必須最少為 1 個字元，最多為 255 個字元。
4. 針對啟動器秘密，提供您要用來驗證您 iSCSI 啟動器的秘密短語。啟動器秘密短語的長度必須最少為 12 個字元，最多為 16 個字元。
5. 針對 Target secret (目標秘密)，提供您要用來驗證您的雙向 CHAP 目標的秘密短語。目標秘密短語的長度必須最少為 12 個字元，最多為 16 個字元。
6. 選擇 Save (儲存) 儲存各個項目。

若要檢視或更新 CHAP 憑證，您必須擁有必要的 IAM 角色許可，才能讓您執行該操作。

檢視和編輯 CHAP 憑證

您可以新增、移除或更新每位使用者的 CHAP 登入資料。若要檢視或編輯 CHAP 憑證，您必須擁有必要的 IAM 角色許可，才能讓您執行該操作，而啟動器目標所連接的閘道必須是正常運作的閘道。

新增 CHAP 登入資料

1. 在 Storage Gateway 主控台中，選擇磁碟區，然後選取您要新增 CHAP 憑證的磁碟區。
2. 針對 Actions (動作)，選擇 Configure CHAP authentication (設定 CHAP 身分驗證)。
3. 在 Configure CHAPS (設定 CHAPS) 頁面中，於個別的方塊中提供 Initiator name (啟動器名稱)、Initiator secret (啟動器秘密) 和 Target secret (目標秘密)，然後選擇 Save (儲存)。

移除 CHAP 登入資料

1. 在 Storage Gateway 主控台中，選擇磁碟區，然後選取您要移除 CHAP 憑證的磁碟區。

2. 針對 Actions (動作)，選擇 Configure CHAP authentication (設定 CHAP 身分驗證)。
3. 按一下您要移除之登入資料旁的 X，然後選擇 Save (儲存)。

更新 CHAP 登入資料

1. 在 Storage Gateway 主控台中，選擇磁碟區，然後選取您要更新 CHAP 的磁碟區。
2. 針對 Actions (動作)，選擇 Configure CHAP authentication (設定 CHAP 身分驗證)。
3. 在 Configure CHAP credentials (設定 CHAP 登入資料) 頁面中，變更您要更新之登入資料的項目。
4. 選擇儲存。

Identity and Access Management for AWS Storage Gateway

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
- 適用於 Storage Gateway 的身分型政策範例
- 故障診斷 AWS Storage Gateway 身分和存取

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 適用於 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，該身分具有對所有 AWS 服務 和 資源的完整存取權。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，或使用來自身分來源的 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 的形式存放在 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《IAM 使用者指南》中的工作階段政策。

多種政策類型

當多種類型的政策套用到請求時，產生的許可會更複雜而無法理解。若要了解如何 AWS 在涉及多種政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

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
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵 (服務特定)	是
ACL	否
ABAC(政策中的標籤)	部分
臨時憑證	是
轉送存取工作階段 (FAS)	是

IAM 功能	AWS SGW 支援
服務角色	是
服務連結角色	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 適用於 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。委託人可以包含帳戶、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以下字首：

```
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 適用於 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的清單，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 適用於 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 適用於 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。

適用於 Storage Gateway 的身分型政策範例

根據預設，使用者和角色沒有建立或修改 AWS SGW 資源的許可。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 等使用服務動作 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 使用者檢視附加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:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
```

```
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

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。

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 IAM 使用者中提供存取權。
- 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。

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。這些措施包括 SOC、PCI、ISO、FedRAMP、HIPAA、MTSC、C5、K-ISMS、ENS High、OSPAR 和 HITRUST CSF。

如需特定合規計劃範圍內 AWS 的服務清單，請參閱AWS 合規計劃範圍內的服務。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，請參閱下載報告 in 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 的彈性

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分隔AZs。與其他雲端供應商不同，這些供應商通常將區域定義為單一資料中心，每個 的多個可用區域設計都 AWS 區域 具有獨特的優勢。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、合規和資料保護。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 km (60 ml) 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 還提供數種功能，以協助支援您的資料彈性和備份需求：

- 使用 VMware vSphere 高可用性 (VMware HA)，協助保護儲存工作負載免於硬體、虛擬層或網路故障。如需詳細資訊，請參閱將 VMware vSphere High Availability 與 Storage Gateway 搭配使用。
- 使用 AWS Backup 來備份您的磁碟區。如需詳細資訊，請參閱備份您的磁碟區。

- 從復原點複製您的磁碟區。如需詳細資訊，請參閱從復原點複製快取磁碟區。

基礎設施安全 in AWS Storage Gateway

作為受管服務， AWS Storage Gateway 受到 Amazon Web Services：安全程序概觀白皮書中所述的 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 管理閘道更新。

AWS 安全最佳實務

AWS 提供許多安全功能，供您在開發和實作自己的安全政策時考慮。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。如果您建立線索，就可以將 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 主控台中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

在您建立帳戶時，系統即會在 Amazon Web Services 帳戶中啟用 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。您可以檢視、搜尋和下載 Amazon Web Services 帳戶中的最近事件。如需詳細資訊，請參閱《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。

如需 Amazon Web Services 帳戶中正在進行事件的記錄 (包含 Storage Gateway 的事件)，請建立線索。追蹤可讓 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 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 從多個區域接收 CloudTrail 日誌檔案，以及從多個帳戶接收 CloudTrail 日誌檔案

所有 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": "AIDAII5AUEPBH2M7JTNVC",
                "arn": "arn:aws:iam::111122223333:user/StorageGateway-team/JohnDoe",
                "accountId": "111122223333",
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                 "userName": "JohnDoe"
               },
                  "eventTime": "2014-12-04T16:19:00Z",
                  "eventSource": "storagegateway.amazonaws.com",
                  "eventName": "ActivateGateway",
                  "awsRegion": "us-east-2",
                  "sourceIPAddress": "192.0.2.0",
                  "userAgent": "aws-cli/1.6.2 Python/2.7.6 Linux/2.6.18-164.el5",
                   "requestParameters": {
                                        "gatewayTimezone": "GMT-5:00",
                                        "gatewayName": "cloudtrailgatewayvtl",
                                        "gatewayRegion": "us-east-2",
                                        "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
                                        "gatewayType": "VTL"
                                             },
                                             "responseElements": {
                                                                    "gatewayARN":
 "arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayvtl"
                                             },
                                             "requestID":
 "54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
                                             "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
                                             "eventType": "AwsApiCall",
                                             "apiVersion": "20130630",
```

```
                                                    "recipientAccountId": "444455556666"
            }]
}
```

以下範例顯示的是展示 ListGateways 動作的 CloudTrail 日誌項目。

```
{
 "Records": [{
               "eventVersion": "1.02",
               "userIdentity": {
                                "type": "IAMUser",
                                "principalId": "AIDAII5AUEPBH2M7JTNVC",
                                "arn": "arn:aws:iam::111122223333:user/StorageGateway-
team/JohnDoe",
                                "accountId:" 111122223333", " accessKeyId ":"
 AKIAIOSFODNN7EXAMPLE",
                                " userName ":" JohnDoe "
                                },

                                " eventTime ":" 2014 - 12 - 03T19: 41: 53Z ",
                                " eventSource ":" storagegateway.amazonaws.com ",
                                " eventName ":" ListGateways ",
                                " awsRegion ":" us-east-2 ",
                                " sourceIPAddress ":" 192.0.2.0 ",
                                " userAgent ":" aws - cli / 1.6.2 Python / 2.7.6
 Linux / 2.6.18 - 164.el5 ",
                                " requestParameters ":null,
                                " responseElements ":null,
                                "requestID ":"
 6U2N42CU37KAO8BG6V1I23FRSJ1Q8GLLE1QEU3KPGG6F0KSTAUU0 ",
                                " eventID ":" f76e5919 - 9362 - 48ff - a7c4 -
 d203a189ec8d ",
                                " eventType ":" AwsApiCall ",
                                " apiVersion ":" 20130630 ",
                                " recipientAccountId ":" 444455556666"
              }]
}
```

為您的閘道進行疑難排解

接下來，您可以找到與閘道、主機平台、磁碟區、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閘道在 Storage Gateway 主控台中離線顯示的問題。
- 故障診斷：閘道啟用期間的內部錯誤 - 了解如何在嘗試啟用 Storage Gateway 時收到內部錯誤訊息。
- 對內部部署閘道問題進行疑難排解 - 了解使用內部部署閘道時可能遇到的典型問題，以及如何允許支援 連線至閘道以協助故障診斷。
- 為 Microsoft Hyper-V 設定進行疑難排解 - 了解在 Microsoft Hyper-V 平台上部署 Storage Gateway 時可能遇到的典型問題。
- 為 Amazon EC2 閘道問題進行疑難排解 - 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。
- 為硬體設備問題進行疑難排解 - 了解如何解決 Storage Gateway 硬體設備可能遇到的問題。
- 對磁碟區問題進行疑難排解 - 尋找您在使用磁碟區時可能遇到的大多數典型問題，以及我們建議您採取的動作來修正這些問題的相關資訊。
- 對高可用性問題進行疑難排解 - 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：閘道離線問題

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

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。

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的最佳實務。

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：

1. 關機閘道。
2. 重設快取磁碟。
3. 重新設定快取儲存的磁碟。

4. 重新啟動閘道。

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，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，請參閱測試閘道對網際網路的連線測試閘道對網際網路的連線。

> **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，則命令會傳回類似以下的回應：

```
$ 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 Time。

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

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 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，則命令會傳回類似以下的回應：

```
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 Time。

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 上的流量來自 Amazon EC2 上 HTTP 代理的 IP 地址。

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 中發現 Amazon Virtual Private Cloud (Amazon VPC) 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。

對內部部署閘道問題進行疑難排解

您可以在下面找到有關使用內部部署閘道時可能遇到的典型問題的資訊，以及如何啟用 支援 以協助對閘道進行故障診斷。

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。	使用虛擬化管理程序用戶端連線到您的主機，尋找閘道 IP 地址。 • 若為 VMware ESXi，VM 的 IP 地址可在 Summary (摘要) 標籤的 vSphere 用戶端中找到。 • 若為 Microsoft Hyper-V，登入本機主控台即可找到 VM 的 IP 地址。 如果仍找不到閘道 IP 地址： • 請檢查 VM 是否開啟。只有在 VM 開啟時，才會將 IP 地址指派給您的閘道。 • 等候 VM 啟動完成。如果您的 VM 才剛開啟，閘道可能需要幾分鐘才能完成開機序列。
您有網路或防火牆的問題。	• 允許閘道使用適當的連接埠。

問題	採取動作
	• 不應啟用 SSL 憑證驗證/檢查。Storage Gateway 使用相互 TLS 身分驗證。如果任何第三方應用程式嘗試攔截/簽署任一憑證，則該身分驗證將會失敗。 • 若您使用防火牆或路由器來篩選或限制網路流量，則必須設定防火牆和路由器，以允許這些服務端點可與 AWS進行傳出通訊。如需網路和防火牆需求的詳細資訊，請參閱 網路與防火牆需求。
當您在 Storage Gateway 管理主控台中按一下繼續啟用按鈕時，您的閘道啟用會失敗。	• 從您的用戶端 ping VM，檢查是否可存取閘道 VM。 • 檢查您的 VM 是否有網際網路的網路連線。否則，您需要設定 SOCKS 代理。如需這項作業的詳細資訊，請參閱為您的內部部署閘道設定 SOCKS5 代理。 • 檢查主機時間是否正確、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，請參閱同步 VM 時間與 Hyper-V 或 Linux KVM 主機時間。 • 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。 • 不應啟用 SSL 憑證驗證/檢查。Storage Gateway 使用相互 TLS 身分驗證。如果任何第三方應用程式嘗試攔截/簽署任一憑證，則該身分驗證將會失敗。 • 確認您的 VM 至少有 7.5 GB 的 RAM。如果 RAM 少於 7.5 GB，閘道配置會失敗。如需詳細資訊，請參閱設定磁碟區閘道的需求。
您需要移除配置為上傳緩衝空間的磁碟。例如，您可能希望減少閘道的上傳緩衝空間，或者您可能需要替換用作上傳緩衝但故障的磁碟。	如需關於移除配置為上傳緩衝空間之磁碟的說明，請參閱 從閘道移除磁碟。

問題	採取動作
您需要改善閘道與 AWS之間的頻寬。	您可以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 Direct Connect 在內部部署閘道和 AWS之間建立專用網路連線。若要測量閘道連線的頻寬 AWS，請使用閘道的 `CloudBytesDownloaded` 和 `CloudBytesUploaded` 指標。如需此主題的詳細資訊，請參閱測量閘道與 之間的效能 AWS。提升網際網路連線能力有助於確保您的上傳緩衝區不會用盡。

閘道的出入輸送量降到零。	• 在 Storage Gateway 主控台的閘道標籤上，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 關閉閘道 VM 所述。重新啟動後，Storage Gateway 主控台之閘道標籤中的 IP 地址清單中的地址，應該符合您從虛擬化管理程序用戶端決定的閘道 IP 地址。
	  • 若為 VMware ESXi，VM 的 IP 地址可在 Summary (摘要) 標籤的 vSphere 用戶端中找到。
	  • 若為 Microsoft Hyper-V，登入本機主控台即可找到 VM 的 IP 地址。
	• 檢查閘道對 的連線 AWS ，如 中所述測試閘道與網際網路的連線。
	• 檢查您閘道的 NIC 組態，並確保所有打算為閘道啟用的介面皆已啟用。若要查看您閘道的網路轉接器組態，請按照設定您的閘道網路中的指示操作，並選取檢視您閘道網路組態的選項。
	
	您可以從 Amazon CloudWatch 主控台檢視在您閘道出入的輸送量。如需測量閘道和 之間輸送量的詳細資訊 AWS，請參閱 測量閘道與之間的效能 AWS。

您無法在 Microsoft Hyper-V 匯入 (部署) Storage Gateway。	請參閱 為 Microsoft Hyper-V 設定進行疑難排解，以了解在 Microsoft Hyper-V 部署閘道的常見問題。

問題	採取動作
您會收到以下訊息：「The data that has been written to the volume in your gateway isn't securely stored at AWS」。	如果您的閘道 VM 是從另一個閘道 VM 的複製或快照所建立，就會收到此訊息。如果不是這種情況，請聯絡 支援。

允許 支援 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，包括啟用 支援 以存取您的閘道，協助您疑難排解閘道問題。預設會停用 支援 存取您的閘道。您可以透過主機的本機主控台提供此存取。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。

允許 支援 存取您的閘道

1. 登入您主機的本機主控台。
   - VMware ESXi：如需詳細資訊，請參閱 使用 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 ， 支援 以便 支援 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** 以登出閘道主控台。
8. 依照提示結束本機主控台。

為 Microsoft Hyper-V 設定進行疑難排解

在 Microsoft Hyper-V 平台上部署 Storage Gateway 時通常可能會遇到的問題如下表所列。

問題	採取動作
您嘗試匯入閘道並收到下列錯誤訊息： 「嘗試匯入虛擬機器時發生伺服器錯誤。匯入失敗。在位置 【...】 下找不到虛擬機器匯入檔案。只有在使用 Hyper-V 建立和匯出虛擬機器時，才能匯入虛擬機器。」	此錯誤的發生原因如下： • 如果您不是指向解壓縮閘道來源檔案的根目錄。您在匯入虛擬機器對話方塊中指定的最後一個部分應為 `AWS-Storage-Gateway` 。例如： `C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\` . • 如已部署閘道，但未選取複製虛擬機器選項及勾選匯入虛擬機器對話方塊中的複製所有檔案選項，則 VM 會建立在您解壓縮閘道檔案的位置，而您無法再次由此位置匯入檔案。為修正此問題，請取得原始的解壓縮閘道來源檔案，然後複製到新的位置。使用新的位置做為匯入來源。 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。

問題	採取動作
您嘗試匯入閘道並收到下列錯誤訊息： 「嘗試匯入虛擬機器時發生伺服器錯誤。匯入失敗。匯入任務無法從 【...】 複製檔案：檔案存在。(0x80070050)"	如已部署閘道，而您嘗試重複使用存放虛擬硬碟檔案和虛擬機器組態檔案的預設資料夾，則會發生此錯誤。若要修正此問題，請在 Hyper-V 設定對話方塊左側面板的伺服器下指定新位置。
您嘗試匯入閘道並收到下列錯誤訊息： 「嘗試匯入虛擬機器時發生伺服器錯誤。匯入失敗。Import failed because the virtual machine must have a new identifier. Select a new identifier and try the import again."。	當您匯入閘道時，請務必選取複製虛擬機器，並勾選匯入虛擬機器對話方塊中的複製所有檔案方塊，為虛擬機器建立新的唯一 ID。
您嘗試啟動閘道 VM 並收到下列錯誤訊息： （嘗試啟動）選取的虛擬機器時發生錯誤。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 設定磁碟區閘道的需求。

問題	採取動作
您嘗試啟動閘道 VM 並收到下列錯誤訊息： （嘗試啟動）選取的虛擬機器時發生錯誤。'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 設定磁碟區閘道的需求。
您的快照和閘道軟體更新出現的次數會和預期的稍有不同。	閘道 VM 的時鐘可能會從實際的時間偏移，稱為時鐘飄移。請使用本機閘道主控台的時間同步選項，檢查並更正 VM 的時間。如需詳細資訊，請參閱同步 VM 時間與 Hyper-V 或 Linux KVM 主機時間。
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。
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。	如需有關解決方法的資訊，請參閱 Microsoft 文件，請參閱開啟 VMQ 時 Windows Server 2012 Hyper-V 主機上虛擬機器的網路效能不佳。

為 Amazon EC2 閘道問題進行疑難排解

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 部署磁碟區閘道的自訂 Amazon EC2 執行個體。

主題

- 您的閘道在一段時間後仍未啟用
- 執行個體清單中找不到您的 EC2 閘道執行個體
- 您建立了 Amazon EBS 磁碟區，但無法連接到您的 EC2 閘道執行個體
- 您無法將啟動器連接到您 EC2 閘道的磁碟區目標
- 當您嘗試新增儲存磁碟區時，收到無磁碟可用的訊息
- 您想要移除配置為上傳緩衝空間的磁碟，以減少上傳緩衝空間
- 您的 EC2 閘道出入輸送量降到零
- 支援 您想要協助對 EC2 閘道進行故障診斷
- 使用 Amazon EC2 序列主控台連接到您的閘道執行個體

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：

- 已於執行個體相關聯的安全群組中啟用連接埠 80。如需新增安全群組規則的詳細資訊，請參閱《Amazon EC2 使用者指南》中的新增安全群組規則。
- 閘道執行個體標示為執行中。在 Amazon 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。

您建立了 Amazon EBS 磁碟區，但無法連接到您的 EC2 閘道執行個體

檢查有問題的 Amazon EBS 磁碟區是否與閘道執行個體位於相同的可用區域中。如果可用區域有差異，請在與您執行個體相同的可用區域中建立新的 Amazon EBS 磁碟區。

您無法將啟動器連接到您 EC2 閘道的磁碟區目標

檢查您啟動執行個體所用的安全群組是否包含以下規則：允許您用於 iSCSI 存取的連接埠。此連接埠通常設定為 3260。如需連線到磁碟區的詳細資訊，請參閱從 Windows 用戶端連線至您的磁碟區。

當您嘗試新增儲存磁碟區時，收到無磁碟可用的訊息

最近啟用的閘道未定義儲存磁碟區。您必須先配置本機磁碟到閘道，用作上傳緩衝和快取儲存，才能定義磁碟區儲存。若為部署到 Amazon EC2 的閘道，本機磁碟為連接到執行個體的 Amazon EBS 磁碟區。此錯誤訊息可能是因為執行個體無定義的 Amazon EBS 磁碟區而產生。

檢查執行閘道的執行個體是否有定義的區塊型儲存裝置。如果只有兩個區塊型儲存裝置 (AMI 隨附的預設裝置)，則應該新增儲存體。如需這項作業的詳細資訊，請參閱部署磁碟區閘道的自訂 Amazon EC2 執行個體。連接兩個或更多 Amazon EBS 磁碟區後，嘗試在閘道上建立磁碟區儲存。

您想要移除配置為上傳緩衝空間的磁碟，以減少上傳緩衝空間

請遵循 判斷要配置的上傳緩衝大小 中的步驟。

您的 EC2 閘道出入輸送量降到零

確認閘道執行個體正在執行。如果執行個體因為重新啟動等原因而啟動，請等待執行個體重新啟動。

此外，請確認閘道 IP 沒有變更。如果執行個體在停止後又重新啟動，則執行個體的 IP 地址可能會變更。在這種情況下，您需要啟用新的閘道。

您可以從 Amazon CloudWatch 主控台檢視在您閘道出入的輸送量。如需測量閘道和 之間輸送量的詳細資訊 AWS，請參閱 測量閘道與 之間的效能 AWS。

支援 您想要協助對 EC2 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，包括啟用 支援 以存取您的閘道，協助您疑難排解閘道問題。預設會停用 支援 存取您的閘道。您可以透過 Amazon EC2 本機主控台提供

此存取。您可以透過 Secure Shell (SSH) 登入 Amazon EC2 本機主控台。若要透過 SSH 成功登入，您執行個體的安全群組必須有開啟 TCP 連接埠 22 的規則。

> **Note**
>
> 如果您將新的規則新增至現有的安全群組，新的規則將套用到使用該安全群組的所有執行個體。如需安全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。

啟用對部署在 Amazon EC2 執行個體上的閘道的 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 ， 支援 以便 支援 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 支援 通知您支援工作階段已完成之前，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。

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。

為硬體設備問題進行疑難排解

下列主題討論您可能會遇到的 Storage Gateway 硬體設備問題，以及疑難排解的建議。

您無法確定服務 IP 地址

嘗試連接到服務時，請務必使用服務的 IP 地址，而非主機 IP 地址。在服務主控台中設定服務 IP 地址，並在硬體主控台設定主機 IP 地址。當您啟動硬體設備時會看到硬體主控台。若要從硬體主控台前往服務主控台，請選擇 Open Service Console (開啟服務主控台)。

如何執行重設成出廠預設值？

如果您需要在裝置上執行重設成出廠預設值，請聯絡 Storage Gateway 硬體設備團隊以請求支援，如下列「支援」部分所述。

如何執行遠端重新啟動？

如果您需要執行裝置的遠端重新啟動，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 Storage Gateway 主控台尋找 Storage Gateway 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. 從清單中選擇您的硬體設備。
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。

對磁碟區問題進行疑難排解

您可以找到使用磁碟區時一般最可能遇到的問題相關資訊，以及我們建議您修正問題所要採取的動作。

主題

- 主控台指出您的磁碟區尚未設定
- 主控台指出您的磁碟區無法還原
- 您的快取閘道無法連接，而您想要復原資料
- 主控台指出您的磁碟區狀態為 PASS THROUGH (傳遞)
- 您想要驗證磁碟區完整性並修復可能的錯誤
- 您磁碟區的 iSCSI 目標未出現在 Windows 磁碟管理主控台
- 您想要變更您磁碟區的 iSCSI 目標名稱
- 您的排程磁碟區快照未出現
- 您需要移除或取代故障的磁碟
- 從您應用程式到磁碟區的輸送量降到零
- 您閘道的快取磁碟發生故障
- 磁碟區快照的 PENDING (擱置) 狀態比預期久
- 高可用性運作狀態通知

主控台指出您的磁碟區尚未設定

如果 Storage Gateway 主控台指出您的磁碟區狀態為未設定上傳緩衝，請在您的閘道新增上傳緩衝容量。如未設定閘道上傳緩衝，您無法使用閘道來存放您的應用程式資料。如需詳細資訊，請參閱為您的閘道設定額外的上傳緩衝或快取儲存體。

主控台指出您的磁碟區無法還原

對於存放的磁碟區，如果 Storage Gateway 主控台指出您的磁碟區狀態為無法還原，您就不能再使用此磁碟區。您可以嘗試在 Storage Gateway 主控台中刪除磁碟區。如果磁碟區上有資料，則可在以最

初建立磁碟區所用 VM 之本機磁碟為基礎建立新磁碟區時，還原資料。當您建立新的磁碟區時，選取 Preserve existing data (保留現有的資料)。請務必在刪除磁碟區前，先刪除等待中的磁碟區快照。如需詳細資訊，請參閱刪除儲存磁碟區的快照。如果在 Storage Gateway 主控台中刪除磁碟區無效，可能是為磁碟區配置的磁碟已從 VM 中不當移除，且無法從設備中移除。

對於快取的磁碟區，如果 Storage Gateway 主控台指出您的磁碟區狀態為無法還原，您就不能再使用此磁碟區。如果磁碟區上有資料，您可以建立磁碟區快照，然後使用該快照還原您的資料，或者從最後一個復原點複製磁碟區。您可以在還原您的資料之後刪除磁碟區。如需詳細資訊，請參閱您的快取閘道無法連接，而您想要復原資料。

對於存放的磁碟區，您可以從建立無法還原之磁碟區所用的磁碟建立新磁碟區。如需詳細資訊，請參閱建立儲存磁碟區。如需磁碟區狀態的資訊，請參閱了解磁碟區狀態和轉換。

您的快取閘道無法連接，而您想要復原資料

當您的閘道無法連線時 (例如，當您關閉它時)，您可以選擇從磁碟區復原點建立快照並使用該快照，或從現有磁碟區的最新復原點複製新的磁碟區。從磁碟區復原點複製比建立快照更迅速且更經濟實惠。如需複製磁碟區的詳細資訊，請參閱從復原點複製快取磁碟區。

Storage Gateway 在快取的磁碟區閘道架構中為每個磁碟區提供復原點。磁碟區復原點是一個時間點，此時的磁碟區所有資料皆一致，而且您可建立快照或複製磁碟區。

主控台指出您的磁碟區狀態為 PASS THROUGH (傳遞)

在某些情況下，Storage Gateway 主控台可能會指出您的磁碟區狀態為傳遞。磁碟區狀態為 PASSTHROUGH (傳遞) 有幾個原因。有些原因需要採取動作，有些不需要。

應該採取動作的時機，例如，如果您磁碟區的狀態為 PASS THROUGH (傳遞)，即表示您的閘道已用盡上傳緩衝空間。若要驗證是否已超過您的上傳緩衝，您可以在 Amazon CloudWatch 主控台中檢視 `UploadBufferPercentUsed` 指標。如需詳細資訊，請參閱 監控上傳緩衝區。如果您的閘道因為上傳緩衝區空間不足而具有傳遞狀態，您應該為閘道配置更多上傳緩衝區空間。新增更多緩衝區空間將導致您的磁碟區自動從傳遞轉換為啟動載入可用。雖然磁碟區的狀態為引導，但閘道會讀取完磁碟區的磁碟資料、將此資料上傳至 Amazon S3 並視需要趕上。當閘道趕上並將磁碟區資料儲存到 Amazon S3 後，磁碟區的狀態就會變成可用，快照可再次啟動。請注意，當您的磁碟區狀態為 PASS THROUGH (傳遞) 或 BOOTSTRAPPING (引導) 時，您可以持續從磁碟區磁碟讀取和寫入資料。如需新增更多上傳緩衝空間的詳細資訊，請參閱判斷要配置的上傳緩衝大小。

您可以在閘道的上傳緩衝設定閾值警示，於上傳緩衝超過以前先採取動作。如需詳細資訊，請參閱設定閘道上傳緩衝區的閾值警示上限。

反之，當磁碟區狀態為 PASS THROUGH (傳遞) 時，若磁碟區在等待引導，原因是另一個磁碟區處於引導中，即為不需要採取動作的範例。閘道會一次引導一個磁碟區。

PASS THROUGH (傳遞) 狀態有時可能代表上傳緩衝的配置磁碟失效。如果是這種情況，您應該移除磁碟。如需詳細資訊，請參閱使用磁碟區閘道儲存資源。如需磁碟區狀態的資訊，請參閱了解磁碟區狀態和轉換。

您想要驗證磁碟區完整性並修復可能的錯誤

如果您想要驗證磁碟區完整性並修正可能的錯誤，而您的閘道使用 Microsoft Windows 啟動器連線到其磁碟區，您可以使用 Windows CHKDSK 公用程式來驗證磁碟區的完整性並修復磁碟區中任何錯誤。當偵測到磁碟區損毀時，Windows 會自動執行 CHKDSK 工具，或者您可以自己執行它。

您磁碟區的 iSCSI 目標未出現在 Windows 磁碟管理主控台

如果您磁碟區的 iSCSI 目標未出現在 Windows 的磁碟管理主控台中，請檢查您是否已設定閘道的上傳緩衝。如需詳細資訊，請參閱為您的閘道設定額外的上傳緩衝或快取儲存體。

您想要變更您磁碟區的 iSCSI 目標名稱

如果您想要變更您磁碟區的 iSCSI 目標名稱，您必須刪除該磁碟區，並以新的目標名稱再次新增它。如果這樣做，您就可以保留磁碟區中的資料。

您的排程磁碟區快照未出現

如果您的磁碟區排程快照未出現，請檢查您的磁碟區狀態是否為 PASSTHROUGH (傳遞)，或閘道的上傳緩衝是否剛好在排定快照時間前填滿。您可以在 Amazon CloudWatch 主控台中檢查閘道的 `UploadBufferPercentUsed` 指標，並建立此指標的警示。如需詳細資訊，請參閱監控上傳緩衝區及設定閘道上傳緩衝區的閾值警示上限。

您需要移除或取代故障的磁碟

如果您需要取代故障的磁碟區磁碟，或取代不需要的磁碟區，您應該先使用 Storage Gateway 主控台移除磁碟區。如需詳細資訊，請參閱刪除磁碟區。然後，使用虛擬化管理程序用戶端移除支援儲存裝置：

- 若為 VMware ESXi，請移除支援儲存裝置，如刪除儲存磁碟區中所述。
- 若為 Microsoft Hyper-V，請移除支援儲存裝置。

從您應用程式到磁碟區的輸送量降到零

如果從您應用程式到磁碟區的輸送量已降到零，請嘗試下列作業：

- 如果您使用的是 VMware vSphere 用戶端，請檢查您磁碟區的 Host IP (主機 IP) 地址是否符合 Summary (摘要) 標籤之 vSphere 用戶端所顯示的其中一個地址。您可以在磁碟區的詳細資訊標籤中，在 Storage Gateway 主控台中找到儲存磁碟區的主機 IP 地址。IP 地址可能發生差異，例如，當您將新的靜態 IP 地址指派給您的閘道時。如有差異，請從 Storage Gateway 主控台重新啟動您的閘道，如 關閉閘道 VM 所述。重新啟動後，儲存磁碟區之 ISCSI Target Info (ISCSI 目標資訊) 標籤中的 Host IP (主機 IP) 地址，應該符合閘道 Summary (摘要) 標籤之 vSphere 用戶端中顯示的 IP 地址。
- 如果磁碟區的 Host IP (主機 IP) 方塊中沒有 IP 地址，而閘道已上線。例如，如果您建立與閘道網路轉接器 IP 地址相關聯的磁碟區，且閘道有兩個或更多的網路轉接器，就可能發生這種狀況。當您移除或停用與磁碟區相關聯的 NIC 時，IP 地址可能不會顯示在主機 IP 方塊中。為解決此問題，請刪除磁碟區，然後重新予以建立，以便保留現有的資料。
- 檢查您應用程式使用的 iSCSI 啟動器是否正確映射到儲存磁碟區的 iSCSI 目標。如需連線至儲存磁碟區的詳細資訊，請參閱從 Windows 用戶端連線至您的磁碟區。

您可從 Amazon CloudWatch 主控台檢視磁碟區的輸送量並建立警示。如需測量您應用程式到磁碟區之輸送量的詳細資訊，請參閱測量您應用程式和閘道之間的效能。

您閘道的快取磁碟發生故障

如果您閘道的一個或多個快取磁碟發生故障，閘道會阻止對虛擬磁帶和磁碟區的讀寫操作。若要還原正常功能，請依照下列說明重新設定閘道：

- 如果快取磁碟無法存取或無法使用，請從閘道組態中刪除磁碟。
- 如果快取磁碟仍然可以存取且可使用，請將其重新連線到閘道。

> **Note**
>
> 當閘道恢復正常功能時，如果刪除具有清除資料 (亦即快取磁碟和 Amazon S3 中的資料同步處理的快取磁碟、磁帶或磁碟區)仍可用。例如，如果您的閘道有三個快取磁碟，而您刪除兩個快取磁碟，則清除的磁帶或磁碟區將會有「可用」狀態。其他磁帶和磁碟區將具有無法復原的狀態。

如果您使用暫時磁碟做為閘道的快取磁碟，或將快取磁碟掛載到暫時磁碟機上，當您關閉閘道時，快取磁碟將會遺失。在快取磁碟和 Amazon S3 不同步時關閉閘道可能會導致資料遺失。因此，我們建議您不要使用臨時磁碟機或磁碟。

磁碟區快照的 PENDING (擱置) 狀態比預期久

如果磁碟區快照保持 PENDING (擱置) 狀態的時間過久，很可能是閘道 VM 已經意外損毀，或是磁碟區狀態已變更為 PASS THROUGH (傳遞) 或 IRRECOVERABLE (無法還原)。如果是其中任一狀況，快照會保持 PENDING (擱置) 狀態，且快照不會成功完成。在這些情況下，我們建議您刪除快照。如需詳細資訊，請參閱刪除儲存磁碟區的快照。

當磁碟區傳回 AVAILABLE (可用) 狀態時，請建立新的磁碟區快照。如需磁碟區狀態的資訊，請參閱了解磁碟區狀態和轉換。

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，請參閱對高可用性問題進行疑難排解。

對高可用性問題進行疑難排解

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。您也可以在閘道維護週期期間使用閘道軟體來重新啟動。

採取動作

如果重新啟動的時間在閘道所設定之維護開始時間的 10 分鐘以內，這可能是正常的情況，而不是任何問題的徵兆。如果重新啟動很常在維護時段外發生，請檢查閘道是否已手動重新啟動。

通知：HardReboot

當閘道 VM 意外重新啟動時，您可能會收到 `HardReboot` 通知。這種重新啟動可能是因為電源中斷、硬體故障或其他事件。若是 VMware 閘道，由 vSphere High Availability Application Monitoring 執行的重設可能會啟動此事件。

採取動作

當閘道在這種環境中執行時，請檢查 `HealthCheckFailure` 通知是否存在，並參閱 VM 的 VMware 事件記錄。

通知：HealthCheckFailure

若是 VMware vSphere HA 上的閘道，當運作狀態檢查失敗且請求 VM 重新啟動時，您可能會收到 `HealthCheckFailure` 通知。此事件也會在監控可用性的測試期間發生，並顯示於 `AvailabilityMonitorTest` 通知中。在此情況下，則預期會收到`HealthCheckFailure` 通知。

> **Note**
>
> 此通知僅適用於 VMware 閘道。

採取動作

如果此事件在沒有 `AvailabilityMonitorTest` 通知的情況下重複發生，請檢查您的 VM 基礎設施是否有問題 (儲存空間、記憶體等)。如果您需要其他協助，請聯絡 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。

磁碟區閘道的最佳實務

本節包含下列主題，提供使用閘道、本機磁碟、快照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 為您的閘道進行疑難排解。

主題

- 最佳實務：復原您的資料
- 清除不必要的資源
- 減少磁碟區上的計費儲存量

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。

主題

- 從非預期的虛擬機器關機復原
- 從故障的閘道或 VM 復原資料
- 從無法復原的磁碟區復原資料
- 從故障的快取磁碟復原資料
- 從損毀的檔案系統復原資料
- 從無法存取的資料中心復原資料

從非預期的虛擬機器關機復原

如果您的 VM 因非預期原因關閉 (例如停電)，您的閘道就會無法連接。當電力和網路連線還原後，您的閘道就可以連接並開始正常運作。下列是您可在此時採取的步驟，有利於復原您的資料：

- 如果中斷導致網路連線問題，您可以故障診斷此問題。如需如何測試網路連線的資訊，請參閱測試閘道與網際網路的連線。
- 針對快取磁碟區設定，當您的閘道可以連接時，您的磁碟區會變成引導狀態。此功能可確保您的本機儲存資料持續與 同步 AWS。如需此狀態的詳細資訊，請參閱了解磁碟區狀態和轉換。
- 如果您的閘道發生磁碟區或磁帶故障和問題，以致非預期關機，您可以復原您的資料。有關如何復原資料的資訊，請參閱下列適用於您案例的各節。

從故障的閘道或 VM 復原資料

如果您的閘道或虛擬機器故障，您可以復原已上傳至 AWS 並存放在 Amazon S3 磁碟區的資料。若為快取磁碟區閘道，您是從復原快照還原資料。針對存放的磁碟區閘道，您可以從您磁碟區的最新 Amazon EBS 快照復原資料。針對磁帶閘道，您可從復原點將一個或多個磁帶復原至新的磁帶閘道。

如果您無法連接快取磁碟區閘道，您可以使用下列步驟從復原快照復原資料：

1. 在 中 AWS 管理主控台，選擇故障的閘道，選擇您要復原的磁碟區，然後從中建立復原快照。
2. 部署並啟用新的磁碟區閘道。或者，如果您現有的磁碟區閘道可正常運作，您可以使用該閘道來復原磁碟區資料。
3. 尋找您建立的快照，將它還原到運作正常的閘道新磁碟區。
4. 將新的磁碟區掛載為您內部部署應用程式伺服器的 iSCSI 裝置。

如需如何從復原快照復原快取磁碟區資料的詳細資訊，請參閱您的快取閘道無法連接，而您想要復原資料。

從無法復原的磁碟區復原資料

如果您的磁碟區狀態為 IRRECOVERABLE (無法復原)，您就不能再使用此磁碟區。

針對存放磁碟區，您可以使用下列步驟，將無法復原的磁碟區資料擷取到新的磁碟區：

1. 從建立無法復原之磁碟區所用的磁碟建立新磁碟區。
2. 當您建立新的磁碟區時，保留現有的資料。

3. 刪除所有無法復原磁碟區的待定快照任務。
4. 從閘道刪除無法復原的磁碟區。

若為快取磁碟區，我們建議您使用最新的復原點複製新的磁碟區。

如需如何將無法復原磁碟區的資料擷取到新磁碟區的詳細資訊，請參閱主控台指出您的磁碟區無法還原。

從故障的快取磁碟復原資料

如果您的快取磁碟發生故障，我們建議根據您的情況，使用下列步驟復原您的資料：

- 如果發生故障的原因是快取磁碟已從您的主機移除，請關閉閘道、重新新增磁碟並重新啟動閘道。
- 如果快取磁碟損毀或無法存取，請關閉閘道、重設快取磁碟、重設快取儲存磁碟並重新啟動閘道。

從損毀的檔案系統復原資料

如果您的檔案系統毀損，您可以使用 **fsck** 命令檢查您的檔案系統錯誤並予以修復。如果您可以修復檔案系統，您就可以從檔案系統的磁碟區復原資料，如下所述：

1. 關閉您的虛擬機器，然後使用 Storage Gateway 管理主控台建立復原快照。此快照代表存放於 的最新資料 AWS。

   > **Note**
   >
   > 如果您的檔案系統無法修復，或快照建立程序無法順利完成，您可使用此快照做為後援。

   如需如何建立復原快照的資訊，請參閱您的快取閘道無法連接，而您想要復原資料。
2. 使用 **fsck** 命令檢查您的檔案系統錯誤並嘗試修復。
3. 重新啟動您的閘道 VM。
4. 當您的虛擬化管理程序主機開始啟動時，請按住 shift 鍵進入 GRUB 開機選單。
5. 在選單中按下 **e** 編輯。
6. 選擇核心行 (第二行)，然後按下 **e** 編輯。
7. 將下列選項附加到核心命令列：**init=/bin/bash**。使用空間區隔之前的選項和您剛才附加的選項。

8. 刪除這兩行 `console=`，確保刪除 = 符號後面的所有值，包括以逗號分隔的值。
9. 按下 **`Return`** 以儲存變更。
10. 按下 **`b`** 以修改過的核心選項來將電腦開機。您的電腦會開機到 `bash#` 提示。
11. 輸入 **`/sbin/fsck -f`** ***`/dev/sda1`*** 依照提示手動執行此命令，以檢查並修復您的檔案系統。如果指令不適用於 `/dev/sda1` 路徑，您可以使用 **`lsblk`** 來判定 `/` 的根檔案系統裝置，並改用該路徑。
12. 當檔案系統完成檢查和修復之後，重新啟動執行個體。GRUB 設定會還原為原始值，閘道則正常開機。
13. 等待正從原始閘道逐漸完成的快照，然後驗證快照資料。

您可以依現狀繼續使用原始磁碟區，或者您可以根據復原快照或已完成的快照，使用新磁碟區來建立新的閘道。或者，您可以從這個磁碟區中任何已完成的快照建立新磁碟區。

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。

從無法存取之資料中心的磁碟區閘道復原資料

1. 在 Amazon EC2 主機上建立和啟用新的磁碟區閘道。如需詳細資訊，請參閱部署磁碟區閘道的自訂 Amazon EC2 執行個體。

   > **Note**
   >
   > Amazon EC2 執行個體無法託管閘道存放的磁碟區。

2. 建立新的磁碟區並選擇 EC2 閘道做為目標閘道。如需詳細資訊，請參閱建立儲存磁碟區。

   根據 Amazon EBS 快照或從您想復原之最新磁碟區復原點進行複製來建立新的磁碟區。

   如果您的磁碟區是以快照為基礎，請提供快照 ID。

   如果您是從復原點複製磁碟區，請選擇來源磁碟區。

清除不必要的資源

如果您已建立閘道做為範例練習或測試，請考慮清除，避免產生意外或非必要的費用。

清除不需要的資源

1. 刪除任何快照。如需說明，請參閱刪除儲存磁碟區的快照。
2. 除非您計劃繼續使用閘道，否則請將其刪除。如需詳細資訊，請參閱刪除您的閘道並移除相關聯的資源。
3. 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。

減少磁碟區上的計費儲存量

刪除檔案系統中的檔案不一定會刪除基本區塊型儲存裝置中的資料，或降低磁碟區上所存放的資料量。如果您要降低磁碟區上的計費儲存數量，建議您將檔案覆寫為零，以將儲存壓縮至極少的實際儲存量。Storage Gateway 根據壓縮儲存來收取磁碟區用量費用。

> **Note**
>
> 如果您使用刪除工具將磁碟區上的資料覆寫為隨機資料，則不會降低使用量。這是因為隨機資料無法壓縮。

其他 Storage Gateway 資源

本節說明 AWS 和第三方軟體、工具和資源，可協助您設定或管理閘道，以及 Storage Gateway 配額。

主題

- 部署和設定閘道 VM 主機 - 了解如何為您的閘道部署和設定虛擬機器主機。
- 使用磁碟區閘道儲存資源 - 了解與磁碟區閘道儲存資源相關的程序，例如移除本機磁碟和管理閘道 Amazon EC2 執行個體上的 Amazon EBS 磁碟區。
- 取得閘道的啟用金鑰 - 了解如何尋找部署新閘道時需要提供的啟用金鑰。
- 連線 iSCSI 啟動器 - 了解如何使用公開為網際網路小型電腦系統界面 (iSCSI) 目標的磁碟區或虛擬磁帶庫 (VTL) 裝置。
- Direct Connect 搭配 Storage Gateway 使用 - 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。
- 取得閘道設備的 IP 地址 - 了解在何處尋找閘道的虛擬機器主機 IP 地址，當您部署新的閘道時，您需要提供這些地址。
- IPv6 支援 - 了解 IPv6 的需求。
- 了解 Storage Gateway 資源和資源 ID - 了解如何 AWS 識別 Storage Gateway 建立的資源和子資源。
- 為 Storage Gateway 資源加上標籤 - 了解如何使用中繼資料標籤來分類您的資源，並讓它們更容易管理。
- 使用 Storage Gateway 的開放原始碼元件 - 了解用於提供 Storage Gateway 功能的第三方工具和授權。
- AWS Storage Gateway 配額 - 了解磁碟區閘道的限制和配額，包括磁碟區大小和數量的最大限制，以及本機磁碟大小建議。

部署和設定閘道 VM 主機

本節中的主題說明如何設定和管理 Storage Gateway 設備的虛擬機器主機，包括在 VMware、Hyper-V 或 Linux KVM 上執行的現場部署設備，以及在 AWS 雲端 Amazon EC2 執行個體上執行的設備。

主題

- 部署磁碟區閘道的預設 Amazon EC2 主機 - 了解如何使用預設規格在 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體上部署和啟用磁碟區閘道。
- 部署磁碟區閘道的自訂 Amazon EC2 執行個體 - 了解如何使用自訂設定在 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體上部署和啟用磁碟區閘道。
- 修改 Amazon EC2 執行個體中繼資料選項 - 了解如何設定 Amazon EC2 閘道執行個體以接受使用 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)。
- 同步 VM 時間與 Hyper-V 或 Linux KVM 主機時間 - 了解如何檢視內部部署 Hyper-V 或 Linux KVM 閘道虛擬機器的時間，並將其同步至網路時間通訊協定 (NTP) 伺服器。
- 同步 VM 時間與 VMware 主機時間 - 了解如何檢查 VMware 閘道虛擬機器的主機時間，並視需要設定時間並設定主機將其時間自動同步至網路時間通訊協定 (NTP) 伺服器。
- 在 VMware 主機上設定全虛擬化 - 了解如何設定 Storage Gateway 設備的 VMware 主機平台，以使用全虛擬化網際網路小型電腦系統界面協定 (iSCSI) 控制器。
- 為您的閘道設定網路轉接器 - 了解如何重新設定閘道以使用 VMXNET3 (10 GbE) 網路轉接器，或使用多個網路轉接器，以便存取 fron nultiple IP 地址。
- 將 VMware vSphere High Availability 與 Storage Gateway 搭配使用 - 了解如何透過設定 Storage Gateway 與 VMware vSphere 高可用性搭配使用，保護您的儲存工作負載免於硬體、Hypervisor 或網路故障。

部署磁碟區閘道的預設 Amazon EC2 主機

本主題列出使用預設規格部署 Amazon EC2 主機的步驟。

您可以在 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體上部署和啟用磁碟區閘道。 AWS Storage Gateway Amazon Machine Image (AMI) 會以社群 AMI 的形式提供。

> **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。

1. 若要設定 Amazon EC2instance，請在工作流程的平台選項區段中選擇 Amazon EC2 做為主機平台。如需設定 Amazon EC2 執行個體的指示，請參閱部署 Amazon EC2 執行個體以託管磁碟區閘道。

2. 選取啟動執行個體以在 Amazon EC2 主控台中開啟 AWS Storage Gateway AMI 範本，並自訂其他設定，例如執行個體類型、網路設定和設定儲存。
3. 或者，您可以選取 Storage Gateway 主控台中的使用預設設定，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**
     >
     > 只有當 VPC 子網路從 VPC 管理主控台啟用了自動指派公用 IPv4 地址設定時，VPC 子網路才會顯示在下拉式清單中。

     - 自動分配公用 IP：已啟動

   EC2 安全群組會建立關聯 EC2 執行個體。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 iSCSI 目標只能從與閘道位於相同 VPC 中的主機存取。如果 iSCSI 目標需要從 VPC 以外的主機存取，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				

連接埠	通訊協定	檔案系統協定				
3260	TCP	iSCSI				

- 設定儲存

預設設定	AMI 根磁碟區	磁碟區 2 快取	磁碟區 3 快取			
裝置名稱		'/dev/sdb'	'/dev/sdc'			
大小	80 GiB	165 GiB	150 GiB			
磁碟區類型	gp3	gp3	gp3			
IOPS	3000	3000	3000			
在終止時刪除	是	是	是			
加密	否	否	否			
輸送量	125	125	125			

部署磁碟區閘道的自訂 Amazon EC2 執行個體

您可以在 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體上部署和啟用磁碟區閘道。 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。
> 磁碟區閘道 AMIs 使用以下命名慣例。附加至 AMI 名稱的版本編號會隨著每個版本版本而變更。
> `aws-storage-gateway-CLASSIC-2.9.0`

若要部署 Amazon EC2 執行個體以託管磁碟區閘道

1. 使用 Storage Gateway 主控台開始設定新閘道。如需指示，請參閱設定磁碟區閘道。進入平台選項區段時，選擇 Amazon EC2 做為主機平台，然後使用下列步驟啟動將託管您的磁碟區閘道的 Amazon EC2 執行個體。

   > **Note**
   >
   > Amazon EC2 主機平台僅支援快取磁碟區。儲存磁碟區閘道無法部署在 EC2 執行個體上。

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 快速啟動預設規格的詳細資訊，請參閱 Amazon EC2 的。Amazon EC2 的快速啟動組態規格。

3. 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。

4. 在執行個體類型區段中，從執行個體類型清單中，為執行個體選擇硬體組態。硬體組態必須符合特定的最低需求，才能支援閘道。建議您從 m5.xlarge 執行個體類型開始，它符合您閘道正常運作的最低硬體要求。如需詳細資訊，請參閱Amazon EC2 執行個體類型的需求。

   必要時，您可以在啟動執行個體之後調整執行個體的大小。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的調整執行個體的大小。

   > **Note**
   >
   > 有些執行個體類型，特別是 i3 EC2，會使用 NVMe SSD 磁碟。它們會在您啟動或停止磁碟區閘道時產生問題；例如，您可能會遺失快取的資料。監控 `CachePercentDirty` Amazon CloudWatch 指標，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。

5. 在金鑰對 (登入) 區段中，針對金鑰對名稱(必要)，選取您要用來安全連線至執行個體的金鑰對。如有必要，您可以建立新的金鑰對。如需詳細資訊，請參閱《適用於 Linux 執行個體的 Amazon Elastic Compute Cloud 使用者指南》中的建立金輪對。

6. 在網路設定區段中，檢閱預先設定的設定值，然後選擇編輯以變更下列欄位：

a. 對於 VPC：必要項目，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。

b. (選用) 對於子網路，請選擇要在其中啟動 Amazon EC2 執行個體的子網路。

c. 在 Auto-assign Public IP (自動指派公有 IP) 中，選擇 Enable (啟用)。

7. 在防火牆 (安全群組) 子區段中，檢閱預先設定的設定值。您可以視需要變更要為 Amazon EC2 執行個體建立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。

8. 在傳入安全群組規則子區段中，新增防火牆規則，以開啟用戶端將用來連線至執行個體的連接埠。如需磁碟區閘道所需連接埠的詳細資訊，請參閱連接埠需求。如需詳細資訊，請參閱《適用於 Linux 執行個體的 Amazon Elastic Compute Cloud 使用者指南》中的安全群組規則。

> **Note**
>
> 磁碟區閘道需要開放 TCP 連接埠 80 以供傳入流量使用，並在閘道啟動期間進行一次性 HTTP 存取。啟用後，您可以關閉此連接埠。
> 此外，您必須為 iSCSI 存取開啟 TCP 連接埠 3260。

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，您還必須新增至少一個具有 165 GiB 容量的 Amazon EBS 磁碟區以供快取儲存使用，以及至少一個具有 150 GiB 容量的 Amazon EBS 磁碟區以供上傳緩衝區使用。為了提高效能，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 主控台中的執行個體頁面，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用 IPv4 地址，然後傳回 Storage Gateway 主控台中的設定閘道頁面，繼續設定磁碟區閘道。

您可以使用 Storage Gateway 閘道磁碟區閘道的 AMI ID。 AWS Systems Manager

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。如需指示，請參閱設定磁碟區閘道。當您到達平台選項區段時，請選擇 Amazon EC2 做為主機平台，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 中查看您 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，在快取磁碟區閘道或存放磁碟區閘道`/aws/service/storagegateway/ami/CACHED/latest`的命名空間下查詢 Systems Manager 公`/aws/service/storagegateway/ami/STORED/latest`有參數。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/
  STORED/latest
  ```

  CLI 命令會傳回類似以下的輸出。

  ```
  {
      "Parameter": {
          "Type": "String",
          "LastModifiedDate": 1561054105.083,
          "Version": 4,
          "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/
  STORED/latest",
          "Name": "/aws/service/storagegateway/ami/STORED/latest",
          "Value": "ami-123c45dd67d891000"
      }
  }
  ```

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，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確切差異，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。

在 VMware 主機上設定全虛擬化

下列程序說明如何設定 Storage Gateway 設備的 VMware 主機平台，以使用全虛擬化網際網路小型電腦系統界面協定 (iSCSI) 控制器。全虛擬 iSCSI 控制器是高效能儲存控制器，可能會導致更高的輸送量和更低的 CPU 使用量。這些控制器最適合高效能儲存環境。當您以這種方式設定 iSCSI 控制器時，Storage Gateway 虛擬機器會與主機作業系統搭配使用，以允許閘道主控台識別您新增至虛擬機器的虛擬磁碟。

> **Note**
>
> 您需要完成此步驟，以避免在閘道主控台中設定這些磁碟時發生問題。

將 VMware 主機平台設定為使用全虛擬化控制器

1. 在 VMware vSphere 用戶端中，在應用程式視窗左側導覽窗格中的閘道虛擬機器名稱上按一下滑鼠右鍵，以開啟內容選單，然後選擇編輯設定。
2. 在虛擬機器屬性對話方塊中，選擇硬體索引標籤。
3. 在硬體索引標籤上，選取 SCSI 控制器 0，然後選擇變更類型。
4. 在變更 SCSI 控制器類型對話方塊中，選取 VMware Paravirtual SCSI 控制器類型，然後選擇確定以儲存組態。

為您的閘道設定網路轉接器

您可以設定 Storage Gateway，讓多個 IP 地址存取它。設定您的閘道使用多個網路轉接器以完成此作業。

為多個 NIC 設定閘道

如果您設定閘道使用多個網路轉接器 (NIC)，它就可由多個 IP 地址存取。建議您在下列其中一種狀況中執行此作業：

- 最大化輸送量 – 當網路轉接器遇到瓶頸時，建議您最大化閘道輸送量。
- 分隔應用程式：您可能需要區隔應用程式寫入閘道磁碟區的方式。例如，您可以選擇只讓關鍵儲存應用程式使用一種為您閘道定義的特定轉接器。
- 限制網路 – 您的應用程式環境可能需要您保留 iSCSI 目標，而連線到它們之啟動器所在的隔離網路，與閘道和 AWS的通訊網路不同。

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（也就是預設閘道）。除此轉接器外，啟動器必須和包含 iSCSI 目標的轉接器位於相同的子網路中 (轉接器連線到這些 iSCSI 目標)。否則，可能無法與預定目標通訊。如果在用於通訊的相同轉接器上設定目標 AWS，則該目標和 AWS 流量的 iSCSI 流量將流經相同的轉接器。

當您設定一個介面卡連線到 Storage Gateway 主控台，然後新增第二個介面卡時，Storage Gateway 會自動設定路由表使用第二個介面卡為慣用的路由。如需如何設定多個轉接器的指示，請參閱下列各節。

- 在 VMware ESXi 主機上設定多個網路轉接器
- 在 Microsoft Hyper-V 主機上設定多個網路轉接器

在 VMware ESXi 主機上設定多個網路轉接器

下列程序假設您的閘道 VM 已定義一個 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 VM 本機主控台上執行任務

在 Microsoft Hyper-V 主機上設定多個網路轉接器

下列程序假設您的閘道 VM 已定義一個網路轉接器，而且您將會新增第二個轉接器。此程序顯示如何為 Microsoft Hyper-V 主機新增轉接器。

在 Microsoft Hyper-V 主機中設定您的閘道，以使用額外的網路轉接器

1. 在 Storage Gateway 主控台上，關閉閘道。
2. 在 Microsoft Hyper-V Manager 中，從虛擬機器面板選取閘道 VM。
3. 如果閘道 VM 尚未關閉，請在 VM 名稱上按一下滑鼠右鍵以開啟內容選單，然後選擇關閉。
4. 在閘道 VM 名稱上按一下滑鼠右鍵以開啟內容功能表，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。
8. 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。
9. 使用 Storage Gateway 主控台開啟閘道。
10. 在 Storage Gateway 主控台的導覽面板中，選擇閘道，然後選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 VM 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。

vSphere HA 的運作方式是將虛擬機器及其所在的主機集區到叢集中，以提供備援。叢集中的主機會受到監控，如果發生故障，則會在替代主機上重新啟動故障主機上的虛擬機器。一般而言，此復原會快速進行，不會遺失資料。如需 vSphere HA 的詳細資訊，請參閱 VMware 文件中的 vSphere HA 運作方式。

> **Note**
>
> 重新啟動故障虛擬機器並在新主機上重新建立 iSCSI 連線所需的時間取決於許多因素，例如主機作業系統和資源負載、磁碟速度、網路連線和 SAN/儲存基礎設施。為了將容錯移轉停機時間降至最低，請實作最佳化閘道效能中概述的建議。
>
> 若要搭配使用 Storage Gateway 與 VMware HA，建議執行下列事項：
>
> - 僅在叢集的一個主機上部署 VMware ESX `.ova` 可下載套件，其中包含 Storage Gateway VM。
> - 部署 `.ova` 套件時，請選取不在某個主機本機的資料存放區。相反地，使用叢集中所有主機都可以存取的資料存放區。如果您選取在主機本機的資料存放區，而且主機故障，則可能無法從叢集的其他主機存取資料來源，而且容錯移轉到另一個主機可能不會成功。
> - 若要防止啟動器在容錯移轉期間與儲存磁碟區中斷連線，請遵循您作業系統的建議 iSCSI 設定。在容錯移轉事件中，可能需要幾秒到幾分鐘的時間，才能在容錯移轉叢集的新主機中啟動閘道 VM。Windows 和 Linux 用戶端的建議 iSCSI 逾時大於容錯移轉發生所需的一般時間。如需自訂 Windows 用戶端逾時設定的詳細資訊，請參閱自訂您的 Windows iSCSI 設定。如需自訂 Linux 用戶端逾時設定的詳細資訊，請參閱自訂您的 Linux iSCSI 設定。
> - 使用叢集處理時，如果您將 `.ova` 套件部署至叢集，則請在系統提示您選取主機時選取主機。或者，您可以直接部署至叢集中的主機。

下列主題說明如何在 VMware HA 叢集中部署 Storage Gateway：

主題

- 設定 vSphere VMware HA 叢集
- 從 Storage Gateway 主控台下載 .ova 映像
- 部署閘道
- (選用) 為叢集上的其他 VM 新增覆寫選項
- 啟用閘道
- 測試 VMware High Availability 組態

設定 vSphere VMware HA 叢集

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

接下來，將 VMware 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。

從 Storage Gateway 主控台下載 .ova 映像

下載您的閘道的 .ova 映像

- 在 Storage Gateway 主控台的設定閘道頁面上，選取您的閘道類型和主機平台，然後使用主控台中提供的連結來下載 .ova，如設定磁碟區閘道所述。

部署閘道

在您設定的叢集中，將 .ova 映像部署到其中一個叢集主機。

部署閘道 .ova 映像

1. 將 .ova 映像部署到叢集中的其中一個主機。
2. 確認您選擇用於根磁碟的資料存放區以及快取可供叢集中的所有主機使用。在 VMware 或內部部署環境中部署 Storage Gateway .ova 檔案時，會將磁碟描述為半虛擬化 SCSI 磁碟。「全虛擬化」是閘道 VM 與主機作業系統搭配運作的模式，讓主控台可以識別您新增至 VM 的虛擬磁碟。

   設定 VM 以使用全虛擬化控制器

   1. 在 VMware vSphere 用戶端中，開啟閘道 VM 的內容 (按右鍵) 選單，然後選擇 編輯設定。
   2. 在 Virtual Machine Properties (虛擬機器屬性) 對話方塊中，選擇 Hardware (硬體) 標籤，並選取 SCSI controller 0 (SCSI 控制器 0)，然後選擇 Change Type (變更類型)。
   3. 在 Change SCSI Controller Type (變更 SCSI 控制器類型) 對話方塊中，選取 VMware Paravirtual (VMware 全虛擬化) SCSI 控制器類型，然後選擇 OK (確定)。

(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

部署閘道的 .ova 後，請啟用您的閘道。做法說明會依各個閘道類型而有所不同。

啟用閘道

- 請遵循下列主題中概述的程式：

  a. 將您的磁碟區閘道連線至 AWS
  b. 檢閱設定並啟用磁碟區閘道
  c. 設定磁碟區閘道

測試 VMware High Availability 組態

啟用閘道後，請測試您的組態。

測試 VMware HA 組態

1. 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，請參閱透過 CloudWatch 日誌群組取得磁碟區閘道運作狀態日誌。

使用磁碟區閘道儲存資源

本節中的主題說明如何管理與磁碟區閘道設備及其虛擬主機平台相關聯的儲存資源。這包括連接至閘道 Hypervisor 主機平台的實體磁碟等資源，以及從 VMware vSphere ESXi、Microsoft Hyper-V 或 Linux 核心型虛擬機器 (KVM) 虛擬化主機移除磁碟的特定程序。這也包括管理連接到閘道 Amazon EC2 執行個體的 Amazon EBS 磁碟區，用於在 AWS 雲端 Amazon EC2 上託管的閘道。

主題

- 從閘道移除磁碟 - 了解如果您需要從閘道的 VMware vSphere ESXi、Microsoft Hyper-V 或 Linux 核心型虛擬機器 (KVM) 虛擬化主機平台移除磁碟時該怎麼做，例如，如果您發生實體磁碟故障。
- 在 Amazon EC2 閘道上管理 Amazon EBS 磁碟區 - 了解如何增加或減少配置做為 Amazon EC2 執行個體上託管之閘道的上傳緩衝區或快取儲存體的 Amazon EBS 磁碟區數量，例如，如果您的應用程式儲存體需要隨著時間增加或減少。

從閘道移除磁碟

雖然不建議從閘道移除基礎磁碟，但建議您從閘道移除磁碟 (例如，您有一個故障的磁碟時)。

從 VMware ESXi 上託管的閘道移除磁碟

您可以使用下列程序，從 VMware 虛擬化管理程序上託管的閘道移除磁碟。

移除針對上傳緩衝區所配置的磁碟 (VMware ESXi)

1. 在 vSphere 用戶端中，開啟內容 (按右鍵) 選單，並選擇閘道 VM 名稱，然後選擇 Edit Settings (編輯設定)。
2. 在 Virtual Machine Properties (虛擬機器屬性) 對話方塊的 Hardware (硬體) 標籤上，選取配置為上傳緩衝區空間的磁碟，然後選擇 Remove (移除)。

   請確認虛擬機器屬性對話方塊中的虛擬裝置節點值具有您先前記下的相同值。這樣做有助於確保您移除正確的磁碟。
3. 選擇 Removal Options (移除選項) 面板中的選項，然後選擇 OK (確定) 來完成移除磁碟程序。

從 Microsoft Hyper-V 上託管的閘道移除磁碟

您可以使用下列程序，從 Microsoft Hyper-V 虛擬化管理程序上託管的閘道移除磁碟。

移除針對上傳緩衝區所配置的基礎磁碟 (Microsoft Hyper-V)

1. 在 Microsoft Hyper-V Manager 中，開啟內容 (按右鍵) 選單，並選擇閘道 VM 名稱，然後選擇 Settings (設定)。
2. 在 Settings (設定) 對話方塊的 Hardware (硬體) 清單中，選取要移除的磁碟，然後選擇 Remove (移除)。

   您新增至閘道的磁碟會出現在硬體清單中的 SCSI 控制器項目下。請確認 Controller (控制器) 和 Location (位置) 值具有您先前記下的相同值。這樣做有助於確保您移除正確的磁碟。

   Microsoft Hyper-V Manager 中所顯示的第一個 SCSI 控制器是控制器 0。
3. 選擇 OK (確定) 以套用變更。

從 Linux KVM 上託管的閘道移除磁碟

若要將磁碟從裝載在 Linux 核心虛擬機器 (KVM) 虛擬機器 Hypervisor 上的閘道分離，您可以使用類似下列其中一個 `virsh` 命令。

```
$ virsh detach-disk domain_name /device/path
```

如需管理 KVM 磁碟的詳細資訊，請參閱 Linux 發行版的說明文件。

在 Amazon EC2 閘道上管理 Amazon EBS 磁碟區

當您一開始設定閘道執行為 Amazon EC2 執行個體時，您已配置 Amazon EBS 磁碟區做為上傳緩衝和快取儲存體使用。一段時間之後，當您的應用程式需要改變時，您可以配置其他的 Amazon EBS 磁碟區做為此用。您也可以移除之前配置的 Amazon EBS 磁碟區，降低您配置的儲存體。如需 Amazon EBS 的詳細資訊，請參閱《Amazon EC2 使用者指南》中的 Amazon Elastic Block Store (Amazon EBS)。 Amazon EC2

在閘道中新增更多儲存體之前，您應該先檢閱如何根據閘道的應用程式需求，決定上傳緩衝和快取儲存的大小。若要執行此作業，請參閱判斷要配置的上傳緩衝大小和判斷要配置的快取儲存體大小。

您可配置為上傳緩衝和快取儲存的儲存體配額有限制。您可以將任意數量的 Amazon EBS 磁碟區連接到您的執行個體，但您只能將這些磁碟區設定為上傳緩衝和快取儲存空間，不得超過這些儲存體的配額。如需詳細資訊，請參閱AWS Storage Gateway 配額。

為您的閘道新增及設定 Amazon EBS 磁碟區

1. 建立 Amazon EBS 磁碟區。如需說明，請參閱《Amazon EC2 使用者指南》中的建立或還原 Amazon EBS 磁碟區。 Amazon EC2
2. 將 Amazon EBS 磁碟區連接至您的 Amazon EC2 執行個體。如需說明，請參閱《Amazon EC2 使用者指南》中的將 Amazon EBS 磁碟區連接至執行個體。 Amazon EC2
3. 設定您新增為上傳緩衝或快取儲存的 Amazon EBS 磁碟區。如需說明，請參閱管理 Storage Gateway 的本機磁碟。

有時候您可能發現您不需要為上傳緩衝所配置的儲存量。

移除 Amazon EBS 磁碟區

> **Warning**
>
> 這些步驟僅適用於分配為上傳緩衝區空間的 Amazon EBS 磁碟區，不適用於分配給快取的磁碟區。

1. 依照關閉閘道 VM 一節中所述的方法關閉閘道。
2. 將 Amazon EBS 磁碟區從 Amazon EC2 執行個體分開。如需說明，請參閱《Amazon EC2 使用者指南》中的從執行個體分離 Amazon EBS 磁碟區。 Amazon EC2

3. 刪除 Amazon EBS 磁碟區。如需說明，請參閱《Amazon EC2 使用者指南》中的刪除 Amazon EBS 磁碟區。 Amazon EC2
4. 依照關閉閘道 VM 一節中所述的方法啟動閘道。

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。

您向閘道 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**
>
> Storage Gateway 硬體設備、虛擬機器映像範本和 Amazon EC2 Amazon 機器映像 (AMI) 已預先設定好接收和回應本頁所述的 Web 請求所需的 HTTP 服務。您不需要或建議您在閘道上安裝任何其他服務。

主題

- Linux (curl)
- Linux (bash/zsh)
- Microsoft 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* - 閘道的 VPC 端點名稱，例如 vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com，或在具有 FIPS 可用性的vpce-050f90485f28f2fd0-iep0e8vq.storagegateway-fips.us-west-2.vpce.amazonaws.com區域中。

標準端點

若要取得標準端點的啟用金鑰：

```
curl "http://gateway_ip_address/?activationRegion=region_code&no_redirect"
```

雙堆疊端點

若要取得雙堆疊端點的啟用金鑰：

IPv4

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=DUALSTACK&ipVersion=ipv4&no_redirect"
```

IPv6

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=DUALSTACK&ipVersion=ipv6&no_redirect"
```

FIPS 端點

若要取得 FIPS 端點的啟用金鑰：

IPv4

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=FIPS_DUALSTACK&ipVersion=ipv4&no_redirect"
```

IPv6

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=FIPS_DUALSTACK&ipVersion=ipv6&no_redirect"
```

VPC 端點

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"
```

使用 FIPS 的 VPC 端點

使用下列命令來取得啟用 FIPS 之 VPC 端點的啟用金鑰。

針對 IPv4 使用以下命令：

```
curl "http://gateway_ip_address/?
activationRegion=region_code&vpcEndpoint=vpc_endpoint&endpointType=FIPS&ipVersion=ipv4&no_redir
```

針對 IPv6 使用以下命令：

```
curl "http://gateway_ip_address/?
activationRegion=region_code&vpcEndpoint=vpc_endpoint&endpointType=FIPS&ipVersion=ipv6&no_redir
```

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

下列範例示範如何使用本機主控台來產生和顯示啟用金鑰。

Amazon Linux 2 (AL2) 型閘道

您可以根據 AL2 為閘道選取標準或 FIPS 端點。

> **Note**
>
> FIPS 端點並非全部可用 AWS 區域。如需詳細資訊，請參閱依服務分類的 FIPS 端點。

從本機主控台取得 AL2-based閘道的啟用金鑰

1. 以管理員身分登入您的本機主控台。
2. 從AWS 設備啟用 - 組態主功能表中，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. 輸入您要啟用閘道 AWS 的區域。
5. 針對網路類型，輸入 1 表示公有，或輸入 2表示 VPC。
6. 對於端點類型，輸入 1 表示標準，或輸入 2 表示聯邦資訊處理標準 (FIPS)。

Amazon Linux 2023 (AL2023) 型閘道

對於以 AL2023 為基礎的閘道，可使用下列端點：

- 標準端點（僅支援 IPv4)
- FIPS 端點（僅支援 IPv4)
- 雙堆疊端點（支援 IPv4 和 IPv6)
- 雙堆疊 FIPS 端點（支援 IPv4 和 IPv6)

如需詳細資訊，請參閱端點類型。

從本機主控台取得 AL2023-based閘道的啟用金鑰

1. 登入您的本機主控台。如果您是從 Windows 電腦連線到您的 Amazon EC2 執行個體，請以 admin 身分登入。

2. 從AWS 設備啟用 - 組態主功能表中，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. 輸入您要啟用閘道 AWS 的區域。
5. 對於網路類型，輸入 1 表示公有或輸入 2 表示 VPC 端點。
6. 對於選取端點類型，啟用 FIPS？，輸入 Y 以啟用 FIPS N 或使用非 FIPS 端點。
7. 對於端點類型，輸入 1 表示標準端點，或輸入 2 表示雙堆疊端點。
    - 對於雙堆疊端點，對於選取 IP 版本或結束：，輸入 1 表示 IPv4 或 2 表示 IPv6。

連線 iSCSI 啟動器

在管理网关时，您将使用作为 Internet 小型计算机系统接口 (iSCSI) 目标公开的卷或虚拟磁带库 (VTL) 设备。对于磁碟區閘道，iSCSI 目标是卷。針對磁帶閘道，目標是 VTL 裝置。在此工作期間，您執行連線至這些目標、自訂 iSCSI 設定、從 Red Hat Linux 用戶端連線，以及設定挑戰交握驗證協定 (Challenge-Handshake Authentication Protocol, CHAP) 這類任務。

主題

- 從 Windows 用戶端連線至您的磁碟區
- 將您的 volumes連接到 Linux 用戶端
- 自訂 iSCSI 設定
- 設定 iSCSI 目標的 CHAP 身分驗證

iSCSI 標準是網際網路通訊協定 (IP) 類型儲存聯網標準，可用於啟動和管理 IP 類型儲存裝置與用戶端之間的連線。下列清單定義一些詞語，用來說明 iSCSI 連線和所含的元件。

iSCSI initiator (iSCSI 啟動器)

iSCSI 網路的用戶端元件。啟動器會將請求傳送至 iSCSI 目標。啟動器可以在軟體或硬體中予以實作。Storage Gateway 僅支援軟體啟動器。

iSCSI target (iSCSI 目標)

iSCSI 網路的伺服器元件，可接收和回應來自啟動器的請求。每個磁碟區都會公開為 iSCSI 目標。只將一個 iSCSI 啟動器連線至一個 iSCSI 目標。

Microsoft iSCSI initiator (Microsoft iSCSI 啟動器)

Microsoft Windows 電腦上的軟體程式，可讓您將用戶端電腦 (即執行要將其資料寫入至閘道之應用程式的電腦) 連線至外部 iSCSI 類型陣列 (即閘道)。使用主機電腦的乙太網路轉接卡建立連線。Microsoft iSCSI 啟動器已透過 Windows Server 2022 上的 Storage Gateway 進行驗證。啟動器內建於作業系統中。

Red Hat iSCSI initiator (Red Hat iSCSI 啟動器)

`iscsi-initiator-utils` Resource Package Manager (RPM) 套件提供 Red Hat Linux 軟體中所實作的 iSCSI 啟動器。此套件包含 iSCSI 通訊協定的伺服器協助程式。

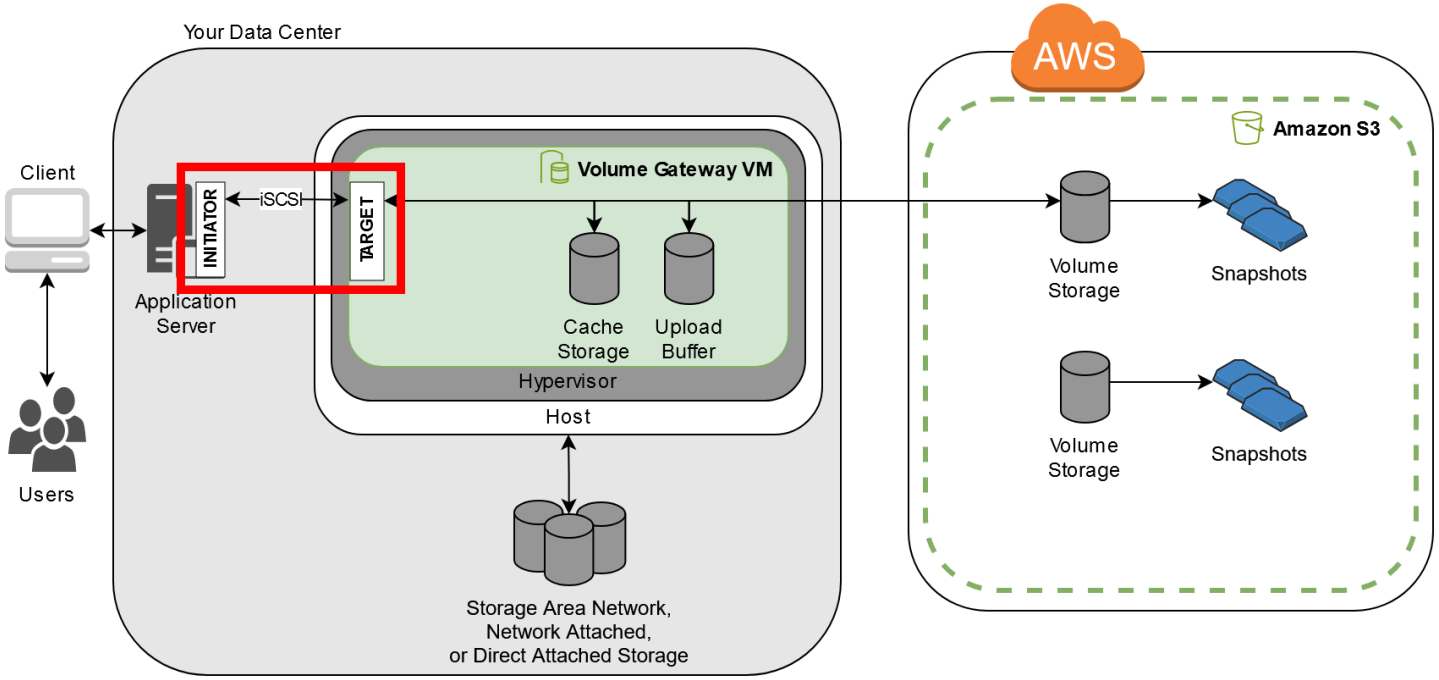
每種類型的閘道都可以連線至 iSCSI 裝置，而且您可以自訂這些連線，如下所述。

從 Windows 用戶端連線至您的磁碟區

磁碟區閘道會將您已針對閘道所建立的磁碟區公開為 iSCSI 目標。如需詳細資訊，請參閱將磁碟區連接到用戶端。

> **Note**
>
> 若要連線至磁碟區目標，閘道必須已設定上傳緩衝區。如果未設定閘道的上傳緩衝區，則磁碟區狀態會顯示為 UPLOAD BUFFER NOT CONFIGURED (未設定上傳緩衝區)。若要設定存放磁碟區設定中閘道的上傳緩衝區，請參閱為您的閘道設定額外的上傳緩衝或快取儲存體。若要設定快取磁碟區設定中閘道的上傳緩衝區，請參閱為您的閘道設定額外的上傳緩衝或快取儲存體。

下圖反白顯示大型 Storage Gateway 架構中的 iSCSI 目標。如需詳細資訊，請參閱磁碟區閘道的運作方式。



您可以從 Windows 或 Red Hat Linux 用戶端連線至磁碟區。您可以選用地設定 CHAP 做為任一用戶端類型。

您的閘道會將磁碟區公開為具有您所指定名稱的 iSCSI 目標，並且前面加上 `iqn.1997-05.com.amazon:`。例如，如果您指定目標名稱 `myvolume`，則您用來連線至磁碟區的 iSCSI 目標是 `iqn.1997-05.com.amazon:myvolume`。如需如何設定應用程式透過 iSCSI 掛載磁碟區的詳細資訊，請參閱從 Windows 用戶端連線至您的磁碟區。

到	請參閱
從 Windows 連線至磁碟區。	連線至 Microsoft Windows 用戶端
從 Red Hat Linux 連線至磁碟區。	連線至 Red Hat Enterprise Linux 用戶端
設定 Windows 和 Red Hat Linux 的 CHAP 身分驗證。	設定 iSCSI 目標的 CHAP 身分驗證

將 Windows 用戶端連線至儲存磁碟區

1. 在 Windows 用戶端電腦的開始選單上，於搜尋程式和檔案方塊中輸入 **`iscsicpl.exe`**，並找到 iSCSI 啟動器程式，然後予以執行。

> **Note**
>
> 您必須擁有用戶端電腦的管理員權利，才能執行 iSCSI 啟動器。

2. 如果系統提示，則選擇是啟動 Microsoft iSCSI 啟動器服務。
3. 在 iSCSI Initiator Properties (iSCSI 啟動器屬性) 對話方塊中，選擇 Discovery (搜索) 標籤，然後選擇 Discover Portal (搜索入口網站)。
4. 在搜索目標入口網站對話方塊中，針對 IP 地址或 DNS 名稱輸入 iSCSI 目標的 IP 地址，然後選擇確定。若要取得閘道的 IP 地址，請檢查 Storage Gateway 主控台上的閘道標籤。如果您已在 Amazon EC2 執行個體上部署閘道，則可以在 Amazon EC2 主控台的描述標籤中找到公有 IP 或 DNS 地址。

   IP 地址現在會出現在 Discovery (搜索) 標籤的 Target portals (目標入口網站) 清單中。

   > **Warning**
   >
   > 針對 Amazon EC2 執行個體上所部署的閘道，不支援透過公有網際網路連線來存取閘道。Amazon EC2 執行個體的彈性 IP 地址無法當成目標地址使用。

5. 將新的目標入口網站連線至閘道上的儲存磁碟區目標：

   a. 選擇 Targets (目標) 標籤。

      新的目標入口網站即會與非作用中狀態一起顯示。顯示的目標名稱應該與您在步驟 1 中針對儲存磁碟區所指定的名稱相同。

   b. 選取目標，然後選擇 Connect (連線)。

      如果尚未填入目標名稱，請輸入如步驟 1 所示的目標名稱。在連線至目標對話方塊中，選取將此連線新增至「最愛目標」清單，然後選擇確定。

   c. 在目標標籤中，確定目標狀態的值為已連線 (這指出已連線目標)，然後選擇確定。

您現在可以針對 Windows 初始化和格式化此儲存磁碟區，以開始在其上儲存資料。若要執行此作業，請使用 Windows 磁碟管理工具。

> **Note**
>
> 雖然本練習不需要這麼做，但強烈建議依照自訂您的 Windows iSCSI 設定討論的內容自訂真實應用程式的 iSCSI 設定。

將您的 volumes連接到 Linux 用戶端

使用 Red Hat Enterprise Linux (RHEL) 時，您可以使用 `iscsi-initiator-utils` RPM 套件連線至閘道 iSCSI 目標 (磁碟區或 VTL 裝置)。

將 Linux 用戶端連線至 iSCSI 目標

1. 安裝 `iscsi-initiator-utils` RPM 套件 (若尚未安裝在用戶端上)。

   您可以使用下列命令來安裝套件。

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

2. 確定 iSCSI 協助程式正在執行。

   a. 使用下列其中一個命令，確認 iSCSI 協助程式正在執行。

      對於 RHEL 8 或 9，請使用下列命令。

      ```
      sudo service iscsid status
      ```

   b. 如果狀態命令未傳回狀態正在執行，則請使用下列其中一個命令來啟動常駐程式。

      對於 RHEL 8 或 9，請使用下列命令。您通常不需要明確啟動`iscsid`服務。

      ```
      sudo service iscsid start
      ```

3. 若要搜索針對閘道所定義的磁碟區或 VTL 裝置目標，請使用下列搜索命令。

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

   將前一個命令中的 *[GATEWAY_IP]* 變數，替代為您閘道的 IP 地址。您可以在 Storage Gateway 主控台之磁碟區的 iSCSI 目標資訊屬性中找到閘道 IP。

   搜索命令的輸出看起來會像下列範例輸出。

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

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

您的 iSCSI 合格名稱 (IQN) 會與前面所顯示的名稱不同，因為 IQN 值對於組織而言是唯一的。目標的名稱就是您在建立磁碟區時指定的名稱。當您在 Storage Gateway 主控台上選取磁碟區時，也可以在 iSCSI 目標資訊屬性窗格中找到此目標名稱。

4. 若要連線至目標，請使用下列命令。

   請注意，您需要在連線命令中指定正確的 *[GATEWAY_IP]* 和 IQN。

   > **Warning**
   >
   > 針對 Amazon EC2 執行個體上所部署的閘道，不支援透過公有網際網路連線來存取閘道。Amazon EC2 執行個體的彈性 IP 地址無法當成目標地址使用。

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

5. 若要確認磁碟區連接至用戶端機器 (啟動器)，請使用下列命令。

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

   命令的輸出看起來會像下列範例輸出。

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

   強烈建議您在設定啟動器之後，依照 自訂您的 Linux iSCSI 設定 中討論的內容自訂 iSCSI 設定。

自訂 iSCSI 設定

我們強烈建議您在設定啓動器之後，自訂您的 iSCSI 設定以防止啟動器中斷與目標的連線。

如下列步驟所示增加 iSCSI 逾時值，您讓您的應用程式更善於處理需時甚久的寫入操作，以及其他暫時性問題，例如網路中斷。

> **Note**
>
> 變更登錄之前，您應該先備份一份登錄。如需建立在處理登錄時遵循之備份副本及其他最佳實務的資訊，請參閱 Microsoft TechNet Library 的 Registry best practices。

主題

- 自訂您的 Windows iSCSI 設定
- 自訂您的 Linux iSCSI 設定
- 自訂磁碟區閘道的 Linux 磁碟逾時設定

自訂您的 Windows iSCSI 設定

使用 Windows 用戶端時，您要使用 Microsoft iSCSI 啟動器連線到您的閘道磁碟區。如需如何連線到磁碟區的指示，請參閱將磁碟區連接到用戶端。

自訂您的 Windows iSCSI 設定

1. 提高請求佇列的時間上限。

   a. 啟動登錄編輯器 (`Regedit.exe`)。

   b. 導覽至裝置類別的全域唯一識別碼 (GUID) 金鑰，其包含 iSCSI 控制器設定，如下所示。

   > **Warning**
   >
   > 確定您是在 CurrentControlSet 子機碼中工作，而不是其他的控制集，例如 ControlSet001 或 ControlSet002。

   ```
   HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}
   ```

   c. 尋找適用於 Microsoft iSCSI 啟動器的子機碼，如下所示為 *<[######]*。

   此機碼由四位數的號碼組成，例如 `0000`。

```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\[<Instance Number]
```

視您在電腦上安裝的內容而定，Microsoft iSCSI 啟動器可能不是子機碼 `0000`。您可以透過驗證字串`DriverDesc`具有 值，來確保您已選取正確的子索引鍵`Microsoft iSCSI Initiator`。

d. 若要顯示 iSCSI 設定，請選擇 Parameters (參數) 子機碼。

e. 開啟內容 (按右鍵) 選單取得 MaxRequestHoldTime DWORD (32 位元) 值，選擇 修改，然後將值變更為 **600**。

MaxRequestHoldTime 指定在通知`Device Removal`事件上層之前，Microsoft iSCSI 啟動器應保留並重試未完成命令的秒數。此值表示保留通話時間為 600 秒。

2. 您可以修改下列參數，增加 iSCSI 封包中可傳送的資料量上限：

- FirstBurstLength 可控制未經要求的寫入請求能夠傳輸的資料量上限。將此值設為 **262144** 或 Windows 作業系統預設值，以較高者為準。
- MaxBurstLength 類似於 FirstBurstLength，但其控制的是經要求的寫入請求能夠傳輸的資料量上限。將此值設為 **1048576** 或 Windows 作業系統預設值，以較高者為準。
- MaxRecvDataSegmentLength 可控制與單一協定資料單元 (PDU) 相關聯的資料區段大小上限。將此值設為 **262144** 或 Windows 作業系統預設值，以較高者為準。

> **Note**
>
> 可利用不同 iSCSI 設定將各個備份軟體最佳化，以發揮最大效益。如要確認這些參數的哪些值能夠帶來最佳效能，請參閱備份軟體的文件。

3. 提高磁碟逾時值，如下所示：

a. 如尚未啟動，請啟動登錄編輯器 (`Regedit.exe`)。

b. 導覽到 CurrentControlSet 之 Services (服務) 子機碼中的 Disk (磁碟) 子機碼，如下所示。

```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Services\Disk
```

c. 開啟內容 (按右鍵) 選單取得 TimeOutValue DWORD (32 位元) 值，選擇修改，然後將值變更為 **600**。

TimeOutValue 指定在捨棄並重新建立連線嘗試工作階段復原之前，iSCSI 啟動器等待目標回應的秒數。此值代表 600 秒的逾時期間。

4. 為確保新的組態值生效，請重新啟動您的系統。

   重新啟動之前，您必須確定磁碟區所有寫入操作的結果都已排清。若要執行此作業，請先將所有映射儲存磁碟區的磁碟離線，再重新啟動。

自訂您的 Linux iSCSI 設定

我們強烈建議您在設定閘道之後，自訂您的 iSCSI 設定以防止啟動器中斷與目標的連線。如下列步驟所示增加 iSCSI 逾時值，您讓您的應用程式更善於處理需時甚久的寫入操作，以及其他暫時性問題，例如網路中斷。

> **Note**
>
> 用於 Linux 其他類型的命令可能稍有不同。下列範例是以 Red Hat Linux 為基礎。

自訂您的 Linux iSCSI 設定

1. 提高請求佇列的時間上限。

   a. 開啟 `/etc/iscsi/iscsid.conf` 檔案並尋找下列各行。

   ```
   node.session.timeo.replacement_timeout = [replacement_timeout_value]
   node.conn[0].timeo.noop_out_interval = [noop_out_interval_value]
   node.conn[0].timeo.noop_out_timeout = [noop_out_timeout_value]
   ```

   b. 將 *[replacement_timeout_value]* 值設為 **600**。

      將 *[noop_out_interval_value]* 值設為 **60**。

      將 *[noop_out_timeout_value]* 值設為 **600**。

      這三種值全以秒為單位。

> **Note**
>
> 必須先設定 iscsid.conf 設定才能探索閘道。如已探索到您的閘道或登入目標，或兩項都完成，您可以使用下列命令從探索資料庫刪除項目。然後，您可以重新探索或再次登入以挑選新的組態。
>
> ```
> iscsiadm -m discoverydb -t sendtargets -p [GATEWAY_IP]:3260 -o delete
> ```

2. 增加每個回應可傳輸的資料量上限值。

   a. 開啓 /etc/iscsi/iscsid.conf 檔案並尋找下列各行。

   ```
   node.session.iscsi.FirstBurstLength = [replacement_first_burst_length_value]
   node.session.iscsi.MaxBurstLength = [replacement_max_burst_length_value]
   node.conn[0].iscsi.MaxRecvDataSegmentLength
    = [replacement_segment_length_value]
   ```

   b. 建議您使用下列值，以提升效能。您的備份軟體可能需使用不同值來進行最佳化，因此請參閱備份軟體文件以取得最佳結果。

   將 *[replacement_first_burst_length_value]* 值設定為 **262144** 或 Linux 作業系統預設值，以較高者為準。

   將 *[replacement_max_burst_length_value]* 值設定為 **1048576** 或 Linux 作業系統預設值，以較高者為準。

   將 *[replacement_segment_length_value]* 值設定為 **262144** 或 Linux 作業系統預設值，以較高者為準。

   > **Note**
   >
   > 可利用不同 iSCSI 設定將各個備份軟體最佳化，以發揮最大效益。如要確認這些參數的哪些值能夠帶來最佳效能，請參閱備份軟體的文件。

3. 為確保新的組態值生效，請重新啟動您的系統。

   重新啟動之前，您必須確定磁帶所有寫入操作的結果都已排清。若要這麼做，請先卸載磁帶再重新啟動。

自訂磁碟區閘道的 Linux 磁碟逾時設定

如果您使用的是磁碟區閘道，除了上一節所述的 iSCSI 設定之外，您還可以自訂下列 Linux 磁碟逾時設定。

自訂您的 Linux 磁碟逾時設定

1. 在規則檔案中提高磁碟逾時值。

   a. 如果您使用的是 RHEL 5 啟動器，請開啟 `/etc/udev/rules.d/50-udev.rules` 檔案並尋找下行。

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

   此規則檔案不存在於 RHEL 6 或 7 啟動器中，因此您必須使用下列規則來建立它。

   ```
   ACTION=="add", SUBSYSTEMS=="scsi" , ATTRS{model}=="Storage Gateway",
   RUN+="/bin/sh -c 'echo [timeout] > /sys$$DEVPATH/timeout'"
   ```

   若要在 RHEL 6 中修改逾時值，請使用下列命令，然後新增前文所示的程式碼。

   ```
   sudo vim /etc/udev/rules.d/50-udev.rules
   ```

   若要在 RHEL 7 中修改逾時值，請使用下列命令，然後新增前文所示的程式碼。

   ```
   sudo su -c "echo 600 > /sys/block/[device name]/device/timeout"
   ```

   b. 將 *[##]* 值設為 **600**。

   此值表示逾時為 600 秒。

2. 為確保新的組態值生效，請重新啟動您的系統。

   重新啟動之前，您必須確定磁碟區所有寫入操作的結果都已排清。若要執行此作業，請先卸載儲存磁碟區，再重新啟動。

3. 您可使用下列命令來測試組態。

   ```
   udevadm test [PATH_TO_ISCSI_DEVICE]
   ```

此命令會顯示套用到 iSCSI 裝置的 udev 規則。

設定 iSCSI 目標的 CHAP 身分驗證

Storage Gateway 使用挑戰交握驗證通訊協定 (CHAP)，在閘道和 iSCSI 啟動器之間進行驗證。CHAP 會定期驗證 iSCSI 啟動器的身分識別，以存取磁碟區和 VTL 裝置目標，提供保護以防止播放攻擊。

> **Note**
>
> CHAP 組態為選用項，但強烈建議選擇。

若要設定 CHAP，您必須同時在 Storage Gateway 主控台以及用來連線至目標的 iSCSI 啟動器軟體中設定它。Storage Gateway 會使用雙向 CHAP，即啟動器驗證目標且目標驗證啟動器時。

設定目標的雙向 CHAP

1. 在 Storage Gateway 主控台上設定 CHAP，如 在 Storage Gateway 主控台上設定磁碟區目標的 CHAP 中所討論。
2. 在您的用戶端啟動器軟體中，完成 CHAP 組態：
   - 若要在 Windows 用戶端上設定雙向 CHAP，請參閱在 Windows 用戶端上設定雙向 CHAP。
   - 若要在 Red Hat Linux 用戶端上設定雙向 CHAP，請參閱在 Red Hat Linux 用戶端上設定雙向 CHAP。

在 Storage Gateway 主控台上設定磁碟區目標的 CHAP

在此程序中，您指定兩個用於讀取和寫入磁碟區的秘密金鑰。在此程序中，會使用這些相同的金鑰來設定用戶端啟動器。

1. 在 Storage Gateway 主控台的導覽窗格上，選擇磁碟區。
2. 針對 Actions (動作)，選擇 Configure CHAP authentication (設定 CHAP 身分驗證)。
3. 在設定 CHAP 身分驗證對話方塊中提供請求的資訊。
   a. 針對啟動器名稱，輸入您 iSCSI 啟動器的名稱。此名稱是Amazon iSCSI 合格名稱 (IQN)，前接 `iqn.1997-05.com.amazon:`，后為目標名稱。下列是 範例。

      ```
      iqn.1997-05.com.amazon:your-volume-name
      ```

您可以使用 iSCSI 啟動器軟體來找到啟動器名稱。例如，針對 Windows 用戶端，名稱就是 iSCSI 啟動器之 Configuration (組態) 標籤上的值。如需詳細資訊，請參閱在 Windows 用戶端上設定雙向 CHAP。

> **Note**
>
> 若要變更啟動器名稱，您必須先停用 CHAP，並在 iSCSI 啟動器軟體中變更啟動器名稱，然後使用新的名稱啟用 CHAP。

b. 針對啟動器驗證所用的秘密，輸入所請求的秘密。

此秘密的長度必須最少為 12 個字元，最多為 16 個字元。此值是秘密金鑰，而啟動器 (即 Windows 用戶端) 必須知道秘密金鑰才能參與和目標的 CHAP。

c. 針對目標驗證所用的秘密 (雙向 CHAP)，輸入所請求的秘密。

此秘密的長度必須最少為 12 個字元，最多為 16 個字元。此值是秘密金鑰，而目標必須知道秘密金鑰才能參與和啟動器的 CHAP。

> **Note**
>
> 用來驗證目標的秘密必須與驗證啟動器的秘密不同。

d. 選擇儲存。

4. 選擇 Details (詳細資訊) 標籤，並確認 iSCSI CHAP authentication (iSCSI CHAP 身分驗證) 設定為 true。

在 Windows 用戶端上設定雙向 CHAP

在此程序中，您使用用來在主控台上設定磁碟區之 CHAP 的相同金鑰，在 Microsoft iSCSI 啟動器中設定 CHAP。

1. 如果尚未啟動 iSCSI 啟動器，請在 Windows 用戶端電腦的開始選單上選擇執行，並輸入 **`iscsicpl.exe`**，然後選擇 確定 執行程式。
2. 設定啟動器 (即 Windows 用戶端) 的雙向 CHAP 組態：

a. 選擇 Configuration (組態) 索引標籤。

> **Note**
>
> Initiator Name (啟動器名稱) 值對於啟動器和公司必須是唯一的。前面所顯示的名稱是您在 Storage Gateway 主控台之設定 CHAP 身分驗證對話方塊中所使用的值。範例影像中所顯示的名稱僅供示範之用。

b. 選擇 CHAP。

c. 在 iSCSI 啟動器雙向 CHAP 秘密對話方塊中，輸入雙向 CHAP 秘密值。

在此對話方塊中，您輸入啟動器 (Windows 用戶端) 用來驗證目標 (儲存磁碟區) 的秘密。此秘密可讓目標讀取和寫入啟動器。此秘密與設定 CHAP 身分驗證對話方塊中的目標驗證所用的秘密 (雙向 CHAP) 方塊中所輸入的秘密相同。如需詳細資訊，請參閱設定 iSCSI 目標的 CHAP 身分驗證。

d. 如果您輸入的金鑰長度少於 12 個字元或超過 16 個字元，則會出現啟動器 CHAP 秘密錯誤對話方塊。

選擇確定，然後重新輸入金鑰。

3. 使用啟動器的秘密設定目標，以完成雙向 CHAP 組態。

a. 選擇 Targets (目標) 標籤。

b. 如果目前已連線您要針對 CHAP 設定的目標，則請選取目標，並選擇 Disconnect (中斷連線)，以將目標中斷連線。

c. 選取您要針對 CHAP 設定的目標，然後選擇 Connect (連線)。

d. 在 Connect to Target (連線至目標) 對話方塊中，選擇 Advanced (進階)。

e. 在 Advanced Settings (進階設定) 對話方塊中，設定 CHAP。

i. 選取啟動 CHAP 登入。

ii. 輸入驗證啟動器所需的秘密。此秘密與設定 CHAP 身分驗證對話方塊中的啟動器驗證所用的秘密方塊所輸入的秘密相同。如需詳細資訊，請參閱設定 iSCSI 目標的 CHAP 身分驗證。

iii. 選取 Perform mutual authentication (執行交互身分驗證)。

iv. 若要套用變更，請選擇 OK (確定)。

f. 在 Connect to Target (連線至目標) 對話方塊中，選擇 OK (確定)。

4. 如果您已提供正確的秘密金鑰，則目標會顯示 Connected (已連線) 狀態。

在 Red Hat Linux 用戶端上設定雙向 CHAP

在此程序中，您使用用來在 Storage Gateway 主控台上設定磁碟區之 CHAP 的相同金鑰，在 Linux iSCSI 啟動器中設定 CHAP。

1. 確定 iSCSI 協助程式正在執行，而且您已經連線至目標。如果您尚未完成這兩項工作，請參閱連線至 Red Hat Enterprise Linux 用戶端。
2. 中斷連線和移除您要設定 CHAP 之目標的任何現有組態。

   a. 若要尋找目標名稱，並確保它是已定義的組態，請使用下列命令列出儲存的組態。

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

   b. 與目標中斷連線。

   下列命令會與名為 **myvolume** 且定義於 Amazon iSCSI 合格名稱 (IQN) 中的目標中斷連線。視需要針對您的情況變更目標名稱和 IQN。

   ```
   sudo /sbin/iscsiadm --mode node --logout GATEWAY_IP:3260,1
    iqn.1997-05.com.amazon:myvolume
   ```

   c. 移除目標的組態。

   下列命令會移除 **myvolume** 目標的組態。

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

3. 編輯 iSCSI 組態檔案以啟用 CHAP。

   a. 取得啟動器的名稱 (即您正在使用的用戶端)。

   下列命令會從 `/etc/iscsi/initiatorname.iscsi` 檔案取得啟動器名稱。

   ```
   sudo cat /etc/iscsi/initiatorname.iscsi
   ```

   此命令的輸出如下所示：

   ```
   InitiatorName=iqn.1994-05.com.redhat:8e89b27b5b8
   ```

   b. 開啟 `/etc/iscsi/iscsid.conf` 檔案。

c. 取消檔案中下列數行的註解，並指定 *username*、*password*、*username_in* 和 *password_in* 的正確值。

```
node.session.auth.authmethod = CHAP
node.session.auth.username = username
node.session.auth.password = password
node.session.auth.username_in = username_in
node.session.auth.password_in = password_in
```

如需所要指定值的指導，請參閱下表。

組態設定	Value
username	您在此程序的前一個步驟中找到的啟動器名稱。此值的開頭為 iqn。例如，**iqn.1994-05.com.redhat:8e89b27b5b8** 是有效的 *username* 值。
password	啟動器 (您正在使用的用戶端) 與磁碟區通訊時，用來驗證啟動器的秘密金鑰。
username_in	目標磁碟區的 IQN。此值的開頭為 iqn，且結尾為目標名稱。例如，**iqn.1997-05.com.amazon:myvolume** 是有效的 *username_in* 值。
password_in	目標 (磁碟區) 與啟動器通訊時，用來驗證目標的秘密金鑰。

d. 儲存組態檔案中的變更，然後關閉檔案。

4. 搜索和登入目標。若要這麼做，請依照連線至 Red Hat Enterprise Linux 用戶端中的步驟進行。

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. 將內部部署 Storage Gateway 設備連接至 Direct Connect 路由器。
3. 建立公有虛擬界面，然後以同樣方式設定您的內部部署路由器。即便使用 Direct Connect，也必須使用 HAProxy 建立 VPC 端點。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 。

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，請參閱登入至您的 Amazon EC2 閘道本機主控台。

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。
4. 在啟用您的閘道之後，請選擇您剛剛啟用的閘道，然後選擇底部面板中的 VTL devices (VTL 裝置) 標籤。
5. 取得您所有 VTL 裝置的名稱。
6. 針對每個目標，執行下列命令來設定目標。

   ```
   iscsiadm -m node -o new -T [$TARGET_NAME] -p [$Elastic_IP]:3260
   ```

7. 針對每個目標，執行下列命令來登入。

   ```
   iscsiadm -m node -p [$ELASTIC_IP]:3260 --login
   ```

   您的閘道現在可以使用 EC2 執行個體的彈性 IP 地址予以連線。

IPv6 支援

IPv6 支援僅適用於閘道設備 3.x 版或更新版本。閘道設備 1.x 和 2.x 版無法更新為 3.x。您必須遷移或取代閘道設備 1.x 或 2.x 版，才能取得 IPv6 支援。

IPv6 需要下列雙堆疊端點。如需詳細資訊，請參閱端點類型。

```
storagegateway.region.api.aws:443
activation-storagegateway.region.api.aws:443
controlplane-storagegateway.region.api.aws:443
proxy-storagegateway.region.api.aws:443
dataplane-storagegateway.region.api.aws:443
```

了解 Storage Gateway 資源和資源 ID

在 Storage Gateway 中，主要資源是一種閘道，但其他資源類型包含：磁碟區、虛擬磁帶、iSCSI 目標和 VTL 裝置。它們稱為子資源，必須與閘道相關聯才能存在。

這些資源和子資源都有獨一無二的 Amazon Resource Name (ARN) 與其相關聯，如下表所示。

資源類型	ARN 格式
閘道 ARN	arn:aws:storagegateway: *region*:*account-id* :gateway/ *gateway-id*
磁碟區 ARN	arn:aws:storagegateway: *region*:*account-id* :gateway/ *gateway-id* /volume/*volume-id*
目標 ARN (iSCSI 目標)	arn:aws:storagegateway: *region*:*account-id* :gateway/ *gateway-id* /target/*iSCSItarget*

Storage Gateway 也支援使用 EC2 執行個體以及 EBS 磁碟區和快照。這些資源是 Storage Gateway 中所使用的 Amazon EC2 資源。

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 採用資源識別符的形式，後面接著連字號，以及八個字母和數字的唯一組合，或磁碟區或快照

的 17 個數字和字母。例如，閘道 ID 的格式為 ，sgw-12A3456B其中 sgw是閘道的資源識別符，而磁碟區 ID 的格式為 vol-112233AABBCCDDEEF，其中 vol是磁碟區的資源識別符。

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，磁碟區的 ID 可能是 vol-112233AABBCCDDEEF。如果您將此 ID 與 EC2 API 搭配使用，則必須將其變更為 vol-112233aabbccddeef。否則，EC2 API 可能無法如預期運作。

為 Storage Gateway 資源加上標籤

在 Storage Gateway 中，您可以使用標籤來管理您的資源。標籤可讓您將中繼資料新增到您的資源並對您的資源進行分類，使資源更易於管理。每個標籤都是由您定義的金鑰/值對所構成。您可以將標籤新增到閘道、磁碟區和虛擬磁帶。您可以根據您新增的標籤搜尋及篩選這些資源。

例如，您可以使用標籤來識別您組織中各部門所使用的 Storage Gateway 資源。您可以為會計部門所使用的閘道和磁碟區新增標籤如下：(key=department 和 value=accounting)。您接著可以使用此標籤進行篩選，識別您的會計部門所使用的所有閘道和磁碟區，然後運用此資訊來判斷成本。如需詳細資訊，請參閱使用成本配置標籤和使用標籤編輯器。

若您存檔已加上標籤的虛擬磁帶，磁帶會在存檔中維持其標籤。同樣地，若您從存檔將磁帶擷取至另一個閘道，標籤也會保留在新的閘道中。

標籤不具有任何語意意義，而是會解譯成字元字串。

以下限制適用於標籤：

- 標籤金鑰與值皆區分大小寫。
- 每個資源的標籤數上限為 50。
- 標籤金鑰的開頭不可為 aws:。此字首已保留供 AWS 使用。
- 金鑰屬性的有效字元為 UTF-8 字母和數字、空格及特殊字元 + - = . _ : / 和 @。

處理標籤

您可以使用 Storage Gateway 主控台、Storage Gateway API，或是 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. 選擇您希望編輯之標籤旁的鉛筆圖示，然後編輯標籤。
5. 完成編輯標籤後，選擇儲存。

若要刪除標籤

1. 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 Storage Gateway 的開放原始碼元件

本節說明我們為提供 Storage Gateway 功能所仰賴的第三方工具和授權。

下列位置提供 AWS Storage Gateway 軟體所隨附之特定開放原始碼軟體元件的來源碼，以供下載：

- 對於部署在 VMware ESXi 上的閘道，請下載 sources.tar
- 對於部署在 Microsoft Hyper-V 上的閘道，請下載 sources_hyperv.tar
- 對於部署在 Linux 核心架構虛擬機器 (KVM) 上的閘道，請下載 sources_KVM.tar

此產品包含 OpenSSL Project 所開發以用於 OpenSSL Toolkit 的軟體 (http://www.openssl.org/)。如需所有相依第三方工具的相關授權，請參閱第三方授權。

AWS Storage Gateway 配額

在本主題中，您可以找到 Storage Gateway 磁碟區與磁碟配額、組態和效能配額的相關資訊。

主題

- 磁碟區的配額
- 適用於您閘道的建議本機磁碟大小

磁碟區的配額

下表列出磁碟區的配額。

描述	快取磁碟區	存放磁碟區
磁碟區大小上限	32 TiB	16 TiB

> **Note**
>
> 若您從快取磁碟區建立的快照大小超過 16 TiB，您可將快照還原至 Storage Gateway 磁碟區，但不可還原至 Amazon

描述	快取磁碟區	存放磁碟區
Elastic Block Store (Amazon EBS) 磁碟區。		
每個閘道的磁碟區數目上限	32	32
閘道的所有磁碟區總大小	1,024 TiB	512 TiB

適用於您閘道的建議本機磁碟大小

閘道類型	快取 (最小值)	快取 (最大值)	上傳緩衝區 (最小值)	上傳緩衝區 (最大值)
磁帶閘道	150 GiB	64 TiB	150 GiB	2 TiB

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

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**
>
> 您也可以使用 開發應用程式時使用 AWS SDKs AWS Storage Gateway。適用於 Java、.NET 和 PHP AWS SDKs 包裝基礎 AWS 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

- Storage Gateway 的必要請求標頭
- 簽署請求
- 錯誤回應
- 動作

Storage Gateway 的必要請求標頭

本節說明您必須在每個傳送到 Storage Gateway 的 POST 請求中附上的必要標頭。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
```

以下為必須包含在您傳送至 Storage Gateway 之 POST 請求中的標頭。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`	授權標頭包含幾段請求的資訊，讓 Storage Gateway 能判斷該請求對申請者而言是否為有效動作。此標頭的格式如下 (為求可讀性已新增分行)： `Authorization: AWS4-HMAC_SHA456 Credentials= YourAccessKey /yyymmdd/region/storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature= CalculatedSignature` 在前述語法中，您指定 YourAccessKey、年、月、日 (yyyymmdd)、region，以及 CalculatedSignature。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簽署請求主題中討論。
`Content-Type`	使用 `application/x-amz-json-1.1` 做為所有傳送至 Storage Gateway 請求的內容類型。 `Content-Type: application/x-amz-json-1.1`
`Host`	使用主機標頭來指定您要傳送請求的 Storage Gateway 端點。舉例來說，`storagegateway.us-east-2.amazonaws.com` 代表美國東部 (俄亥俄) 區域的端點。如需 Storage Gateway 可用端點的詳細資訊，請參閱 AWS 一般參考 中的 AWS Storage Gateway 端點與配額。 `Host: storagegateway. region.amazonaws.com`
`x-amz-date`	您必須提供 HTTP `Date`標頭或 AWS `x-amz-date` 標頭中的時間戳記。(有些 HTTP 用戶端程式庫不讓您設定 `Date` 標頭。) 當 `x-amz-`

標頭	Description
	`date` 標頭存在時，Storage Gateway 會在請求身分驗證時略過任何 `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。 `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
`x-amz-target`	此標頭會指定 API 的版本，以及您請求的操作。目標標頭值是透過串連 API 版本及 API 名稱構成，且其格式如下。 `x-amz-target: StorageGateway_ APIversion .operationName` operationName 值 (例如："ActivateGateway") 可從 API 清單 (Storage Gateway 的 API 參考) 中找到。

簽署請求

Storage Gateway 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。Amazon Web Services 詞彙表的 Signature Version 4 Test Suite 包含其他參考計算。

該範例假設如下：

- 請求的時間戳記為 "Mon, 10 Sep 2012 00:00:00" GMT。
- 端點是美國東部 (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
IncompleteSignatureException	指定的簽章不完整。	400 錯誤的請求
InternalFailure	由於不明的錯誤、異常或故障，處理請求失敗。	500 內部伺服器錯誤
InternalServerError	操作錯誤代碼 的其中一項操作錯誤代碼訊息。	500 內部伺服器錯誤
InvalidAction	請求的動作或操作無效。	400 錯誤的請求
InvalidClientTokenId	提供的 X.509 憑證或 AWS 存取金鑰 ID 不存在於我們的記錄中。	403 禁止
InvalidGatewayRequestException	操作錯誤代碼 中的其中一項操作錯誤代碼訊息。	400 錯誤的請求

異常情形	訊息	HTTP 狀態碼
InvalidSignatureException	我們計算的請求簽章不符合您提供的簽章。檢查您的 AWS 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 Storage Gateway 中的操作 中列出。	400 錯誤的請求
UnrecognizedClientException	包含在請求中的安全性權杖無效。	400 錯誤的請求
ValidationException	輸入參數的值不符或超出範圍。	400 錯誤的請求

操作錯誤代碼

下表顯示 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。	ActivateGateway
ActivationKeyInvalid	指定的啟用金鑰無效。	ActivateGateway
ActivationKeyNotFound	找不到指定的啟用金鑰。	ActivateGateway
BandwidthThrottleScheduleNotFound	找不到指定的頻寬調節。	DeleteBandwidthRateLimit
CannotExportSnapshot	無法匯出指定的快照。	CreateCachediSCSIVolume CreateStorediSCSIVolume
InitiatorNotFound	找不到指定的啟動器。	DeleteChapCredentials
DiskAlreadyAllocated	指定的磁碟已配置。	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
DiskDoesNotExist	指定的磁碟不存在。	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
DiskSizeNotGigAligned	指定的磁碟未調整為 GB。	CreateStorediSCSIVolume
DiskSizeGreaterThanVolumeMaxSize	指定的磁碟大小大於磁碟區大小上限。	CreateStorediSCSIVolume
DiskSizeLessThanVolumeSize	指定的磁碟大小小於磁碟區大小。	CreateStorediSCSIVolume
DuplicateCertificateInfo	指定的憑證資訊重複。	ActivateGateway

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
GatewayInternalError	發生閘道內部錯誤。	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
GatewayNotConnected	指定的閘道並未連線。	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
GatewayNotFound	找不到指定的閘道。	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
		ListLocalDisks ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
GatewayProxyNetworkConnectionBusy	指定的閘道代理網路連線忙碌中。	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
InternalError	發生內部錯誤。	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
InvalidParameters	指定的請求包含不正確的參數。	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
LocalStorageLimitExceeded	超過本機儲存限制。	AddCache AddUploadBuffer AddWorkingStorage
LunInvalid	指定的 LUN 不正確。	CreateStorediSCSIVolume
MaximumVolumeCountExceeded	超過磁碟區計數上限。	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
NetworkConfigurationChanged	閘道網路組態已變更。	CreateCachediSCSIVolume CreateStorediSCSIVolume

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
NotSupported	不支援指定的操作。	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
OutdatedGateway	指定的閘道已過期。	ActivateGateway
SnapshotInProgressException	指定的快照正在進行。	DeleteVolume
SnapshotIdInvalid	指定的快照無效。	CreateCachediSCSIVolume CreateStorediSCSIVolume
StagingAreaFull	預備區域已滿。	CreateCachediSCSIVolume CreateStorediSCSIVolume

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
TargetAlreadyExists	指定的目標已存在。	CreateCachediSCSIVolume CreateStorediSCSIVolume
TargetInvalid	指定的目標無效。	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials UpdateChapCredentials
TargetNotFound	找不到指定的目標。	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials DeleteVolume UpdateChapCredentials

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
UnsupportedOperationForGatewayType	指定的操作對於閘道類型無效。	AddCache AddWorkingStorage CreateCachediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteSnapshotSchedule DescribeCache DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
VolumeAlreadyExists	指定的磁碟區已存在。	CreateCachediSCSIVolume CreateStorediSCSIVolume
VolumeIdInvalid	指定的磁碟區無效。	DeleteVolume
VolumeInUse	指定的磁碟區已在使用。	DeleteVolume

操作錯誤代碼	訊息	傳回此錯誤代碼的操作
VolumeNotFound	找不到指定的磁碟區。	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint DeleteVolume DescribeCachediSCSIVolumes DescribeSnapshotSchedule DescribeStorediSCSIVolumes UpdateSnapshotSchedule
VolumeNotReady	指定的磁碟區尚未準備就緒。	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

錯誤回應

當發生錯誤時，回應標頭資訊會包含：

- 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 中的操作

如需 Storage Gateway 操作的清單，請參閱 AWS Storage Gateway API 參考中的動作。

磁碟區閘道使用者指南的文件歷史記錄

下表會說明 2018 年 4 月後《AWS Storage Gateway 使用者指南》每個版本的重要變更。如需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
IPv6 支援	IPv6 支援可在閘道設備 3.x 版或更新版本上使用。	2025 年 9 月 10 日
FSx File Gateway 可用性變更通知	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。	2024 年 10 月 28 日
FSx File Gateway 可用性變更通知	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，請造訪此部落格文章。	2024 年 9 月 26 日
新增開啟或關閉維護更新的選項	Storage Gateway 會收到定期維護更新，其中包括作業系統和軟體升級、解決穩定性、效能和安全性的修正，以及新功能的存取。您現在可以設定 設定，為部署中的每個個別閘道開啟或關閉這些更新。如需詳細資訊，請參閱使用 AWS Storage Gateway 主控台管理閘道更新。	2024 年 6 月 6 日

Snowball Edge 上磁帶閘道的已棄用支援	您無法再在 Snowball Edge 裝置上託管磁帶閘道。	2024 年 3 月 14 日
更新使用第三方應用程式測試閘道設定的指示	使用第三方應用程式測試閘道設定的說明現在會說明閘道在進行中的備份工作期間重新啟動時的預期行為。如需詳細資訊，請參閱。	2023 年 10 月 24 日
更新建議 CloudWatch 警示	CloudWatch `HealthNotifications` 警示現在適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。	2023 年 10 月 2 日
獨立的磁帶與磁碟區閘道使用者指南	《Storage Gateway 使用者指南》先前包含磁帶和磁碟區閘道類型的相關資訊，已分為《磁帶閘道使用者指南》和《磁碟區閘道使用者指南》，每一種僅包含一種閘道類型的資訊。如需詳細資訊，請參閱磁帶閘道使用者指南和磁碟區閘道使用者指南。	2022 年 3 月 23 日
更新的閘道建立程序	已更新使用 Storage Gateway 主控台建立所有閘道類型的程序。如需詳細資訊，請參閱建立閘道。	2022 年 1 月 18 日

全新磁帶介面	AWS Storage Gateway 主控台中的磁帶概觀頁面已更新為新的搜尋和篩選功能。本指南中的所有相關程序已更新以說明新功能。如需詳細資訊，請參閱管理磁帶閘道。	2021 年 9 月 23 日
支援磁帶閘道專用的 Quest NetVault Backup 13	磁帶閘道現在支援 Microsoft 視窗伺服器 2012 R2 或 Microsoft Windows Server 2016 上執行的 Quest NetVault Backup 13。如需詳細資訊，請參閱使用 Quest NetVault Backup 來測試您的設定。	2021 年 8 月 22 日
從磁帶和磁碟區閘道指南移除的 S3 檔案閘道主題	為了讓客戶設定各自的閘道類型時，更容易遵循磁帶閘道和磁碟區閘道的使用者指南，部分不必要的主題已移除。	2021 年 7 月 21 日
磁帶閘道支援 IBM 頻譜保護 8.1.10 在 Windows 和 Linux 上的執行	磁帶閘道現在支持 IBM 頻譜保護版本 8.1.10 在Microsoft 視窗伺服器和 Linux 上執行。如需詳細資訊，請參閱使用 IBM 頻譜保護來測試您的設定。	2020 年 11 月 24 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
以排程為基礎的頻寬限流	Storage Gateway 現在支援磁帶和磁碟區閘道的排程式頻寬限流。如需詳細資訊，請參閱使用 Storage Gateway 主控台排程頻寬限流。	2020 年 11 月 9 日

快取磁碟區和磁帶閘道本機快取儲存體增至 4 倍	Storage Gateway 現在針對快取磁碟區和磁帶閘道支援高達 64 TB 的本機快取，藉由提供低延遲存取較大的工作資料集，提升內部部署應用程式的效能。如需詳細資訊，請參閱建議的閘道本機磁碟大小。	2020 年 11 月 9 日
閘道移轉	Storage Gateway 現在支援將快取的磁碟區閘道移轉至新的虛擬機器。如需詳細資訊，請參閱將快取磁碟區移至新的快取磁碟區閘道虛擬機器。	2020 年 9 月 10 日
支援磁帶保留鎖定和單寫多讀 (WORM) 磁帶保護	Storage Gateway 支援虛擬磁帶上的磁帶保留鎖定，以及單寫多讀 (WORM)。磁帶保留鎖定可讓您指定封存虛擬磁帶上的保留模式和期間，防止它們遭到刪除，最長可達 100 年的固定時間。其中包括誰可以刪除磁帶或修改保留設定的權限控制。如需詳細資訊，請參閱使用磁帶保留鎖定。WORM 啟動的虛擬磁帶有助於確保虛擬磁帶櫃中主動磁帶上的資料不會被覆寫或清除。如需詳細資訊，請參閱單寫多讀 (WORM) 磁帶保護。	2020 年 8 月 19 日
透過主控台訂購硬體設備	您現在可以透過 AWS Storage Gateway 主控台訂購硬體設備。如需詳細資訊，請參閱使用 Storage Gateway 硬體設備。	2020 年 8 月 12 日

支援新 AWS 區域中的聯邦資訊處理標準 (FIPS) 端點	您現在可在美國東部 (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
閘道移轉	Storage Gateway 現在支援將磁帶和儲存磁碟區閘道移轉至新的虛擬機器。如需詳細資訊，請參閱將資料移至新閘道。	2020 年 7 月 31 日
在 Storage Gateway 主控台中檢視 Amazon CloudWatch 警示	您現在可在 Storage Gateway 主控台中檢視 CloudWatch 警示。如需詳細資訊，請參閱了解 CloudWatch 警示。	2020 年 5 月 29 日
支援聯邦資訊處理標準 (FIPS) 端點	您現在可以在 AWS GovCloud (US) 區域中啟用具有 FIPS 端點的閘道。若要為磁碟區閘道選擇 FIPS 端點，請參閱選擇服務端點。若要為磁帶閘道選擇 FIPS 端點，請參閱將磁帶閘道連接到 AWS。	2020 年 5 月 22 日
新 AWS 區域	Storage Gateway 現已在非洲 (開普敦) 和歐洲 (米蘭) 區域提供。如需詳細資訊，請參閱 AWS 一般參考 中的 AWS Storage Gateway 端點和配額。	2020 年 5 月 7 日

S3 Intelligent-Tiering 儲存體方案的支援	Storage Gateway 現支援 S3 Intelligent-Tiering 儲存體方案。S3 Intelligent-Tiering 儲存體方案旨在透過自動將資料移動到最具成本效益的儲存體存取層，將儲存成本最佳化，且不會影響效能或帶來額外負荷。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的自動最佳化經常存取物件與不常存取物件的儲存體方案。	2020 年 4 月 30 日
磁帶閘道讀寫效能增至 2 倍	Storage Gateway 將磁帶閘道上的虛擬磁帶讀寫效能增至 2 倍，讓您可比以前更快速的執行備份和復原。如需詳細資訊，請參閱《Storage Gateway 使用者指南》中的磁帶閘道效能指引。	2020 年 4 月 23 日
自動磁帶建立的支援	Storage Gateway 現能夠自動建立新的虛擬磁帶。磁帶閘道可自動建立新的虛擬磁帶，以維持您設定的可用磁帶數目下限，然後這些新磁帶可供備份應用程式進行匯入，讓您執行備份任務時無須中斷。如需詳細資訊，請參閱《Storage Gateway 使用者指南》中的自動建立磁帶。	2020 年 4 月 23 日

新 AWS 區域	Storage Gateway 現已在 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 AWS Storage Gateway 端點和配額。	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
磁帶閘道的新 AWS 區域	磁帶閘道正式於南美洲 (聖保羅) 區域推出。如需詳細資訊，請參閱 AWS 一般參考 中的 AWS Storage Gateway 端點和配額。	2019 年 9 月 24 日

支援 Linux 上的 IBM 頻譜保護 7.1.9 版，以及磁帶閘道的磁帶大小上限提高至 5 TiB	除了在 Microsoft Windows 上執行，磁帶閘道現在支援在 Linux 上執行的 IBM 頻譜保護 (Tivoli Storage Manager) 7.1.9 版。如需詳細資訊，請參閱《Storage Gateway 使用者指南》中的使用 IBM 頻譜保護來測試您的設定。此外，針對磁帶閘道，虛擬磁帶的大小上限現在已從 2.5 TiB 提高至 5 TiB。如需詳細資訊，請參閱《Storage Gateway 使用者指南》中的磁帶配額。	2019 年 9 月 10 日
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
新 AWS 區域	Storage Gateway 現已在亞太區域 (香港) 提供。如需詳細資訊，請參閱 AWS 一般參考 中的 AWS Storage Gateway 端點和配額。	2019 年 8 月 14 日
新 AWS 區域	Storage Gateway 現已在中東 (巴林) 區域提供。如需詳細資訊，請參閱 AWS 一般參考 中的 AWS Storage Gateway 端點和配額。	2019 年 7 月 29 日

支援在虛擬私有雲端 (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
支援將虛擬磁帶從 S3 Glacier Flexible Retrieval 遷移至 S3 Glacier Deep Archive	您現在可以將存檔在 S3 Glacier Flexible Retrieval 儲存類別的虛擬磁帶移到 S3 Glacier Deep Archive 儲存類別，以獲得經濟效益與長期資料保留。如需詳細資訊，請參閱從 S3 Glacier Flexible Retrieval 移動磁帶到 S3 Glacier Deep Archive。	2019 年 5 月 28 日
SMB 檔案共享支援 Microsoft Windows ACL	對於檔案閘道，您現在可以使用 Microsoft Windows 存取控制清單 (ACL) 來控制伺服器訊息區塊 (SMB) 檔案共享的存取。如需詳細資訊，請參閱使用 Microsoft Windows ACL 來控制 SMB 檔案共享的存取。	2019 年 5 月 8 日
與 S3 Glacier Deep Archive 整合	磁帶閘道可與 S3 Glacier Deep Archive 整合。您現在可以將虛擬磁帶存檔在 S3 Glacier Deep Archive 以進行長期資料保留。如需詳細資訊，請參閱存檔虛擬磁帶。	2019 年 3 月 27 日

歐洲 Storage Gateway 硬體設備的可用性	可在歐洲購買 Storage Gateway 硬體設備。如需詳細資訊，請參閱 AWS 一般參考中的 AWS Storage Gateway 硬體設備區域。此外，您現在可以將 Storage Gateway 硬體設備上可使用的儲存體從 5 TB 增加至 12 TB，並將所安裝的銅線網路卡以 10 Gb 光纖網路卡取代。如需詳細資訊，請參閱設定您的硬體設備。	2019 年 2 月 25 日
與 整合 AWS Backup	Storage Gateway 與 整合 AWS Backup。您現在可以使用 AWS Backup 來備份使用 Storage Gateway 磁碟區進行雲端儲存的內部部署商業應用程式。如需詳細資訊，請參閱備份您的磁碟區。	2019 年 1 月 16 日
支援 Bacula Enterprise 和 IBM 頻譜保護	磁帶閘道現在支援 Bacula Enterprise 和 IBM 頻譜保護。磁帶閘道現在也支援新版本的 Veritas NetBackup、Veritas Backup Exec 和 Quest NetVault Backup。您現在可以使用這些備份應用程式將您的資料備份到 Amazon S3，並直接存檔到離線儲存體 (S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive)。如需詳細資訊，請參閱使用您的備份軟體來測試您的閘道設定。	2018 年 11 月 13 日

支援 Storage Gateway 硬體設備	Storage Gateway 硬體設備包含預先安裝在第三方伺服器的 Storage Gateway 軟體。您可以從 AWS 管理主控台管理裝置。設備可以託管檔案、磁帶和磁碟區閘道。如需詳細資訊，請參閱使用 Storage Gateway 硬體設備。	2018 年 9 月 18 日
與 Microsoft System Center 2016 Data Protection Manager (DPM) 的相容性	磁帶閘道現與 Microsoft System Center 2016 Data Protection Manager (DPM) 相容。您現在可以使用 Microsoft DPM 將您的資料備份到 Amazon S3，並直接存檔到離線儲存體 (S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive)。如需詳細資訊，請參閱使用 Microsoft System Center Data Protection Manager 測試設定。	2018 年 7 月 18 日
支援伺服器訊息區塊 (SMB) 通訊協定	檔案閘道新增檔案共享的伺服器訊息區塊 (SMB) 通訊協定支援。如需詳細資訊，請參閱建立檔案共享。	2018 年 6 月 20 日
支援檔案共享、快取磁碟區和虛擬磁帶加密	您現在可以使用 AWS Key Management Service (AWS KMS) 加密寫入檔案共享、快取磁碟區或虛擬磁帶的資料。您現可使用 AWS Storage Gateway API 執行此作業。如需詳細資訊，請參閱使用 AWS KMS進行資料加密。	2018 年 6 月 12 日

NovaStor DataCenter/Network 的支援	磁帶閘道現在支援 NovaStor DataCenter/Network。您現在可以使用 NovaStor DataCenter/Network 6.4 版或 7.1 版將您的資料備份到 Amazon S3，並直接存檔到離線儲存體 (S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive)。如需詳細資訊，請參閱使用 NovaStor DataCenter/Network 測試設定。	2018 年 5 月 24 日

舊版更新

下表說明 2018 年 5 月前每個《AWS Storage Gateway 使用者指南》版本的重要變更。

變更	描述	變更日期
支援 S3 One Zone_IA 儲存類別	您現在可為檔案閘道選擇 S3 One Zone_IA，做為您檔案共享的預設儲存類別。使用此儲存類別，您可以將您的物件資料存放在 Amazon S3 的單一可用區域中。如需詳細資訊，請參閱建立檔案共享。	2018 年 4 月 4 日
新 區域	磁帶閘道現已在亞太區域 (新加坡) 提供。如需詳細資訊，請參閱 AWS 區域 支援 Storage Gateway。	2018 年 4 月 3 日
支援重新整理快取通知、申請者付款，以及適用於 Amazon S3 儲存貯體的標準 ACL。	當閘道完成重新整理您 Amazon S3 儲存貯體的快取時，您現在可以使用檔案閘道收到通知。如需詳細資訊，請參閱 Storage Gateway API 參考中的 RefreshCache.html。 檔案閘道現可讓申請者或讀者支付存取的費用，而不是儲存貯體擁有者支付存取的費用。 檔案閘道現可讓您向映射至 NFS 檔案共享之 S3 儲存貯體的擁有者提供完全控制。	2018 年 3 月 1 日

變更	描述	變更日期
	如需詳細資訊，請參閱建立檔案共享。	
支援 Dell EMC NetWorker V9.x	磁帶閘道現在支援 Dell EMC NetWorker V9.x。您現在可以使用 Dell EMC NetWorker V9.x 將您的資料備份到 Amazon S3，並直接存檔到離線儲存體 (S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive)。如需詳細資訊，請參閱使用 Dell EMC NetWorker 測試設定。	2018 年 2 月 27 日
新 區域	Storage Gateway 現已在歐洲 (巴黎) 區域提供。如需詳細資訊，請參閱 AWS 區域 支援 Storage Gateway。	2017 年 12 月 18 日
支援 MIME 類型的檔案上傳通知和猜想	當所有寫入您 NFS 檔案共享的檔案皆已上傳到 Amazon S3 時，檔案閘道現在可讓您收到通知。如需詳細資訊，請參閱 Storage Gateway API 參考中的 NotifyWhenUploaded。 檔案閘道現在可對以副檔名為基礎的上傳物件使用 MIME 類型的猜想。如需詳細資訊，請參閱建立檔案共享。	2017 年 11 月 21 日
支援 VMware ESXi 虛擬化管理程序 6.5 版	AWS Storage Gateway 現在支援 VMware ESXi Hypervisor 6.5 版。這是 4.1、5.0、5.1、5.5 和 6.0 版以外的支援。如需詳細資訊，請參閱支援的 Hypervisor 與主機需求。	2017 年 9 月 13 日
Commvault 11 相容性	磁帶閘道現在與 Commvault 11 相容。您現在可以使用 Commvault 將您的資料備份到 Amazon S3，並直接存檔到離線儲存體 (S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive)。如需詳細資訊，請參閱使用 Commvault 測試您的設定。	2017 年 9 月 12 日
檔案閘道支援 Microsoft Hyper-V Hypervisor	您現在可以將檔案閘道部署在 Microsoft Hyper-V Hypervisor。如需相關資訊，請參閱 支援的 Hypervisor 與主機需求。	2017 年 6 月 22 日

變更	描述	變更日期
支援 3 到 5 小時的存檔磁帶擷取	您現在可使用磁帶閘道從存檔擷取磁帶，為時 3 到 5 小時。您也可以從您的備份應用程式或您的虛擬磁帶櫃 (VTL) 判斷寫入磁帶的資料量。如需詳細資訊，請參閱檢視磁帶使用情況。	2017 年 5 月 23 日
新 區域	Storage Gateway 現已在亞太區域 (孟買) 提供。如需詳細資訊，請參閱 AWS 區域 支援 Storage Gateway。	2017 年 5 月 02 日
更新檔案共享設定 支援檔案共享的快取重新整理	檔案閘道現於檔案共享設定中新增掛載選項。您現在可為您的檔案共享設定 squash 和唯讀選項。如需詳細資訊，請參閱建立檔案共享。 檔案閘道現可在 Amazon S3 儲存貯體中尋找自閘道上次列出儲存貯體內容並快取結果後，曾新增或移除的物件。如需詳細資訊，請參閱 API 參考中的 RefreshCache。	2017 年 3 月 28 日
支援複製磁碟區	對於快取磁碟區閘道， AWS Storage Gateway 現在支援從現有磁碟區複製磁碟區的功能。如需複製磁碟區的詳細資訊，請參閱複製磁碟區。	2017 年 3 月 16 日
支援 Amazon 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。如需如何建立檔案閘道並將其部署到 EC2 執行個體的詳細資訊，請參閱建立和啟用 Amazon S3 檔案閘道或建立並啟用 Amazon FSx 檔案閘道。如需如何啟動檔案閘道 AMI 的詳細資訊，請參閱在 Amazon EC2 主機上部署 S3 檔案閘道或在 Amazon EC2 主機上部署 FSx 檔案閘道。	2017 年 2 月 08 日
Arcserve 17 相容性	磁帶閘道現在與 Arcserve 17 相容。您現在可以使用 Arcserve 將您的資料備份到 Amazon S3 並直接存檔到 S3 Glacier Flexible Retrieval。如需詳細資訊，請參閱使用 Arcserve Backup r17.0 來測試您的設定。	2017 年 1 月 17 日

變更	描述	變更日期
新 區域	Storage Gateway 現已在歐洲 (倫敦) 區域提供。如需詳細資訊，請參閱 AWS 區域 支援 Storage Gateway。	2016 年 12 月 13 日
新 區域	Storage Gateway 現已在加拿大 (中部) 區域提供。如需詳細資訊，請參閱 AWS 區域 支援 Storage Gateway。	2016 年 12 月 08 日
支援檔案閘道	除了磁碟區閘道和磁帶閘道之外，Storage Gateway 道現在還提供檔案閘道。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
Backup Exec 16	磁帶閘道現在與 Backup Exec 16 相容。您現在可以使用 Backup Exec 16 將您的資料備份到 Amazon S3，並直接存檔到離線儲存體 (S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive)。如需詳細資訊，請參閱使用 Veritas Backup Exec 測試您的設定。	2016 年 11 月 7 日
Micro Focus (HPE) Data Protector 9.x 相容性	磁帶閘道現在與 Micro Focus (HPE) Data Protector 9.x 相容。您現在可以使用 HPE Data Protector 將您的資料備份到 Amazon S3 並直接存檔到 S3 Glacier Flexible Retrieval。如需詳細資訊，請參閱使用 Micro Focus (HPE) Data Protector 測試您的設定。	2016 年 11 月 2 日
新 區域	Storage Gateway 現已在美國東部 (俄亥俄) 區域提供。如需詳細資訊，請參閱 AWS 區域 支援 Storage Gateway。	2016 年 10 月 17 日
重新設計 Storage Gateway 主控台	Storage Gateway 管理主控台已重新設計，讓閘道、磁碟區和虛擬磁帶的設定、管理和監控變得更容易。使用者介面現在提供可篩選的檢視，並提供 CloudWatch 和 Amazon EBS 等整合 AWS 服務的直接連結。如需詳細資訊，請參閱註冊 AWS 帳戶。	2016 年 8 月 30 日

變更	描述	變更日期
Veeam Backup & Replication V9 Update 2 或更新版本相容性	磁帶閘道現在與 Veeam Backup & Replication V9 Update 2 或更新版本相容 (即 9.0.0.1715 版或更新版本)。您現在可以使用 Veeam Backup Replication V9 Update 2 或更新版本將您的資料備份到 Amazon S3，並直接存檔到離線儲存體 (S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive)。如需詳細資訊，請參閱使用 Veeam Backup & Replication 測試設定。	2016 年 8 月 15 日
較長的磁碟區和快照 ID	Storage Gateway 引入了較長的磁碟區和快照 ID。您可以為磁碟區、快照和其他支援 AWS 的資源啟用較長的 ID 格式。如需詳細資訊，請參閱了解 Storage Gateway 資源和資源 ID。	2016 年 4 月 25 日
新 區域 支援存放磁碟區大小上限為 512 TiB 的儲存體 Storage Gateway 本機主控台的其他閘道更新和增強功能	亞太區域 (首爾) 區域現在可以使用磁帶閘道。如需詳細資訊，請參閱AWS 區域 支援 Storage Gateway。 您現在可以建立上限 32 個儲存體磁碟區、每個磁碟區大小上限 16 TiB、儲存總量上限 512 TiB 的存放磁碟區。如需詳細資訊，請參閱儲存磁碟區架構和 AWS Storage Gateway 配額。 虛擬磁帶櫃中所有磁帶的總大小增加到 1 PiB。如需詳細資訊，請參閱AWS Storage Gateway 配額。 您現在可以在 Storage Gateway 主控台上設定您 VM 本機主控台的密碼。如需相關資訊，請參閱從 Storage Gateway 主控台設定本機主控台密碼。	2016 年 3 月 21 日
Dell EMC NetWorker 8.x 相容性	磁帶閘道現在與 Dell EMC NetWorker 8.x 相容。您現在可以使用 Dell EMC NetWorker 將您的資料備份到 Amazon S3，並直接存檔到離線儲存體 (S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive)。如需詳細資訊，請參閱使用 Dell EMC NetWorker 測試設定。	2016 年 2 月 29 日

變更	描述	變更日期
支援 VMware ESXi Hypervisor 6.0 版和 Red Hat Enterprise Linux 7 iSCSI 啟動器	AWS Storage Gateway 現在支援 VMware ESXi Hypervisor 6.0 版和 Red Hat Enterprise Linux 7 iSCSI 啟動器。如需詳細資訊，請參閱支援的 Hypervisor 與主機需求及支援的 iSCSI 啟動器。	2015 年 10 月 20 日
內容重組	此版本包含這項改善：文件現在包含管理啟用的閘道一節，其結合所有閘道解決方案常見的管理任務。您可在後文中找到在部署和啟用閘道後，如何管理閘道的說明。如需詳細資訊，請參閱管理磁碟區閘道。	
支援快取磁碟區大小上限為 1,024 TiB 的儲存體	您現在可以建立上限 32 個儲存磁碟區、每個磁碟區大小上限 32 TiB、儲存總量上限 1,024 TiB 的快取磁碟區。如需詳細資訊，請參閱快取磁碟區架構和 AWS Storage Gateway 配額。	2015 年 9 月 16 日
支援 VMware ESXi 虛擬化管理程序的 VMXNET3 (10 GbE) 網路轉接器類型	如果您的閘道是託管在 VMware ESXi 虛擬化管理程序上，您就可以重新設定閘道使用 VMXNET3 轉接器類型。如需詳細資訊，請參閱為您的閘道設定網路轉接器。	
效能增強功能	Storage Gateway 上傳率上限已增加到每秒 120 MB，下載速率上限也已增加到每秒 20 MB。	
Storage Gateway 本機主控台的其他增強功能和更新	Storage Gateway 本機主控台已更新並使用額外的功能強化，協助您執行維護任務。如需詳細資訊，請參閱設定您的閘道網路。	
支援標籤	Storage Gateway 現在支援資源標籤。您現在可以將標籤新增到閘道、磁碟區和虛擬磁帶，以便更容易管理它們。如需詳細資訊，請參閱為 Storage Gateway 資源加上標籤。	2015 年 9 月 2 日

變更	描述	變更日期
Quest (之前稱為 Dell) NetVault Backup 10.0 相容性	磁帶閘道現在與 Quest NetVault Backup 10.0 相容。您現在可以使用 Quest NetVault Backup 10.0 將您的資料備份到 Amazon S3，並直接存檔到離線儲存體 (S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive)。如需詳細資訊，請參閱使用 Quest NetVault Backup 來測試您的設定。	2015 年 6 月 22 日
支援存放磁碟區閘道設定的 16 TiB 的儲存體磁碟區 支援 Storage Gateway 本機主控台的系統資源檢查 支援 Red Hat Enterprise Linux 6 iSCSI 啟動器	Storage Gateway 現在支援存放磁碟區閘道設定的 16 TiB 的儲存體磁碟區。您現在可以建立 12 個 16 TiB 的儲存磁碟區，儲存總量上限為 192 TiB。如需詳細資訊，請參閱儲存磁碟區架構。 您現在可以判斷您的系統資源 (虛擬 CPU 核心、根磁碟區大小和 RAM) 是否足夠閘道正常運作。如需詳細資訊，請參閱 檢視閘道系統資源狀態 或 檢視閘道系統資源狀態 。 Storage Gateway 現在支援 Red Hat Enterprise Linux 6 iSCSI 啟動器。如需詳細資訊，請參閱設定磁碟區閘道的需求。 此版本包含下列 Storage Gateway 改善功能和更新： • 您現在可在 Storage Gateway 主控台中查看到您閘道上次成功套用軟體更新的日期和時間。如需詳細資訊，請參閱管理閘道更新。 • 您可以使用 Storage Gateway 提供的 API 列出連線到您儲存磁碟區的 iSCSI 啟動器。如需詳細資訊，請參閱 API 參考中的 ListVolumeInitiators。	2015 年 6 月 3 日

變更	描述	變更日期
支援 Microsoft Hyper-V 虛擬化管理程序 2012 版和 2012 R2	Storage Gateway 現在支援 Microsoft Hyper-V Hypervisor 2012 版和 2012 R2。這是 Microsoft Hyper-V 虛擬化管理程序 2008 R2 版以外的支援。如需詳細資訊，請參閱支援的 Hypervisor 與主機需求。	2015 年 4 月 30 日
Symantec Backup Exec 15 相容性	磁帶閘道現在與 Symantec Backup Exec 15 相容。您現在可以使用 Symantec Backup Exec 15 將您的資料備份到 Amazon S3，並直接存檔到離線儲存體 (S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive)。如需詳細資訊，請參閱使用 Veritas Backup Exec 測試您的設定。	2015 年 4 月 6 日
儲存磁碟區的 CHAP 身分驗證支援	Storage Gateway 現在支援設定儲存磁碟區的 CHAP 身分驗證。如需詳細資訊，請參閱為您的磁碟區設定 CHAP 驗證。	2015 年 4 月 2 日
支援 VMware ESXi 虛擬化管理程序 5.1 和 5.5 版	Storage Gateway 現在支援 VMware ESXi Hypervisor 5.1 和 5.5 版。這是 VMware ESXi Hypervisor 4.1 和 5.0 版以外的支援。如需詳細資訊，請參閱支援的 Hypervisor 與主機需求。	2015 年 3 月 30 日
支援 Windows CHKDSK 公用程式	Storage Gateway 現在支援 Windows CHKDSK 公用程式。您可以使用此公用程式來驗證磁碟區的完整性以及修正磁碟區的錯誤。如需詳細資訊，請參閱針對磁碟區問題進行疑難排解。	2015 年 3 月 04 日

變更	描述	變更日期
與 整合 AWS CloudTrail 以擷取 API 呼叫	Storage Gateway 現在已與 AWS CloudTrail Amazon Web Services 帳戶中由 Storage Gateway 發出或代表發出的 . AWS CloudTrail captures API 呼叫整合，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。如需詳細資訊，請參閱在 中記錄和監控 AWS Storage Gateway。 此版本包含下列 Storage Gateway 改善功能和更新： • 在快取儲存中有髒數據的虛擬磁帶 (亦即包含已上傳至 AWS的內容)，現在會在閘道的快取磁碟機發生變更時復原。如需詳細資訊，請參閱從無法還原的閘道復原虛擬磁帶。	2014 年 12 月 16 日

變更	描述	變更日期
其他備份軟體和媒體更換器相容性	磁帶閘道現在與下列備份軟體相容： • Symantec Backup Exec 2014 • Microsoft System Center 2012 R2 Data Protection Manager • Veeam Backup & Replication V7 • Veeam Backup & Replication V8 您現在可以使用這四種備份軟體產品配合 Storage Gateway 虛擬磁帶櫃 (VTL)，備份到 Amazon S3 並直接存檔到離線儲存體 (S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive)。如需詳細資訊，請參閱使用您的備份軟體來測試您的閘道設定。 Storage Gateway 現在提供的額外媒體更換器，可使用新的備份軟體。 此版本包含其他 AWS Storage Gateway 改善和更新。	2014 年 11 月 3 日
歐洲 (法蘭克福) 區域	Storag Gateway 現已在歐洲 (法蘭克福) 區域提供。如需詳細資訊，請參閱 AWS 區域 支援 Storage Gateway。	2014 年 10 月 23 日
內容重組	已建立入門一節，其適用於所有閘道解決方案。您可在後文中尋找下載、部署和啟用閘道的指示。在您部署和啟用閘道之後，您可以繼續進一步了解存放磁碟區、快取磁碟區和磁帶閘道設定的特定說明。如需詳細資訊，請參閱建立磁帶閘道。	2014 年 5 月 19 日

變更	描述	變更日期
Symantec Backup Exec 2012 相容性	磁帶閘道現在與 Symantec Backup Exec 2012 相容。您現在可以使用 Symantec Backup Exec 2012 將您的資料備份到 Amazon S3，並直接存檔到離線儲存體 (S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive)。如需詳細資訊，請參閱使用 Veritas Backup Exec 測試您的設定。	2014 年 4 月 28 日
支援 Windows Server 容錯移轉叢集 支援 VMware ESX 啟動器 支援在 Storage Gateway 本機主控台上執行組態任務	• 如果主機使用 Windows Server 容錯移轉叢集 (WSFC) 協調存取，Storage Gateway 現在支援將多個主機連線到相同的磁碟區。不過，您無法在不使用 WSFC 的情況下，將多個主機連線到該相同的磁碟區。 • Storage Gateway 現在可讓您透過 ESX 主機直接管理儲存連線。這提供使用位在 VM 訪客作業系統中之啟動器的替代選項。 • Storage Gateway 現可支援在 Storage Gateway 本機主控台上執行組態任務。如需在部署於內部部署之閘道上執行組態任務的資訊，請參閱在 VM 本機主控台上執行任務或在 VM 本機主控台上執行任務。如需在部署於 EC2 執行個體之閘道上執行組態任務的資訊，請參閱在 Amazon EC2 本機主控台上執行任務或在 Amazon EC2 本機主控台上執行任務。	2014 年 1 月 31 日

變更	描述	變更日期
支援虛擬磁帶櫃 (VTL) 以及 API 版本 2013-06-30 簡介	Storage Gateway 會將內部部署軟體設備與雲端儲存連線，以整合您的內部部署 IT 環境與 AWS 儲存基礎設施。在磁碟區閘道之外 (快取磁碟區和存放磁碟區)，Storage Gateway 現可支援使用虛擬磁帶櫃 (VTL) 的閘道。您可以設定磁帶閘道在每個閘道最多 10 個虛擬磁帶機。每個虛擬磁帶機都會回應 SCSI 命令集，因此您現有的內部部署備份應用程式不必修改即可運作。如需詳細資訊，請參閱《AWS Storage Gateway 使用者指南》中的以下主題： • 如需架構概觀，請參閱磁帶閘道的運作方式 (架構)。 • 若要開始使用磁帶閘道，請參閱建立磁帶閘道。	2013 年 11 月 5 日
支援 Microsoft Hyper-V	Storage Gateway 現在能夠讓您在 Microsoft Hyper-V 虛擬化平台上部署內部部署閘道。部署在 Microsoft Hyper-V 的閘道擁有和現有內部部署 Storage Gateway 相同的所有功能和特性。若要開始使用 Microsoft Hyper-V 部署閘道，請參閱支援的 Hypervisor 與主機需求。	2013 年 4 月 10 日
支援在 Amazon EC2 上部署閘道	Storage Gateway 現在提供了在 Amazon Elastic Compute Cloud (Amazon EC2) 中部署閘道的功能。您可以使用 AWS Marketplace 中提供的 Storage Gateway AMI 在 Amazon EC2 中啟動閘道執行個體。若要使用 Storage Gateway AMI 開始部署閘道，請參閱 部署磁碟區閘道的自訂 Amazon EC2 執行個體。	2013 年 1 月 15 日

變更	描述	變更日期
支援快取磁碟區和 API 2012-06-30 版簡介	在此版本中，Storage Gateway 引入了對快取磁碟區的支援。快取磁碟區可將擴展內部部署儲存基礎設施的需求減到最低，同時讓應用程式以低延遲方式存取其作用中的資料。您可以建立最高 32 TiB 的儲存磁碟區，並透過內部部署應用程式伺服器，將這些磁碟區掛載為 iSCSI 裝置。寫入您快取磁碟區的資料，會存放在 Amazon Simple Storage Service (Amazon S3) 中，而只有最近寫入和讀取資料的快取，才會存放在您內部部署儲存硬體的本機上。快取磁碟區允許您利用 Amazon S3 處理接受較高延遲的資料，例如不常存取的較舊資料，同時為需要低延遲存取的資料保持內部部署儲存體。 在此版本中，Storage Gateway 也引進了新的 API 版本，除支援目前的操作外，還提供新的操作以支援快取磁碟區。 如需兩種 Storage Gateway 解決方案的詳細資訊，請參閱 磁碟區閘道的運作方式。 您也可以嘗試測試設定。如需相關指示，請參閱建立磁帶閘道。	2012 年 10 月 29 日

變更	描述	變更日期
API 和 IAM 支援	在此版本中，Storage Gateway 推出 API 支援以及對 AWS Identity and Access Management(IAM) 的支援。 • API 支援：您現在可以透過撰寫程式的方式設定與管理您的 Storage Gateway 資源。如需 API 的詳細資訊，請參閱《AWS Storage Gateway 使用者指南》中的 Storage Gateway 的 API 參考。 • IAM 支援： AWS Identity and Access Management (IAM) 可透過 IAM 政策，讓您建立使用者以及管理使用者對您 Storage Gateway 資源的存取。如需 IAM 政策範例，請參閱Identity and Access Management for AWS Storage Gateway。如需 IAM 的詳細資訊，請參閱 AWS Identity and Access Management (IAM)的詳細資訊頁面。	2012 年 5 月 9 日
靜態 IP 支援	您現在可以為本機閘道指定靜態 IP。如需詳細資訊，請參閱設定您的閘道網路。	2012 年 3 月 5 日
新指南	這是《AWS Storage Gateway 使用者指南》的第一版。	2012 年 1 月 24 日

Storage Gateway AL2 至 AL2023 遷移行銷活動

AWS 正在將 Storage Gateway 設備作業系統 (OS) 從 Amazon Linux 2 轉換為 AL2023，以啟用新的混合雲端儲存功能，並維持最佳效能和安全標準。此轉換將影響所有以 AL2-based Storage Gateway 設備版本 S3 檔案閘道版本 1.x、磁帶閘道版本 2.x 和磁碟區閘道版本 2.x。您需要在 2026 年 6 月 30 日之前完成遷移，之後 AWS 將停止支援這些系統。

您可以識別閘道是否需要透過多種方法進行遷移。 AWS 主控台會在受影響閘道的閘道詳細資訊索引標籤中顯示棄用訊息。此外，`DescribeGatewayInformation`API 提供程式設計存取權，以檢查棄用日期欄位。 AWS 運作狀態儀表板會在受影響的資源索引標籤下列出受影響的閘道。不過，遷移閘道之後，不會立即更新清單。遷移程序本身以資料安全為優先考量，在遷移開始 AWS 之前將內部部署閘道 VM 資料的副本存放在 中，以便在需要時輕鬆復原。

AWS 提供針對每個閘道類型的完整遷移指南。完成遷移後，您應該檢查 AWS 主控台閘道詳細資訊索引標籤中是否不再顯示棄用警告，或使用 `DescribeGatewayInformation` API 確認棄用日期欄位不存在，以確認成功。關鍵是，在成功遷移至 AL2023 之後，您不得還原至 AL2 閘道，因為還原可能會導致操作問題。

在整個遷移期間， AWS 會透過電子郵件傳送每月提醒通知，以及 AWS 運作狀態儀表板的排程變更索引標籤，協助您規劃和完成遷移。如果您在遷移期間遇到問題，請聯絡 AWS Support 尋求協助和故障診斷指引。

快速連結和資源

閘道版本遷移參考

根據閘道軟體版本編號，了解哪些閘道需要遷移非常簡單。請務必注意，即使最近啟動以 Amazon Linux 2 作業系統為基礎的閘道，仍需要在 2026 年 6 月 30 日之前遷移。

閘道類型	AL2 版本 （需要遷移）	AL2023 版本 （目標）
S3 檔案閘道	1.x 版	2.x 版
Tape Gateway	2.x 版	3.x 版
Volume Gateway	2.x 版	3.x 版

遷移時間軸

遷移時間表包含數個關鍵里程碑：

- 2025 年 10 月 28 日：從 Storage Gateway 主控台啟動的所有新閘道部署都將預設為 AL2023 映像。
- 2026 年 1 月 5 日： AWS 將開始限制新的 AL2 閘道啟用。
- 2026 年 6 月 30 日：AL2-based閘道將停止接收軟體更新，且 AWS 支援將結束。在此日期之後，雖然您可以繼續使用 AL2-based設備，但它們不會收到新的軟體更新、安全修補程式或錯誤修正，而維護這些系統將成為您的唯一責任。

遷移前檢查清單

> **Important**
>
> 開始遷移程序之前，請確認下列要求，以確保成功遷移。

- 使用最新的閘道映像。建立新的 Storage Gateway VM 時：
  - 對於 Amazon EC2 閘道，請使用公有 SSM 參數的最新 AMI，或使用 Storage Gateway 主控台。
  - 對於內部部署閘道，請從 Storage Gateway 主控台下載最新的 VM 映像。
- 符合硬體組態。確保新的閘道 VM 使用與現有閘道相同的 CPU、記憶體和網路輸送量。對於 EC2 閘道，請使用相同的執行個體類型。
- 驗證根磁碟大小。新閘道 VM 的根磁碟大小必須至少與現有閘道的根磁碟相同。如果現有根磁碟的可用空間少於 20 GB，請將新的根磁碟大小調整為：（現有根磁碟大小）+ (20 GB 減去現有根磁碟上的可用空間）。
- 套用待定軟體更新。開始遷移之前，請在現有閘道上套用任何待定的軟體更新。開啟 Storage Gateway 主控台，選取您的閘道，然後在可用時選擇立即更新。
- 驗證來自新閘道的網路連線。開始遷移之前，請確認新的閘道 VM 可以到達：
  - Storage Gateway 服務端點（或您的 VPC 端點）。
  - 使用閘道本機主控台的網路連線測試來驗證所有端點通過。

遷移指南

- S3 檔案閘道遷移指南

- 磁帶閘道遷移指南
- 磁碟區閘道遷移指南

支援和監控

- Storage Gateway 主控台
- AWS 個人運作狀態儀表板
- 聯絡 AWS 支援

常見問答集

遷移期間我的資料會發生什麼情況？

AWS 在整個遷移過程中，您的資料會長期存放在 中。遷移程序包括在 中存放現場部署閘道 VM 資料的副本 AWS ，以便在需要時輕鬆復原。

遷移期間是否會停機？

遷移時間和任何潛在的服務中斷取決於您的閘道類型和組態。如需詳細資訊，請參閱您部署的閘道特定遷移指南。

如果我未在 2026 年 6 月 30 日之前遷移，會發生什麼情況？

您的閘道會繼續正常運作，且資料會安全地存放在 中 AWS，但您必須在 2026 年 6 月 30 日之前遷移受影響的閘道，才能繼續接收更新和支援。

遷移後是否可以繼續使用以 AL2 為基礎的閘道？

否，在成功遷移後，您不應該將 AL2 閘道與新的 AL2023 閘道搭配使用。之後請僅使用新的 AL2023-based閘道。同時使用 AL2 和 AL2023 閘道可能會導致操作問題。

我在遷移期間遇到問題。我該怎麼辦？

如需協助，請聯絡 AWS Support。我們的支援團隊可協助您疑難排解遷移問題，並引導您完成整個程序。

磁碟區閘道設備軟體的版本備註

這些版本備註說明磁碟區閘道設備每個版本隨附的新功能和更新功能、改善和修正。每個軟體版本都會以發行日期和唯一的版本編號來識別。

您可以在 Storage Gateway 主控台中檢查閘道的詳細資訊頁面，或使用類似下列的 AWS CLI 命令呼叫 DescribeGatewayInformation API 動作，以判斷閘道的軟體版本編號： Storage Gateway

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

版本編號會在 API 回應的 `SoftwareVersion` 欄位中傳回。

> **Note**
>
> 在下列情況下，閘道不會報告軟體版本資訊：
>
> - 閘道已離線。
> - 閘道正在執行不支援版本報告的較舊軟體。
> - 閘道類型為 FSx 檔案閘道。

如需磁碟區閘道更新的詳細資訊，包括如何修改閘道的預設自動維護和更新排程，請參閱使用 AWS Storage Gateway更新。

如需將磁碟區閘道從 Amazon Linux 2 遷移至 AL2023 的詳細資訊，請參閱 AL2 到 AL2023 遷移。

Amazon Linux 2023 (AL2023) 型閘道

下表列出以 AL2023 為基礎的閘道版本備註。

> **Note**
>
> 閘道版本 2.x.x 無法更新為 3.x.x。

版本日期	軟體版本	版本備註
2026-08-24	3.2.9	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能 • 已解決意外關機的問題
2026-07-30	3.2.8	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2026-06-30	3.2.7	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能 • 新增對 PrivateLink FIPS 端點的支援
2026-05-28	3.2.6	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能 • 已改善 2.x 到 3.x (AL2 到 AL2023) 的遷移
2026-05-04	3.2.5	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能 • 已解決預設網路 MTU 設定影響 HyperV 型閘道的問題
2026-04-01	3.2.4	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2026-03-02	3.2.3	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能

版本日期	軟體版本	版本備註
		• 已解決某些閘道上閘道日誌的問題
2026-02-12	3.2.2	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能 • 已解決將 VPC 端點 (VPCE) 設定為靜態 IP 地址之 AL2023 閘道上軟體更新的問題
2026-02-02	3.2.0	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2026-01-06	3.1.0	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2025-12-04	3.0.6	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2025-11-06	3.0.5	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2025-10-10	3.0.4	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2025-09-12	3.0.3	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能

版本日期	軟體版本	版本備註
2025-08-29	3.0.2	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能 • 已解決靜態 IP 組態的問題
2025-08-18	3.0.1	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2025-07-16	3.0.0	• 新作業系統的初始版本 • 新增 IPv6 支援

以 Amazon Linux 2 (AL2) 為基礎的閘道

下表列出以 為基礎的閘道版本備註AL2。

版本日期	軟體版本	版本備註
2026-09-01	2.14.8	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2026-07-30	2.14.7	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2026-06-30	2.14.6	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2026-05-28	2.14.5	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能

版本日期	軟體版本	版本備註
2026-05-04	2.14.4	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2026-04-01	2.14.3	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2026-03-02	2.14.2	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2026-02-02	2.14.1	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2026-01-05	2.14.0	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2025-12-05	2.13.0	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2025-11-03	2.12.15	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2025-10-01	2.12.14	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2025-09-02	2.12.13	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能

版本日期	軟體版本	版本備註
2025-07-31	2.12.12	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2025-07-01	2.12.11	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2025-06-02	2.12.10	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2025-05-01	2.12.9	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2025-05-01	2.12.8	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2025-04-01	2.12.7	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2025-03-04	2.12.6	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2025-02-04	2.12.5	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能 • 已解決在軟體更新後，閘道可能卡在關閉狀態的問題

版本日期	軟體版本	版本備註
2025-01-07	2.12.3	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2024-12-06	2.12.2	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2024-11-06	2.12.1	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2024-10-03	2.12.0	• 已解決 iSCSI 啟動器在閘道重新啟動或閘道軟體更新後不會自動重新連線至磁碟區的問題 • 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2024-08-30	2.11.0	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能
2024-07-29	2.10.0	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能 • 其他錯誤修正和增強功能
2024-06-17	2.9.2	• 更新作業系統和軟體元素，以改善新閘道和現有閘道的安全性和效能

版本日期	軟體版本	版本備註
2024-05-28	2.9.0	• 減少軟體更新期間的閘道重新啟動時間 • 減少用於估計網路頻寬的傳輸資料量
2024-05-08	2.8.3	• 解決使用 SOCKS5 Proxy 時的雲端連線問題
2024-04-10	2.8.1	• 解決 2.8.0 中引入的記憶體用量問題 • 安全性修補程式更新 • 改善軟體更新程序 • 已解決新閘道遺失的網路時間通訊協定 (NTP) 元件
2024-03-06	2.8.0	• 更新作業系統和軟體元素，以改善新閘道的安全性和效能 • 安全性修補程式更新
2023-12-19	2.7.0	• 更新作業系統和軟體元素，以改善新閘道的安全性和效能
2023-12-14	2.6.6	• 維護版本

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。