



ONTAP 使用者指南

# FSx for OnTAP



# FSx for OnTAP: ONTAP 使用者指南

Copyright © 2025 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 Amazon FSx for NetApp ONTAP ? ..... | 1  |
| FSx for ONTAP 的功能 .....                 | 2  |
| 安全性和資料保護 .....                          | 2  |
| 監控工具 .....                              | 3  |
| FSx for ONTAP 定價 .....                  | 3  |
| 上的 FSx for ONTAP AWS re:Post .....      | 3  |
| 您是第一次使用 Amazon FSx 嗎 ? .....            | 4  |
| 運作方式 .....                              | 5  |
| 檔案系統 .....                              | 5  |
| 儲存虛擬機器 .....                            | 5  |
| 磁碟區 .....                               | 6  |
| 儲存層 .....                               | 6  |
| 資料分層 .....                              | 6  |
| 儲存效率 .....                              | 6  |
| 存取您的資料 .....                            | 7  |
| 管理 FSx for ONTAP 資源 .....               | 7  |
| 開始使用 .....                              | 8  |
| 設定 .....                                | 8  |
| 註冊 AWS 帳戶 .....                         | 8  |
| 建立具有管理存取權的使用者 .....                     | 9  |
| 下一步驟 .....                              | 10 |
| 建立 FSx for ONTAP 檔案系統 .....             | 10 |
| 掛載您的檔案系統 .....                          | 13 |
| 清除資源 .....                              | 14 |
| AWS 區域 .....                            | 15 |
| 存取您的資料 .....                            | 19 |
| 支援的用戶端 .....                            | 20 |
| 使用區塊儲存協定 .....                          | 21 |
| 從 內存取資料 AWS 雲端 .....                    | 21 |
| 從相同的 VPC 存取資料 .....                     | 22 |
| 從不同的 VPC 存取資料 .....                     | 22 |
| 從內部部署存取資料 .....                         | 25 |
| 從內部部署存取 NFS、SMB、ONTAP CLI 和 API .....   | 25 |
| 從內部部署存取叢集間端點 .....                      | 27 |

|                                     |    |
|-------------------------------------|----|
| 設定路由以從 VPC 外部存取多可用區域檔案系統 .....      | 27 |
| 設定路由以從內部部署存取多可用區域檔案系統 .....         | 28 |
| 在 Linux 用戶端上掛載 .....                | 29 |
| 使用 /etc/fstab 在執行個體重新啟動時自動掛載 .....  | 30 |
| 在 Windows 用戶端上掛載 .....              | 32 |
| 先決條件 .....                          | 32 |
| 在 macOS 用戶端上掛載 .....                | 33 |
| 佈建 Linux 的 iSCSI .....              | 35 |
| 開始之前 .....                          | 36 |
| 在 Linux 主機上安裝和設定 iSCSI .....        | 37 |
| 在 FSx for ONTAP 檔案系統上設定 iSCSI ..... | 39 |
| 在 Linux 用戶端上安裝 iSCSI LUN .....      | 41 |
| 佈建適用於 Windows 的 iSCSI .....         | 47 |
| 在 Windows 用戶端上設定 iSCSI .....        | 48 |
| 在 FSx for ONTAP 檔案系統上設定 iSCSI ..... | 49 |
| 在 Windows 用戶端上掛載 iSCSI LUN .....    | 51 |
| 驗證您的 iSCSI 組態 .....                 | 54 |
| 佈建適用於 Linux 的 NVMe/TCP .....        | 55 |
| 開始之前 .....                          | 56 |
| 在 Linux 主機上安裝和設定 NVMe .....         | 56 |
| 在 FSx for ONTAP 檔案系統上設定 NVMe .....  | 57 |
| 在 Linux 用戶端上掛載 NVMe 裝置 .....        | 60 |
| 佈建適用於 Windows 的 NVMe/TCP .....      | 65 |
| 使用其他服務 AWS 存取資料 .....               | 65 |
| 使用 Amazon WorkSpaces .....          | 65 |
| 使用 Amazon ECS .....                 | 71 |
| 使用 Amazon EVS .....                 | 74 |
| 使用 VMware 雲端 .....                  | 74 |
| 可用性、耐用性和部署選項 .....                  | 75 |
| 選擇檔案系統部署類型 .....                    | 75 |
| 單一可用區部署類型 .....                     | 75 |
| 異地同步備份部署類型 .....                    | 76 |
| 選擇檔案系統產生 .....                      | 77 |
| FSx for ONTAP 的容錯移轉程序 .....         | 78 |
| 在檔案系統上測試容錯移轉 .....                  | 79 |
| 網路資源 .....                          | 79 |

|                                |     |
|--------------------------------|-----|
| 子網路 .....                      | 79  |
| 檔案系統彈性網路介面 .....               | 80  |
| 效能 .....                       | 82  |
| 測量效能 .....                     | 82  |
| Latency (延遲) .....             | 82  |
| 輸送量和 IOPS .....                | 82  |
| SMB 多通道和 NFS nconnect 支援 ..... | 82  |
| 效能詳細資訊 .....                   | 83  |
| 部署類型對效能的影響 .....               | 85  |
| 儲存容量對效能的影響 .....               | 87  |
| 輸送量容量對效能的影響 .....              | 87  |
| 範例：儲存容量和輸送量容量 .....            | 92  |
| 管理 資源 .....                    | 94  |
| 管理儲存容量 .....                   | 94  |
| 儲存層 .....                      | 95  |
| 選擇檔案系統儲存容量 .....               | 96  |
| 檔案系統儲存容量和 IOPS .....           | 99  |
| 磁碟區儲存容量 .....                  | 117 |
| 管理檔案系統 .....                   | 138 |
| 檔案系統資源 .....                   | 138 |
| 建立檔案系統 .....                   | 140 |
| 更新檔案系統 .....                   | 152 |
| 管理 HA 對 .....                  | 155 |
| 管理 NVMe 快取 .....               | 162 |
| 監控檔案系統詳細資訊 .....               | 162 |
| 刪除檔案系統 .....                   | 164 |
| 管理 SVMs .....                  | 164 |
| 每個檔案系統的 SVMs 數目上限 .....        | 164 |
| 建立 SVMs .....                  | 165 |
| 更新 SVMs .....                  | 170 |
| 稽核檔案存取 .....                   | 172 |
| 設定工作群組 .....                   | 182 |
| 監控 SVM 詳細資訊 .....              | 188 |
| 刪除 SVMs .....                  | 188 |
| 管理磁碟區 .....                    | 190 |
| 磁碟區樣式 .....                    | 191 |

|                           |     |
|---------------------------|-----|
| 磁碟區類型 .....               | 192 |
| 磁碟區安全樣式 .....             | 193 |
| 建立磁碟區 .....               | 194 |
| 更新磁碟區 .....               | 198 |
| 移動磁碟區 .....               | 201 |
| 監控磁碟區 .....               | 204 |
| 刪除磁碟區 .....               | 206 |
| 建立 iSCSI LUN .....        | 208 |
| 後續步驟 .....                | 210 |
| 更新維護時段 .....              | 210 |
| 管理輸送量容量 .....             | 211 |
| 何時修改輸送量容量 .....           | 212 |
| 如何處理並行請求 .....            | 212 |
| 更新輸送量容量 .....             | 213 |
| 監控輸送量容量變更 .....           | 214 |
| 管理 SMB 共用 .....           | 216 |
| 使用NetApp應用程式管理 .....      | 217 |
| 註冊NetApp帳戶 .....          | 218 |
| 使用 NetApp BlueXP .....    | 219 |
| 使用 NetApp ONTAP CLI ..... | 220 |
| 使用 ONTAP REST API .....   | 223 |
| 標記 資源 .....               | 224 |
| 標籤基本概念 .....              | 224 |
| 標記您的 資源 .....             | 225 |
| 將標籤複製到備份 .....            | 226 |
| 標籤限制 .....                | 226 |
| 許可和標記 .....               | 227 |
| 保護您的資料 .....              | 228 |
| 備份磁碟區 .....               | 228 |
| 備份的運作方式 .....             | 229 |
| 儲存需求 .....                | 230 |
| 自動每日備份 .....              | 230 |
| 使用者啟動的備份 .....            | 231 |
| 將標籤複製到備份 .....            | 231 |
| 使用 AWS Backup .....       | 231 |
| 還原備份 .....                | 232 |

|                             |     |
|-----------------------------|-----|
| 備份效能 .....                  | 233 |
| 備份磁碟SnapLock區 .....         | 234 |
| 建立使用者啟動的備份 .....            | 234 |
| 還原備份 .....                  | 235 |
| 還原資料子集 .....                | 238 |
| 監控磁碟區還原進度 .....             | 239 |
| 刪除備份 .....                  | 241 |
| 使用磁碟區快照 .....               | 242 |
| 快照政策 .....                  | 243 |
| 從快照還原檔案 .....               | 243 |
| 檢視常見快照 .....                | 244 |
| 更新快照預留空間 .....              | 245 |
| 停用自動快照 .....                | 246 |
| 刪除快照 .....                  | 248 |
| 刪除快照 .....                  | 248 |
| 快照預留 .....                  | 249 |
| 使用自治勒索軟體保護來保護資料 .....       | 250 |
| ARP 的運作方式 .....             | 250 |
| ARP 所尋找的內容 .....            | 251 |
| 如何使用 ARP 回應可疑的攻擊 .....      | 251 |
| 啟用 ARP .....                | 252 |
| 回應 ARP 提醒 .....             | 254 |
| 了解 ARP 的 EMS 警示 .....       | 255 |
| 使用 保護資料 SnapLock .....      | 257 |
| SnapLock 的運作方式 .....        | 257 |
| 了解SnapLock合規 .....          | 261 |
| 了解SnapLock企業 .....          | 261 |
| 了解SnapLock保留期 .....         | 263 |
| 將檔案遞交至 WORM .....           | 265 |
| 使用 複寫您的資料 FlexCache .....   | 269 |
| FlexCache 的運作方式 .....       | 270 |
| FlexCache 寫入模式 .....        | 270 |
| FlexCache 磁碟區建立概觀 .....     | 270 |
| 建立FlexCache .....           | 271 |
| 使用 SnapMirror進行排程複寫 .....   | 276 |
| 使用 NetApp BlueXP 排程複寫 ..... | 277 |

|                                   |     |
|-----------------------------------|-----|
| 使用 ONTAP CLI 排程複寫 .....           | 277 |
| 帳單與用量報告 .....                     | 278 |
| FSx for ONTAP 帳單報告 .....          | 278 |
| FSx for ONTAP 用量報告 .....          | 281 |
| 監控檔案系統 .....                      | 285 |
| 使用 CloudWatch 進行監控 .....          | 285 |
| 存取 CloudWatch 指標 .....            | 286 |
| 在 Amazon FSx 主控台中監控 .....         | 288 |
| 檔案系統指標 .....                      | 296 |
| 第二代檔案系統指標 .....                   | 311 |
| 磁碟區指標 .....                       | 324 |
| 監控 EMS 事件 .....                   | 331 |
| EMS 事件概觀 .....                    | 332 |
| 檢視 EMS 事件 .....                   | 332 |
| 將 EMS 事件轉送至 Syslog 伺服器 .....      | 337 |
| 使用資料基礎設施洞見進行監控 .....              | 339 |
| 使用 Harvest 和 Grafana 進行監控 .....   | 339 |
| Harvest 和 Grafana 入門 .....        | 339 |
| 支援的 Harvest 儀表板 .....             | 340 |
| 不支援的 Harvest 儀表板 .....            | 341 |
| AWS CloudFormation 範本 .....       | 341 |
| Amazon EC2 執行個體類型 .....           | 341 |
| 部署程序 .....                        | 342 |
| 登入 Grafana .....                  | 345 |
| 針對 Harvest 和 Grafana 進行故障診斷 ..... | 345 |
| 使用 監控 AWS CloudTrail .....        | 348 |
| CloudTrail 中的 Amazon FSx 資訊 ..... | 348 |
| 了解 Amazon FSx 日誌檔案項目 .....        | 349 |
| 使用 Active Directory .....         | 352 |
| 自我管理 Active Directory 先決條件 .....  | 352 |
| 自我管理 Active Directory 需求 .....    | 353 |
| 網路組態需求 .....                      | 353 |
| Active Directory 服務帳戶需求 .....     | 355 |
| 自我管理 Active Directory 最佳實務 .....  | 356 |
| 將許可委派給您的 Amazon FSx 服務帳戶 .....    | 356 |
| 保持 AD 組態更新 .....                  | 357 |



|                                            |     |
|--------------------------------------------|-----|
| 使用安全群組限制 VPC 內的流量 .....                    | 358 |
| 建立傳出安全群組規則 .....                           | 358 |
| 將 SVMs 加入 Active Directory 的運作方式 .....     | 358 |
| 所需的 Active Directory 資訊 .....              | 359 |
| 管理 SVM Active Directory 組態 .....           | 360 |
| 將 SVMs 加入 Active Directory .....           | 360 |
| 更新 Active Directory 組態 .....               | 363 |
| 使用 NetApp CLI 更新 Active Directory 組態 ..... | 364 |
| 遷移至 Amazon FSx .....                       | 370 |
| 使用 SnapMirror 遷移 .....                     | 370 |
| 開始之前 .....                                 | 372 |
| 建立目的地磁碟區 .....                             | 373 |
| 記錄來源和目的地叢集間 LIFs .....                     | 374 |
| 在來源和目的地之間建立叢集對等 .....                      | 375 |
| 建立 SVM 對等互連關係 .....                        | 375 |
| 建立 SnapMirror 關係 .....                     | 376 |
| 將資料傳輸至 FSx for ONTAP 檔案系統 .....            | 377 |
| 切換至 Amazon FSx .....                       | 377 |
| 使用 遷移檔案 AWS DataSync .....                 | 379 |
| 先決條件 .....                                 | 380 |
| DataSync 遷移基本步驟 .....                      | 380 |
| 安全 .....                                   | 381 |
| 資料保護 .....                                 | 381 |
| FSx for ONTAP 中的資料加密 .....                 | 382 |
| 靜態加密 .....                                 | 383 |
| 加密傳輸中的資料 .....                             | 384 |
| 身分與存取管理 .....                              | 404 |
| 目標對象 .....                                 | 404 |
| 使用身分驗證 .....                               | 405 |
| 使用政策管理存取權 .....                            | 407 |
| FSx for ONTAP 和 IAM .....                  | 409 |
| 身分型政策範例 .....                              | 414 |
| 疑難排解 IAM .....                             | 417 |
| 使用服務連結角色 .....                             | 418 |
| 搭配 Amazon FSx 使用標籤 .....                   | 423 |
| AWS 受管政策 .....                             | 429 |

|                                              |     |
|----------------------------------------------|-----|
| AmazonFSxServiceRolePolicy .....             | 429 |
| AmazonFSxDeleteServiceLinkedRoleAccess ..... | 429 |
| AmazonFSxFullAccess .....                    | 429 |
| AmazonFSxConsoleFullAccess .....             | 430 |
| AmazonFSxConsoleReadOnlyAccess .....         | 431 |
| AmazonFSxReadOnlyAccess .....                | 432 |
| 政策更新 .....                                   | 432 |
| 使用 Amazon VPC 的檔案系統存取控制 .....                | 440 |
| Amazon VPC 安全群組 .....                        | 440 |
| 合規驗證 .....                                   | 443 |
| 介面 VPC 端點 .....                              | 444 |
| Amazon FSx 介面 VPC 端點的考量事項 .....              | 444 |
| 為 Amazon FSx API 建立介面 VPC 端點 .....           | 445 |
| 為 Amazon FSx 建立 VPC 端點政策 .....               | 445 |
| 恢復能力 .....                                   | 445 |
| 備份和還原 .....                                  | 446 |
| 快照 .....                                     | 446 |
| 可用區域 .....                                   | 446 |
| 基礎設施安全性 .....                                | 447 |
| 使用防毒軟體 .....                                 | 447 |
| ONTAP 角色和使用者 .....                           | 447 |
| 檔案系統管理員角色和使用者 .....                          | 448 |
| SVM 管理員角色和使用者 .....                          | 449 |
| 使用 Active Directory 驗證ONTAP使用者 .....         | 451 |
| 為檔案系統和 SVM 管理建立新的ONTAP使用者 .....              | 451 |
| 建立 ONTAP 使用者 .....                           | 452 |
| 建立 SVM 角色 .....                              | 454 |
| 為ONTAP使用者設定 Active Directory 身分驗證 .....      | 456 |
| 設定公有金鑰身分驗證 .....                             | 458 |
| 更新密碼需求 .....                                 | 459 |
| 更新fsxadmin帳戶密碼失敗 .....                       | 459 |
| 配額 .....                                     | 461 |
| 您可以提高的配額 .....                               | 461 |
| 每個檔案系統的資源配額 .....                            | 462 |
| 故障診斷 .....                                   | 466 |
| 設定錯誤的檔案系統 .....                              | 466 |

|                                                            |     |
|------------------------------------------------------------|-----|
| VPC 共用已停用 .....                                            | 466 |
| 無法建立多可用區域檔案系統 .....                                        | 467 |
| SSD 層已滿 90% .....                                          | 467 |
| 您無法存取您的檔案系統 .....                                          | 467 |
| 缺少路由表標籤 .....                                              | 468 |
| 太多路由 .....                                                 | 468 |
| 伺服器遺失路由 .....                                              | 469 |
| 修改或刪除 ENI .....                                            | 469 |
| 已刪除的 ENI .....                                             | 469 |
| 缺少傳入規則 .....                                               | 469 |
| 缺少傳出規則 .....                                               | 469 |
| 運算執行個體的子網路不會使用任何與檔案系統相關聯的路由表 .....                         | 469 |
| 無法更新多可用區域路由表 .....                                         | 470 |
| 無法存取 iSCSI .....                                           | 470 |
| 未共用的 VPC 子網路 .....                                         | 470 |
| 無法從不同的 VPC 和內部部署存取 NFS、SMB、ONTAP CLI 和 API .....           | 470 |
| 設定錯誤的 SVM .....                                            | 471 |
| 您的 SVM 具有離線磁碟區 .....                                       | 471 |
| 您的 SVM 具有具有 iSCSI LUN 或 NVMe/TCP 命名空間的離線磁碟區 .....          | 471 |
| 無法將 SVM 加入 AD .....                                        | 471 |
| SVM NetBIOS 名稱與主網域相同 .....                                 | 472 |
| SVM 已加入另一個 AD .....                                        | 472 |
| SVM NetBIOS 名稱已使用 .....                                    | 473 |
| FSx 無法連線到 AD 網域控制站 .....                                   | 473 |
| 連接埠組態或服務帳戶許可不足 .....                                       | 473 |
| 無效的服務帳戶登入資料 .....                                          | 474 |
| 由於服務帳戶登入資料不足，Amazon FSx 無法連線至 Active Directory 網域控制站 ..... | 474 |
| 無法連線到 AD DNS 伺服器或網域控制站 .....                               | 475 |
| 無效的 AD 網域名稱 .....                                          | 477 |
| 服務帳戶無法存取 AD 管理員群組 .....                                    | 477 |
| 指定的 OU 無效 .....                                            | 478 |
| 無法刪除 SVM 或磁碟區 .....                                        | 478 |
| 識別刪除失敗 .....                                               | 479 |
| SVM 刪除：無法存取路由表 .....                                       | 479 |
| SVM 刪除：對等關係 .....                                          | 481 |
| SVM 或磁碟區刪除：SnapMirror .....                                | 482 |

|                                |     |
|--------------------------------|-----|
| SVM 刪除：啟用 Kerberos 的 LIF ..... | 483 |
| SVM 刪除：其他原因 .....              | 485 |
| 磁碟區刪除：FlexCache 關係 .....       | 487 |
| 設定錯誤的磁碟區 .....                 | 487 |
| 磁碟區超過 98% 已滿 .....             | 487 |
| 區塊儲存磁碟區離線 .....                | 488 |
| 離線FlexCache原始磁碟區 .....         | 488 |
| 具有SnapMirror關係的離線磁碟區 .....     | 488 |
| 區塊儲存磁碟區受到限制 .....              | 489 |
| 受限制的 FlexCache 原始磁碟區 .....     | 489 |
| SnapMirror 關係受限的磁碟區 .....      | 489 |
| 磁碟區儲存空間不足 .....                | 490 |
| 判斷磁碟區儲存容量的使用方式 .....           | 490 |
| 增加磁碟區的儲存容量 .....               | 490 |
| 使用磁碟區自動調整大小 .....              | 490 |
| 檔案系統的主要儲存體已滿 .....             | 490 |
| 刪除快照 .....                     | 491 |
| 增加磁碟區的檔案容量上限 .....             | 491 |
| 失敗的磁碟區備份 .....                 | 491 |
| 故障診斷網路問題 .....                 | 492 |
| 您想要擷取封包追蹤 .....                | 492 |
| 文件歷史紀錄 .....                   | 496 |
| .....                          | dxi |

# 什麼是 Amazon FSx for NetApp ONTAP ?

Amazon FSx for NetApp ONTAP 是一項全受管服務，可提供高度可靠、可擴展、高效能和功能豐富的檔案儲存，建置在 NetApp 的熱門 ONTAP 檔案系統上。FSx for ONTAP 結合了 NetApp 檔案系統的熟悉功能、效能、功能和 API 操作，以及全受管的靈活性、可擴展性和簡易性 AWS 服務。

FSx for ONTAP 提供功能豐富、快速且靈活的共用檔案儲存，可從 Linux、Windows 和 macOS 運算執行個體廣泛存取，這些執行個體在內部部署 AWS 中或內部部署執行。FSx for ONTAP 提供高效能固態硬碟 (SSD) 儲存體，延遲低於一毫秒。使用 FSx for ONTAP，您可以為工作負載達到 SSD 效能層級，同時只需支付一小部分資料的 SSD 儲存費用。

使用 FSx for ONTAP 管理您的資料更為容易，因為只要按一下按鈕，即可快照、複製和複寫檔案。此外，FSx for ONTAP 會自動將您的資料分層為成本較低的彈性儲存，讓您減少佈建或管理容量的需求。

FSx for ONTAP 也提供高可用性和耐用的儲存，具有全受管備份和跨區域災難復原的支援。為了更輕鬆地保護和保護您的資料，FSx for ONTAP 支援熱門的資料安全和防毒應用程式。

對於使用 NetApp ONTAP 內部部署的客戶，FSx for ONTAP 是將檔案型應用程式從內部部署遷移、備份或爆量到的理想解決方案，AWS 而無需變更應用程式碼或管理資料的方式。

做為全受管服務，FSx for ONTAP 可讓您更輕鬆地在雲端中啟動和擴展可靠、高效能且安全的共用檔案儲存。使用 FSx for ONTAP，您不再需要擔心：

- 設定和佈建檔案伺服器 and 儲存磁碟區
- 複寫資料
- 安裝和修補檔案伺服器軟體
- 偵測和解決硬體故障
- 管理容錯移轉和容錯回復
- 手動執行備份

FSx for ONTAP 也提供與其他 AWS 服務的豐富整合，例如 AWS Identity and Access Management (IAM)、Amazon WorkSpaces、AWS Key Management Service (AWS KMS) 和 AWS CloudTrail。

## 主題

- [FSx for ONTAP 的功能](#)

- [安全性和資料保護](#)
- [監控工具](#)
- [FSx for ONTAP 定價](#)
- [上的 FSx for ONTAP AWS re:Post](#)
- [您是第一次使用 Amazon FSx 嗎？](#)

## FSx for ONTAP 的功能

使用 FSx for ONTAP，您可以取得全受管檔案儲存解決方案：

- 支援單一命名空間中的 PB 級資料集
- 每個檔案系統每秒高達 0 GB (GBps) 的輸送量 [???](#)
- 使用網路檔案系統 (NFS)、伺服器訊息區塊 (SMB)、網際網路小型電腦系統界面 (iSCSI) 和非揮發性 Memory Express (NVMe) 通訊協定[存取資料的](#)多協定
- 高可用性且耐用的[異地同步備份和單一可用區](#)部署選項
- 根據您的存取模式，自動將不常存取的資料轉換為成本較低的儲存層，進而降低儲存成本
- 資料壓縮、重複資料刪除和壓縮，以減少您的儲存體使用量
- 支援 NetApp 的[SnapMirror 複寫](#)功能
- 支援 NetApp 的內部部署快取解決方案：NetApp 全域檔案快取和 FlexCache
- 支援使用原生 AWS 或 NetApp 工具和 API 操作進行存取和管理
  - AWS Management Console、AWS Command Line Interface (AWS CLI) 和 SDKs
  - [NetApp ONTAP CLI、REST API 和 BlueXP](#)

## 安全性和資料保護

共同責任模型的採用是因為它與相關[Amazon FSx for NetApp ONTAP 的安全性](#)。Amazon FSx 提供多層安全性和[合規性](#)，以協助保護您的資料。

FSx for ONTAP 支援下列資料保護、安全性和存取控制功能：

- 使用 [加密檔案系統資料和備份的靜態](#)資料 AWS KMS keys
- 使用 加密傳輸中的資料：
  - [SMB Kerberos](#)

- [IPSEC](#)
- [Nitro 型加密](#)
- 隨需[防毒掃描](#)
- 使用 [Microsoft Active Directory](#) 進行身分驗證和授權
- [檔案存取稽核](#)
- [NetAppSnapLock](#) 具有合規和企業保留模式的 WORM

如需詳細資訊，請參閱[Amazon FSx for NetApp ONTAP 中的資料保護及保護您的資料](#)。

此外，Amazon FSx 使用高耐用性的檔案系統備份來保護您的資料。Amazon FSx 會執行自動每日備份，而且您可以隨時進行其他備份。如需詳細資訊，請參閱[保護您的資料](#)。

## 監控工具

監控工具包括 [CloudWatch](#)、[CloudTrail](#)、[ONTAPEMS 事件](#)、[NetAppData Infrastructure Insights](#) 和 [NetApp Harvest](#)。

## FSx for ONTAP 定價

根據下列類別，您需要支付檔案系統的費用：

- SSD 儲存容量（每月 GB 或每月 GB）
- 您佈建超過三個 IOPS/GB 的 SSD IOPS（每月 IOPS）
- 輸送量容量（每秒每 MB 【MBps】個月）
- 容量集區儲存體使用量（每月 GB）
- 容量集區請求（每次讀取和寫入）
- 備份儲存體使用量（每月 GB）

如需與服務相關的定價和費用的詳細資訊，請參閱 [Amazon FSx for NetApp ONTAP 定價](#)。

## 上的 FSx for ONTAP AWS re:Post

如果您在使用 Amazon FSx 時遇到問題，請使用 [AWS re:Post](#) 取得 FSx 的 ONTAP 問題解答。

## 您是第一次使用 Amazon FSx 嗎？

如果您是第一次使用 Amazon FSx，建議您依序閱讀下列各節：

1. 如果您是初次使用 AWS，請參閱 [設定 FSx for ONTAP](#) 以設定 AWS 帳戶。
2. 如果您準備好建立第一個 Amazon FSx 檔案系統，請遵循 中的指示[Amazon FSx for NetApp ONTAP 入門](#)。
3. 如需有關效能的詳細資訊，請參閱[Amazon FSx for NetApp ONTAP 效能](#)。
4. 如需 Amazon FSx 安全詳細資訊，請參閱 [Amazon FSx for NetApp ONTAP 的安全性](#)。
5. 如需 Amazon FSx API 的相關資訊，請參閱 [Amazon FSx API 參考](#)。



# Amazon FSx for NetApp ONTAP 的運作方式

本主題介紹 Amazon FSx for NetApp ONTAP 檔案系統的主要功能及其運作方式，以及具有深入描述、重要實作詳細資訊和step-by-step組態程序的區段連結。

## 主題

- [FSx for OnTAP 檔案系統](#)
- [儲存虛擬機器](#)
- [磁碟區](#)
- [儲存層](#)
- [儲存效率](#)
- [存取儲存在 FSx for ONTAP 檔案系統上的資料](#)
- [管理 FSx for ONTAP 資源](#)

## FSx for OnTAP 檔案系統

檔案系統是 ONTAP 資源的主要 FSx，類似於內部部署 NetApp ONTAP 叢集。您可以指定檔案系統的固態硬碟 (SSD) 儲存容量和輸送量容量，然後選擇建立檔案系統的 Amazon Virtual Private Cloud (VPC)。如需詳細資訊，請參閱[管理 FSx for ONTAP 檔案系統](#)。

您的檔案系統可以有 1 到 12 個高可用性 (HA) 對，具體取決於其組態。HA 對由作用中待命組態中的兩個檔案伺服器組成。適用於 ONTAP 檔案系統的第一代 FSx 和第二代多可用區域檔案系統支援一個 HA 對。第二代單一可用區檔案系統最多支援 12 個 HA 對。如需詳細資訊，請參閱[管理高可用性 \(HA\) 對](#)。

## 儲存虛擬機器

儲存虛擬機器 (SVM) 是隔離的檔案伺服器，具有自己的管理和資料存取端點，用於管理和存取資料。當您存取 FSx for ONTAP 檔案系統中的資料時，您的用戶端和工作站會使用 SVM 的端點 IP 地址與 SVM 連接。如需詳細資訊，請參閱[管理 SVMs](#)。

您可以將 SVMs 加入 Microsoft Active Directory 以進行檔案存取身分驗證和授權。如需詳細資訊，請參閱[在 FSx for ONTAP 中使用 Microsoft Active Directory](#)。

## 磁碟區

ONTAP 磁碟區的 FSx 是您用來組織和分組資料的虛擬資源。磁碟區是託管在 SVMs 上的邏輯容器，而存放在其中的資料會在檔案系統上使用實體儲存容量。

當您建立磁碟區時，您可以設定其大小，這決定了您可以存放其中的實體資料量，無論資料存放於哪個儲存層。您也可以設定磁碟區類型，RW（可讀取）或 DP（資料保護）。DP 磁碟區是唯讀的，可用於 NetApp SnapMirror 或 SnapVault 關係中的目的地。

ONTAP 磁碟區的 FSx 是精簡佈建的，這表示它們只會針對存放在其中的資料使用儲存容量。對於精簡佈建的磁碟區，儲存容量不會事先保留。相反地，儲存會視需要動態配置。當磁碟區或 LUN 中的資料遭到刪除時，可用空間會釋出回檔案系統。例如，您可以在設定 10 TiB 可用儲存容量的檔案系統上建立三個 10 TiB 磁碟區，只要存放在三個磁碟區中的資料總量在任何時候都不超過 10 TiB。實際存放在磁碟區上的資料量會計入您的整體儲存容量耗用。如需詳細資訊，請參閱[管理 ONTAP 磁碟區的 FSx](#)。

## 儲存層

FSx for ONTAP 檔案系統有兩個儲存層：主要儲存體和容量集區儲存體。主要儲存體是佈建、可擴展、高效能的 SSD 儲存體，專為資料集的作用中部分而打造。容量集區儲存是一個全彈性儲存層，可以擴展到 PB 大小，並針對不常存取的資料進行成本最佳化。您寫入磁碟區的資料會消耗儲存層的容量。如需詳細資訊，請參閱[FSx for ONTAP 儲存層](#)。

## 資料分層

資料分層是 Amazon FSx for NetApp ONTAP 在 SSD 和容量集區儲存層之間自動移動資料的程序。每個磁碟區都有分層政策，可控制資料在變成非作用中（冷）時是否移至容量層。磁碟區的分層政策冷卻期間會決定資料何時變成非作用中（冷）。如需詳細資訊，請參閱[磁碟區資料分層](#)。

## 儲存效率

Amazon FSx for NetApp ONTAP 支援 ONTAP 的區塊層級儲存效率功能 - 壓縮、壓縮和重複資料刪除 - 以減少資料使用的儲存容量。儲存效率功能可以減少 SSD 儲存、容量集區儲存和備份中資料的足跡。在 SSD 和容量集區儲存層上，一般用途檔案共用工作負載的一般儲存容量節省，但又不會犧牲效能，從壓縮、重複資料刪除和壓縮中節省了 65%。如需詳細資訊，請參閱[儲存效率](#)。

## 存取儲存在 FSx for ONTAP 檔案系統上的資料

您可以透過 NFS (v3、v4、v4.1、v4.2) 和 SMB 通訊協定，從多個 Linux、Windows 或 macOS 用戶端同時存取 FSx 上的 ONTAP 磁碟區資料。macOS 您也可以使用非揮發性 Memory Express (NVMe) 和網際網路小型電腦系統介面 (iSCSI) 區塊通訊協定來存取資料。如需詳細資訊，請參閱[存取 FSx for ONTAP 資料](#)。

## 管理 FSx for ONTAP 資源

您可以透過多種方式與 FSx for ONTAP 檔案系統互動，並管理其資源。您可以使用 AWS 和 NetApp ONTAP 管理工具來管理 FSx for ONTAP 資源：

- AWS 管理工具
  - 的 AWS Management Console
  - The AWS Command Line Interface (AWS CLI)
  - Amazon FSx API 和 SDKs
  - AWS CloudFormation
- NetApp 管理工具：
  - NetApp BlueXP
  - NetApp ONTAP CLI
  - NetApp ONTAP REST API

如需詳細資訊，請參閱[管理 資源](#)。

# Amazon FSx for NetApp ONTAP 入門

了解如何開始使用 Amazon FSx for NetApp ONTAP。此入門練習包含下列步驟。

1. 註冊 AWS 帳戶 並在帳戶中建立管理使用者。
2. 使用 Amazon FSx 主控台建立 Amazon FSx for NetApp ONTAP 檔案系統。
3. 從 Amazon EC2 Linux 執行個體掛載檔案系統。
4. 清除您建立的 資源。

## 主題

- [設定 FSx for ONTAP](#)
- [建立 Amazon FSx for NetApp ONTAP 檔案系統](#)
- [從 Amazon EC2 Linux 執行個體掛載檔案系統](#)
- [清除資源](#)

## 設定 FSx for ONTAP

首次使用 Amazon FSx 之前，請先完成下列任務：

1. [註冊 AWS 帳戶](#)
2. [建立具有管理存取權的使用者](#)

## 主題

- [註冊 AWS 帳戶](#)
- [建立具有管理存取權的使用者](#)
- [下一步驟](#)

## 註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

### 註冊 AWS 帳戶

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

## 2. 請遵循線上指示進行。

部分註冊程序需接收來電或簡訊，並在電話鍵盤輸入驗證碼。

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

AWS 在註冊程序完成後，會傳送確認電子郵件給您。您可以隨時登錄 <https://aws.amazon.com/> 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

## 建立具有管理存取權的使用者

註冊後 AWS 帳戶，請保護 AWS 帳戶根使用者、啟用 AWS IAM Identity Center 和建立管理使用者，以免將根使用者用於日常任務。

保護您的 AWS 帳戶根使用者

1. 選擇根使用者並輸入 AWS 帳戶您的電子郵件地址，以帳戶擁有者[AWS Management Console](#)身分登入。在下一頁中，輸入您的密碼。

如需使用根使用者登入的說明，請參閱 AWS 登入使用者指南中的[以根使用者身分登入](#)。

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

如需說明，請參閱《IAM 使用者指南》中的[為您的 AWS 帳戶根使用者（主控台）啟用虛擬 MFA 裝置](#)。

建立具有管理存取權的使用者

1. 啟用 IAM Identity Center。

如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的[啟用 AWS IAM Identity Center](#)。

2. 在 IAM Identity Center 中，將管理存取權授予使用者。

如需使用 IAM Identity Center 目錄做為身分來源的教學課程，請參閱 AWS IAM Identity Center 《使用者指南》中的[使用預設值設定使用者存取 IAM Identity Center 目錄](#)。

以具有管理存取權的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者簽署，請使用建立 IAM Identity Center 使用者時傳送至您電子郵件地址的簽署 URL。

如需使用 IAM Identity Center 使用者登入的說明，請參閱AWS 登入 《使用者指南》中的[登入 AWS 存取入口網站](#)。

指派存取權給其他使用者

- 在 IAM Identity Center 中，建立一個許可集來遵循套用最低權限的最佳實務。

如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的[建立許可集](#)。

- 將使用者指派至群組，然後對該群組指派單一登入存取權。

如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的[新增群組](#)。

## 下一步驟

若要開始使用 FSx for ONTAP，請參閱 [Amazon FSx for NetApp ONTAP 入門](#) 以取得建立 Amazon FSx 資源的指示。

## 建立 Amazon FSx for NetApp ONTAP 檔案系統

Amazon FSx 主控台有兩個建立檔案系統的選項：快速建立選項和標準建立選項。若要使用服務建議的組態快速輕鬆地建立 Amazon FSx for NetApp ONTAP 檔案系統，請使用快速建立選項。

快速建立選項會設定此檔案系統，以允許透過網路檔案系統 (NFS) 通訊協定從 Linux 執行個體存取資料。建立檔案系統之後，您可以視需要建立其他 SVMs 和磁碟區，包括加入 Active Directory 的 SVM，以允許透過伺服器訊息區塊 (SMB) 通訊協定從 Windows 和 macOS 用戶端存取。您也可以新增其他高可用性 (HA) 對，具體取決於您選擇的部署類型，以及您在建立時新增的 HA 對數量。

如需使用標準建立選項建立具有自訂組態的檔案系統，以及使用 AWS CLI 和 API 的詳細資訊，請參閱[建立檔案系統](#)。

建立 檔案系統

- 在 <https://console.aws.amazon.com/fsx/>：// 開啟 Amazon FSx 主控台。
- 在儀表板上，選擇 Create file system (建立檔案系統) 以啟動檔案系統建立精靈。

3. 在選取檔案系統類型頁面上，選擇 Amazon FSx for NetApp ONTAP，然後選擇下一步。建立 ONTAP 檔案系統頁面隨即出現。
4. 針對建立方法，選擇快速建立。
5. 在快速組態區段中，針對檔案系統名稱 - 選用，輸入檔案系統的名稱。當您命名檔案系統時，更容易找到並管理您的檔案系統。您最多可以使用 256 個 Unicode 字母、空格和數字，加上這些特殊字元：+ - ( 連字號 ) = . \_ ( 底線 ) : /
6. 針對部署類型，選擇異地同步備份或單一異地同步備份。
  - 異地同步備份檔案系統會複寫您的資料，並支援在同一區域跨多個可用區域的容錯移轉 AWS 區域。
  - 單一可用區檔案系統會複寫您的資料，並在單一可用區域內提供自動容錯移轉。

如需詳細資訊，請參閱[可用性、耐用性和部署選項](#)。

 Note

預設 AWS 區域 會選擇適用於您的最新一代 FSx for ONTAP 檔案系統。您可以使用標準建立選項指定檔案系統的產生 (在可用時 AWS 區域)。如需詳細資訊，請參閱[建立檔案系統](#)。

7. 對於 SSD 儲存容量，請以 GB (GiB) 為單位指定檔案系統的儲存容量。輸入 1,024–1,048,576 範圍內的任何整數。如需詳細資訊，請參閱[建立檔案系統 \(主控台\)](#)。

您可以在建立檔案系統之後，隨時視需要增加儲存容量。如需詳細資訊，請參閱[管理儲存容量](#)。

8. 對於輸送量容量，Amazon FSx 會根據您的 SSD 儲存體自動提供建議的輸送量容量。您也可以選擇檔案系統的輸送量 (最高 73,728 MBps，視部署類型和 HA 對數量而定)。
9. 針對 Virtual Private Cloud (VPC)，選擇您要與檔案系統建立關聯的 Amazon VPC。
10. 若要提高儲存效率，請選擇啟用以開啟 ONTAP 儲存效率功能 (壓縮、重複資料刪除和壓縮)，或選擇停用以將其關閉。
11. (僅限異地同步備份) 端點 IP 地址範圍指定要存取檔案系統的端點建立所在的 IP 地址範圍。

為端點 IP 地址範圍選擇快速建立選項：

- 來自 VPC 的未配置 IP 地址範圍 – 選擇此選項可讓 Amazon FSx 使用 VPC 主要 CIDR 範圍的最後 64 個 IP 地址作為檔案系統的端點 IP 地址範圍。請注意，如果您多次選擇此選項，此範圍會跨多個檔案系統共用。



 Note

- 您建立的每個檔案系統都會從此範圍使用兩個 IP 地址，一個用於叢集，另一個用於第一個 SVM。第一個和最後一個 IP 地址也會保留。對於每個額外的 SVM，檔案系統會使用另一個 IP 地址。例如，託管 10 SVMs 的檔案系統會使用 11 個 IP 地址。其他檔案系統的運作方式相同。它們會使用兩個初始 IP 地址，加上每個額外的 SVM 一個。使用相同 IP 地址範圍的檔案系統數目上限是 31，每個都有單一 SVM。
  - 如果子網路正在使用 VPC 主要 CIDR 範圍內的最後 64 個 IP 地址中的任何一個，則此選項會變成灰色。
- 浮動 VPC 之外的 IP 地址範圍 – 選擇此選項可讓 Amazon FSx 使用 198.19.x.0/24 地址範圍，該範圍尚未由具有相同 VPC 和路由表的任何其他檔案系統使用。

您也可以標準建立選項中指定自己的 IP 地址範圍。您選擇的 IP 地址範圍可以在 VPC 的 IP 地址範圍內或之外，只要它不會與任何子網路重疊，而且只要另一個具有相同 VPC 和路由表的檔案系統尚未使用它。建議使用 VPC IP 地址範圍內的範圍。

 Note

確定您使用的所有路由表都與您的多可用區域檔案系統相關聯。這樣做有助於防止容錯移轉期間無法使用。如需將 Amazon VPC 路由表與檔案系統建立關聯的資訊，請參閱 [更新檔案系統](#)。

12. 選擇下一步，然後在建立 ONTAP 檔案系統頁面上檢閱檔案系統組態。請注意，在建立檔案系統之後，您可以修改哪些檔案系統設定。
13. 選擇 Create file system (建立檔案系統)。

快速建立會使用一個 SVM (名為 fsx) 和一個磁碟區 (名為) 建立檔案系統vol1。磁碟區具有的連接路徑/vol1和 Auto 的容量集區分層政策 (它會自動將 31 天內未存取的任何資料分層，以降低容量集區儲存成本)。預設快照政策會指派給預設磁碟區。檔案系統資料會使用預設服務受管 AWS KMS 金鑰進行靜態加密。



## 從 Amazon EC2 Linux 執行個體掛載檔案系統

您可以從 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體掛載檔案系統。此程序使用執行 Amazon Linux 2 的執行個體。

### 從 Amazon EC2 掛載檔案系統

1. 前往 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 建立或選取執行 Amazon Linux 2 的 Amazon EC2 執行個體，該執行個體位於與檔案系統相同的虛擬私有雲端 (VPC) 中。如需啟動執行個體的詳細資訊，請參閱《Amazon EC2 使用者指南》中的 [步驟 1：啟動執行個體](#)。
3. 連線至 Amazon EC2 Linux 執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的 [連線至 Linux 執行個體](#)。
4. 使用安全殼層 (SSH) 在 Amazon EC2 執行個體上開啟終端機，並使用適當的登入資料登入。
5. 使用下列命令在 Amazon EC2 執行個體上建立目錄，以用作磁碟區的掛載點。在下列範例中，將 *mount-point* 取代為您自己的資訊。

```
$ sudo mkdir /mount-point
```

6. 將 Amazon FSx for NetApp ONTAP 檔案系統掛載到您建立的目錄。使用類似以下範例的 mount 命令。在下列範例中，將下列預留位置值取代為您自己的資訊。
  - *nfs\_version* – 您使用的 NFS 版本；FSx for ONTAP 支援版本 3、4.0、4.1 和 4.2。
  - *nfs-dns-name* – 您要掛載之磁碟區的儲存虛擬機器 (SVM) 的 NFS DNS 名稱。您可以在 Amazon FSx 主控台中找到 NFS DNS 名稱，方法是選擇儲存虛擬機器，然後選擇您要掛載磁碟區的 SVM。NFS DNS 名稱位於端點面板。
  - *volume-junction-path* – 您要掛載之磁碟區的連接路徑。您可以在磁碟區詳細資訊頁面的摘要面板上的 Amazon FSx 主控台中找到磁碟區的連接路徑。
  - *mount-point* – 您在 EC2 執行個體上為磁碟區掛載點建立的目錄名稱。

```
sudo mount -t nfs -o nfsvers=nfs_version nfs-dns-name:/volume-junction-path /mount-point
```

下列命令使用範例值。

```
sudo mount -t nfs -o nfsvers=4.1 svm-abcdef1234567890c.fs-012345abcdef6789b.fsx.us-east-2.amazonaws.com:/vol1 /fsxN
```

如果您的 Amazon EC2 執行個體發生問題（例如連線逾時），請參閱《Amazon [EC2 使用者指南](#)》中的[對 EC2 執行個體進行故障診斷](#)。Amazon EC2

## 清除資源

完成本練習後，您應該遵循這些步驟來清理資源並保護您的 AWS 帳戶。

### 清理資源

1. 在 Amazon EC2 主控台上，終止您的執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[終止您的執行個體](#)。
2. 在 <https://console.aws.amazon.com/fsx/>：// 開啟 Amazon FSx 主控台。
3. 在 Amazon FSx 主控台上，刪除不是 SVM 根磁碟區的所有 FSx for ONTAP 磁碟區。如需詳細資訊，請參閱[刪除磁碟區](#)。
4. 刪除 ONTAP SVMs 的所有 FSx。如需詳細資訊，請參閱[刪除儲存虛擬機器 \(SVM\)](#)。
5. 在 Amazon FSx 主控台上，刪除您的檔案系統。當您刪除檔案系統時，所有自動備份都會自動刪除。不過，您仍然必須刪除任何手動建立的備份。下列步驟概述此程序。
  - a. 從主控台儀表板中，選擇您為此練習建立的檔案系統名稱。
  - b. 針對 Actions (動作)，選擇 Delete file system (刪除檔案系統)。
  - c. 在刪除檔案系統對話方塊中，在檔案系統 ID 方塊中輸入您要刪除的檔案系統 ID。
  - d. 選擇刪除檔案系統。
  - e. 當 Amazon FSx 刪除檔案系統時，儀表板中的狀態會變更為刪除。一旦刪除檔案系統，它就不會再出現在儀表板中。任何自動備份都會與檔案系統一併刪除。
  - f. 現在您可以刪除檔案系統的任何手動建立的備份。從左側導覽中，選擇備份。
  - g. 從儀表板中，選擇與您刪除的檔案系統 ID 相同的任何備份，然後選擇刪除備份。如果您建立了最終備份，請務必保留該備份。
  - h. 刪除備份對話方塊隨即開啟。針對您要刪除 IDs 保持選取核取方塊，然後選擇刪除備份。

您的 Amazon FSx 檔案系統和任何相關的自動備份現在也會一併刪除，以及您選擇刪除的任何手動備份。

## 可用性 AWS 區域

下列提供 Amazon FSx for NetApp ONTAP 檔案系統 AWS 區域，並針對每個區域指定部署類型支援：

| AWS 區域                   | 單一可用區 1 | 異地同步備份 1 | 單一可用區 2 | 異地同步備份 2 |  |  |
|--------------------------|---------|----------|---------|----------|--|--|
| 美國東部 (維吉尼亞北部)            | ✓       | ✓        | ✓       | ✓        |  |  |
| 美國東部 (俄亥俄)               | ✓       | ✓        | ✓       | ✓        |  |  |
| 美國西部 (加利佛尼亞北部)           | ✓       | ✓        | ✓       | ✓        |  |  |
| 美國西部 (奧勒岡)               | ✓       | ✓        | ✓       | ✓        |  |  |
| AWS GovCloud (美國東部)      | ✓       | ✓        |         |          |  |  |
| AWS GovCloud (美國西部)      | ✓       | ✓        |         |          |  |  |
| 非洲 (開普敦)                 | ✓       | ✓        |         |          |  |  |
| Asia Pacific (Hong Kong) | ✓       | ✓        |         |          |  |  |

| AWS 區域      | 單一可用區 1 | 異地同步備份 1 | 單一可用區 2 | 異地同步備份 2 |  |  |
|-------------|---------|----------|---------|----------|--|--|
| 亞太區域 (東京)   | ✓       | ✓        | ✓       | ✓        |  |  |
| 亞太區域 (首爾)   | ✓       | ✓        |         |          |  |  |
| 亞太區域 (大阪)   | ✓       | ✓        |         |          |  |  |
| 亞太區域 (孟買)   | ✓       | ✓        | ✓       | ✓        |  |  |
| 亞太區域 (海德拉巴) | ✓       | ✓        |         |          |  |  |
| 亞太區域 (新加坡)  | ✓       | ✓        | ✓       | ✓        |  |  |
| 亞太區域 (悉尼)   | ✓       | ✓        | ✓       | ✓        |  |  |
| 亞太區域 (雅加達)  | ✓       | ✓        |         |          |  |  |
| 亞太區域 (墨爾本)  | ✓       | ✓        |         |          |  |  |
| 亞太區域 (馬來西亞) | ✓       | ✓        |         |          |  |  |
| 亞太區域 (泰國)   | ✓       | ✓        |         |          |  |  |
| 加拿大 (中部)    | ✓       | ✓        |         |          |  |  |

| AWS 區域         | 單一可用區 1 | 異地同步備份 1 | 單一可用區 2 | 異地同步備份 2 |  |  |
|----------------|---------|----------|---------|----------|--|--|
| 加拿大西部 (卡加利)    | ✓       | ✓        |         |          |  |  |
| 歐洲 (法蘭克福)      | ✓       | ✓        | ✓       | ✓        |  |  |
| 歐洲 (蘇黎世)       | ✓       | ✓        |         |          |  |  |
| 歐洲 (斯德哥爾摩)     | ✓       | ✓        | ✓       | ✓        |  |  |
| 歐洲 (米蘭)        | ✓       | ✓        |         |          |  |  |
| 歐洲 (西班牙)       | ✓       | ✓        |         |          |  |  |
| 歐洲 (愛爾蘭)       | ✓       | ✓        | ✓       | ✓        |  |  |
| 歐洲 (倫敦)        | ✓       | ✓        |         |          |  |  |
| Europe (Paris) | ✓       | ✓        |         |          |  |  |
| 以色列 (特拉維夫)     | ✓       | ✓        |         |          |  |  |
| 墨西哥 (中部)       | ✓       | ✓        |         |          |  |  |
| 中東 (阿拉伯聯合大公國)  | ✓       | ✓        |         |          |  |  |

| AWS 區域                | 單一可用區 1 | 異地同步備份 1 | 單一可用區 2 | 異地同步備份 2 |  |  |
|-----------------------|---------|----------|---------|----------|--|--|
| Middle East (Bahrain) | ✓       | ✓        |         |          |  |  |
| 南美洲 (聖保羅)             | ✓       | ✓        |         |          |  |  |

# 存取 FSx for ONTAP 資料

您可以在 和內部部署環境中，使用各種支援的用戶端 AWS 雲端 和方法存取 Amazon FSx 檔案系統。

每個 SVM 都有四個端點，用於存取資料或使用 NetApp ONTAP CLI 或 REST API 管理 SVM：

- Nfs – 使用網路檔案系統 (NFS) 通訊協定進行連線
- Smb – 用於使用服務訊息區塊 (SMB) 通訊協定進行連線（如果您的 SVM 已加入 Active Directory，或者您正在使用工作群組。）
- Iscsi – 用於使用網際網路小型電腦系統界面 (iSCSI) 通訊協定進行連線，以取得共用區塊儲存支援。
- Nvme – 用於透過 TCP/IP 使用非揮發性 Memory Express (NVMe) 進行連線，以支援共用區塊儲存。
- Management – 用於使用 NetApp ONTAP CLI 或 API 或 NetApp BlueXP 管理 SVMs

## Note

iSCSI 通訊協定適用於所有具有 6 個或更少 [高可用性對 \(HA\) 對](#) 的檔案系統。NVMe/TCP 通訊協定適用於具有 6 個或更少 HA 對的第二代檔案系統。

## 主題

- [支援的用戶端](#)
- [使用區塊儲存協定](#)
- [從 內存取資料 AWS 雲端](#)
- [從內部部署存取資料](#)
- [設定路由以從 VPC 外部存取多可用區域檔案系統](#)
- [設定路由以從內部部署存取多可用區域檔案系統](#)
- [Linux 用戶端上的掛載磁碟區](#)
- [在 Microsoft Windows 用戶端上掛載磁碟區](#)
- [macOS 用戶端上的掛載磁碟區](#)
- [佈建 Linux 的 iSCSI](#)
- [佈建適用於 Windows 的 iSCSI](#)

- [佈建適用於 Linux 的 NVMe/TCP](#)
- [佈建適用於 Windows 的 NVMe/TCP](#)
- [使用其他服務 AWS 存取資料](#)

## 支援的用戶端

FSx for ONTAP 檔案系統支援從各種運算執行個體和作業系統存取資料。其做法是支援使用網路檔案系統 (NFS) 通訊協定 (v3、v4.0、v4.1 和 v4.2)、所有版本的伺服器訊息區塊 (SMB) 通訊協定 (包括 2.0、3.0 和 3.1.1) 和網際網路小型電腦系統界面 (iSCSI) 通訊協定進行存取。

### Important

Amazon FSx 不支援從公有網際網路存取檔案系統。Amazon FSx 會自動分離任何彈性 IP 地址，這是可從網際網路連線的公有 IP 地址，該地址會連接到檔案系統的彈性網路界面。

下列 AWS 運算執行個體支援與 FSx for ONTAP 搭配使用：

- 使用 NFS 或 SMB 支援、Microsoft Windows 和 MacOS 執行 Linux 的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。如需詳細資訊，請參閱 [Linux 用戶端上的掛載磁碟區](#) 在 [Microsoft Windows 用戶端上掛載磁碟區](#)、和 [macOS 用戶端上的掛載磁碟區](#)。
- Amazon EC2 Windows 和 Linux 執行個體上的 Amazon EC2) Docker 容器。如需詳細資訊，請參閱 [將 Amazon Elastic Container Service 與 FSx for ONTAP 搭配使用](#)。
- Amazon Elastic Kubernetes Service – 若要進一步了解，請參閱《[Amazon EKS 使用者指南](#)》中的 [Amazon FSx for NetApp ONTAP CSI 驅動程式](#)。
- Red Hat OpenShift Service on AWS (ROSA) – 若要進一步了解，請參閱 AWS 《使用者指南》中的 [什麼是 Red Hat OpenShift Service on AWS ?](#)。OpenShift
- Amazon WorkSpaces 執行個體。如需詳細資訊，請參閱 [將 Amazon WorkSpaces 與 FSx for ONTAP 搭配使用](#)。
- Amazon AppStream 2.0 執行個體。
- AWS Lambda – 如需詳細資訊，請參閱 AWS 部落格文章 [使用 Amazon FSx 啟用無伺服器工作負載的 SMB 存取](#)。
- 在 VMware Cloud on AWS 環境中執行的虛擬機器 (VMs)。如需詳細資訊，請參閱 [設定 Amazon FSx for NetApp ONTAP 為外部儲存](#) 和 [AWS VMware VMware Cloud on with Amazon FSx for NetApp ONTAP 部署指南](#)。



掛載後，FSx for ONTAP 檔案系統會透過 NFS 和 SMB 顯示為本機目錄或磁碟機代號，提供全受管的共用網路檔案儲存體，最多可由數千個用戶端同時存取。透過 iSCSI 掛載時，iSCSI LUNS 可作為區塊型裝置存取。

## 使用區塊儲存協定

Amazon FSx for NetApp ONTAP 透過 TCP (NVMe/TCP) 區塊儲存通訊協定支援網際網路小型電腦系統介面 (iSCSI) 和非揮發性記憶體快速 (NVMe)。在儲存區域網路 (SAN) 環境中，儲存系統是具有儲存目標裝置的目標。對於 iSCSI，儲存目標裝置稱為邏輯單位 (LUNs)。對於 NVMe/TCP，儲存目標裝置稱為命名空間。

您可以使用 SVM 的 iSCSI 邏輯界面 (LIF) 來連線至 NVMe 和 iSCSI 區塊儲存。

您可以透過為 iSCSI 建立 LUNs，以及為 NVMe 建立命名空間來設定儲存體。然後，主機會使用 iSCSI 或 TCP 通訊協定存取 LUNs 和命名空間。

如需設定 iSCSI 和 NVMe/TCP 區塊儲存的詳細資訊，請參閱：

- [佈建 Linux 的 iSCSI](#)
- [佈建適用於 Windows 的 iSCSI](#)
- [佈建適用於 Linux 的 NVMe/TCP](#)
- [佈建適用於 Windows 的 NVMe/TCP](#)

### Note

佈建適用於 Windows 的 NVMe/TCP 需要使用第三方 NVMe 啟動器。

## 從 內存取資料 AWS 雲端

每個 Amazon FSx 檔案系統都與 Virtual Private Cloud (VPC) 相關聯。無論可用區域為何，您都可以從檔案系統 VPC 中的任何位置存取 FSx for ONTAP 檔案系統。您也可以從其他 VPCs 可以位於不同的 AWS 帳戶或中 AWS 區域。除了以下各節所述存取 FSx for ONTAP 資源的要求之外，您還需要確保已設定檔案系統的 VPC 安全群組，以便資料和管理流量可在檔案系統和用戶端之間流動。如需使用所需連接埠設定安全群組的詳細資訊，請參閱 [Amazon VPC 安全群組](#)。

## 從相同 VPC 內存取資料

當您建立 Amazon FSx for NetApp ONTAP 檔案系統時，請選取其所在的 Amazon VPC。與 Amazon FSx for NetApp ONTAP 檔案系統相關聯的所有 SVMs 和磁碟區也位於相同的 VPC 中。掛載磁碟區時，如果檔案系統和掛載磁碟區的用戶端位於相同的 VPC AWS 帳戶，而且您可以根據用戶端使用 SVM 的 DNS 名稱和磁碟區連接或 SMB 共用。

如果用戶端和磁碟區位於與檔案系統子網路相同的可用區域，或多可用區域檔案系統偏好的子網路中，您可以達到最佳效能。若要識別檔案系統的子網路或偏好的子網路，請在 Amazon FSx 主控台中選擇檔案系統，然後選擇要掛載磁碟區的 ONTAP 檔案系統，子網路或偏好的子網路（多可用區域）會顯示在子網路或偏好的子網路面板中。

## 從部署 VPC 外部存取資料

本節說明如何從檔案系統部署 VPC 外部 AWS 的位置存取 FSx for ONTAP 檔案系統的端點。

### 在多可用區域檔案系統上存取 NFS、SMB 和 ONTAP 管理端點

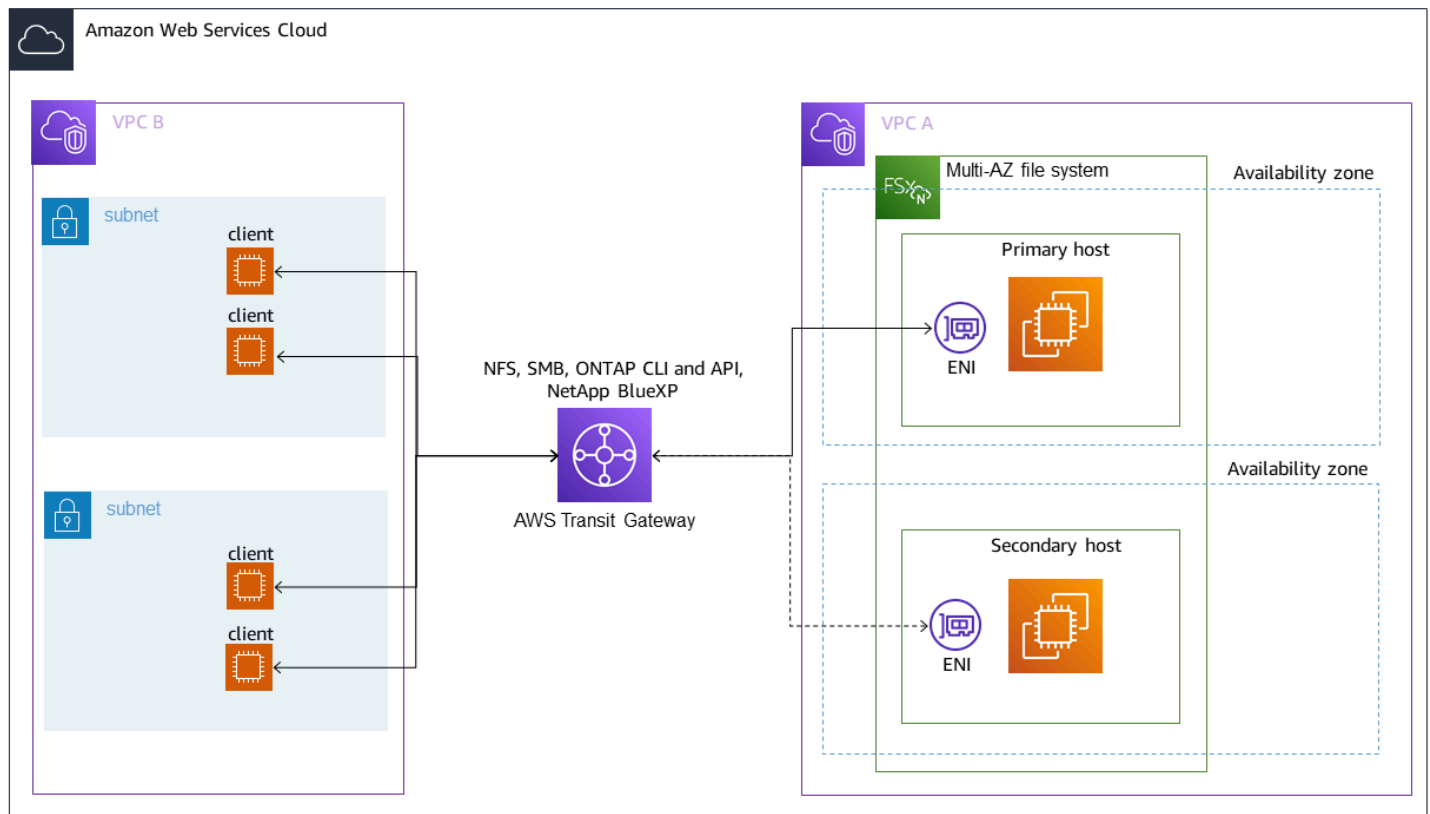
Amazon FSx for NetApp ONTAP 多可用區域檔案系統的 NFS、SMB 和 ONTAP 管理端點使用浮動國際網路通訊協定 (IP) 地址，以便連線的用戶端在容錯移轉事件期間順暢地在偏好的和待命檔案伺服器之間轉換。如需容錯移轉的詳細資訊，請參閱 [FSx for ONTAP 的容錯移轉程序](#)。

這些浮動 IP 地址會在您與您的檔案系統建立關聯的 VPC 路由表中建立，並且位於 `EndpointIpAddressRange` 您可以在建立期間指定的檔案系統中。根據檔案系統的建立方式，`EndpointIpAddressRange` 使用以下地址範圍：

- 根據 `EndpointIpAddressRange` 預設，使用 Amazon FSx 主控台建立的異地同步備份檔案系統會使用 VPC 主要 CIDR 範圍內的最後 64 個 IP 地址，做為檔案系統的主要 CIDR 範圍。
- 使用 AWS CLI 或 Amazon FSx API 建立的多可用區域檔案系統 `EndpointIpAddressRange` 預設會使用地址區塊內的 IP 198.19.0.0/16 地址範圍。
- 您也可以在使用標準建立選項時指定自己的 IP 地址範圍。您選擇的 IP 地址範圍可以在 VPC 的 IP 地址範圍內或之外，只要它不會與任何子網路重疊，而且只要另一個具有相同 VPC 和路由表的檔案系統尚未使用它。針對此選項，我們建議您使用 VPC IP 地址範圍內的範圍。

僅 [AWS Transit Gateway](#) 支援路由到浮動 IP 地址，也稱為被動對等互連。VPC 對等 AWS Direct Connect 互連，AWS VPN 不支援傳輸對等互連。因此，您必須使用 Transit Gateway，才能從檔案系統 VPC 外部的網路存取這些介面。

下圖說明使用 Transit Gateway 進行 NFS、SMB 或管理存取多可用區域檔案系統，該檔案系統與存取它的用戶端位於不同的 VPC 中。



#### Note

確定您使用的所有路由表都與您的多可用區域檔案系統相關聯。這樣做有助於防止容錯移轉期間無法使用。如需將 Amazon VPC 路由表與檔案系統建立關聯的資訊，請參閱 [更新檔案系統](#)。

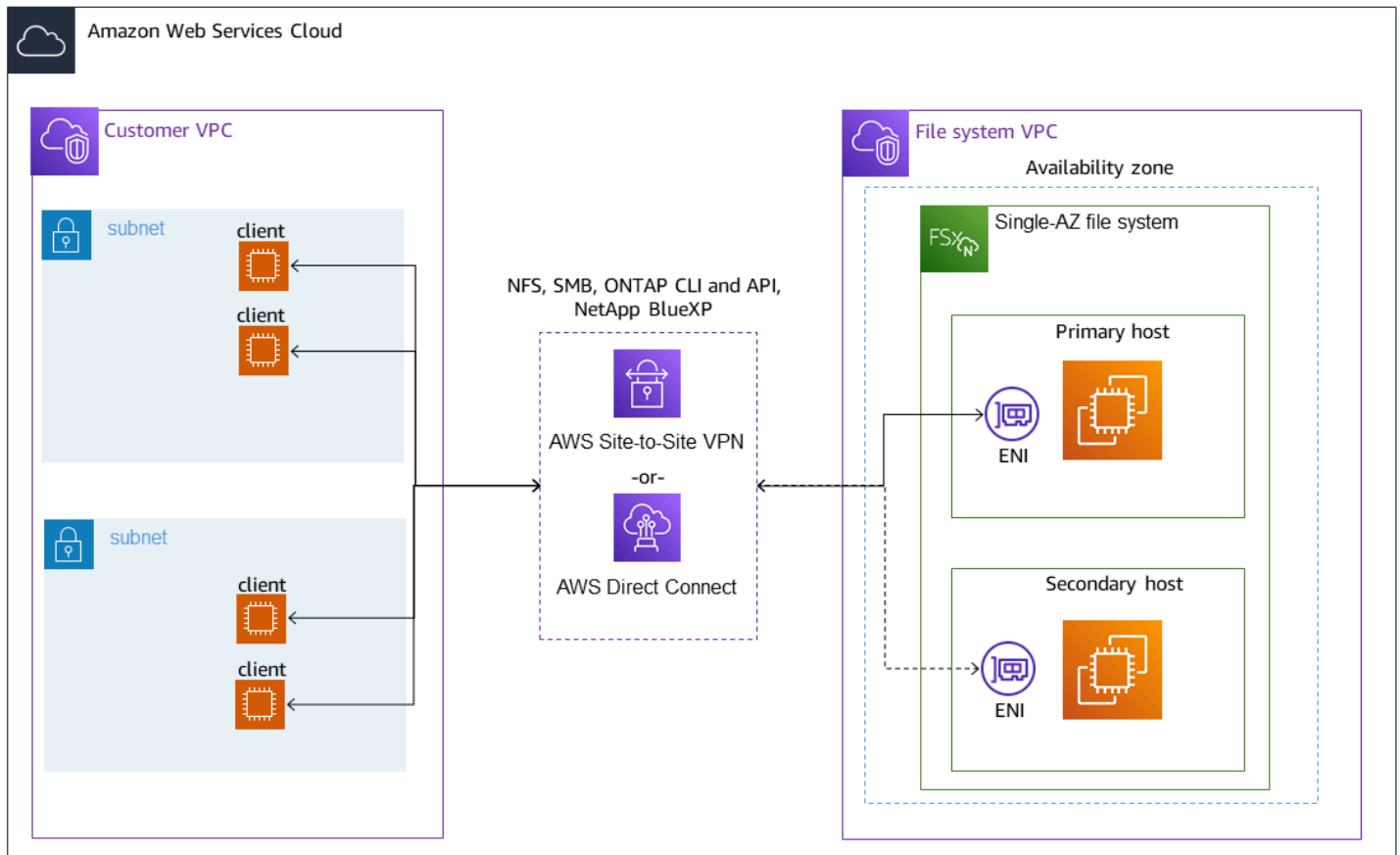
如需何時需要使用 Transit Gateway 存取 FSx for ONTAP 檔案系統的詳細資訊，請參閱 [何時需要 Transit Gateway ?](#)。

Amazon FSx 會使用標籤型身分驗證來管理多可用區域檔案系統的 VPC 路由表。這些路由表會以標記 Key: AmazonFSx; Value: ManagedByAmazonFSx。使用 建立或更新 FSx for ONTAP 多可用區域檔案系統時，AWS CloudFormation 建議您手動新增 Key: AmazonFSx; Value: ManagedByAmazonFSx 標籤。

## 存取適用於單一可用區檔案系統的 NFS、SMB 或 ONTAP CLI 和 API

用於透過 NFS 或 SMB 存取 FSx for ONTAP 單一可用區檔案系統的端點，以及用於使用 ONTAP CLI 或 REST API 管理檔案系統的端點，是作用中檔案伺服器的 ENI 上的次要 IP 地址。次要 IP 地址位於 VPC 的 CIDR 範圍內，因此用戶端可以使用 VPC 對等互連存取資料和管理連接埠 AWS Direct Connect，或者 AWS VPN 不需要 AWS Transit Gateway。

下圖說明將 AWS VPN 或 AWS Direct Connect 用於 NFS、SMB 或管理存取單一可用區檔案系統，該系統與存取它的用戶端位於不同的 VPC 中。



## 何時需要 Transit Gateway？

多可用區域檔案系統是否需要 Transit Gateway，取決於您用來存取檔案系統資料的方法。單一可用區檔案系統不需要 Transit Gateway。下表說明何時需要使用 AWS Transit Gateway 來存取多可用區域檔案系統。

| 資料存取                                                   | 需要傳輸閘道？                                                                                                                        |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| 透過 NFS、SMB 或 NetApp ONTAP REST API、CLI 或 BlueXP 存取 FSx | 僅在下列情況下： <ul style="list-style-type: none"> <li>從對等網路（例如內部部署）存取，以及</li> <li>您未透過 NetApp FlexCache 或全域檔案快取執行個體存取 FSx</li> </ul> |
| 透過 iSCSI 存取資料                                          | 否                                                                                                                              |
| 透過 NVMe 存取資料                                           | 否                                                                                                                              |
| 將 SVM 加入 Active Directory                              | 否                                                                                                                              |
| SnapMirror                                             | 否                                                                                                                              |
| FlexCache 快取                                           | 否                                                                                                                              |
| 全域檔案快取                                                 | 否                                                                                                                              |

## 在部署 VPC 外部存取 NVMe、iSCSI 和叢集間端點

您可以使用 VPC 對等互連 AWS Transit Gateway 或從檔案系統的部署 VPC 外部存取檔案系統的 NVMe、iSCSI 和叢集間端點。您可以使用 VPC 對等互連，在 VPCs 之間路由 NVMe、iSCSI 和叢集間流量。VPC 互連連線是兩個 VPCs 之間的網路連線，用於使用私有 IPv4 地址路由它們之間的流量。您可以使用 VPC 對等互連來連接相同 AWS 區域或不同 VPCs AWS 區域。如需 VPC 對等互連的詳細資訊，請參閱《Amazon [VPC 對等互連指南](#)》中的什麼是 VPC 對等互連？。

## 從內部部署存取資料

您可以使用 [AWS VPN](#) 和從內部部署存取 FSx for ONTAP 檔案系統 [AWS Direct Connect](#)；以下章節提供更具體的使用案例指導方針。除了下列從內部部署存取不同 FSx for ONTAP 資源的要求之外，您還需要確保檔案系統的 VPC 安全群組允許資料在您的檔案系統和用戶端之間流動；如需必要連接埠的清單，請參閱 [Amazon VPC 安全群組](#)。

## 從內部部署存取 NFS、SMB 和 ONTAP CLI 和 REST API 端點

本節說明如何從內部部署網路存取 FSx for ONTAP 檔案系統上的 NFS、SMB 和 ONTAP 管理連接埠。

## 從內部部署存取異地同步備份檔案系統

Amazon FSx 要求您使用 AWS Transit Gateway 或 設定遠端 NetApp 全域檔案快取或 NetApp FlexCache，以從內部部署網路存取多可用區域檔案系統。為了支援異地同步備份檔案系統的跨可用區域容錯移轉，Amazon FSx 會將浮點數 IP 地址用於 NFS、SMB 和 ONTAP 管理端點的介面。

由於 NFS、SMB 和管理端點使用浮動 IP 地址，您必須[AWS Transit Gateway](#)搭配 AWS Direct Connect 或使用 AWS VPN，才能從內部部署網路存取這些介面。用於這些界面的浮動 IP 地址位於 `EndpointIpAddressRange` 您在建立多可用區域檔案系統時指定的內。根據檔案系統的建立方式，`EndpointIpAddressRange` 使用以下地址範圍：

- 根據 `EndpointIpAddressRange` 預設，使用 Amazon FSx 主控台建立的異地同步備份檔案系統會使用 VPC 主要 CIDR 範圍內的最後 64 個 IP 地址，做為檔案系統的主要 CIDR 範圍。
- 使用 AWS CLI 或 Amazon FSx API 建立的多可用區域檔案系統 `EndpointIpAddressRange` 預設會使用地址區塊內的 IP 198.19.0.0/16 地址範圍。
- 您也可以 Amazon FSx 主控台中使用標準建立選項時指定自己的 IP 地址範圍。您選擇的 IP 地址範圍可以在 VPC 的 IP 地址範圍內或之外，只要它不會與任何子網路重疊，而且只要另一個具有相同 VPC 和路由表的檔案系統尚未使用它。針對此選項，我們建議您使用 VPC IP 地址範圍內的範圍。

浮動 IP 地址用於在需要容錯移轉時，讓用戶端無縫轉換至待命檔案系統。如需詳細資訊，請參閱[FSx for ONTAP 的容錯移轉程序](#)。

### Important

若要使用 Transit Gateway 存取多可用區域檔案系統，每個 Transit Gateway 的附件都必須在子網路中建立，其路由表與您的檔案系統相關聯。

如需詳細資訊，請參閱[設定路由以從內部部署存取多可用區域檔案系統](#)。

## 從內部部署存取單一可用區檔案系統

單一可用區檔案系統不存在 AWS Transit Gateway 使用從內部部署網路存取資料的需求。單一可用區檔案系統部署在單一子網路中，不需要浮動 IP 地址，即可在節點之間提供容錯移轉。反之，您在單一可用區檔案系統上存取的 IP 地址會實作為檔案系統 VPC CIDR 範圍內的次要 IP 地址，可讓您從另一個網路存取資料，而不需要 AWS Transit Gateway。



## 從內部部署存取叢集間端點

FSx for ONTAP 的叢集間端點專用於複寫 NetApp ONTAP 檔案系統之間的流量，包括內部部署 NetApp 部署與 FSx for ONTAP。複寫流量包括不同檔案系統中儲存虛擬機器 (SVMs) 和磁碟區之間的 SnapMirror、FlexCache 和 FlexClone 關係，以及 NetApp 全域檔案快取。叢集間端點也用於 Active Directory 流量。

由於檔案系統的叢集間端點使用您在建立 FSx for ONTAP 檔案系統時所提供 VPC CIDR 範圍內的 IP 地址，因此您不需要使用 Transit Gateway 在內部部署和 之間路由叢集間流量 AWS 雲端。不過，現場部署用戶端仍必須使用 AWS VPN 或 AWS Direct Connect 來建立與 VPC 的安全連線。

如需詳細資訊，請參閱[設定路由以從內部部署存取多可用區域檔案系統](#)。

## 設定路由以從 VPC 外部存取多可用區域檔案系統

如果您的多可用區域檔案系統具有超出 VPC IP 地址範圍的 EndpointIpAddressRange，您需要在其中設定額外的路由 AWS Transit Gateway，才能從對等或內部部署網路存取您的檔案系統。

### Important

若要使用 Transit Gateway 存取多可用區域檔案系統，每個 Transit Gateway 的附件都必須在子網路中建立，其路由表與您的檔案系統相關聯。

### Note

如果單一可用區檔案系統或多可用區檔案系統的 位於 VPC 的 IP 地址範圍內 EndpointIpAddressRange，則不需要額外的 Transit Gateway 組態。

### 使用 設定路由 AWS Transit Gateway

1. 在 <https://console.aws.amazon.com/fsx/>：// 開啟 Amazon FSx 主控台。
2. 選擇您要設定從對等網路存取的 FSx for ONTAP 檔案系統。
3. 在網路和安全中複製端點 IP 地址範圍。
4. 新增路由至 Transit Gateway，將目的地為此 IP 地址範圍的流量路由至檔案系統的 VPC。如需詳細資訊，請參閱《Amazon VPC [傳輸閘道](#)》中的[使用傳輸閘道](#)。

## 5. 確認您可以從對等網路存取 FSx for ONTAP 檔案系統。

若要將路由表新增至檔案系統，請參閱 [更新檔案系統](#)。

### Note

管理、NFS 和 SMB 端點的 DNS 記錄只能從與檔案系統相同的 VPC 內解析。若要掛載磁碟區或從另一個網路連線至管理連接埠，您需要使用端點的 IP 地址。這些 IP 地址不會隨著時間而變更。

## 設定路由以從內部部署存取多可用區域檔案系統

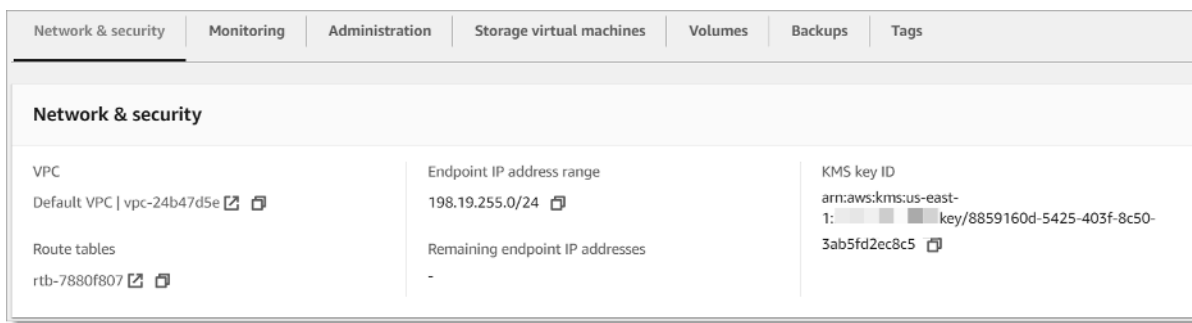
### AWS Transit Gateway 設定 從內部部署存取異地同步備份檔案系統

如果您的多可用區域檔案系統具有超出 VPC CIDR 範圍的 `EndpointIpAddressRange`，您需要在其中設定額外的路由 AWS Transit Gateway，才能從對等或內部部署網路存取您的檔案系統。

### Note

如果單一可用區檔案系統或多可用區檔案系統的 位於 VPC 的 IP 地址範圍內 `EndpointIpAddressRange`，則不需要額外的 Transit Gateway 組態。

1. 在 <https://console.aws.amazon.com/fsx/>：// 開啟 Amazon FSx 主控台。
2. 選擇您要設定從對等網路存取的 FSx for ONTAP 檔案系統。
3. 在網路和安全中複製端點 IP 地址範圍。



4. 將路由新增至 Transit Gateway，將目的地為此 IP 地址範圍的流量路由至檔案系統的 VPC。如需詳細資訊，請參閱《Amazon VPC Transit Gateway 使用者指南》中的 [使用傳輸](#) 閘道。
5. 確認您可以從對等網路存取 FSx for ONTAP 檔案系統。



### ⚠ Important

若要使用 Transit Gateway 存取多可用區域檔案系統，每個 Transit Gateway 的附件都必須在子網路中建立，其路由表與您的檔案系統相關聯。如果您有個別的 Transit Gateway 連接子網路，您還必須將這些子網路的路由表與 Amazon FSx 建立關聯，以便使用 Amazon FSx 端點地址進行更新。

若要將路由表新增至檔案系統，請參閱 [更新檔案系統](#)。

## Linux 用戶端上的掛載磁碟區

我們建議您使用 Linux 用戶端掛載的磁碟區具有 UNIX 或 的安全樣式設定 mixed。如需詳細資訊，請參閱 [管理 ONTAP 磁碟區的 FSx](#)。

### 📘 Note

根據預設，適用於 ONTAP NFS 掛載的 FSx 是 hard 掛載。為了確保在發生時能順利進行容錯移轉，建議您使用預設 hard 掛載選項。

在 Linux 用戶端上掛載 ONTAP 磁碟區

1. 前往 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 建立或選取執行 Amazon Linux 2 的 Amazon EC2 執行個體，該執行個體位於與檔案系統相同的 VPC 中。

如需啟動 EC2 Linux 執行個體的詳細資訊，請參閱《Amazon EC2 使用者指南》中的 [步驟 1：啟動執行個體](#)。

3. 連線至 Amazon EC2 Linux 執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的 [連線至 Linux 執行個體](#)。
4. 使用安全殼層 (SSH) 在 EC2 執行個體上開啟終端機，並使用適當的登入資料登入。
5. 在 EC2 執行個體上建立用於掛載 SVM 磁碟區的目錄，如下所示：

```
sudo mkdir /fsx
```

6. 使用以下命令將磁碟區掛載到您剛建立的目錄：

```
sudo mount -t nfs svm-dns-name:/volume-junction-path /fsx
```

下列範例使用範例值。

```
sudo mount -t nfs svm-01234567890abcdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /fsx
```

您也可以使用 SVM 的 IP 地址，而不是其 DNS 名稱。建議使用 DNS 名稱將用戶端掛載到第二代檔案系統，因為它有助於確保您的用戶端在檔案系統的高可用性 (HA) 對之間取得平衡。

```
sudo mount -t nfs 198.51.100.1:/vol1 /fsx
```

#### Note

對於第二代檔案系統，平行 NFS (pNFS) 通訊協定預設為啟用，並預設用於任何具有 NFS v4.1 或更新版本的用戶端掛載磁碟區。

## 使用 /etc/fstab 在執行個體重新啟動時自動掛載

若要在 Amazon EC2 Linux 執行個體重新啟動時自動重新掛載 FSx for ONTAP 磁碟區，請使用 /etc/fstab 檔案。/etc/fstab 檔案包含檔案系統的資訊，在執行個體啟動期間執行 `mount -a` 的命令會掛載中列出的檔案系統/etc/fstab。

#### Note

FSx for ONTAP 檔案系統不支援在 Amazon EC2 Mac 執行個體/etc/fstab上使用自動掛載。

#### Note

在更新 EC2 執行個體/etc/fstab的檔案之前，請確定您已建立 FSx for ONTAP 檔案系統。如需詳細資訊，請參閱[建立檔案系統](#)。

## 更新 EC2 執行個體上的 /etc/fstab 檔案

### 1. 連線到您的 EC2 執行個體：

- 若要從執行 macOS 或 Linux 的電腦連接至您的執行個體，請指定 SSH 命令的 .pem 檔案。為此，您必須使用 -i 選項和私密金鑰路徑。
- 若要從執行 Windows 的電腦連線至執行個體，您可以使用 MindTerm 或 PuTTY。您需要安裝 PuTTY 並將 .pem 檔案轉換為 .ppk 檔案，才可以使用該程式。

如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的下列主題：

- [使用 SSH 連接至您的 Linux 執行個體](#)
- [使用 PuTTY 從 Windows 連接至您的 Linux 執行個體](#)

### 2. 建立用於掛載 SVM 磁碟區的本機目錄。

```
sudo mkdir /fsx
```

3. 在您選擇的編輯器中開啟 /etc/fstab 檔案。
4. 為 /etc/fstab 檔案新增下行。在每個參數之間插入標籤字元。它應該顯示為一行，沒有換行符號。

```
svm-dns-name:volume-junction-path /fsx nfs nfsvers=version,defaults 0 0
```

您也可以使用磁碟區 SVM 的 IP 地址。最後三個參數表示 NFS 選項（我們設定為預設）、檔案系統和檔案系統檢查的傾印（通常不會使用這些參數，因此我們將其設定為 0）。

5. 儲存對檔案所做的變更。
6. 現在使用以下命令掛載檔案共享。系統下次啟動時，會自動掛載資料夾。

```
sudo mount /fsx  
sudo mount svm-dns-name:volume-junction-path
```

您的 EC2 執行個體現在已設定為在重新啟動時掛載 ONTAP 磁碟區。

## 在 Microsoft Windows 用戶端上掛載磁碟區

本節說明如何使用執行 Microsoft Windows 作業系統的用戶端存取 FSx for ONTAP 檔案系統中的資料。無論您使用的用戶端類型為何，請檢閱下列要求。

此程序假設用戶端和檔案系統位於相同的 VPC 和中 AWS 帳戶。如果用戶端位於內部部署或不同的 VPC AWS 帳戶、或 AWS 區域中，此程序也會假設您已使用 AWS Transit Gateway 或使用的私有安全通道來設定 AWS Direct Connect 或專用網路連線 AWS Virtual Private Network。如需詳細資訊，請參閱[從部署 VPC 外部存取資料](#)。

建議您使用 SMB 通訊協定將磁碟區連接至 Windows 用戶端。

### 先決條件

若要使用 Microsoft Windows 用戶端存取 ONTAP 儲存磁碟區，您必須滿足下列先決條件：

- 您要連接之磁碟區的 SVM 必須加入組織的 Active Directory，或者您必須使用工作群組。如需將 SVM 加入 Active Directory 的詳細資訊，請參閱 [管理 FSx for ONTAP 儲存虛擬機器](#)。如需使用工作群組的詳細資訊，請參閱 [在工作群組中設定 SMB 伺服器](#)。
- 您要連接的磁碟區具有 NTFS 或的安全樣式設定 mixed。如需詳細資訊，請參閱 [磁碟區安全樣式](#)。

使用 SMB 和 Active Directory 在 Windows 用戶端上掛載磁碟區

- 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
- 建立或選取執行 Microsoft Windows 的 Amazon EC2 執行個體，該執行個體位於與檔案系統相同的 VPC 中，並加入與磁碟區 SVM 相同的 Microsoft Active Directory。

如需啟動執行個體的詳細資訊，請參閱《Amazon EC2 使用者指南》中的[步驟 1：啟動執行個體](#)。

如需將 SVM 加入 Active Directory 的詳細資訊，請參閱 [管理 FSx for ONTAP 儲存虛擬機器](#)。

- 連線至 Amazon EC2 Windows 執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[連線至 Windows 執行個體](#)。
- 開啟命令提示。
- 執行下列命令。取代以下項目：
  - Z：以任何可用的磁碟機代號取代。
  - DNS\_NAME 將取代為磁碟區 SVM 的 SMB 端點的 DNS 名稱或 IP 地址。

- `SHARE_NAME` 將取代為 SMB 共用的名稱。`C$` 是 SVM 命名空間根目錄的預設 SMB 共用，但您不應將其掛載為 `C$`，因為 `C$` 會公開儲存體給根磁碟區，並可能導致安全性和服務中斷。您應該提供要掛載的 SMB 共用名稱，而不是 `C$`。如需建立 SMB 共用的詳細資訊，請參閱 [管理 SMB 共用](#)。

```
net use Z: \\DNS_NAME\SHARE_NAME
```

下列範例使用範例值。

```
net use Z: \\corp.example.com\group_share
```

您也可以使用 SVM 的 IP 地址，而不是其 DNS 名稱。建議使用 DNS 名稱將用戶端掛載到第二代檔案系統，因為它有助於確保您的用戶端在檔案系統的高可用性 (HA) 對之間取得平衡。

```
net use Z: \\198.51.100.5\group_share
```

## macOS 用戶端上的掛載磁碟區

本節說明如何使用執行 macOS 作業系統的用戶端存取 FSx for ONTAP 檔案系統中的資料。無論您使用的用戶端類型為何，請檢閱下列需求。

此程序假設用戶端和檔案系統位於相同的 VPC 和 中 AWS 帳戶。如果用戶端位於內部部署，或位於不同的 VPC 中 AWS 區域，AWS 帳戶 或者您已使用 AWS Transit Gateway 或使用的私有安全通道來設定 AWS Direct Connect 或專用網路連線 AWS Virtual Private Network。如需詳細資訊，請參閱[從部署 VPC 外部存取資料](#)。

我們建議您使用 SMB 通訊協定將磁碟區連接至 Mac 用戶端。

使用 SMB 在 macOS 用戶端上掛載 ONTAP 磁碟區

1. 前往 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 建立或選取執行與檔案系統位於相同 VPC 中之 macOS 的 Amazon EC2 Mac 執行個體。

如需啟動執行個體的詳細資訊，請參閱《Amazon EC2 使用者指南》中的[步驟 1：啟動執行個體](#)。

3. 連線至您的 Amazon EC2 Mac 執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[連線至 Linux 執行個體](#)。

4. 使用安全殼層 (SSH) 在 EC2 執行個體上開啟終端機，並使用適當的登入資料登入。
5. 在 EC2 執行個體上建立掛載磁碟區的目錄，如下所示：

```
sudo mkdir /fsx
```

6. 使用以下命令掛載磁碟區。

```
sudo mount -t smbfs filesystem-dns-name:/smb-share-name mount-point
```

下列範例使用範例值。

```
sudo mount -t smbfs svm-01234567890abcde2.fs-01234567890abcde5.fsx.us-east-1.amazonaws.com:/C$ /fsx
```

您也可以使用 SVM 的 IP 地址，而不是其 DNS 名稱。建議使用 DNS 名稱將用戶端掛載到第二代檔案系統，因為它有助於確保您的用戶端在檔案系統的高可用性 (HA) 對之間取得平衡。

```
sudo mount -t smbfs 198.51.100.10:/C$ /fsx
```

C\$ 是您可以掛載的預設 SMB 共用，以查看 SVM 命名空間的根目錄。如果您已在 SVM 中建立任何伺服器訊息區塊 (SMB) 共用，請提供 SMB 共用名稱，而非 C\$。如需建立 SMB 共用的詳細資訊，請參閱 [管理 SMB 共用](#)。

## 使用 NFS 在 macOS 用戶端上掛載 ONTAP 磁碟區

1. 前往 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 建立或選取執行 Amazon Linux 2 的 Amazon EC2 執行個體，該執行個體位於與檔案系統相同的 VPC 中。

如需啟動 EC2 Linux 執行個體的詳細資訊，請參閱《Amazon EC2 使用者指南》中的 [步驟 1：啟動執行個體](#)。

3. 連線至 Amazon EC2 Linux 執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的 [連線至 Linux 執行個體](#)。
4. 在執行個體啟動期間使用使用者資料指令碼，或執行下列命令，在 Linux EC2 執行個體上掛載 FSx for ONTAP 磁碟區：

```
sudo mount -t nfs -o nfsvers=NFS_version svm-dns-name:/volume-junction-path /mount-point
```

下列範例使用範例值。

```
sudo mount -t nfs -o nfsvers=4.1  
svm-01234567890abcdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /  
fsxontap
```

您也可以使用 SVM 的 IP 地址，而不是其 DNS 名稱。建議使用 DNS 名稱將用戶端掛載到第二代檔案系統，因為它有助於確保您的用戶端在檔案系統的 HA 對之間取得平衡。

```
sudo mount -t nfs -o nfsvers=4.1 198.51.100.1:/vol1 /fsxontap
```

5. 使用以下命令將磁碟區掛載到您剛建立的目錄。

```
sudo mount -t nfs svm-dns-name:/volume-junction-path /fsx
```

下列範例使用範例值。

```
sudo mount -t nfs svm-01234567890abcdef0.fs-01234567890abcdef1.fsx.us-  
east-1.amazonaws.com:/vol1 /fsx
```

您也可以使用 SVM 的 IP 地址，而不是其 DNS 名稱。建議使用 DNS 名稱將用戶端掛載到第二代檔案系統，因為它有助於確保您的用戶端在檔案系統的高可用性 (HA) 對之間取得平衡。

```
sudo mount -t nfs 198.51.100.1:/vol1 /fsx
```

## 佈建 Linux 的 iSCSI

FSx for ONTAP 支援 iSCSI 通訊協定。您需要同時在 Linux 用戶端和檔案系統上佈建 iSCSI，才能使用 iSCSI 通訊協定在用戶端和檔案系統之間傳輸資料。iSCSI 通訊協定可用於具有 6 個或更少 [高可用性 \(HA\)](#) 對的所有檔案系統。

在 Amazon FSx for NetApp ONTAP 上設定 iSCSI 有三個主要步驟，涵蓋於下列程序：

1. 在 Linux 主機上安裝和設定 iSCSI 用戶端。

2. 在檔案系統的 SVM 上設定 iSCSI。
  - 建立 iSCSI 啟動器群組。
  - 將啟動器群組對應至 LUN。
3. 在 Linux 用戶端上安裝 iSCSI LUN。

## 開始之前

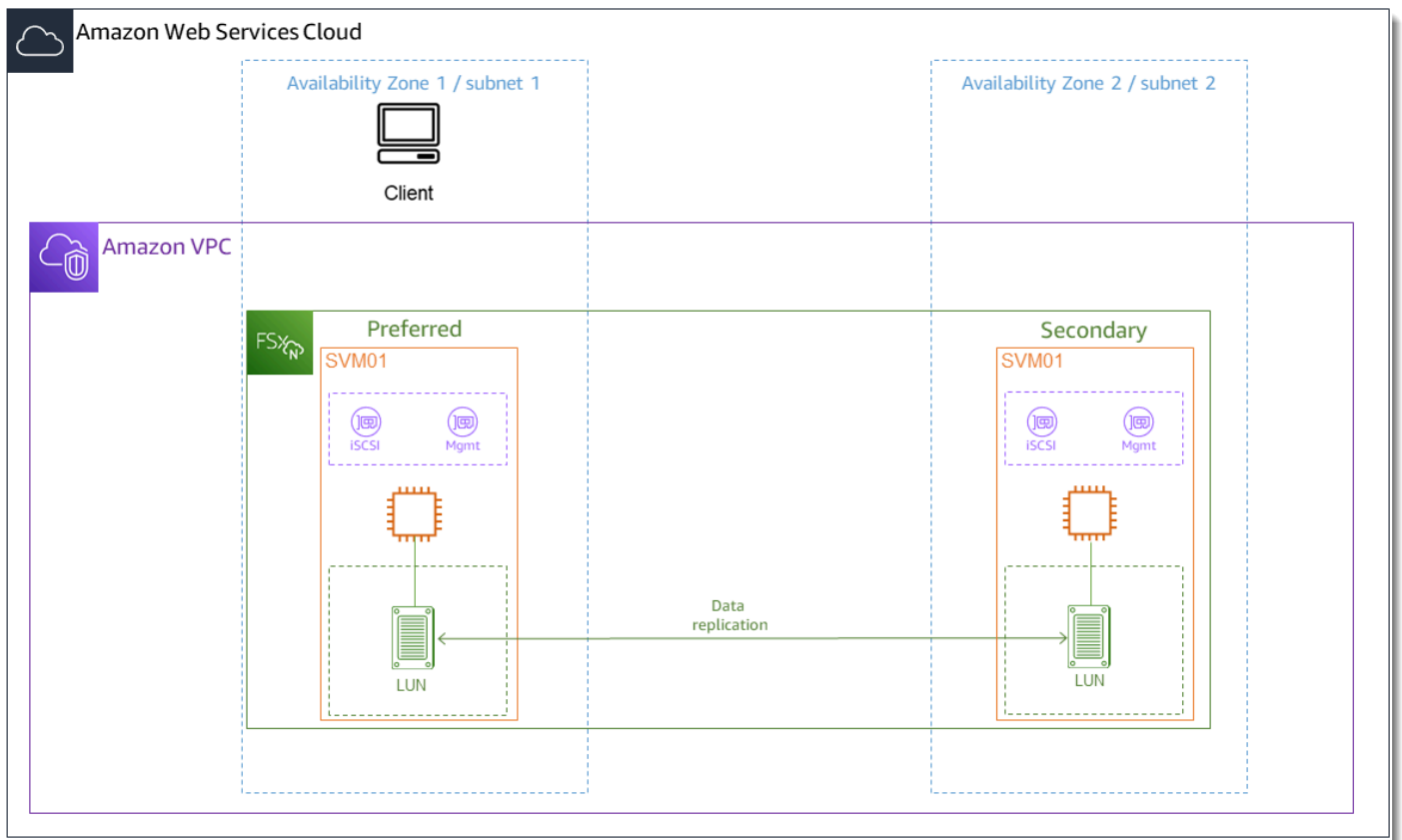
在開始設定 iSCSI 檔案系統的程序之前，您需要完成下列項目。

- 建立適用於 ONTAP 檔案系統的 FSx。如需詳細資訊，請參閱[建立檔案系統](#)。
- 在檔案系統上建立 iSCSI LUN。如需詳細資訊，請參閱[建立 iSCSI LUN](#)。
- 在與檔案系統相同的 VPC 中建立執行 Amazon Linux 2 Amazon Machine Image (AMI) 的 EC2 執行個體。這是您要設定 iSCSI 並存取檔案資料的 Linux 主機。

除了這些程序的範圍之外，如果主機位於另一個 VPC 中，您可以使用 VPC 對等互連 AWS Transit Gateway，或授予其他 VPCs 存取磁碟區的 iSCSI 端點。如需詳細資訊，請參閱[從部署 VPC 外部存取資料](#)。

- 設定 Linux 主機的 VPC 安全群組，以允許傳入和傳出流量，如中所述[使用 Amazon VPC 的檔案系統存取控制](#)。
- 取得具有您將用來存取 CLI ONTAP 之 fsxadmin 權限 ONTAP 的使用者登入資料。如需詳細資訊，請參閱[ONTAP 角色和使用者](#)。
- 您將為 iSCSI 設定的 Linux 主機，以及用於存取 FSx for ONTAP 檔案系統的 Linux 主機位於相同的 VPC 和中 AWS 帳戶。
- 我們建議 EC2 執行個體與您檔案系統偏好的子網路位於相同的可用區域，如下圖所示。





如果您的 EC2 執行個體執行與 Amazon Linux 2 不同的 Linux AMI，則可能已安裝這些程序和範例中使用的一些公用程式，而且您可以使用不同的命令來安裝必要的套件。除了安裝套件之外，本節中使用的命令對其他 EC2 Linux AMIs 有效。

## 主題

- [在 Linux 主機上安裝和設定 iSCSI](#)
- [在 FSx for ONTAP 檔案系統上設定 iSCSI](#)
- [在 Linux 用戶端上安裝 iSCSI LUN](#)

## 在 Linux 主機上安裝和設定 iSCSI

### 安裝 iSCSI 用戶端

1. 確認您的 Linux 裝置已安裝 `device-mapper-multipath` `iscsi-initiator-utils` 和 `iscsi-initiator-utils`。使用 SSH 用戶端連線至 Linux 執行個體。如需詳細資訊，請參閱[使用 SSH 連線至 Linux 執行個體](#)。

2. 使用下列命令安裝 multipath 和 iSCSI 用戶端。如果您想要在檔案伺服器之間自動容錯移轉，multipath 則需要安裝。

```
~$ sudo yum install -y device-mapper-multipath iscsi-initiator-utils
```

3. 若要在使用時，在檔案伺服器之間自動容錯移轉時加快回應速度 multipath，請將 /etc/iscsi/iscsid.conf 檔案中的替代逾時值設定為值，5 而不是使用的預設值 120。

```
~$ sudo sed -i 's/node.session.timeo.replacement_timeout = .*/  
node.session.timeo.replacement_timeout = 5/' /etc/iscsi/iscsid.conf; sudo cat /etc/  
iscsi/iscsid.conf | grep node.session.timeo.replacement_timeout
```

4. 啟動 iSCSI 服務。

```
~$ sudo service iscsid start
```

請注意，根據您的 Linux 版本，您可能需要改用此命令：

```
~$ sudo systemctl start iscsid
```

5. 使用以下命令確認服務正在執行。

```
~$ sudo systemctl status iscsid.service
```

系統會以下列輸出回應：

```
iscsid.service - Open-iSCSI  
   Loaded: loaded (/usr/lib/systemd/system/iscsid.service; disabled; vendor  
   preset: disabled)  
   Active: active (running) since Fri 2021-09-02 00:00:00 UTC; 1min ago  
   Docs: man:iscsid(8)  
         man:iscsiadm(8)  
  Process: 14658 ExecStart=/usr/sbin/iscsid (code=exited, status=0/SUCCESS)  
 Main PID: 14660 (iscsid)  
   CGroup: /system.slice/iscsid.service  
          ##14659 /usr/sbin/iscsid  
          ##14660 /usr/sbin/iscsid
```

## 在 Linux 用戶端上設定 iSCSI

1. 若要讓用戶端在您的檔案伺服器之間自動容錯移轉，您必須設定多路徑。使用下列命令：

```
~$ sudo mpathconf --enable --with_multipathd y
```

2. 使用以下命令判斷 Linux 主機的啟動者名稱。啟動器名稱的位置取決於您的 iSCSI 公用程式。如果您使用的是 `iscsi-initiator-utils`，則啟動器名稱位於檔案 `/etc/iscsi/initiatorname.iscsi`。

```
~$ sudo cat /etc/iscsi/initiatorname.iscsi
```

系統會以啟動者名稱回應。

```
InitiatorName=iqn.1994-05.com.redhat:abcdef12345
```

## 在 FSx for ONTAP 檔案系統上設定 iSCSI

1. 使用下列命令，連線到您建立 iSCSI LUN 之 FSx for ONTAP 檔案系統的 NetApp ONTAP CLI。如需詳細資訊，請參閱[使用 NetApp ONTAP CLI](#)。

```
~$ ssh fsxadmin@your_management_endpoint_ip
```

2. 使用 NetApp ONTAP CLI [lun igroup create](#) 命令建立啟動器群組 (igroup)。啟動器群組會映射至 iSCSI LUNs 並控制哪些啟動器（用戶端）可存取 LUNs。 `host_initiator_name` 將取代為您先前程序中擷取的 Linux 主機的啟動器名稱。

```
::> lun igroup create -vserver svm_name -igroup igroup_name -  
initiator host_initiator_name -protocol iscsi -ostype linux
```

如果您想要將對應至此 igroup LUNs 提供給多個主機，您可以指定多個以逗號分隔的啟動者名稱。如需詳細資訊，請參閱 NetApp ONTAP 文件中心中的 [lun igroup 建立](#)。

3. 使用 [lun igroup show](#) 命令確認 igroup 存在：

```
::> lun igroup show
```

系統會以下列輸出回應：

| Vserver         | Igroup             | Protocol | OS Type | Initiators                         |
|-----------------|--------------------|----------|---------|------------------------------------|
| <i>svm_name</i> | <i>igroup_name</i> | iscsi    | linux   | iqn.1994-05.com.redhat:abcdef12345 |

4. 此步驟假設您已建立 iSCSI LUN。如果尚未執行，請參閱 [建立 iSCSI LUN](#) 以取得執行此作業 step-by-step 說明。

使用 從您建立的 LUN 建立對應到您建立的 igroup [lun mapping create](#)，並指定下列屬性：

- *svm\_name* – 提供 iSCSI 目標的儲存虛擬機器名稱。主機使用此值來到達 LUN。
- *vol\_name* – 託管 LUN 的磁碟區名稱。
- *lun\_name* – 您指派給 LUN 的名稱。
- *igroup\_name* – 啟動器群組的名稱。
- *lun\_id* – LUN ID 整數專屬於映射，而非 LUN 本身。這由 igroup 中的啟動器用作邏輯單位編號，在存取儲存體時，會為啟動器使用此值。

```
::> lun mapping create -vserver svm_name -path /vol/vol_name/lun_name -
igroup igroup_name -lun-id lun_id
```

5. 使用 [lun show -path](#) 命令來確認 LUN 已建立、上線和映射。

```
::> lun show -path /vol/vol_name/lun_name -fields state,mapped,serial-hex
```

系統會以下列輸出回應：

| Vserver         | Path                                    | serial-hex               | state  | mapped |
|-----------------|-----------------------------------------|--------------------------|--------|--------|
| <i>svm_name</i> | /vol/ <i>vol_name</i> / <i>lun_name</i> | 6c5742314e5d52766e796150 | online | mapped |

儲存 serial\_hex 值（在此範例中為 6c5742314e5d52766e796150），您將在後續步驟中使用它來為區塊型裝置建立易記的名稱。

6. 使用 [network interface show -vserver](#) 命令來擷取您已建立 iSCSI LUN 之 SVM 的 iscsi\_1 和 iscsi\_2 介面地址。

```
::> network interface show -vserver svm_name
```

系統會以下列輸出回應：

```

      Logical      Status      Network      Current
      Current Is
Vserver  Interface  Admin/Oper  Address/Mask  Node
      Port      Home
-----
      -----
svm_name
      iscsi_1      up/up      172.31.0.143/20
FSxId0123456789abcdef8-01  e0e      true
      iscsi_2      up/up      172.31.21.81/20
FSxId0123456789abcdef8-02  e0e      true
      nfs_smb_management_1
      up/up      198.19.250.177/20
FSxId0123456789abcdef8-01  e0e      true
3 entries were displayed.

```

在此範例中，的 IP 地址 `iscsi_1` 為 172.31.0.143，而 `iscsi_2` 為 172.31.21.81。

## 在 Linux 用戶端上安裝 iSCSI LUN

在 Linux 用戶端上安裝 iSCSI LUN 的程序包含三個步驟：

1. 探索目標 iSCSI 節點
2. 分割 iSCSI LUN
3. 在用戶端上安裝 iSCSI LUN

下列程序涵蓋這些項目。

### 探索目標 iSCSI 節點

1. 在 Linux 用戶端上，使用下列命令，使用 `iscsi_1` 的 IP 地址 *iscsi\_1\_IP* 探索目標 iSCSI 節點。

```

~$ sudo iscsiadm --mode discovery --op update --type sendtargets --
portal iscsi_1_IP

```

```
172.31.0.143:3260,1029
iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3
172.31.21.81:3260,1028
iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3
```

在此範例中，

iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3 會對應至偏好可用區域中 target\_initiator iSCSI LUN 的。

2. (選用) 若要將高於 Amazon EC2 單一用戶端最高 5 Gbps (~625 MBps) 的輸送量驅動到您的 iSCSI LUN，請遵循適用於 Linux [執行個體的 Amazon Elastic Compute Cloud 使用者指南中所述的 Amazon EC2 執行個體網路頻寬](#) 程序，以建立額外的工作階段以提高輸送量。

下列命令會在每個可用區域中為每個 ONTAP 節點建立每個啟動器 8 個工作階段，讓用戶端能夠驅動高達 40 Gbps (5,000 MBps) 的彙總輸送量至 iSCSI LUN。

```
~$ sudo iscsiadm --mode node -T target_initiator --op update -n
node.session.nr_sessions -v 8
```

3. 登入目標啟動器。您的 iSCSI LUNs 會顯示為可用的磁碟。

```
~$ sudo iscsiadm --mode node -T target_initiator --login
```

```
Logging in to [iface: default, target:
iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3, portal:
172.31.14.66,3260] (multiple)
Login to [iface: default, target:
iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3, portal:
172.31.14.66,3260] successful.
```

上述輸出已截斷；您應該會在每個檔案伺服器上看到每個工作階段 Logging in 的一個 Login successful 回應。如果每個節點有 4 個工作階段，將會有 8 個 Logging in 和 8 個 Login successful 回應。

4. 使用下列命令，透過顯示具有多個政策的單一 LUN 來驗證 dm-multipath 是否已識別和合併 iSCSI 工作階段。應該有相同數量的裝置，列出為 active，而列出為 enabled。

```
~$ sudo multipath -ll
```

在輸出中，磁碟名稱的格式為 `dm-xyz`，其中 `xyz` 是整數。如果沒有其他多路徑磁碟，則此值為 `dm-0`。

```
3600a09806c5742314e5d52766e79614f dm-xyz NETAPP ,LUN C-Mode
size=10G features='4 queue_if_no_path pg_init_retries 50 retain_attached_hw_handle'
hwhandler='0' wp=rw
|+- policy='service-time 0' prio=50 status=active
| |- 0:0:0:1 sda      8:0   active ready running
| |- 1:0:0:1 sdc      8:32  active ready running
| |- 3:0:0:1 sdg      8:96  active ready running
| `-- 4:0:0:1 sdh      8:112 active ready running
`+- policy='service-time 0' prio=10 status=enabled
  |- 2:0:0:1 sdb      8:16  active ready running
  |- 7:0:0:1 sdf      8:80  active ready running
  |- 6:0:0:1 sde      8:64  active ready running
  `-- 5:0:0:1 sdd      8:48  active ready running
```

您的區塊裝置現在已連線至您的 Linux 用戶端。它位於路徑 `/dev/dm-xyz`。您不應將此路徑用於管理用途；而是使用路徑下的符號連結 `/dev/mapper/wwid`，其中 *wwid* 是 LUN 的唯一識別符，在各裝置之間保持一致。在下一個步驟中，您將為提供易記的名稱 *wwid*，以便與其他多路徑磁碟區區別。

### 為區塊裝置指派易記的名稱

- 若要為裝置提供易記的名稱，請在 `/etc/multipath.conf` 檔案中建立別名。若要執行此作業，請使用您偏好的文字編輯器將下列項目新增至檔案，取代下列預留位置：
  - `serial_hex` 將取代為您[在 FSx for ONTAP 檔案系統上設定 iSCSI](#)程序中儲存的值。
  - 將字首 `3600a0980` 新增至 `serial_hex` 值，如範例所示。這是 Amazon FSx for NetApp ONTAP 使用的 NetApp ONTAP 分佈的唯一前導詞。
  - `device_name` 將取代為您想要用於裝置的易記名稱。

```
multipaths {
    multipath {
        wwid 3600a0980serial_hex
        alias device_name
    }
}
```

```
}
```

或者，您可以將下列指令碼複製並儲存為 bash 檔案，例如 `multipath_alias.sh`。您可以使用 `sudo` 權限執行指令碼，將 `serial_hex`（不含 3600a0980 字首）和取代 `device_name` 為各自的序號和所需的易記名稱。此指令碼會在 `/etc/multipath.conf` 檔案中搜尋未註解的 `multipaths` 區段。如果存在項目，它會將 `multipath` 項目附加到該區段；否則，它會為區塊裝置建立一個具有 `multipath` 項目的新 `multipaths` 區段。

```
#!/bin/bash
SN=serial_hex
ALIAS=device_name
CONF=/etc/multipath.conf
grep -q '^multipaths {' $CONF
UNCOMMENTED=$?
if [ $UNCOMMENTED -eq 0 ]
then
    sed -i '/^multipaths {/a\\tmultipath {\\n\\t\\twid 3600a0980'"${SN}"'"\\n\\t\\talias '"${ALIAS}"'"\\n\\t}\\n' $CONF
else
    printf "multipaths {\\n\\tmultipath {\\n\\t\\twid 3600a0980${SN}\\n\\t\\talias $ALIAS\\n\\t}\\n}" >> $CONF
fi
```

2. 重新啟動 `multipathd` 服務，以使變更 `/etc/multipathd.conf` 生效。

```
~$ systemctl restart multipathd.service
```

## 分割 LUN

下一個步驟是使用 格式化和分割 `LUNfdisk`。

1. 使用以下命令來驗證 的路徑 `device_name` 是否存在。

```
~$ ls /dev/mapper/device_name
```

```
/dev/device_name
```

2. 使用 分割磁碟 `fdisk`。您將輸入互動式提示。依顯示的順序輸入選項。您可以使用小於最後一個扇區的值來建立多個分割區 (20971519 在此範例中為 )。



 Note

Last sector 值會根據 iSCSI LUN 的大小 (在此範例中為 10GB) 而有所不同。

```
~$ sudo fdisk /dev/mapper/device_name
```

fdisk 互動式提示隨即啟動。

```
Welcome to fdisk (util-linux 2.30.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0x66595cb0.

Command (m for help): n
Partition type
  p primary (0 primary, 0 extended, 4 free)
  e extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048): 2048
Last sector, +sectors or +size{K,M,G,T,P} (2048-20971519, default
20971519): 20971519

Created a new partition 1 of type 'Linux' and of size 512 B.
Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.
```

進入 後w，您的新分割區/dev/mapper/*partition\_name*就會變成可用。*partition\_name* 的格式為 <*device\_name*><*partition\_number*>。1 做為上一個步驟中fdisk命令中使用的分割區編號。

3. 使用 /dev/mapper/*partition\_name*作為路徑來建立檔案系統。

```
~$ sudo mkfs.ext4 /dev/mapper/partition_name
```

系統會以下列輸出回應：

```
mke2fs 1.42.9 (28-Dec-2013)
Discarding device blocks: done
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=16 blocks
655360 inodes, 2621184 blocks
131059 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
80 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632
Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

在 Linux 用戶端上掛載 LUN

1. 建立 directory *directory\_path* 做為檔案系統的掛載點。

```
~$ sudo mkdir /directory_path/mount_point
```

2. 使用以下命令掛載檔案系統。

```
~$ sudo mount -t ext4 /dev/mapper/partition_name /directory_path/mount_point
```

3. (選用) 如果您想要提供掛載目錄的特定使用者所有權，*username*請以擁有者的使用者名稱取代。

```
~$ sudo chown username:username /directory_path/mount_point
```

4. (選用) 確認您可以從檔案系統讀取和寫入資料。

```
~$ echo "Hello world!" > /directory_path/mount_point/HelloWorld.txt
~$ cat directory_path/HelloWorld.txt
Hello world!
```

您已成功在 Linux 用戶端上建立和掛載 iSCSI LUN。

## 佈建適用於 Windows 的 iSCSI

FSx for ONTAP 支援 iSCSI 通訊協定。您需要在 Windows 用戶端和 SVM 和磁碟區上佈建 iSCSI，才能使用 iSCSI 通訊協定在用戶端和檔案系統之間傳輸資料。iSCSI 通訊協定適用於所有具有 6 個或更少 [高可用性 \(HA\)](#) 對的檔案系統。

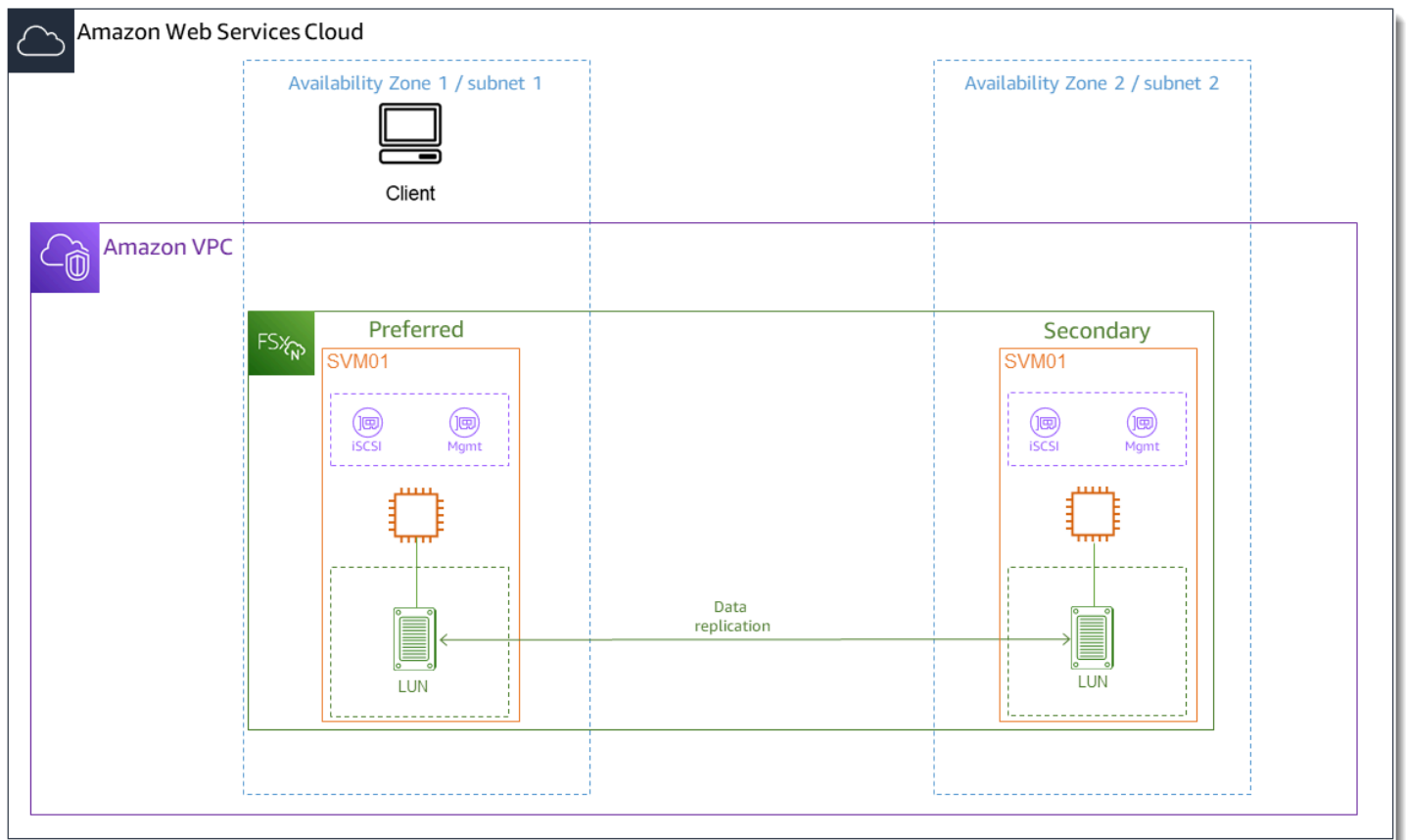
這些程序中的範例示範如何在用戶端和 FSx for ONTAP 檔案系統上佈建 iSCSI 通訊協定，並使用下列設定：

- 掛載至 Windows 主機的 iSCSI LUN 已建立。如需詳細資訊，請參閱[建立 iSCSI LUN](#)。
- 掛載 iSCSI LUN 的 Microsoft Windows 主機是執行 Microsoft Windows Server 2019 Amazon Machine Image (AMI) 的 Amazon EC2 執行個體。它具有設定成允許傳入和傳出流量的 VPC 安全群組，如中所述[使用 Amazon VPC 的檔案系統存取控制](#)。

您可以在設定中使用不同的 Microsoft Windows AMI。

- 用戶端和檔案系統位於相同的 VPC 和中 AWS 帳戶。如果用戶端位於另一個 VPC 中，您可以使用 VPC 對等互連或 AWS Transit Gateway 授予其他 VPCs 存取 iSCSI 端點的權限。如需詳細資訊，請參閱[從部署 VPC 外部存取資料](#)。

我們建議 EC2 執行個體與您檔案系統偏好的子網路位於相同的可用區域，如下圖所示。



## 主題

- [在 Windows 用戶端上設定 iSCSI](#)
- [在 FSx for ONTAP 檔案系統上設定 iSCSI](#)
- [在 Windows 用戶端上掛載 iSCSI LUN](#)
- [驗證您的 iSCSI 組態](#)

## 在 Windows 用戶端上設定 iSCSI

1. 使用 Windows 遠端桌面連線到您要掛載 iSCSI LUN 的 Windows 用戶端。如需詳細資訊，請參閱《Amazon Elastic Compute Cloud 使用者指南》中的[使用 RDP 連線至 Windows 執行個體](#)。
2. 以管理員身分開啟 Windows PowerShell。使用下列命令在 Windows 執行個體上啟用 iSCSI，並將 iSCSI 服務設定為自動啟動。

```
PS C:\> Start-Service MSiSCSI
PS C:\> Set-Service -Name msiscsi -StartupType Automatic
```

3. 擷取 Windows 執行個體的啟動器名稱。您將使用此值，在 FSx for ONTAP 檔案系統上使用 NetApp ONTAP CLI 設定 iSCSI。

```
PS C:\> (Get-InitiatorPort).NodeAddress
```

系統會以啟動器連接埠回應：

```
iqn.1991-05.com.microsoft:ec2amaz-abc123d
```

4. 若要讓用戶端在您的檔案伺服器之間自動容錯移轉，您需要在 Windows 執行個體上安裝 Multipath-I0(MPIO)。使用下列命令：

```
PS C:\> Install-WindowsFeature Multipath-I0
```

5. 安裝完成後重新啟動您的 Windows Multipath-I0 執行個體。保持 Windows 執行個體開啟，以執行在下列區段中掛載 iSCSI LUN 的步驟。

## 在 FSx for ONTAP 檔案系統上設定 iSCSI

1. 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。*management\_endpoint\_ip* 將取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

2. 使用 ONTAP CLI [lun igroup create](#) 建立啟動器群組或 igroup。啟動器群組會映射至 iSCSI LUNs 並控制哪些啟動器（用戶端）可存取 LUNs。host\_initiator\_name 使用您在先前程序中擷取的 Windows 主機中的啟動器名稱取代。

```
::> lun igroup create -vserver svm_name -igroup igroup_name -  
initiator host_initiator_name -protocol iscsi -ostype windows
```

lo 讓與此對應的 LUNs igroup 可供多個主機使用，您可以使用 CLI [lun igroup create](#) ONTAP 命令指定多個逗號分隔的啟動器名稱。

3. 確認 igroup 已成功使用 [lun igroup show](#) CLI ONTAP 命令建立：

```
::> lun igroup show
```

系統會以下列輸出回應：

| Vserver         | Igroup             | Protocol | OS Type | Initiators                          |
|-----------------|--------------------|----------|---------|-------------------------------------|
| <i>svm_name</i> | <i>igroup_name</i> | iscsi    | windows | iqn.1994-05.com.windows:abcdef12345 |

igroup 建立後，您就可以建立 LUNs 並將其對應至 igroup。

- 此步驟假設您已建立 iSCSI LUN。如果沒有，請參閱 [建立 iSCSI LUN](#) 以取得執行此作業 step-by-step 說明。

建立從 LUN 到新的 LUN 映射 igroup。

```
::> lun mapping create -vserver svm_name -path /vol/vol_name/lun_name -  
igroup igroup_name -lun-id lun_id
```

- 確認 LUN 已建立、上線，並使用下列命令映射：

```
::> lun show -path /vol/vol_name/lun_name
```

| Vserver         | Path                                    | State  | Mapped | Type    | Size |
|-----------------|-----------------------------------------|--------|--------|---------|------|
| <i>svm_name</i> | /vol/ <i>vol_name</i> / <i>lun_name</i> | online | mapped | windows | 10GB |

您現在可以在 Windows 執行個體上新增 iSCSI 目標。

- 使用下列命令擷取 SVM 的 iscsi\_1 和 iscsi\_2 介面的 IP 地址：

```
::> network interface show -vserver svm_name
```

| Vserver         | Logical Interface    | Status Admin/Oper | Network Address/Mask | Current Node              | Current Port | Is Home |
|-----------------|----------------------|-------------------|----------------------|---------------------------|--------------|---------|
| <i>svm_name</i> | iscsi_1              | up/up             | 172.31.0.143/20      | FSxId0123456789abcdef8-01 | e0e          | true    |
|                 | iscsi_2              | up/up             | 172.31.21.81/20      | FSxId0123456789abcdef8-02 | e0e          | true    |
|                 | nfs_smb_management_1 |                   |                      |                           |              |         |

```

up/up      198.19.250.177/20  FSxId0123456789abcdef8-01
                                         e0e      true
3 entries were displayed.

```

在此範例中，的 IP 地址 `iscsi_1` 為 172.31.0.143，而 `iscsi_2` 為 172.31.21.81。

## 在 Windows 用戶端上掛載 iSCSI LUN

1. 在 Windows 執行個體上，以管理員身分開啟 PowerShell 終端機。
2. 您將建立執行下列動作的 .ps1 指令碼：
  - 連接到每個檔案系統的 iSCSI 介面。
  - 新增和設定 iSCSI 的 MPIO。
  - 為每個 iSCSI 連線建立 8 個工作階段，可讓用戶端驅動高達 40 Gbps (5,000 MBps) 的彙總輸送量至 iSCSI LUN。擁有 8 個工作階段可確保單一用戶端可為 ONTAP 輸送量容量的最高層級 FSx 驅動完整的 4,000 MBps 輸送量容量。您可以選擇透過修改 `RecommendedConnectionCount` 變數，將工作階段數量變更為更高或更低的工作階段數量（每個工作階段提供高達 625 MBps 的輸送量）。如需詳細資訊，請參閱 [《Amazon Elastic Compute Cloud Windows 執行個體使用者指南》](#) 中的 [Amazon EC2 執行個體網路頻寬](#)。

將下列命令集複製到 檔案以建立 .ps1 指令碼。

- 將 `iscsi_1` 和 `iscsi_2` 取代為您在上一個步驟中擷取的 IP 地址。
- `ec2_ip` 將取代為 Windows 執行個體的 IP 地址。

```

Write-Host "Starting iSCSI connection setup..."
$TargetPortalAddresses = @("iscsi_1","iscsi_2"); $LocaliSCSIAddress = "ec2_ip"
$RecommendedConnectionCount = 8

Foreach ($TargetPortalAddress in $TargetPortalAddresses) {
    New-IscsiTargetPortal -TargetPortalAddress $TargetPortalAddress -
TargetPortalPortNumber 3260 -InitiatorPortalAddress $LocaliSCSIAddress
}

New-MSDSMSupportedHW -VendorId MSFT2005 -ProductId iSCSIBusType_0x9

$currentMPIOSettings = Get-MPIOSetting

```

```

    if ($currentMPIOSettings.PathVerificationState -ne 'Enabled') {
        Write-Host "Setting MPIO path verification state to Enabled"; Set-
MPIOSetting -NewPathVerificationState Enabled
    } else { Write-Host "MPIO path verification state already Enabled" }

    $portalConnectionCounts = @{}
    foreach ($TargetPortalAddress in $TargetPortalAddresses)
    { $portalConnectionCounts[$TargetPortalAddress] = 0 }

    $sessions = Get-IscsiSession
    if ($sessions) {
        foreach ($session in $sessions) {
            if ($session.IsConnected) {
                $targetPortal = (Get-IscsiTargetPortal -iSCSISession
$session).TargetPortalAddress
                if ($portalConnectionCounts.ContainsKey($targetPortal))
                { $portalConnectionCounts[$targetPortal]++ }
            }
        }
    }

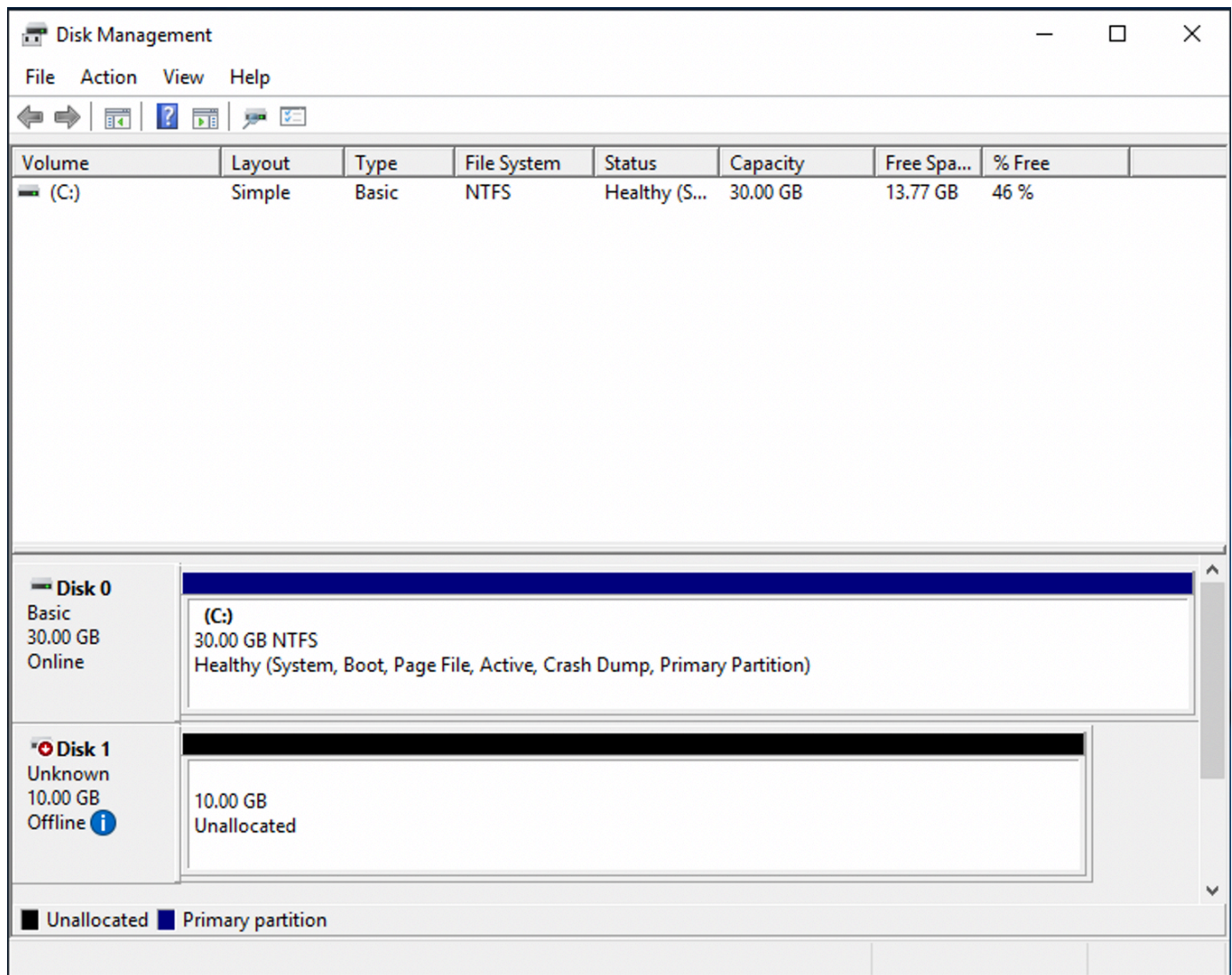
    foreach ($TargetPortalAddress in $TargetPortalAddresses) {
        $existingCount = $portalConnectionCounts[$TargetPortalAddress];
        $remainingConnections = $RecommendedConnectionCount - $existingCount
        Write-Host "Portal $TargetPortalAddress has $existingCount
existing connections, $remainingConnections remaining (max recommended:
$RecommendedConnectionCount)"
        if ($remainingConnections -gt 0) {
            Write-Host "Creating $remainingConnections connections for portal
$TargetPortalAddress"
            1..$remainingConnections | ForEach-Object {
                Get-IscsiTarget | Connect-IscsiTarget -IsMultipathEnabled $true -
TargetPortalAddress $TargetPortalAddress -InitiatorPortalAddress $LocaliSCSIAddress
-IsPersistent $true
            }
        } else { Write-Host "Maximum connections (8) reached for portal
$TargetPortalAddress" }
    }

    Set-MSDSMGlobalDefaultLoadBalancePolicy -Policy RR

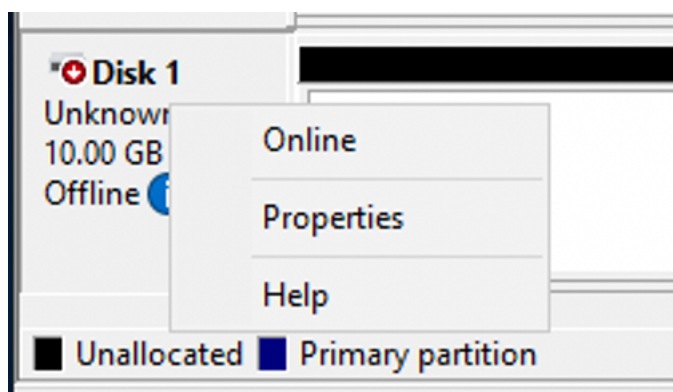
```

3. 啟動 Windows 磁碟管理應用程式。開啟 Windows Run 對話方塊，然後輸入 `diskmgmt.msc` 並按下 Enter。磁碟管理應用程式隨即開啟。





4. 尋找未配置的磁碟 這是 iSCSI LUN。在此範例中，磁碟 1 是 iSCSI 磁碟。已離線。



將游標放在磁碟 1 上並按一下滑鼠右鍵，然後選擇線上，讓磁碟區上線。

**Note**

您可以修改儲存區域網路 (SAN) 政策，讓新的磁碟區自動上線。如需詳細資訊，請參閱 Microsoft Windows Server 命令參考中的 [SAN 政策](#)。

- 若要初始化磁碟，請在磁碟 1 上按一下滑鼠右鍵，然後選擇初始化。初始化對話方塊隨即出現。選擇確定初始化磁碟。
- 像往常一樣格式化磁碟。格式化完成後，iSCSI 磁碟機會在 Windows 用戶端上顯示為可用的磁碟機。

## 驗證您的 iSCSI 組態

我們已提供指令碼來檢查您的 iSCSI 設定是否已正確設定。指令碼會檢查工作階段計數、節點分佈和多路徑 I/O (MPIO) 狀態等參數。下列任務說明如何安裝和使用指令碼。

### 驗證您的 iSCSI 組態

- 開啟 Windows PowerShell 視窗。
- 使用下列命令下載指令碼。

```
PS C:\> Invoke-WebRequest "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/samples/CheckiSCSI.zip" -OutFile "CheckiSCSI.zip"
```

- 使用下列命令展開 zip 檔案。

```
PS C:\> Expand-Archive -Path ".\CheckiSCSI.zip" -DestinationPath "./"
```

- 使用下列命令執行指令碼。

```
PS C:\> ./CheckiSCSI.ps1
```

- 檢閱輸出以了解組態的目前狀態。下列範例示範成功的 iSCSI 組態。

```
PS C:\> ./CheckiSCSI.ps1
```

```
This script checks the iSCSI configuration on the local instance.
It will provide information about the number of connected sessions, connected file
servers, and MPIO status.
```

```
MPIO is installed on this server.
```

```
MPIO Load Balance Policy is set to Round Robin (RR).
```

```
Initiator: 'iqn.1991-05.com.microsoft:ec2amaz-d2cebnb'
```

```
to Target: 'iqn.1992-08.com.netapp:sn.13266b10e61411ee8bc0c76ad263d613:vs.3'
```

```
has 16 total sessions (16 active, 0 non-active)
```

```
spread across 2 node(s).
```

```
MPIO: Yes
```

## 佈建適用於 Linux 的 NVMe/TCP

FSx for ONTAP 支援透過 TCP (NVMe/TCP) 區塊儲存協定的非揮發性記憶體 Express。使用 NVMe/TCP，您可以使用 ONTAP CLI 佈建命名空間和子系統，然後將命名空間映射至子系統，類似於佈建 LUNs 並映射至 iSCSI 啟動器群組 (igroup) 的方式。NVMe/TCP 通訊協定適用於具有 6 個或更少 [高可用性 \(HA\)](#) 對的第二代檔案系統。

### Note

FSx for ONTAP 檔案系統針對 iSCSI 和 NVMe/TCP 區塊儲存通訊協定使用 SVM 的 iSCSI 端點。

在 Amazon FSx for NetApp ONTAP 上設定 NVMe/TCP 有三個主要步驟，請參閱下列程序：

1. 在 Linux 主機上安裝和設定 NVMe 用戶端。
2. 在檔案系統的 SVM 上設定 NVMe。
  - 建立 NVMe 命名空間。
  - 建立 NVMe 子系統。
  - 將命名空間映射至子系統。
  - 將用戶端 NQN 新增至子系統。
3. 在 Linux 用戶端上掛載 NVMe 裝置。

## 開始之前

開始設定 NVMe/TCP 檔案系統的程序之前，您需要完成下列項目。

- 建立 FSx for ONTAP 檔案系統。如需詳細資訊，請參閱[建立檔案系統](#)。
- 在與檔案系統相同的 VPC 中建立執行 Red Hat Enterprise Linux (RHEL) 9.3 的 EC2 執行個體。這是要設定 NVMe 並使用 NVMe/TCP for Linux 存取檔案資料的 Linux 主機。

除了這些程序的範圍之外，如果主機位於另一個 VPC 中，您可以使用 VPC 對等互連 AWS Transit Gateway，或授予其他 VPCs 存取磁碟區的 iSCSI 端點。如需詳細資訊，請參閱[從部署 VPC 外部存取資料](#)。

- 設定 Linux 主機的 VPC 安全群組，以允許傳入和傳出流量，如中所述[使用 Amazon VPC 的檔案系統存取控制](#)。
- 取得具有您將用來存取 CLI ONTAP fsxadmin 權限 ONTAP 之使用者的登入資料。如需詳細資訊，請參閱[ONTAP 角色和使用者](#)。
- 您將為 NVMe 設定的 Linux 主機，並用來存取 FSx for ONTAP 檔案系統，位於相同的 VPC 和 AWS 帳戶。
- 我們建議 EC2 執行個體與您檔案系統偏好的子網路位於相同的可用區域。

如果您的 EC2 執行個體執行的 Linux AMI 與 RHEL 9.3 不同，這些程序和範例中使用的某些公用程式可能已安裝，而且您可以使用不同的命令來安裝必要的套件。除了安裝套件之外，本節中使用的命令對其他 EC2 Linux AMIs 有效。

### 主題

- [在 Linux 主機上安裝和設定 NVMe](#)
- [在 FSx for ONTAP 檔案系統上設定 NVMe](#)
- [在 Linux 用戶端上掛載 NVMe 裝置](#)

## 在 Linux 主機上安裝和設定 NVMe

### 安裝 NVMe 用戶端

1. 使用 SSH 用戶端連線至 Linux 執行個體。如需詳細資訊，請參閱[使用 SSH 從 Linux 或 macOS 連線至 Linux 執行個體](#)。
2. 使用下列命令安裝 nvme-cli：

```
~$ sudo yum install -y nvme-cli
```

3. 將nvme-tcp模組載入主機：

```
$ sudo modprobe nvme-tcp
```

4. 使用下列命令取得 Linux 主機的 NVMe 合格名稱 (NQN)：

```
$ cat /etc/nvme/hostnqn  
nqn.2014-08.org.nvmexpress:uuid:9ed5b327-b9fc-4cf5-97b3-1b5d986345d1
```

記錄回應以供稍後步驟使用。

## 在 FSx for ONTAP 檔案系統上設定 NVMe

### 在檔案系統上設定 NVMe

連線至您計劃建立 NVMe 裝置之 FSx for ONTAP 檔案系統 (FSx for ONTAP) 上的 NetApp ONTAP CLI。

1. 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。將 *management\_endpoint\_ip* 取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

2. 在您用來存取 NVMe 界面的 SVM 上建立新的磁碟區。

```
::> vol create -vserver fsx -volume nvme_vol1 -aggregate aggr1 -size 1t  
[Job 597] Job succeeded: Successful
```

3. ns\_1 使用 [vserver nvme namespace create](#) NetApp ONTAP CLI 命令建立 NVMe 命名空間。命名空間會映射至啟動器（用戶端），並控制哪些啟動器（用戶端）可存取 NVMe 裝置。

```
::> vspace nvme namespace create -vserver fsx -path /vol/nvme_vol1/ns_1 -size 100g  
-ostype linux  
Created a namespace of size 100GB (107374182400).
```

4. 使用 [vserver nvme subsystem create](#) NetApp ONTAP CLI 命令建立 NVMe 子系統。

```
~$ vserver nvme subsystem create -vserver fsx -subsystem sub_1 -ostype linux
```

5. 將命名空間對應至您剛建立的子系統。

```
::> vserver nvme subsystem map add -vserver fsx -subsystem sub_1 -path /vol/
nvme_vol1/ns_1
```

6. 使用您先前擷取的 NQN，將用戶端新增至子系統。

```
::> vserver nvme subsystem host add -subsystem sub_1 -host-nqn
nqn.2014-08.org.nvmexpress:uuid:ec21b083-1860-d690-1f29-44528e4f4e0e -vserver fsx
```

如果您想要讓映射到此子系統的裝置可供多個主機使用，您可以在逗號分隔清單中指定多個啟動器名稱。如需詳細資訊，請參閱 NetApp ONTAP 文件中的 [vserver nvme 子系統主機新增](#)。

7. 使用 [vserver nvme namespace show](#) 命令確認命名空間存在：

```
::> vserver nvme namespace show -vserver fsx -instance
Vserver Name: fsx
    Namespace Path: /vol/nvme_vol1/ns_1
        Size: 100GB
        Size Used: 90.59GB
        OS Type: linux
        Comment:
        Block Size: 4KB
        State: online
    Space Reservation: false
Space Reservations Honored: false
    Is Read Only: false
    Creation Time: 5/20/2024 17:03:08
    Namespace UUID: c51793c0-8840-4a77-903a-c869186e74e3
    Vdisk ID: 80d42c6f00000000187cca9
    Restore Inaccessible: false
    Inconsistent Filesystem: false
    Inconsistent Blocks: false
    NVFail: false
Node Hosting the Namespace: FsxId062e9bb6e05143fcb-01
    Volume Name: nvme_vol1
    Qtree Name:
    Mapped Subsystem: sub_1
    Subsystem UUID: db526ec7-16ca-11ef-a612-d320bd5b74a9
```

```

Namespace ID: 00000001h
ANA Group ID: 00000001h
Vserver UUID: 656d410a-1460-11ef-a612-d320bd5b74a9
  Vserver ID: 3
  Volume MSID: 2161388655
  Volume DSID: 1029
  Aggregate: aggr1
  Aggregate UUID: cfa8e6ee-145f-11ef-a612-d320bd5b74a9
Namespace Container State: online
  Autodelete Enabled: false
  Application UUID: -
  Application: -
  Has Metadata Provisioned: true

```

1 entries were displayed.

8. 使用 [network interface show -vserver](#) 命令來擷取您已建立 NVMe 裝置之 SVM 的區塊儲存介面地址。

```

::> network interface show -vserver svm_name -data-protocol nvme-tcp

```

|                           | Logical    | Status     | Network          | Current |
|---------------------------|------------|------------|------------------|---------|
|                           | Current Is |            |                  |         |
| Vserver                   | Interface  | Admin/Oper | Address/Mask     | Node    |
|                           | Port Home  |            |                  |         |
| -----                     |            |            |                  |         |
| <i>svm_name</i>           | iscsi_1    | up/up      | 172.31.16.19/20  |         |
| FSxId0123456789abcdef8-01 | e0e        | true       |                  |         |
|                           | iscsi_2    | up/up      | 172.31.26.134/20 |         |
| FSxId0123456789abcdef8-02 | e0e        | true       |                  |         |

2 entries were displayed.

#### Note

iscsi\_1 LIF 用於 iSCSI 和 NVMe/TCP。

在此範例中，iscsi\_1 的 IP 地址為 172.31.16.19，iscsi\_2 為 172.31.26.134。

## 在 Linux 用戶端上掛載 NVMe 裝置

在 Linux 用戶端上安裝 NVMe 裝置的程序包含三個步驟：

1. 探索 NVMe 節點
2. 分割 NVMe 裝置
3. 在用戶端上掛載 NVMe 裝置

這些涵蓋在下列程序中。

### 探索目標 NVMe 節點

1. 在 Linux 用戶端上，使用下列命令來探索目標 NVMe 節點。*iscsi\_1\_IP* 將取代為 iscsi\_1 的 IP 地址，以及 *client\_IP* 用戶端的 IP 地址。

#### Note

iscsi\_1 和 iscsi\_2 LIFs 用於 iSCSI 和 NVMe 儲存。

```
~$ sudo nvme discover -t tcp -w client_IP -a iscsi_1_IP
```

```
Discovery Log Number of Records 4, Generation counter 11
=====Discovery Log Entry 0=====
trtype: tcp
adrfam: ipv4
subtype: current discovery subsystem
treq: not specified
portid: 0
trsvcid: 8009
subnqn: nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:discovery
traddr: 172.31.26.134
eflags: explicit discovery connections, duplicate discovery information
sectype: none
=====Discovery Log Entry 1=====
trtype: tcp
adrfam: ipv4
subtype: current discovery subsystem
treq: not specified
```



```
portid: 1
trsvcid: 8009
subnqn: nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:discovery
traddr: 172.31.16.19
eflags: explicit discovery connections, duplicate discovery information
sectype: none
```

2. (選用) 若要為檔案 NVMe 裝置提供高於 Amazon EC2 單一用戶端最大 5 Gbps (~625 MBps) 的輸送量，請遵循 Linux [執行個體的 Amazon Elastic Compute Cloud 使用者指南中所述的 Amazon EC2 執行個體網路頻寬](#) 程序，以建立其他工作階段。
3. 使用 `iscsi_1` 的 IP 地址 `iscsi_1_IP` 和 的用戶端 IP 地址，以至少 1800 秒的控制器遺失逾時登入目標啟動器 `client_IP`。您的 NVMe 裝置會顯示為可用的磁碟。

```
~$ sudo nvme connect-all -t tcp -w client_IP -a iscsi_1 -l 1800
```

4. 使用下列命令來驗證 NVMe 堆疊是否已識別和合併多個工作階段，並已設定多路徑。Y 如果組態成功，命令會傳回。

```
~$ cat /sys/module/nvme_core/parameters/multipath
Y
```

5. 使用下列命令來確認 NVMe-oF 設定 `model` 已設為 `NetApp ONTAP Controller` 且負載平衡 `iopolicy` 已設為 `round-robin`，以便個別 ONTAP 命名空間在所有可用的路徑上分配 I/O

```
~$ cat /sys/class/nvme-subsystem/nvme-subsys*/model
Amazon Elastic Block Store
NetApp ONTAP Controller
~$ cat /sys/class/nvme-subsystem/nvme-subsys*/iopolicy
numa
round-robin
```

6. 使用下列命令來驗證是否已在主機上建立並正確探索命名空間：

```
~$ sudo nvme list
```

| Node  | Generic Namespace | Usage | SN    | Model Format | FW    |
|-------|-------------------|-------|-------|--------------|-------|
| Rev   |                   |       |       |              |       |
| ----- | -----             | ----- | ----- | -----        | ----- |
| ----- | -----             | ----- | ----- | -----        | ----- |
| ----- | -----             | ----- | ----- | -----        | ----- |

|              |            |                       |                |
|--------------|------------|-----------------------|----------------|
| /dev/nvme0n1 | /dev/ng0n1 | vol105955547c003f0580 | Amazon Elastic |
| Block Store  | 0x1        | 25.77 GB / 25.77 GB   | 512 B + 0 B    |
| 1.0          |            |                       |                |
| /dev/nvme2n1 | /dev/ng2n1 | 1WB12JWY/XLKAAAAAAAC  | NetApp ONTAP   |
| Controller   | 0x1        | 107.37 GB / 107.37 GB | 4 KiB + 0 B    |
| FFFFFFFF     |            |                       |                |

輸出中的新裝置為 /dev/nvme2n1。此命名機制可能會因 Linux 安裝而有所不同。

7. 確認每個路徑的控制器狀態為即時，且具有正確的非對稱命名空間存取 (ANA) 多路徑狀態：

```
~$ nvme list-subsys /dev/nvme2n1
nvme-subsys2 -
  NQN=nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:subsystem.rhel
      hostnqn=nqn.2014-08.org.nvmexpress:uuid:ec2a70bf-3ab2-6cb0-
f997-8730057ceb24
      iopolicy=round-robin
\
+- nvme2 tcp
traddr=172.31.26.134,trsvcid=4420,host_traddr=172.31.25.143,src_addr=172.31.25.143
live non-optimized
+- nvme3 tcp
traddr=172.31.16.19,trsvcid=4420,host_traddr=172.31.25.143,src_addr=172.31.25.143
live optimized
```

在此範例中，NVMe 堆疊已自動探索檔案系統的替代 LIF、iscsi\_2、，以及 172.31.26.134。

8. 確認NetApp外掛程式顯示每個ONTAP命名空間裝置的正確值：

```
~$ sudo nvme netapp ontapdevices -o column
Device          Vserver          Namespace Path
              NSID  UUID                               Size
-----
-----
-----
/dev/nvme2n1    fsx              /vol/nvme_vol1/ns_1
              1      0441c609-3db1-4b0b-aa83-790d0d448ece  107.37GB
```

## 分割裝置

1. 使用下列命令來驗證 Device\_name 的路徑nvme2n1是否存在。

```
~$ ls /dev/mapper/nvme2n1  
/dev/nvme2n1
```

2. 使用 分割磁碟fdisk。您將輸入互動式提示。依顯示的順序輸入選項。您可以使用小於最後一個區段的值 (20971519在此範例中為 ) 來建立多個分割區。

 Note

Last sector 值會根據 NVMe 裝置的大小 ( 在此範例中為 100 GiB) 而有所不同。

```
~$ sudo fdisk /dev/mapper/nvme2n1
```

fdisk 互動式提示隨即啟動。

```
Welcome to fdisk (util-linux 2.37.4).  
Changes will remain in memory only, until you decide to write them.  
Be careful before using the write command.  
  
Device does not contain a recognized partition table.  
Created a new DOS disklabel with disk identifier 0x66595cb0.  
  
Command (m for help): n  
Partition type  
   p primary (0 primary, 0 extended, 4 free)  
   e extended (container for logical partitions)  
Select (default p): p  
Partition number (1-4, default 1): 1  
First sector (256-26214399, default 256):  
Last sector, +sectors or +size{K,M,G,T,P} (256-26214399, default  
26214399): 20971519  
  
Created a new partition 1 of type 'Linux' and of size 100 GiB.  
Command (m for help): w  
The partition table has been altered.  
Calling ioctl() to re-read partition table.  
Syncing disks.
```

輸入 後w，新的分割區/dev/nvme2n1就會變成可用。*partition\_name* 的格式為 *<device\_name><partition\_number>*。1 在上一個步驟的 fdisk命令中用作分割區編號。

### 3. 使用 `/dev/nvme2n1` 做為路徑來建立檔案系統。

```
~$ sudo mkfs.ext4 /dev/nvme2n1
```

系統會以下列輸出回應：

```
mke2fs 1.46.5 (30-Dec-2021)
Found a dos partition table in /dev/nvme2n1
Proceed anyway? (y,N) y
Creating filesystem with 26214400 4k blocks and 6553600 inodes
Filesystem UUID: 372fb2fd-ae0e-4e74-ac06-3eb3eabd55fb
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000, 7962624, 11239424, 20480000, 23887872

Allocating group tables: done
Writing inode tables: done
Creating journal (131072 blocks): done
Writing superblocks and filesystem accounting information: done
```

### 在 Linux 用戶端上掛載 NVMe 裝置

#### 1. 在 Linux 執行個體上建立 `directory_path` 做為檔案系統的掛載點。

```
~$ sudo mkdir /directory_path/mount_point
```

#### 2. 使用以下命令掛載檔案系統。

```
~$ sudo mount -t ext4 /dev/nvme2n1 /directory_path/mount_point
```

#### 3. (選用) 如果您想要為特定使用者提供掛載目錄的所有權，請將 `username` 為擁有者的使用者名稱。

```
~$ sudo chown username:username /directory_path/mount_point
```

#### 4. (選用) 確認您可以從檔案系統讀取和寫入資料。

```
~$ echo "Hello world!" > /directory_path/mount_point/HelloWorld.txt
~$ cat directory_path/HelloWorld.txt
Hello world!
```

您已成功在 Linux 用戶端上建立並掛載 NVMe 裝置。

## 佈建適用於 Windows 的 NVMe/TCP

FSx for ONTAP 支援 Windows 透過 TCP (NVMe/TCP) 區塊儲存協定的非揮發性 Memory Express。透過 NVMe/TCP，您可以使用 ONTAP CLI 佈建命名空間和子系統，然後將命名空間映射至子系統，類似於佈建 LUNs 並映射至 iSCSI 啟動器群組 (igroup) 的方式。NVMe/TCP 通訊協定適用於具有 6 個或更少 [高可用性 \(HA\) 對的第二代檔案系統](#)。

若要在 Windows 主機上佈建 NVMe/TCP，您需要從您選擇的廠商下載啟動器，並遵循其安裝和佈建的指示。

## 使用其他服務 AWS 存取資料

除了 Amazon EC2 之外，您還可以 AWS 搭配磁碟區使用其他服務來存取您的資料。

### 主題

- [將 Amazon WorkSpaces 與 FSx for ONTAP 搭配使用](#)
- [將 Amazon Elastic Container Service 與 FSx for ONTAP 搭配使用](#)
- [搭配 FSx for ONTAP 使用 Amazon Elastic VMware Service](#)
- [使用 VMware Cloud 搭配 FSx for ONTAP](#)

## 將 Amazon WorkSpaces 與 FSx for ONTAP 搭配使用

FSx for ONTAP 可與 Amazon WorkSpaces 搭配使用，以提供共用網路連接儲存 (NAS) 或存放 Amazon WorkSpaces 帳戶的漫遊設定檔。連線至與 WorkSpaces 執行個體的 SMB 檔案共用後，使用者可以在檔案共用上建立和編輯檔案。

下列程序說明如何使用 Amazon FSx 搭配 Amazon WorkSpaces，以提供漫遊設定檔和主資料夾存取一致的體驗，並為 Windows 和 Linux WorkSpaces 使用者提供共用團隊資料夾。如果您是初次使用 Amazon WorkSpaces，您可以使用 Amazon WorkSpaces 管理指南中的 [WorkSpaces Quick Setup 入門](#) 中的說明來建立第一個 Amazon WorkSpaces 環境。Amazon WorkSpaces

### 主題

- [提供漫遊設定檔支援](#)

- [提供共用資料夾以存取常見檔案](#)

## 提供漫遊設定檔支援

您可以使用 Amazon FSx 為組織中的使用者提供漫遊設定檔支援。使用者將擁有僅存取其漫遊設定檔的許可。資料夾將使用 Active Directory 群組政策自動連線。透過漫遊設定檔，使用者的資料和桌面設定會在登出 Amazon FSx 檔案共用時儲存，以便在不同的 WorkSpaces 執行個體之間共用文件和設定，並使用 Amazon FSx 每日自動備份自動備份進行備份。

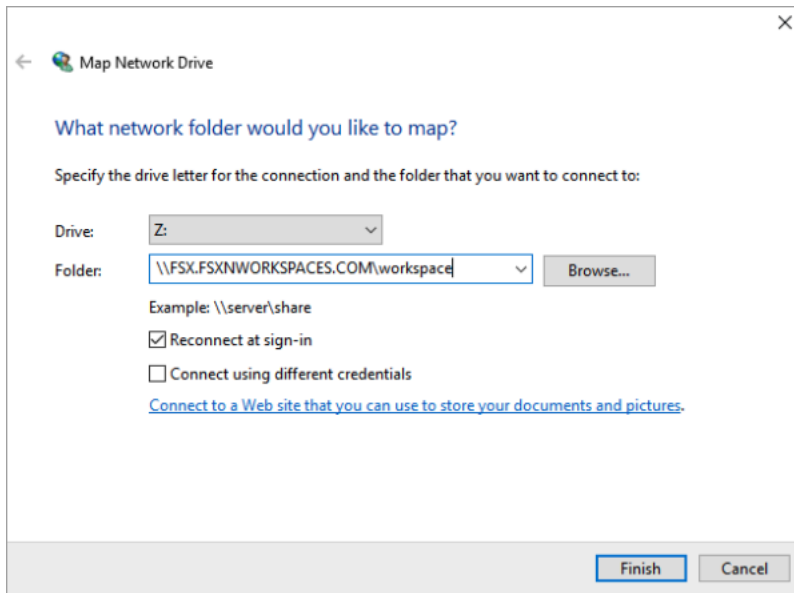
步驟 1：使用 Amazon FSx 為網域使用者建立設定檔資料夾位置

1. 使用 Amazon FSx 主控台建立 FSx for ONTAP 檔案系統。如需詳細資訊，請參閱[建立檔案系統 \(主控台\)](#)。

### Important

每個 FSx for ONTAP 檔案系統都有一個端點 IP 地址範圍，其中會建立與檔案系統相關聯的端點。對於多可用區域檔案系統，FSx for ONTAP 選擇預設未使用的 IP 地址範圍，範圍從 198.19.0.0/16 作為端點 IP 地址範圍。WorkSpaces 也會使用此 IP 地址範圍來管理流量範圍，如 Amazon [WorkSpaces 管理指南中 WorkSpaces 的 IP 地址和連接埠需求](#)所述。Amazon WorkSpaces 因此，若要從 WorkSpaces 存取適用於 ONTAP 檔案系統的多可用區域 FSx，您必須選取與 198.19.0.0/16 不重疊的端點 IP 地址範圍。

2. 如果您沒有加入 Active Directory 的儲存虛擬機器 (SVM)，請立即建立一個。例如，您可以佈建名為 `fsx` 的 SVM，並將安全樣式設定為 NTFS。如需詳細資訊，請參閱[建立儲存虛擬機器 \(主控台\)](#)。
3. 為您的 SVM 建立磁碟區。例如，您可以建立名為 `fsx-vol` 的磁碟區，繼承 SVM 根磁碟區的安全樣式。如需詳細資訊，請參閱[建立 FlexVol 磁碟區 \(主控台\)](#)。
4. 在磁碟區上建立 SMB 共享。例如，您可以在名為 `workspace` 的磁碟區上建立名為 `fsx-vol` 的共用，並在其中建立名為 `profiles` 的資料夾。如需詳細資訊，請參閱[管理 SMB 共用](#)。
5. 從執行 Windows Server 的 Amazon EC2 執行個體或從 WorkSpace 存取您的 Amazon FSx SVM。WorkSpace 如需詳細資訊，請參閱[存取 FSx for ONTAP 資料](#)。
6. 您可以將共用映射至 Windows WorkSpaces 執行個體 `Z:\` 上的：



## 步驟 2：將 FSx for ONTAP 檔案共用連結至使用者帳戶

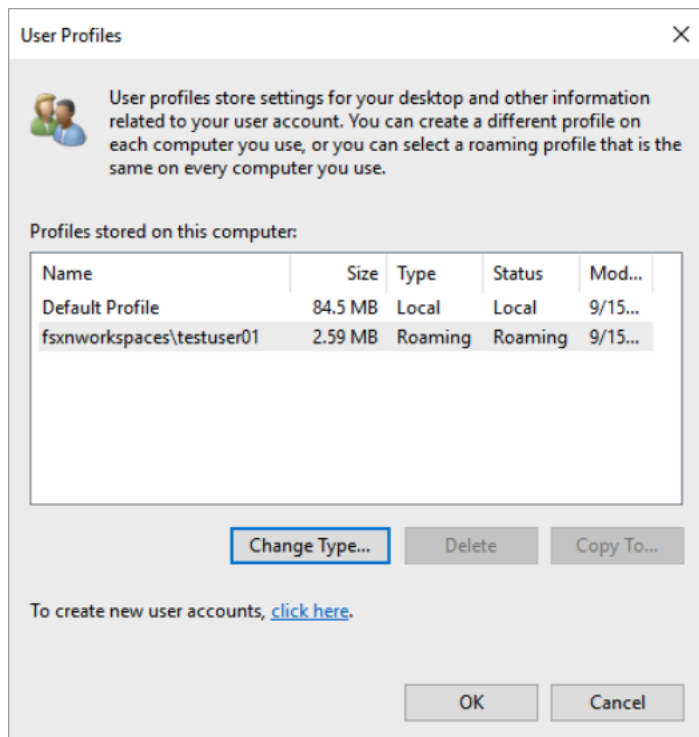
1. 在測試使用者的 WorkSpace 上，選擇 Windows > 系統 > 進階系統設定。
2. 在系統屬性中，選取進階索引標籤，然後按下使用者設定檔區段中的設定按鈕。登入的使用者會有的設定檔類型 Local。
3. 從 WorkSpace 登出測試使用者。
4. 將測試使用者設定為在您的 Amazon FSx 檔案系統上具有漫遊設定檔。在您的管理員 WorkSpaces 中，開啟 PowerShell 主控台，並使用類似下列範例的命令（使用您先前在步驟 1 中建立的 profiles 資料夾）：

```
Set-ADUser username -ProfilePath \\filesystem-dns-name\sharename\foldername\username
```

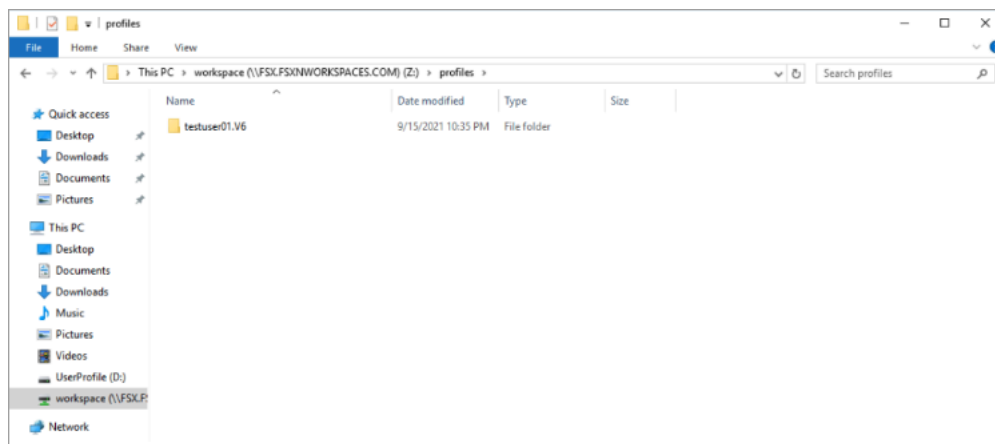
例如：

```
Set-ADUser testuser01 -ProfilePath \\fsx.fsxworkspaces.com\workspace\profiles\testuser01
```

5. 登入測試使用者 WorkSpace。
6. 在系統屬性中，選取進階索引標籤，然後按下使用者設定檔區段中的設定按鈕。登入的使用者會有的設定檔類型 Roaming。

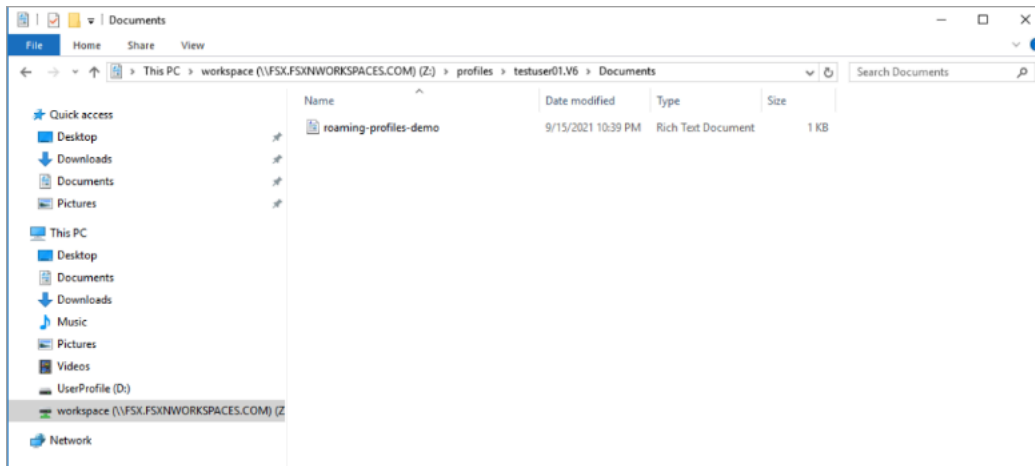


7. 瀏覽 FSx for ONTAP 共用資料夾。在 profiles 資料夾中，您會看到使用者的資料夾。



8. 在測試使用者的Documents資料夾中建立文件
9. 從其 WorkSpace 登出測試使用者。
10. 如果您以測試使用者身分重新登入並瀏覽至其設定檔存放區，您將會看到您建立的文件。



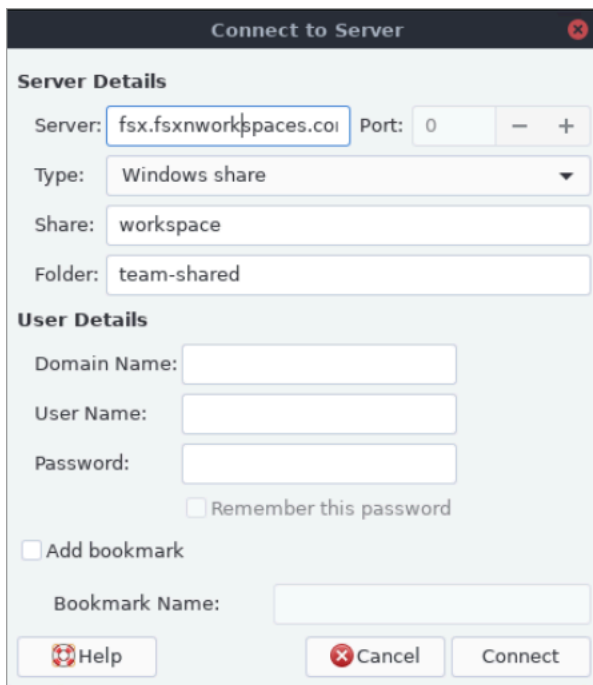


## 提供共用資料夾以存取常見檔案

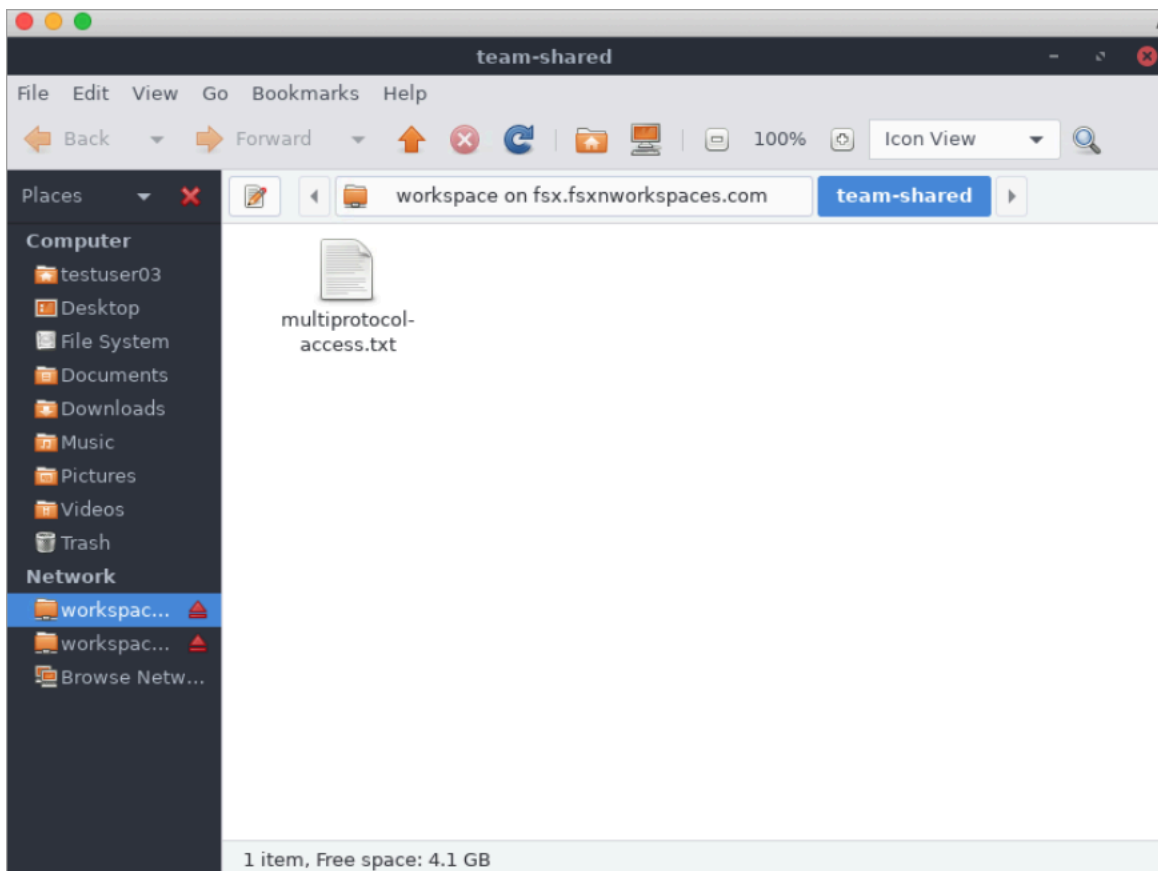
您可以使用 Amazon FSx 為組織中的使用者提供共用資料夾。共用資料夾可用來存放使用者社群使用的檔案，例如示範檔案、程式碼範例和所有使用者所需的指示手冊。一般而言，您擁有對應至共用資料夾的磁碟機；但由於對應磁碟機使用字母，因此您可以擁有的共用數量有限制。此程序會建立 Amazon FSx 共用資料夾，無需磁碟機代號即可使用，讓您更靈活地將共用指派給團隊。

從 Linux 和 Windows WorkSpaces 掛載跨平台存取的共用資料夾

1. 從任務列中，選擇位置 > 連線至伺服器。
  - a. 針對伺服器，輸入 *file-system-dns-name*。
  - b. 將類型設定為 Windows share。
  - c. 將共用設定為 SMB 共用的名稱，例如 workspace。
  - d. 您可以將資料夾保留為 /，或將其設定為資料夾，例如名為 的資料夾team-shared。
  - e. 對於 Linux WorkSpace，如果您的 Linux WorkSpace 與 Amazon FSx 共用位於相同的網域中，則不需要輸入使用者詳細資訊。
  - f. 選擇連線。



2. 建立連線後，您可以在名為 `team-shared` 的 SMB 共用中看到共用資料夾 (在此範例中命名為 `workspace`)。



## 將 Amazon Elastic Container Service 與 FSx for ONTAP 搭配使用

您可以從 Amazon EC2 Linux 或 Windows 執行個體上的 Amazon Elastic Container Service (Amazon ECS) Docker 容器存取 Amazon EC2 FSx for NetApp ONTAP 檔案系統。

### 在 Amazon ECS Linux 容器上掛載

1. 使用 Linux 容器的 EC2 Linux + 網路叢集範本建立 ECS 叢集。如需詳細資訊，請參閱《Amazon Elastic Container Service 開發人員指南》中的[建立叢集](#)。
2. 在 EC2 執行個體上建立用於掛載 SVM 磁碟區的目錄，如下所示：

```
sudo mkdir /fsxontap
```

3. 在執行個體啟動期間使用使用者資料指令碼，或執行下列命令，在 Linux EC2 執行個體上掛載 FSx for ONTAP 磁碟區：

```
sudo mount -t nfs svm-ip-address:/vol1 /fsxontap
```

4. 使用以下命令掛載磁碟區：

```
sudo mount -t nfs -o nfsvers=NFS_version svm-dns-name:/volume-junction-path /  
fsxontap
```

下列範例使用範例值。

```
sudo mount -t nfs -o nfsvers=4.1  
svm-01234567890abcdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /  
fsxontap
```

您也可以使用 SVM 的 IP 地址，而不是其 DNS 名稱。

```
sudo mount -t nfs -o nfsvers=4.1 198.51.100.1:/vol1 /fsxontap
```

5. 建立 Amazon ECS 任務定義時，請在 JSON `mountPoints` 容器定義中新增下列 `volumes` 和 容器屬性。將 `sourcePath` 取代為 FSx for ONTAP 檔案系統中的掛載點和目錄。

```
{  
  "volumes": [  
    {  
      "name": "ontap-volume",
```

```

        "host": {
            "sourcePath": "mountpoint"
        }
    ],
    "mountPoints": [
        {
            "containerPath": "containermountpoint",
            "sourceVolume": "ontap-volume"
        }
    ],
    .
    .
    .
}

```

## 在 Amazon ECS Windows 容器上掛載

1. 使用 Windows 容器的 EC2 Windows + 網路叢集範本建立 ECS 叢集。如需詳細資訊，請參閱《Amazon Elastic Container Service 開發人員指南》中的[建立叢集](#)。
2. 將加入網域的 Windows EC2 執行個體新增至 ECS Windows 叢集，並對應 SMB 共用。

啟動已加入 Active Directory 網域的 ECS 最佳化 Windows EC2 執行個體，並執行下列命令來初始化 ECS 代理程式。

```
PS C:\Users\user> Initialize-ECSAgent -Cluster windows-fsx-cluster -
EnableTaskIAMRole
```

您也可以將指令碼中的資訊傳遞至使用者資料文字欄位，如下所示。

```
<powershell>
Initialize-ECSAgent -Cluster windows-fsx-cluster -EnableTaskIAMRole
</powershell>
```

3. 在 EC2 執行個體上建立 SMB 全域映射，讓您可以將 SMB 共用映射至磁碟機。取代 FSx 檔案系統低於 netbios 或 DNS 名稱的值並共用名稱。掛載在 Linux EC2 執行個體上的 NFS 磁碟區 vol1 在 FSx 檔案系統上設定為 CIFS 共享 fsxontap。

```
vserver cifs share show -vserver svm08 -share-name fsxontap
```

```

Vserver: svm08
Share: fsxontap
CIFS Server NetBIOS Name: FSXONTAPDEMO
Path: /vol1
Share Properties: oplocks
                  browsable
                  changenotify
                  show-previous-versions
Symlink Properties: symlinks
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: vol1
Offline Files: manual
Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
UNIX Group for File Create: -

```

4. 使用下列命令在 EC2 執行個體上建立 SMB 全域映射：

```
New-SmbGlobalMapping -RemotePath \\fsxontapdemo.fsxontap.com\fsxontap -LocalPath Z:
```

5. 建立 Amazon ECS 任務定義時，請在 JSON mountPoints 容器定義中新增下列 volumes 和 容器屬性。將 取代sourcePath為 FSx for ONTAP 檔案系統中的掛載點和目錄。

```

{
  "volumes": [
    {
      "name": "ontap-volume",
      "host": {
        "sourcePath": "mountpoint"
      }
    }
  ],
  "mountPoints": [
    {
      "containerPath": "containermountpoint",
      "sourceVolume": "ontap-volume"
    }
  ],

```

```
.  
.   
.   
}
```

## 搭配 FSx for ONTAP 使用 Amazon Elastic VMware Service

您可以使用 FSx for ONTAP 做為 Amazon Elastic VMware Service (Amazon EVS) 軟體定義資料中心 (SDDCs) 的外部資料存放區。如需詳細資訊，請參閱[使用 Amazon FSx for NetApp ONTAP 執行高性能工作負載](#)。如需詳細說明，請參閱將 [Amazon FSx for NetApp ONTAP 設定為 NFS 資料存放區](#)，以及將 [Amazon FSx for NetApp ONTAP 設定為 iSCSI 資料存放區](#)。

## 使用 VMware Cloud 搭配 FSx for ONTAP

您可以使用 FSx for ONTAP 作為 VMware Cloud on AWS Software-Defined Data Centers (SDDCs) 的外部資料存放區。如需詳細資訊，請參閱使用 [Amazon FSx for NetApp ONTAP 部署指南](#)，將 [Amazon FSx for NetApp ONTAP 設定為外部儲存和 VMware Cloud AWS FSx NetApp on](#)。

# 可用性、耐用性和部署選項

Amazon FSx for NetApp ONTAP 使用單一可用區和多可用區部署類型。您可以從四個選項中選擇：單一可用區 1、單一可用區 2、多可用區 1 和多可用區 2。本主題說明每種部署類型的可用性和持久性功能，協助您選擇適合您工作負載的部署類型。如需服務可用性 SLA（服務層級協議）的相關資訊，請參閱 [Amazon FSx 服務層級協議](#)。

## 主題

- [選擇檔案系統部署類型](#)
- [選擇檔案系統產生](#)
- [FSx for ONTAP 的容錯移轉程序](#)
- [網路資源](#)

## 選擇檔案系統部署類型

單一可用區和多可用區檔案系統部署類型的可用性和持久性功能，如下列各節所述。

### 單一可用區部署類型

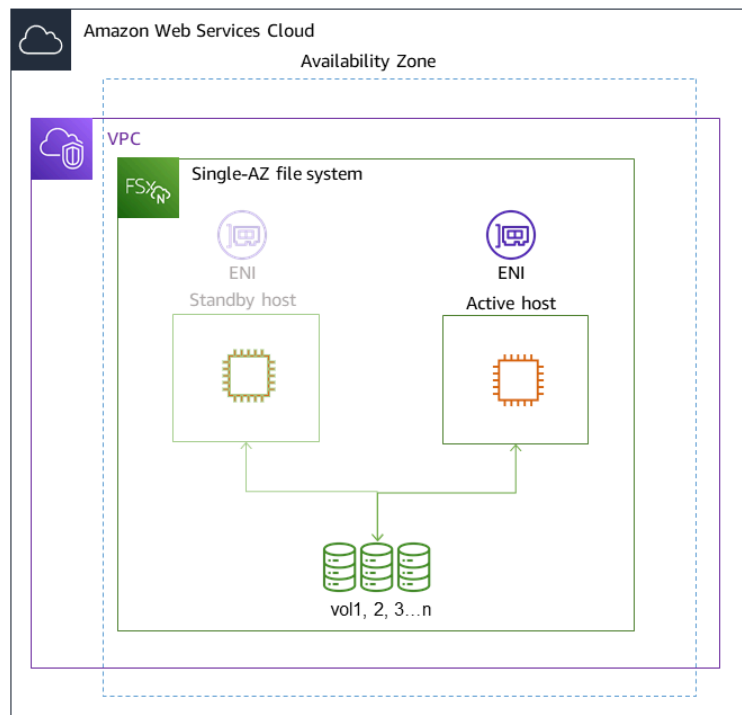
您可以在單一可用區檔案系統的單一可用區 1 和單一可用區 2 之間進行選擇。Single-AZ 1 是具有一個高可用性 (HA) 對的第一代檔案系統，而 Single-AZ 2 是具有 1–12 個 HA 對的第二代檔案系統。如需詳細資訊，請參閱[選擇檔案系統產生](#)。

當您建立單一可用區檔案系統時，Amazon FSx 會自動在作用中待命組態中佈建一到十二對檔案伺服器，其中每對中的作用中和待命檔案伺服器位於中單一可用區域內的個別故障網域。AWS 區域在計劃的檔案系統維護或任何作用中檔案伺服器的計劃外服務中斷期間，Amazon FSx 會自動獨立失敗，超過該高可用性 (HA) 對待命檔案伺服器，通常在幾秒鐘內。在容錯移轉期間，您可以繼續存取資料，而無需手動介入。

為了確保高可用性，Amazon FSx 會持續監控硬體故障，並在發生故障時自動取代基礎設施元件。為了實現高耐用性，Amazon FSx 會自動複寫可用區域內的資料，以防止其元件故障。此外，您可以選擇設定檔案系統資料的自動每日備份。這些備份存放在多個可用區域，為所有備份資料提供多可用區域彈性。

單一可用區檔案系統是專為不需要多可用區檔案系統資料彈性模型的使用案例而設計。它們為開發和測試環境等使用案例提供成本最佳化解決方案，或僅透過在單一可用區域中複寫資料 AWS 區域，來儲存已存放在內部部署或其他中的資料的次要複本。

下圖說明適用於 ONTAP 單一可用區第一代檔案系統的 FSx 架構。



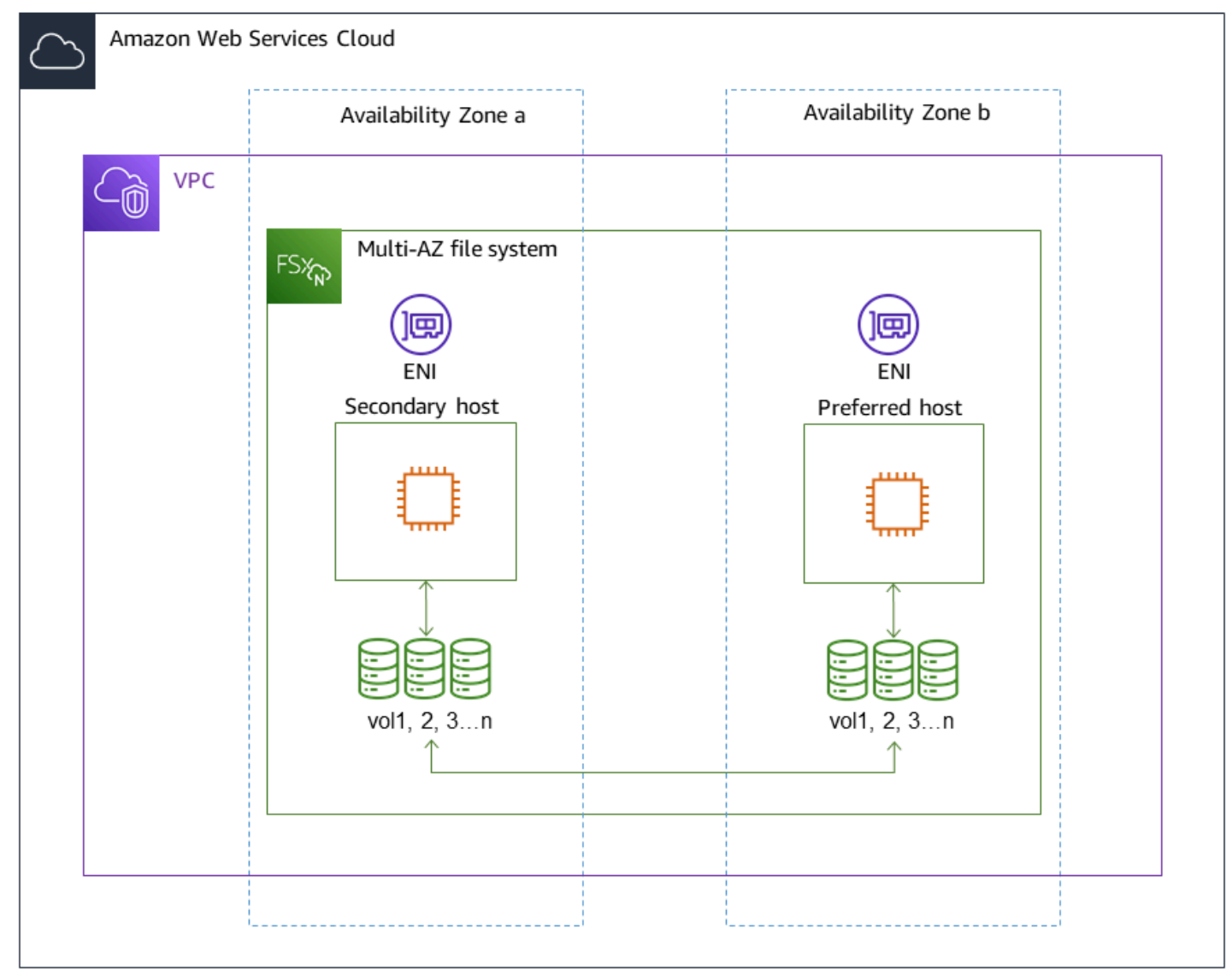
## 異地同步備份部署類型

您可以在異地同步備份檔案系統的異地同步備份 1 和異地同步備份 2 之間進行選擇。Multi-AZ 1 是第一代檔案系統，而 Multi-AZ 2 是第二代檔案系統。這兩個選項都有一個 HA 對。如需詳細資訊，請參閱[選擇檔案系統產生](#)。

多可用區域檔案系統支援單一可用區域檔案系統的所有可用性和耐用性功能。此外，它們旨在提供資料的持續可用性，即使可用區域無法使用。異地同步備份部署具有單一 HA 對檔案伺服器，待命檔案伺服器會部署在相同作用中檔案伺服器的不同可用區域中 AWS 區域。寫入檔案系統的任何變更都會在可用區域之間同步複寫至待命。

多可用區域檔案系統是專為使用案例所設計，例如需要高可用性才能共用 ONTAP 檔案資料的重大業務生產工作負載，以及需要具有跨可用區域內建複寫的儲存體。下圖說明適用於 ONTAP 多可用區域第一代檔案系統的 FSx 架構。





## 選擇檔案系統產生

下表說明適用於 ONTAP 檔案系統的第一代和第二代單一可用區域和多可用區域 FSx 之間的差異。

FSx for ONTAP 檔案系統世代

| 維度   | 第一代         | 第二代（單一 HA 對） | 第二代（多對）     |
|------|-------------|--------------|-------------|
| 部署類型 | SINGLE_AZ_1 | SINGLE_AZ_2  | SINGLE_AZ_2 |
|      | MULTI_AZ_1  | MULTI_AZ_2   |             |

| 維度       | 第一代                                                                               | 第二代 ( 單一 HA 對 )                                                     | 第二代 ( 多對 )                                                                     |
|----------|-----------------------------------------------------------------------------------|---------------------------------------------------------------------|--------------------------------------------------------------------------------|
| HA 對     | 1 個 HA 對                                                                          |                                                                     | 1–12 個 HA 對                                                                    |
| SSD 儲存體  | 下限：1 TiB<br>上限：192 TiB                                                            | 下限：1 TiB<br>上限：512 TiB                                              | 下限：1 TiB<br>( 每個 HA 對 )<br>上限：1 PiB ( 總計 )                                     |
| SSD IOPS | 下限：3 個<br>SSD IOPS/GIB<br>上限：160,000                                              | 下限：3 個<br>SSD IOPS/GIB<br>上限：200,000                                | 下限：3 個<br>SSD IOPS/GIB<br>上限：2,400,000 ( 每個 HA 對<br>200,000 個 )                |
| 輸送量容量    | 128 MBps ; 256<br>MBps ; 512 MBps ;<br>1,024 MBps ;<br>2,048 MBps ;<br>4,096 MBps | 384 MBps ; 768<br>MBps ; 1,536<br>MBps ; 3,072<br>MBps ; 6,144 MBps | 1,536 MBps ( 每個 HA 對 ) ; 3,072<br>MBps ( 每個 HA 對 ) ; 6,144 MBps<br>( 每個 HA 對 ) |

#### Note

您無法在建立後變更檔案系統的部署類型。如果您想要變更部署類型 ( 例如，從單一可用區 1 移至單一可用區 2 )，您可以備份資料並將其還原至新的檔案系統。您也可以使用 NetApp SnapMirror、AWS DataSync 或第三方資料複製工具來遷移資料。如需詳細資訊，請參閱 [使用 NetApp SnapMirror 遷移至 FSx for ONTAP](#) 和 [使用 遷移至 FSx for ONTAP AWS DataSync](#)。

## FSx for ONTAP 的容錯移轉程序

如果發生下列任一情況，單一可用區和多可用區檔案系統會自動從偏好的或作用中檔案伺服器，將指定的 HA 對容錯移轉至待命檔案伺服器：

- 偏好的或作用中檔案伺服器無法使用
- 檔案系統的輸送量已變更

- 偏好的或作用中檔案伺服器經過規劃的維護
- 發生可用區域中斷（僅限多可用區域檔案系統）

#### Note

對於具有多個 HA 對的第二代檔案系統，每個 HA 對的容錯移轉行為都是獨立的。如果一個 HA 對的偏好檔案伺服器無法使用，則只有該 HA 對會容錯移轉到其待命檔案伺服器。

當從一個檔案伺服器容錯移轉到另一個檔案伺服器時，新的作用中檔案伺服器會自動開始向該 HA 對提供所有檔案系統的讀取和寫入請求。對於多可用區域檔案系統，當偏好的檔案伺服器完全復原且可供使用時，Amazon FSx 會自動失敗回它的狀態，而容錯回復通常在 60 秒內完成。對於單一可用區和多可用區檔案系統，容錯移轉通常會在偵測作用中檔案伺服器上的故障到將待命檔案伺服器提升為作用中狀態的 60 秒內完成。由於用戶端用於透過 NFS 或 SMB 存取資料的端點 IP 地址保持不變，因此容錯移轉對 Linux、Windows 和 macOS 應用程式是透明的，其無需手動介入即可恢復檔案系統操作。

若要確保容錯移轉對連接到適用於 ONTAP 單一可用區和多可用區檔案系統的 FSx 的用戶端透明，請參閱 [從內存取資料 AWS 雲端](#)。

## 在檔案系統上測試容錯移轉

您可以修改檔案系統的輸送量容量，以測試容錯移轉。當您修改檔案系統的輸送量容量時，Amazon FSx 會依序將檔案系統的檔案伺服器移出。檔案系統會自動容錯移轉至次要伺服器，而 Amazon FSx 會先取代偏好的檔案伺服器。更新後，檔案系統會自動失敗回新的主要伺服器，Amazon FSx 會取代次要檔案伺服器。

您可以在 Amazon FSx 主控台、CLI 和 API 中監控輸送量容量更新請求的進度。如需修改檔案系統的輸送量容量和監控請求進度的詳細資訊，請參閱 [管理輸送量容量](#)。

## 網路資源

本節說明單一可用區和多可用區檔案系統使用的網路資源。

### 子網路

當您建立單一可用區檔案系統時，您可以為檔案系統指定單一子網路。您選擇的子網路會定義建立檔案系統的可用區域。當您建立多可用區域檔案系統時，您可以指定兩個子網路，一個用於偏好的檔案伺

伺服器，另一個用於待命檔案伺服器。您選擇的兩個子網路必須位於相同區域內的不同可用區域 AWS 區域。如需 Amazon VPC 的詳細資訊，請參閱《Amazon Amazon Virtual Private Cloud [什麼是 Amazon VPC ?](#)》。

#### Note

無論您指定的子網路為何，您都可以從檔案系統 VPC 內的任何子網路存取檔案系統。

## 檔案系統彈性網路介面

對於單一可用區檔案系統，Amazon FSx 會在您與您的檔案系統建立關聯的子網路中佈建兩個[彈性網路介面](#) (ENI)。對於多可用區域檔案系統，Amazon FSx 也會佈建兩個 ENIs，每個子網路中有一個與檔案系統建立關聯的子網路。用戶端會使用彈性網路介面與您的 Amazon FSx 檔案系統通訊。網路介面被視為在 Amazon FSx 的服務範圍內，儘管是您帳戶 VPC 的一部分。多可用區域檔案系統使用浮動國際網路通訊協定 (IP) 地址，以便在容錯移轉事件期間，連線的用戶端在偏好的和待命檔案伺服器之間無縫轉移。

#### Warning

- 您不得修改或刪除與檔案系統相關聯的彈性網路介面。修改或刪除網路介面可能會導致 VPC 和檔案系統之間的連線永久中斷。
- 與您的檔案系統相關聯的彈性網路介面會自動建立路由，並新增至您的預設 VPC 和子網路路由表。修改或刪除這些路由可能會導致檔案系統用戶端的連線暫時或永久中斷。

下表摘要說明每個 FSx for ONTAP 檔案系統部署類型的子網路、彈性網路介面和 IP 地址資源：

|                  | 第一代單一可用區          | 第二代單一可用區         | Multi-AZ          |
|------------------|-------------------|------------------|-------------------|
| 子網路數量            | 1                 | 1                | 2                 |
| 彈性網路介面的數量        | 2                 | 每個 HA 對 2 個      | 2                 |
| 每個 ENI 的 IP 地址數量 | 1 + 檔案系統中 SVMs 數量 | HA 對計數 + HA 對計數乘 | 1 + 檔案系統中 SVMs 數量 |

|            | 第一代單一可用區      | 第二代單一可用區 | Multi-AZ         |
|------------|---------------|----------|------------------|
|            | 以檔案系統中SVMs 數量 |          |                  |
| VPC 路由表路由數 | N/A           | N/A      | 1 + 檔案系統中SVMs 數量 |

建立檔案系統或 SVM 後，其 IP 地址在刪除檔案系統之前不會變更。

**⚠ Important**

Amazon FSx 不支援從 存取檔案系統，或將檔案系統公開至公有網際網路。Amazon FSx 會自動分離任何彈性 IP 地址，這是可從網際網路連線的公有 IP 地址，該地址會連接到檔案系統的彈性網路介面。

# Amazon FSx for NetApp ONTAP 效能

以下是 Amazon FSx for NetApp ONTAP 檔案系統效能的概觀，討論可用的效能和輸送量選項，以及實用的效能秘訣。

## 主題

- [如何測量 FSx for ONTAP 檔案系統的效能](#)
- [效能詳細資訊](#)
- [部署類型對效能的影響](#)
- [儲存容量對效能的影響](#)
- [輸送量容量對效能的影響](#)
- [範例：儲存容量和輸送量容量](#)

## 如何測量 FSx for ONTAP 檔案系統的效能

檔案系統效能是以其延遲、輸送量和每秒 I/O 操作 (IOPS) 來衡量。

### Latency (延遲)

Amazon FSx for NetApp ONTAP 提供具有固態硬碟 (SSD) 儲存的次毫秒檔案操作延遲，以及容量集區儲存的數十毫秒延遲。除此之外，Amazon FSx 在每個檔案伺服器上都有兩層讀取快取：NVMe（非揮發性記憶體表達式）磁碟機和記憶體內，可在您存取最常讀取的資料時提供更低的延遲。

### 輸送量和 IOPS

每個 Amazon FSx 檔案系統提供高達數十 GBps 的輸送量和數百萬個 IOPS。工作負載可在檔案系統上驅動的特定輸送量和 IOPS，取決於檔案系統的總輸送量容量和儲存容量組態，以及工作負載的性質，包括作用中工作集的大小。

### SMB 多通道和 NFS nconnect 支援

使用 Amazon FSx，您可以設定 SMB 多通道，在單一 SMB 工作階段中提供 ONTAP 和用戶端之間的多個連線。SMB 多通道同時在用戶端和伺服器之間使用多個網路連線，以彙總網路頻寬以實現最大使用率。如需使用 NetApp ONTAP CLI 設定 SMB 多頻道的相關資訊，請參閱[設定 SMB 多頻道以取得效能和備援](#)。

NFS 用戶端可以使用 `nconnect` 掛載選項，讓多個 TCP 連線（最多 16 個）與單一 NFS 掛載相關聯。這類 NFS 用戶端會以循環方式將檔案操作多工至多個 TCP 連線，進而從可用的網路頻寬取得更高的輸送量。NFSv3 和 NFSv4.1+ 支援 `nconnect` [Amazon EC2 執行個體網路頻寬](#) 說明每個網路流量頻寬限制的完整雙工 5 Gbps。您可以使用具有 `nconnect` 或 SMB 多通道的多個網路流程來克服此限制。請參閱 NFS 用戶端文件，確認用戶端版本 `nconnect` 中是否支援。如需 NetApp ONTAP 支援的詳細資訊 `nconnect`，請參閱 [ONTAP NFSv4.1 的支援](#)。

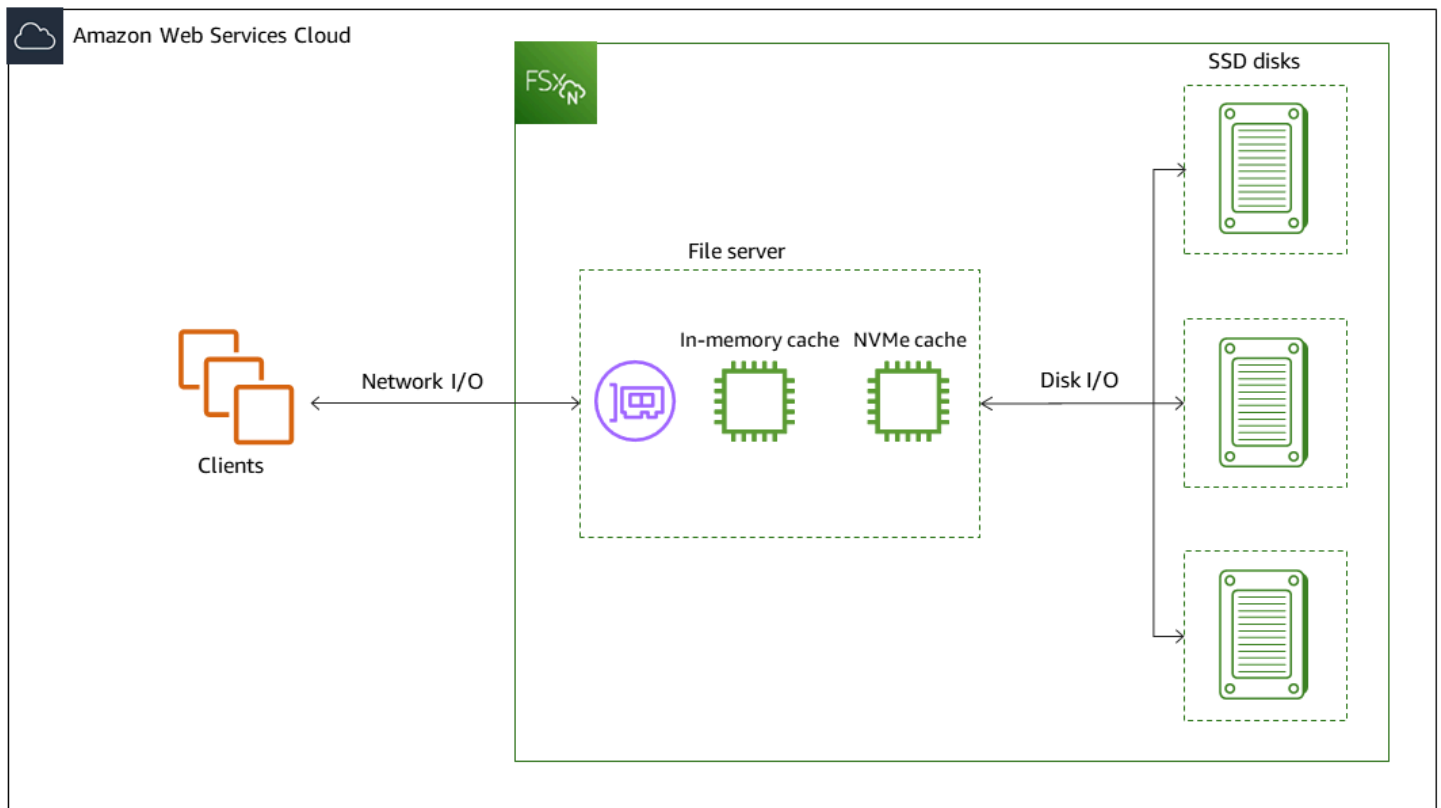
## 巨型訊框

為了達到最大讀取或寫入輸送量，建議您在 Amazon FSx 檔案系統的資料路徑中的所有網路介面上啟用巨型訊框，包括用戶端 EC2 執行個體。FSx for ONTAP 檔案系統上網路介面的預設最大傳輸單位 (MTU) 設定為 9,001 位元組。

## 效能詳細資訊

若要詳細了解 Amazon FSx for NetApp ONTAP 效能模型，您可以檢查 Amazon FSx 檔案系統的架構元件。您的用戶端運算執行個體，無論是存在於內部 AWS 部署還是內部部署，都可以透過一或多個彈性網路界面 (ENI) 存取您的檔案系統。這些網路介面位於您與您的檔案系統建立關聯的 Amazon VPC 中。每個檔案系統 ENI 後方都有一個 NetApp ONTAP 檔案伺服器，透過網路將資料提供給存取檔案系統的用戶端。Amazon FSx 在每個檔案伺服器上提供快速記憶體內快取和 NVMe 快取，以增強最常存取資料的效能。連接到每個檔案伺服器是託管檔案系統資料的 SSD 磁碟。

這些元件如下圖所示。



與這些架構元件對應的網路介面、記憶體內快取、NVMe 快取和儲存磁碟區是 Amazon FSx for NetApp ONTAP 檔案系統的主要效能特性，可決定整體輸送量和 IOPS 效能。

- 網路 I/O 效能：用戶端與檔案伺服器之間的請求輸送量/IOPS（彙總）
- 檔案伺服器上的記憶體內和 NVMe 快取大小：可用於快取的作用中工作集大小
- 磁碟 I/O 效能：檔案伺服器與儲存磁碟之間的請求輸送量/IOPS

決定檔案系統的這些效能特性有兩個因素：您為其設定的 SSD IOPS 總量和輸送量容量。前兩個效能特性 - 網路 I/O 效能和記憶體內和 NVMe 快取大小 - 完全由輸送量容量決定，而第三個效能 - 磁碟 I/O 效能 - 由輸送量容量和 SSD IOPS 的組合決定。

檔案型工作負載通常爆量，特徵為短暫、密集的高 I/O 期間，以及爆量之間的大量閒置時間。為了支援尖峰工作負載，除了檔案系統可維持全年無休的基準速度之外，Amazon FSx 還為網路 I/O 和磁碟 I/O 操作提供在一段時間內爆增至更高速度的功能。Amazon FSx 使用網路 I/O 額度機制根據平均使用率來配置輸送量和 IOPS — 檔案系統會在輸送量和 IOPS 用量低於其基準限制時累積點數，並在執行 I/O 操作時使用這些點數。



**Note**

對於 iSCSI 和 NVMe/TCP SAN 通訊協定，循序讀取用戶端操作最多可達到檔案系統的最大網路 I/O 高載或基準輸送量。

寫入操作使用的網路頻寬是讀取操作的兩倍。寫入操作必須在次要檔案伺服器上複寫，因此單一寫入操作會產生兩倍的網路輸送量。

## 部署類型對效能的影響

您可以使用 FSx for ONTAP 建立單一可用區和多可用區檔案系統。第一代檔案系統（單一可用區域和多可用區域）和第二代多可用區域檔案系統都由一個高可用性 (HA) 對提供支援。第二代單一可用區檔案系統最多由 12 個 HA 對提供支援。如需詳細資訊，請參閱[管理高可用性 \(HA\) 對](#)。

FSx for ONTAP 多可用區和單一可用區檔案系統提供 SSD 儲存的一致低於毫秒的檔案操作延遲，以及容量集區儲存的數十毫秒延遲。此外，符合下列要求的檔案系統提供 NVMe 讀取快取，以減少讀取延遲，並增加經常讀取資料的 IOPS：

- 異地同步備份 1 和異地同步備份 2 檔案系統
- 在 2022 年 11 月 28 日之後建立的單一可用區域 1 檔案系統，輸送量容量至少為 2 GBps
- 單一可用區域 2 檔案系統，每對輸送量容量至少為 6 GBps

**Note**

對於第二代檔案系統（單一可用區 2 和多可用區 2），使用 NVMe 快取可能會導致您的工作負載在高輸送量或大型 I/O 工作負載中達到較少的總輸送量。如果您有輸送量限制工作負載，建議您停用 NVMe 快取。如需詳細資訊，請參閱[管理 NVMe 快取](#)。

下表顯示根據高可用性 (HA) 對數和 AWS 區域 可用性等因素，檔案系統可擴展的輸送量容量。

### First-generation file systems

這些效能規格適用於第一代單一可用區和多可用區檔案系統。

### 針對第一代檔案系統，每個 HA 對 SSD 儲存體的最大輸送量

|        | 美國東部（俄亥俄）區域、<br>美國東部（維吉尼亞北部）<br>區域、美國西部（奧勒岡）<br>區域和歐洲（愛爾蘭） |                 | <a href="#">所有其他可使用 FSx for ONTAP AWS 區域的位置</a> |                 |
|--------|------------------------------------------------------------|-----------------|-------------------------------------------------|-----------------|
|        | 讀取輸送量<br>(MBps)                                            | 寫入輸送量<br>(MBps) | 讀取輸送量<br>(MBps)                                 | 寫入輸送量<br>(MBps) |
| 單一可用區  | 4,096 <sup>1</sup>                                         | 1,000           | 2,048                                           | 750             |
| 異地同步備份 | 4,096 <sup>1</sup>                                         | 1,800           | 2,048                                           | 1,300           |

#### Note

<sup>1</sup> 若要佈建 4 GBps 的輸送量容量，您的檔案系統必須設定為至少 5,120 GiB 的 SSD 儲存容量和 160,000 個 SSD IOPS。

### Second-generation file systems

這些效能規格適用於第二代單一可用區和多可用區檔案系統。一般而言，第二代檔案系統可為讀取提供完整佈建的整個容量，並為寫入提供最多三分之一的佈建輸送量容量。例外狀況是 6,144 MB/s 選項，列於此表格中。

### 針對第二代檔案系統，每個 HA 對 SSD 儲存體的最大輸送量

|        | 讀取輸送量 (MBps)       | 寫入輸送量 (MBps)       |
|--------|--------------------|--------------------|
| 單一可用區  | 6,144 <sup>1</sup> | 1,024 <sup>1</sup> |
| 異地同步備份 | 6,144              | 2,048              |

 Note

每個 HA 對<sup>1</sup> 個（最多 12 個）。如需詳細資訊，請參閱[管理高可用性 \(HA\) 對](#)。

## 儲存容量對效能的影響

檔案系統可達到的最大磁碟輸送量和 IOPS 層級較低：

- 檔案伺服器提供的磁碟效能等級，取決於您為檔案系統選取的輸送量容量
- 您為檔案系統佈建的 SSD IOPS 數量所提供的磁碟效能等級

根據預設，檔案系統的 SSD 儲存提供高達下列層級的磁碟輸送量和 IOPS：

- 磁碟輸送量（每 TiB 儲存體的 MBps）：768
- 磁碟 IOPS (IOPs)：3,072 TiB

## 輸送量容量對效能的影響

每個 Amazon FSx 檔案系統都有您在建立檔案系統時設定的輸送量容量。您的檔案系統的輸送量容量會決定網路 I/O 效能層級，或是託管檔案系統的每個檔案伺服器透過網路將檔案資料提供給存取它的用戶端的速度。更高的輸送量容量具有更多記憶體和非揮發性記憶體表達 (NVMe) 儲存體，用於快取每個檔案伺服器上的資料，以及每個檔案伺服器支援的更高層級磁碟 I/O 效能。

您可以在建立檔案系統時選擇性地佈建更高層級的 SSD IOPS。檔案系統可達到的最大 SSD IOPS 層級也會由您檔案系統的輸送量容量決定，即使佈建額外的 SSD IOPS 也是如此。

下表顯示輸送量容量的完整規格集，以及基準和爆量層級，以及對應中檔案伺服器上快取的記憶體數量 AWS 區域。

### First-generation Single-AZ file system

這些效能規格適用於 2022 年 11 月 28 日之後在指定的中建立的第一代單一可用區檔案系統 AWS 區域。

下列檔案系統的效能規格 AWS 區域：美國東部（維吉尼亞北部）、美國東部（俄亥俄）、美國西部（奧勒岡）和歐洲（愛爾蘭）

| FSx 輸<br>送量<br>容量<br>(MBps) | 網路輸送量容量<br>(MBps) |       | 網路<br>IOPS | 記憶體<br>內快取<br>(GB) | NVMe<br>讀取<br>快取<br>(GB) | 磁碟輸送量<br>(MBps) |       | SSD 磁碟機<br>IOPS * |        |
|-----------------------------|-------------------|-------|------------|--------------------|--------------------------|-----------------|-------|-------------------|--------|
|                             | 基準                | 爆量    |            |                    |                          | 基準              | 爆量    | 基準                | 爆量     |
| 128                         | 188               | 1,500 | 數萬個<br>基準  | 16                 | –                        | 128             | 1,250 | 6,000             | 40,000 |
| 256                         | 375               | 1,500 |            | 32                 | –                        | 256             | 1,250 | 12,000            | 40,000 |
| 512                         | 750               | 1,500 | 數十萬<br>個基準 | 64                 | –                        | 512             | 1,250 | 20,000            | 40,000 |
| 1,024                       | 1,500             | –     |            | 128                | –                        | 1,024           | 1,250 | 40,000            | –      |
| 2,048                       | 3,125             | –     |            | 256                | 1,900                    | 2,048           | –     | 80,000            | –      |
| 4,096                       | 6,250             | –     |            | 512                | 5,400                    | 4,096           | –     | 160,000           | –      |

**Note**

\* 只有在您存取檔案伺服器記憶體內快取或 NVMe 快取中未快取的資料時，才會使用您的 SSD IOPS。

這些效能規格適用於提供 FSx for ONTAP AWS 區域 的所有其他 中的第一代單一可用區域檔案系統。

所有其他 [FSx for ONTAP 可用 AWS 區域 之](#) 檔案系統的效能規格

| FSx 輸<br>送量<br>容量<br>(MBps) | 網路輸送量容量<br>(MBps) |    | 網路<br>IOPS | 記憶體<br>內快取<br>(GB) | 磁碟輸送量<br>(MBps) | SSD 磁碟機 IOPS * |    |
|-----------------------------|-------------------|----|------------|--------------------|-----------------|----------------|----|
|                             | 基準                | 爆量 |            |                    |                 | 基準             | 爆量 |

| FSx 輸<br>送量<br>容量<br>(MBps) | 網路輸送量容量<br>(MBps) |       | 網路<br>IOPS | 記憶體<br>內快取<br>(GB) | 磁碟輸送量<br>(MBps) |     | SSD 磁碟機 IOPS<br>* |        |
|-----------------------------|-------------------|-------|------------|--------------------|-----------------|-----|-------------------|--------|
| 128                         | 150               | 1,250 | 數萬個<br>基準  | 16                 | 128             | 600 | 6,000             | 18,750 |
| 256                         | 300               | 1,250 |            | 32                 | 256             | 600 | 12,000            | 18,750 |
| 512                         | 625               | 1,250 | 數十萬<br>個基準 | 64                 | 512             | 600 | 18,750            | –      |
| 1,024                       | 1,500             | –     |            | 128                | 1,024           | –   | 40,000            | –      |
| 2,048                       | 3,125             | –     |            | 256                | 2,048           | –   | 80,000            | –      |

 Note

\* 只有在您存取檔案伺服器記憶體內快取或 NVMe 快取中未快取的資料時，才會使用您的 SSD IOPS。

## Second-generation Single-AZ file system

這些效能規格適用於第二代單一可用區檔案系統。

### 第二代單一可用區檔案系統的效能規格

| FSx 輸<br>送量<br>容量<br>(MBps) | 網路輸送量容量<br>(MBps) |       | 網路<br>IOPS | 記憶體<br>內快取<br>(GB) | NVMe<br>快取<br>(GB) | 磁碟輸送量<br>(MBps) |       | SSD 磁碟機<br>IOPS * |        |
|-----------------------------|-------------------|-------|------------|--------------------|--------------------|-----------------|-------|-------------------|--------|
|                             | 基準                | 爆量    |            |                    |                    | 基準              | 爆量    | 基準                | 爆量     |
| 384**                       | 781               | 6,250 | 數十萬<br>個基準 | 16                 | –                  | 384             | 3,125 | 12,500            | 65,000 |
| 768**                       | 1,563             | 6,250 |            | 32                 | –                  | 768             | 3,125 | 25,000            | 65,000 |
| 1,536                       | 3,125             | 6,250 |            | 64                 | –                  | 1,536           | 3,125 | 50,000            | 65,000 |

| FSx 輸<br>送量<br>容量<br>(MBps) | 網路輸送量容量<br>(MBps) |   | 網路<br>IOPS | 記憶體<br>內快取<br>(GB) | NVMe<br>快取<br>(GB) | 磁碟輸送量<br>(MBps) |   | SSD 磁碟機<br>IOPS * |   |
|-----------------------------|-------------------|---|------------|--------------------|--------------------|-----------------|---|-------------------|---|
| 3,072                       | 6,250             | – |            | 128                | –                  | 3,072           | – | 100,000           | – |
| 6,144                       | 12,500            | – |            | 256                | 1,900              | 6,144           | – | 200,000           | – |

**Note**

\* 只有在您存取檔案伺服器記憶體內快取或 NVMe 快取中未快取的資料時，才會使用您的 SSD IOPS。

\*\* 第二代單一可用區檔案系統支援 384 和 768 輸送量容量，但只有一個 HA 對。若要新增 HA 對，您的檔案系統必須至少設定 1,536 MBps 的輸送量容量。

## First-generation Multi-AZ file system

這些效能規格適用於指定中 2022 年 11 月 28 日之後建立的第一代異地同步備份檔案系統 AWS 區域。

下列檔案系統的效能規格 AWS 區域：美國東部（維吉尼亞北部）、美國東部（俄亥俄）、美國西部（奧勒岡）和歐洲（愛爾蘭）

| FSx 輸<br>送量<br>容量<br>(MBps) | 網路輸送量容量<br>(MBps) |       | 網路<br>IOPS | 記憶體<br>內快取<br>(GB) | NVMe<br>快取<br>(GB) | 磁碟輸送量<br>(MBps) |       | SSD 磁碟機<br>IOPS * |        |
|-----------------------------|-------------------|-------|------------|--------------------|--------------------|-----------------|-------|-------------------|--------|
|                             | 基準                | 爆量    |            |                    |                    | 基準              | 爆量    | 基準                | 爆量     |
| 128                         | 188               | 1,500 | 數萬個<br>基準  | 16                 | 238                | 128             | 1,250 | 6,000             | 40,000 |
| 256                         | 375               | 1,500 |            | 32                 | 475                | 256             | 1,250 | 12,000            | 40,000 |
| 512                         | 750               | 1,500 | 數十萬<br>個基準 | 64                 | 950                | 512             | 1,250 | 20,000            | 40,000 |
| 1,024                       | 1,500             | –     |            | 128                | 1,900              | 1,024           | 1,250 | 40,000            | –      |

| FSx 輸<br>送量<br>容量<br>(MBps) | 網路輸送量容量<br>(MBps) |   | 網路<br>IOPS | 記憶體<br>內快取<br>(GB) | NVMe<br>快取<br>(GB) | 磁碟輸送量<br>(MBps) |   | SSD 磁碟機<br>IOPS * |   |
|-----------------------------|-------------------|---|------------|--------------------|--------------------|-----------------|---|-------------------|---|
| 2,048                       | 3,125             | – |            | 256                | 3,800              | 2,048           | – | 80,000            | – |
| 4,096                       | 6,250             | – |            | 512                | 7,600              | 4,096           | – | 160,000           | – |

 Note

\* 只有在您存取檔案伺服器記憶體內快取或 NVMe 快取中未快取的資料時，才會使用您的 SSD IOPS。

這些效能規格適用於提供 FSx for ONTAP AWS 區域 的所有其他 中的第一代多可用區域檔案系統。

所有其他 [FSx for ONTAP 可用 AWS 區域 之](#) 檔案系統的效能規格

| FSx 輸<br>送量<br>容量<br>(MBps) | 網路輸送量容量<br>(MBps) |       | 網路<br>IOPS | 記憶體<br>內快取<br>(GB) | NVMe<br>快取<br>(GB) | 磁碟輸送量<br>(MBps) |     | SSD 磁碟機<br>IOPS * |        |
|-----------------------------|-------------------|-------|------------|--------------------|--------------------|-----------------|-----|-------------------|--------|
|                             | 基準                | 爆量    |            |                    |                    | 基準              | 爆量  | 基準                | 爆量     |
| 128                         | 150               | 1,250 | 數萬個<br>基準  | 16                 | 150                | 128             | 600 | 6,000             | 18,750 |
| 256                         | 300               | 1,250 |            | 32                 | 300                | 256             | 600 | 12,000            | 18,750 |
| 512                         | 625               | 1,250 | 數十萬<br>個基準 | 64                 | 600                | 512             | 600 | 18,750            | –      |
| 1,024                       | 1,500             | –     |            | 128                | 1,200              | 1,024           | –   | 40,000            | –      |
| 2,048                       | 3,125             | –     |            | 256                | 2,400              | 2,048           | –   | 80,000            | –      |

 **Note**

\* 只有在您存取檔案伺服器記憶體內快取或 NVMe 快取中未快取的資料時，才會使用您的 SSD IOPS。

Second-generation Multi-AZ file systems

這些效能規格適用於第二代多可用區域檔案系統。

第二代異地同步備份檔案系統的效能規格

| FSx 輸<br>送量<br>容量<br>(MBps) | 網路輸送量容量<br>(MBps) |       | 網路<br>IOPS | 記憶體<br>內快取<br>(GB) | NVMe<br>快取<br>(GB) | 磁碟輸送量<br>(MBps) |       | SSD 磁碟機<br>IOPS * |        |
|-----------------------------|-------------------|-------|------------|--------------------|--------------------|-----------------|-------|-------------------|--------|
|                             | 基準                | 爆量    |            |                    |                    | 基準              | 爆量    | 基準                | 爆量     |
| 384                         | 781               | 6,250 | 數十萬<br>個基準 | 16                 | 237                | 384             | 3,125 | 12,500            | 65,000 |
| 768                         | 1,563             | 6,250 |            | 32                 | 474                | 768             | 3,125 | 25,000            | 65,000 |
| 1,536                       | 3,125             | 6,250 |            | 64                 | 950                | 1,536           | 3,125 | 50,000            | 65,000 |
| 3 , 072                     | 6,250             | –     |            | 128                | 1,900              | 3,072           | –     | 100,000           | –      |
| 6,144                       | 12,500            | –     |            | 256                | 3,800              | 6,144           | –     | 200,000           | –      |

 **Note**

\* 只有在您存取檔案伺服器記憶體內快取或 NVMe 快取中未快取的資料時，才會使用您的 SSD IOPS。

範例：儲存容量和輸送量容量

下列範例說明儲存容量和輸送量容量如何影響檔案系統效能。

第一代檔案系統設定為 2 TiB 的 SSD 儲存容量和 512 MBps 的輸送量容量，具有下列輸送量層級：



- 網路輸送量 – 基準 625 MBps 和高載 1,250 MBps ( 請參閱輸送量資料表 )
- 磁碟輸送量 – 512 MBps 基準和 600 MBps 高載。

因此，您存取檔案系統的工作負載將能夠驅動高達 625 MBps 的基準和 1,250 MBps 的爆量輸送量，用於在檔案伺服器記憶體內快取和 NVMe 快取中主動存取的資料上執行的檔案操作。

# 管理 FSx for ONTAP 資源

您可以使用 AWS CLI、AWS Management Console、和 ONTAP CLI 和 API，為 FSx for ONTAP 資源執行下列管理動作：

- 建立、列出、更新和刪除檔案系統、儲存虛擬機器 (SVMs)、磁碟區、備份和標籤。
- 管理現有檔案系統掛載目標的存取、管理帳戶和密碼、密碼要求、SMB 和 iSCSI 通訊協定、網路存取

## 主題

- [管理儲存容量](#)
- [管理 FSx for ONTAP 檔案系統](#)
- [管理 FSx for ONTAP 儲存虛擬機器](#)
- [管理 ONTAP 磁碟區的 FSx](#)
- [建立 iSCSI LUN](#)
- [使用 Amazon FSx 維護時段最佳化效能](#)
- [管理輸送量容量](#)
- [管理 SMB 共用](#)
- [使用 NetApp 應用程式管理 FSx for ONTAP 資源](#)
- [標記 Amazon FSx 資源](#)

## 管理儲存容量

Amazon FSx for NetApp ONTAP 提供多種儲存相關功能，可讓您用來管理檔案系統的儲存容量。

## 主題

- [FSx for ONTAP 儲存層](#)
- [選擇適當數量的檔案系統 SSD 儲存體](#)
- [檔案系統儲存容量和 IOPS](#)
- [磁碟區儲存容量](#)

## FSx for ONTAP 儲存層

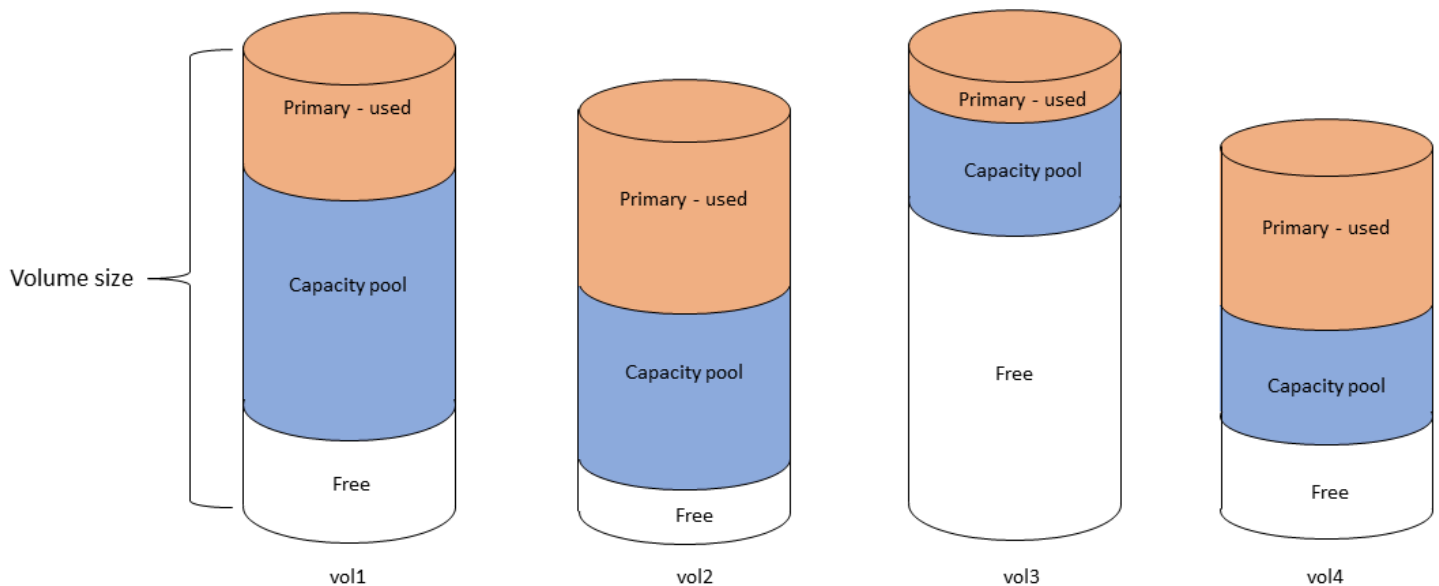
儲存層是 Amazon FSx for NetApp ONTAP 檔案系統的實體儲存媒體。FSx for ONTAP 提供下列儲存層：

- SSD 層 – 使用者佈建的高效能固態硬碟 (SSD) 儲存體，專為資料集的作用中部分而打造。
- 容量集區層 – 完全彈性的儲存體，可自動擴展至 PB 大小，並針對不常存取的資料進行成本最佳化。

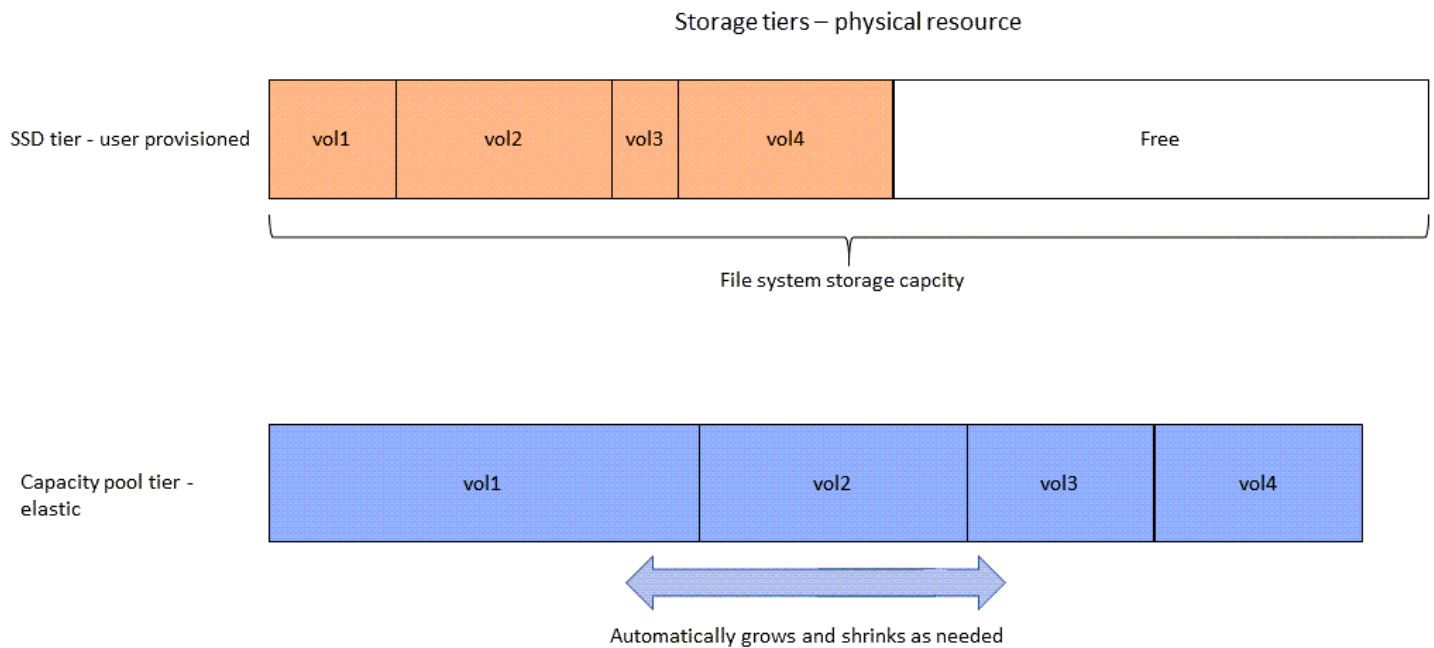
FSx for ONTAP 磁碟區是一種虛擬資源，類似於資料夾，不會消耗儲存容量。您存放且耗用實體儲存的資料會存在於磁碟區中。建立磁碟區時，您可以指定其大小，您可以在建立磁碟區後修改。ONTAP 磁碟區的 FSx 是精簡佈建的，而且檔案系統儲存不會事先保留。反之，SSD 和容量集區儲存會視需要動態配置。您在磁碟區層級設定的[分層政策](#)，會判斷存放在 SSD 層中的資料是否以及何時轉換至容量集區層。

下圖說明檔案系統中跨多個 FSx for ONTAP 磁碟區配置的資料範例。

Volume thin provisioning



下圖說明檔案系統的實體儲存容量如何由上圖四個磁碟區中的資料使用。



您可以選擇最符合您檔案系統上每個磁碟區需求的分層政策，以降低儲存成本。如需詳細資訊，請參閱[磁碟區資料分層](#)。

## 選擇適當數量的檔案系統 SSD 儲存體

選擇 FSx for ONTAP 檔案系統的 SSD 儲存容量時，您需要記住下列會影響資料儲存可用 SSD 儲存容量的項目：

- 為 NetApp ONTAP 軟體額外負荷預留的儲存容量。
- 檔案中繼資料
- 最近寫入的資料
- 您想要存放在 SSD 儲存體上的檔案，無論是未達到冷卻期間的資料，或是您最近讀取並擷取回 SSD 的資料。

## 如何使用 SSD 儲存體

檔案系統的 SSD 儲存體用於 NetApp ONTAP 軟體（額外負荷）、檔案中繼資料和資料的組合。

### NetApp ONTAP 軟體額外負荷

如同其他 NetApp ONTAP 檔案系統，檔案系統的 SSD 儲存容量最多可保留 16% 用於 ONTAP 額外負荷，這表示它不適用於儲存您的檔案。ONTAP 額外負荷的配置方式如下：

- 11% 保留給 NetApp ONTAP 軟體。對於 SSD 儲存容量超過 30 tebibytes (TiB) 的檔案系統，會保留 6%。
- 5% 保留給彙總快照，這是在兩個檔案系統的檔案伺服器之間同步資料的必要項目。

## 檔案中繼資料

檔案中繼資料通常會耗用檔案所耗用 3-7% 的儲存容量。此百分比取決於平均檔案大小（較小的平均檔案大小需要更多中繼資料），以及檔案節省的儲存效率。請注意，檔案中繼資料不會受益於儲存效率節省。您可以使用下列準則來估計檔案系統上用於中繼資料的 SSD 儲存量。

| 平均檔案大小    | 中繼資料的大小，以檔案資料的百分比表示 |
|-----------|---------------------|
| 4 KB      | 7%                  |
| 8 KB      | 3.5%                |
| 32 KB 或更高 | 1-3%                |

調整您計劃在容量集區層上存放之檔案中繼資料所需的 SSD 儲存容量時，建議您針對計劃存放在容量集區層的每 10 GiB 資料，使用 1 GiB SSD 儲存體的保守比率。

## 存放在 SSD 層的檔案資料

除了作用中的資料集和所有檔案中繼資料之外，寫入檔案系統的所有資料最初都會寫入 SSD 層，然後再分層至容量集區儲存。無論磁碟區的分層政策為何，都適用，但在設定了所有資料分層政策的磁碟區上使用 SnapMirror 時，資料會直接寫入容量集區儲存體。

只要 SSD 層的使用率低於 90%，容量集區層的隨機讀取就會快取在 SSD 層中。如需詳細資訊，請參閱[磁碟區資料分層](#)。

## 建議的 SSD 容量使用率

我們建議您不要超過 SSD 儲存層持續使用率的 80%。對於第二代檔案系統，我們另外建議您不要超過任何檔案系統彙總持續使用率的 80%。這些建議與 NetApp 對 ONTAP 的建議一致。由於檔案系統的 SSD 層也用於容量集區層的預備寫入，以及隨機讀取，因此存取模式的任何突然變更都可能快速增加 SSD 層的使用率。

在 90% 的 SSD 使用率下，從容量集區層讀取的資料不會再快取在 SSD 層上，以便為寫入檔案系統的任何新資料保留剩餘的 SSD 容量。這會導致從容量集區層重複讀取相同的資料，而從容量集區儲存體讀取，而不是從 SSD 層快取和讀取，這可能會影響檔案系統的輸送量容量。

當 SSD 層達到或超過 98% 使用率時，所有分層功能都會停止。如需詳細資訊，請參閱[分層閾值](#)。

## 儲存效率

NetApp ONTAP 在磁碟區層級提供區塊層級儲存效率功能，包括壓縮、壓縮和重複資料刪除。這些功能可節省一般檔案共用高達 65% 的儲存容量，而不會犧牲效能。您可以根據每個磁碟區啟用儲存效率。這些功能可降低資料使用的儲存容量，讓您可以在 SSD、容量集區和備份儲存體中消耗較少的儲存空間。您可以針對 SSD 儲存體中的資料，在每個磁碟區上啟用壓縮和重複資料刪除。當資料分層至容量集區儲存體時，會保留 SSD 儲存體中壓縮和重複資料刪除的儲存體節省成本。無論檔案系統的儲存效率組態為何，都會為備份資料啟用儲存效率。

下表顯示典型儲存節省的範例。

|          | 僅限壓縮   | 僅重複資料刪除 | 壓縮和重複資料刪除 |
|----------|--------|---------|-----------|
| 一般用途檔案共享 | 50%    | 30%     | 65%       |
| 虛擬伺服器和桌面 | 55%    | 70%     | 70%       |
| 資料庫      | 65-70% | 0%      | 65-70%    |
| 工程資料     | 55%    | 30%     | 75%       |
| 地理地震資料   | 40%    | 3%      | 40%       |

對於大多數工作負載，啟用壓縮和重複資料刪除不會對檔案系統效能造成負面影響。對於大多數工作負載，壓縮會增加整體效能。為了從 RAM 快取提供快速讀取和寫入，FSx for ONTAP 檔案伺服器在前端網路介面卡 (NICs) 上配備了比檔案伺服器和儲存磁碟之間可用的更高層級的網路頻寬。由於資料壓縮可減少檔案伺服器和儲存磁碟之間傳送的資料量，因此對於大多數工作負載而言，使用資料壓縮時，整體檔案系統輸送量容量會增加。一旦您使檔案系統的前端 NIC 飽和，就會限制與資料壓縮相關的輸送量容量增加。

Amazon FSx for NetApp ONTAP 也支援其他可節省空間 ONTAP 的功能，包括快照、精簡佈建和 FlexClone 磁碟區。

預設不會啟用儲存效率功能。您可以啟用它們，如下所示：

- [建立檔案系統時](#)，在 SVM 的根磁碟區上。
- [建立新磁碟區時](#)。
- 當您[修改現有的磁碟區時](#)。

若要檢視已啟用儲存效率之檔案系統的儲存節省量，請參閱 [監控儲存效率節省](#)。

## 計算儲存效率節省

您可以使用 LogicalDataStored 和 StorageUsed FSx for ONTAP CloudWatch 檔案系統指標，計算壓縮、重複資料刪除、壓縮、快照和的儲存節省 FlexClones。這些指標具有單一維度 FileSystemId。如需詳細資訊，請參閱 [檔案系統指標](#)。

- 若要以位元組為單位計算儲存效率節省，請採用 StorageUsed 指定期間的平均，並將其從 LogicalDataStored 相同期間的平均中減去。
- 若要以總邏輯資料大小的百分比來計算儲存效率節省，StorageUsed 請在指定期間取得 Average 的，並在 LogicalDataStored 相同期間從 Average 減去它。然後將差異除以 LogicalDataStored 相同期間的 Average。

## SSD 大小範例

假設您想要為不常存取 80% 資料的應用程式存放 100 TiB 的資料。在此案例中，80% (80 TiB) 的資料會自動分層為容量集區層，而剩餘的 20% (20 TiB) 仍保留在 SSD 儲存中。根據一般用途檔案共用工作負載的典型儲存效率節省 65%，相當於 7 TiB 的資料。若要維持 80% 的 SSD 使用率，您需要 8.75 TiB 的 SSD 儲存容量，以處理 20 TiB 的主動存取資料。您佈建的 SSD 儲存體數量也需要考量 16% 的 ONTAP 軟體儲存體額外負荷，如下列計算所示。

```
ssdNeeded = ssdProvisioned * (1 - 0.16)
8.75 TiB / 0.84 = ssdProvisioned
10.42 TiB = ssdProvisioned
```

因此，在此範例中，您需要佈建至少 10.42 TiB 的 SSD 儲存體。您也將使用 28 TiB 的容量集區儲存，用於其餘 80 TiB 不常存取的資料。

## 檔案系統儲存容量和 IOPS

當您建立 FSx for ONTAP 檔案系統時，您可以指定 SSD 層的儲存容量。對於第二代單一可用區檔案系統，您指定的儲存容量會平均分散在每個高可用性 (HA) 對的儲存集區中；這些儲存集區稱為彙總。

對於您佈建的每個 SSD 儲存 GiB，Amazon FSx 會自動為檔案系統每秒佈建 3 個 SSD 輸入/輸出操作 (IOPS)，每個檔案系統最多 160,000 個 SSD IOPS。對於第二代單一可用區檔案系統，您的 SSD IOPS 會平均分散到每個檔案系統的彙總。您可以選擇指定高於每 GiB 自動 3 個 SSD IOPS 的佈建 SSD IOPS 層級。如需可為 FSx for ONTAP 檔案系統佈建之 SSD IOPS 數量上限的詳細資訊，請參閱[輸送量容量對效能的影響](#)。

## 主題

- [更新檔案系統 SSD 儲存體和 IOPS](#)
- [為您的檔案系統建立儲存容量使用率警示](#)
- [更新儲存容量和佈建 IOPS](#)
- [動態更新儲存容量](#)
- [監控 SSD 儲存體使用率](#)
- [監控儲存效率節省](#)
- [監控儲存容量和 IOPS 更新](#)

## 更新檔案系統 SSD 儲存體和 IOPS

當您需要為資料集的作用中部分增加額外儲存空間時，您可以增加 Amazon FSx for NetApp ONTAP 檔案系統的 SSD 儲存容量。使用 Amazon FSx 主控台、Amazon FSx API 或 AWS Command Line Interface (AWS CLI) 來增加 SSD 儲存容量。如需詳細資訊，請參閱[更新儲存容量和佈建 IOPS](#)。

當您增加 Amazon FSx 檔案系統的 SSD 儲存容量時，新容量通常可在幾分鐘內使用。新的 SSD 儲存容量在可供您使用之後，會向您收取費用。如需定價的詳細資訊，請參閱[Amazon FSx for NetApp ONTAP 定價](#)。

增加儲存容量後，Amazon FSx 會在背景執行儲存最佳化程序，以重新平衡您的資料。對於大多數檔案系統，儲存最佳化需要幾個小時，對您的工作負載效能影響最小。

您可以使用 Amazon FSx 主控台、CLI 和 API，隨時追蹤儲存最佳化程序的進度。如需詳細資訊，請參閱[監控儲存容量和 IOPS 更新](#)。

## 考量事項

以下是修改檔案系統的 SSD 儲存容量和佈建 IOPS 時需要考慮的一些重要事項：

- 僅限增加儲存容量 – 您只能增加檔案系統的 SSD 儲存容量；您無法減少儲存容量。
- 儲存容量下限：每個 SSD 儲存容量下限都必須是檔案系統目前 SSD 儲存容量的 10%，最高可達檔案系統組態的 SSD 儲存容量上限。



- ( 僅限第二代單一可用區檔案系統 ) 儲存容量分散 – 您為檔案系統選取的新儲存容量或 SSD IOPS 會平均分散至每個檔案系統的彙總。
- 增加之間的時間 – 在修改檔案系統的 SSD 儲存容量、佈建 IOPS 或輸送量容量之後，您必須等待至少六小時，才能再次修改相同檔案系統上的任何這些組態。這有時被稱為冷卻時間。
- 佈建 IOPS 模式 – 對於佈建 IOPS 變更，您必須指定兩種 IOPS 模式之一：
  - 自動模式 – Amazon FSx 會自動擴展您的 SSD IOPS，以維持每 GiB SSD 儲存容量 3 個佈建的 SSD IOPS，最高可達檔案系統組態的 SSD IOPS 上限。

**Note**

如需可為 FSx for ONTAP 檔案系統佈建之 SSD IOPS 數量上限的詳細資訊，請參閱 [輸送量容量對效能的影響](#)。

- 使用者佈建模式 – 您可以指定 SSD IOPS 的數量，其必須大於或等於每 GiB SSD 儲存容量 3 IOPS。如果您選擇佈建更高層級的 IOPS，則需為該月平均佈建的 IOPS 支付高於包含速率的費用，以 IOPS 月為單位。

如需定價的詳細資訊，請參閱 [Amazon FSx for NetApp ONTAP 定價](#)。

## 何時增加 SSD 儲存容量

如果您用盡可用的 SSD 層儲存，建議您增加檔案系統的儲存容量。儲存空間不足表示您的 SSD 層對於資料集的作用中部分過小。

若要監控檔案系統上可用的可用儲存量，請使用檔案系統層級 StorageCapacity 和 StorageUsed Amazon CloudWatch 指標。您可以在指標上建立 CloudWatch 警示，並在其低於特定閾值時收到通知。如需詳細資訊，請參閱 [使用 Amazon CloudWatch 監控](#)。

**Note**

我們建議您不要超過 80% 的 SSD 儲存容量使用率，以確保資料分層、輸送量擴展和其他維護活動正常運作，並且有容量可用於其他資料。對於第二代檔案系統，此建議適用於所有檔案系統彙總的平均使用率，以及每個個別彙總。

如需如何使用檔案系統的 SSD 儲存體，以及為檔案中繼資料和操作軟體預留多少 SSD 儲存體的詳細資訊，請參閱 [選擇適當數量的檔案系統 SSD 儲存體](#)。

## 為您的檔案系統建立儲存容量使用率警示

我們建議您不要超過持續平均 SSD 儲存容量使用率 80%。偶爾可以接受超過 80% 的 SSD 儲存使用率峰值。將平均使用率維持在 80% 以下，可提供足夠的容量來增加儲存體，而不會遇到問題。下列程序說明如何建立 CloudWatch 警示，在檔案系統的 SSD 儲存使用率接近 80% 時提醒您。

### 建立檔案系統儲存容量使用率警示

您可以使用 `StorageCapacityUtilization` 指標來建立警示，該警示會在一或多個 FSx for ONTAP 檔案系統達到儲存使用率閾值時觸發。

1. 透過 <https://console.aws.amazon.com/cloudwatch/> 開啟 CloudWatch 主控台。
2. 在左側導覽窗格中的警示下，選擇所有警示。然後，選擇建立警示。在建立警示精靈中，選擇選取指標。
3. 在圖形總管中，選擇多來源查詢索引標籤。
4. 在查詢建置器中，選擇下列項目：
  - 針對命名空間，選取 AWS/FSx > 詳細檔案系統指標。
  - 針對指標名稱，選取 `MAX(StorageCapacityUtilization)`。
  - 對於篩選條件，您可以選擇依特定檔案系統的 ID 來包含或排除該檔案系統。如果您將篩選條件保留空白，則您的警示會在任何檔案系統超過警示的儲存容量使用率閾值時觸發。
  - 將其餘選項保留空白，然後選擇圖形查詢。
5. 選擇選取指標。回到精靈，在指標區段中為您的指標提供標籤。我們建議將期間保留為 5 分鐘。
6. 在條件下，選擇靜態閾值類型，每當指標大於/等於 80 時。
7. 選擇下一步以前往設定動作頁面。

### 設定警示動作

您可以為警示設定各種動作，以在達到您設定的閾值時觸發警示。在此範例中，我們選擇 Simple Notification Service (SNS) 主題，但您可以在 [Amazon CloudWatch 使用者指南中的使用 Amazon CloudWatch 警示](#) 中了解其他動作。Amazon CloudWatch

1. 在通知區段中，選擇警示處於 ALARM 狀態時要通知的 SNS 主題。您可以選擇現有的主題或建立新的主題。您將收到訂閱通知，您需要先確認，才能將警示通知傳送到電子郵件地址。
2. 選擇下一步。

## 完成警示

請依照這些指示完成建立 CloudWatch 警示的程序。

1. 在新增名稱和描述頁面上，為您的警示命名，並選擇性地提供描述，然後選擇下一步。
2. 檢閱您在預覽和建立頁面中設定的所有項目，然後選擇建立警示。

## 更新儲存容量和佈建 IOPS

您可以使用 Amazon FSx 主控台、和 API 來增加或減少檔案系統的 SSD 型儲存，並增加 AWS CLI 或減少佈建的 SSD IOPS 數量。

更新檔案系統的 SSD 儲存容量或佈建 IOPS（主控台）

1. 開啟 Amazon FSx 主控台，網址為 <https://console.aws.amazon.com/fsx/> : //www.。
2. 在左側導覽窗格中選擇檔案系統。在檔案系統清單中，選取您要更新 SSD 儲存容量和 SSD IOPS 的 FSx for ONTAP 檔案系統。
3. 選擇動作 > 更新儲存容量。或者，在摘要區段中，選擇檔案系統的 SSD 儲存容量值旁的更新。

更新 SSD 儲存容量和 IOPS 對話方塊隨即出現。

## Update SSD storage capacity and IOPS



File system ID

fs-01234567890abcdef

### Current configuration

**SSD storage capacity:** 4096 GiB  
**IOPS mode:** Automatic (3 IOPS per GiB of SSD storage)  
**SSD IOPS:** 12288

### SSD storage capacity

☒ Modify storage capacity

Input type

- ☒ Percentage  
☐ Absolute

Desired % increase

10

%

Minimum 4506 GiB (10% above current); Maximum 1048576 GiB.

### Provisioned SSD IOPS

- ☒ Automatic (3 IOPS per GiB of SSD storage)  
☐ User-provisioned

### Configuration preview

| Attribute            | Current configuration                | New configuration                    |
|----------------------|--------------------------------------|--------------------------------------|
| SSD storage capacity | 4,096 GiB<br>(2,048 GiB per HA pair) | 4,506 GiB<br>(2,253 GiB per HA pair) |
|                      | Mode: Automatic                      | Mode: Automatic                      |

4. 若要增加 SSD 儲存容量，請選擇修改儲存容量。
5. 針對輸入類型，選擇下列其中一項：
  - 若要輸入新的 SSD 儲存容量做為與目前值的百分比變更，請選擇百分比。
  - 若要以 GiB 輸入新值，請選擇絕對。
6. 根據輸入類型，輸入所需百分比增加的值。
  - 針對百分比，輸入百分比增加值。此值必須至少大於目前值的 10%。
  - 對於絕對值，以 GiB 輸入新值，最大允許值為 196,608 GiB。
7. 對於佈建 SSD IOPS，您有兩個選項可修改檔案系統的佈建 SSD IOPS 數量：
  - 如果您希望 Amazon FSx 自動擴展 SSD IOPS，以維持每 GiB SSD 儲存容量 3 個佈建的 SSD IOPS（最多 160,000 個），請選擇自動。
  - 如果您想要指定 SSD IOPS 的數量，請選擇使用者佈建。輸入 IOPS 的絕對數量，其至少是 SSD 儲存層 GiB 數量的三倍，且小於或等於 160,000。

 Note

如需您可以為 FSx for ONTAP 檔案系統佈建之 SSD IOPS 數量上限的詳細資訊，請參閱 [輸送量容量對效能的影響](#)。

8. 選擇更新。

 Note

在提示底部，會顯示新 SSD 儲存容量和 SSD IOPS 的組態預覽。對於第二代檔案系統，也會顯示 per-HA-pair 值。

## 更新檔案系統的 SSD 儲存容量和佈建 IOPS (CLI)

若要更新 FSx for ONTAP 檔案系統的 SSD 儲存容量和佈建 IOPS，請使用 AWS CLI 命令 [update-file-system](#) 或同等的 [UpdateFileSystem](#) API 動作。使用值設定下列參數：

- 將 `--file-system-id` 設定為您要更新之檔案系統的 ID。
- 若要增加 SSD 儲存容量，請將 `--storage-capacity` 設定為目標儲存容量值，該值必須至少大於目前值的 10%。

- 若要修改佈建的 SSD IOPS，請使用 `--ontap-configuration DiskIopsConfiguration` 屬性。此屬性有兩個參數 `Iops` 和 `Mode`：
  - 如果您想要指定佈建 IOPS 的數量，請使用 `Iops=number_of_IOPS`（最多 160,000 個）和 `Mode=USER_PROVISIONED`。IOPS 值必須大於或等於所請求 SSD 儲存容量的三倍。如果您未增加儲存容量，則 IOPS 值必須大於或等於目前 SSD 儲存容量的三倍。
  - 如果您希望 Amazon FSx 自動增加您的 SSD IOPS，請使用 `Mode=AUTOMATIC`，請勿使用 `Iops` 參數。Amazon FSx 會自動維護佈建 SSD 儲存容量的每個 GiB 3 個 SSD IOPS（最多 160,000 個）。

#### Note

如需您可以為 FSx for ONTAP 檔案系統佈建之 SSD IOPS 數量上限的詳細資訊，請參閱 [輸送量容量對效能的影響](#)。

下列範例會將檔案系統的 SSD 儲存體增加至 2000 GiB，並將使用者佈建的 SSD IOPS 數量設定為 7000。

```
aws fsx update-file-system \  
--file-system-id fs-0123456789abcdef0 \  
--storage-capacity 2000 \  
--ontap-configuration 'DiskIopsConfiguration={Iops=7000,Mode=USER_PROVISIONED}'
```

若要監控更新進度，請使用 [describe-file-systems](#) AWS CLI 命令。尋找輸出中的 `AdministrativeActions` 區段。

如需詳細資訊，請參閱《Amazon FSx for NetApp ONTAP API 參考》中的 [AdministrativeAction](#)。

## 動態更新儲存容量

當使用過的 SSD 儲存容量超過您指定的閾值時，您可以使用下列解決方案動態增加 FSx for ONTAP 檔案系統的 SSD 儲存容量。此 AWS CloudFormation 範本會自動部署定義儲存容量閾值所需的所有元件、根據此閾值的 Amazon CloudWatch 警示，以及增加檔案系統儲存容量的 AWS Lambda 函數。

解決方案會自動部署所需的所有元件，並使用下列參數：

- 您的 FSx for ONTAP 檔案系統 ID。
- 使用的 SSD 儲存容量閾值（數值）。這是 CloudWatch 警示將觸發的百分比。
- 增加儲存容量的百分比 (%)。

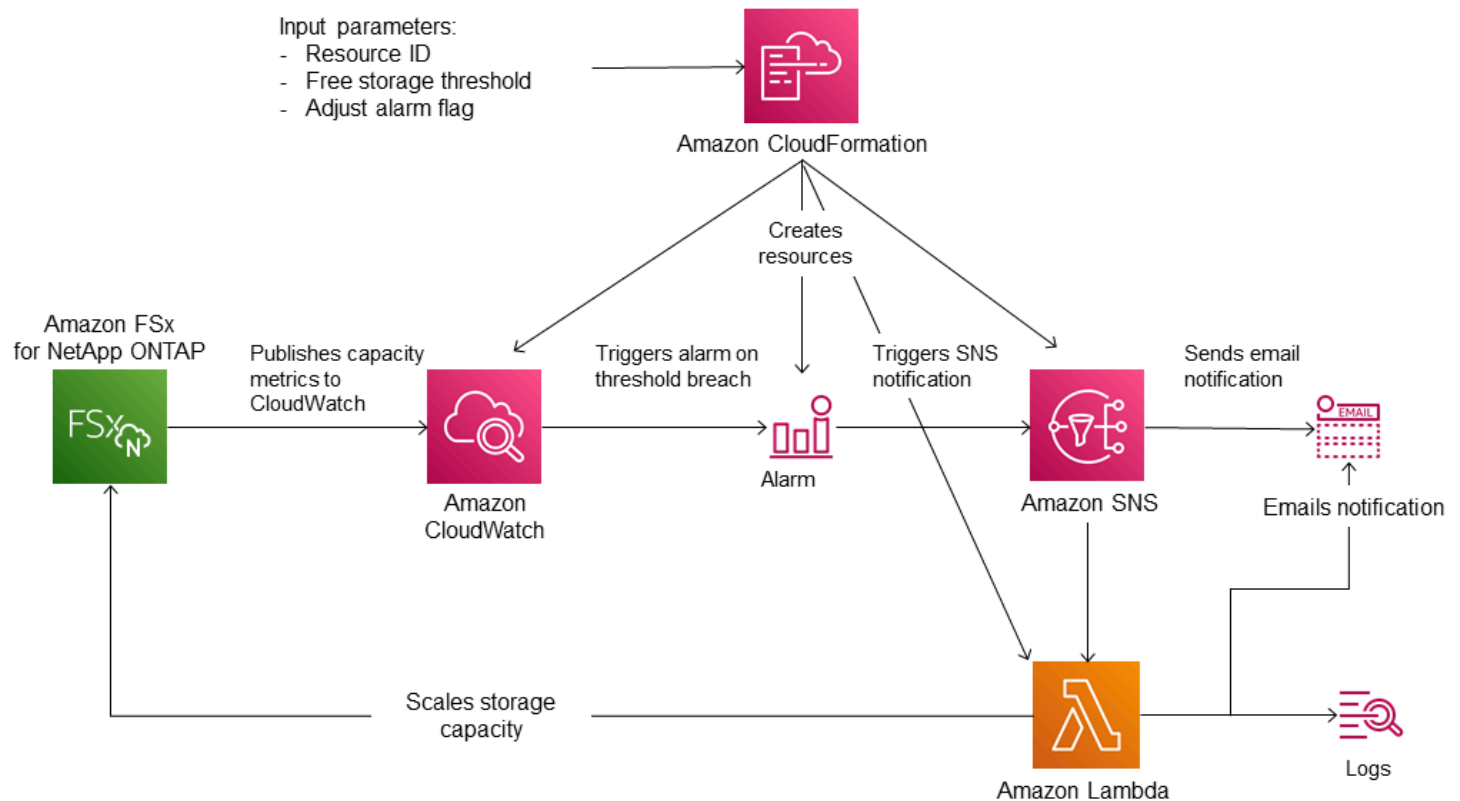
- 用來接收擴展通知的電子郵件地址。

## 主題

- [架構概觀](#)
- [AWS CloudFormation 範本](#)
- [使用 自動部署 AWS CloudFormation](#)

## 架構概觀

部署此解決方案會在 中建置下列資源 AWS 雲端。



此圖說明了下列步驟：

1. AWS CloudFormation 範本會部署 CloudWatch 警示、AWS Lambda 函數、Amazon Simple Notification Service (Amazon SNS) 佇列，以及所有必要 AWS Identity and Access Management (IAM) 角色。IAM 角色提供 Lambda 函數叫用 Amazon FSx API 操作的許可。
2. 當檔案系統使用的儲存容量超過指定的閾值時，CloudWatch 會觸發警示，並將訊息傳送至 Amazon SNS 佇列。只有在檔案系統使用容量持續超過閾值 5 分鐘時，才會觸發警示。
3. 解決方案接著會觸發訂閱此 Amazon SNS 主題的 Lambda 函數。

4. Lambda 函數會根據指定的百分比增加值計算新的檔案系統儲存容量，並設定新的檔案系統儲存容量。
5. 原始 CloudWatch 警示狀態和 Lambda 函數操作的結果會傳送至 Amazon SNS 佇列。

若要接收作為 CloudWatch 警示回應所執行動作的通知，您必須依照訂閱確認電子郵件中提供的連結來確認 Amazon SNS 主題訂閱。

## AWS CloudFormation 範本

此解決方案使用 AWS CloudFormation 自動部署元件，這些元件用於自動增加 FSx for ONTAP 檔案系統的儲存容量。若要使用此解決方案，請下載 [FSxOntapDynamicStorageScaling](#) AWS CloudFormation 範本。

範本使用如下所述的參數。檢閱範本參數及其預設值，並根據檔案系統的需求修改它們。

### FileSystemId

無預設值。您要自動增加儲存容量的檔案系統 ID。

### LowFreeDataStorageCapacityThreshold

無預設值。指定用來觸發警示並自動增加檔案系統的儲存容量的已使用儲存容量閾值，以檔案系統目前儲存容量的百分比 (%) 指定。當使用的儲存超過此閾值時，檔案系統會被視為具有低可用儲存容量。

### EmailAddress

無預設值。指定用於 SNS 訂閱的電子郵件地址，並接收儲存容量閾值警示。

### PercentIncrease

預設為 20%。指定增加儲存容量的數量，以目前儲存容量的百分比表示。

#### Note

每次 CloudWatch 警示進入 ALARM 狀態時，都會嘗試一次儲存體擴展。如果您的 SSD 儲存容量使用率在嘗試儲存擴展操作後仍高於閾值，則不會再次嘗試儲存擴展操作。

### MaxFSxSizeinGiB

預設為 196608。指定 SSD 儲存體支援的最大儲存容量。



## 使用 自動部署 AWS CloudFormation

下列程序會設定和部署 AWS CloudFormation 堆疊，以自動增加 FSx for ONTAP 檔案系統的儲存容量。部署需要幾分鐘的時間。如需建立 CloudFormation 堆疊的詳細資訊，請參閱 AWS CloudFormation 《使用者指南》中的[在 AWS CloudFormation 主控台上建立堆疊](#)。

### Note

實作此解決方案會產生相關聯 AWS 服務的帳單。如需詳細資訊，請參閱這些服務的定價詳細資訊頁面。

開始之前，您必須擁有在 Amazon Virtual Private Cloud (Amazon VPC) 中執行的 Amazon FSx 檔案系統 ID AWS 帳戶。如需建立 Amazon FSx 資源的詳細資訊，請參閱 [Amazon FSx for NetApp ONTAP 入門](#)。

### 啟動自動儲存容量增加解決方案堆疊

1. 下載 [FSxOntapDynamicStorageScaling](#) AWS CloudFormation 範本。

### Note

Amazon FSx 目前僅適用於特定 AWS 區域。您必須在可使用 Amazon FSx 的 AWS 區域中啟動此解決方案。如需詳細資訊，請參閱《》中的 [Amazon FSx 端點和配額](#) AWS 一般參考。

2. 從 AWS CloudFormation 主控台中，選擇建立堆疊 > 使用新資源。
3. 選擇 範本已就緒。在指定範本區段中，選擇上傳範本檔案並上傳您下載的範本。
4. 在指定堆疊詳細資訊中，輸入自動儲存容量增加解決方案的值。

**Stack name**

Stack name

FsxN-Storage-Scaling

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

**Parameters**

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

**Dynamic Storage Scaling Parameters**

**File system ID**  
Amazon FSx file system ID

fs-0123456789abcd

**Threshold**  
Used storage capacity threshold (%)

70

**Percentage Capacity increase**  
The percentage increase in storage capacity when used storage exceeds LowFreeDataStorageCapacityThreshold. Minimum increase is 10 %

20

**Email address**  
The email address for alarm notification.

storagescaler@example.com

**Maximum supported file system storage capacity (DO NOT MODIFY)**  
Maximum size supported for the primary SSD storage tier.

196608

Cancel Previous Next

5. 輸入堆疊名稱。
6. 對於參數，請檢閱範本的參數，並修改它們以符合檔案系統的需求。然後選擇下一步。

 **Note**

若要在此 CloudFormation 範本嘗試擴展時接收電子郵件通知，請確認您在部署範本後收到的 SNS 訂閱電子郵件。

7. 輸入您要用於自訂解決方案的選項設定，然後選擇下一步。
8. 針對檢閱，檢閱並確認解決方案設定。您必須選取確認範本建立 IAM 資源的核取方塊。
9. 選擇建立以部署堆疊。

您可以在狀態欄的 AWS CloudFormation 主控台中檢視堆疊的狀態。您應該會在幾分鐘內看到 CREATE\_COMPLETE 狀態。

## 更新堆疊

建立堆疊之後，您可以使用相同的範本並提供參數的新值來更新堆疊。如需詳細資訊，請參閱AWS CloudFormation 《使用者指南》中的[直接更新堆疊](#)。

## 監控 SSD 儲存體使用率

您可以使用各種 AWS 和 NetApp工具來監控檔案系統的 SSD 儲存容量使用率。使用 Amazon CloudWatch，您可以監控儲存容量使用率，並設定警示，以在儲存容量使用率達到可自訂閾值時提醒您。

### Note

建議您不要超過 SSD 儲存層的 80% 儲存容量使用率。這可確保分層正常運作，並為新資料提供額外負荷。如果您的 SSD 儲存層持續超過 80% 的儲存容量使用率，您可以增加 SSD 儲存層的容量。如需詳細資訊，請參閱[更新檔案系統 SSD 儲存體和 IOPS](#)。

您可以在 Amazon FSx 主控台中檢視檔案系統的可用 SSD 儲存和整體儲存分佈。可用主要儲存容量圖表會顯示檔案系統隨時間的可用 SSD 型儲存容量。儲存分佈圖顯示檔案系統目前如何分佈於 3 個類別：

- 容量集區層
- SSD 層 - 可用
- SSD 層 - 已使用

您可以使用下列程序 AWS Management Console，在 中監控檔案系統的 SSD 儲存容量使用率。

監控檔案系統可用的 SSD 層儲存容量（主控台）

1. 在 Amazon FSx 主控台開啟 <https://console.aws.amazon.com/fsx/>。
2. 選擇左側導覽欄中的檔案系統，然後選擇您要檢視儲存容量資訊ONTAP的檔案系統。檔案系統詳細資訊頁面隨即出現。
3. 在第二個面板中，選擇監控與效能索引標籤，然後選擇儲存。每個彙總圖形會顯示可用的主要儲存容量和儲存容量使用率。

## 監控儲存效率節省

啟用時，您可以在 Amazon FSx 主控台、Amazon CloudWatch 主控台和 ONTAP CLI 中查看要節省多少儲存容量。

### 檢視儲存效率節省（主控台）

FSx for ONTAP 檔案系統在 Amazon FSx 主控台中顯示的儲存效率節省包括 FlexClones 和 Snapshots 的節省。

1. 開啟 Amazon FSx 主控台，網址為 <https://console.aws.amazon.com/fsx/> : //https : //https : //https : //https : ///
2. 從檔案系統清單中選擇您要檢視儲存效率節省的 FSx for ONTAP 檔案系統。
3. 在檔案系統詳細資訊頁面的第二個面板的監控與效能索引標籤中選擇摘要。
4. 儲存效率節省圖表顯示您節省的空間，以邏輯資料大小的百分比和實體位元組表示。

### 檢視儲存效率節省 (ONTAP CLI)

您可以使用 CLI FlexClones 執行 `storage aggregate show-efficiency` 命令，即可查看僅壓縮、壓縮和重複資料刪除的儲存效率節省，而不會影響快照和 ONTAP。如需詳細資訊，請參閱 NetApp ONTAP 文件中心的 [儲存彙總 show-efficiency](#)。

1. 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。*management\_endpoint\_ip* 將取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱 [使用 CLI ONTAP 管理檔案系統](#)。

2. `storage aggregate show-efficiency` 命令會顯示所有彙總儲存效率的相關資訊。儲存效率會顯示在四個不同的層級：
  - 總計
  - Aggregate
  - 資料量
  - 快照和 FlexClone 磁碟區

```
::*> aggr show-efficiency
```

```
Aggregate: aggr1  
Node: node1
```

```
Total Data Reduction Efficiency Ratio: 3.29:1  
Total Storage Efficiency Ratio: 4.29:1  
Aggregate: aggr2  
Node: node1
```

```
Total Data Reduction Efficiency Ratio: 4.50:1  
Total Storage Efficiency Ratio: 5.49:1
```

```
cluster::*> aggr show-efficiency -details
```

```
Aggregate: aggr1  
Node: node1
```

```
Total Data Reduction Ratio: 2.39:1  
Total Storage Efficiency Ratio: 4.29:1
```

```
Aggregate level Storage Efficiency  
(Aggregate Deduplication and Data Compaction): 1.00:1  
Volume Deduplication Efficiency: 5.03:1  
Compression Efficiency: 1.00:1
```

```
Snapshot Volume Storage Efficiency: 8.81:1  
FlexClone Volume Storage Efficiency: 1.00:1  
Number of Efficiency Disabled Volumes: 1
```

```
Aggregate: aggr2  
Node: node1
```

```
Total Data Reduction Ratio: 2.39:1  
Total Storage Efficiency Ratio: 4.29:1
```

```
Aggregate level Storage Efficiency  
(Aggregate Deduplication and Data Compaction): 1.00:1  
Volume Deduplication Efficiency: 5.03:1  
Compression Efficiency: 1.00:1
```

|                                        |        |
|----------------------------------------|--------|
| Snapshot Volume Storage Efficiency:    | 8.81:1 |
| FlexClone Volume Storage Efficiency:   | 1.00:1 |
| Number of Efficiency Disabled Volumes: | 1      |

## 監控儲存容量和 IOPS 更新

您可以使用 Amazon FSx 主控台、CLI 和 API 來監控 SSD 儲存容量和 IOPS 更新的進度。

### 監控儲存體和 IOPS 更新（主控台）

在 FSx for ONTAP 檔案系統的檔案系統詳細資訊頁面上的更新索引標籤中，您可以檢視每個更新類型的 10 個最近更新。

| Updates (2)                                                                                                                           |                |                       |              |                           |
|---------------------------------------------------------------------------------------------------------------------------------------|----------------|-----------------------|--------------|---------------------------|
| <input type="text" value="Filter updates"/> < 1 >  |                |                       |              |                           |
| Update type ▼                                                                                                                         | Target value ▼ | Status ▼              | Progress % ▼ | Request time ▼            |
| Throughput capacity                                                                                                                   | 256            | ✔ Completed           | -            | 2022-03-12T12:16:46-05:00 |
| Storage capacity                                                                                                                      | 1127           | 🕒 Updated; Optimizing | -            | 2022-03-12T12:17:02-05:00 |

對於 SSD 儲存容量和 IOPS 更新，您可以檢視下列資訊：

### 更新類型

支援的類型包括儲存容量、模式和 IOPS。會列出所有儲存容量和 IOPS 擴展請求的模式和 IOPS 值。

### 目標值

您指定用來更新檔案系統 SSD 儲存容量或 IOPS 的值。

### 狀態

更新的目前狀態。可能的值如下：

- 待定 – Amazon FSx 收到更新請求，但尚未開始處理。
- 進行中 – Amazon FSx 正在處理更新請求。
- 已更新；最佳化 – Amazon FSx 增加檔案系統的 SSD 儲存容量。儲存最佳化程序現在正在背景重新平衡您的資料。

- 已完成 – 更新已成功完成。
- 失敗 – 更新請求失敗。選擇問號 (?) 以查看詳細資訊。

進度 %

在百分比完成時顯示儲存最佳化程序的進度。

請求時間

Amazon FSx 收到更新動作請求的時間。

## 監控儲存和 IOPS 更新 (CLI)

您可以使用 [describe-file-systems](#) AWS CLI 命令和 [DescribeFileSystems](#) API 操作來檢視和監控檔案系統 SSD 儲存容量增加請求。AdministrativeActions 陣列會列出每個管理動作類型的 10 個最近更新動作。當您增加檔案系統的 SSD 儲存容量時，會產生兩個AdministrativeActions動作：FILE\_SYSTEM\_UPDATE和 STORAGE\_OPTIMIZATION動作。

下列範例顯示 CLI describe-file-systems 命令回應的摘錄。檔案系統具有待定的管理動作，可將 SSD 儲存容量增加至 2000 GiB，並將佈建的 SSD IOPS 增加至 7000。

```
"AdministrativeActions": [  
  {  
    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",  
    "RequestTime": 1586797629.095,  
    "Status": "PENDING",  
    "TargetFileSystemValues": {  
      "StorageCapacity": 2000,  
      "OntapConfiguration": {  
        "DiskIopsConfiguration": {  
          "Mode": "USER_PROVISIONED",  
          "Iops": 7000  
        }  
      }  
    }  
  },  
  {  
    "AdministrativeActionType": "STORAGE_OPTIMIZATION",  
    "RequestTime": 1586797629.095,  
    "Status": "PENDING"  
  }  
]
```

Amazon FSx 會先處理FILE\_SYSTEM\_UPDATE動作，將新的較大儲存磁碟新增至檔案系統。當新的儲存可供檔案系統使用時，FILE\_SYSTEM\_UPDATE狀態會變更為 UPDATED\_OPTIMIZING。儲存容量會顯示新的較大值，Amazon FSx 會開始處理STORAGE\_OPTIMIZATION管理動作。此行為會顯示在 CLI describe-file-systems 命令回應的下列摘錄中。

ProgressPercent 屬性會顯示儲存最佳化程序的進度。儲存最佳化程序成功完成後，FILE\_SYSTEM\_UPDATE動作的狀態會變更為 COMPLETED，且STORAGE\_OPTIMIZATION動作不會再出現。

```
"AdministrativeActions": [  
  {  
    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",  
    "RequestTime": 1586799169.445,  
    "Status": "UPDATED_OPTIMIZING",  
    "TargetFileSystemValues": {  
      "StorageCapacity": 2000,  
      "OntapConfiguration": {  
        "DiskIopsConfiguration": {  
          "Mode": "USER_PROVISIONED",  
          "Iops": 7000  
        }  
      }  
    }  
  },  
  {  
    "AdministrativeActionType": "STORAGE_OPTIMIZATION",  
    "ProgressPercent": 41,  
    "RequestTime": 1586799169.445,  
    "Status": "IN_PROGRESS"  
  }  
]
```

如果儲存容量或 IOPS 更新請求失敗，FILE\_SYSTEM\_UPDATE動作的狀態會變更為 FAILED，如下列範例所示。FailureDetails 屬性提供失敗的相關資訊。

```
"AdministrativeActions": [  
  {  
    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",  
    "RequestTime": 1586373915.697,  
    "Status": "FAILED",  
    "TargetFileSystemValues": {  
      "StorageCapacity": 2000,  
      "FailureDetails": {  
        "Message": "Storage capacity update failed due to insufficient free space on the disk."  
      }  
    }  
  }  
]
```



```
    "OntapConfiguration": {
      "DiskIopsConfiguration": {
        "Mode": "USER_PROVISIONED",
        "Iops": 7000
      }
    },
    "FailureDetails": {
      "Message": "failure-message"
    }
  }
]
```

## 磁碟區儲存容量

FSx for ONTAP 磁碟區是您用來分組資料的虛擬資源、決定資料的儲存方式，以及決定資料的存取類型。磁碟區就像資料夾一樣，不會自行使用檔案系統儲存容量。只有存放在磁碟區中的資料會耗用 SSD 儲存體，並根據[磁碟區的分層政策](#)，使用容量集區儲存體。您可以在建立磁碟區時設定磁碟區的大小，之後可以變更磁碟區的大小。您可以使用 AWS Management Console、AWS CLI 和 API 以及 ONTAP CLI 來監控和管理 FSx for ONTAP 磁碟區的儲存容量。

### 主題

- [磁碟區資料分層](#)
- [快照和磁碟區儲存容量](#)
- [磁碟區檔案容量](#)
- [管理儲存效率](#)
- [啟用自動調整大小](#)
- [啟用雲端寫入模式](#)
- [更新儲存容量](#)
- [更新分層政策](#)
- [更新最低冷卻天數](#)
- [更新磁碟區的雲端擷取政策](#)
- [更新磁碟區上的檔案數量上限](#)
- [監控磁碟區儲存容量](#)
- [監控磁碟區的檔案容量](#)

## 磁碟區資料分層

Amazon FSx for NetApp ONTAP 檔案系統有兩個儲存層：主要儲存體和容量集區儲存體。主要儲存體是佈建、可擴展且高效能的 SSD 儲存體，專為資料集的作用中部分而打造。容量集區儲存是一個全彈性儲存層，可擴展至 PB 大小，並針對不常存取的資料進行成本最佳化。

每個磁碟區上的資料會根據磁碟區的分層政策、冷卻期間和閾值設定，自動分層至容量集區儲存層。下列各節說明 ONTAP 磁碟區分層政策，以及用於判斷資料何時分層至容量集區的閾值。

### Note

FSx for ONTAP 支援將資料分層到所有 SnapLock 磁碟區的容量集區，無論 SnapLock 類型為何。如需詳細資訊，請參閱[SnapLock 的運作方式](#)。

## 磁碟區分層政策

您可以為檔案系統上的每個磁碟區選擇分層政策，以決定如何使用 FSx for ONTAP 檔案系統的儲存層。您可以在建立磁碟區時選擇分層政策，而且您可以隨時使用 Amazon FSx 主控台、AWS CLI API 或使用 [NetApp 管理工具](#) 進行修改。您可以選擇下列其中一個政策，決定哪些資料會分層到容量集區儲存。

### Note

分層可以將檔案資料和快照資料移至容量集區層。不過，檔案中繼資料一律會保留在 SSD 層。如需詳細資訊，請參閱[如何使用 SSD 儲存體](#)。

- 自動 – 此政策會將所有冷資料—使用者資料和快照—移至容量集區層。資料的冷卻速率取決於政策的冷卻期間，預設為 31 天，並可設定為 2–183 天之間的值。隨機讀取基礎冷資料區塊時（如同一般檔案存取），它們會變得很熱，並寫入主要儲存層。當冷資料區塊循序讀取時（例如，透過防毒掃描），它們會保持冷，並保留在容量集區儲存層上。這是使用 Amazon FSx 主控台建立磁碟區時的預設政策。
- 僅限快照 – 此政策只會將快照資料移至容量集區儲存層。快照分層至容量集區的速率取決於政策的冷卻期間，該期間預設為 2 天，並可設定為 2–183 天之間的值。讀取冷快照資料時，它們會變得很熱，並寫入主要儲存層。這是使用 AWS CLI、Amazon FSx API 或 NetApp ONTAP CLI 建立磁碟區時的預設政策。
- 全部 – 此政策會將所有使用者資料和快照資料標記為冷，並將其存放在容量集區層中。讀取資料區塊時，它們會保持冷，不會寫入主要儲存層。當資料寫入具有所有分層政策的磁碟區時，它最初仍會

寫入 SSD 儲存層，並透過背景程序分層至容量集區。如果所有政策都套用到已包含資料的磁碟區，現有資料會從 SSD 分層到容量集區。請注意，檔案中繼資料一律保留在 SSD 層。

- 無 – 此政策會將磁碟區的所有資料保留在主要儲存層上，並防止其移至容量集區儲存。如果您在使用任何其他政策後將磁碟區設定為此政策，則容量集區儲存體中的現有資料（包括快照）會透過背景程序移至 SSD 儲存體。只有當您的 SSD 使用率低於 90% 且雲端擷取政策設定為 `promote` 或時，才會發生此資料遷移 `on-read`。您可以刻意讀取資料來加速此背景程序。如需詳細資訊，請參閱 [雲端擷取政策](#)。

如需設定或修改磁碟區分層政策的詳細資訊，請參閱 [更新分層政策](#)。

最佳實務是，遷移您計劃長期存放在容量集區儲存中的資料時，建議您在磁碟區上使用自動分層政策。使用自動分層時，資料會在 SSD 儲存層上存放至少 2 天（根據磁碟區的冷卻期間），然後再移至容量集區層。會定期對存放在 SSD 儲存層中的資料 ONTAP 執行後製重複資料刪除，根據磁碟區中的資料變更速率自動調整頻率 - 較高的速率會更頻繁地觸發後製重複資料刪除任務。

根據預設，在 中停用後置程序壓縮，ONTAP 因為它可能會對檔案系統上的持續工作負載產生效能影響。您應該先評估工作負載效能的影響，再啟用後製壓縮。若要啟用程序後壓縮，請在 CLI ONTAP 中擔任診斷權限層級，並執行下列命令：

```
::> volume efficiency inactive-data-compression modify -vserver svm-name -volume vol-name -is-enabled true
```

ONTAP 會對保留在 SSD 儲存體至少 14 天的資料執执行程序後壓縮。對於在較短期間後不太可能存取資料的工作負載，您可以修改後製壓縮設定，以更快地執行後製壓縮。例如，若要將程序後壓縮節省套用到 5 天內未存取的資料，請執行下列 ONTAP CLI 命令：

```
::> volume efficiency inactive-data-compression modify -vserver svm-name -volume vol-name -threshold-days 5 -threshold-days-min 2 -threshold-days-max 14
```

如需 命令的詳細資訊，請參閱磁碟 [區效率inactive-data-compression修改](#)

透過保留 SSD 上的資料，您可以最大限度地提高您建立的磁碟區備份的傳輸速度，因為 SSD 儲存體的資料傳輸率較高。

### 分層冷卻期間

磁碟區的分層冷卻期間會設定 SSD 層中資料標記為冷所需的時間量。冷卻期間適用於 Auto 和 Snapshot-only 分層政策。您可以將冷卻期間設定為 2–183 天範圍內的值。如需設定冷卻期間的詳細資訊，請參閱 [更新最低冷卻天數](#)。

資料會在其冷卻期間到期後 24-48 小時分層。分層是使用網路資源的背景程序，優先順序低於面向用戶端的請求。當有持續面對用戶端的請求時，會調節分層活動。

## 雲端擷取政策

磁碟區的雲端擷取政策會設定條件，指定何時允許從容量集區層讀取的資料提升至 SSD 層。當雲端擷取政策設為 以外的任何項目時Default，此政策會覆寫磁碟區分層政策的擷取行為。磁碟區可以有下列其中一個雲端擷取政策：

- 預設 – 此政策會根據磁碟區的基礎分層政策擷取分層資料。這是所有磁碟區的預設雲端擷取政策。
- 從不 – 此政策永遠不會擷取分層資料，無論讀取是循序還是隨機。這類似於將磁碟區的分層政策設定為全部，但您可以根據最短冷卻期間將它與其他政策 - 自動、僅限快照 - 用於分層資料，而不是立即。
- 讀取中 – 此政策會擷取所有用戶端驅動資料讀取的分層資料。使用所有分層政策時，此政策沒有作用。
- 提升 – 此政策會標記容量集區中的所有磁碟區資料，以擷取至 SSD 層。資料會在下一次執行每日背景分層掃描器時標記。此政策適用於具有不常執行的循環工作負載，但在執行時需要 SSD 層效能的應用程式。使用所有分層政策時，此政策沒有作用。

如需設定磁碟區雲端擷取政策的資訊，請參閱 [更新磁碟區的雲端擷取政策](#)。

## 分層閾值

檔案系統的 SSD 儲存容量使用率會決定 如何ONTAP管理所有磁碟區的分層行為。根據檔案系統的 SSD 儲存容量使用量，下列閾值會如所述設定分層行為。如需如何監控磁碟區 SSD 儲存層容量使用率的資訊，請參閱 [監控磁碟區儲存容量](#)。

### Note

建議您不要超過 SSD 儲存層的 80% 儲存容量使用率。對於第二代檔案系統，此建議同時適用於所有檔案系統彙總的總平均使用率，以及每個個別彙總的使用率。這可確保分層正常運作，並為新資料提供額外負荷。如果您的 SSD 儲存層持續超過 80% 的儲存容量使用率，您可以增加 SSD 儲存層的容量。如需詳細資訊，請參閱[更新檔案系統 SSD 儲存體和 IOPS](#)。

FSx for ONTAP 使用以下儲存容量閾值來管理磁碟區的分層：

- $\leq 50\%$  SSD 儲存層使用率 – 在此閾值下，SSD 儲存層會被視為未充分利用，而且只有使用所有分層政策的磁碟區已將資料分層至容量集區儲存。具有 Auto 和僅限快照政策的磁碟區不會在此閾值分層資料。
- $> 50\%$  SSD 儲存層使用率 – 根據分層最短冷卻天數設定，具有 Auto 和僅限快照分層政策層資料的磁碟區。預設設定為 31 天。
- $\geq 90\%$  SSD 儲存層使用率 – 在此閾值中，Amazon FSx 會優先保留 SSD 儲存層中的空間。使用 Auto 和僅限快照政策讀取磁碟區時，不會再將來自容量集區層的冷資料移至 SSD 儲存層。
- $\geq 98\%$  SSD 儲存層使用率 – 當 SSD 儲存層使用率達到或超過 98% 時，所有分層功能都會停止。您可以繼續從儲存層讀取，但無法寫入層。

## 快照和磁碟區儲存容量

快照是 Amazon FSx for NetApp ONTAP 磁碟區的唯讀影像。快照可保護您磁碟區中的檔案，避免意外刪除或修改。透過快照，您的使用者可以輕鬆地從較早的快照檢視和還原個別檔案或資料夾。

快照會與您的檔案系統資料一起存放，而且會耗用檔案系統的儲存容量。不過，快照只會針對自上次快照以來變更的檔案部分使用儲存容量。檔案系統磁碟區的備份中不包含快照。

您的磁碟區預設會使用預設快照政策來啟用快照。快照會存放在磁碟區根目錄的 `.snapshot` 目錄中。您可以透過下列方式管理快照的磁碟區儲存容量：

- [快照政策](#) – 選取內建快照政策，或選擇您在 ONTAP CLI 或 REST API 中建立的自訂政策。
- [手動刪除快照](#) – 透過手動刪除快照來回收儲存容量。
- [建立快照自動刪除政策](#) – 建立刪除比預設快照政策更多快照的政策。
- [關閉自動快照](#) – 關閉自動快照以節省儲存容量。

如需詳細資訊，請參閱[使用快照保護您的資料](#)。

## 磁碟區檔案容量

Amazon FSx for NetApp ONTAP 磁碟區具有檔案指標，用於存放檔案中繼資料，例如檔案名稱、上次存取時間、許可、大小，以及做為資料區塊的指標。這些檔案指標稱為 Inode，而且每個磁碟區都有無限的 Inode 數量容量，稱為磁碟區檔案容量。當磁碟區在上執行不足或耗盡其可用檔案 (inodes) 時，您無法將其他資料寫入該磁碟區。

檔案系統物件的數量 - 檔案、目錄、快照複本 - 磁碟區可包含的數量取決於它有多少個索引。磁碟區中的索引數量會隨著磁碟區的儲存容量（以及 FlexGroup 磁碟區的磁碟區成分數量）而增加。根據

預設，儲存容量為 648 GiB 或更多的 FlexVol 磁碟區（或 FlexGroup 元件）都有相同數量的 Inode：21, 251, 126。如果您建立大於 648 GiB 的磁碟區，並且希望它具有超過 21, 251, 126 個索引，則必須手動增加索引（檔案）的數量上限。如需檢視磁碟區檔案數量上限的詳細資訊，請參閱 [監控磁碟區的檔案容量](#)。

磁碟區上的預設 Inode 數量為每 32 KiB 磁碟區儲存容量 1 個 Inode，磁碟區大小上限為 648 GiB。對於 1 GiB 磁碟區：

$$\text{Volume\_size\_in\_bytes} \times (1 \text{ 個檔案} \div \text{inode\_size\_in\_bytes}) = \text{maximum\_number\_of\_files}$$
$$1,073,741,824 \text{ 個位元組} \times (1 \text{ 個檔案} \div 32,768 \text{ 個位元組}) = 32,768 \text{ 個檔案}$$

您可以增加磁碟區可以包含的索引數量上限，每 4 KiB 儲存容量最多可以有 1 個索引。對於 1 GiB 磁碟區，會將 32,768 個索引或檔案的數量上限從 32,768 個增加到 262,144 個：

$$1,073,741,824 \text{ 個位元組} \times (1 \text{ 個檔案} \div 4096 \text{ 個位元組}) = 262,144 \text{ 個檔案}$$

ONTAP 磁碟區的 FSx 最多可以有 20 億個節點。

如需變更磁碟區可存放檔案數量上限的資訊，請參閱 [更新磁碟區上的檔案數量上限](#)。

## 管理儲存效率

透過在 FSx for ONTAP 磁碟區上啟用儲存效率，您可以最佳化儲存使用率、降低儲存成本，並改善檔案系統的整體效能。

ONTAP 會將檔案整理成 4 KB (KiB) 的資料區塊。儲存效率是在資料區塊層級而非個別檔案層級進行。啟用儲存效率時，ONTAP 採用資料縮減技術組合來消除重複的資料、壓縮資料大小，以及重新組織資料配置，以獲得最佳磁碟使用率。

儲存效率的套用方式有兩種。它們會套用至內嵌資料（在資料寫入磁碟之前，在記憶體中），以立即節省儲存成本。它們也會透過定期效率任務套用至 SSD 儲存層背景中的資料（在資料寫入磁碟之後），以隨著時間最佳化儲存使用率。背景儲存效率在分層至容量集區之後，不會在資料上執行。不過，如果資料在 SSD 中有任何儲存節省，則在資料分層至容量集區時，會保留這些節省。

### Note

ONTAP 不支援啟用資料保護 (DP) 磁碟區的儲存效率。不過，當資料複寫至目的地 DP 磁碟區時，會保留來源可讀寫入 (RW) 磁碟區中達到的儲存節省。



## 資料區塊的壓縮

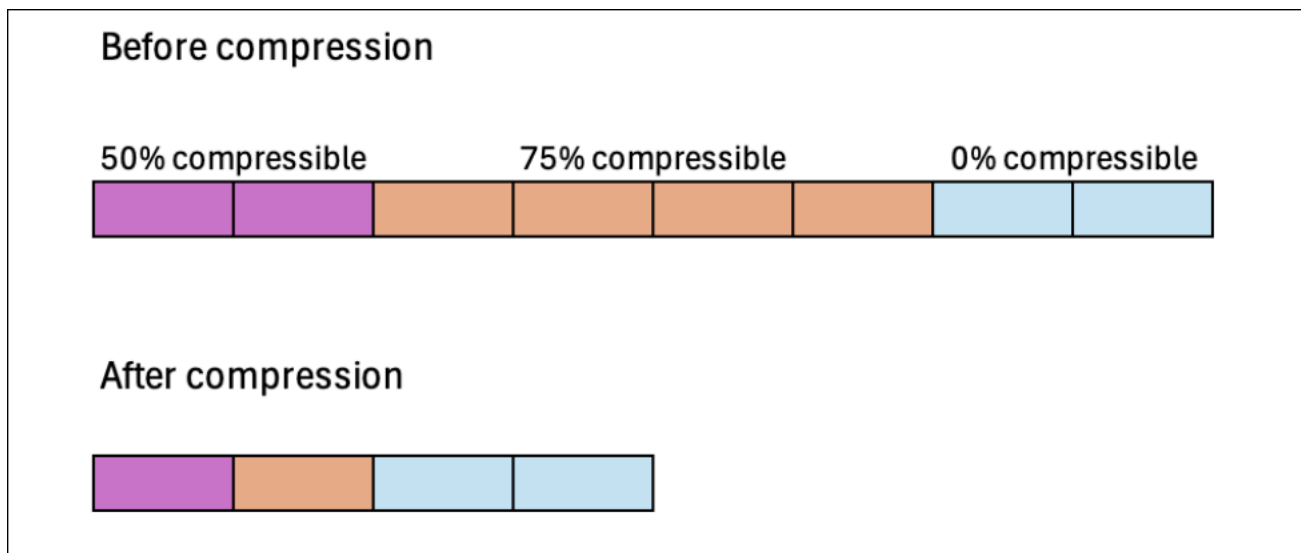
壓縮群組是以單一區塊形式管理和壓縮在一起的資料邏輯分組。ONTAP會自動將資料區塊封裝到壓縮群組中，以減少磁碟上耗用的空間。為了最佳化效能和儲存使用率，會根據資料存取模式調整套用到資料的壓縮程度，ONTAP提供管理資料的平衡方法。

根據預設，資料會使用 8 KB 壓縮群組進行內嵌壓縮，以確保將資料寫入磁碟區時的最佳效能。或者，您可以在磁碟區上啟用非作用中的資料壓縮，以進一步壓縮 SSD 中的資料，藉此將較重的壓縮套用到資料。非作用中資料壓縮會在冷資料上使用 32 KB 壓縮群組，以節省額外的儲存空間。如需詳細資訊，請參閱 中的 [volume efficiency inactive-data-compression modify](#) 命令NetApp ONTAP Documentation Center。

### Note

非作用中資料壓縮會耗用額外的 CPU 和磁碟 IOPS，而且可以是資源密集型任務。建議您在啟用此功能之前，先評估對工作負載執行非作用中資料壓縮的效能影響。

下圖說明可透過壓縮資料區塊達成的儲存節省。



## 重複資料區塊的刪除

ONTAP 會偵測並消除重複的資料區塊，以減少資料中的冗餘。重複的區塊會取代為共用唯一區塊的參考。

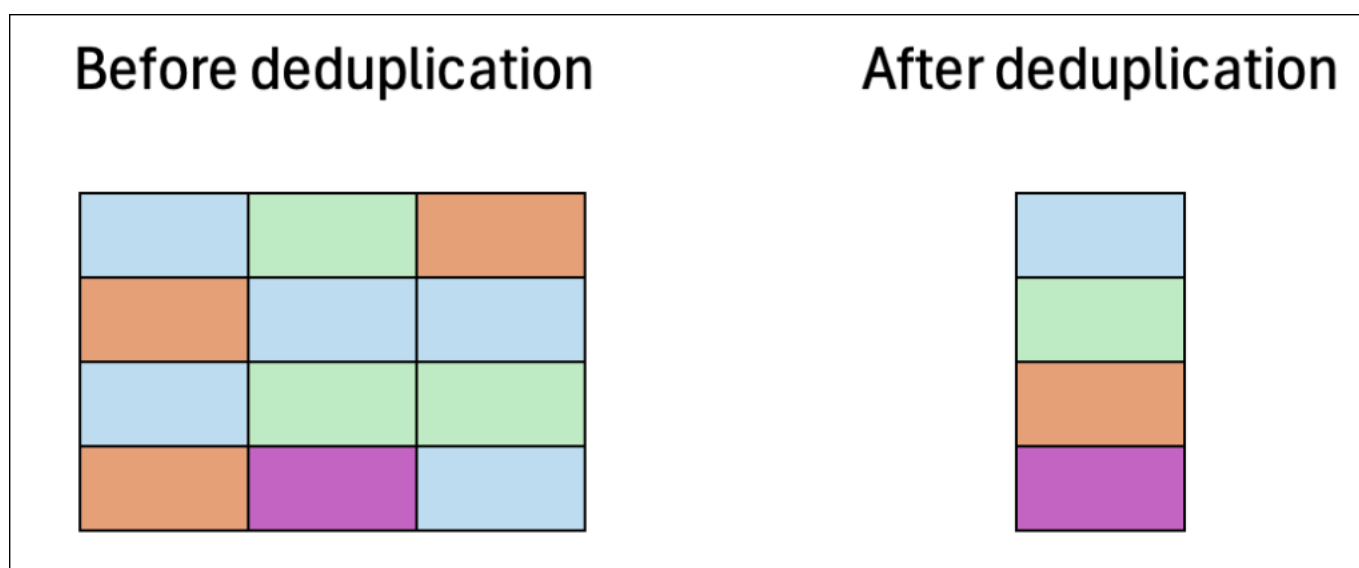
根據預設，資料會在寫入磁碟之前內嵌刪除重複資料，以減少儲存體使用量。ONTAP也會以指定的間隔執行背景刪除重複資料掃描器，以在寫入磁碟後識別並消除重複資料。在這些排定的掃描期間，會

ONTAP處理變更日誌，以識別自上次掃描以來尚未刪除重複資料的新資料區塊或修改的資料區塊。找到重複項目時，會ONTAP更新中繼資料以指向重複區塊的單一複本，並將備援區塊標記為已準備好回收的可用空間。

**Note**

ONTAP 一次將重複資料刪除套用至 4 KB 的傳入寫入，因此在執行大小小於 4 KB 的寫入工作負載時，可能會節省較低的重複資料刪除成本。  
FSx for ONTAP 不支援跨磁碟區重複資料刪除。

下圖說明可透過重複資料刪除實現的儲存節省。



### 壓縮資料區塊

ONTAP 會將每個小於 4 KB 的部分填充資料區塊合併為更有效率使用的 4 KB 區塊。

根據預設，資料會內嵌壓縮，以在寫入磁碟時最佳化資料配置，以將儲存開銷降至最低、減少分段並改善讀取效能。

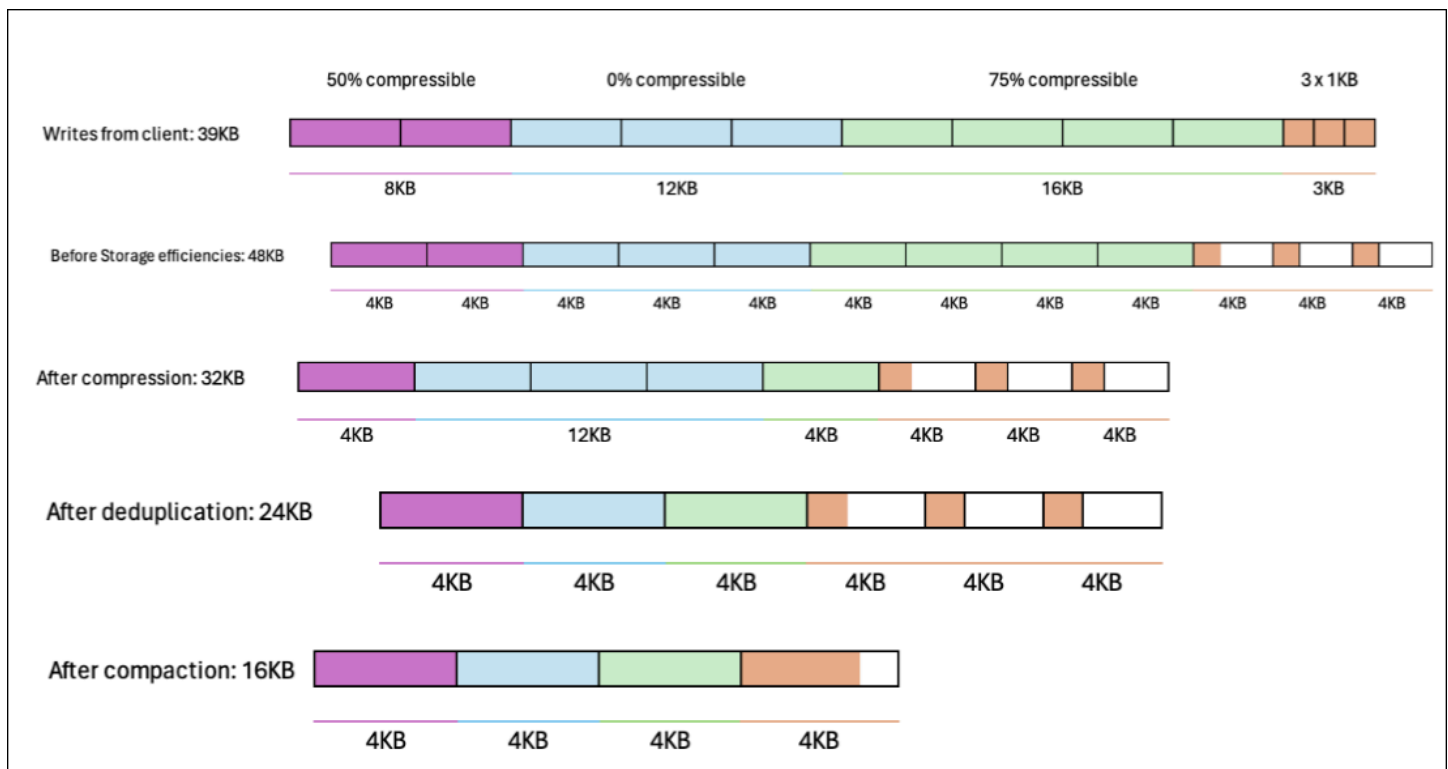
下圖說明可透過壓縮實現的儲存節省。





### 範例：儲存效率

下圖說明如何將儲存效率套用至資料。



### 啟用自動調整大小

磁碟區自動調整大小，讓磁碟區在達到使用的空間閾值時自動成長到指定的大小。您可以使用 ONTAP CLI 命令對 FlexVol 磁碟區類型 (FSx for ONTAP 的預設磁碟區類型) [volume autosize](#) 執行此操作。

#### 啟用磁碟區自動調整大小 (ONTAP CLI)

- 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。*management\_endpoint\_ip* 將取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

2. 如所示使用 `volume autosize` 命令，取代下列值：

- *svm\_name* 將取代為磁碟區建立所在的 SVM 名稱。
- *vol\_name* 將取代為您要調整大小的磁碟區名稱。
- *grow\_threshold* 以使用的空間百分比值（例如 90）取代，其中磁碟區會自動增加大小（最高為 *max\_size* 值）。
- *max\_size* 將取代為磁碟區可成長的大小上限。使用格式 *integer*[KB|MB|GB|TB|PB]，例如 300TB。大小上限為 300 TB。預設值為磁碟區大小的 120%。
- 將 *min\_size* 取代為磁碟區將縮減的最小大小。使用與 *max\_size* 相同的格式。
- 將 *shrink\_threshold* 取代為磁碟區會自動縮減大小的已用空間百分比。

```
::> volume autosize -vserver svm_name -volume vol_name -mode grow_shrink -  
grow-threshold-percent grow_threshold -maximum-size max_size -shrink-threshold-  
percent shrink_threshold -minimum-size min_size
```

3. 若要顯示目前的自動調整大小設定，請執行下列命令。將 *svm\_name* 和 *vol\_name* 取代為您的資訊。

```
::> volume autosize -vserver svm_name -volume vol_name
```

## 啟用雲端寫入模式

使用 `volume modify` ONTAP CLI 命令來啟用或停用現有磁碟區的雲端寫入模式。如需詳細資訊，請參閱 NetApp ONTAP 文件中心[volume modify](#)中的。

設定雲端寫入模式的先決條件為：

- 磁碟區必須是現有的磁碟區。您只能在現有磁碟區上啟用功能。
- 磁碟區必須是讀寫 (RW) 磁碟區。
- 磁碟區必須具有所有分層政策。如需修改磁碟區分層政策的詳細資訊，請參閱[更新分層政策](#)。

雲端寫入模式適用於遷移等情況，例如，使用 NFS 通訊協定將大量資料傳輸到檔案系統的情況。

### 設定磁碟區的雲端寫入模式 (ONTAP CLI)

- 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。*management\_endpoint\_ip* 將取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

- 使用以下命令進入 ONTAP CLI 進階模式。

```
FSx::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y
```

- 使用下列命令來設定磁碟區的雲端寫入模式，並取代下列值：

- svm\_name* 將取代為磁碟區建立所在的 SVM 名稱。
- vol\_name* 將取代為您設定雲端寫入模式的磁碟區名稱。
- vol\_cw\_mode* 將取代為 true 以在磁碟區上啟用雲端寫入模式，或 false 將其停用。

```
FSx::> volume modify -vserver svm_name -volume vol_name -is-cloud-write-
enabled vol_cw_mode
```

系統會回應成功的請求，如下所示。

```
Volume modify successful on volume vol_name of Vserver svm_name.
```

## 更新儲存容量

您可以使用 AWS Management Console、AWS CLI API 和 ONTAP CLI，手動增加或減少磁碟區大小來管理磁碟區儲存容量。您也可以啟用磁碟區自動調整大小，讓磁碟區大小在達到特定使用過的儲存容量閾值時自動成長或縮小。您可以使用 ONTAP CLI 來管理磁碟區自動調整大小。

## 變更磁碟區的儲存容量（主控台）

- 您可以使用 Amazon FSx 主控台 AWS CLI 和 API 來增加或減少磁碟區的儲存容量。如需詳細資訊，請參閱[更新磁碟區](#)。

您也可以使用 ONTAP CLI，使用 `volume modify` 命令修改磁碟區的儲存容量。

### 修改磁碟區的大小 (ONTAP CLI)

- 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。`management_endpoint_ip` 將取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

- 使用 `volume modify` ONTAP CLI 命令來修改磁碟區的儲存容量。執行下列命令，使用您的資料取代下列值：
- `svm_name` 將取代為磁碟區建立所在的儲存虛擬機器 (SVM) 名稱。
  - `vol_name` 以您要調整大小的磁碟區名稱取代。
  - `vol_size` 以格式為 的新磁碟區大小取代 `integer`[KB|MB|GB|TB|PB]；例如，100GB 將磁碟區大小增加到 100 GB。

```
::> volume modify -vserver svm_name -volume vol_name -size vol_size
```

## 更新分層政策

您可以使用 AWS Management Console、AWS CLI API 和 ONTAP CLI 來修改磁碟區的分層政策。

### 修改磁碟區的資料分層政策（主控台）

使用下列程序來修改磁碟區的資料分層政策 AWS Management Console。

- 在 <https://console.aws.amazon.com/fsx/>：// 開啟 Amazon FSx 主控台。
- 在左側導覽窗格中選擇磁碟區，然後選擇您要修改資料分層政策的 ONTAP 磁碟區。
- 從動作下拉式選單中選擇更新磁碟區。更新磁碟區視窗隨即出現。

4. 針對容量集區分層政策，選擇磁碟區的新政策。如需詳細資訊，請參閱[磁碟區分層政策](#)。
5. 選擇更新，將新政策套用至磁碟區。

### 設定磁碟區的分層政策 (CLI)

- 使用 [update-volume](#) CLI 命令修改磁碟區的分層政策 ([UpdateVolume](#) 是對等的 Amazon FSx API 動作)。下列 CLI 命令範例會將磁碟區的資料分層政策設定為 SNAPSHOT\_ONLY。

```
aws fsx update-volume \  
  --volume-id fsxvol-abcde0123456789f \  
  --ontap-configuration TieringPolicy={Name=SNAPSHOT_ONLY}
```

對於成功的請求，系統會以磁碟區描述來回應。

```
{  
  "Volume": {  
    "CreationTime": "2021-10-05T14:27:44.332000-04:00",  
    "FileSystemId": "fs-abcde0123456789f",  
    "Lifecycle": "CREATED",  
    "Name": "vol1",  
    "OntapConfiguration": {  
      "FlexCacheEndpointType": "NONE",  
      "JunctionPath": "/vol1",  
      "SecurityStyle": "UNIX",  
      "SizeInMegabytes": 1048576,  
      "StorageEfficiencyEnabled": true,  
      "StorageVirtualMachineId": "svm-abc0123de456789f",  
      "StorageVirtualMachineRoot": false,  
      "TieringPolicy": {  
        "CoolingPeriod": 2,  
        "Name": "SNAPSHOT_ONLY"  
      },  
      "UUID": "aaaa1111-bb22-cc33-dd44-abcde01234f5",  
      "OntapVolumeType": "RW"  
    },  
    "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-  
abcde0123456789f/fsvol-abc012def3456789a",  
    "VolumeId": "fsvol-abc012def3456789a",  
    "VolumeType": "ONTAP"  
  }  
}
```

## 修改磁碟區的分層政策 (ONTAP CLI)

您可以使用 `volume modify` ONTAP CLI 命令來設定磁碟區的分層政策。如需詳細資訊，請參閱 NetApp ONTAP 文件中心[volume modify](#)中的。

1. 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。`management_endpoint_ip` 將取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

2. 使用以下命令進入 ONTAP CLI 進階模式。

```
FSx::> set adv
```

```
Warning: These advanced commands are potentially dangerous; use them only when  
directed to do so by NetApp personnel.
```

```
Do you want to continue? {y|n}: y
```

3. 使用下列命令來修改磁碟區資料分層政策，並取代下列值：

- `svm_name` 將取代為磁碟區建立所在的 SVM 名稱。
- `vol_name` 將取代為您設定資料分層政策的磁碟區名稱。
- 將取代`tiering_policy`為所需的政策。有效值為 `snapshot-only`、`auto`、`all` 或 `none`。如需詳細資訊，請參閱[磁碟區分層政策](#)。

```
FSx::> volume modify -vserver svm_name -volume vol_name -tiering-  
policy tiering_policy
```

## 更新最低冷卻天數

磁碟區的最短冷卻天數會設定閾值，用於判斷哪些資料是暖和的，哪些資料是冷的。您可以使用 AWS CLI 和 API 以及 ONTAP CLI 來設定磁碟區的最短冷卻天數。

## 設定磁碟區的最短冷卻天數 (CLI)

- 使用 [update-volume](#) CLI 命令修改磁碟區組態 ([UpdateVolume](#) 是同等的 Amazon FSx API 動作)。下列 CLI 命令範例會將磁碟區的 CoolingPeriod 設定為 104 天。

```
aws fsx update-volume \  
  --volume-id fsxvol-abcde0123456789f \  
  --ontap-configuration TieringPolicy={Name=SNAPSHOT_ONLY}  
aws fsx update-volume --volume-id fsvol-006530558c14224ac --ontap-configuration  
  TieringPolicy={CoolingPeriod=104}
```

系統會回應成功請求的磁碟區描述。

```
{  
  "Volume": {  
    "CreationTime": "2021-10-05T14:27:44.332000-04:00",  
    "FileSystemId": "fs-abcde0123456789f",  
    "Lifecycle": "CREATED",  
    "Name": "vol1",  
    "OntapConfiguration": {  
      "FlexCacheEndpointType": "NONE",  
      "JunctionPath": "/vol1",  
      "SecurityStyle": "UNIX",  
      "SizeInMegabytes": 1048576,  
      "StorageEfficiencyEnabled": true,  
      "StorageVirtualMachineId": "svm-abc0123de456789f",  
      "StorageVirtualMachineRoot": false,  
      "TieringPolicy": {  
        "CoolingPeriod": 104,  
        "Name": "SNAPSHOT_ONLY"  
      },  
      "UUID": "aaaa1111-bb22-cc33-dd44-abcde01234f5",  
      "OntapVolumeType": "RW"  
    },  
    "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-  
abcde0123456789f/fsvol-abc012def3456789a",  
    "VolumeId": "fsvol-abc012def3456789a",  
    "VolumeType": "ONTAP"  
  }  
}
```

## 設定磁碟區的最短冷卻天數 (ONTAP CLI)

使用 `volume modify` ONTAP CLI 命令來設定現有磁碟區的冷卻天數下限。如需詳細資訊，請參閱 NetApp ONTAP 文件中心[volume modify](#)中的。

1. 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。*management\_endpoint\_ip* 將取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

2. 使用下列命令進入 ONTAP CLI 進階模式。

```
FSx::> set adv
```

```
Warning: These advanced commands are potentially dangerous; use them only when  
directed to do so by NetApp personnel.
```

```
Do you want to continue? {y|n}: y
```

3. 使用下列命令來變更磁碟區的分層最短冷卻天數，並取代下列值：

- *svm\_name* 將取代為磁碟區建立所在的 SVM 名稱。
- *vol\_name* 將取代為您設定冷卻日的磁碟區名稱。
- *cooling\_days* 將取代為所需的整數，介於 2-183 之間。

```
FSx::> volume modify -vserver svm_name -volume vol_name -tiering-minimum-cooling-  
days cooling_days
```

系統會回應成功的請求，如下所示。

```
Volume modify successful on volume vol_name of Vserver svm_name.
```

## 更新磁碟區的雲端擷取政策

使用 `volume modify` ONTAP CLI 命令來設定現有磁碟區的雲端擷取政策。如需詳細資訊，請參閱 NetApp ONTAP 文件中心[volume modify](#)中的。



## 設定磁碟區的雲端擷取政策 (ONTAP CLI)

- 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。*management\_endpoint\_ip* 將取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

- 使用下列命令進入 ONTAP CLI 進階模式。

```
FSx::> set adv
```

```
Warning: These advanced commands are potentially dangerous; use them only when  
directed to do so by NetApp personnel.
```

```
Do you want to continue? {y|n}: y
```

- 使用下列命令來設定磁碟區的雲端擷取政策，並取代下列值：

- svm\_name* 將取代為磁碟區建立所在的 SVM 名稱。
- vol\_name* 將取代為您設定雲端擷取政策的磁碟區名稱。
- retrieval\_policy* 將取代為所需的值，default、never、on-read或 promote。

```
FSx::> volume modify -vserver svm_name -volume vol_name -cloud-retrieval-  
policy retrieval_policy
```

系統會回應成功的請求，如下所示。

```
Volume modify successful on volume vol_name of Vserver svm_name.
```

## 更新磁碟區上的檔案數量上限

FSx for ONTAP 磁碟區在用盡可用節點或檔案指標的數量時，可能會耗盡檔案容量。

### 若要增加磁碟區上的檔案數量上限 (ONTAP CLI)

您可以使用 volume modify ONTAP CLI 命令來增加磁碟區上的檔案數量上限。如需詳細資訊，請參閱 NetApp ONTAP 文件中心[volume modify](#)中的。

- 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。*management\_endpoint\_ip* 將取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

- 根據使用案例執行以下其中一項操作。將 *svm\_name* 和 *vol\_name* 取代為您的值。
  - 若要將磁碟區設定為一律具有可用的檔案 (inodes) 數目上限，請執行下列動作：
    - 使用下列命令，在 ONTAP CLI 中輸入進階模式。

```
::> set adv
```

- 執行此命令後，您會看到此輸出。輸入 y 以繼續。

```
Warning: These advanced commands are potentially dangerous; use them only
when
directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y
```

- 輸入下列命令以一律使用磁碟區上的檔案數量上限：

```
::> volume modify -vserver svm_name -volume vol_name -files-set-maximum true
```

- 若要使用 手動指定磁碟區上允許的檔案總數 *max\_number\_files* = (current\_size\_of\_volume) × (1 file ÷ 4 KiB)，最大可能值為 20 億，請使用下列命令：

```
::> volume modify -vserver svm_name -volume vol_name -files max_number_files
```

## 監控磁碟區儲存容量

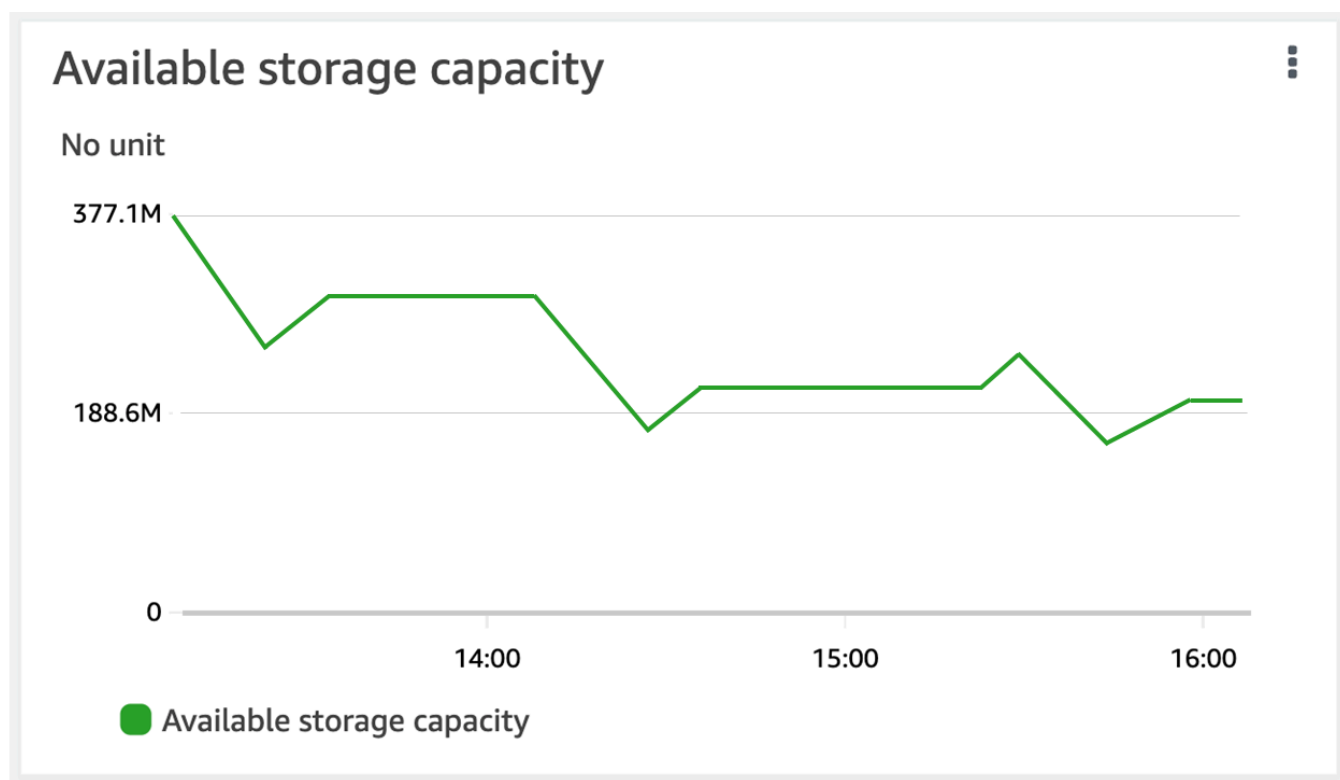
您可以檢視磁碟區的可用儲存體及其儲存分佈 AWS Management Console AWS CLI，以及 NetApp ONTAP CLI。

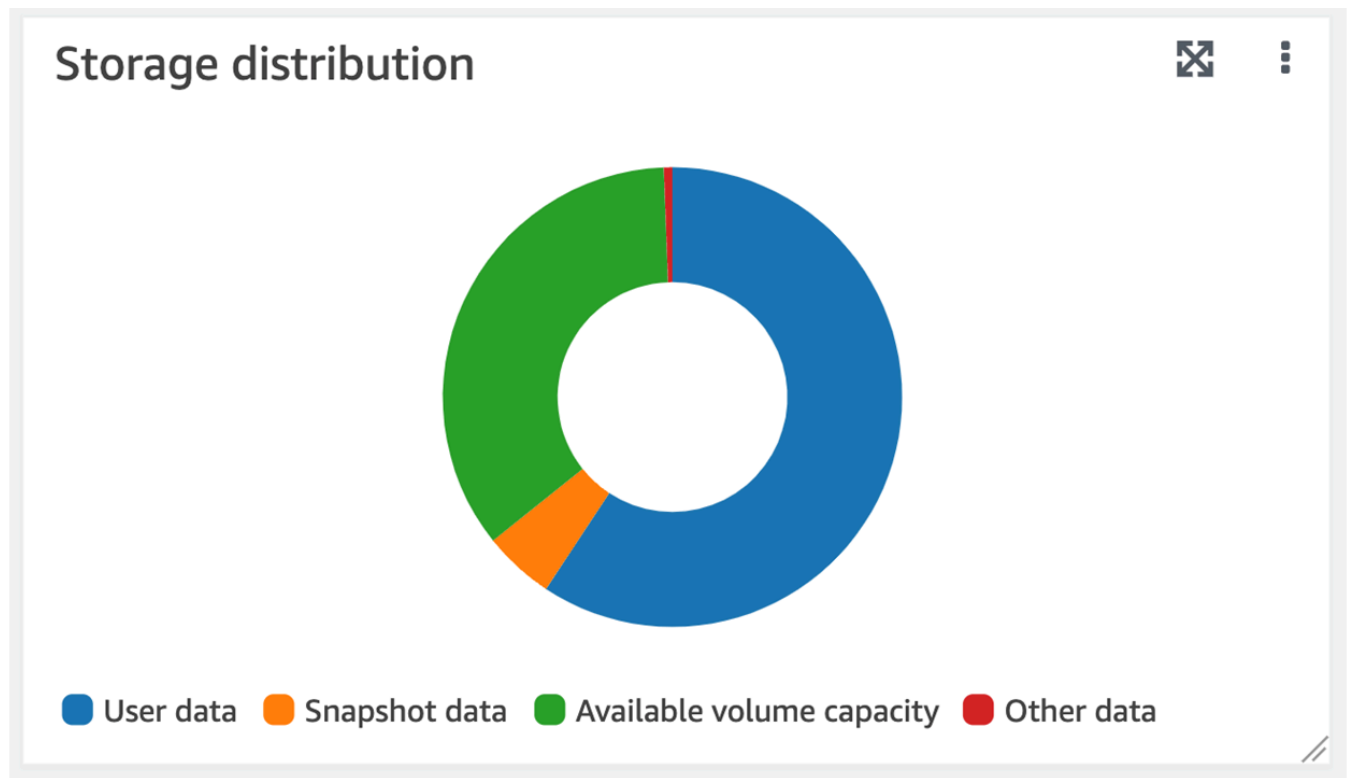
## 監控磁碟區的儲存容量（主控台）

可用儲存圖表會顯示一段時間內磁碟區上的可用儲存容量。儲存分佈圖顯示磁碟區的儲存容量目前如何分佈於 4 個類別：

- 使用者資料
- 快照資料
- 可用的磁碟區容量
- 其他資料

1. 開啟位於 <https://console.aws.amazon.com/fsx/> 的 Amazon FSx 主控台。
2. 在左側導覽欄中選擇磁碟區，然後選擇您要檢視儲存容量資訊的 ONTAP 磁碟區。磁碟區詳細資訊頁面隨即出現。
3. 在第二個面板中，選擇監控索引標籤。顯示可用的儲存和儲存分佈圖表，以及數個其他圖表。





## 監控磁碟區的儲存容量 (ONTAP CLI)

您可以使用 CLI `volume show-space` ONTAP 命令來監控磁碟區的儲存容量使用情形。如需詳細資訊，請參閱 NetApp ONTAP 文件中心[volume show-space](#)中的。

- 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。*management\_endpoint\_ip* 將取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

- 透過發出下列命令來檢視磁碟區的儲存容量用量，並取代下列值：

- svm\_name* 將取代為磁碟區建立所在的 SVM 名稱。
- vol\_name* 將取代為您設定資料分層政策的磁碟區名稱。

```
::> volume show-space -vserver svm_name -volume vol_name
```

如果命令成功，您會看到類似以下的輸出：

```
Vserver : svm_name
Volume  : vol_name
Feature                                Used          Used%
-----
User Data                             140KB          0%
Filesystem Metadata                   164.4MB        1%
Inodes                               10.28MB        0%
Snapshot Reserve                      563.2MB        5%
Deduplication                         12KB          0%
Snapshot Spill                        9.31GB        85%
Performance Metadata                  668KB          0%

Total Used                            10.03GB        91%

Total Physical Used                   10.03GB        91%
```

此命令的輸出會顯示此磁碟區上不同類型的資料佔用的實體空間量。它也會顯示每種資料類型所耗用的總磁碟區容量百分比。在此範例中，Snapshot Spill和Snapshot Reserve會耗用合併的 90% 磁碟區容量。

Snapshot Reserve 顯示儲存快照複本的預留磁碟空間量。如果快照複製儲存體超過預留空間，則會溢出到檔案系統，此數量會顯示在下Snapshot Spill。

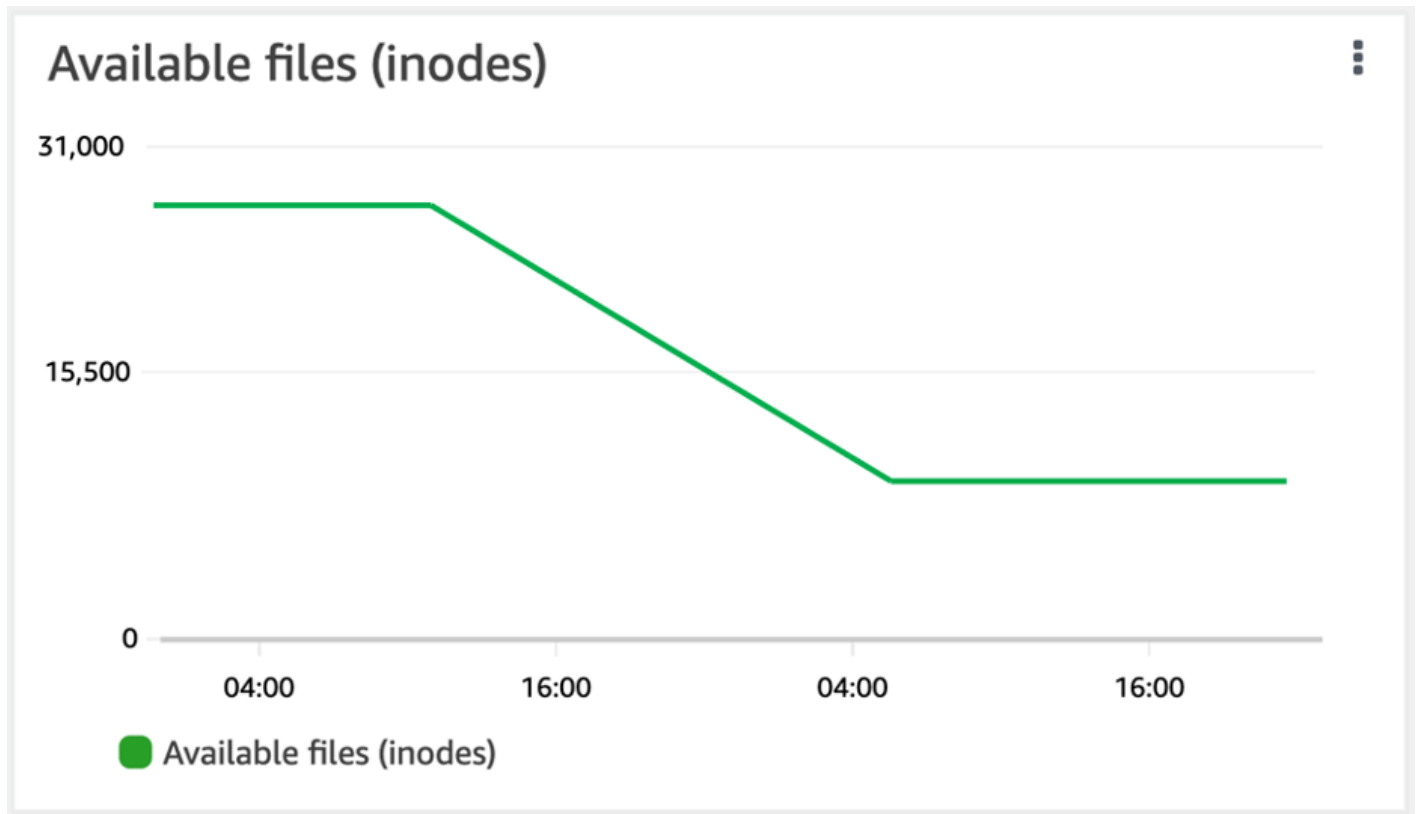
若要增加可用空間量，您可以[增加磁碟區的大小](#)，也可以[刪除未使用的快照](#)，如下列程序所示。

對於 FlexVol 磁碟區類型 (FSx for ONTAP 磁碟區的預設磁碟區類型)，您也可以啟用[磁碟區自動調整大小](#)。當您啟用自動調整大小時，磁碟區大小會在達到特定閾值時自動增加。您也可以停用自動快照。以下各節將說明這兩種功能。

## 監控磁碟區的檔案容量

您可以使用下列其中一種方法來檢視允許的檔案數目上限，以及磁碟區上已使用的檔案數目。

- CloudWatch 磁碟區指標 FilesCapacity和 FilesUsed。
- 在 Amazon FSx 主控台中，導覽至磁碟區的監控索引標籤中的可用檔案 (inodes) 圖表。下圖顯示磁碟區上的可用檔案 (inodes) 隨時間減少。



## 管理 FSx for ONTAP 檔案系統

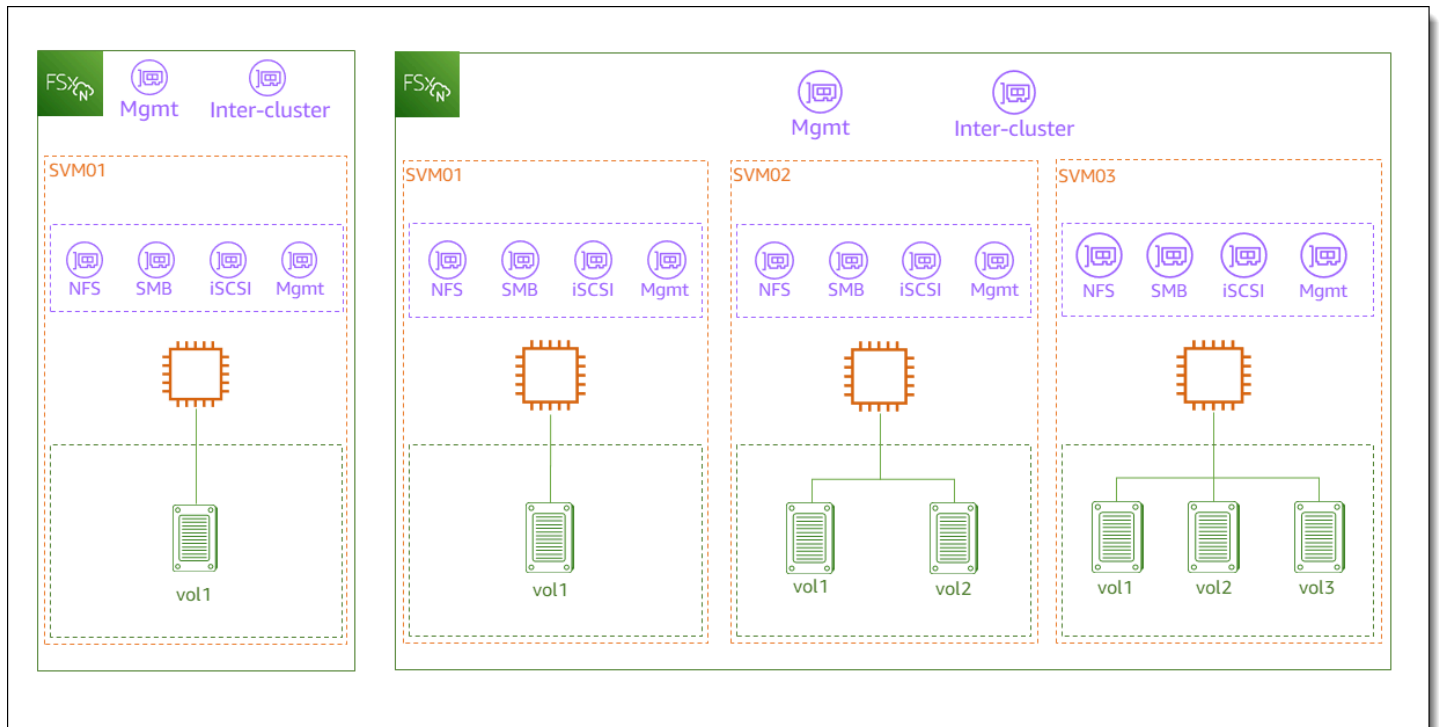
檔案系統是主要的 Amazon FSx 資源，類似於內部部署 ONTAP 叢集。您可以指定檔案系統的固態硬碟 (SSD) 儲存容量和輸送量容量，然後選擇要在其中建立檔案系統的虛擬私有雲端 (VPC)。每個檔案系統都有一個管理端點，您可以使用它來管理使用 ONTAP CLI 或 REST API 的資源和資料。

### 檔案系統資源

Amazon FSx for NetApp ONTAP 檔案系統由下列主要資源組成：

- 檔案系統本身的實體硬體，其中包含檔案伺服器和儲存媒體。
- 一或多個高可用性 (HA) 檔案伺服器對，用於託管您的儲存虛擬機器 SVMs)。第一代檔案系統和多可用區域第二代檔案系統有一個 HA 對，第二代單一可用區域檔案系統最多有 12 個 HA 對。每個 HA 對都有稱為 彙總的儲存集區。所有 HA 對的彙總集合構成您的 SSD 儲存層。
- 託管檔案系統磁碟區的一或多個 SVMs，並擁有自己的登入資料和存取管理。
- 一或多個磁碟區，可虛擬整理您的資料，並由您的用戶端掛載。

下圖說明第一代 FSx for ONTAP 檔案系統的架構，以及其主要資源之間的關係。左側的 FSx for ONTAP 檔案系統是最簡單的檔案系統，具有一個 SVM 和一個磁碟區。右側的檔案系統具有多個 SVMs，有些 SVMs 具有多個磁碟區。檔案系統和 SVMs 各有多個管理端點，而 SVMs 也有資料存取端點。



建立 FSx for ONTAP 檔案系統時，您可以定義下列屬性：

- **部署類型** – 檔案系統的部署類型（多可用區或單一可用區）。單一可用區檔案系統會複寫您的資料，並在單一可用區域內提供自動容錯移轉。第一代單一可用區檔案系統支援一個 HA 對。第二代單一可用區檔案系統最多支援 12 個 HA 對。多可用區域檔案系統透過同時複寫您的資料，並支援在相同內的多個可用區域進行容錯移轉，來提供更高的彈性 AWS 區域。第一代和第二代多可用區域檔案系統都支援一個 HA 對。

#### Note

您無法在建立後變更檔案系統的部署類型。如果您想要變更部署類型（例如，從單一可用區 1 移至單一可用區 2），您可以備份資料，並將其還原到新的檔案系統。您也可以使用 NetApp SnapMirror、AWS DataSync 或第三方資料複製工具來遷移資料。如需詳細資訊，請參閱 [使用 NetApp SnapMirror 遷移至 FSx for ONTAP](#) 及 [使用 遷移至 FSx for ONTAP AWS DataSync](#)。

- 儲存容量 – 這是 SSD 儲存量，第一代檔案系統高達 192 TB (TiB)，第二代多可用區域檔案系統高達 512 TiB，第二代單一可用區域檔案系統高達 1 PB (PiB)。
- SSD IOPS – 根據預設，每個 GB 的 SSD 儲存體包含三個 SSD IOPS（最高可達檔案系統組態支援的最大數量）。您可以視需要選擇性地佈建額外的 SSD IOPS。
- 輸送量容量 – 檔案伺服器可以提供資料的持續速度。
- 網路 – 檔案系統建立之管理和資料存取端點的 VPC 和子網路。對於多可用區檔案系統，您也可以定義 IP 地址範圍和路由表。
- Encryption – 用來加密靜態檔案系統資料的 AWS Key Management Service (AWS KMS) 金鑰。
- 管理存取 – 您可以指定 `fsxadmin` 使用者的密碼。您可以使用此使用者，透過 NetApp ONTAP CLI 和 REST API 來管理檔案系統。

您可以使用 NetApp ONTAP CLI 或 REST API 來管理 FSx for ONTAP 檔案系統。您也可以在 Amazon FSx 檔案系統與另一個 ONTAP 部署（包括另一個 Amazon FSx 檔案系統）之間設定 SnapMirror 或 SnapVault 關係。每個 FSx for ONTAP 檔案系統都有下列檔案系統端點，提供 NetApp 應用程式的存取權：

- 管理 – 使用此端點透過 Secure Shell (SSH) 存取 NetApp ONTAP CLI，或搭配您的檔案系統使用 NetApp ONTAP REST API。
- 叢集間 – 使用 NetApp SnapMirror 設定複寫或使用 NetApp FlexCache 快取時，請使用此端點。

如需詳細資訊，請參閱[使用NetApp應用程式管理 FSx for ONTAP 資源](#)及[使用 複寫您的資料 NetApp SnapMirror](#)。

## 建立檔案系統

本節說明如何使用 Amazon FSx 主控台 AWS CLI 或 Amazon FSx API 建立 FSx FSx for ONTAP 檔案系統。您可以在您擁有的虛擬私有雲端 (VPC) 中建立檔案系統，或在另一個 AWS 帳戶與您共用的 VPC 中建立檔案系統。在 VPC 中建立多可用區域檔案系統時，如果您是參與者，則需考量這些事項。本主題說明這些考量。

根據預設，當您從 Amazon FSx 主控台建立新的檔案系統時，Amazon FSx 會自動建立具有單一儲存虛擬機器 (SVM) 和一個磁碟區的檔案系統，以便透過網路檔案系統 (NFS) 通訊協定快速存取 Linux 執行個體的資料。建立檔案系統時，您可以選擇將 SVM 加入 Active Directory，以透過伺服器訊息區塊 (SMB) 通訊協定啟用從 Windows 和 macOS 用戶端的存取。建立檔案系統之後，您可以視需要建立其他 SVMs 和磁碟區。



## 建立檔案系統（主控台）

此程序使用標準建立選項來建立 FSx for ONTAP 檔案系統，其中包含您針對需求自訂的組態。如需使用快速建立選項快速建立具有預設組態參數集的檔案系統的相關資訊，請參閱 [建立 Amazon FSx for NetApp ONTAP 檔案系統](#)。

1. 開啟 Amazon FSx 主控台，網址為 Amazon FSx 主控台，網址為 <https://console.aws.amazon.com/fsx/> : //https : //https : ///
2. 在儀表板上，選擇建立檔案系統。
3. 在選取檔案系統類型頁面上，針對檔案系統選項，選擇 Amazon FSx for NetApp ONTAP，然後選擇下一步。
4. 在建立方法區段中，選擇標準建立。
5. 在檔案系統詳細資訊區段中，提供下列資訊：
  - 針對檔案系統名稱 - 選用，輸入檔案系統的名稱。當您命名檔案系統時，可以更輕鬆地尋找和管理檔案系統。您最多可以使用 256 個 Unicode 字母、空格和數字，加上這些特殊字元：+ - = . \_ : /
  - 針對部署類型，選擇異地同步備份 2、單一可用區 2、異地同步備份 1 或單一可用區 1。
    - 多可用區域檔案系統會複寫您的資料，並支援在相同的多個可用區域中進行容錯移轉 AWS 區域。Multi-AZ 1 是 ONTAP 檔案系統的第一代 FSx。異地同步備份 2 是第二代檔案系統。它們都支援一個高可用性 (HA) 對。
    - 單一可用區檔案系統會複寫您的資料，並在單一可用區域內提供自動容錯移轉。單一可用區 1 是支援一個 HA 對的第一代 FSx for ONTAP 檔案系統。單一可用區 2 是第二代檔案系統，最多支援 12 個 HA 對。如需詳細資訊，請參閱[管理高可用性 \(HA\) 對](#)。

如需部署類型的詳細資訊，請參閱 [可用性、耐用性和部署選項](#)。

### Note

您無法在建立後變更檔案系統的部署類型。如果您想要變更部署類型（例如，從單一可用區 1 移至單一可用區 2），您可以備份資料，並將其還原到新的檔案系統。您也可以使用 NetApp SnapMirror、AWS DataSync 或第三方資料複製工具來遷移資料。如需詳細資訊，請參閱[使用 NetApp SnapMirror 遷移至 FSx for ONTAP](#)及[使用 遷移至 FSx for ONTAP AWS DataSync](#)。

- 針對 SSD 儲存容量，以 GB (GiB) 為單位輸入檔案系統的儲存容量。輸入 1,024–1,048,576 GiB（最多 1 pebibyte 【PiB】）範圍內的任何整數。

您可以在建立檔案系統之後，隨時視需要增加儲存容量。如需詳細資訊，請參閱[管理儲存容量](#)。

- 對於佈建的 SSD IOPS，您有兩個選項可為您的檔案系統佈建 IOPS 數量：
  - 如果您希望 Amazon FSx 自動佈建每 GiB SSD 儲存體 3 IOPS，請選擇自動（預設值）。
  - 如果您想要指定 IOPS 數量，請選擇使用者佈建。每個檔案系統最多可佈建 200,000 個 SSD IOPS。

**Note**

您可以在建立檔案系統後增加佈建的 SSD IOPS。請記住，即使佈建額外的 SSD IOPS，檔案系統也能達到 SSD IOPS 的最大層級，由檔案系統的輸送量容量決定。如需詳細資訊，請參閱[輸送量容量對效能的影響](#)及[管理儲存容量](#)。

- 對於輸送量容量，您有兩個選項可決定每秒 MB (MBps) 的輸送量容量：
  - 如果您希望 Amazon FSx 根據您選擇的儲存容量自動選擇輸送量容量，請選擇建議的輸送量容量。
  - 如果您想要指定輸送量容量，請選擇指定輸送量容量。如果您選擇此選項，則會顯示輸送量容量下拉式清單，並根據您選擇的部署類型填入。您也可以選擇 HA 對的數量（最多 12 個）。如需詳細資訊，請參閱[管理高可用性 \(HA\) 對](#)。

輸送量容量是託管檔案系統的檔案伺服器可以提供資料的持續速度。如需詳細資訊，請參閱[Amazon FSx for NetApp ONTAP 效能](#)。

6. 在聯網區段中，提供下列資訊：

- 針對 Virtual Private Cloud (VPC)，選擇您要與檔案系統建立關聯的 VPC。
- 對於 VPC 安全群組，您可以選擇要與檔案系統網路介面建立關聯的安全群組。如果您未指定，Amazon FSx 會將 VPC 的預設安全群組與您的檔案系統建立關聯。
- 為您的檔案伺服器指定子網路。如果您要建立多可用區檔案系統，請同時為待命檔案伺服器選擇待命子網路。
- （僅限多個可用區）對於 VPC 路由表，指定 VPC 路由表以建立檔案系統的端點。選取與用戶端所在子網路相關聯的所有 VPC 路由表。根據預設，Amazon FSx 會選取您 VPC 的預設路由表。如需詳細資訊，請參閱[從部署 VPC 外部存取資料](#)。

**Note**

Amazon FSx 會使用標籤型身分驗證來管理多可用區域檔案系統的這些路由表。這些路由表會加上 的標籤Key: AmazonFSx; Value: ManagedByAmazonFSx。使用 建

立 FSx for ONTAP 多可用區檔案系統時，AWS CloudFormation 建議您手動新增 Key: AmazonFSx; Value: ManagedByAmazonFSx 標籤。

- ( 僅限異地同步備份 ) 端點 IP 地址範圍指定要存取檔案系統的端點建立所在的 IP 地址範圍。

端點 IP 地址範圍有三個選項：

- 來自 VPC 的未配置 IP 地址範圍 – Amazon FSx 會從 VPC 的主要 CIDR 範圍中選擇最後 64 個 IP 地址，以用作檔案系統的端點 IP 地址範圍。如果您多次選擇此選項，則會在多個檔案系統中共用此範圍。

 Note

如果子網路正在使用 VPC 主要 CIDR 範圍中最後 64 個 IP 地址中的任何一個，此選項就會變成灰色。在此情況下，您仍然可以透過選擇輸入 IP 地址範圍選項，選擇 VPC 內地址範圍（即不在主要 CIDR 範圍結尾的範圍，或位於 VPC 次要 CIDR 中的範圍）。

- 針對偏好的子網路，為您的檔案伺服器指定子網路。如果您要建立多可用區檔案系統，請同時為待命檔案伺服器選擇待命子網路。
- ( 僅限多個可用區 ) 對於 VPC 路由表，指定 VPC 路由表以建立檔案系統的端點。選取與用戶端所在子網路相關聯的所有 VPC 路由表。根據預設，Amazon FSx 會選取您 VPC 的預設路由表。
- ( 僅限異地同步備份 ) 端點 IP 地址範圍指定要存取檔案系統的端點建立所在的 IP 地址範圍。

端點 IP 地址範圍有三個選項：

- 來自 VPC 的未配置 IP 地址範圍 – Amazon FSx 會從 VPC 的主要 CIDR 範圍中選擇最後 64 個 IP 地址，以用作檔案系統的端點 IP 地址範圍。如果您多次選擇此選項，則會在多個檔案系統中共用此範圍。

 Note

如果子網路正在使用 VPC 主要 CIDR 範圍中最後 64 個 IP 地址中的任何一個，此選項就會變成灰色。在這種情況下，您仍然可以透過選擇輸入 IP 地址範圍選項，選擇 VPC 內地址範圍（即不在主要 CIDR 範圍結尾的範圍，或位於 VPC 次要 CIDR 中的範圍）。

- 浮動 VPC 之外的 IP 地址範圍 – Amazon FSx 會選擇 198.19.x.0/24 地址範圍，而其他具有相同 VPC 和路由表的檔案系統尚未使用。
- 輸入 IP 地址範圍 – 您可以提供您選擇的 CIDR 範圍。您選擇的 IP 地址範圍可以在 VPC 的 IP 地址範圍內或之外，只要它不與任何子網路重疊即可。

 Note

請勿選擇任何落在下列 CIDR 範圍內的範圍，因為它們與 FSx for ONTAP 不相容：

- 0.0.0.0/8
- 127.0.0.0/8
- 198.19.0.0/20
- 224.0.0.0/4
- 240.0.0.0/4
- 255.255.255.255/32

7. 在加密區段中 AWS Key Management Service，針對加密金鑰，選擇可保護檔案系統靜態資料的 (AWS KMS) 加密金鑰。
8. 針對檔案系統管理密碼，輸入 fsxadmin 使用者的安全密碼。確認密碼。

您可以使用 fsxadmin 使用者來使用 ONTAP CLI 和 REST API 管理您的檔案系統。如需 fsxadmin 使用者的詳細資訊，請參閱 [使用 CLI ONTAP 管理檔案系統](#)。

9. 在預設儲存虛擬機器組態區段中，提供下列資訊：
  - 在儲存虛擬機器名稱欄位中，提供儲存虛擬機器的名稱。您最多可以使用 47 個英數字元，加上底線 (\_) 特殊字元。
  - 對於 SVM 管理密碼，您可以選擇指定密碼，並為 SVM vsadmin 的使用者提供密碼。您可以使用 vsadmin 使用者，使用 ONTAP CLI 或 REST API 來管理 SVM。如需 vsadmin 使用者的詳細資訊，請參閱 [使用 CLI ONTAP 管理 SVMs](#)。

如果您選擇不指定密碼（預設值），您仍然可以使用檔案系統的 fsxadmin 使用者，使用 ONTAP CLI 或 REST API 來管理您的檔案系統，但無法使用 SVM vsadmin 的使用者來執行相同的操作。

- 對於磁碟區安全樣式，請在磁碟區的 Unix (Linux) 和 NTFS 之間進行選擇。如需詳細資訊，請參閱 [磁碟區安全樣式](#)。

- 在 Active Directory 區段中，您可以將 Active Directory 加入 SVM。如需詳細資訊，請參閱[在 FSx for ONTAP 中使用 Microsoft Active Directory](#)。

如果您不想將 SVM 加入 Active Directory，請選擇不要加入 Active Directory。

如果您想要將 SVM 加入自我管理的 Active Directory 網域，請選擇加入 Active Directory，並為 Active Directory 提供下列詳細資訊：

- 要為 SVM 建立之 Active Directory 電腦物件的 NetBIOS 名稱。NetBIOS 名稱不能超過 15 個字元。
- Active Directory 的完整網域名稱。網域名稱不能超過 255 個字元。
- DNS 伺服器 IP 地址 – 網域的網域名稱系統 (DNS) 伺服器的 IPv4 地址。
- 服務帳戶使用者名稱 – 現有 Active Directory 中服務帳戶的使用者名稱。請勿包含網域字首或尾碼。
- 服務帳戶密碼 – 服務帳戶的密碼。
- 確認密碼 – 服務帳戶的密碼。
- ( 選用 ) 組織單位 (OU) – 您要加入檔案系統之組織單位的辨別路徑名稱。
- 委派檔案系統管理員群組 – Active Directory 中可管理檔案系統的群組名稱。

如果您使用 AWS Managed Microsoft AD，則需要指定群組，例如 AWS 委派 FSx 管理員、AWS 委派管理員，或具有委派 OU 許可的自訂群組。

如果您要加入自我管理 AD，請使用 AD 中的 群組名稱。預設群組為 Domain Admins。

#### 10. 在預設磁碟區組態區段中，提供使用 檔案系統建立的預設磁碟區資訊：

- 在磁碟區名稱欄位中，提供磁碟區的名稱。您最多可以使用 203 個英數字元或底線 (\_) 字元。
- ( 僅限具有一個 HA 對的檔案系統 ) 對於磁碟區樣式，請選擇 FlexVol 或 FlexGroup。FlexVol 磁碟區是一般用途磁碟區，大小最多可達 300 tebibyte (TiB)。FlexGroup 磁碟區適用於高效能工作負載，大小最多可達 20 PiB。
- 針對磁碟區大小，輸入磁碟區範圍介於 20–314, 572, 800 MB (MiB) 或 FlexGroup 磁碟 FlexVol 區每個 HA 對 800 GB (GiB)–2, 400 TiB 的任何整數。例如，具有 12 個 HA 對的檔案系統，其磁碟區大小下限為 9, 600 GiB，大小上限為 20, 480 TiB。
- 對於磁碟區類型，選擇讀寫 (RW) 以建立可讀且可寫入的磁碟區，或選擇資料保護 (DP) 以建立唯讀且可以用作 NetApp SnapMirror 或 SnapVault 關係目的地的磁碟區。如需詳細資訊，請參閱[磁碟區類型](#)。
- 在 Junction 路徑中，輸入檔案系統中的位置以掛載磁碟區。名稱必須有正斜線，例如 /vol3。

- 為了提高儲存效率，請選擇啟用以啟用 ONTAP 儲存效率功能（重複資料刪除、壓縮和壓縮）。如需詳細資訊，請參閱[儲存效率](#)。
- 針對快照政策，選擇磁碟區的快照政策。如需快照政策的詳細資訊，請參閱[快照政策](#)。

如果您選擇自訂政策，則必須在自訂政策欄位中指定政策的名稱。自訂政策必須已存在於 SVM 或檔案系統中。您可以使用 ONTAP CLI 或 REST API 建立自訂快照政策。如需詳細資訊，請參閱 NetApp ONTAP [產品文件中的建立快照政策](#)。

11. 在預設磁碟區儲存分層區段中，針對容量集區分層政策，選擇磁碟區的儲存集區分層政策，可以是自動（預設）、僅限快照、全部或無。如需容量集區分層政策的詳細資訊，請參閱[磁碟區分層政策](#)。

對於分層政策冷卻期間，如果您已將儲存分層設定為 Auto 和 Snapshot-only policies.valid 值為 2-183 天。磁碟區的分層政策冷卻期間會定義尚未存取的資料標記為冷並移至容量集區儲存之前的天數。

12. 在預設磁碟區 SnapLock 組態區段中，針對 SnapLock 組態選擇已啟用和已停用。如需設定 SnapLock 合規磁碟區或 SnapLock 企業磁碟區的詳細資訊，請參閱[了解 SnapLock 合規](#)和[了解 SnapLock 企業](#)。如需 SnapLock 的相關資訊，請參閱[使用 保護您的資料 SnapLock](#)。
13. 在備份和維護 - 選用中，您可以設定下列選項：
  - 針對每日自動備份，選擇已啟用以進行自動每日備份。此選項預設為啟用。
  - 對於每日自動備份時段，請以國際標準時間 (UTC) 設定您要啟動每日自動備份時段的時間。從此指定時間開始，視窗為 30 分鐘。此時段無法與每週維護備份時段重疊。
  - 對於自動備份保留期間，請將您要保留自動備份的期間設定為 1-90 天。
  - 對於每週維護時段，您可以設定您希望維護時段開始的一週時間。第 1 天是星期一，第 2 天是星期二，以此類推。從此指定時間開始，視窗為 30 分鐘。此時段無法與每日自動備份時段重疊。
14. 對於標籤 - 選用，您可以輸入索引鍵和值，將標籤新增至檔案系統。標籤是區分大小寫的鍵值組，可協助您管理、篩選和搜尋檔案系統。

選擇下一步。

15. 檢閱顯示在 Create file system (建立檔案系統) 頁面上的檔案系統組態。為供您參考，請注意在建立檔案系統之後，您可以修改哪些檔案系統設定。
16. 選擇 Create file system (建立檔案系統)。



## 建立檔案系統 (CLI)

- 若要建立 FSx for ONTAP 檔案系統，請使用 [create-file-system](#) CLI 命令（或同等的 [CreateFileSystem](#) API 操作），如下列範例所示。

### Note

您無法在建立後變更檔案系統的部署類型。如果您想要變更部署類型（例如，從單一可用區 1 移至單一可用區 2），您可以備份資料，並將其還原至新的檔案系統。您也可以使用 NetApp SnapMirror、AWS DataSync 或第三方資料複製工具來遷移資料。如需詳細資訊，請參閱 [使用 NetApp SnapMirror 遷移至 FSx for ONTAP](#) 及 [使用 遷移至 FSx for ONTAP AWS DataSync](#)。

```
aws fsx create-file-system \  
  --file-system-type ONTAP \  
  --storage-capacity 1024 \  
  --storage-type SSD \  
  --security-group-ids security-group-id \  
  
  --subnet-ids subnet-abcdef1234567890b subnet-abcdef1234567890c \  
  --ontap-configuration DeploymentType=MULTI_AZ_1,  
    ThroughputCapacity=512,PreferredSubnetId=subnet-abcdef1234567890b
```

成功建立檔案系統後，Amazon FSx 會以 JSON 格式傳回檔案系統的描述，如下列範例所示。

```
{  
  "FileSystem": {  
    "OwnerId": "111122223333",  
    "CreationTime": 1625066825.306,  
    "FileSystemId": "fs-0123456789abcdef0",  
    "FileSystemType": "ONTAP",  
    "Lifecycle": "CREATING",  
    "StorageCapacity": 1024,  
    "StorageType": "SSD",  
    "VpcId": "vpc-11223344556677aab",  
    "SubnetIds": [  
      "subnet-abcdef1234567890b",  
      "subnet-abcdef1234567890c"  
    ],  
  },  
}
```

```

    "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "ResourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/
fs-0123456789abcdef0",
    "Tags": [],
    "OntapConfiguration": {
        "DeploymentType": "MULTI_AZ_HA_1",
        "EndpointIpAddressRange": "198.19.0.0/24",
        "Endpoints": {
            "Management": {
                "DnsName": "management.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com"
            },
            "Intercluster": {
                "DnsName": "intercluster.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com"
            }
        },
        "DiskIopsConfiguration": {
            "Mode": "AUTOMATIC",
            "Iops": 3072
        },
        "PreferredSubnetId": "subnet-abcdef1234567890b",
        "RouteTableIds": [
            "rtb-abcdef1234567890e",
            "rtb-abcd1234ef567890b"
        ],
        "ThroughputCapacity": 512,
        "WeeklyMaintenanceStartTime": "4:10:00"
    }
}
}
}

```

### Note

與在主控台中建立檔案系統的程序不同，CLI `create-file-system` 命令和 `CreateFileSystem` API 操作不會建立預設 SVM 或磁碟區。若要建立 SVM，請參閱 [建立儲存虛擬機器 \(SVM\)](#)；若要建立磁碟區，請參閱 [建立磁碟區](#)。



## 在共用子網路中建立 FSx for ONTAP 檔案系統

VPC 共用可讓多個 AWS 帳戶 建立資源到共用、集中管理的虛擬私有雲端 (VPCs)。在此模型中，擁有 VPC (擁有者) 的帳戶會與其他屬於相同組織的帳戶 (參與者) 共用一或多個子網路 AWS Organizations。

參與者帳戶可以在擁有者帳戶與其共用的 VPC 子網路中，為 ONTAP 單一可用區和多可用區檔案系統建立 FSx。若要讓參與者帳戶建立多可用區域檔案系統，擁有者帳戶也需要授予 Amazon FSx 許可，才能代表參與者帳戶修改共用子網路中的路由表。如需詳細資訊，請參閱[管理多可用區域檔案系統的共用 VPC 支援](#)。

### Note

參與者帳戶有責任與 VPC 擁有者協調，以防止建立任何後續 VPC 子網路，這些子網路將與參與者檔案系統的 VPC CIDR 重疊。如果子網路重疊，則檔案系統的流程可能會中斷。

### 共用子網路需求和注意事項

在共用子網路中建立 FSx for ONTAP 檔案系統時，請注意下列事項：

- VPC 子網路的擁有者必須與參與者帳戶共用子網路，該帳戶才能在其中建立 FSx for ONTAP 檔案系統。
- 您無法啟動使用 VPC 預設安全群組的資源，因為該資源屬於擁有者。此外，參與者帳戶無法使用其他參與者或擁有者擁有的安全群組啟動資源。
- 在共用子網路中，參與者和擁有者會分別控制每個各別帳戶內的安全群組。擁有者帳戶可以查看參與者建立的安全群組，但無法對其執行任何動作。如果擁有者帳戶想要移除或修改這些安全群組，則建立安全群組的參與者必須採取動作。
- 參與者帳戶可以在擁有者帳戶與其共用的子網路中檢視、建立、修改和刪除單一可用區檔案系統及其相關資源。
- 參與者帳戶可以在擁有者帳戶與其共用的子網路中建立、檢視、修改和刪除多可用區域檔案系統及其相關資源。此外，擁有者帳戶也必須授予 Amazon FSx 服務許可，以代表參與者帳戶修改共用子網路中的路由表。如需詳細資訊，請參閱[管理多可用區域檔案系統的共用 VPC 支援](#)
- 共用 VPC 擁有者無法檢視、修改或刪除參與者在共用子網路中建立的資源。此為 VPC 資源 (每個帳戶具有不同存取權) 以外。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中[擁有者和參與者的責任和許可](#)。

如需詳細資訊，請參閱《Amazon [VPC 使用者指南](#)》中的[與其他帳戶共用](#)您的 VPC。

## 共用 VPC 子網路時

與將在共用子網路中建立 FSx for ONTAP 檔案系統的參與者帳戶共用子網路時，您將需要執行下列動作：

- VPC 擁有者需要使用 AWS Resource Access Manager 與其他安全地共用 VPCs 和子網路 AWS 帳戶。如需詳細資訊，請參閱 AWS Resource Access Manager 《使用者指南》中的[共用您的 AWS 資源](#)。
- VPC 擁有者需要與參與者帳戶共用一或多個 VPCs。如需詳細資訊，請參閱《Amazon Virtual Private Cloud 使用者指南》中的[與其他帳戶共用 VPC](#)。
- 若要讓參與者帳戶建立 FSx for ONTAP 多可用區域檔案系統，VPC 擁有者也必須授予 Amazon FSx 服務許可，才能代表參與者帳戶在共用子網路中建立和修改路由表。這是因為 FSx for ONTAP 多可用區檔案系統使用浮動 IP 地址，因此連線的用戶端可以在容錯移轉事件期間無縫轉換偏好的和待命檔案伺服器。發生容錯移轉事件時，Amazon FSx 會更新與檔案系統關聯之所有路由表中的所有路由，以指向目前作用中的檔案伺服器。

## 管理多可用區域檔案系統的共用 VPC 支援

擁有者帳戶可以管理參與者帳戶是否可以使用和 API，在擁有者與參與者共用的 VPC 子網路中建立適用於 ONTAP 檔案系統的多可用區域 FSx AWS Management Console AWS CLI，如以下各節所述。

## 管理多可用區檔案系統的 VPC 共用（主控台）

開啟 Amazon FSx 主控台，網址為 <https://console.aws.amazon.com/fsx/> : //https : //https : //https : //https : ///

1. 在導覽窗格中，選擇設定。
2. 在設定頁面上找到異地同步備份共用 VPC 設定。
  - 若要在您共用的 VPC 子網路中啟用多可用區域檔案系統的 VPC 共用，請選擇從參與者帳戶啟用路由表更新。
  - 若要在您擁有的所有 VPC 中停用異地同步備份檔案系統的 VPCs 共用，請選擇停用參與者帳戶的路由表更新。確認畫面隨即顯示。

**⚠ Important**

強烈建議在停用此功能之前，先刪除共用 VPC 中參與者建立的多可用區檔案系統。停用此功能後，這些檔案系統將進入 MISCONFIGURED 狀態，且會有無法使用的風險。

3. 輸入 **confirm** 並選擇確認以停用此功能。

### 管理多可用區檔案系統的 VPC 共用 (AWS CLI)

1. 若要檢視 Multi-AZ VPC 共用的目前設定，請使用 [describe-shared-vpc-configuration](#) CLI 命令或同等的 [DescribeSharedVpcConfiguration](#) API 命令，如下所示：

```
$ aws fsx describe-shared-vpc-configuration
```

服務會回應成功的請求，如下所示：

```
{
  "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
}
```

2. 若要管理異地同步備份共用 VPC 組態，請使用 [update-shared-vpc-configuration](#) CLI 命令或同等的 [UpdateSharedVpcConfiguration](#) API 命令。下列範例會啟用多可用區域檔案系統的 VPC 共用。

```
$ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-participant-accounts true
```

服務會回應成功的請求，如下所示：

```
{
  "EnableFsxRouteTableUpdatesFromParticipantAccounts": "true"
}
```

3. 若要停用此功能，請將 `EnableFsxRouteTableUpdatesFromParticipantAccounts` 設定為 `false`，如下列範例所示。

```
$ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-participant-accounts false
```

服務會回應成功的請求，如下所示：

```
{
  "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
}
```

## 更新檔案系統

本主題說明您可以更新的現有檔案系統屬性，並提供使用 Amazon FSx 主控台和 CLI 執行此操作的程序。您可以使用 Amazon FSx 主控台 AWS CLI 和 API 更新下列 FSx for ONTAP 檔案系統屬性：

- 自動每日備份。開啟或關閉自動每日備份，修改備份時段和備份保留期。如需詳細資訊，請參閱[自動每日備份](#)。
- 每週維護時段。設定 Amazon FSx 執行檔案系統維護和更新的星期幾和時間。如需詳細資訊，請參閱[使用 Amazon FSx 維護時段最佳化效能](#)。
- 檔案系統管理密碼。變更檔案系統 fsxadmin 使用者的密碼。您可以使用 fsxadmin 使用者，使用 ONTAP CLI 和 REST API 來管理您的檔案系統。如需 fsxadmin 使用者的詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。
- Amazon VPC 路由表。使用適用於 ONTAP 檔案系統的異地同步備份 FSx，您用來透過 NFS 或 SMB 存取資料的端點，以及用來存取 ONTAP CLI、API 和 BlueXP 的管理端點，會使用與您檔案系統相關聯的 Amazon VPC 路由表中的浮動 IP 地址。您可以將您建立的新路由表與現有的多可用區域檔案系統建立關聯，讓您可以設定哪些用戶端可以存取您的資料，即使您的網路演進也一樣。您也可以取消現有路由表與檔案系統的關聯（移除）。

### Note

Amazon FSx 會使用標籤型身分驗證來管理多可用區檔案系統的 VPC 路由表。這些路由表會加上 的標籤 Key: AmazonFSx; Value: ManagedByAmazonFSx。使用 建立或更新 FSx for ONTAP 多可用區檔案系統時，AWS CloudFormation 建議您手動新增 Key: AmazonFSx; Value: ManagedByAmazonFSx 標籤。

## 更新檔案系統（主控台）

下列程序提供如何使用 更新現有 FSx for ONTAP 檔案系統的指示 AWS Management Console。

### 更新自動每日備份

1. 開啟 Amazon FSx 主控台，網址為 <https://console.aws.amazon.com/fsx/> : //https : //https : //https : //https : //
2. 若要顯示檔案系統詳細資訊頁面，請在左側導覽窗格中，選擇檔案系統，然後選擇您要更新的 FSx for ONTAP 檔案系統。
3. 在頁面的第二個面板中選擇備份索引標籤。
4. 選擇更新。
5. 修改此檔案系統的自動每日備份設定。
6. 選擇儲存，以儲存變更。

### 更新每週維護時段

1. 開啟 Amazon FSx 主控台，網址為 <https://console.aws.amazon.com/fsx/> : //https : //https : //https : //https : //
2. 若要顯示檔案系統詳細資訊頁面，請在左側導覽窗格中，選擇檔案系統，然後選擇您要更新的 FSx for ONTAP 檔案系統。
3. 在頁面的第二個面板中選擇管理索引標籤。
4. 在維護窗格中，選擇更新。
5. 修改此檔案系統的每週維護時段。
6. 選擇儲存，以儲存變更。

### 變更檔案系統管理密碼

1. 開啟 Amazon FSx 主控台，網址為 <https://console.aws.amazon.com/fsx/> : //https : //https : //https : //https : //
2. 若要顯示檔案系統詳細資訊頁面，請在左側導覽窗格中，選擇檔案系統，然後選擇您要更新的 FSx for ONTAP 檔案系統。
3. 選擇管理索引標籤。
4. 在 ONTAP 管理窗格中，選擇 ONTAP 管理員密碼下的更新。

5. 在更新 ONTAP 管理員登入資料對話方塊中，在 ONTAP 管理密碼欄位中輸入新密碼。
6. 使用確認密碼欄位來確認密碼。
7. 選擇更新登入資料以儲存變更。

 Note

如果您收到錯誤，指出新密碼不符合密碼要求，您可以使用 [security login role config show](#) ONTAP CLI 命令在檔案系統上檢視密碼要求設定。如需詳細資訊，包括如何變更密碼設定的指示，請參閱 [更新fsxadmin帳戶密碼失敗](#)。

### 更新多可用區檔案系統的 VPC 路由表

1. 開啟 Amazon FSx 主控台，網址為 <https://console.aws.amazon.com/fsx/> : //www.。
2. 若要顯示檔案系統詳細資訊頁面，請在左側導覽窗格中，選擇檔案系統，然後選擇您要更新的 FSx for ONTAP 檔案系統。
3. 針對動作，選擇管理路由表。此選項僅適用於多可用區檔案系統。
4. 在管理路由表對話方塊中，執行下列其中一項操作：
  - 若要關聯新的 VPC 路由表，請從關聯新的路由表下拉式清單中選取路由表，然後選擇關聯。
  - 若要取消現有 VPC 路由表的關聯，請從目前路由表窗格中選取路由表，然後選擇取消關聯。
5. 選擇關閉。

### 更新檔案系統 (CLI)

下列程序說明如何使用 更新現有的 FSx for ONTAP 檔案系統 AWS CLI。

1. 若要更新 FSx for ONTAP 檔案系統的組態，請使用 [update-file-system](#) CLI 命令（或同等的 [UpdateFileSystem](#) API 操作），如下列範例所示。

```
aws fsx update-file-system \
  --file-system-id fs-0123456789abcdef0 \
  --ontap-configuration
AutomaticBackupRetentionDays=30,DailyAutomaticBackupStartTime=01:00, \
  WeeklyMaintenanceStartTime=1:01:30,AddRouteTableIds=rtb-0123abcd, \
  FsxAdminPassword=new-fsx-admin-password
```

2. 若要停用自動每日備份，請將 AutomaticBackupRetentionDays 屬性設定為 0。

```
aws fsx update-file-system \  
  --file-system-id fs-0123456789abcdef0 \  
  --ontap-configuration AutomaticBackupRetentionDays=0
```

## 管理高可用性 (HA) 對

每個 FSx for ONTAP 檔案系統都由作用中待命組態中的一或多個檔案伺服器的高可用性 (HA) 對提供支援。在此組態中，有一個偏好的檔案伺服器，可主動為流量提供服務，而次要檔案伺服器會在作用中伺服器無法使用時接管。FSx for ONTAP 第一代檔案系統由一個 HA 對提供支援，可提供高達 4 GBps 的輸送量容量和 160,000 個 SSD IOPs。FSx for ONTAP 第二代多可用區域檔案系統也採用一個 HA 對，可提供高達 6 GBps 的輸送量容量和 200,000 個 SSD IOPS。FSx for ONTAP 第二代單一可用區檔案系統支援高達 12 個 HA 對，可提供高達 72 GBps 的輸送量容量和 2,400,000 個 SSD IOPS (6 GBps 的輸送量容量和每個 HA 對 200,000 個 SSD IOPS)。

當您從 Amazon FSx 主控台建立檔案系統時，Amazon FSx 會根據您想要的 SSD 儲存體建議應使用的 HA 對數量。您也可以根據您的工作負載和效能需求，手動選擇 HA 對的數量。如果您的檔案系統需求滿足高達 6 GBps 的輸送量容量和 200,000 個 SSD IOPS，我們建議您使用單一 HA 對，如果您的工作負載需要更高層級的效能可擴展性，則使用多個 HA 對。

每個 HA 對都有一個彙總，這是一組邏輯的實體磁碟。

### Note

您可以將 HA 對新增至第二代單一可用區檔案系統。如需詳細資訊，請參閱[新增高可用性 \(HA\) 對](#)。否則，您可以使用 [SnapMirror](#) 或在檔案系統之間遷移資料（使用不同的 HA 對）[SnapMirror AWS DataSync](#)，或將資料從備份還原至新的檔案系統。

## 新增高可用性 (HA) 對

FSx for ONTAP 檔案系統由一或多個檔案伺服器的 HA 對組成。第一代檔案系統和第二代多可用區域檔案系統支援一個 HA 對，而第二代單一可用區域檔案系統支援最多 12 個 HA 對。您可以在建立第二代單一可用區檔案系統後新增更多 HA 對（最多 12 個）。新增 HA 對不會造成干擾，通常只需要幾分鐘的時間即可完成。

將 HA 對新增至檔案系統時，請考慮下列幾點：



- 將 HA 對新增至您的檔案系統，會引入具有其儲存體（或彙總）的新檔案伺服器。新的 HA 對具有與您檔案系統現有 HA 對相同的輸送量容量和儲存容量。例如，假設您的檔案系統有兩個 HA 對，總輸送量容量為 12 GBps，而 SSD 儲存容量為 2 tebibyte (TiB)。如果您新增一個 HA 對，則檔案系統會有 18 GBps 的輸送量容量和 3 TiB 的 SSD 儲存體。
- 若要受益於新 HA 對的額外效能，您需要將一些現有磁碟區移至新 HA 對，並重新掛載用戶端以連接到它們。如需詳細資訊，請參閱[平衡跨 HA 對的工作負載](#)。
- 在新增 HA 對或正在更新以新增 HA 對時，您無法修改檔案系統的輸送量容量、SSD 儲存容量或佈建的 SSD IOPS。
- 新增 HA 對後就無法移除。如果您暫時需要更多效能（假設您的檔案系統未處於最高輸送量容量），建議您擴展檔案系統的輸送量容量。這會增加檔案系統現有 HA 對的輸送量容量。
- 若要將第二代檔案系統的 HA 對從一到兩個或多個，您的檔案系統最多可以有五個 SVMS。
- iSCSI 通訊協定適用於具有六個或更少高可用性對 (HA 對) 的檔案系統。NVMe/TCP 通訊協定適用於具有六個或更少 HA 對的第二代檔案系統。如需詳細資訊，請參閱[存取 FSx for ONTAP 資料](#)。
- 當您將新的 HA 對新增至檔案系統時，預設會為新的檔案系統節點啟用 NVMe 快取。我們建議針對輸送量密集的工作負載停用此功能。如需詳細資訊，請參閱[管理 NVMe 快取](#)。

## 新增 HA 對

1. 開啟 Amazon FSx 主控台，網址為 Amazon FSx 主控台，網址為 <https://console.aws.amazon.com/fsx/> : //https : //https : ///
2. 若要顯示檔案系統詳細資訊頁面，請在左側導覽窗格中，選擇檔案系統，然後選擇您要更新的 FSx for ONTAP 檔案系統。
3. 在摘要面板上，針對 HA 對的數量，選擇更新。
4. 從 HA 對下拉式清單中，選取要新增至檔案系統的 HA 對數目。
5. 選擇更新按鈕。

新增 HA 對後，請務必重新平衡現有資料，以確保 I/O 在檔案系統的 HA 對中保持平均分佈。如需詳細資訊，請參閱[平衡跨 HA 對的工作負載](#)。

## 平衡跨 HA 對的工作負載

如果您有具有多個高可用性 (HA) 對的檔案系統，則其輸送量和儲存體會分散到每個 HA 對。FSx for ONTAP 會在檔案系統寫入檔案時自動平衡檔案，但您的工作負載資料和 I/O 在您新增 HA 對後不再平衡。此外，在極少數情況下，您的工作負載資料或 I/O 在檔案系統的現有 HA 對之間可能會變得不平



衡，這可能會影響工作負載的整體效能。如果您的工作負載曾經不平衡，您可以重新平衡每個檔案系統的 HA 對（及其對應的檔案伺服器和彙總，也就是構成主要儲存層的儲存集區）。

## 主題

- [主要儲存使用率平衡](#)
- [檔案伺服器和磁碟效能使用率不平衡](#)
- [將 CloudWatch 維度映射至 ONTAP CLI 和 REST API 資源](#)
- [重新平衡用戶端](#)
- [重新平衡磁碟區](#)

## 主要儲存使用率平衡

檔案系統的主要儲存容量會平均分配到儲存集區中稱為彙總的每個 HA 對。每個 HA 對都有一個彙總。我們建議您持續維持主要儲存層的平均使用率不高於 80%。對於具有多個 HA 對的檔案系統，我們建議您為每個彙總維持高達 80% 的平均使用率。

維持 80% 的使用率可確保新傳入資料有可用空間，並維持維護操作正常的額外負荷，可暫時取得彙總的可用空間。

如果您發現彙總不平衡，您可以增加檔案系統的主要儲存容量（相對增加每個彙總的儲存容量），也可以在彙總之間移動磁碟區。如需詳細資訊，請參閱[在彙總之間移動磁碟區](#)。

## 檔案伺服器和磁碟效能使用率不平衡

檔案系統的整體效能功能（例如網路輸送量、檔案伺服器到磁碟輸送量和 IOPS，以及磁碟 IOPS）會平均分配到檔案系統的 HA 對。我們建議您持續維持所有效能限制的平均使用率低於 50%（最高尖峰使用率低於 80%），這適用於所有 HA 對的檔案系統檔案伺服器資源的整體使用率，以及每個檔案伺服器的整體使用率。

如果您注意到檔案伺服器效能使用率不平衡，且工作負載不平衡的檔案伺服器持續使用率超過 80%，您可以使用 ONTAP CLI 和 REST API 進一步診斷效能不平衡的原因並進行修復。以下是可能不平衡指標的表格，以及進一步診斷的後續步驟。

| 如果您的檔案系統的...                | Then...                                                                                                |
|-----------------------------|--------------------------------------------------------------------------------------------------------|
| 檔案伺服器磁碟輸送量或檔案伺服器磁碟 IOPS 不平衡 | 您可能會遇到 HA 對子集（磁碟區的一部分，其中包含所存取的資料量過大）的 I/O 熱點，這可能會限制工作負載的整體效能，因為它對 HA 對子集造成瓶頸。對於每個高度使用的檔案伺服器，請檢查最常使用的磁碟 |

| 如果您的檔案系統的...                                     | Then...                                                                                                                                                         |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                  | 區，以查看哪些磁碟區在彙總中具有最多的活動。如需此程序的詳細資訊，請參閱 <a href="#">重新平衡磁碟區</a> 。                                                                                                  |
| 網路輸送量不平衡，但您的檔案伺服器磁碟輸送量、檔案伺服器磁碟 IOPS 或磁碟 IOPS 不平衡 | 您的資料會平均分散到 HA 對，但您的用戶端則不是。對於網路輸送量使用率高於其他的檔案伺服器，請檢查每個檔案伺服器的最高用戶端，然後從這些用戶端卸載任何磁碟區，並在不同的 HA 對上使用不同的端點重新掛載這些用戶端，以重新平衡這些用戶端。如需此程序的詳細資訊，請參閱 <a href="#">重新平衡用戶端</a> 。 |

將 CloudWatch 維度映射至 ONTAP CLI 和 REST API 資源

您的第二代檔案系統具有 FileServer 或 Aggregate 維度的 Amazon CloudWatch 指標。為了進一步診斷不平衡情況，您需要將這些維度值映射到 ONTAP CLI 或 REST API 中的特定檔案伺服器（或節點）和彙總。

- 對於檔案伺服器，每個檔案伺服器名稱都會映射到 ONTAP 中的檔案伺服器（或節點）名稱（例如 FsxId01234567890abcdef-01）。奇數編號的檔案伺服器是偏好的檔案伺服器（也就是，除非檔案系統容錯移轉至次要檔案伺服器，否則它們會服務流量），而偶數編號的檔案伺服器是次要檔案伺服器（也就是，只有在其合作夥伴無法使用時才會提供流量）。因此，次要檔案伺服器通常會比偏好的檔案伺服器顯示較少的使用率。
- 對於彙總，每個彙總名稱都會映射到 ONTAP 中的彙總（例如 aggr1）。每個 HA 對都有一個彙總，這表示彙總 aggr1 由 HA 對中的檔案伺服器 FsxId01234567890abcdef-01（作用中檔案伺服器）和 FsxId01234567890abcdef-02（次要檔案伺服器）共用，彙總由檔案伺服器 FsxId01234567890abcdef-03 和 aggr2 共用 FsxId01234567890abcdef-04，以此類推。

您可以使用 ONTAP CLI 檢視所有彙總和檔案伺服器之間的映射。

- 若要將 SSH 插入檔案系統的 NetApp ONTAP CLI，請遵循《Amazon FSx for NetApp ONTAP 使用者指南》中的 [使用 NetApp ONTAP CLI](#) 區段中記載的步驟。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

- 使用 [儲存彙總 show](#) 命令，指定 -fields node 參數。

```
::> storage aggregate show -fields node
aggregate                               node
```

```
-----
aggr1          FsxId01234567890abcdef-01
aggr2          FsxId01234567890abcdef-03
aggr3          FsxId01234567890abcdef-05
aggr4          FsxId01234567890abcdef-07
aggr5          FsxId01234567890abcdef-09
aggr6          FsxId01234567890abcdef-11
6 entries were displayed.
```

## 重新平衡用戶端

新增 HA 對後，或者如果您在檔案伺服器之間遇到 I/O 不平衡（特別是網路輸送量使用率），您可以重新平衡用戶端。如果您在新增 HA 對後重新平衡用戶端，您可以跳至 [重新掛載用戶端](#)。否則，您應該先識別要移動的高流量用戶端，以重新平衡工作負載 I/O。

如果您在檔案伺服器之間遇到 I/O 不平衡（特別是網路輸送量使用率），則高 I/O 用戶端可能是原因。若要識別高流量用戶端，請使用 ONTAP CLI。

## 識別高流量用戶端

- 若要 SSH 至檔案系統的 NetApp ONTAP CLI，請遵循《Amazon FSx for NetApp ONTAP 使用者指南》中的 [使用 NetApp ONTAP CLI](#) 區段中記載的步驟。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

- 若要檢視最高流量的用戶端，請使用 [統計資料頂端用戶端](#) `show` ONTAP CLI 命令。您可以選擇指定 `-node` 參數，只檢視特定檔案伺服器的熱門用戶端。如果您診斷特定檔案伺服器的不平衡，請使用 `-node` 參數，`node_name` 將取代為檔案伺服器的名稱（例如 `FsxId01234567890abcdef-01`）。

您可以選擇性地新增 `-interval` 參數，提供輸出每個報告前要測量的間隔（以秒為單位）。增加間隔（例如，增加到最多 300 秒）可為驅動到每個磁碟區的流量提供長期範例。預設值為 5（秒）。

```
::> statistics top client show -node FsxId01234567890abcdef-01 [-interval [5,300]]
```

在輸出中，最高用戶端會以其 IP 地址和連接埠顯示。

| Client | Vserver | Node | *Total<br>Ops | Total<br>(Bps) |
|--------|---------|------|---------------|----------------|
|--------|---------|------|---------------|----------------|

```
-----
172.17.236.53:938 svm01      FsxId01234567890abcdef-01    2143 140443648
172.17.236.160:898 svm02      FsxId01234567890abcdef-01    812  53215232
```

## 重新掛載用戶端

- 您可以重新平衡用戶端到其他 HA 對。若要這樣做，請從用戶端卸載磁碟區，並使用 SVM NFS/SMB 端點的 DNS 名稱重新掛載磁碟區，這會傳回對應於隨機 HA 對的隨機端點。

我們建議您重複使用 DNS 名稱，但您可以選擇明確選擇指定用戶端掛載的 HA 對。若要保證您將用戶端掛載到不同的端點，您可以改為指定與對應到發生高流量的檔案伺服器不同的端點 IP 地址。您可以執行下列命令來執行此操作：

```
::> network interface show -vserver svm_name -lif nfs_smb_management* -fields
      address,curr-node
vserver  lif                address      curr-node
-----
svm01    nfs_smb_management_1 172.31.15.89 FsxId01234567890abcdef-01
svm01    nfs_smb_management_3 172.31.8.112 FsxId01234567890abcdef-03
2 entries were displayed.
```

根據 `statistics top client show` 命令的範例輸出，用戶端 172.17.236.53 正在將高流量驅動到 FsxId01234567890abcdef-01。network interface show 命令的輸出指出這是地址 172.31.15.89。若要掛載到不同的端點，請選取任何其他地址（在此範例中，唯一的其他地址是 172.31.8.112，對應於 FsxId01234567890abcdef-03）。

## 重新平衡磁碟區

如果您在磁碟區或彙總中遇到 I/O 不平衡，您可以重新平衡磁碟區，以將 I/O 流量重新分配到磁碟區。

### Note

如果您在彙總中遇到儲存使用率不平衡，通常不會對效能造成任何影響，除非高使用率與 I/O 不平衡結合。雖然您可以在彙總之間移動磁碟區以平衡儲存使用率，但我們建議您只在看到效能影響時移動磁碟區，因為如果您不考慮將 I/O 驅動到您考慮移動的每個磁碟區，移動磁碟區可能會對效能產生負面影響。

- 若要 SSH 至檔案系統的 NetApp ONTAP CLI，請遵循《Amazon FSx for NetApp ONTAP 使用者指南》中的[使用 NetApp ONTAP CLI](#)一節中記載的步驟。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

- 使用[統計資料磁碟區 show](#) ONTAP CLI 命令來檢視指定彙總的最高流量磁碟區，但有下列變更：
  - 將 *aggregate\_name* 取代為彙總的名稱（例如，aggr1）。
  - 您可以選擇性地新增 `-interval` 參數，提供輸出每個報告前要測量的間隔（以秒為單位）。增加間隔（例如，增加到最多 300 秒）可為驅動到每個磁碟區的流量提供長期範例。預設值為 5（秒）。

```
::> statistics volume show -aggregate aggregate_name -sort-key total_ops [-interval [5,300]]
```

根據您選擇的間隔，最多可能需要 5 分鐘才能顯示資料。此命令會顯示彙總中的所有磁碟區，以及要驅動至每個彙總的流量。

| Volume     | Vserver | Aggregate | *Total<br>Ops | Read<br>Ops | Write<br>Ops | Other<br>Ops | Read<br>(Bps) | Write<br>(Bps) | Latency<br>(us) |
|------------|---------|-----------|---------------|-------------|--------------|--------------|---------------|----------------|-----------------|
| vol1__0007 | svm1    | aggr1     | 4078          | 4078        | 0            | 0            | 267255808     | 0              | 1092            |
| vol1__0005 | svm1    | aggr1     | 4078          | 4078        | 0            | 0            | 267255808     | 0              | 1086            |
| vol1__0003 | svm1    | aggr1     | 4077          | 4077        | 0            | 0            | 267223040     | 0              | 1086            |
| vol1__0001 | svm1    | aggr1     | 4077          | 4077        | 0            | 0            | 267239424     | 0              | 1087            |
| vol1__0008 | svm1    | aggr2     | 2314          | 2314        | 0            | 0            | 151650304     | 0              | 1112            |
| vol1__0006 | svm1    | aggr2     | 2144          | 2144        | 0            | 0            | 140509184     | 0              | 1104            |
| vol1__0002 | svm1    | aggr2     | 2183          | 2183        | 0            | 0            | 143065088     | 0              | 1106            |
| vol1__0004 | svm1    | aggr2     | 2183          | 2183        | 0            | 0            | 143065088     | 0              | 1103            |

磁碟區統計資料是以每個成分為基礎（例如，vol1\_\_0015 是 的第 15 個成分 vol1）FlexGroup 顯示。您可以從範例輸出中看到，的元件比 的元件使用率 aggr1 更高 aggr2。若要平衡彙總之間的流量，您可以在彙總之間移動組成磁碟區，以便更平均地分配流量。

- 如果您已新增新的 HA 對，則應該將現有的磁碟區移至新的彙總。如需詳細資訊，請參閱[在彙總之間移動磁碟區](#)。

## 管理 NVMe 快取

NVMe 快取預設為在第二代檔案系統上啟用。如果您的第二代檔案系統具有輸送量密集的工作負載，您可以停用 NVMe 快取來改善效能。下列程序說明如何啟用、停用和驗證檔案系統的 NVMe 快取。

### 管理 NVMe 快取

1. SSH 到您的 ONTAP 檔案系統。如需詳細資訊，請參閱[the section called “使用 NetApp ONTAP CLI”](#)。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. 使用 [system node external-cache modify](#) ONTAP CLI command。選擇 **true** 以啟用 NVMe 快取或 **false** 停用它。

```
::> system node external-cache modify -node * -is-enabled [true|false]
```

3. 使用 [system node external-cache show](#) ONTAP CLI 命令來檢查 NVMe 快取是否啟用或停用。

```
::> system node external-cache show -node * -fields is-enabled
```

NVMe 快取是以每個節點為基礎啟用或停用。當您將新的高可用性 (HA) 對新增至檔案系統時，每個新節點都有與新檔案系統節點相同的預設行為。因此，即使現有節點已停用，也會為檔案系統上的任何新節點啟用 NVMe 快取。如需詳細資訊，請參閱[新增高可用性 \(HA\) 對](#)。

## 監控檔案系統詳細資訊

您可以使用 Amazon FSx 主控台、AWS CLI 和 API 和支援的 AWS SDKs，檢視 FSx for ONTAP 檔案系統的詳細組態資訊。

若要檢視詳細的檔案系統資訊：

- 使用主控台 – 選擇檔案系統以檢視檔案系統詳細資訊頁面。摘要面板顯示檔案系統的 ID、生命週期狀態、部署類型、SSD 儲存容量、輸送量容量、佈建 IOPS、可用區域和建立時間。

下列索引標籤提供詳細的組態資訊和編輯可修改的屬性：

- 網路與安全
- 監控與效能 – 顯示您已建立的 CloudWatch 警示，以及下列類別的指標和警告：
  - 摘要 – 檔案系統活動指標的高階摘要

- 檔案系統儲存容量
- 檔案伺服器磁碟效能

如需詳細資訊，請參閱[使用 Amazon CloudWatch 監控](#)。

- 管理 – 顯示下列檔案系統管理資訊：
  - 檔案系統管理和叢集間端點DNS的名稱和IP地址。
  - ONTAP 管理員使用者名稱。
  - 更新ONTAP管理員密碼的選項。
- 檔案系統的 SVMs清單
- 檔案系統的磁碟區清單
- 備份設定 – 變更檔案系統的自動每日備份設定。
- 更新 – 顯示使用者對檔案系統的組態所啟動更新的狀態。
- 標籤 – 檢視、編輯、新增、移除標籤鍵值對。
- 使用 CLI 或 API – 使用 [describe-file-systems](#) CLI 命令或 [DescribeFileSystems](#) API 操作。

## FSx for ONTAP 檔案系統狀態

您可以使用 Amazon FSx 主控台、AWS CLI 命令 [describe-file-systems](#) 或 API 操作 [DescribeFileSystems](#) 來檢視 Amazon FSx 檔案系統的狀態。

| 檔案系統狀態        | 描述                                                                                                                        |
|---------------|---------------------------------------------------------------------------------------------------------------------------|
| AVAILABLE     | 檔案系統已成功建立，可供使用。                                                                                                           |
| CREATING      | Amazon FSx 正在建立新的檔案系統。                                                                                                    |
| DELETING      | Amazon FSx 正在刪除現有的檔案系統。                                                                                                   |
| MISCONFIGURED | 檔案系統處於設定錯誤但可復原的狀態。                                                                                                        |
| 失敗            | <ol style="list-style-type: none"> <li>1. 檔案系統失敗，Amazon FSx 無法復原它。</li> <li>2. 建立新檔案系統時，Amazon FSx 無法建立新的檔案系統。</li> </ol> |



## 刪除檔案系統

您可以使用 Amazon FSx 主控台、AWS CLI 和 Amazon FSx API 和 SDKs 刪除 FSx for ONTAP 檔案系統。

若要刪除檔案系統：

- 使用 主控台 – 遵循中所述的程序 [清除資源](#)。
- 使用 CLI 或 API – 首先刪除檔案系統上的所有磁碟區和 SVMs。然後使用 [delete-file-system](#) CLI 命令或 [DeleteFileSystem](#) API 操作。

## 管理 FSx for ONTAP 儲存虛擬機器

在 FSx for ONTAP 中，磁碟區託管在稱為儲存虛擬機器 (SVMs) 虛擬檔案伺服器上。SVM 是隔離的檔案伺服器，具有自己的管理登入資料和端點，用於管理和存取資料。當您存取 FSx for ONTAP 中的資料時，用戶端和工作站會使用 SVM 的端點 (IP 地址) 掛載由 SVM 託管的磁碟區、SMB 共用或 iSCSI LUN。

當您使用 建立檔案系統時，Amazon FSx 會自動在您的檔案系統上建立預設 SVM AWS Management Console。您可以隨時使用 主控台 AWS CLI 或 Amazon FSx API 和 SDKs，在您的檔案系統上建立其他 SVMs。您無法使用 ONTAP CLI 或 REST API 建立 SVMs。

您可以將 SVMs 加入 Microsoft Active Directory 以進行檔案存取身分驗證和授權。如需詳細資訊，請參閱 [在 FSx for ONTAP 中使用 Microsoft Active Directory](#)。

## 每個檔案系統的 SVMs 數目上限

下表列出您可以為檔案系統建立 SVMs 數目上限。SVMs 的最大數量取決於佈建的輸送量容量，以每秒 MB (MBps) 為單位。

| 高可用性 (HA) 對 | 輸送量容量 (MBps) | 每個檔案系統的 SVMs 數目上限 |
|-------------|--------------|-------------------|
| 1 個 HA 對    | 128          | 6                 |
|             | 256          | 6                 |
|             | 384          | 6                 |



| 高可用性 (HA) 對 | 輸送量容量 (MBps) | 每個檔案系統的 SVMs 數目上限 |
|-------------|--------------|-------------------|
|             | 512          | 14                |
|             | 768          | 14                |
|             | 1,024        | 14                |
|             | 1,536        | 14                |
|             | 2,048        | 24                |
|             | 3 , 072      | 14                |
|             | 4,096        | 24                |
|             | 6,144        | 24                |
| 2–12 個 HA 對 | 任何           | 5                 |

## 主題

- [建立儲存虛擬機器 \(SVM\)](#)
- [更新儲存虛擬機器 \(SVM\)](#)
- [稽核檔案存取](#)
- [在工作群組中設定 SMB 伺服器](#)
- [監控儲存虛擬機器 \(SVM\) 組態詳細資訊](#)
- [刪除儲存虛擬機器 \(SVM\)](#)

## 建立儲存虛擬機器 (SVM)

您可以使用 AWS Management Console AWS CLI、和 API 建立 FSx for ONTAP SVM。

您可以為檔案系統建立的 SVMs 數量上限取決於檔案系統的部署類型和佈建的輸送量容量。如需詳細資訊，請參閱[每個檔案系統的 SVMs 數目上限](#)。

## SVM 屬性

建立 SVM 時，您可以定義下列屬性：

- 其所屬的 FSx for ONTAP 檔案系統。
- Microsoft Active Directory (AD) 組態 – 您可以選擇性地將 SVM 加入自我管理 AD，以驗證和控制 Windows 和 macOS 用戶端的存取控制。如需詳細資訊，請參閱[在 FSx for ONTAP 中使用 Microsoft Active Directory](#)。
- 根磁碟區安全樣式 – 設定根磁碟區安全樣式 (Unix 或 NTFS)，以與您用來存取 SVM 內資料的用戶端類型保持一致。如需詳細資訊，請參閱[磁碟區安全樣式](#)。
- SVM 管理密碼 – 您可以選擇性地設定 SVM vsadmin 使用者的密碼。如需詳細資訊，請參閱[使用 CLI ONTAP 管理 SVMs](#)。

### 建立儲存虛擬機器（主控台）

1. 開啟 Amazon FSx 主控台，網址為 <https://console.aws.amazon.com/fsx/>：//。
2. 在左側導覽窗格中，選擇儲存虛擬機器。
3. 選擇建立新的儲存虛擬機器。

建立新的儲存虛擬機器對話方塊隨即出現。

Create new storage virtual machine

×

File System

Select a filesystem ▼

Storage virtual machine name

Maximum of 47 alphanumeric characters, plus . - \_ .

SVM administrative password

Password for this SVM's "vsadmin" user, which you can use to access the ONTAP CLI or REST API.

☒ Don't specify a password
 ☐ Specify a password

Active Directory

Joining an Active Directory enables access from Windows and MacOS clients over the SMB protocol.

☐ Do not join an Active Directory
 ☒ Join an Active Directory

Net BIOS name

Active Directory domain name

This is the fully qualified domain name of your self-managed directory

example.com

DNS server IP addresses

IPv4 addresses of the DNS servers for your domain

10.0.0.1

10.0.0.2 - optional

10.0.0.3 - optional

Service account username

The username of the service account in your existing Active Directory. Do not include a domain prefix or suffix.

FSxServiceAccount

Service account password

The password for the service account provided above.

Maximum of 128 characters.

Confirm password

Organizational Unit (OU) within which you want to join your file system - optional

Specify the distinguished path name of the OU here

OU=org,DC=example,DC=com

Ensure that the service account provided has permissions delegated to the above OU or to the default OU if none is provided.

4. 針對檔案系統，選擇要建立儲存虛擬機器的檔案系統。
5. 在儲存虛擬機器名稱欄位中，提供儲存虛擬機器的名稱。您最多可以使用 47 個英數字元，加上底線 (\_) 特殊字元。
6. 對於 SVM 管理密碼，您可以選擇指定密碼，並為此 SVM vsadmin 的使用者提供密碼。您可以使用 vsadmin 使用者，使用 ONTAP CLI 或 REST API 來管理 SVM。如需 vsadmin 使用者的詳細資訊，請參閱 [使用 CLI ONTAP 管理 SVMs](#)。

如果您選擇不指定密碼（預設值），您仍然可以使用檔案系統的 fsxadmin 使用者，使用 ONTAP CLI 或 REST API 來管理您的檔案系統，但無法使用 SVM 的 vsadmin 使用者來執行相同的操作。

7. 針對 Active Directory，您有下列選項：
  - 如果您未將檔案系統加入 Active Directory (AD)，請選擇不加入 Active Directory。
  - 如果您要將 SVM 加入自我管理 AD 網域，請選擇加入 Active Directory，並提供 AD 的下列詳細資訊。如需詳細資訊，請參閱 [將 SVM 加入自我管理 Microsoft AD 的先決條件](#)。
    - 要為 SVM 建立之 Active Directory 電腦物件的 NetBIOS 名稱。NetBIOS 名稱不能超過 15 個字元。這是 Active Directory 中此 SVM 的名稱。
    - Active Directory 的完整網域名稱 (FQDN)。FQDN 不能超過 255 個字元。
    - DNS 伺服器 IP 地址 – 網域 DNS 伺服器的 IPv4 地址。
    - 服務帳戶使用者名稱 – 現有 Active Directory 中服務帳戶的使用者名稱。請勿包含網域字首或尾碼。對於 EXAMPLE\ADMIN，請使用 ADMIN。
    - 服務帳戶密碼 – 服務帳戶的密碼。
    - 確認密碼 – 服務帳戶的密碼。
    - (選用) 組織單位 (OU) – 您要加入檔案系統之組織單位的辨別路徑名稱。
    - 委派檔案系統管理員群組 – AD 中可管理檔案系統的群組名稱。

如果您使用的是 AWS AWS Managed Microsoft AD，則必須指定群組，例如委派的 FSx 管理員、AWS 委派的管理員，或具有委派 OU 許可的自訂群組。

如果您要加入自我管理 AD，請使用 AD 中的群組名稱。預設群組為 Domain Admins。

8. 針對 SVM 根磁碟區安全樣式，根據存取資料的用戶端類型，選擇 SVM 的安全樣式。如果您主要使用 Linux 用戶端存取資料，請選擇 Unix (Linux)；如果您主要使用 Windows 用戶端存取資料，請選擇 NTFS。如需詳細資訊，請參閱 [磁碟區安全樣式](#)。
9. 選擇確認以建立儲存虛擬機器。

您可以在儲存虛擬機器窗格的狀態欄中，監控檔案系統詳細資訊頁面上的更新進度。儲存虛擬機器的狀態建立時，即可供使用。

## 建立儲存虛擬機器 (CLI)

- 若要建立 FSx for ONTAP 儲存虛擬機器 (SVM)，請使用 [create-storage-virtual-machine](#) CLI 命令（或同等 [CreateStorageVirtualMachine](#) API 操作），如下列範例所示。

```
aws fsx create-storage-virtual-machine \
  --file-system-id fs-0123456789abcdef0 \
  --name svm1 \
  --svm-admin-password password \
  --active-directory-configuration
  SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
  OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",FileSystemAd
  \
  UserName="FSxService",Password="password", \
  DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

成功建立儲存虛擬機器後，Amazon FSx 會以 JSON 格式傳回其描述，如下列範例所示。

```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddresses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddresses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddresses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddresses": ["198.19.0.5", "198.19.0.6"]
      },
    },
  },
}
```

```

    "Iscsi": {
      "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com",
      "IpAddresses": ["198.19.0.7", "198.19.0.8"]
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATING",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/fs-0123456789abcdef0/svm-abcdef0123456789a",
    "StorageVirtualMachineId": "svm-abcdef0123456789a",
    "Subtype": "default",
    "Tags": [],
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
  }
}

```

## 更新儲存虛擬機器 (SVM)

您可以使用 Amazon FSx 主控台、AWS CLI 和 Amazon FSx API 更新下列儲存虛擬機器 (SVM) 組態屬性：

- SVM 管理帳戶密碼。
- SVM Active Directory (AD) 組態 – 您可以將 SVM 加入 AD，或修改已加入 AD 之 SVM 的 AD 組態。如需詳細資訊，請參閱 [管理 SVM Active Directory 組態](#)。

### 更新 SVM 管理員帳戶登入資料（主控台）

1. 開啟 Amazon FSx 主控台，網址為 <https://console.aws.amazon.com/fsx/>：//。

## 2. 選擇要更新的 SVM，如下所示：

- 在左側導覽窗格中，選擇檔案系統，然後選擇您要更新 SVM 的 ONTAP 檔案系統。
- 選擇儲存虛擬機器索引標籤。

–或–

- 若要顯示 AWS 帳戶 目前 中 中所有可用 SVMs 的清單 AWS 區域，請展開 ONTAP 並選擇儲存虛擬機器。

## 3. 選擇您要更新的儲存虛擬機器。

## 4. 選擇動作 > 更新管理員密碼。更新 SVM 管理登入資料視窗隨即出現。

## 5. 輸入vsadmin使用者的新密碼，並確認。

## 6. 選擇更新登入資料以儲存新密碼。

### 更新 SVM 管理員帳戶登入資料 (CLI)

- 若要更新 FSx for ONTAP SVM 的組態，請使用 [update-storage-virtual-machine](#) CLI 命令（或同等的 [UpdateStorageVirtualMachine](#) API 操作），如下列範例所示。

```
aws fsx update-storage-virtual-machine \
--storage-virtual-machine-id svm-abcdef01234567890 \
--svm-admin-password new-svm-password \
```

成功建立儲存虛擬機器後，Amazon FSx 會以 JSON 格式傳回其描述，如下列範例所示。

```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com",
        "IpAddresses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com",
        "IpAddresses": ["198.19.0.4"]
      }
    }
  }
}
```

```

    "Smb": {
      "DnsName": "amznfsx12345",
      "IpAddresses": ["198.19.0.4"]
    },
    "SmbWindowsInterVpc": {
      "IpAddresses": ["198.19.0.5", "198.19.0.6"]
    },
    "Iscsi": {
      "DnsName": "iscsi.svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com",
      "IpAddresses": ["198.19.0.7", "198.19.0.8"]
    }
  },
  "FileSystemId": "fs-0123456789abcdef0",
  "Lifecycle": "CREATING",
  "Name": "vol1",
  "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/fs-0123456789abcdef0/svm-abcdef01234567890",
  "StorageVirtualMachineId": "svm-abcdef01234567890",
  "Subtype": "default",
  "Tags": [],
  "ActiveDirectoryConfiguration": {
    "NetBiosName": "amznfsx12345",
    "SelfManagedActiveDirectoryConfiguration": {
      "UserName": "Admin",
      "DnsIps": [
        "10.0.1.3",
        "10.0.91.97"
      ],
      "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-ad,DC=customer-ad,DC=example,DC=com",
      "DomainName": "customer-ad.example.com"
    }
  }
}

```

## 稽核檔案存取

Amazon FSx for NetApp ONTAP 支援稽核最終使用者對儲存虛擬機器 (SVM) 中檔案和目錄的存取。

### 主題

- [檔案存取稽核概觀](#)



- [設定檔案存取稽核的任務概觀](#)

## 檔案存取稽核概觀

檔案存取稽核可讓您根據您定義的稽核政策，記錄個別檔案和目錄的最終使用者存取。檔案存取稽核可協助您改善系統的安全性，並降低未經授權存取系統資料的風險。檔案存取稽核可協助您的組織持續符合資料保護要求、及早識別潛在威脅，並降低資料外洩的風險。

在檔案和目錄存取中，Amazon FSx 支援記錄成功的嘗試（例如具有足夠許可的使用者成功存取檔案）、失敗的嘗試或兩者。您也可以隨時關閉檔案存取稽核。

根據預設，稽核事件日誌會以 EVTX 檔案格式存放，可讓您使用 Microsoft Event Viewer 檢視它們。

### 可稽核的 SMB 存取事件

下表列出可稽核的 SMB 檔案和資料夾存取事件。

| 事件 ID (EVT/EVTX) | 事件                      | 描述                                                                      | 類別   |
|------------------|-------------------------|-------------------------------------------------------------------------|------|
| 560/4656         | 開啟物件/建立物件               | OBJECT ACCESS :<br>開啟物件（檔案或目錄）                                          | 檔案存取 |
| 563/4659         | 具有要刪除意圖的開放物件            | OBJECT ACCESS :<br>使用刪除意圖來請求物件（檔案或目錄）的控制代碼                              | 檔案存取 |
| 564/4660         | 刪除物件                    | OBJECT ACCESS :<br>刪除物件（檔案或目錄）。當 Windows 用戶端嘗試刪除物件（檔案或目錄）時，ONTAP 會產生此事件 | 檔案存取 |
| 567/4663         | 讀取物件/寫入物件/取得物件屬性/設定物件屬性 | OBJECT ACCESS :<br>物件存取嘗試（讀                                             | 檔案存取 |

| 事件 ID (EVT/EVTX)         | 事件     | 描述                                                                                                                                                                                                                                                                 | 類別   |
|--------------------------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
|                          |        | <p>取、寫入、取得屬性、設定屬性 )。</p> <div>  <b>Note</b><br/>           在此事件中，ONTAP 只會稽核物件上的第一個 SMB 讀取和第一個 SMB 寫入操作（成功或失敗）。這可防止 ONTAP 在單一用戶端開啟物件並對相同物件執行許多連續的讀取或寫入操作時建立過多的日誌項目。         </div> |      |
| N/A/4664                 | 硬連結    | OBJECT ACCESS : 嘗試建立硬連結                                                                                                                                                                                                                                            | 檔案存取 |
| N/A/N/A ONTAP 事件 ID 9999 | 重新命名物件 | 物件存取：物件已重新命名。這是 ONTAP 事件。Windows 目前不支援它做為單一事件。                                                                                                                                                                                                                     | 檔案存取 |

| 事件 ID (EVT/EVTX)         | 事件     | 描述                                           | 類別   |
|--------------------------|--------|----------------------------------------------|------|
| N/A/N/A ONTAP 事件 ID 9998 | 取消連結物件 | 物件存取：物件未連結。這是 ONTAP 事件。Windows 目前不支援它做為單一事件。 | 檔案存取 |

## 可稽核的 NFS 存取事件

可以稽核下列 NFS 檔案和資料夾存取事件。

- READ
- OPEN
- CLOSE
- REaddir
- WRITE
- SETATTR
- CREATE
- 連結
- OPENATTR
- 移除
- GETATTR
- 驗證
- NVERIFY
- RENAME

## 設定檔案存取稽核的任務概觀

為檔案存取稽核設定 FSx for ONTAP 涉及下列高階任務：

1. [熟悉](#) 檔案存取稽核要求和考量事項。
2. 在特定 SVM 上 [建立稽核組態](#)。
3. 在該 SVM [上啟用稽核](#)。

4. 在檔案和目錄上[設定稽核政策](#)。
5. [在 FSx for ONTAP 發出稽核事件日誌之後，檢視稽核事件日誌](#)。FSx

任務詳細資訊會在下列程序中提供。

針對您要啟用檔案存取稽核之檔案系統上的任何其他 SVM 重複任務。

### 稽核需求

在 SVM 上設定和啟用稽核之前，您應該注意下列要求和考量事項。

- NFS 稽核支援稽核指定為類型 的存取控制項目 (ACEs)u，這會在物件上嘗試存取時產生稽核日誌項目。對於 NFS 稽核，模式位元和稽核 ACEs 之間沒有映射。將 ACLs 轉換為模式位元時，會略過稽核 ACEs。將模式位元轉換為 ACLs 時，不會產生稽核 ACEs。
- 稽核取決於預備磁碟區中的可用空間。（預備磁碟區是由 ONTAP 建立的專用磁碟區，用於存放預備檔案，這些檔案是在將稽核記錄轉換為 EVT X 或 XML 檔案格式之前存放於個別節點上的中繼二進位檔案。）您必須確保在包含稽核磁碟區的彙總中，預備磁碟區有足夠的空間。
- 稽核取決於磁碟區中的可用空間，其中包含存放轉換後稽核事件日誌的目錄。您必須確保用於存放事件日誌的磁碟區中有足夠的空間。您可以在建立稽核組態時使用 `-rotate-limit` 參數，指定要在稽核目錄中保留的稽核日誌數量，這有助於確保磁碟區中有足夠的可用空間供稽核日誌使用。

### 在 SVMs 上建立稽核組態

您必須先在儲存虛擬機器 (SVM) 上建立稽核組態，才能開始稽核檔案和目錄事件。建立稽核組態之後，您必須在 SVM 上啟用它。

使用 `vserver audit create` 命令建立稽核組態之前，請確定您已建立要做為日誌目的地的目錄，且該目錄沒有符號連結。您可以使用 `-destination` 參數指定目的地目錄。

您可以建立稽核組態，根據日誌大小或排程輪換稽核日誌，如下所示：

- 若要根據日誌大小輪換稽核日誌，請使用下列命令：

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}] [-rotate-limit integer] [-rotate-size {integer[KB|MB|GB|TB|PB]}]
```

下列範例會為名為 `svm1` 的 SVM 建立稽核組態，以使用以大小為基礎的輪換來稽核檔案操作和 CIFS (SMB) 登入和登出事件（預設）。日誌格式為 EVT X（預設值），日誌會存放在 `/audit_log` 目錄中，而且您一次會有一個日誌檔案（大小上限為 200MB）。

```
vserver audit create -vserver svm1 -destination /audit_log -rotate-size 200MB
```

- 若要根據排程輪換稽核日誌，請使用下列命令：

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}]  
[-rotate-limit integer] [-rotate-schedule-month chron_month]  
[-rotate-schedule-dayofweek chron_dayofweek] [-rotate-schedule-  
day chron_dayofmonth]  
[-rotate-schedule-hour chron_hour] [-rotate-schedule-minute chron_minute]
```

如果您要設定以時間為基礎的稽核日誌輪換，則需要 `-rotate-schedule-minute` 參數。

下列範例svm2會使用以時間為基礎的輪換，為名為 `svm2` 的 SVM 建立稽核組態。日誌格式為 EVTX（預設值），而稽核日誌會在一週內每天的中午 12：30 輪換。

```
vserver audit create -vserver svm2 -destination /audit_log -rotate-size 200MB -  
rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour 12 -  
rotate-schedule-minute 30
```

您可以使用 `-format` 參數來指定是以轉換後的EVTX格式（預設）還是XML檔案格式建立稽核日誌。EVTX 格式可讓您使用 Microsoft Event Viewer 檢視日誌檔案。

根據預設，要稽核的事件類別為檔案存取事件 (SMB 和 NFS)、CIFS (SMB) 登入和登出事件，以及授權政策變更事件。您可以更好地控制 參數要記錄哪些事件-events，其格式如下：

```
-events {file-ops|cifs-logon-logoff|cap-staging|file-share|audit-policy-change|user-  
account|authorization-policy-change|security-group}
```

例如，使用 `-events file-share`可稽核檔案共享事件。

如需 `vserver audit create`命令的詳細資訊，請參閱[建立稽核組態](#)。

在 SVM 上啟用稽核

完成稽核組態的設定後，您必須在 SVM 上啟用稽核。若要這麼做，請使用下列命令：

```
vserver audit enable -vserver svm_name
```

例如，使用下列命令在名為 `svm1` 的 SVM 上啟用稽核。

```
vserver audit enable -vserver svm1
```

您可以隨時停用存取稽核。例如，使用下列命令來關閉名為的 SVM 稽核svm4。

```
vserver audit disable -vserver svm4
```

當您停用稽核時，不會刪除 SVM 上的稽核組態，這表示您可以隨時對該 SVM 重新啟用稽核。

## 設定檔案和資料夾稽核政策

您需要針對要針對使用者存取嘗試進行稽核的檔案和資料夾設定稽核政策。您可以設定稽核政策來監控成功和失敗的存取嘗試。

您可以同時設定 SMB 和 NFS 稽核政策。根據磁碟區的安全樣式，SMB 和 NFS 稽核政策具有不同的組態要求和稽核功能。

## NTFS 安全樣式檔案和目錄上的稽核政策

您可以使用 Windows 安全索引標籤或 ONTAP CLI 來設定 NTFS 稽核政策。

### 設定 NTFS 稽核政策 (Windows 安全索引標籤)

您可以透過將項目新增至與 NTFS 安全描述項相關聯的 NTFS SACLs 來設定 NTFS 稽核政策。然後，安全描述項會套用至 NTFS 檔案和目錄。這些任務由 Windows GUI 自動處理。安全描述項可包含用於套用檔案和資料夾存取許可的選擇性存取控制清單 (DACLS)、用於檔案和資料夾稽核的 SACLs，或同時 SACLs 和 DACLS。

1. 在 Windows Explorer 的工具選單中，選取映射網路磁碟機。
2. 完成映射網路磁碟機方塊：
  - a. 選擇磁碟機代號。
  - b. 在資料夾方塊中，輸入包含共用的 SMB (CIFS) 伺服器名稱，保留您要稽核的資料和共用的名稱。
  - c. 選擇 Finish (完成)。

您選取的磁碟機已掛載，並準備好 Windows Explorer 視窗，其中顯示共用中包含的檔案和資料夾。

3. 選取您要啟用稽核存取權的檔案或目錄。

4. 在檔案或目錄上按一下滑鼠右鍵，然後選擇屬性。
5. 選擇 Security (安全) 標籤。
6. 按一下進階。
7. 選擇稽核索引標籤。
8. 執行所需的動作：

| 如果您想要...     | 執行下列動作                                                                                                                                        |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| 設定新使用者或群組的稽核 | <ol style="list-style-type: none"> <li>1. 選擇新增。</li> <li>2. 在輸入要選取的物件名稱方塊中，輸入您要新增的使用者或群組名稱。</li> <li>3. 選擇確定。</li> </ol>                      |
| 從使用者或群組移除稽核  | <ol style="list-style-type: none"> <li>1. 在輸入要選取的物件名稱方塊中，選取要移除的使用者或群組。</li> <li>2. 選擇移除。</li> <li>3. 選擇確定。</li> <li>4. 略過此程序的其餘部分。</li> </ol> |
| 變更使用者或群組的稽核  | <ol style="list-style-type: none"> <li>1. 在輸入要選取的物件名稱方塊中，選擇您要變更的使用者或群組。</li> <li>2. 選擇編輯。</li> <li>3. 選擇確定。</li> </ol>                        |

如果您要在使用者或群組上設定稽核，或在現有使用者或群組上變更稽核，則會開啟##的稽核項目方塊。

9. 在套用至方塊中，選取您要如何套用此稽核項目。

如果您要在單一檔案上設定稽核，則套用至方塊不會處於作用中狀態，因為它預設為僅此物件。

10. 在存取方塊中，選取您想要稽核的內容，以及您要稽核成功的事件、失敗事件或兩者。
  - 若要稽核成功事件，請選擇成功方塊。
  - 若要稽核失敗事件，請選擇失敗方塊。

選擇您需要監控的動作，以符合您的安全需求。如需這些可稽核事件的詳細資訊，請參閱您的 Windows 文件。您可以稽核下列事件：

- 完全控制
  - 周遊資料夾/執行檔案
  - 列出資料夾/讀取資料
  - 讀取屬性
  - 讀取延伸屬性
  - 建立檔案/寫入資料
  - 建立資料夾/附加資料
  - 寫入屬性
  - 寫入延伸屬性
  - 刪除子資料夾和檔案
  - Delete
  - 讀取許可
  - 變更許可
  - 取得所有權
11. 如果您不希望稽核設定傳播至原始容器的後續檔案和資料夾，請選擇僅將這些稽核項目套用至此容器內的物件和/或容器方塊。
12. 選擇套用。
13. 完成新增、移除或編輯稽核項目後，請選擇確定。

**##**的稽核項目方塊會關閉。

14. 在稽核方塊中，選擇此資料夾的繼承設定。僅選擇提供符合您安全需求的稽核事件的最低層級。

您可以選擇下列其中之一：

- 從此物件的父方塊中選擇包含可繼承稽核項目。
- 選擇從此物件方塊中使用可繼承稽核項目取代所有子系上所有現有的可繼承稽核項目。
- 選擇兩個方塊。
- 選擇任一方塊。

如果您要在單一檔案上設定 SACLS，則稽核方塊中不會出現使用來自此物件方塊的可繼承稽核項目取代所有子系上所有現有的可繼承稽核項目。

#### 15. 選擇確定。



## 設定 NTFS 稽核政策 (ONTAP CLI)

透過使用 ONTAP CLI，您可以設定 NTFS 稽核政策，而無需使用 Windows 用戶端上的 SMB 共用連線到資料。

- 您可以使用 [vserver 安全檔案目錄 ntfs sac1 新增](#) 命令系列來設定 NTFS 稽核政策。

例如，下列命令 p1 會為名為 `vs0` 的 SVM 建立名為 `vs0` 的安全政策。

```
vserver security file-directory policy create -policy-name p1 -vserver vs0
```

然後，以下命令會將 p1 安全政策套用至 `vs0` SVM。

```
vserver security file-directory apply -vserver vs0 -policy-name p1
```

## UNIX 安全樣式檔案和目錄上的稽核政策

您可以將稽核 ACEs（存取控制表達式）新增至 NFS v4.x ACLs 稽核。這可讓您基於安全考量，監控特定 NFS 檔案和目錄存取事件。

### Note

對於 NFS v4.x，可自由決定的和系統 ACEs 都存放在相同的 ACL 中。因此，在將稽核 ACEs 新增至現有的 ACL 時必須小心，以避免覆寫和遺失現有的 ACL。將稽核 ACEs 新增至現有 ACL 的順序並不重要。

## 設定 UNIX 稽核政策

1. 使用 `getfacl` 或 `ls -la` 命令擷取檔案 `nfs4_getfacl` 或目錄的現有 ACL。
2. 附加所需的稽核 ACEs。
3. 使用 `setfacl` 或 `ls -la` 命令，將更新的 ACL 套用至檔案 `nfs4_setfacl` 或目錄。

此範例使用 `-a` 選項為使用者（名為 `testuser`）提供名為 `file1` 的檔案讀取許可。

```
nfs4_setfacl -a "A::testuser@example.com:R" file1
```

## 檢視稽核事件日誌

您可以檢視以 EVTX 或 XML 檔案格式儲存的稽核事件日誌。

- EVTX 檔案格式 – 您可以使用 Microsoft Event Viewer 將轉換後的 EVTX 稽核事件日誌開啟為已儲存的檔案。

使用事件檢視器檢視事件日誌時，您可以使用兩個選項：

- 一般檢視：事件記錄會顯示所有事件的常見資訊。不會顯示事件記錄的事件特定資料。您可以使用詳細檢視來顯示事件特定資料。
- 詳細檢視：提供易記檢視和 XML 檢視。易記檢視和 XML 檢視會顯示所有事件的常見資訊，以及事件記錄的事件特定資料。
- XML 檔案格式 – 您可以在支援 XML 檔案格式的第三方應用程式上檢視和處理 XML 稽核事件日誌。只要您有 XML 結構描述和 XML 欄位定義的相關資訊，就可以使用 XML 檢視工具來檢視稽核日誌。

## 在工作群組中設定 SMB 伺服器

您可以在工作群組中設定伺服器訊息區塊 (SMB) 伺服器，做為在 [Microsoft Active Directory 網域基礎設施無法使用時將 SVM](#) 加入 Microsoft Active Directory 的替代方案。工作群組是使用 SMB 通訊協定的 peer-to-peer 網路，且只有本機帳戶和群組。

將 SMB 伺服器設定為工作群組中成員的程序包含下列項目：

- 在儲存虛擬機器 (SVM) 上建立 SMB 伺服器。
- 建立本機使用者和群組。
- 新增本機使用者或群組做為工作群組的成員。

請記住，工作群組模式中的 SMB 伺服器不支援下列 SMB 功能：

- SMB3 見證通訊協定
- SMB3 CA 共用
- 透過 SMB 的 SQL
- 資料夾重新導向
- 漫遊設定檔
- 群組政策物件 (GPO)
- 磁碟區快照服務 (VSS)

此外，工作群組模式中的 SMB 伺服器僅支援 NTLM 身分驗證，不支援 Kerberos 身分驗證。

下列程序會逐步引導您在工作群組的 SVM 上設定 SMB 伺服器、建立本機帳戶，以及將這些帳戶新增至工作群組成員資格。您將從檔案系統或 SVM 管理界面使用 NetApp ONTAP CLI 來實作這些程序。如需詳細資訊，請參閱[使用 NetApp ONTAP CLI](#)。

## 主題

- [在工作群組中建立 SMB 伺服器](#)
- [在 SMB 伺服器上建立本機使用者帳戶](#)
- [在 SMB 伺服器上建立本機群組](#)
- [將本機使用者新增至本機群組](#)

## 在工作群組中建立 SMB 伺服器

您可以使用 [vserver cifs create](#) ONTAP CLI 命令在 SVM 上建立 SMB 伺服器，並指定其所屬的工作群組。

### 開始之前

您用來提供資料的 SVM 和磁碟區（和介面）必須已設定為允許 SMB 通訊協定。

LIFs 必須能夠連線到 SVM 上設定的 DNS 伺服器。檔案系統可能需要 CIFS 授權，但如果 SMB 伺服器僅用於身分驗證，則不需要 CIFS 授權。

### 在工作群組中建立 SMB 伺服器

1. 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。*management\_endpoint\_ip* 將取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

2. 在工作群組中建立 SMB 伺服器：

```
FSxIdabcde123456::> vserver cifs create -vserver vserver_name -cifs-  
server cifs_server_name -workgroup workgroup_name [-comment workgroup_description]
```

下列命令會在工作群組 `smb_server01` 中建立 SMB 伺服器 `workgroup01`：

```
FSxIdabcde123456:> vservers cifs create -vservers svm1 -cifs-server SMB_SERVER01 -
workgroup workgroup01
```

如果您連線到 SVM 的管理連接埠，則不需要指定 `-vservers`。

### 3. 使用 `vservers cifs show` 命令驗證 SMB 伺服器組態。

在下列範例中，命令輸出顯示名為 `smb_server01` 的 SMB 伺服器是在工作群組 `svm1` 的 SVM 上建立 `workgroup01`：

```
FSxIdabcde123456:> vservers cifs show -vservers svm1

Vserver: svm1
CIFS Server NetBIOS Name: SMB_SERVER01
NetBIOS Domain/Workgroup Name: workgroup01
Fully Qualified Domain Name: -
Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
Workgroup Name: workgroup01
Authentication Style: workgroup
CIFS Server Administrative Status: up
CIFS Server Description:
List of NetBIOS Aliases: -
```

## 在 SMB 伺服器上建立本機使用者帳戶

您可以建立本機使用者帳戶，用來授權透過 SMB 連線存取 SVM 中包含的資料。您也可以在建立 SMB 工作階段時使用本機使用者帳戶進行身分驗證。SVM 建立時，預設會啟用本機使用者功能。建立本機使用者帳戶時，您必須指定使用者名稱，而且必須指定要與帳戶建立關聯的 SVM。

### 在 SMB 伺服器上建立本機使用者帳戶

#### 1. 使用 CLI [vservers cifs users-and-groups local-user create](#) ONTAP 命令建立本機使用者：

```
vservers cifs users-and-groups local-user create -vservers svm_name -user-
name user_name optional_parameters
```

下列選用參數可能很有用：

- `-full-name` – 使用者的全名。
- `-description` – 本機使用者的描述。
- `-is-account-disabled {true|false}` – 指定使用者帳戶是啟用或停用。如果未指定此參數，則預設為啟用使用者帳戶。

命令會提示輸入本機使用者的密碼。

2. 輸入本機使用者的密碼，然後確認密碼。
3. 確認使用者已成功建立：

```
vserver cifs users-and-groups local-user show -vserver svm_name
```

下列範例會建立與 SVM 相關聯的本機使用者 Sue Chang，SMB\_SERVER01\sue 其全名為 svm1：

```
FSxIdabcde123456:> vserver cifs users-and-groups local-user create -vserver svm1  
-user-name SMB_SERVER01\sue -full-name "Sue Chang"
```

Enter the password:

Confirm the password:

```
FSxIdabcde123456:> vserver cifs users-and-groups local-user show
```

| Vserver | User Name                  | Full Name | Description                    |
|---------|----------------------------|-----------|--------------------------------|
| svm1    | SMB_SERVER01\Administrator |           | Built-in administrator account |
| svm1    | SMB_SERVER01\sue           | Sue Chang |                                |

## 在 SMB 伺服器上建立本機群組

您可以建立本機群組，用於授權透過 SMB 連線存取與 SVM 相關聯的資料。您也可以指派權限來定義群組成員擁有的使用者權利或功能。

本機群組功能預設會在建立 SVM 時啟用。建立本機群組時，您必須指定群組的名稱，而且必須指定要與群組建立關聯的 SVM。您可以指定具有或沒有本機網域名稱的群組名稱，也可以選擇性地指定本機群組的描述。您無法將本機群組新增至另一個本機群組。

### 在 SMB 伺服器上建立本機群組

1. 使用 CLI [`vserver cifs users-and-groups local-group create`](#) ONTAP 命令建立本機群組。

```
vserver cifs users-and-groups local-group create -vserver svm_name -group-  
name group_name [-description local_group_description]
```

包含本機群組的描述很有用。

## 2. 確認已成功建立群組：

```
vserver cifs users-and-groups local-group show -vserver svm_name
```

下列範例會建立與 SVM SMB\_SERVER01\engineering 相關聯的本機群組 svm1：

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group create -vserver svm1 -  
group-name SMB_SERVER01\engineering
```

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group show -vserver svm1
```

| Vserver | Group Name               | Description                          |
|---------|--------------------------|--------------------------------------|
| svm1    | BUILTIN\Administrators   | Built-in Administrators group        |
| svm1    | BUILTIN\Backup Operators | Backup Operators group               |
| svm1    | BUILTIN\Guests           | Built-in Guests group                |
| svm1    | BUILTIN\Power Users      | Restricted administrative privileges |
| svm1    | BUILTIN\Users            | All users                            |
| svm1    | SMB_SERVER01\engineering |                                      |

## 將本機使用者新增至本機群組

您可以新增和移除本機或網域使用者，或新增和移除網域群組，以管理本機群組成員資格。如果您想要根據放置在群組上的存取控制來控制對資料的存取，或者您希望使用者擁有與該群組相關聯的權限，這會很有用。如果您不再希望本機使用者、網域使用者或網域群組根據群組中的成員資格擁有存取權或權限，您可以從群組中移除成員。

將成員新增至本機群組時，請記住下列事項：

- 您無法將使用者新增至特殊的每個人群組。
- 您無法將本機群組新增至另一個本機群組。
- 若要將網域使用者或群組新增至本機群組，ONTAP 必須能夠將名稱解析為 SID。

從本機群組移除成員時，請記住下列事項：

- 您無法從特殊的每個人群組中移除成員。
- 若要從本機群組移除成員，ONTAP 必須能夠將其名稱解析為 SID。

您需要 fsxadmin 角色才能執行此程序中使用的命令。如需詳細資訊，請參閱 [ONTAP 角色和使用者](#)。

### 管理本機群組成員資格

- 使用 [vserver cifs users-and-groups local-group add-members](#) 和 [vserver cifs users-and-groups local-group remove-members](#) CLI 命令，將成員新增至群組或從群組中移除成員。ONTAP
- 若要將成員新增至工作群組：

```
vserver cifs users-and-groups local-group add-members -vserver svm_name -group-name group_name -member-names name[,...]
```

您可以指定以逗號分隔的本機使用者、網域使用者或網域群組清單，以新增至指定的本機群組。

- 若要檢視工作群組的成員：

```
vserver cifs users-and-groups local-group show-members -vserver svm_name -group-name group_name
```

- 若要從工作群組移除成員：

```
vserver cifs users-and-groups local-group remove-members -vserver svm_name -group-name group_name -member-names name[,...]
```

您可以指定以逗號分隔的本機使用者、網域使用者或網域群組清單，以從指定的本機群組中移除。

下列範例 SMB\_SERVER01\sue 會將本機使用者新增至 SVM SMB\_SERVER01\engineering 上的本機群組 svm1：

```
FSxIdabcde123456:> vserver cifs users-and-groups local-group add-members -vserver svm1 -group-name SMB_SERVER01\engineering -member-names SMB_SERVER01\sue
```

下列範例會從 SMB\_SERVER01\engineering 上的 SMB\_SERVER01\james 本機群組移除本機使用者 SMB\_SERVER01\sue 和 svm1：

```
FSxIdabcde123456::> vservers cifs users-and-groups local-group remove-  
members -vservers svm1 -group-name SMB_SERVER01\engineering -member-names  
SMB_SERVER01\sue,SMB_SERVER01\james
```

下列範例列出本機群組的成員 SMB\_SERVER01\engineering：

```
FSxIdabcdef01234::> vservers cifs users-and-groups local-group show-members -  
vservers svm_name -group-name group_name  
  
Vserver: svm1  
Domain Name: SMB_SERVER01  
Group Name: SMB_SERVER01\engineering  
Member Name: SMB_SERVER01\anita  
SMB_SERVER01\james  
SMB_SERVER01\liang
```

## 監控儲存虛擬機器 (SVM) 組態詳細資訊

您可以使用 Amazon FSx 主控台、AWS CLI、和 Amazon FSx API，查看目前位於檔案系統的 FSx for ONTAP 儲存虛擬機器。

若要在檔案系統上檢視儲存虛擬機器：

- 使用主控台 – 選擇檔案系統以檢視其檔案系統詳細資訊頁面。若要列出檔案系統上的所有儲存虛擬機器，請選擇儲存虛擬機器索引標籤，然後選擇您要檢視的儲存虛擬機器。
- 使用 CLI 或 API – 使用 [describe-storage-virtual-machines](#) CLI 命令或 [DescribeStorageVirtualMachines](#) API 操作。

系統回應是帳戶中所有 SVMs 的完整描述清單 AWS 區域。

## 刪除儲存虛擬機器 (SVM)

您只能使用 Amazon FSx 主控台、AWS CLI、和 API 刪除 FSx for ONTAP SVM。您必須先刪除連接到 SVM 的所有非根磁碟區，才能刪除 SVM。



**⚠ Important**

您無法使用 NetApp ONTAP CLI 或 API 刪除 SVM。

**ℹ Note**

刪除儲存虛擬機器之前，請確定沒有任何應用程式正在存取 SVM 中的資料，而且您已刪除所有連接到 SVM 的非根磁碟區。

### 刪除儲存虛擬機器（主控台）

1. 在 Amazon FSx 主控台開啟 <https://console.aws.amazon.com/fsx/>。
2. 選擇您要刪除的 SVM，如下所示：
  - 在左側導覽窗格中，選擇檔案系統，然後選擇要刪除 SVM 的 ONTAP 檔案系統。
  - 選擇儲存虛擬機器索引標籤。

–或–

  - 若要顯示所有可用 SVMs 的清單，請展開 ONTAP 並選擇儲存虛擬機器。

從清單中選擇要刪除的 SVM。

3. 在磁碟區索引標籤中，檢視連接到 SVM 的磁碟區清單。如果有任何非根磁碟區連接到 SVM，您必須先刪除它們，才能刪除 SVM。如需更多資訊，請參閱[刪除磁碟區](#)。
4. 從動作功能表中選擇刪除儲存虛擬機器。
5. 在刪除確認對話方塊中，選擇刪除儲存虛擬機器。

### 刪除儲存虛擬機器 (CLI)

- 若要刪除 FSx for ONTAP 儲存虛擬機器，請使用 [delete-storage-virtual-machine](#) CLI 命令（或同等 [DeleteStorageVirtualMachine](#) API 操作），如下列範例所示。

```
aws fsx delete-storage-virtual-machine --storage-virtual-machine-id svm-
abcdef0123456789d
```

## 管理 ONTAP 磁碟區的 FSx

FSx for ONTAP 檔案系統上的每個儲存虛擬機器 (SVM) 可以有一或多個磁碟區。磁碟區是檔案、目錄或 iSCSI 邏輯儲存單位 (LUNs) 的隔離資料容器。磁碟區是精簡佈建的，這表示它們只會針對存放在其中的資料使用儲存容量。

您可以透過網路檔案系統 (NFS) 通訊協定、伺服器訊息區塊 (SMB) 通訊協定，或透過網際網路小型電腦系統介面 (iSCSI) 通訊協定，建立 iSCSI LUN (共用區塊儲存)，從 Linux、Windows 或 macOS 用戶端存取磁碟區。FSx for ONTAP 也支援對相同磁碟區的多協定存取 (並行 NFS 和 SMB 存取)。

您可以使用 AWS Management Console、AWS CLI、Amazon FSx API 或 NetApp BlueXP 來建立磁碟區。您也可以使用檔案系統或 SVM 的管理端點，透過 NetApp ONTAP CLI 或 REST API 來建立、更新和刪除磁碟區。

### Note

您可以為每個 HA 對建立 500 個磁碟區，所有 HA 對最多可建立 1,000 個磁碟區。FlexGroup 組成磁碟區會計入此限制。根據預設，每個磁碟區總有八個組成磁碟區 FlexGroup。

建立磁碟區時，您可以定義下列屬性：

- 磁碟區樣式 – [磁碟區樣式](#) 可以是 FlexVol 或 FlexGroup。
- 磁碟區名稱 – 磁碟區的名稱。
- 磁碟區類型 – [磁碟區類型](#) 可以是讀寫 (RW) 或資料保護 (DP)。DP 磁碟區是唯讀的，並用作 NetApp SnapMirror 或 SnapVault 關係中的目的地。
- 磁碟區大小 – 這是磁碟區可存放的最大資料量，無論儲存層為何。
- 連接路徑 – 這是 SVM 命名空間中磁碟區掛載的位置。
- 儲存效率 – [儲存效率](#) 功能，包括資料壓縮、壓縮和重複資料刪除，可為一般用途的檔案共用工作負載提供節省 65% 的典型儲存。
- 磁碟區 [安全樣式](#) (Unix 或 NTFS) – 決定在授權使用者時，用於磁碟區資料存取的許可類型。
- 資料分層 – [分層政策](#) 會定義哪些資料存放在經濟實惠的容量集區層中。
- [分層政策冷卻期間](#) – 定義資料標示為冷並移至容量集區儲存的時間。
- 快照政策 – [快照政策](#) 定義系統如何為磁碟區建立快照。您可以從三個預先定義的政策中選擇，或使用自訂政策。您已使用 ONTAP CLI 或 REST API 建立。

- [將標籤複製到備份](#) – Amazon FSx 會使用此選項自動將任何標籤從磁碟區複製到備份。您可以使用 AWS CLI 或 Amazon FSx API 設定此選項。

## 主題

- [磁碟區樣式](#)
- [磁碟區類型](#)
- [磁碟區安全樣式](#)
- [建立磁碟區](#)
- [更新磁碟區](#)
- [在彙總之間移動磁碟區](#)
- [監控磁碟區](#)
- [刪除磁碟區](#)

## 磁碟區樣式

FSx for ONTAP 提供兩種類型的磁碟區，可用於不同的用途。您可以使用 Amazon FSx 主控台、AWS CLI 和 Amazon FSx API 建立 FlexVol 或 FlexGroup 磁碟區。

- FlexVol 磁碟區為具有一個高可用性 (HA) 對的檔案系統提供最簡單的體驗，因此它們是第一代檔案系統和具有一個 HA 對的第二代檔案系統的預設磁碟區樣式。FlexVol 磁碟區的最小大小為 20 MB (MiB)，最大大小為 314,572,800 MiB。
- FlexGroup 磁碟區由多個組成 FlexVol 磁碟區組成，這使得它們能夠提供比具有多個 HA 對的檔案系統 FlexVol 磁碟區更高的效能和儲存可擴展性。FlexGroup 磁碟區是具有多個 HA 對的第二代檔案系統的預設磁碟區樣式。磁碟 FlexGroup 區的大小下限為每個組份 100 GB (GiB)，而大小上限為 20 GB (PiB)。

您可以使用 CLI 將具有 FlexVol 樣式的磁碟區轉換為 ONTAP FlexGroup 樣式，這會建立 FlexGroup 具有單一成分的。不過，我們建議您使用 AWS DataSync 在 FlexVol 磁碟區和新 FlexGroup 磁碟區之間移動資料，以確保資料平均分散到 FlexGroup's 元件。如需詳細資訊，請參閱[FlexGroup 成分](#)。

**Note**

如果您想要使用 ONTAP CLI 將 FlexVol 磁碟區轉換為 FlexGroup 磁碟區，請務必先刪除磁碟 FlexVol 區的任何備份，再進行轉換。ONTAP 不會自動重新平衡資料做為轉換的一部分，因此資料可能會在 FlexGroup 元件之間不平衡。

## FlexGroup 成分

FlexGroup 磁碟區是由 磁碟 FlexVol 區組成。根據預設，適用於 ONTAP 的 FSx 會將八個成分指派給每個 HA 對的 FlexGroup 磁碟區。

當您建立磁碟 FlexGroup 區時，其大小會平均分散在各組份中。例如，如果您建立具有八個組分的 800 GB (GB) FlexGroup 磁碟區，則每個組分的大小為 100 GB。FlexGroup 磁碟區的大小可以介於 100 GB 到 20 PiB 之間，但總大小取決於元件的大小。每個元件的大小下限為 100 GB，大小上限為 300 TiB。例如，具有八個組成元素的 FlexGroup 磁碟區大小下限為 800 GB，大小上限為 20 PiB。

ONTAP 會在檔案層級將資料分散至各組份。您可以在磁碟 FlexGroup 區的每個組份中儲存最多 20 億個檔案。

當您更新 FlexGroup 磁碟區的大小時，新大小會平均分散在現有的元件中。

您也可以使用 CLI ONTAP 或 REST API 將更多元件新增至磁碟 FlexGroup 區。不過，我們建議您只有在需要額外的儲存容量，且所有元件都已處於其大小上限（每個元件 300 TiB）時，才這麼做。新增組份可能會導致各組份的資料和 I/O 不平衡。在成分平衡之前，寫入輸送量可能會比平衡 FlexGroup 磁碟區低 5–10%。將新資料寫入 FlexGroup 磁碟區時，ONTAP 會優先將其分散到新的元件中，直到元件平衡為止。如果您確實新增了元件，建議您選擇偶數，但每個彙總不超過八個。

**Note**

如果您新增元件，現有的快照會變成部分快照；因此，它們無法用來將您的 FlexGroup 磁碟區完全還原為先前的狀態。先前的快照無法提供磁碟 FlexGroup 區的完整 point-in-time 影像，因為新的元件尚未存在。不過，部分快照可用來還原個別檔案和目錄、建立新磁碟區，或使用複製 SnapMirror。

## 磁碟區類型

FSx for ONTAP 提供兩種類型的磁碟區，您可以使用 Amazon FSx 主控台、AWS CLI 和 Amazon FSx API 建立。

- 在大多數情況下會使用讀寫 (RW) 磁碟區。如其名稱所示，它們是可讀取的。
- 資料保護 (DP) 磁碟區是您用來做為 NetAppSnapMirror或 SnapVault 關係目的地的唯讀磁碟區。當您想要[遷移](#)或[保護](#)單一磁碟區的資料時，應使用 DP 磁碟區。

FlexVol 和 FlexGroup磁碟區可以是 RW 或 DP。

#### Note

您無法在建立磁碟區後更新磁碟區的類型。

## 磁碟區安全樣式

為 ONTAP 磁碟區建立 FSx 時，您可以從兩種安全樣式中選擇：Unix 和 NTFS。每個安全樣式對處理資料許可的方式都有不同的影響。您必須了解不同的效果，以確保您為目的選擇適當的安全樣式。

請務必了解安全樣式無法判斷哪些用戶端類型可以存取或無法存取資料。安全樣式只會決定 FSx for ONTAP 用於控制資料存取的許可類型，以及哪些用戶端類型可以修改這些許可。

您用來判斷磁碟區安全樣式的兩個因素是管理檔案系統的管理員類型，以及存取磁碟區資料的使用者或服務類型。

在 Amazon FSx 主控台、CLI 和 API 中建立磁碟區時，安全樣式會自動設定為根磁碟區的安全樣式。您可以使用 AWS CLI 或 API 來修改磁碟區的安全樣式。您可以在建立磁碟區後修改此設定。如需更多資訊，請參閱[更新磁碟區](#)。

當您在磁碟區上設定安全樣式時，請考慮環境的需求，以確保您選取最佳安全樣式，以避免管理許可的問題。請記住，安全樣式無法判斷哪些用戶端類型可以存取資料。安全樣式會決定用於允許資料存取的許可，以及可修改這些許可的用戶端類型。以下是可協助您決定磁碟區選擇哪種安全樣式的考量：

- Unix (Linux) – 如果檔案系統是由 Unix 管理員管理、大多數使用者是 NFS 用戶端，而存取資料的應用程式使用 Unix 使用者做為服務帳戶，請選擇此安全樣式。只有 Linux 用戶端可以使用 Unix 安全樣式修改許可，而且檔案和目錄上使用的許可類型是 mode-bits 或 NFS v4.x ACLs。
- NTFS – 如果檔案系統是由 Windows 管理員管理，且大多數使用者是 SMB 用戶端，而存取資料的應用程式使用 Windows 使用者做為服務帳戶，請選擇此安全樣式。如果磁碟區需要任何 Windows 存取，建議您使用 NTFS 安全樣式。只有 Windows 用戶端可以使用 NTFS 安全樣式修改許可，檔案和目錄中使用的許可類型是 NTFS ACLs。

## 建立磁碟區

除了 ONTAP 命令列界面 (CLI) FlexVol 和 REST API 之外，您還可以使用 Amazon FSx 主控台 AWS CLI、和 Amazon FSx API 建立 FSx FSx for NetApp ONTAP 或 FlexGroup 磁碟區。

### 建立 FlexVol 磁碟區 (主控台)

#### Note

磁碟區的安全樣式會自動設定為根磁碟區的安全樣式。

1. 在 <https://console.aws.amazon.com/fsx/> : // 開啟 Amazon FSx 主控台。
2. 在左側導覽窗格中，選擇磁碟區。
3. 選擇建立磁碟區。
4. 針對檔案系統類型，選擇 Amazon FSx for NetApp ONTAP。
5. 在檔案系統詳細資訊區段中，提供下列資訊：
  - 對於檔案系統，選擇要建立磁碟區的檔案系統。
  - 對於儲存虛擬機器，選擇要建立磁碟區的儲存虛擬機器 (SVM)。
6. 在磁碟區樣式區段中，選擇 FlexVol。
7. 在磁碟區詳細資訊區段中，提供下列資訊：
  - 在磁碟區名稱欄位中，提供磁碟區的名稱。您最多可以使用 203 個英數字元或底線 (\_) 字元。
  - 對於磁碟區大小，輸入 20–314572800 範圍內的任何整數，以指定以 MB (MiB) 為單位的大小。
  - 對於磁碟區類型，選擇讀寫 (RW) 以建立可讀取且可寫入的磁碟區，或選擇資料保護 (DP) 以建立唯讀且可以用作 NetApp SnapMirror 或 SnapVault 關係目的地的磁碟區。如需詳細資訊，請參閱 [磁碟區類型](#)。
  - 在 Junction 路徑中，輸入檔案系統中的位置以掛載磁碟區。名稱必須有正斜線，例如 /vol3。
  - 為了提高儲存效率，請選擇啟用以啟用此磁碟區的 ONTAP 儲存效率功能（重複資料刪除、壓縮和壓縮）。如需詳細資訊，請參閱 [儲存效率](#)。
  - 對於磁碟區安全樣式，請在磁碟區的 Unix (Linux) 和 NTFS 之間進行選擇。如需詳細資訊，請參閱 [磁碟區安全樣式](#)。
  - 針對快照政策，選擇磁碟區的快照政策。如需快照政策的詳細資訊，請參閱 [快照政策](#)。

如果您選擇自訂政策，您必須在自訂政策欄位中指定政策的名稱。自訂政策必須已存在於 SVM 或檔案系統中。您可以使用 ONTAP CLI 或 REST API 建立自訂快照政策。如需詳細資訊，請參閱 NetApp ONTAP 產品文件中[的建立快照政策](#)。

8. 在儲存層區段中，提供下列資訊：

- 針對容量集區分層政策，選擇磁碟區的儲存集區分層政策，可以是自動（預設）、僅限快照、全部或無。如需詳細資訊，請參閱[磁碟區分層政策](#)。
- 如果您選擇僅自動或快照，您可以設定分層政策冷卻期間，以定義未存取的資料標記為冷並移至容量集區儲存之前的天數。您可以提供介於 2 到 183 天之間的值。預設設定為 31 天。

9. 在進階區段的 SnapLock 組態中，選擇已啟用和已停用。如需設定 SnapLock 合規磁碟區或 SnapLock 企業磁碟區的詳細資訊，請參閱 [了解 SnapLock 合規](#) 和 [了解 SnapLock 企業](#)。如需有關 SnapLock 的詳細資訊，請參閱 [使用 保護您的資料 SnapLock](#)。

10. 選擇確認以建立磁碟區。

您可以在磁碟區窗格的狀態欄，監控檔案系統詳細資訊頁面上的更新進度。當磁碟區的狀態建立時，即可供使用。

建立 FlexGroup 磁碟區（主控台）

 Note

您只能使用 Amazon FSx 主控台為具有多個 HA 對的檔案系統建立 FlexGroup 磁碟區。若要為具有多個 HA 對的檔案系統建立 FlexVol 磁碟區，請使用 AWS CLI、Amazon FSx API 或 NetApp 管理工具。

1. 在 <https://console.aws.amazon.com/fsx/>：// 開啟 Amazon FSx 主控台。
2. 在左側導覽窗格中，選擇磁碟區。
3. 選擇建立磁碟區。
4. 針對檔案系統類型，選擇 Amazon FSx for NetApp ONTAP。
5. 在檔案系統詳細資訊區段中，提供下列資訊：
  - 對於檔案系統，選擇要建立磁碟區的檔案系統。
  - 對於儲存虛擬機器，選擇要建立磁碟區的儲存虛擬機器 (SVM)。
6. 在磁碟區樣式區段中，選擇 FlexGroup。



## 7. 在磁碟區詳細資訊區段中，提供下列資訊：

- 在磁碟區名稱欄位中，提供磁碟區的名稱。您最多可以使用 203 個英數字元或底線 (\_) 字元。
- 對於磁碟區大小，輸入每個 HA 對 800 GB (GiB)–2,400 TB (TiB) 範圍內的任何整數。例如，具有 12 個高可用性 (HA) 對的檔案系統最小磁碟區大小為 9,600 GiB，最大磁碟區大小為 20,480 TiB。
- 針對磁碟區類型，選擇讀寫 (RW) 以建立可讀取且可寫入的磁碟區，或選擇資料保護 (DP) 以建立唯讀且可用於 NetAppSnapMirror或SnapVault關係的目的地的磁碟區。如需詳細資訊，請參閱[磁碟區類型](#)。
- 在 Junction 路徑中，輸入檔案系統中的位置以掛載磁碟區。名稱必須有正斜線，例如 /vol3。
- 為了提高儲存效率，請選擇啟用以啟用 ONTAP 儲存效率功能（重複資料刪除、壓縮和壓縮）。如需詳細資訊，請參閱[儲存效率](#)。
- 對於磁碟區安全樣式，請在磁碟區的 Unix (Linux) 和 NTFS 之間進行選擇。如需詳細資訊，請參閱[磁碟區安全樣式](#)。

### Note

磁碟區的安全樣式會自動設定為根磁碟區的安全樣式。

- 針對快照政策，選擇磁碟區的快照政策。如需快照政策的詳細資訊，請參閱[快照政策](#)。

如果您選擇自訂政策，您必須在自訂政策欄位中指定政策的名稱。自訂政策必須已存在於 SVM 或檔案系統中。您可以使用 ONTAP CLI 或 REST API 建立自訂快照政策。如需詳細資訊，請參閱 NetApp ONTAP 產品文件中[的建立快照政策](#)。

## 8. 在儲存層區段中，提供下列資訊：

- 針對容量集區分層政策，選擇磁碟區的儲存集區分層政策，可以是自動（預設）、僅限快照、全部或無。如需詳細資訊，請參閱[磁碟區分層政策](#)。
- 如果您選擇僅限自動或快照，您可以設定分層政策冷卻期間，以定義未存取資料的天數，然後標記為冷資料並移至容量集區儲存體。您可以提供介於 2–183 天之間的值。預設設定為 31 天。

## 9. 在進階區段的SnapLock組態中，選擇已啟用和已停用。如需設定SnapLock合規磁碟區或SnapLock企業磁碟區的詳細資訊，請參閱[了解SnapLock合規](#)和[了解SnapLock企業](#)。如需有關SnapLock的詳細資訊，請參閱[使用保護您的資料 SnapLock](#)。

## 10. 選擇確認以建立磁碟區。



您可以在磁碟區窗格的狀態欄，監控檔案系統詳細資訊頁面上的更新進度。磁碟區在建立狀態時已就緒可供使用。

## 建立磁碟區 (CLI)

- 若要為 ONTAP 磁碟區建立 FSx，請使用 [create-volume](#) CLI 命令（或同等的 [CreateVolume](#) API 操作），如下列範例所示。

```
aws fsx create-volume \
  --volume-type ONTAP \
  --name vol1 \
  --ontap-configuration CopyTagsToBackups=true,JunctionPath=/
vol1,SecurityStyle=NTFS, \
  SizeInMegabytes=1024,SnapshotPolicy=default, \
  StorageVirtualMachineId=svm-abcdef0123456789a,OntapVolumeType=RW, \
  StorageEfficiencyEnabled=true
```

成功建立磁碟區後，Amazon FSx 會以 JSON 格式傳回其描述，如下列範例所示。

```
{
  "Volume": {
    "CreationTime": "2022-08-12T13:03:37.625000-04:00",
    "FileSystemId": "fs-abcdef0123456789c",
    "Lifecycle": "CREATING",
    "Name": "vol1",
    "OntapConfiguration": {
      "CopyTagsToBackups": true,
      "FlexCacheEndpointType": "NONE",
      "JunctionPath": "/vol1",
      "SecurityStyle": "NTFS",
      "SizeInMegabytes": 1024,
      "SnapshotPolicy": "default",
      "StorageEfficiencyEnabled": true,
      "StorageVirtualMachineId": "svm-abcdef0123456789a",
      "StorageVirtualMachineRoot": false,
      "TieringPolicy": {
        "Name": "NONE"
      },
      "OntapVolumeType": "RW"
    },
    "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-abcdef0123456789c/
fsvol-abcdef0123456789b",
```

```
"VolumeId": "fsvol-abcdef0123456789b",  
"VolumeType": "ONTAP"  
  
}  
}
```

您也可以將磁碟區備份還原至新的磁碟區，以建立新的磁碟區。如需詳細資訊，請參閱[將備份還原至新磁碟區](#)。

## 更新磁碟區

您可以使用 Amazon FSx 主控台、AWS CLI 和 Amazon FSx API，以及 ONTAP 命令列界面 (CLI) 和 REST API，更新 FSx for NetApp ONTAP 磁碟區的組態。您可以修改現有 FSx for ONTAP 磁碟區的下列屬性：

- 磁碟區名稱
- 交會路徑
- 磁碟區大小
- 儲存效率
- 容量集區分層政策
- 磁碟區安全樣式
- 快照政策
- 分層政策冷卻期間
- 將標籤複製到備份（使用 AWS CLI 和 Amazon FSx API）

如需詳細資訊，請參閱[管理 ONTAP 磁碟區的 FSx](#)。

### 更新磁碟區組態（主控台）

1. 在 <https://console.aws.amazon.com/fsx/>：// 開啟 Amazon FSx 主控台。
2. 導覽至檔案系統，然後選擇您要更新磁碟區的 ONTAP 檔案系統。
3. 選擇磁碟區索引標籤。
4. 選擇您要更新的磁碟區。
5. 針對動作，選擇更新磁碟區。

更新磁碟區對話方塊會顯示磁碟區目前的設定。

6. 在 Junction 路徑中，輸入檔案系統中的現有位置來掛載磁碟區。名稱必須有正斜線，例如 /vol5。
7. 對於磁碟區大小，您可以在 Amazon FSx 主控台中指定的範圍內增加或減少磁碟區的大小。對於磁碟 FlexVol 區，大小上限為 300 TiB。對於磁碟 FlexGroup 區，大小上限為 300 TiB，乘以您的 FlexGroup 擁有的組成磁碟區總數，上限為 20 PiB。
8. 為了提高[儲存效率](#)，請選擇啟用以啟用磁碟區的 ONTAP 儲存效率功能（重複資料刪除、壓縮和壓縮），或選擇停用以停用它們。
9. 針對容量集區分層政策，選擇磁碟區的新儲存集區分層政策，可以是自動（預設）、僅限快照、全部或無。如需容量集區分層政策的詳細資訊，請參閱[磁碟區分層政策](#)。
10. 針對[磁碟區安全樣式](#)，選擇 Unix (Linux)、NTFS 或 Mixed。磁碟區的安全樣式會決定要將偏好設定提供給 NTFS 或 UNIX ACLs 以進行多協定存取。多重通訊協定存取不需要 MIXED 模式，且僅適用於進階使用者。
11. 針對快照政策，選擇磁碟區的快照政策。如需快照政策的詳細資訊，請參閱[快照政策](#)。

如果您選擇自訂政策，您必須在自訂政策欄位中指定政策的名稱。自訂政策必須已存在於 SVM 或檔案系統中。您可以使用 ONTAP CLI 或 REST API 建立自訂快照政策。如需詳細資訊，請參閱 NetApp ONTAP 產品文件中的[的建立快照政策](#)。

12. 對於分層政策冷卻期間，有效值為 2-183 天。磁碟區的分層政策冷卻期間會定義未存取的資料標記為冷並移至容量集區儲存之前的天數。此設定只會影響 Auto 和 Snapshot-only 政策。
13. 選擇更新以更新磁碟區。

### 更新磁碟區的組態 (CLI)

- 若要更新 FSx for ONTAP 磁碟區的組態，請使用 [update-volume](#) CLI 命令（或同等的 [UpdateVolume](#) API 操作），如下列範例所示。

```
aws fsx update-volume \
  --volume-id fsvol-1234567890abcdefa \
  --name new_vol \
  --ontap-configuration CopyTagsToBackups=true,JunctionPath=/new_vol, \
    SizeInMegabytes=2048,SnapshotPolicy=default-1weekly, \
    StorageEfficiencyEnabled=true, \
    TieringPolicy=all
```

## 擴展磁碟FlexGroup區

您可以使用 ONTAP CLI 中的 `volume expand` 命令，將其他組成磁碟區新增至磁碟FlexGroup區。這是將高可用性 (HA) 對新增至檔案系統後的最佳實務，因為它可確保磁碟FlexGroup區保持平衡。

在擴展磁碟FlexGroup區之前，請考慮下列事項：

- 所有FlexGroup's組成磁碟區都有相同的儲存容量。當您使用其他組份擴展磁碟FlexGroup區時，每個組份的大小與現有組份相同。因此，請確保每個彙總都有足夠的可用空間，然後再新增元件。
- AWS 建議針對每個磁碟區，維護每個彙總八個組成FlexGroup磁碟區。每個彙總的八個組成磁碟區可最大化FlexGroup磁碟區的平行處理，並為工作負載提供最佳效能。一般而言，如果您新增 HA 對，建議您只使用其他元件來擴展FlexGroup磁碟區。這是唯一您需要新增組份來維護每個彙總八個組份的情況。
- 如果您的FlexGroup磁碟區處於SnapMirror關係中，則來源磁碟區和目的地磁碟FlexGroup區都需要具有相同數量的元件。否則，SnapMirror傳輸將會失敗。會在組分層級SnapMirror運作，並在各個組分之間傳輸資料。因此，如果您使用其他組成FlexGroup磁碟區來展開磁碟區，您還必須手動展開與其建立SnapMirror關係的任何磁碟區。
- 當您使用其他元件擴展FlexGroup磁碟區時，其所有現有的快照複本都會變成「部分」複本。部分複本無法還原，但可以瀏覽並還原個別檔案。此外，這會導致 Amazon FSx 備份、AWS 備份或 SnapMirror關係的任何增量遺失。
- 您無法在新增組成磁碟區後移除組成磁碟區。

### 新增FlexGroup磁碟區元件

您可以使用 ONTAP CLI 將組成磁碟區新增至磁碟FlexGroup區。

### 新增FlexGroup磁碟區元件

1. 若要存取 NetApp ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統的管理連接埠上建立 SSH 工作階段。`management_endpoint_ip` 將取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

2. 使用[磁碟區展開](#) ONTAP CLI 命令，以其他元件來展開磁碟FlexGroup區。取代以下的值：
  - `svm_name` 使用託管磁碟FlexGroup區的儲存虛擬機器 (SVM) 名稱（例如 `svm1`）。

- `vol_name` 使用您要展開的FlexGroup磁碟區名稱 (例如 `vol1`)。
- `aggregates` 以逗號分隔的彙總清單，您想要將FlexGroup組成磁碟區新增至其中。例如，`aggr1`針對單一彙總或`aggr1,aggr2`針對多個彙總。
- `constituent_per_aggregate` 包含您要新增至每個指定的其他元件數量`aggregates`。您只應新增足夠的成分，以確保您的FlexGroup磁碟區在其所在的彙總中具有平衡數量的成分。

```
::> volume expand -vserver svm_name -volume vol_name -aggr-list aggregates -aggr-list-multiplier constituents_per_aggregate
```

### Important

您無法在新增FlexGroup元件之後移除它們，因此請先檢查您的輸入，再執行先前的命令。

## 在彙總之間移動磁碟區

當您將高可用性 (HA) 對新增至檔案系統時，您需要透過將磁碟區移至新的彙總來重新平衡現有資料。若要在彙總之間移動磁碟區，您可以在 ONTAP CLI 中使用 `volume move` 命令。

使用 `volume move` 命令之前，請考慮下列事項：

- 使用 `volume move` 命令可能會影響效能，因為它會在您的檔案系統上耗用網路和磁碟資源。因此，我們建議在低活動期間在彙總之間移動磁碟區。或者，您可以在移動磁碟區時，將檔案系統的網路輸送量使用率和磁碟輸送量使用率降低至不超過 50%。
- 為了降低對檔案系統的效能影響，我們建議您一次在兩個 HA 對和彙總之間移動單一磁碟區。例如，如果您的檔案系統有四個 HA 對，我們建議您一次移動兩個磁碟區（假設磁碟區移動不是來自或朝向相同的 HA 對）。ONTAP 支援一次在每個 HA 對上最多移動八個磁碟區，但更多同時的磁碟區移動將降低用戶端 I/O 和任何進行中磁碟區移動的效能。
- 存放在受影響磁碟區 SSD 層上的任何資料都會實際移至不同檔案伺服器上的不同磁碟組。此操作會在背景中進行，且需要一些時間。傳輸所需的時間速率取決於檔案系統的輸送量容量，以及檔案系統上的活動量。不過，可以調節磁碟區移動。如需詳細資訊，請參閱[調節磁碟區移動](#)。
- 由於 HA 對共用相同的容量集區儲存體，因此儲存在容量層上的任何資料都不會實際移動。因此，以其大部分資料分層移動磁碟區的速度會更快。請記住，檔案中繼資料一律存放在 SSD 層。如需詳細資訊，請參閱[磁碟區資料分層](#)。

## 移動磁碟區的階段

磁碟區移動操作有兩個階段：複寫階段和切換階段。在複寫階段，現有資料會複寫到磁碟區的新彙總。在切換階段期間，ONTAP 會嘗試最終快速轉移到磁碟區的新彙總。這包括傳輸在傳輸階段寫入的任何資料，並將新流量重新導向至磁碟區的新彙總。根據預設，切換時段為 30 秒，並停止磁碟區的所有輸入/輸出。如果 ONTAP 無法在切換時段期間執行所有這些步驟，將會失敗。根據預設，ONTAP 會嘗試連續縮減三次。如果所有三次連續嘗試都失敗，則 ONTAP 將每小時重試一次，直到成功為止。您可以減少檔案系統的負載，在切換階段開始之前減少或暫停磁碟區的 I/O 流量，以確保切換階段成功。

## 啟動磁碟區移動

### 啟動磁碟區移動

1. 若要存取 NetApp ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統的管理連接埠上建立 SSH 工作階段。*management\_endpoint\_ip* 將取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

2. 執行[磁碟區移動啟動](#) ONTAP CLI 命令。取代以下的值：
  - *vserver\_name* 使用託管您正在移動之磁碟區的 SVM 名稱。
  - *volume\_name* 具有磁碟區成分的名稱（例如 *vol1\_\_0001*）。
  - *aggregate\_name* 具有磁碟區目的地彙總的名稱。
  - *-enforce-network-throttling* 調節磁碟區移動的總輸送量。這是選用的。

```
::> volume move start -vserver svm_name -volume volume_name --destination-  
aggregate aggregate_name -foreground false  
[Job 1] Job is queued: Move "vol1__0001" in Vserver "svm01" to aggregate "aggr1".  
Use the "volume move show -vserver svm01 -volume vol1__0001" command to view the  
status of this operation.
```

### ⚠ Important

移動磁碟區會耗用來源和目的地檔案伺服器的網路和磁碟資源。因此，工作負載的效能可能會受到正在進行的任何磁碟區移動的影響。此外，您在磁碟區移動的切換階段期間，對磁碟區的 I/O 流量將暫時暫停。

## 監控磁碟區移動

### 監控磁碟區移動

- 若要檢查磁碟區移動操作的狀態，請使用 `volume move show` ONTAP CLI 命令。

```
::> volume move show -vserver svm_name -volume volume_name
```

```
Vserver Name: svm01
Volume Name: vol1__0001
Actual Completion Time: -
Bytes Remaining: 1.00TB
Specified Action For Cutover: retry_on_failure
Specified Cutover Time Window: 30
Destination Aggregate: aggr2
Destination Node: FsxId01234567890abcdef-03
Detailed Status: Transferring data: 12.23GB sent.
Percentage Complete: 1%
Move Phase: replicating
Prior Issues Encountered: -
Estimated Remaining Duration: 00:40:25
Replication Throughput: 434.3MB/s
Duration of Move: 00:00:27
Source Aggregate: aggr1
Source Node: FsxId01234567890abcdef-01
Move State: healthy
```

命令輸出會顯示完成移動的預估時間。完成後，Move phase會顯示 completed 狀態。

## 維持平衡的FlexGroup磁碟區

為了讓您的工作負載以最佳方式執行，您的FlexGroup磁碟區應跨越所有彙總，且每個彙總的組分磁碟區數目均相等。我們建議每個彙總有八個元件。重新平衡FlexGroup磁碟區時，請考慮下列案例：

- 在現有彙總之間移動組FlexGroup份：如果您將FlexGroup's組份磁碟區移至其他平衡的 的另一個彙總FlexGroup，則應該將另一個較不用於原始彙總的組份移動。這可確保您的 每個彙總FlexGroup都有偶數的組份。

新增 HA 對後將FlexGroup組份移至新的彙總：如果您在新增 HA 對後將FlexGroup's組份磁碟區移至新的彙總，則應在失去組份的彙總上FlexGroup，使用其他組份展開。這可確保您的 每個彙總FlexGroup都有偶數的組份。如需詳細資訊，請參閱[the section called “擴展磁碟FlexGroup區”](#)。

## 調節磁碟區移動

如果您想要限制檔案系統上磁碟區移動的頻寬，您可以在操作開始時新增 `-enforce-network-throttling` 選項。

### Note

使用此選項會影響檔案系統的傳入SnapMirror複寫資料傳輸。追蹤如何設定檔案系統的複寫選項，因為您在設定檔案系統後無法檢視它們。

## 調節磁碟區移動

1. 調節會使用全域複寫調節。若要設定全域複寫節流，請在 CLI ONTAP 中使用下列命令。

```
::> options -option-name replication.throttle.enable on
```

2. 指定複寫可以使用的最大總頻寬，取代下列選項：

- `kbs_throttle` 具有用於任何複寫（包括 SnapMirror和 磁碟區移動）所需的最大輸送量，以每秒 KB 為單位。

```
::> options -option-name replication.throttle.incoming.max_kbs kbs_throttle  
::> options -option-name replication.throttle.outgoing.max_kbs kbs_throttle
```

## 監控磁碟區

您可以使用 Amazon FSx 主控台、AWS CLI和 Amazon FSx API 和 SDKs 來查看目前位於檔案系統的磁碟區。



若要監控檔案系統上的磁碟區：

- 使用主控台 – 選擇檔案系統以檢視檔案系統詳細資訊頁面。選擇磁碟區索引標籤，列出檔案系統上的所有磁碟區，然後選擇您要檢視的磁碟區。
- 使用 CLI 或 API – 使用 [describe-volumes](#) CLI 命令或 [DescribeVolumes](#) API 操作。

```
$ aws fsx describe-volumes
{
  "Volumes": [
    {
      "CreationTime": "2024-03-04T20:17:44+00:00",
      "FileSystemId": "fs-abcdef0123a0bb087",
      "Lifecycle": "CREATED",
      "Name": "SVM8_ext_root",
      "OntapConfiguration": {
        "FlexCacheEndpointType": "NONE",
        "JunctionPath": "/",
        "SecurityStyle": "NTFS",
        "SizeInMegabytes": 1024,
        "StorageEfficiencyEnabled": false,
        "StorageVirtualMachineId": "svm-01234567890abcdef",
        "StorageVirtualMachineRoot": true,
        "TieringPolicy": {
          "Name": "NONE"
        },
        "UUID": "42ce3de0-da64-11ee-a22d-7f7cdfb8d381",
        "OntapVolumeType": "RW",
        "SnapshotPolicy": "default",
        "CopyTagsToBackups": false,
        "VolumeStyle": "FLEXVOL",
        "AggregateConfiguration": {
          "Aggregates": [
            "aggr1"
          ]
        },
        "SizeInBytes": 1073741824
      },
      "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-abcdef0123a0bb087/fsvol-abcdef0123456789a",
      "VolumeId": "fsvol-abcdef0123456789a",
      "VolumeType": "ONTAP"
    }
  ]
}
```

}

## 檢視離線磁碟區

當來源磁碟區離線時，您無法建立或刪除磁碟區備份。您可以使用 [volume show](#) ONTAP CLI 命令來判斷磁碟區的目前狀態。

```
volume show -vserver svm-name
```

如需存取檔案系統上 ONTAP CLI 的相關資訊，請參閱[使用 NetApp ONTAP CLI](#)。

```
FsxIdabc12345::> volume show -vserver vs1
```

| Vserver | Volume  | Aggregate | State  | Type | Size  | Available | Used% |
|---------|---------|-----------|--------|------|-------|-----------|-------|
| vs1     | vol1    | aggr1     | online | RW   | 2GB   | 1.9GB     | 5%    |
| vs1     | vol1_dr | aggr0_dp  | online | DP   | 200GB | 160.0GB   | 20%   |
| vs1     | vol2    | aggr0     | online | RW   | 150GB | 110.3GB   | 26%   |
| vs1     | vol2_dr | aggr0_dp  | online | DP   | 150GB | 110.3GB   | 26%   |
| vs1     | vol3    | aggr1     | online | RW   | 150GB | 120.0GB   | 20%   |
| vs1     | vol3_dr | aggr1_dp  | online | DP   | 150GB | 120.0GB   | 20%   |
| vs1     | vol4    | aggr1     | online | RW   | 200GB | 159.8GB   | 20%   |

7 entries were displayed.

若要讓離線磁碟區恢復上線，請使用 [volume online](#) ONTAP CLI 命令，如下列範例所示。如果只有一個 SVM (Vserver)，則不需要指定 `-vserver` 參數。

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

## 刪除磁碟區

除了 ONTAP 命令列界面 (CLI) 和 REST API 之外，您還可以使用 Amazon FSx 主控台 AWS CLI、和 Amazon FSx API 刪除 FSx FSx for NetApp ONTAP 磁碟區。

刪除磁碟區之前，請確定沒有應用程式正在存取您要刪除之磁碟區中的資料。

### Important

如果磁碟區已啟用 Amazon FSx 備份，您只能使用 Amazon FSx 主控台、API 或 CLI 刪除磁碟區。

## 取得最終磁碟區備份

當您使用 Amazon FSx 主控台刪除磁碟區時，您可以選擇進行磁碟區的最終備份。最佳實務是，建議您選擇進行最終備份。如果您發現在一段時間後不需要它，您可以刪除這個和其他手動建立的磁碟區備份。當您使用 CLI `delete-volume` 命令刪除磁碟區時，Amazon FSx 預設會進行最終備份。

如需磁碟區備份的詳細資訊，請參閱 [使用磁碟區備份保護您的資料](#)。

### 刪除磁碟區（主控台）

1. 在 <https://console.aws.amazon.com/fsx/>：// 開啟 Amazon FSx 主控台。
2. 在左側導覽窗格中，選擇檔案系統，然後選擇您要從中刪除磁碟區的 ONTAP 檔案系統。
3. 選擇磁碟區索引標籤。
4. 選擇您要刪除的磁碟區。
5. 針對動作，選擇刪除磁碟區。
6. (SnapLock Enterprise 僅限 磁碟區) 對於繞過 SnapLock 企業保留，請選擇是。
7. 在確認對話方塊中，對於建立最終備份，您有兩個選項：
  - 選擇是以取得磁碟區的最終備份。最終備份的名稱隨即顯示。
  - 如果您不希望磁碟區的最終備份，請選擇否。系統會要求您確認一旦刪除磁碟區，自動備份就不再可用。
8. 在確認刪除欄位中輸入刪除，以確認磁碟區刪除。
9. 選擇刪除磁碟區 (s)。

### 刪除磁碟區 (CLI)

- 若要刪除 ONTAP 磁碟區的 FSx，請使用 [delete-volume](#) CLI 命令（或同等的 [DeleteVolume](#) API 操作），如下列範例所示。

```
aws fsx delete-volume --volume-id fsvol-1234567890abcde
```

## 刪除SnapLock磁碟區

本節說明如何刪除SnapLock磁碟區。

如果所有寫入的保留期間過期，您可以刪除SnapLock合規磁碟區，讀取其中的許多 (WORM) 檔案。

### Note

當您關閉包含 AWS 帳戶 SnapLock Enterprise或 Compliance磁碟區的 時，AWS 且 FSx for ONTAP 會暫停您的帳戶 90 天，讓資料保持完整。如果您在這 90 天內未重新開啟帳戶，會 AWS 刪除您的資料，包括磁碟SnapLock區中的資料，而無論您的保留設定為何。

如果您具有必要的許可，您可以隨時刪除SnapLock企業磁碟區。若要使用 CLI ONTAP 刪除SnapLock 企業磁碟區，您必須具有 fsxadmin角色。如需詳細資訊，請參閱[檔案系統管理員角色和使用者](#)。

若要使用 Amazon FSx 主控台、CLI 或 Amazon FSx API 刪除包含具有作用中保留政策之 WORM 資料SnapLock的企業磁碟區，您必須擁有 fsx:BypassSnapLockEnterpriseRetention IAM 許可。

### Warning

SnapLock 稽核日誌磁碟區的最短保留期間為六個月。在此保留期間到期之前，您無法刪除 SnapLock稽核日誌磁碟區、儲存虛擬機器 (SVM) 或與 SVM 相關聯的檔案系統，即使磁碟區是在SnapLock企業模式下建立。如需詳細資訊，請參閱[SnapLock 稽核日誌磁碟區](#)。

## 建立 iSCSI LUN

此程序說明如何使用 CLI lun create命令在 Amazon FSx for NetApp ONTAP 檔案系統上建立 NetApp ONTAP iSCSI LUN。如需詳細資訊，請參閱 NetApp ONTAP 文件中心[lun create](#)中的。

### Note

超過六個 HA 對的檔案系統不支援 iSCSI 通訊協定。

此程序假設您已在檔案系統上建立磁碟區。如需詳細資訊，請參閱[建立磁碟區](#)。

- 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。*management\_endpoint\_ip* 將取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

- 使用 `lun createNetApp` CLI 命令建立 LUN，取代下列值：
- svm\_name* - 提供 iSCSI 目標的儲存虛擬機器 (SVM) 名稱。主機使用此值來到達 LUN。
  - vol\_name* - 託管 LUN 的磁碟區名稱。
  - lun\_name* - 您要指派給 LUN 的名稱。
  - size* - LUN 的大小，以位元組為單位。您可以建立的大小上限為 128 TB。

 Note

我們建議您使用比 LUN 大小至少大 5% 的磁碟區。此邊界會保留磁碟區快照的空間。

- ostype* - 主機的作業系統，windows\_2008 或 linux。windows\_2008 用於所有版本的 Windows；這可確保 LUN 具有適當的作業系統區塊位移，並最佳化效能。

 Note

建議您在 LUN 上啟用空間配置。啟用空間配置後，ONTAP 可以在 LUN 容量不足時通知主機，並在您從 LUN 刪除資料時回收空間。

如需詳細資訊，請參閱 NetApp ONTAP CLI 文件[lun create](#)中的。

```
> lun create -vserver svm_name -path /vol/vol_name/lun_name -size size -  
ostype ostype -space-allocation enabled
```

```
Created a LUN of size 10g (10737418240)
```

- 確認 LUN 已建立、上線並映射。

```
> lun show
```

系統會以下列輸出回應：

| Vserver         | Path                          | State  | Mapped   | Type         | Size |
|-----------------|-------------------------------|--------|----------|--------------|------|
| <i>svm_name</i> | <i>/vol/vol_name/lun_name</i> | online | unmapped | windows_2008 | 10GB |

## 後續步驟

現在您已建立 iSCSI LUN，使用 iSCSI LUN 做為區塊儲存程序的下一個步驟是將 LUN 映射至 igroup。如需詳細資訊，請參閱 [佈建 Linux 的 iSCSI](#) 或 [佈建適用於 Windows 的 iSCSI](#)。

## 使用 Amazon FSx 維護時段最佳化效能

做為全受管服務，FSx for ONTAP 會定期對檔案系統執行維護和更新。此維護對大多數工作負載沒有影響。對於對效能敏感的工作負載，在極少數情況下，您可能會在發生維護時注意到對效能的短暫 (<60 秒) 影響；Amazon FSx 可讓您使用維護時段來控制發生此類潛在維護活動的時間。

修補不常發生，通常是每幾週一次。進行修補時，每個檔案系統的檔案伺服器會一次修補一個，而每個檔案伺服器通常最多需要一小時才能修補。在 HA 對內修補任何檔案伺服器之前，您的檔案系統會自動容錯移轉至檔案伺服器的 HA 合作夥伴，這可能會導致針對該 HA 對的任何 I/O 短暫（少於 60 秒）的 I/O 暫停。然後，您的檔案系統將會失敗，這可能會導致另一個短暫（少於 60 秒）的 I/O 暫停。您可以在建立檔案系統期間選擇維護時段開始時間。如果您未選擇視窗，系統會自動指派一個視窗。

### Important

為了確保您的檔案系統可以成功修補，FSx for ONTAP 會在修補程序期間讓任何離線磁碟區上線。用戶端無法存取 Amazon FSx 恢復連線的任何磁碟區。

FSx for ONTAP 可讓您視需要調整維護時段，以因應工作負載和操作需求。您可以視需要頻繁移動維護時段，前提是至少每 14 天進行一次維護時段。如果修補程式已發行，且維護時段未在 14 天內發生，則 FSx for ONTAP 將繼續維護檔案系統，以確保其安全性和可靠性。

**Note**

為了確保維護活動期間的資料完整性，FSx for ONTAP 會關閉所有機會鎖定，並在維護開始之前，完成託管檔案系統的基礎儲存磁碟區的任何待定寫入操作。

您可以使用 Amazon FSx 管理主控台、AWS CLI AWS API 或其中一個 AWS SDKs 來變更檔案系統的維護時段。

**變更每週維護時段（主控台）**

1. 開啟 Amazon FSx 主控台，網址為 <https://console.aws.amazon.com/fsx/> : //www.。
2. 選擇左側導覽欄中的檔案系統。
3. 選擇您要變更每週維護時段的檔案系統。摘要檔案系統詳細資訊頁面隨即出現。
4. 選擇管理以顯示檔案系統管理設定面板。
5. 選擇更新以顯示變更維護時段。
6. 輸入您希望每週維護時段開始的新日期和時間。
7. 選擇儲存，以儲存變更。新的維護開始時間會顯示在檔案系統管理設定面板中。

若要使用 [update-file-system](#) CLI 命令變更每週維護時段，請參閱 [更新檔案系統 \(CLI\)](#)。

## 管理輸送量容量

FSx for ONTAP 會在您建立檔案系統時設定輸送量容量。您可以隨時修改檔案系統的輸送量容量。請記住，您的檔案系統需要特定組態，才能達到最大輸送量容量。例如，若要為第一代檔案系統佈建 4 GBps 的輸送量容量，您的檔案系統需要至少 5, 120 GiB 的 SSD 儲存容量和 160, 000 個 SSD IOPS 的組態。如需詳細資訊，請參閱[輸送量容量對效能的影響](#)。

輸送量容量是決定託管檔案系統之檔案伺服器提供檔案資料的速度的一個因素。更高的輸送量容量具有更高層級的網路、磁碟讀取 I/O 每秒操作 (IOPS)，以及檔案伺服器上的資料快取容量。如需詳細資訊，請參閱[效能](#)。

當您修改檔案系統的輸送量容量時，Amazon FSx 會切換為支援檔案系統的檔案伺服器。單一可用區和多可用區檔案系統都會在此過程中發生自動容錯移轉和容錯回復，這通常需要幾分鐘的時間才能完成。容錯移轉和容錯回復程序對 NFS（網路檔案共用）、SMB（伺服器訊息區塊）和 iSCSI（網際網路小型電腦系統介面）用戶端而言是透明的，可讓您的工作負載繼續執行，而不會中斷或手動介入。您的檔案系統一旦有新的輸送量容量，就會向您收費。

### Note

為了確保維護活動期間的資料完整性，FSx for ONTAP 會關閉所有機會鎖定，並在維護開始之前，完成託管檔案系統的基礎儲存磁碟區的任何待定寫入操作。在排定的檔案系統維護時段期間，系統修改（例如修改您的輸送量容量）可能會延遲。系統維護可能會導致這些變更在處理之前排入佇列。如需詳細資訊，請參閱[the section called “更新維護時段”](#)。

## 主題

- [何時修改輸送量容量](#)
- [如何處理並行請求](#)
- [更新輸送量容量](#)
- [監控輸送量容量變更](#)

## 何時修改輸送量容量

Amazon FSx 與 Amazon CloudWatch 整合，可協助您監控檔案系統的持續輸送量用量層級。除了檔案系統的輸送量之外，您可以透過檔案系統驅動的輸送量和 IOPS 效能，還取決於特定工作負載的特性。一般而言，您應該佈建足夠的輸送量容量，以支援工作負載的讀取輸送量，以及工作負載的寫入輸送量的兩倍。您可以使用 CloudWatch 指標來決定要變更哪些維度，以改善效能。如需詳細資訊，請參閱[the section called “在 Amazon FSx 主控台中監控”](#)。

## 如何處理並行請求

對於第一代檔案系統，您可以在 SSD 儲存容量和佈建 IOPS 更新工作流程開始之前或進行期間請求傳輸量容量更新。Amazon FSx 如何處理兩個請求的順序如下：

- 如果您同時提交 SSD/IOPS 更新和傳輸量容量更新，則會接受這兩個請求。SSD/IOPS 更新在輸送量容量更新之前會優先進行。
- 如果您在 SSD/IOPS 更新進行時提交輸送量容量更新，則會接受輸送量容量更新請求，並在 SSD/IOPS 更新後排入佇列。傳輸量容量更新會在 SSD/IOPS 更新後（有可用的新值）和最佳化步驟期間開始。這通常需要不到 10 分鐘的時間。
- 如果您在傳輸量容量更新進行時提交 SSD/IOPS 更新，則會接受 SSD/IOPS 儲存體更新請求，並在傳輸量容量更新完成後排入佇列以啟動（有新的傳輸量容量可用）。這通常需要 20 分鐘。



請求第二代檔案系統的輸送量容量更新時，請考慮下列事項：

- 在更新第二代檔案系統的輸送量容量之間，您必須等待至少六小時。
- 傳輸量容量冷卻期間與 SSD/IOPS 擴展共用。
- 傳輸量容量擴展和 SSD/IOPS 擴展無法在進行時以模擬或佇列方式完成。
- 當輸送量容量擴展或 SSD/IOPS 擴展正在進行時，您無法新增高可用性 (HA) 對與或搭配使用。不過，新增 HA 對不會與 SSD/IOPS 擴展和輸送量容量擴展共用冷卻時間。如需詳細資訊，請參閱[新增高可用性 \(HA\) 對](#)。

如需 SSD 儲存體和佈建 IOPS 更新的詳細資訊，請參閱[管理儲存容量](#)。

## 更新輸送量容量

您可以使用 Amazon FSx 主控台、AWS Command Line Interface (AWS CLI) 或 Amazon FSx API 來修改檔案系統的輸送量容量。

### Note

在更新第二代檔案系統的輸送量容量之間，您必須等待至少六小時。

### 修改檔案系統的輸送量容量（主控台）

1. 在 <https://console.aws.amazon.com/fsx/>：// 開啟 Amazon FSx 主控台。
2. 導覽至檔案系統，然後選擇您要增加輸送量容量的 ONTAP 檔案系統。
3. 針對動作，選擇更新輸送量容量。或者，在摘要面板中，選擇檔案系統輸送量容量旁的更新。
4. 從清單中選擇輸送量容量的新值。
5. 選擇更新以啟動輸送量容量更新。
6. 您可以在檔案系統詳細資訊頁面的更新索引標籤上監控更新進度。

您可以使用 Amazon FSx 主控台、AWS CLI 和 API 來監控更新進度。如需詳細資訊，請參閱[監控輸送量容量變更](#)。

### 修改檔案系統的輸送量容量 (CLI)

若要修改檔案系統的輸送量容量，請使用 AWS CLI 命令 [update-file-system](#)。設定下列參數：

- `--file-system-id` 至您正在更新之檔案系統的 ID。
- `ThroughputCapacity` 至所需的值，以更新檔案系統。

您可以使用 Amazon FSx 主控台、AWS CLI 和 API 來監控更新進度。如需詳細資訊，請參閱[監控輸送量容量變更](#)。

## 監控輸送量容量變更

您可以使用 Amazon FSx 主控台、API 和 監控輸送量容量修改的進度 AWS CLI。

### 在主控台中監控輸送量容量變更

在檔案系統詳細資訊視窗中的更新索引標籤上，您可以檢視每個更新動作類型的 10 個最新更新動作。

對於輸送量容量更新動作，您可以檢視下列資訊。

#### 更新類型

支援的類型包括輸送量容量、儲存容量和儲存最佳化。

#### 目標值

要變更檔案系統輸送量容量的所需值。

#### 狀態

更新的目前狀態。對於輸送量容量更新，可能的值如下所示：

- 待處理 – Amazon FSx 已收到更新請求，但尚未開始處理。
- 進行中 – Amazon FSx 正在處理更新請求。
- 已完成 – 輸送量容量更新已成功完成。
- 失敗 – 輸送量容量更新失敗。選擇問號 (?) 以查看輸送量更新失敗原因的詳細資訊。

#### 請求時間

Amazon FSx 收到更新請求的時間。

### 使用 AWS CLI 和 API 監控變更

您可以使用 [describe-file-systems](#) CLI 命令和 [DescribeFileSystems](#) API 動作來檢視和監控檔案系統輸送量修改請求。AdministrativeActions 陣列會列出每個管理動作類型的 10 個最近更新動作。當您修改檔案系統的輸送量容量時，會產生 FILE\_SYSTEM\_UPDATE 管理動作。

下列範例顯示 CLI `describe-file-systems` 命令的回應摘錄。檔案系統的輸送量容量為 128 MBps，目標輸送量容量為 256 MBps。

```
.
.
.
  "ThroughputCapacity": 128,
"AdministrativeActions": [
  {
    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
    "RequestTime": 1581694764.757,
    "Status": "PENDING",
    "TargetFileSystemValues": {
      "OntapConfiguration": {
        "ThroughputCapacity": 256
      }
    }
  }
]
```

當 Amazon FSx 成功處理動作時，狀態會變更為 `COMPLETED`。然後，新的輸送量容量可供檔案系統使用，並在 `ThroughputCapacity` 屬性中顯示。這會顯示在 CLI `describe-file-systems` 命令的下列回應摘錄中。

```
.
.
.
  "ThroughputCapacity": 256,
"AdministrativeActions": [
  {
    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
    "RequestTime": 1581694764.757,
    "Status": "COMPLETED",
    "TargetFileSystemValues": {
      "OntapConfiguration": {
        "ThroughputCapacity": 256
      }
    }
  }
]
```

如果傳輸量容量修改失敗，狀態會變更為 FAILED，而 `FailureDetails` 屬性會提供失敗的相關資訊。

## 管理 SMB 共用

若要在 Amazon FSx 檔案系統上管理 SMB 檔案共用，您可以使用 Microsoft Windows 共用資料夾 GUI。共用資料夾 GUI 提供一個集中位置，用於管理儲存虛擬機器 (SVM) 中的所有共用資料夾。下列程序詳細說明如何建立、更新和移除檔案共享。

### Note

您也可以使用 NetApp System Manager 來管理 SMB 檔案共享。如需詳細資訊，請參閱[搭配使用 NetApp System Manager BlueXP](#)。

將共用資料夾連線至 Amazon FSx 檔案系統

1. 啟動您的 Amazon EC2 執行個體，並將其連接至您的 Amazon FSx 檔案系統加入的 Microsoft Active Directory。若要這樣做，請從 AWS Directory Service 管理指南中選擇下列其中一個程序：
  - [無縫加入 Windows EC2 執行個體](#)
  - [手動加入 Windows 執行個體](#)
2. 以檔案系統管理員群組成員的使用者身分連線至您的執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[連線至您的 Windows 執行個體](#)。
3. 開啟開始功能表，並使用以管理員身分執行 `fsmgmt.msc`。這樣做會開啟共用資料夾 GUI 工具。
4. 針對動作，選擇連線至另一部電腦。
5. 針對另一部電腦，輸入儲存虛擬機器 (SVM) 的 DNS 名稱，例如 **netbios\_name.corp.example.com**。

若要在 Amazon FSx 主控台上尋找 SVM 的 DNS 名稱，請選擇儲存虛擬機器，選擇您的 SVM，然後向下捲動至端點，直到您找到 SMB DNS 名稱為止。您也可以在 [DescribeStorageVirtualMachines](#) API 操作的回應中取得 DNS 名稱。

6. 選擇確定。然後，Amazon FSx 檔案系統的項目會出現在共用資料夾工具的清單中。

現在共用資料夾已連線至您的 Amazon FSx 檔案系統，您可以使用下列動作來管理檔案系統上的 Windows 檔案共用：

**Note**

建議您在根磁碟區以外的磁碟區上尋找 SMB 共用。

- 建立新的檔案共享 – 在共用資料夾工具中，選擇左側窗格中的共享，以查看 Amazon FSx 檔案系統的作用中共享。磁碟區會顯示在磁碟區建立期間選擇的路徑上。選擇新增共用並完成建立共用資料夾精靈。

您必須先建立本機資料夾，才能建立新的檔案共享。您可以執行下列動作：

- 使用共用資料夾工具：在指定本機資料夾路徑時選擇瀏覽，選擇建立新資料夾以建立本機資料夾。
- 使用命令列：

```
New-Item -Type Directory -Path \\netbios_name.corp.example.com\C  
$volume_path\MyNewFolder
```

- 修改檔案共享 – 在共用資料夾工具中，開啟您要在右側窗格中修改之檔案共享的內容（按一下滑鼠右鍵）選單，然後選擇屬性。修改屬性，然後選擇確定。
- 移除檔案共享 – 在共用資料夾工具中，開啟您要在右側窗格中移除的檔案共享內容（按一下滑鼠右鍵）選單，然後選擇停止共享。

**Note**

只有在您使用 Amazon FSx 檔案系統的 DNS 名稱連線到 fsmgmt.msc 時，才能從 GUI 移除檔案共享。如果您使用檔案系統的 IP 地址或 DNS 別名名稱連線，則停止共用選項將無法運作，且檔案共用不會移除。

## 使用 NetApp 應用程式管理 FSx for ONTAP 資源

除了 AWS Management Console AWS CLI、和 AWS API 和 SDKs，您也可以使用這些 NetApp 管理工具和應用程式來管理 FSx for ONTAP 資源：

### 主題

- [註冊 NetApp 帳戶](#)
- [使用 NetApp BlueXP](#)
- [使用 NetApp ONTAP CLI](#)

- [使用 ONTAP REST API](#)

 Important

Amazon FSx 會定期與 同步ONTAP，以確保一致性。如果您使用NetApp應用程式建立或修改磁碟區，這些變更可能需要幾分鐘的時間才會反映在 AWS Management Console AWS CLI、API 和 SDKs中。

## 註冊NetApp帳戶

若要下載一些NetApp軟體，例如 BlueXP、 SnapCenter和ONTAP防毒連接器，您需要擁有 NetApp帳戶。若要註冊NetApp帳戶，請執行下列步驟：

1. 前往[NetApp使用者註冊](#)頁面並註冊新的NetApp使用者帳戶。
2. 使用您的資訊填寫表單（表格）。請務必選取NetApp客戶/最終使用者存取層級。在 SERIAL NUMBER 欄位中，複製並貼上 FSx for ONTAP 檔案系統的檔案系統 ID。請參閱下列範例：

## USER ACCESS LEVEL

- ☐ Guest User    ☒ NetApp Customer / End User
- ☐ NetApp Reseller / Service Provider / System Integrator / Partner

**Product Information (Optional)**

Please enter a Serial Number or System ID to help us validate your access level.

**Please note:** Not providing a Serial Number or System ID may delay processing of your request.

## SERIAL NUMBER

fs-0de9123abcf12368a

(Either a NetApp hardware Serial Number, often located on back of unit; or a NetApp software Serial Number.)

OR

## SYSTEM ID

(Run a "sysconfig -a" command on your NetApp product. The output should list the System ID.)

## NETAPP TOKEN

## 註冊後預期會發生的情況

擁有現有NetApp產品的客戶將在一個工作天內將其 NSS 帳戶升級為客戶層級存取權。除了將 NSS 帳戶升級到客戶層級存取權之外，新加入的客戶NetApp將使用標準商業實務加入。提供檔案系統 ID 有助於加速此程序。您可以透過登入 [mysupport.netapp.com](https://mysupport.netapp.com) : ///https : //https : //https : //www.https : //www./www.healthnet./www.healthnet.com/healthnet.com/healthnet.com/healthnet.com/healthnet.com/healthnet.com/healthnet.com/com/healthnet. 您帳戶的存取層級應為客戶存取。

## 使用 NetApp BlueXP

NetApp BlueXP 是統一的控制平面，可簡化內部部署和雲端環境中儲存和資料服務的管理體驗。BlueXP 提供集中式使用者介面，可管理、監控和自動化內部部署和內部部署 AWS 中的 ONTAP 部署。如需詳細資訊，請參閱 [NetApp BlueXP 文件](#)和 [Amazon FSx for NetApp ONTAP 文件的 NetApp BlueXP](#)。

**Note**

NetApp BlueXP 具有多個高可用性 (HA) 對的第二代檔案系統不支援。

## 搭配 使用 NetApp System Manager BlueXP

您可以直接從 使用 System Manager 來管理 Amazon FSx for NetApp ONTAP 檔案系統 BlueXP。BlueXP 可讓您使用您習慣使用的相同 System Manager 介面，因此您可以從單一控制平面管理您的混合多雲端基礎設施。您也可以存取 BlueXP 的其他功能。如需詳細資訊，請參閱 NetApp ONTAP 文件中的 [System Manager 與 BlueXP 整合](#) 主題。

**Note**

具有多個 HA 對的第二代檔案系統不支援 NetApp System Manager。

## 使用 NetApp ONTAP CLI

您可以使用 NetApp ONTAP CLI 管理您的 Amazon FSx for NetApp ONTAP 資源。您可以在檔案系統（類似於 NetApp ONTAP 叢集）層級和 SVM 層級管理資源。

### 使用 CLI ONTAP 管理檔案系統

您可以在 ONTAP FSx for ONTAP 檔案系統上執行 CLI 命令，類似於在 NetApp ONTAP 叢集上執行命令。您可以透過建立與檔案系統管理端點的安全 shell ONTAP (SSH) 連線，並使用 fsxadmin 使用者名稱和密碼登入，來存取檔案系統上的 CLI。當您使用 [自訂建立流程](#) 或使用 建立檔案系統時，您可以選擇設定 fsxadmin 密碼 AWS CLI。如果您使用快速建立選項建立檔案系統，則未設定 fsxadmin 密碼，因此您需要設定一個才能登入 ONTAP CLI。如需設定檔案系統的 fsxadmin 密碼的詳細資訊，請參閱 [更新檔案系統](#)。您可以在 Amazon FSx 主控台中，在 FSx for ONTAP 檔案系統詳細資訊頁面的管理索引標籤中找到檔案系統管理端點的 DNS 名稱和 IP 地址。

若要使用 SSH 連線至檔案系統的管理端點，請先登入與 FSx for ONTAP 檔案系統位於相同 VPC 中的 EC2 執行個體。登入 EC2 執行個體後，請使用 fsxadmin 使用者和密碼將 SSH 輸入檔案系統的管理端點 IP 地址或 DNS 名稱，如下列範例所示。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

具有範例值的 SSH 命令：



```
ec2user $ ssh fsxadmin@198.51.100.0
```

使用管理端點 DNS 名稱的 SSH 命令：

```
ec2user $ ssh fsxadmin@file-system-management-endpoint-dns-name
```

使用範例 DNS 名稱的 SSH 命令：

```
ec2user $ ssh fsxadmin@management.fs-0abcdef123456789.fsx.us-east-2.aws.com
Password: fsxadmin_password
```

```
This is your first recorded login.
FsxId0abcdef123456789::>
```

可供使用的 ONTAP CLI 命令範圍 **fsxadmin**

fsxadmin 的管理檢視位於檔案系統層級，其中包含檔案系統中的所有 SVMs 和磁碟區。fsxadmin 角色會執行 ONTAP 叢集管理員的角色。由於 Amazon FSx for NetApp ONTAP 檔案系統是完全受管的，因此該 fsxadmin 角色可以執行一部分可用的 CLI ONTAP 命令。

若要查看 fsxadmin 可執行的命令清單，請使用下列 CLI [security login role show](#) ONTAP 命令：

```
FsxId0abc123def456::> security login role show -role fsxadmin -access !none
```

| Vserver               | Role Name | Command/Directory                   | Access Query Level |
|-----------------------|-----------|-------------------------------------|--------------------|
| FsxId0abcdef123456789 |           |                                     |                    |
|                       | fsxadmin  | application                         | all                |
|                       |           | cluster application-record          | all                |
|                       |           | cluster date show                   | readonly           |
|                       |           | cluster ha modify                   | readonly           |
|                       |           | cluster ha show                     | readonly           |
|                       |           | cluster identity modify             | readonly           |
|                       |           | cluster identity show               | readonly           |
|                       |           | cluster log-forwarding -port !55555 | all                |
|                       |           | cluster modify                      | readonly           |
|                       |           | cluster peer                        | all                |
|                       |           | cluster show                        | readonly           |
|                       |           | cluster statistics show             | readonly           |

```
cluster time-service ntp server create      readonly
cluster time-service ntp server delete    readonly
cluster time-service ntp server modify     readonly
cluster time-service ntp server show       readonly
debug network tcpdump -ipspace !Cluster  all
debug san lun                               all
df -vserver !FsxId* -vserver !Cluster     readonly
echo                                       all
event catalog show                       readonly
event config                             all
```

.  
.  
.

378 entries were displayed.

## 使用 CLI ONTAP 管理 SVMs

您可以使用 `vsadmin` 使用者名稱和密碼，建立 SVM ONTAP 管理端點的安全 shell (SSH) 連線，以存取 SVM 上的 CLI。您可以在 Amazon FSx 主控台的儲存虛擬機器詳細資訊頁面的端點面板中找到 SVM 的管理端點 DNS 名稱和 IP 地址，如下圖所示。

| Endpoints                                                              |                            |
|------------------------------------------------------------------------|----------------------------|
| Management DNS name                                                    | Management IP address      |
| svm-06bd701ce68090281.fs-0f17f52f84f11b409.fsx.us-east-2.aws.com       | 198.19.254.86              |
| NFS DNS name                                                           | NFS IP address             |
| svm-06bd701ce68090281.fs-0f17f52f84f11b409.fsx.us-east-2.aws.com       | 198.19.254.86              |
| iSCSI DNS name                                                         | iSCSI IP addresses         |
| iscsi.svm-06bd701ce68090281.fs-0f17f52f84f11b409.fsx.us-east-2.aws.com | 172.31.23.54, 172.31.0.124 |

若要使用 SSH 連線至 SVM 的管理端點，您可以使用 `vsadmin` 使用者名稱和密碼。如果您在建立 SVM 時未為 `vsadmin` 使用者設定密碼，您可以隨時設定 `vsadmin` 密碼。如需詳細資訊，請參閱 [更新儲存虛擬機器 \(SVM\)](#)。您可以使用管理端點 IP 地址或 DNS 名稱，從與檔案系統位於相同 VPC 的用戶端 SSH 進入 SVM。

```
ssh vsadmin@svm-management-endpoint-ip-address
```

具有範例值的命令：

```
ssh vsadmin@198.51.100.10
```

使用管理端點 DNS 名稱的 SSH 命令：

```
ssh vsadmin@svm-management-endpoint-dns-name
```

使用範例 DNS 名稱的 SSH 命令：

```
ssh vsadmin@management.svm-abcdef0123456789fs-0abcdef123456789.fsx.us-east-2.aws.com
```

Password: *vsadmin-password*

This is your first recorded login.

FsxId0abcdef123456789::>

Amazon FSx for NetApp ONTAP 支援 NetApp ONTAP CLI 命令。

如需 CLI NetApp ONTAP 命令的完整參考，請參閱 [ONTAP 命令：手動頁面參考](#)。

## 使用 ONTAP REST API

使用 fsxadmin 登入資料透過 ONTAP REST API 存取 FSx for ONTAP 檔案系統時，請執行下列其中一項操作：

- 停用 TLS 驗證。

或

- 信任 AWS 憑證授權機構 (CAs) – 每個區域中 CAs 的憑證套件可在下列 URLs 中找到：
  - 適用於公有的 <https://fsx-aws-certificates.s3.amazonaws.com/bundle-aws-region.pem> AWS 區域
  - [https://fsx-aws-us-gov-certificates.s3.us-gov-west-1.amazonaws.com/bundle AWS GovCloud 的 -aws-region.pem](https://fsx-aws-us-gov-certificates.s3.us-gov-west-1.amazonaws.com/bundle-AWS-GovCloud-aws-region.pem) 區域
  - 適用於 AWS 中國區域的 <https://fsx-aws-cn-certificates.s3.cn-north-1.amazonaws.com.cn/bundle-aws-region.pem>

如需 NetApp ONTAP REST API 命令的完整參考，請參閱 [NetApp ONTAP REST API 線上參考](#)。

# 標記 Amazon FSx 資源

為了協助您管理檔案系統和其他 Amazon FSx 資源，您可以以標籤的形式將自己的中繼資料指派給每個資源。使用標籤，您可以用不同的方式分類 AWS 資源，例如依用途、擁有者或環境。當您有許多相同類型的資源時，此分類很有用，您可以根據指派給該資源的標籤快速識別特定資源。本主題說明標籤並示範如何建立它們。

## 主題

- [標籤基本概念](#)
- [標記您的 資源](#)
- [將標籤複製到備份](#)
- [標籤限制](#)
- [許可和標記](#)

## 標籤基本概念

標籤是您指派給 AWS 資源的標籤。每個標籤包含您定義的兩個部分：

- 標籤鍵 (例如，CostCenter、Environment 或 Project)。標籤鍵會區分大小寫。
- 標籤值 (例如 111122223333 或 Production)。與標籤鍵相同，標籤值會區分大小寫。標籤值為選用。

您可以使用標籤以不同方式分類 AWS 資源，例如依用途、擁有者或環境。例如，您可以為帳戶的 Amazon FSx 檔案系統定義一組標籤，協助您追蹤每個執行個體的擁有者和堆疊層級。

我們建議您為每種資源類型建立符合您需求的標籤金鑰。使用一致的標籤金鑰組可讓您更輕鬆管理您的資源。您可以根據新增的標籤來搜尋和篩選資源。如需如何實作有效資源標記策略的詳細資訊，請參閱中的[標記 AWS 資源](#) AWS 一般參考。

要記住的一些標記行為：

- 標籤對 Amazon FSx 沒有任何語意意義，並嚴格解譯為字元字串。
- 標籤不會自動指派給您的資源。
- 您可以編輯標籤金鑰和值，並且可以隨時從資源移除標籤。

- 您可以將標籤的值設定為空字串，但無法將標籤的值設定為 null。
- 若您將與現有標籤具有相同鍵的標籤新增到該資源，則新值會覆寫舊值。
- 如果您刪除資源，也會刪除任何該資源的標籤。
- 如果您使用的是 Amazon FSx API、AWS Command Line Interface (AWS CLI) 或 AWS SDK，您可以執行下列動作：
  - 您可以使用 TagResource API 動作將標籤套用至現有資源。
  - 對於某些資源建立動作，您可以在建立資源時為資源指定標籤。藉由在建立時為資源建立標籤，您可以消除在資源建立後執行自訂標籤指令碼的必要。

如果無法在資源建立期間套用標籤，Amazon FSx 會復原資源建立程序。此行為有助於確保使用標籤建立資源，或完全沒有建立資源，並且隨時不會保留任何未標記的資源。

#### Note

使用者在建立時標記資源需要特定 AWS Identity and Access Management (IAM) 許可。如需詳細資訊，請參閱[在建立期間授予標籤資源的許可](#)。

## 標記您的 資源

您可以標記帳戶中存在的 Amazon FSx 資源。如果您使用的是 Amazon FSx 主控台，您可以使用相關資源畫面上的標籤索引標籤，將標籤套用至資源。建立資源時，您可以使用值套用名稱金鑰，並在建立新的檔案系統時套用您選擇的標籤。不過，即使主控台根據名稱金鑰組織資源，此金鑰對 Amazon FSx 服務沒有任何語意意義。

若要對可在建立時標記資源的使用者和群組實作精細控制，您可以將 IAM 政策中的標籤型資源層級許可套用至支援建立時標記的 Amazon FSx API 動作。透過在政策中使用此類許可，您可獲得以下好處：

- 您的資源已正確保護，無法建立。
- 由於標籤會立即套用至您的資源，因此控制資源使用的任何標籤型資源層級許可都會立即生效。
- 您可以更準確的追蹤和報告您的資源。
- 您可以強制新資源使用標籤，並控制哪些標籤金鑰和值會在您的資源上設定。

若要控制現有資源上設定的標籤索引鍵和值，您可以將資源層級許可套用至 IAM 政策中的 TagResource 和 UntagResource Amazon FSx API 動作。

如需建立時標記 Amazon FSx 資源所需許可的詳細資訊，請參閱[在建立期間授予標籤資源的許可](#)。

如需在 IAM 政策中使用標籤來限制對 Amazon FSx 資源的存取的詳細資訊，請參閱[使用標籤來控制對 Amazon FSx 資源的存取](#)。

如需為計費標記資源的相關資訊，請參閱AWS Billing 《使用者指南》中的[使用成本分配標籤](#)。

## 將標籤複製到備份

當您在 Amazon FSx API 或 中建立或更新磁碟區時 AWS CLI，您可以讓 CopyTagsToBackups 自動將磁碟區中的任何標籤複製到備份。

### Note

如果您在建立使用者啟動的備份時指定標籤（包括使用 Amazon FSx 主控台建立備份時的名稱標籤），即使您已啟用，也不會從磁碟區複製標籤 CopyTagsToBackups。

如需備份的詳細資訊，請參閱[使用磁碟區備份保護您的資料](#)。如需啟用的詳細資訊 CopyTagsToBackups，請參閱《Amazon FSx for NetApp ONTAP 使用者指南[更新磁碟區的組態 \(CLI\)](#)》中的 [建立磁碟區 \(CLI\)](#) 和 或《Amazon FSx for NetApp ONTAP API 參考》中的 [CreateVolume](#) 和 [UpdateVolume](#)。

## 標籤限制

以下基本限制適用於標籤：

- 每一資源標籤數最多為 50。
- 索引鍵的長度上限為 128 個 Unicode 字元 (UTF-8)。
- 值的長度上限則為 256 個 Unicode 字元 (UTF-8)。
- 允許的字元為以 UTF-8 表示的字母、數字和空格，以及下列字元：+- (連字號) = . \_ (底線) : / @。
- 對於每一個資源，每個標籤金鑰必須是唯一的，且每個標籤金鑰只能有一個值。
- 標籤鍵與值皆區分大小寫。
- 字aws: 首會保留供 AWS 使用。如果標籤具有使用此字首的標籤金鑰，則您無法編輯或刪除標籤的金鑰或值。具 aws: 字首的標籤，不算在受資源限制的標籤計數內。

您無法僅根據資源的標籤刪除資源；您必須指定資源識別符。例如，若要刪除您以名為 的標籤金鑰標記的檔案系統DeleteMe，您必須使用 DeleteFileSystem動作搭配檔案系統資源識別符，例如 fs-1234567890abcdef0。

當您標記公有或共用資源時，您指派的標籤只能提供給 AWS 帳戶；其他 無法存取 AWS 帳戶 這些標籤。對於共用資源的標籤型存取控制，每個 AWS 帳戶 都必須指派自己的一組標籤來控制對資源的存取。

## 許可和標記

如需建立時標記 Amazon FSx 資源所需許可的詳細資訊，請參閱[在建立期間授予標籤資源的許可](#)。

如需在 IAM 政策中使用標籤來限制對 Amazon FSx 資源的存取的詳細資訊，請參閱 [使用標籤來控制對 Amazon FSx 資源的存取](#)。

# 保護您的資料

除了自動複寫檔案系統的資料以確保[高耐用性](#)之外，使用 Amazon FSx 您還可以使用下列選項來進一步保護資料：

- 原生 Amazon FSx 磁碟區備份，可支援 Amazon FSx 內的備份保留和合規需求。
- 使用 AWS Backup 跨多個 實作集中管理的自動化備份和保留策略 AWS 服務。
- 透過將檔案還原到舊版，讓您的使用者輕鬆復原不需要的檔案變更的快照。
- 使用 SnapLock 建立寫入一次，讀取多個 (WORM) 儲存磁碟區，以防止在指定的保留期間內進行檔案修改或刪除。
- FlexCache 磁碟區提供儲存效率、經濟實惠、高效能的資料複寫，適用於具有大部分不變資料的大量讀取工作負載。
- 使用 SnapMirror 建立排程的自動檔案系統複寫至第二個檔案系統，以進行資料保護和災難復原。

## 主題

- [使用磁碟區備份保護您的資料](#)
- [使用快照保護您的資料](#)
- [使用自治勒索軟體保護來保護您的資料](#)
- [使用 保護您的資料 SnapLock](#)
- [使用 複寫您的資料 FlexCache](#)
- [使用 複寫您的資料 NetApp SnapMirror](#)

## 使用磁碟區備份保護您的資料

透過 FSx for ONTAP，您可以對檔案系統上的磁碟區進行自動每日備份和使用者起始的備份，以保護資料。為您的磁碟區建立定期備份是最佳實務，可協助支援您的資料保留和合規需求。您可以將磁碟區備份還原至您有權存取的任何現有 FSx for ONTAP 檔案系統，其位於存放備份 AWS 區域 的相同位置。使用 Amazon FSx 備份可讓您輕鬆地建立、檢視、還原和刪除磁碟區的備份。

Amazon FSx 支援使用 `OntapVolumeType` 的讀寫 (RW) 備份 ONTAP 磁碟區。



 Note

Amazon FSx 不支援備份 FlexCache 和 的資料保護 (DP) 磁碟區、負載共用鏡像 (LSM) 磁碟區或目的地磁碟區 SnapMirror。

## 主題

- [備份的運作方式](#)
- [儲存需求](#)
- [自動每日備份](#)
- [使用者啟動的備份](#)
- [將標籤複製到備份](#)
- [AWS Backup 搭配 Amazon FSx 使用](#)
- [將備份還原至新磁碟區](#)
- [備份和還原效能](#)
- [備份磁碟 SnapLock 區](#)
- [建立使用者啟動的備份](#)
- [將備份還原至新磁碟區](#)
- [還原資料子集](#)
- [還原備份時監控進度](#)
- [刪除備份](#)

## 備份的運作方式

所有 Amazon FSx 備份（自動每日備份和使用者啟動的備份）都是增量備份，這表示它們只會儲存自上次備份完成後的資料變更。這可最大限度地減少建立備份所需的時間和每個備份使用的儲存量。增量備份不會儲存重複的資料，以最佳化儲存成本。ONTAP 備份的 FSx 是每個磁碟區，每個備份只包含一個特定磁碟區的資料。Amazon FSx 備份會以備援方式跨多個可用區域存放，以達到高耐用性。

Amazon FSx 備份使用快照 – point-in-time 唯讀映像 – 來維持備份之間的增量。每次進行備份時，Amazon FSx 會先拍攝磁碟區的快照。備份快照會存放在您的磁碟區中，並在磁碟區上耗用儲存空間。然後，Amazon FSx 會將此快照與先前的備份快照（如果有的話）進行比較，並僅將變更的資料複製到備份中。

如果沒有先前的備份快照，則會將最新備份快照的整個內容複製到您的備份。成功取得最新的備份快照後，Amazon FSx 會刪除先前的備份快照。用於最新備份的快照會保留在您的磁碟區中，直到程序重複進行下一個備份為止。為了最佳化備份儲存成本，會在備份中ONTAP保留磁碟區的儲存效率節省。

當您[刪除](#)備份時，只會刪除該備份特有的資料。每個 Amazon FSx 備份都包含從備份建立新磁碟區所需的所有資訊，有效地還原磁碟區的point-in-time快照。

您可以為每個磁碟區 AWS 帳戶 和每個磁碟區存放的備份數量有限制。如需詳細資訊，請參閱[您可以提高的配額](#)及[每個檔案系統的資源配額](#)。

## 儲存需求

您的磁碟區和檔案系統必須各自有足夠的可用 SSD 儲存容量來存放備份快照。拍攝備份快照時，快照使用的額外儲存容量不會導致磁碟區超過 98% 的 SSD 儲存使用率。如果發生這種情況，備份將會失敗。您可以隨時[增加磁碟區](#)或[檔案系統的 SSD](#) 儲存體，以確保您的備份不會中斷。

## 自動每日備份

當您建立檔案系統時，預設會針對檔案系統的磁碟區啟用自動每日備份。您可以隨時啟用或停用現有檔案系統的自動每日備份。所有磁碟區的自動每日備份會在檔案系統的每日備份時段期間進行，該時段會在您建立檔案系統時自動設定。您可以隨時修改每日備份時段。為了獲得最佳[備份效能](#)，我們建議您在用戶端和應用程式存取磁碟區上的資料時，選擇超出正常操作時間的每日備份時段。

使用 主控台，您可以在建立檔案系統時或隨時將自動每日備份的保留期間設定為 1 到 90 天的值。預設的每日自動備份保留期為 30 天。Amazon FSx 會在保留期間過期時刪除自動每日備份。使用 AWS CLI 和 API，您可以將保留期間設定為 0 到 90 天的值；將其設定為 0 會關閉自動每日備份。

自動每日備份、每日備份時段和備份保留期間是檔案系統設定，並套用到檔案系統上的所有磁碟區。您可以使用 Amazon FSx 主控台 AWS CLI、或 API 來變更這些設定。如需詳細資訊，請參閱[更新檔案系統](#)。

如果磁碟區離線，則無法建立磁碟區備份（自動每日備份或使用者啟動的備份）。如需詳細資訊，請參閱[檢視離線磁碟區](#)。

### Note

自動每日備份的保留期間上限為 90 天，但除非您 AWS Backup 或刪除備份，否則您建立的[使用者起始備份](#)，包括使用 建立的備份 AWS Backup，都會永久保留。

您可以使用 Amazon FSx 主控台、CLI 和 API 手動[刪除](#)自動每日備份。當您刪除磁碟區時，也會刪除該磁碟區的自動每日備份。Amazon FSx 提供在刪除磁碟區之前建立磁碟區最終備份的選項。除非您刪除，否則最終備份會永久保留。

## 使用者啟動的備份

使用 Amazon FSx，您可以隨時使用 AWS Management Console AWS CLI 和 API 手動備份檔案系統的磁碟區。您的使用者起始備份是相對於為磁碟區建立並永久保留的其他備份遞增的，除非您刪除它們。即使您刪除磁碟區或建立備份的檔案系統，也會保留使用者啟動的備份。您只能使用 Amazon FSx 主控台、API 或 CLI [刪除使用者啟動的備份](#)。Amazon FSx 永遠不會自動刪除它們。

如需如何建立使用者起始備份的說明，請參閱 [建立使用者啟動的備份](#)。

## 將標籤複製到備份

當您使用 CLI 或 API 建立或更新磁碟區時，您可以讓 CopyTagsToBackups 自動[將磁碟區上的任何標籤複製到](#)其備份。不過，如果您在建立使用者起始的備份時新增任何標籤，包括在使用主控台時命名備份，即使 CopyTagsToBackups 已啟用，Amazon FSx 也不會從磁碟區複製標籤。

## AWS Backup 搭配 Amazon FSx 使用

AWS Backup 是一種簡單且經濟實惠的方式，可透過備份 Amazon FSx for NetApp ONTAP 磁碟區來保護您的資料。AWS Backup 是一種統一的備份服務，旨在簡化備份的建立、還原和刪除，同時改善報告和稽核。使用 AWS Backup 可讓您更輕鬆地開發集中式備份策略，以實現法律、法規和專業合規。它也提供您可以執行下列動作的集中位置，讓保護 AWS 儲存磁碟區、資料庫和檔案系統變得更簡單：

- 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、複製和還原活動。

AWS Backup 使用 Amazon FSx 的內建備份功能。使用 AWS Backup 主控台建立的備份具有相同層級的檔案系統一致性和效能，與任何其他 Amazon FSx 使用者啟動的磁碟區備份相對遞增，並提供與使用 Amazon FSx 主控台取得的備份相同的還原選項。使用 AWS Backup 管理這些備份提供額外的功能，包括能夠每小時頻繁地建立排程備份。您可以新增額外的防禦層，透過將備份存放在備份[文件庫](#)中來保護備份免於意外或惡意刪除。

建立的備份 AWS Backup 會被視為使用者啟動的備份，並計入 Amazon FSx 的使用者啟動備份配額。如需詳細資訊，請參閱[您可以提高的配額](#)。您可以使用 Amazon FSx 主控台、CLI 和 API 檢視和還原建立 AWS Backup 的備份。不過，您無法刪除在 Amazon FSx 主控台、CLI 或 API AWS Backup 中建立的備份。如需詳細資訊，請參閱《AWS Backup 開發人員指南》中的[入門 AWS Backup](#)。

AWS Backup 無法備份離線的磁碟區。

您可以使用標籤來選取備份計劃中保護哪些 FSx for ONTAP 資源。這些標籤必須套用在磁碟區層級，而非整個檔案系統層級。如需詳細資訊，請參閱《AWS Backup 開發人員指南》中的[將資源指派給備份計劃](#)。

## 將備份還原至新磁碟區

您可以將磁碟區備份還原至檔案系統上的新磁碟區，該檔案系統與儲存備份所在的磁碟區相同 AWS 區域。您無法將備份還原至與備份 AWS 區域不同的檔案系統。

在適用於 ONTAP 第二代檔案系統的 FSx 上還原備份時，用戶端可以在還原磁碟區時掛載和讀取資料。一旦 Amazon FSx 將所有中繼資料載入新磁碟區，且磁碟區回報生命週期狀態為 `CREATED`，用戶端就可以掛載您要還原的磁碟區並讀取檔案資料。您可以在 Amazon FSx 主控台的磁碟區[詳細資訊](#)頁面上，以及[describe-volumes CLI 命令的回應中找到磁碟區](#)的生命週期狀態。

從備份還原時從磁碟區讀取資料時，如果資料尚未下載到磁碟區，則第一次存取時會產生高達 00 毫秒的讀取延遲。這些讀取會快取在 SSD 層中，您可以預期後續讀取的讀取延遲會低於一毫秒。

Amazon FSx 讓磁碟區可供唯讀存取所需的時間，與備份中存放的檔案中繼資料量成比例。檔案中繼資料通常會使用 1-7% 的整體備份資料，取決於資料集的平均檔案大小（小型檔案資料集比大型檔案資料集使用更多的中繼資料）。

當您將 FlexGroup 磁碟區備份還原至與原始檔案系統具有不同數量[高可用性 \(HA\) 對](#)的檔案系統時，Amazon FSx 會新增額外的元件磁碟區，以確保元件平均分配。

### Note

從磁碟區或第一代檔案系統的任何磁碟區備份還原 SnapLock 磁碟區時，Amazon FSx 不支援資料的讀取存取。還原這些備份時，磁碟區會在還原程序完成後可供掛載和存取資料，且所有中繼資料和資料都會載入新磁碟區。

還原備份時，所有資料一開始都會寫入 SSD 儲存層。還原進行中時，資料會根據要還原之磁碟區的分層政策，分層至容量集區儲存體。由於資料會先寫入 SSD 層，如果檔案系統用盡 SSD 儲存空

間，Amazon FSx 會暫停還原程序。一旦有足夠的 SSD 空間可供繼續程序，還原就會自動繼續。如果還原磁碟區的分層政策為 All，則定期背景程序會將資料分層至容量集區。如果還原磁碟區的分層政策是 Snapshot Only 或 Auto，且檔案系統的 SSD 使用率大於 50%，且冷卻速率取決於分層政策的冷卻期間，則資料會分層至容量集區。

如果您的工作負載在第二代檔案系統上將備份還原至新磁碟區時需要一致的低於毫秒的讀取延遲，我們建議您在啟動還原 None 時將磁碟區的分層政策設定為 `None`，然後等到所有資料完全下載至磁碟區後才能存取。在您嘗試存取所有資料之前，所有資料都會載入 SSD 儲存體，為您提供一致的低延遲存取資料。

如需如何將備份還原至新磁碟區的 step-by-step 說明，請參閱 [將備份還原至新磁碟區](#)。

在第二代檔案系統上，您也可以只從備份還原一部分的資料，而不必等待整個還原操作完成。僅還原備份資料的一部分，可讓您在意外刪除、修改或損毀資料時更快恢復操作。如需詳細資訊，請參閱 [還原資料子集](#)。

您可以在 [和 AWS Management Console](#) [AWS CLI](#) [API](#) 中的第二代檔案系統上還原備份時監控進度。如需詳細資訊，請參閱 [還原備份時監控進度](#)。

#### Note

- 您無法建立磁碟區快照或執行快照型操作，例如複製、SnapMirror 複寫，以及從備份還原時建立磁碟區的備份。
- 還原的磁碟區一律具有與原始磁碟區相同的磁碟區樣式。您無法在還原時變更磁碟區樣式。

## 備份和還原效能

各種因素可能會影響備份和還原操作的效能。備份和還原操作是背景程序，這表示它們的優先順序比用戶端 IO 操作低。用戶端 IO 操作包括 NFS、CIFS 和 iSCSI 資料，以及中繼資料讀取和寫入。所有背景程序只會使用檔案系統輸送量容量的未使用部分，而且可能需要幾分鐘到幾小時才能完成，具體取決於備份的大小以及檔案系統上未使用的輸送量容量。

影響備份和還原效能的其他因素包括儲存資料的儲存層和資料集描述檔。我們建議您在大部分資料位於 SSD 儲存體時，建立磁碟區的第一個備份。與包含大部分大型檔案的類似大小資料集相比，包含大部分小型檔案的資料集通常效能較低。這是因為處理大量小型檔案會耗用比處理較少大型檔案更多的 CPU 週期和網路額外負荷。

一般而言，在備份存放在 SSD 儲存層中的資料時，您可以預期下列備份速率：

- 750 MBps 跨多個並行備份，其中包含大部分大型檔案。

- 100 MBps 跨多個並行備份，其中包含大部分的小型檔案。

一般而言，您可以預期下列還原率：

- 250 MBps，跨包含大部分大型檔案的數個並行還原。
- 100 MBps 跨多個並行還原，其中包含大部分的小型檔案。

## 備份磁碟SnapLock區

您可以備份[SnapLock](#)磁碟區以提供額外的資料保護。當您還原磁碟SnapLock區時，會保留磁碟區的原始設定，例如預設保留期、最短保留期和最長保留期。寫入一次，讀取許多 (WORM) 設定和法務保存也會保留。

### Note

您無法備份SnapLock FlexGroup磁碟區。

您可以將SnapLock磁碟區的備份還原為 SnapLock或非SnapLock 磁碟區。不過，您無法將非SnapLock 磁碟區的備份還原為SnapLock磁碟區。

如需詳細資訊，請參閱[SnapLock 的運作方式](#)。

## 建立使用者啟動的備份

下列程序說明如何建立使用者啟動的磁碟區備份。

如果磁碟區離線，則無法建立磁碟區備份。如需詳細資訊，請參閱[檢視離線磁碟區](#)。

建立使用者起始的備份（主控台）

1. 在 <https://console.aws.amazon.com/fsx/>：// 開啟 Amazon FSx 主控台。
2. 導覽至檔案系統，然後選擇您要為其備份磁碟區ONTAP的檔案系統。
3. 選擇磁碟區索引標籤。
4. 選擇您要備份的磁碟區。
5. 在動作中，選擇建立備份。
6. 在開啟的建立備份對話方塊中，提供備份的名稱。備份名稱最多可有 256 個 Unicode 字元，包括字母、空格、數字和特殊字元。+ - = \_ : /



## 7. 選擇 Create backup (建立備份)。

您現在已建立其中一個檔案系統磁碟區的備份。您可以在左側導覽中選擇備份，在 Amazon FSx 主控台中查看所有備份。您可以搜尋您提供備份的名稱，以及資料表篩選條件，只顯示相符的結果。

當您依照此程序所述建立使用者啟動的備份時，其類型為 `USER_INITIATED`，且狀態為 `CREATING` 直到完全可用為止。

## 將備份還原至新磁碟區

下列程序說明如何使用 AWS Management Console 和 將 FSx for ONTAP 備份還原至新的磁碟區 AWS CLI。將磁碟區還原至第二代檔案系統時，您可以使用 AWS Management Console AWS CLI、和 API [來監控](#)進度。

將磁碟區備份還原至新磁碟區（主控台）

1. 在 <https://console.aws.amazon.com/fsx/>：// 開啟 Amazon FSx 主控台。
2. 在導覽窗格中，選擇備份，然後選擇您要還原的 FSx for ONTAP 磁碟區備份。
3. 在右上角的動作選單中，選擇還原備份。隨即顯示從備份建立磁碟區頁面。
4. 從下拉式選單中選擇您要還原備份的 FSx for ONTAP 檔案系統和儲存虛擬機器。
5. 在右上角的動作選單中，選擇還原備份。從備份建立磁碟區頁面隨即出現。
6. 從下拉式功能表中選擇您要還原備份的 FSx for ONTAP 檔案系統和儲存虛擬機器。
7. 在磁碟區詳細資訊下，有數個選擇。首先，輸入磁碟區名稱。您最多可以使用 203 個英數字元或底線 ( \_ ) 字元。
8. 對於磁碟區大小，輸入 20–314572800 範圍內的任何整數，以指定以 MB (MiB) 為單位的大小。
9. 針對磁碟區類型，選擇讀寫 (RW) 以建立可讀取且可寫入的磁碟區，或選擇資料保護 (DP) 以建立唯讀且可作為 NetAppSnapMirror 或 SnapVault 關係目的地的磁碟區。如需詳細資訊，請參閱[磁碟區類型](#)。
10. 在 Junction 路徑中，輸入檔案系統中的位置以掛載磁碟區。名稱必須有正斜線，例如 `/vol3`。
11. 為了提高儲存效率，請選擇啟用以啟用 ONTAP 儲存效率功能（重複資料刪除、壓縮和壓縮）。如需詳細資訊，請參閱[儲存效率](#)。
12. 針對磁碟區安全樣式，選擇 Unix (Linux)、NTFS 或 Mixed。磁碟區的安全樣式會決定是否將偏好設定提供給 NTFS 或 UNIX ACLs 以進行多協定存取。多重通訊協定存取不需要 MIXED 模式，且僅適用於進階使用者。
13. 針對快照政策，選擇磁碟區的快照政策。如需快照政策的詳細資訊，請參閱[快照政策](#)。

如果您選擇自訂政策，您必須在自訂政策欄位中指定政策的名稱。自訂政策必須已存在於 SVM 或檔案系統中。您可以使用 CLI 或 REST API ONTAP 建立自訂快照政策。如需詳細資訊，請參閱 NetApp ONTAP 產品文件中[的建立快照政策](#)。

14. 對於分層政策冷卻期間，有效值為 2-183 天。磁碟區的分層政策冷卻期間會定義未存取的資料標記為冷並移至容量集區儲存體之前的天數。此設定只會影響 Auto 和 Snapshot-only 政策。
15. 在進階區段的 SnapLock 組態中，您可以保留預設的已停用設定，或選擇已啟用來設定 SnapLock 磁碟區。如需設定 SnapLock 合規磁碟區或 SnapLock 企業磁碟區的詳細資訊，請參閱 [了解 SnapLock 合規](#) 和 [了解 SnapLock 企業](#)。如需 SnapLock 的相關資訊，請參閱 [使用 保護您的資料 SnapLock](#)。
16. 選擇確認以建立磁碟區。
17. 如果您要將備份還原至第二代檔案系統，您可以在磁碟區頁面上的更新索引標籤上監控備份還原進度。如需詳細資訊，請參閱[還原備份時監控進度](#)。

### 將備份還原至新磁碟區 (CLI)

使用 [create-volume-from-backup](#) CLI 命令或對等的 [CreateVolumeFromBackup](#) API 命令，將磁碟區備份還原至新的磁碟區。

```
$ aws fsx create-volume-from-backup --backup-id backup-08e6fc1133fff3532 \
  --name demo --ontap-configuration JunctionPath=/demo,SizeInMegabytes=100000,\
  StorageVirtualMachineId=svm-0f04a9c7c27e1908b,TieringPolicy={Name=ALL}
```

成功還原請求將備份還原至第二代檔案系統的系統回應如下所示。回應包含 "AdministrativeActions" 物件，提供請求的狀態和進度資訊。

```
{
  "Volume": {
    "CreationTime": 1692721488.428,
    "FileSystemId": "fs-07ab735385276ed60",
    "Lifecycle": "CREATING",
    "Name": "demo",
    "OntapConfiguration": {
      "FlexCacheEndpointType": "NONE",
      "JunctionPath": "/demo",
      "SizeInMegabytes": 100000,
      "StorageEfficiencyEnabled": true,
      "StorageVirtualMachineId": "svm-0f04a9c7c27e1908b",
      "StorageVirtualMachineRoot": false,
      "TieringPolicy": {
```



```

        "Name": "ALL"
    },
    "OntapVolumeType": "DP",
    "SnapshotPolicy": "default",
    "CopyTagsToBackups": false,
},
"ResourceARN": "arn:aws:fsx:us-east-1:752825163408:volume/
fs-07ab735385276ed60/fsvol-0b6ec764c9c5f654a",
"VolumeId": "fsvol-0b6ec764c9c5f654a",
"VolumeType": "ONTAP",
---> "AdministrativeActions": [
    {
        "AdministrativeActionType": "DOWNLOAD_DATA_FROM_BACKUP",
        "RequestTime": 1685729972.069,
        "Status": "PENDING"
    }
]
<----
}
}

```

成功請求將備份還原至第一代檔案系統的系統回應如下所示。

```
{
  "Volume": {
    "CreationTime": 1692721488.428,
    "FileSystemId": "fs-07ab735385276ed60",
    "Lifecycle": "CREATING",
    "Name": "demo",
    "OntapConfiguration": {
      "FlexCacheEndpointType": "NONE",
      "JunctionPath": "/demo",
      "SizeInMegabytes": 100000,
      "StorageEfficiencyEnabled": true,
      "StorageVirtualMachineId": "svm-0f04a9c7c27e1908b",
      "StorageVirtualMachineRoot": false,
      "TieringPolicy": {
        "Name": "ALL"
      },
      "OntapVolumeType": "DP",
      "SnapshotPolicy": "default",
      "CopyTagsToBackups": false,
    },
  },
}
```

```
"ResourceARN": "arn:aws:fsx:us-east-1:752825163408:volume/
fs-07ab735385276ed60/fsvol-0b6ec764c9c5f654a",
  "VolumeId": "fsvol-0b6ec764c9c5f654a",
  "VolumeType": "ONTAP",
}
}
```

將磁碟區還原至第二代檔案系統時，您可以使用 AWS Management Console AWS CLI、和 API [來監控進度](#)。

## 還原資料子集

您可以在備份還原至第二代檔案系統上的新磁碟區時，從備份還原一部分的資料，而不必等到整個備份資料集完全還原為止。

下列程序列出當您在還原備份時需要復原一部分資料，且無法等待整個還原完成時所要採取的步驟：

在還原備份時還原資料子集

1. 在 <https://console.aws.amazon.com/fsx/>：// 開啟 Amazon FSx 主控台。
2. 在備份頁面中，找到包含您要還原之資料版本的備份。
3. 在右上角的動作選單中，選擇還原備份。從備份建立磁碟區頁面隨即出現。
4. 從下拉式功能表中選擇您要還原備份的 FSx for ONTAP 檔案系統和儲存虛擬機器。
5. 在磁碟區詳細資訊下，設定磁碟區以符合您的需求。
6. 選擇確認以建立磁碟區。
7. [監控備份還原的進度](#)。
8. 掛載報告生命週期狀態為 時要還原的 [磁碟區](#) CREATED。
9. 在您需要複製的磁碟區上尋找資料的子集。
10. 將資料複製到應用程式使用的現有磁碟區。
11. 將備份中的必要資料複製到目標位置後，您可以在完成之前刪除要還原的磁碟區，以最佳化檔案系統資源的使用率。

## 還原備份時監控進度

您可以在 和 API 中將磁碟區備份還原至第二代檔案系統時 AWS Management Console AWS CLI 監控進度。如同所有 Amazon FSx 管理動作，在操作完成後 30 天內，可在主控台、CLI 和 API 中使用備份還原狀態。

### 在還原備份時監控進度（主控台）

開啟位於 <https://console.aws.amazon.com/fsx/> 的 Amazon FSx 主控台。

1. 在左側導覽功能表中，選擇磁碟區。
2. 選擇要還原備份的磁碟區。
3. 選擇更新索引標籤。
4. 備份還原更新類型提供下列資訊：
  - PENDING 表示檔案中繼資料正在下載到磁碟區。磁碟區的生命週期狀態為 CREATING。
  - IN\_PROGRESS 表示磁碟區可用，而且用戶端可以掛載具有資料唯讀存取權的磁碟區。進度 % 顯示已下載至磁碟區的資料百分比。
  - COMPLETED 表示所有資料都已下載至磁碟區，且備份還原已完成。用戶端現在具有讀寫存取權。對於磁碟 RW 區，磁碟區的類型 RW 此時會從 DP 變更為 。

### 在還原備份時監控進度 (CLI)

- 當您將備份還原到第二代 FSx for ONTAP 檔案系統上的新磁碟區時，您可以使用 CLI [describe-volumes](#) 命令來監控還原的進度。

將備份還原至第二代檔案系統時，回應會包含 AdministrativeActions 物件，提供資料下載程序的狀態資訊。所以此

```
$ aws fsx describe-volumes
{
  "Volumes": [
    {
      "CreationTime": 1691686114.674,
      "FileSystemId": fs-029ff92192bd4d375,
      "LifeCycle": "CREATING",
      "Name": vol1,
      "OntapConfiguration": {
        "FlexCacheEndpointType": "NONE",
```

```

    "JunctionPath": "/vol1",
    "SizeInMegabytes": 100000,
    "StorageEfficiencyEnabled": true,
    "StorageVirtualMachineId": "svm-0ed1d714019426ca9",
    "StorageVirtualMachineRoot": false,
    "TieringPolicy": {
      "Name": "ALL"
    },
    "OntapVolumeType": "DP",
    "SnapshotPolicy": "default",
    "CopyTagsToBackups": false,
  },
  "ResourceARN": "arn:aws:fsx:us-east-1:630831496844:volume/
fs-08ac75f715c6aec76/fsvol-094c015af930790fa",
  "VolumeId": "fsvol-094c015af930790fa",
  "VolumeType": "ONTAP",
  "AdministrativeActions": [
    {
      "AdministrativeActionType": "DOWNLOAD_DATA_FROM_BACKUP",
      "RequestTime": 1685729972.069,
      "Status": "PENDING"
    }
  ]
}

```

Amazon FSx 將所有檔案中繼資料載入還原的磁碟區後，這些欄位會有下列值：

- "LifeCycle": "CREATED" – 表示磁碟區已準備好掛載。
- "OntapVolumeType": "DP" – 表示下載檔案資料時磁碟區為唯讀。
- "ProgressPercent" – 顯示載入磁碟區的檔案資料百分比。
- "Status": "IN\_PROGRESS" – 正在將檔案資料下載至磁碟區。

在還原程序的這個階段，您可以掛載磁碟區，以唯讀方式存取您要還原之備份中的所有資料。

當 Amazon FSx 已完成將所有檔案資料下載到新磁碟區時，如果這是RW磁碟區，則用戶端具有完整的讀寫存取權。這些指標具有下列值：

- "LifeCycle": "CREATED" – 不變
- "OntapVolumeType": "RW" – 表示用戶端具有完整的讀寫存取權。
- "Status": "COMPLETED" – 表示還原已完成。

如果還原程序失敗，的值 `AdministrativeAction > Status` 將為 `FAILED`。 `FailureDetails` 物件中會提供錯誤訊息。如需詳細資訊，請參閱《Amazon FSx API 參考》中的 [AdministrativeActionFailureDetails](#)

## 刪除備份

您可以使用 Amazon FSx 主控台、Amazon FSx FSx API 或 AWS Command Line Interface () 刪除磁碟區的自動每日備份和使用者啟動備份 AWS CLI。刪除備份是永久且無法復原的動作。也會刪除已刪除備份中的任何資料。除非您確定未來不需要該備份，否則請勿刪除備份。如果來源磁碟區 [離線](#)，則無法刪除備份。

您可以在從所有 FSx for ONTAP 檔案系統的備份還原磁碟區時將其刪除。在還原期間刪除磁碟區會有效地取消進行中還原操作。

### Note

除非已刪除 ONTAP 磁碟區的所有其他 AVAILABLE 備份，否則 Amazon FSx 不支援刪除磁碟區的最新備份。

若要刪除使用 建立的備份 AWS Backup，請參閱 [《開發人員指南》中的刪除備份](#)。AWS Backup

### 刪除備份原則 (主控台)

1. 在 <https://console.aws.amazon.com/fsx/> : // 開啟 Amazon FSx 主控台。
2. 從主控台儀表板中，從左側導覽中選擇備份。
3. 從備份資料表中選擇要刪除的備份，然後選擇刪除備份。
4. 在開啟的刪除備份對話方塊中，確認顯示的備份 ID 是您想要刪除的備份。
5. 確認已針對您要刪除的備份勾選核取方塊。
6. 選擇刪除備份。

您的備份和所有包含的資料現在都會永久且無法復原地刪除。

## 刪除備份 (CLI)

- 使用 delete-backup CLI 命令或同等 DeleteBackup API 動作來刪除 FSx for ONTAP 磁碟區備份，如下列範例所示。

```
$ aws fsx delete-backup --backup-id backup-a0123456789abcdef
```

系統回應包含要刪除的備份 ID，及其生命週期狀態，值為 DELETED，表示請求成功。

```
{
  "BackupId": "backup-a0123456789abcdef",
  "Lifecycle": "DELETED"
}
```

## 使用快照保護您的資料

快照是 Amazon FSx for NetApp ONTAP 磁碟區的唯一讀影像。快照可保護您磁碟區中的檔案，避免意外刪除或修改。使用快照，您的使用者可以輕鬆地從較早的快照檢視和還原個別檔案或資料夾，以復原變更、復原已刪除的內容，以及比較檔案版本。

快照包含自上次快照後變更的資料，該快照會耗用檔案系統的 SSD 儲存容量。快照不包含在任何磁碟區**備份**中。您的磁碟區預設會使用快照政策啟用 default 快照。快照會存放在磁碟區根目錄的 .snapshot 目錄中。您隨時可以儲存每個磁碟區最多 1,023 個快照。達到此限制後，您必須先[刪除現有的快照](#)，才能建立新的磁碟區快照。

### 主題

- [快照政策](#)
- [從快照還原檔案](#)
- [檢視常見快照](#)
- [更新磁碟區的快照保留](#)
- [停用自動快照](#)
- [刪除快照](#)
- [刪除快照](#)
- [快照預留](#)

## 快照政策

快照政策會定義系統如何為磁碟區建立快照。此政策指定何時建立快照、要保留多少副本，以及如何命名快照。FSx for ONTAP 有三種內建快照政策：

- default
- default-1weekly
- none

根據預設，每個磁碟區都會與檔案系統的default快照政策相關聯。我們建議對大多數工作負載使用此政策。

default 政策會根據下列排程自動建立快照，並刪除最舊的快照複本，為較新的複本騰出空間：

- 每小時五分鐘後，最多可擷取六個每小時快照。
- 週一至週六午夜後 10 分鐘，最多可擷取兩個每日快照。
- 每週日午夜後 15 分鐘，最多可擷取兩個每週快照。

### Note

快照時間是根據檔案系統的時區，預設為國際標準時間 (UTC)。您可以使用 `timezone - timezone time_zone` ONTAP CLI 命令設定 FSx for ONTAP 檔案系統的時區。如需存取 ONTAP CLI 的詳細資訊，請參閱 [使用 NetApp ONTAP CLI](#)。

default-1weekly 政策的運作方式與default政策相同，只是它只會保留每週排程的一個快照。

none 政策不會拍攝任何快照。您可以將此政策指派給磁碟區，以防止自動擷取快照。

您也可以使用 ONTAP CLI 或 REST API 建立自訂快照政策。如需詳細資訊，請參閱 NetApp ONTAP 產品文件中[的建立快照政策](#)。您可以在 Amazon FSx 主控台、或 Amazon AWS CLI FSx API 中建立或更新磁碟區時，選擇快照政策。如需詳細資訊，請參閱[建立磁碟區](#)及[更新磁碟區](#)。

## 從快照還原檔案

在 Amazon FSx 檔案系統上使用快照，您可以快速還原個別檔案或資料夾的先前版本。

如果您使用 Linux 和 macOS 用戶端，您可以在磁碟區的根 `.snapshot` 目錄中檢視快照。如果您使用 Windows 用戶端，您可以在 Windows Explorer 的 Previous Versions 索引標籤中檢視快照（在檔案或資料夾上按一下滑鼠右鍵時）。

### 從快照還原檔案 (Linux 和 macOS 用戶端)

1. 如果原始檔案仍然存在，而且您不希望快照中的檔案覆寫，請使用 Linux 或 macOS 用戶端重新命名原始檔案，或將其移至不同的目錄。
2. 在 `.snapshot` 目錄中，找到包含您要還原之檔案版本的快照。
3. 將檔案從 `.snapshot` 目錄複製到檔案最初存在的目錄。

### 從快照還原檔案 (Windows 用戶端)

Windows 用戶端上的使用者可以使用熟悉的 Windows File Explorer 介面，將檔案還原至先前的版本。

1. 若要還原檔案，使用者選擇要還原的檔案，然後從內容選單中選擇還原先前的版本（按一下滑鼠右鍵）。
2. 然後，使用者可以從先前版本清單中檢視和還原先前版本。

快照中的資料為唯讀。如果您想要對先前版本標籤中列出的檔案和資料夾進行修改，您必須將要修改的檔案和資料夾複本儲存為可寫入位置，並對複本進行修改。

## 檢視常見快照

通用快照用於在備份之間維持增量。此程序說明如何識別磁碟區上的常見快照。

### 檢視磁碟區的常見快照

- 若要判斷哪個快照是磁碟區的常見快照，請使用 CLI [volume snapshot show](#) ONTAP 命令。

```
volume snapshot show -volume volume-name
```

在輸出中，通用快照的名稱格式為 `backup-id`，其中 *id* 是 17 位數英數字串，如下列範例所示：

```
FsxIdabc12345::> volume snapshot show -volume test_vol
                        ---Blocks---
Vserver Volume      Snapshot                               Size      Total% Used%
-----
-----
```



```
dest-svm test_vol
      snap1                144KB    0%    3%
      snap2                832KB    0%    16%
----> backup-abcdef0123456789a 4.87MB    0%    53% <---
      weekly.2024-05-26_0015 5.02MB    0%    54%
      weekly.2024-06-02_0015 2.22MB    0%    34%
      daily.2024-06-04_0010  284KB    0%    6%
      daily.2024-06-05_0010 4.29MB    0%    50%
      hourly.2024-06-05_0705 168KB    0%    4%
8 entries were displayed.
```

### ⚠ Important

請勿刪除磁碟區上的常見快照，因為它用於維護備份之間的增量。刪除磁碟區的一般快照會導致下一個備份是磁碟區的完整備份，而不是增量備份。

## 更新磁碟區的快照保留

您可以使用 CLI NetApp ONTAP 或 API 變更磁碟區的快照保留量，如下列程序所述。

- 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。*management\_endpoint\_ip* 將取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

- 使用 `volume modify` ONTAP CII 命令來變更用於快照複製預留的磁碟空間百分比。將下列預留位置值取代為您的資料：

- *svm\_name* — 使用 SVM 的名稱。
- *vol\_name* — 使用磁碟區的名稱。
- *percent* — 您要保留給快照複本的磁碟空間百分比。

```
::> volume modify -vserver svm_name -volume vol_name -percent-snapshot-  
space percent
```

下列範例會將 vol1 的快照保留變更為磁碟區儲存容量的 25%。

```
::> volume modify -vserver vs0 -volume vol1 -percent-snapshot-space 25
```

## 停用自動快照

FSx for ONTAP 檔案系統中磁碟區的預設快照政策會啟用自動快照。如果您不需要資料的快照（例如，如果您使用的是測試資料），您可以將磁碟區的快照[政策設定為使用、API 和 CLI 來停用快照](#)，如下列程序所述。

none AWS Management Console AWS CLI ONTAP

### 停用自動快照 (AWS 主控台)

1. 在 <https://console.aws.amazon.com/fsx/> : // 開啟 Amazon FSx 主控台。
2. 導覽至檔案系統，然後選擇您要更新磁碟區的 ONTAP 檔案系統。
3. 選擇磁碟區索引標籤。
4. 選擇您要更新的磁碟區。
5. 針對動作，選擇更新磁碟區。

更新磁碟區對話方塊會顯示磁碟區目前的設定。

6. 針對快照政策，選擇無。
7. 選擇更新以更新磁碟區。

### 停用自動快照 (AWS CLI)

- 使用 [update-volume](#) AWS CLI 命令（或同等的 [UpdateVolume](#) API 命令），將 SnapshotPolicy 設定為 none，如下列範例所示。

```
aws fsx update-volume \  
  --volume-id fsvol-1234567890abcdefa \  
  --name new_vol \  
  --ontap-configuration CopyTagsToBackups=true,JunctionPath=/new_vol, \  
    SizeInMegabytes=2048,SnapshotPolicy=none, \  
    StorageEfficiencyEnabled=true, \  
    TieringPolicy=all
```

## 停用自動快照 (ONTAP CLI)

將磁碟區的快照政策設定為使用none預設政策來關閉自動快照。

1. 使用 [volume snapshot policy show](#) ONTAP CLI 命令來顯示none政策。

```
::> snapshot policy show -policy none
```

```
Vserver: FsxIdabcdef01234567892
```

| Policy Name | Number of Is Schedules | Enabled | Comment                            |
|-------------|------------------------|---------|------------------------------------|
| none        | 0                      | false   | Policy for no automatic snapshots. |
| Schedule    | Count                  | Prefix  | SnapMirror Label                   |
| -           | -                      | -       | -                                  |

2. 使用 [volume modify](#) ONTAP CII 命令將磁碟區的快照政策設定為 none，以停用自動快照。將下列預留位置值取代為您的資料：

- *svm\_name* — 使用 SVM 的名稱。
- *vol\_name* — 使用磁碟區的名稱。

提示繼續時，請輸入 **y**。

```
::> volume modify -vserver svm_name -volume vol_name -snapshot-policy none
```

```
Warning: You are changing the Snapshot policy on volume "vol_name" to "none".
```

```
Snapshot copies on this volume
```

```
that do not match any of the prefixes of the new Snapshot policy will not
be deleted. However, when
```

```
the new Snapshot policy takes effect, depending on the new retention
count, any existing Snapshot copies
```

```
that continue to use the same prefixes might be deleted. See the 'volume
modify' man page for more information.
```

```
Do you want to continue? {y|n}: y
```

```
Volume modify successful on volume vol_name of Vserver svm_name.
```

## 刪除快照

快照只會針對自上次快照以來變更的磁碟區上的資料使用儲存容量。因此，如果您的工作負載快速寫入資料，舊資料的快照可能會佔用大量磁碟區的儲存容量。

例如，CLI [volume show-space](#) ONTAP 命令輸出會顯示 140 KB 的 User Data。不過，在刪除使用者資料 User Data 之前，磁碟區有 9.8 GB 的。即使您已從磁碟區中刪除檔案，快照仍可能參考舊的使用者資料。因此，Snapshot Reserve Snapshot Spill 在先前的範例中，即使磁碟區上幾乎沒有使用者資料，也會佔用總共 9.8 GB 的空間。

若要釋放磁碟區上的空間，您可以刪除不再需要的舊快照。由於快照是增量的，因此在刪除快照時，不會回收與快照大小相等的儲存量。您可以使用磁碟 [區快照運算可回收 -vserver](#) ONTAP CLI 命令，使用資料取代 *svm\_name*、*vol\_name* 和 *snapshot\_name*，來查看刪除快照時可回收的儲存量。

```
fsid8970abc52::> volume snapshot compute-reclaimable -vserver svm_name -volume vol_name
                  -snapshot snapshot_name
A total of 667648 bytes can be reclaimed.
```

您可以透過建立快照 [自動刪除政策](#) 或 [手動刪除快照來刪除快照](#)。刪除快照會刪除儲存在快照上變更的資料。

## 刪除快照

使用 [volume snapshot delete](#) ONTAP CLI 命令手動刪除快照，將下列預留位置值取代為您的資料：

- *svm\_name* 將取代為磁碟區建立所在的 SVM 名稱。
- *vol\_name* 將取代為磁碟區的名稱。
- *snapshot\_name* 將取代為快照的名稱。此命令支援的萬用字元 (\*) *snapshot\_name*。因此，您可以刪除所有每小時快照，例如使用 hourly\*。

### Important

如果您已啟用 Amazon FSx 備份，Amazon FSx 會為每個磁碟區的最新 Amazon FSx 備份保留快照。這些快照用於維護備份之間的增量，且不得使用此方法刪除。如需詳細資訊，請參閱 [檢視常見快照](#)。

```
FsxIdabcdef01234567892::> volume snapshot delete -vserver svm_name -volume vol_name -  
snapshot snapshot_name
```

## 建立快照自動刪除政策

您可以建立政策，以便在磁碟區中的可用空間量不足時自動刪除快照。使用[磁碟區快照自動刪除修改](#) ONTAP CLI 命令來建立磁碟區的自動刪除政策。

使用此命令時，請使用您的資料來取代下列預留位置值：

- *svm\_name* 將取代為磁碟區建立所在的 SVM 名稱。
- *vol\_name* 將取代為磁碟區的名稱。

對於 `-trigger`，請指派下列其中一個值：

- `volume - volume` 如果您希望刪除快照的閾值對應於總使用量容量閾值，請使用。觸發快照刪除的已使用磁碟區容量閾值取決於磁碟區的大小，閾值擴展範圍為已使用容量的 85-98%。較小的磁碟區具有較小的閾值，較大的磁碟區具有較大的閾值。
- `snap_reserve - snap_reserve` 如果您想要根據快照保留中可保留的內容刪除快照，請使用。

```
::> volume snapshot autodelete modify -vserver svm_name -volume vol_name -enabled true  
-trigger [volume|snap_reserve]
```

如需詳細資訊，請參閱 NetApp ONTAP 文件中心中的[磁碟區快照自動刪除修改](#)命令。

## 快照預留

快照複本預留會設定磁碟區儲存容量的特定百分比，用於儲存快照複本，預設值為 5%。快照複本預留必須針對快照複本配置足夠的空間，包括[磁碟區備份](#)。如果快照複本超過快照預留空間，您必須從作用中檔案系統刪除現有的快照複本，以復原儲存容量以供檔案系統使用。您也可以修改分配給快照複本的磁碟空間百分比。

每當快照耗用超過 100% 的快照保留時，就會開始佔用主要 SSD 儲存空間。此程序稱為快照溢出。當快照繼續佔用作用中的檔案系統空間時，檔案系統會有變滿的風險。如果檔案系統因為快照溢出而變滿，您只能在刪除足夠的快照之後建立檔案。

當快照保留中的快照有足夠的磁碟空間可用時，從主要 SSD 層刪除檔案會釋放新檔案的磁碟空間，而參考這些檔案的快照複本只會耗用快照複本保留中的空間。

由於無法防止快照耗用大於預留數量的磁碟空間（快照預留），因此請務必為快照預留足夠的磁碟空間，以便主要 SSD 層永遠有空間可以建立新檔案或修改現有檔案。

如果在磁碟已滿時建立快照，從主要 SSD 層刪除檔案不會建立任何可用空間，因為新建立的快照也會參考所有資料。您必須[刪除快照](#)，才能釋放儲存體，以建立或更新任何檔案。

您可以使用 NetApp ONTAP CLI 修改磁碟區上的快照預留數量。如需詳細資訊，請參閱[更新磁碟區的快照保留](#)。

## 使用自治勒索軟體保護來保護您的資料

自治勒索軟體防護 (ARP) 是一種 NetApp ONTAP AI 驅動的功能，可在 Windows 或 Linux 用戶端遭到入侵時，監控和保護您的資料免受勒索軟體和惡意軟體攻擊。使用機器學習時，ARP 會熟悉 FSx for ONTAP 檔案系統，以主動偵測異常活動。ARP 適用於所有可用 Amazon FSx for NetApp ONTAP AWS 區域的所有新的和現有的 FSx for ONTAP 檔案系統。

### ARP 的運作方式

您可以使用 CLI 或 REST API，以每個磁碟區為基礎或在 SVM ONTAP 中的所有新磁碟區上預設啟用 ARP。如需啟用 ARP 的詳細資訊，請參閱[啟用自治勒索軟體保護](#)。

ARP 以兩種模式運作：學習和作用中。當您第一次為 FSx for ONTAP 磁碟區啟用 ARP 時，它會在學習模式中執行。在學習模式中，ARP 會分析工作負載存取模式。會根據您磁碟區的工作負載 ONTAP 自動決定最佳的學習期間，這最多可能需要 30 天。完成後，ARP 會轉換為作用中模式。在作用中模式中，ARP 會監控磁碟區上的傳入資料和活動，以識別潛在的勒索軟體和惡意軟體攻擊。如需詳細資訊，請參閱[ARP 所尋找的內容](#)。如果 ARP 偵測到任何異常活動，會自動建立 ONTAP 快照，協助您盡可能在接近潛在攻擊時復原資料。快照的字首為 Anti\_ransomware\_backup，因此很容易識別。如果判斷攻擊機率為中等，ONTAP 將產生事件管理系統 (EMS) 訊息供您檢閱。如需詳細資訊，請參閱[如何使用 ARP 回應可疑的攻擊及了解 EMS 警示以進行自治勒索軟體防護](#)。

ARP 的效能額外負荷對於大多數工作負載來說都很小。如果您的磁碟區具有讀取密集型工作負載，NetApp 建議為每個檔案系統保護不超過 150 個這類磁碟區。如果您超過此數字，該工作負載的 IOPS 可能會下降高達 4%。如果您的磁碟區具有寫入密集型工作負載，NetApp 建議為每個檔案系統保護不超過 60 個這類磁碟區。否則，該工作負載的 IOPS 可能會下降高達 10%。如需有關效能的詳細資訊，請參閱[Amazon FSx for NetApp ONTAP 效能](#)。

在您的 FSx for ONTAP 檔案系統上啟用 ARP 無需額外費用。

## ARP 所尋找的內容

ARP 會尋找 Windows 或 Linux 用戶端遭到入侵的跡象。一旦 ARP 了解您的 FSx for ONTAP 磁碟區並切換到作用中模式，它會在磁碟區上尋找下列類型的活動：

- 熵變更，這表示檔案中資料隨機性的差異。
- 副檔名類型的變更，這表示新的副檔名與常用的副檔名類型不一致。預設值為 20 個檔案，其中包含磁碟區中先前未觀察到的副檔名。
- 檔案 IOPS 的變更，這表示具有加密資料的異常磁碟區活動激增。

您可以視需要修改磁碟區的勒索軟體偵測參數。例如，如果您的磁碟區託管許多類型的副檔名。如需詳細資訊，請參閱 NetApp 文件中心中的[管理 ONTAP 自治勒索軟體防護攻擊偵測參數](#)。

### Note

ARP 不會阻止具有登入資料之惡意管理員存取 FSx for ONTAP 檔案系統。AWS 建議採用分層安全方法 AWS Backup，包括ONTAP快照和 SnapLock。

## 如何使用 ARP 回應可疑的攻擊

如果 ARP 偵測到攻擊，則會產生快照，做為復原點。快照已鎖定，無法透過正常方式刪除。根據攻擊的嚴重性，它也會產生 EMS 警示，顯示受影響的磁碟區、攻擊機率和攻擊時間表。如果您想要接收建立新快照或觀察磁碟區上新副檔名的提醒，您可以設定 ARP 傳送這些提醒。如需詳細資訊，請參閱 NetApp 文件中心中的[設定 ARP 警示](#)。

您可以產生報告來檢視可疑攻擊的詳細資訊。檢閱報告後，您可以判斷ONTAP警示是由誤報或可疑攻擊產生。如果您將警示標記為可疑攻擊，您應該判斷攻擊範圍，然後從 ARP 建立的快照復原資料。如果您將攻擊標記為誤判，則會自動刪除 ARP 建立的快照。如需詳細資訊，請參閱[回應自治勒索軟體防護警示](#)。

建議您在 CLI 和 REST API ONTAP 中監控檔案系統的 EMS 訊息，以及磁碟區的狀態。如需 ARP 的 EMS 訊息詳細資訊，請參閱 [了解 EMS 警示以進行自治勒索軟體防護](#)。

### 主題

- [啟用自治勒索軟體保護](#)
- [回應自治勒索軟體防護警示](#)



- [了解 EMS 警示以進行自治勒索軟體防護](#)

## 啟用自治勒索軟體保護

下列程序說明如何使用 ONTAP CLI 在學習模式和作用中模式中啟用自治勒索軟體防護 (ARP)，以及如何驗證 ARP 已啟用。如需 ARP 的詳細資訊，請參閱 [ARP 的運作方式](#)。

在學習模式中啟用 ARP

使用 ONTAPCLI 在現有磁碟區上以學習模式啟用 ARP

- 執行下列命令。將 *vol\_name* 和 *svm\_name* 取代為您自己的資訊。

```
security anti-ransomware volume dry-run -volume vol_name -vserver svm_name
```

如需此命令的詳細資訊，請參閱 NetApp 文件中心的 [security anti-ransomware volume dry-run](#)。

### Note

學習模式僅適用於新寫入的資料。不會掃描或分析現有資料。一般資料流量行為是根據在磁碟區上啟用 ARP 後寫入的新資料來決定。

使用 CLI 在新磁碟區上啟用學習模式中ONTAP的 ARP

- 執行下列命令。將 *vol\_name*、*svm\_name*、*size* 和 */path\_name* 取代為您的資訊。

```
volume create -volume vol_name -vserver svm_name -aggregate aggr_name -size size -  
anti-ransomware-state dry-run -junction-path /path_name
```

如需此命令的詳細資訊，請參閱 NetApp 文件中心的 [volume create](#)。

在作用中模式中啟用 ARP

使用 ONTAPCLI 在現有磁碟區上以作用中模式啟用 ARP

- 執行下列命令。將 *vol\_name* 和 *svm\_name* 取代為您自己的資訊。



```
security anti-ransomware volume enable -volume vol_name -vserver svm_name
```

如需此命令的詳細資訊，請參閱 NetApp 文件中心的 [security anti-ransomware volume enable](#)。

 Note

建議您將磁碟區保持在學習模式中至少 30 天，然後再轉換為作用中模式。ARP 會自動決定最佳的學習期間，並在準備好時從學習模式切換。此程序可能會在 30 天內發生。

根據預設，在 SVM 層級啟用 ARP

使用 CLI 在現有 SVM ONTAP 上預設啟用 ARP

- 執行下列命令。將 *svm\_name* 取代為您自己的資訊。

```
vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run
```

如需此命令的詳細資訊，請參閱 NetApp 文件中心的 [vserver modify](#)。

驗證 ARP 的狀態

使用 CLI 驗證 ARP ONTAP 的狀態

- 執行下列命令。

```
security anti-ransomware volume show
```

如需此命令的詳細資訊，請參閱 NetApp 文件中心的 [security anti-ransomware volume show](#)。

如果您預期工作負載繁重，您可以暫停（然後繼續）ARP。如需詳細資訊，請參閱 NetApp 文件中心的 [暫停 ONTAP 自治勒索軟體保護，以將工作負載事件排除在分析之外](#)。

## 回應自治勒索軟體防護警示

下列程序說明如何使用 ONTAP CLI 來檢視自治勒索軟體防護 (ARP) 警示、產生攻擊報告，以及對報告採取動作。如需 ARP 如何偵測和回應攻擊的詳細資訊，請參閱 [ARP 所尋找的內容](#) 和 [如何使用 ARP 回應可疑的攻擊](#)。

### 檢視 ARP 提醒

#### 使用 CLI 檢視磁碟區的 ARP ONTAP 提醒

- 執行下列命令。將 *svm\_name* 和 *vol\_name* 取代為您自己的資訊。

```
security anti-ransomware volume show -vserver svm_name -volume vol_name
```

執行命令後，您會看到類似下列範例的輸出：

```
Vserver Name: fsx
Volume Name: vol1
State: enabled
Attack Probability: moderate
Attack Timeline: 9/14/2021 01:03:23
Number of Attacks: 1
```

如需此命令的詳細資訊，請參閱 [security anti-ransomware volume show](#) NetApp 文件中心的。

### 產生 ARP 報告

#### 使用 CLI 產生 ARP ONTAP 報告

- 執行下列命令。將 *vol\_name* 和 */file\_location/* 取代為您自己的資訊。產生報告後，您可以在用戶端系統上檢視報告。

```
security anti-ransomware volume attack generate-report -volume vol_name -dest-path /file_location/
```

如需此命令的詳細資訊，請參閱 NetApp 文件中心的 [security anti-ransomware volume attack generate-report](#)。

## 對 ARP 報告採取動作

使用 CLI 對來自 ARP ONTAP 報告的誤判攻擊採取行動

- 執行下列命令。使用您自己的資訊取代 *svm\_name*、*vol\_name* 和 #####。

```
security anti-ransomware volume attack clear-suspect -vserver svm_name -  
volume vol_name [extension identifiers] -false-positive true
```

如需此命令的詳細資訊，請參閱 NetApp 文件中心的 [security anti-ransomware volume attack clear-suspect](#)。

### Note

當您將警示標記為誤判時，它會更新勒索軟體設定檔。這麼做之後，您不會再次收到有關該特定案例的提醒。

使用 CLI 從 ARP ONTAP 報告對潛在攻擊採取動作

- 執行下列命令。使用您自己的資訊取代 *svm\_name*、*vol\_name* 和 #####。

```
security anti-ransomware volume attack clear-suspect -vserver svm_name -  
volume vol_name [extension identifiers] -false-positive false
```

如需此命令的詳細資訊，請參閱 NetApp 文件中心的 [security anti-ransomware volume attack clear-suspect](#)。

## 了解 EMS 警示以進行自治勒索軟體防護

您可以使用 NetApp ONTAP's 事件管理系統 (EMS) 來監控與 ARP 相關的事件，包括潛在的攻擊。如需 ARP 及其偵測攻擊方式的詳細資訊，請參閱 [ARP 的運作方式](#) 和 [ARP 所尋找的內容](#)。

下表包含與 ARP 相關的所有提醒。如需 EMS 的詳細資訊，請參閱 [監控 FSx 的 ONTAP EMS 事件](#)。

| EMS 訊息名稱                                | EMS 訊息描述                                                        |
|-----------------------------------------|-----------------------------------------------------------------|
| <code>arw.analytics.ext.report</code>   | 當反勒索軟體分析產生或更新磁碟區的可疑副檔名報告時，就會發生此訊息。                              |
| <code>arw.analytics.high.entropy</code> | 當高熵性資料日誌訊息的數量（與勒索軟體偵測和分析相關）超過磁碟區的預先定義閾值時，就會發生此訊息。               |
| <code>arw.analytics.probability</code>  | 當磁碟區lowhigh上的反勒索軟體攻擊機率從變更為時，就會發生此訊息。                            |
| <code>arw.analytics.report</code>       | 當產生或更新磁碟區的反勒索軟體分析報告時，就會發生此訊息。                                   |
| <code>arw.analytics.suspects</code>     | 當反勒索軟體分析產生的可疑項目清單成長到需要進一步調查的時間點時，就會發生此訊息。                       |
| <code>arw.auto.switch.enabled</code>    | 當在滿足各種條件後，例如學習期間、檔案建立、檔案寫入和副檔名探索活動，反勒索軟體會自動從學習模式切換到啟用時，就會發生此訊息。 |
| <code>arw.new.file.extn.seen</code>     | 當在啟用反勒索軟體的磁碟區中觀察到新的副檔名時，就會發生此訊息。其目的是及時通知使用者所觀察到的延伸項目，以便及時調查。    |
| <code>arw.snapshot.created</code>       | 在啟用反勒索軟體的磁碟區中建立新的 ARP 快照時，就會發生此訊息。此外，它提供建立快照的原因資訊。              |
| <code>arw.volume.state</code>           | 當磁碟區的反勒索軟體狀態變更時，就會發生此訊息。                                        |
| <code>arw.vserver.state</code>          | 當 SVM 的反勒索軟體狀態變更時，就會發生此訊息。                                      |

# 使用 保護您的資料 SnapLock

SnapLock 是一項功能，可讓您透過將檔案轉換為寫入一次、讀取許多 (WORM) 狀態來保護檔案，以防止在指定的保留期間內修改或刪除。您可以使用 SnapLock 來符合法規合規、保護業務關鍵資料免受勒索軟體攻擊，以及為您的資料提供多一層保護，以防止資料遭到變更或刪除。

Amazon FSx for NetApp ONTAP 支援使用的合規和企業保留模式 SnapLock。如需詳細資訊，請參閱[了解 SnapLock 合規](#)及[了解 SnapLock 企業](#)。

您可以在 2023 年 7 月 13 日當天或之後建立的 FSx for ONTAP 檔案系統上建立磁碟 SnapLock 區。現有的檔案系統將在即將到來的每週維護時段獲得 SnapLock 支援。

## 主題

- [SnapLock 的運作方式](#)
- [了解 SnapLock 合規](#)
- [了解 SnapLock 企業](#)
- [了解 SnapLock 保留期](#)
- [將檔案遞交至 WORM 狀態](#)

## SnapLock 的運作方式

SnapLock 可以防止您的檔案遭到刪除、變更或重新命名，協助您達成法規和管控目的。建立 SnapLock 磁碟區時，您會遞交檔案寫入一次、讀取許多 (WORM) 儲存，並設定資料的保留期間。您的檔案可以存放於指定期間內不可清除、不可寫入的狀態，或無限期儲存。

### Important

您必須指定磁碟區在建立時是否將使用 SnapLock 設定。非 SnapLock 磁碟區無法在建立後轉換為 SnapLock 磁碟區。

## 保留模式

SnapLock 有兩種保留模式：合規和企業。Amazon FSx for NetApp ONTAP 支援這兩種功能。它們有不同的使用案例，而其中一些功能不同，但它們都使用 WORM 模型保護您的資料免於修改或刪除。下表說明這些保留模式之間的一些相似性和差異。

| SnapLock 功能                             | <a href="#">了解SnapLock合規</a>                                                                                                       | <a href="#">了解SnapLock企業</a>                                                                       |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| 描述                                      | 在合規磁碟區上轉換至 WORM 的檔案在保留期間到期之前，都無法刪除。                                                                                                | 企業磁碟區上轉換至 WORM 的檔案，可在其保留期間過期之前，由授權使用者使用特殊權限刪除來刪除。                                                  |
| 使用案例                                    | <ul style="list-style-type: none"> <li>解決政府或產業特定的要求，例如 SEC 規則 17a-4(f)、FINRA 規則 4511 和 CFTC 規則 1.31。</li> <li>防範勒索軟體攻擊。</li> </ul> | <ul style="list-style-type: none"> <li>提升組織的資料完整性和內部合規。</li> <li>在使用SnapLock合規之前測試保留設定。</li> </ul> |
| <a href="#">自動遞交</a>                    | 是                                                                                                                                  | 是                                                                                                  |
| <a href="#">事件型保留 (EBR)<sup>1</sup></a> | 是                                                                                                                                  | 是                                                                                                  |
| <a href="#">法務保存<sup>1</sup></a>        | 是                                                                                                                                  | 否                                                                                                  |
| <a href="#">使用特殊權限刪除</a>                | 否                                                                                                                                  | 是                                                                                                  |
| <a href="#">磁碟區附加模式</a>                 | 是                                                                                                                                  | 是                                                                                                  |
| <a href="#">SnapLock 稽核日誌磁碟區</a>        | 是                                                                                                                                  | 是                                                                                                  |

**Note**

CLI 和 REST API 支援 ONTAP <sup>1</sup>EBR 和法務保存操作。

**Note**

FSx for ONTAP 支援將資料分層至所有SnapLock磁碟區的容量集區，無論SnapLock類型為何。如需詳細資訊，請參閱[磁碟區資料分層](#)。

## SnapLock 管理員

您必須具有SnapLock管理員權限才能對SnapLock磁碟區執行特定動作。SnapLock管理員權限是在CLI ONTAP 中vsadmin-snaplock的角色中定義的。您必須是叢集管理員，才能使用管理員角色建立儲存虛擬機器 (SVM) SnapLock管理員帳戶。

您可以使用 CLI ONTAP 中的 vsadmin-snaplock角色執行下列動作：

- 管理您自己的使用者帳戶、本機密碼和金鑰資訊
- 管理磁碟區，移動磁碟區除外
- 管理配額、qtrees、快照複本和檔案
- 執行SnapLock動作，包括特殊權限刪除和法務保存
- 設定網路檔案系統 (NFS) 和伺服器訊息區塊 (SMB) 通訊協定
- 設定網域名稱系統 (DNS)、輕量型目錄存取通訊協定 (LDAP) 和網路資訊服務 (NIS) 服務
- 監控作業

下列程序詳細說明如何在 CLI ONTAP 中建立SnapLock管理員。您必須以安全連線的叢集管理員身分登入，例如 Secure Shell Protocol (SSH)，才能執行此任務。

在 CLI 中使用 vsadmin-snaplock 角色建立 SVM ONTAP 管理員帳戶

- 執行下列命令。將 *SVM\_name* 和 *SnapLockAdmin* 取代為您自己的資訊。

```
cluster1:> security login create -vserver SVM_name -user-or-group-  
name SnapLockAdmin -application ssh -authentication-method password -role vsadmin-  
snaplock
```

如需詳細資訊，請參閱[ONTAP 角色和使用者](#)。

## SnapLock 稽核日誌磁碟區

SnapLock 稽核日誌磁碟區包含SnapLock稽核日誌，其中包含事件的時間戳記，例如建立SnapLock管理員的時間、執行特殊權限刪除操作的時間，或將法務保存置於檔案的時間。SnapLock 稽核日誌磁碟區是不可清除的事件記錄。

您必須在與下列動作的磁碟區相同的 SVM 中建立SnapLock稽核日誌SnapLock磁碟區：

- 在SnapLock企業磁碟區上開啟或關閉特殊權限刪除。

- 對SnapLock合規磁碟區中的檔案套用法務保存。

#### Warning

- SnapLock 稽核日誌磁碟區的最短保留期間為六個月。在此保留期間到期之前，即使磁碟區是在SnapLock企業模式下建立，也無法刪除與其相關聯的SnapLock稽核日誌磁碟區和 SVM 和檔案系統。
- 如果使用特殊權限刪除來刪除檔案，且其保留期間超過磁碟區的保留期間，則稽核日誌磁碟區會繼承檔案的保留期間。例如，如果使用特殊權限刪除來刪除保留期間為 10 個月的檔案，且稽核日誌磁碟區的保留期間為六個月，則稽核日誌磁碟區的保留期間會延長至 10 個月。

SVM 中只能有一個作用中的SnapLock稽核日誌磁碟區，但 SVM 中的多個SnapLock磁碟區可以共用。若要成功掛載SnapLock稽核日誌磁碟區，請將連接路徑設定為 `/snaplock_audit_log`。沒有其他磁碟區可以使用此連接路徑，包括非稽核日誌磁碟區的磁碟區。

您可以在SnapLock稽核日誌磁碟區的根`/snaplock_log`目錄下找到稽核日誌。特殊權限刪除操作會記錄在 `privdel_log` 子目錄中。法務保存開始和結束操作會記錄在 `/snaplock_log/legal_hold_logs/`。所有其他日誌都存放在 `system_log`子目錄中。

您可以使用 Amazon FSx 主控台、AWS CLI、Amazon FSx API 以及 CLI 和 REST API ONTAP 建立 SnapLock稽核日誌磁碟區。

#### Note

資料保護 (DP) 磁碟區無法用作SnapLock稽核日誌磁碟區。

若要使用 Amazon FSx API 開啟SnapLock稽核日誌磁碟區，請在 `AuditLogVolume`中使用 [CreateSnaplockConfiguration](#)。在 Amazon FSx 主控台的稽核日誌磁碟區中，選擇已啟用。確定 Junction 路徑設定為 `/snaplock_audit_log`。

## 存取SnapLock磁碟區中的資料

您可以使用 NFS 和 SMB 等開啟的檔案通訊協定來存取SnapLock磁碟區中的資料。將資料寫入 SnapLock磁碟區或讀取受 WORM 保護的資料不會影響效能。



您可以使用 NFS 和 SMB 跨SnapLock磁碟區複製檔案，但它們不會將其 WORM 屬性保留在目的地 SnapLock磁碟區上。您必須將複製的檔案重新遞交給 WORM，以防止它們遭到修改或刪除。如需詳細資訊，請參閱[將檔案遞交至 WORM 狀態](#)。

您也可以使用 複寫SnapLock資料SnapMirror，但來源和目的地磁碟區必須是具有相同保留模式的 SnapLock磁碟區（例如，兩者都必須是合規或企業）。

## 了解SnapLock合規

本節說明SnapLock合規保留模式的使用案例和考量事項。

您可以針對下列使用案例選擇合規保留模式。

- 您可以使用SnapLock合規來處理政府或產業特定的命令，例如 SEC 規則 17a-4(f)、FINRA 規則 4511 和 CFTC 規則 1.31。SnapLockAmazon FSx for NetApp ONTAP 的合規性已由 評估這些命令和法規Cohasset Associates。如需詳細資訊，請參閱 [Amazon FSx for NetApp ONTAP 的合規評估報告](#)。
- 您可以使用SnapLock合規來補充或增強全面的資料保護策略，以對抗勒索軟體攻擊。

以下是有關SnapLock合規保留模式的一些重要事項。

- 在檔案轉換為寫入一次後，讀取SnapLock合規磁碟區的許多 (WORM) 狀態後，任何使用者都無法在其保留期間到期之前將其刪除。
- 只有在磁碟區上所有 WORM 檔案的保留期間已過期，而且已從磁碟區中刪除 WORM 檔案時，才能刪除SnapLock合規磁碟區。
- 您無法在建立之後重新命名SnapLock合規磁碟區。
- 您可以使用 SnapMirror 複寫 WORM 檔案，但來源磁碟區和目的地磁碟區必須具有相同的保留模式（例如，兩者都必須是合規）。
- SnapLock 合規磁碟區無法轉換為SnapLock企業磁碟區，反之亦然。

## 了解SnapLock企業

本節說明SnapLock企業保留模式的使用案例和考量事項。

您可以為下列使用案例選擇SnapLock企業保留模式。

- 您可以使用 SnapLock Enterprise 僅授權特定使用者刪除檔案。

- 您可以使用 SnapLock Enterprise 來提升組織的資料完整性和內部合規。
- 您可以使用 SnapLock Enterprise 來測試保留設定，然後再使用 SnapLock Compliance。

以下是有關SnapLock企業保留模式的一些重要事項。

- 您可以使用 SnapMirror複寫 WORM 檔案，但來源磁碟區和目的地磁碟區必須具有相同的保留模式（例如，兩者都必須是 Enterprise）。
- 磁碟SnapLock區無法從 Enterprise 轉換為 Compliance，或從 Compliance 轉換為 Enterprise。
- SnapLock 企業不支援法務保存。

## 使用特殊權限刪除

SnapLock 企業與SnapLock合規之間的其中一個主要差異是，SnapLock管理員可以在SnapLock企業磁碟區上開啟特權刪除，以便在檔案的保留期間到期之前刪除檔案。SnapLock 管理員是唯一可以刪除具有作用中保留政策之SnapLock企業磁碟區中的檔案的使用者。如需詳細資訊，請參閱[SnapLock 管理員](#)。

您可以使用 Amazon FSx 主控台、AWS CLI、Amazon FSx API 以及 CLI 和 REST API ONTAP 來開啟或關閉特殊權限刪除。若要開啟特殊權限刪除，您必須先在與磁碟區相同的 SVM 中建立SnapLock 稽核日誌SnapLock磁碟區。如需詳細資訊，請參閱[SnapLock 稽核日誌磁碟區](#)。

若要使用 Amazon FSx API 開啟特權刪除，請在 PrivilegedDelete中使用 [CreateSnaplockConfiguration](#)。在 Amazon FSx 主控台中，針對特殊權限刪除，選擇已啟用。

### Note

您無法發出特殊權限刪除命令來刪除一次寫入，請讀取許多具有過期保留期的 (WORM) 檔案。您可以在保留期間到期後發出正常刪除操作。

您可以選擇永久關閉特殊權限刪除，但此動作無法復原。如果永久關閉特殊權限刪除，則您不需要有與 SnapLock企業磁碟區相關聯的SnapLock稽核日誌磁碟區。

若要使用 Amazon FSx API 永久關閉特權刪除，請在 PrivilegedDelete中使用 [CreateSnaplockConfiguration](#)。在 Amazon FSx 主控台中，針對特殊權限刪除，選擇永久停用。

## 繞過SnapLock企業模式

如果您使用的是 Amazon FSx 主控台或 Amazon FSx API，您必須擁有 IAM `fsx:BypassSnapLockEnterpriseRetention` 許可，才能刪除包含具有作用中保留政策之 WORM 檔案 SnapLock 的企業磁碟區。

如需詳細資訊，請參閱[刪除 SnapLock 磁碟區](#)。

## 了解 SnapLock 保留期

建立 SnapLock 磁碟區時，您可以設定磁碟區的預設保留期間，也可以設定一次寫入的保留期間，明確讀取許多 (WORM) 檔案。在保留期間，您無法刪除或修改受 WORM 保護的檔案。保留期間用於計算保留時間。例如，如果您在 2023 年 7 月 14 日午夜將檔案轉移至 WORM，並將保留期間設定為 5 年，則保留時間將是 2028 年 7 月 14 日午夜。

如需 WORM 的詳細資訊，請參閱[將檔案遞交至 WORM 狀態](#)。

## 保留期政策

保留期取決於您指派給下列參數的值：

- 預設保留 – 如果您未提供 WORM 檔案的明確保留期，則會指派給該檔案的預設保留期。
- 最短保留期 – 可指派給 WORM 檔案的最短保留期。
- 最長保留期 – 可指派給 WORM 檔案的最長保留期。

### Note

即使保留期間過期，您也無法修改 WORM 檔案。您只能將其刪除或設定新的保留期，以再次開啟 WORM 保護。

您可以使用數個不同的時間單位來指定保留期。下表列出支援的特定範圍。

| Type | Value       | 備註 |
|------|-------------|----|
| 秒鐘   | 0 - 65, 535 |    |
| 分鐘   | 0 - 65, 535 |    |

| Type             | Value   | 備註                                 |
|------------------|---------|------------------------------------|
| 小時               | 0 - 24  |                                    |
| 天                | 0 - 365 |                                    |
| 月                | 0 - 12  |                                    |
| 年                | 0 - 100 |                                    |
| 無限               | -       | 永久保留檔案。<br><br>可用於預設保留、保留上限和保留下限。  |
| 未指定 <sup>1</sup> | -       | 保留檔案，直到您設定保留期間為止。<br><br>僅適用於預設保留。 |

#### Note

<sup>1</sup>當您將檔案轉換為具有未指定保留期的 WORM 時，它們會獲得為 SnapLock 磁碟區設定的最短保留期。當您將受 WORM 保護的檔案轉換為絕對保留時間時，新的保留期間必須大於您先前在檔案上設定的最短期間。

## 過期的保留期間

在 WORM 檔案的保留期到期後，您可以刪除檔案或設定新的保留期以重新開啟 WORM 保護。WORM 檔案的保留期間過期後，就不會自動刪除。您仍然無法修改 WORM 檔案的內容，即使其保留期間已過期。

## 設定 SnapLock 磁碟區的保留期間

您可以使用 Amazon FSx 主控台、AWS CLI、Amazon FSx API 以及 CLI 和 REST API ONTAP 來設定 SnapLock 磁碟區的保留期間。

若要使用 Amazon FSx API 設定保留期，請使用 [SnaplockRetentionPeriod](#) 組態。在 Amazon FSx 主控台的保留期間，輸入預設保留、最短保留和最長保留的值。然後為每個單位選擇對應的單位。

## 將檔案遞交至 WORM 狀態

本節討論如何將檔案轉換為一次寫入、讀取許多 (WORM) 狀態。它還討論了磁碟區附加模式，這是一種將資料增量寫入 WORM 保護檔案的方式。

### 自動遞交

如果檔案在您指定的期間內未修改，您可以使用自動遞交將檔案轉換為 WORM。您可以使用 Amazon FSx 主控台、AWS CLI、Amazon FSx API 以及 CLI 和 REST API ONTAP 開啟自動遞交。

您可以指定介於五分鐘到 10 年的自動遞交期間。下表列出支援的特定範圍。

| 單位 | Value        |
|----|--------------|
| 分鐘 | 5 - 65 , 535 |
| 小時 | 1 - 65 , 535 |
| 天  | 1 - 3 , 650  |
| 月  | 1 - 120      |
| 年  | 1 - 10       |

若要使用 Amazon FSx API 開啟自動遞交，請在 `AutocommitPeriod` 中使用 [CreateSnaplockConfiguration](#)。在 Amazon FSx 主控台中，針對自動遞交，選擇已啟用。然後，在自動遞交期間輸入值，然後選擇對應的自動遞交單位。

您可以指定介於 5 分鐘到 10 年之間的值。

### 磁碟區附加模式

您無法修改 WORM 保護檔案中的現有資料。不過，SnapLock 可讓您使用 WORM 可附加檔案來維護現有資料的保護。例如，您可以產生日誌檔案或保留音訊或影片串流資料，同時遞增寫入資料。您可以使用 Amazon FSx 主控台、AWS CLI、Amazon FSx API 以及 ONTAP CLI 和 REST API 來開啟或關閉磁碟區附加模式。

## 更新磁碟區附加模式的需求

- 必須卸載磁碟SnapLock區。
- SnapLock 磁碟區必須清空快照複本和使用者資料。

若要使用 Amazon FSx API 開啟磁碟區附加模式，請在 VolumeAppendModeEnabled中使用 [CreateSnaplockConfiguration](#)。在 Amazon FSx 主控台中，針對磁碟區附加模式，選擇已啟用。

## 事件型保留 (EBR)

您可以使用事件型保留 (EBR) 來建立具有相關聯保留期的自訂政策。例如，您可以將指定路徑中的所有檔案轉換為 WORM，並使用 `snaplock event-retention policy create` 和 `snaplock event-retention apply` 命令設定一年的保留期。使用 EBR 時，您必須指定磁碟區、目錄或檔案。您在建立 EBR 政策時選取的保留期會套用至指定路徑中的所有檔案。

CLI 和 REST API ONTAP 支援 EBR。

### Note

ONTAP 不支援具有 FlexGroup 磁碟區的 EBR。

下列程序說明如何建立、套用、修改和刪除 EBR 政策。您必須是 SnapLock 管理員（具有 `vsadmin-snaplock` 角色），才能在 CLI ONTAP 中完成這些任務。如需詳細資訊，請參閱 [SnapLock 管理員](#)。

在 CLI 中建立 EBR ONTAP 政策

在 CLI 中建立 EBR ONTAP 政策

- 執行下列命令。將 *p1* 和 *"10 #"* 取代為您自己的資訊。

```
vs1::> snaplock event-retention policy create -name p1 -retention-period "10 years"
```

## 在 CLI 中套用 EBR ONTAP 政策

### 在 CLI 中套用 EBR ONTAP 政策

- 執行下列命令。將 *p1* 和 *slc* 取代為您自己的資訊。如果您想要指定 EBR 政策的特定路徑，您可以在正斜線 (/) 之後新增路徑。否則，此命令會將 EBR 政策套用至磁碟區上的所有檔案。

```
vs1::> snaplock event-retention apply -policy-name p1 -volume slc -path /
```

### 在 CLI 中修改 EBR ONTAP 政策

### 在 CLI 中修改 EBR ONTAP 政策

- 執行下列命令。使用您自己的資訊取代 *p1* 和 "5 #".

```
vs1::> snaplock event-retention policy modify -name p1 -retention-period "5 years"
```

### 在 CLI 中刪除 EBR ONTAP 政策

### 在 CLI 中刪除 EBR ONTAP 政策

- 執行下列命令。將 *p1* 取代為您自己的資訊。

```
vs1::> snaplock event-retention policy delete -name p1
```

NetApp 文件中心的相關命令：

- [snaplock 事件保留中止](#)
- [snaplock event-retention show-vservers](#)
- [snaplock 事件保留顯示](#)
- [snaplock 事件保留政策顯示](#)

## 法務保存

您可以使用法務保存將 WORM 檔案無限期保留。法務保存通常用於訴訟目的。在解除法務保存之前，無法刪除受法務保存約束的 WORM 檔案。

CLI 和 REST API ONTAP 支援法務保存。

 Note

ONTAP 不支援使用 FlexGroup 磁碟區進行法務保存。

下列程序說明如何開始和結束法務保存。您必須是 SnapLock 管理員（具有 vsadmin-snaplock 角色），才能在 CLI ONTAP 中完成這些任務。如需詳細資訊，請參閱 [SnapLock 管理員](#)。

使用 ONTAPCLI 啟動 SnapLock 合規磁碟區中檔案的法務保存

使用 ONTAPCLI 啟動 SnapLock 合規磁碟區中檔案的法務保存

- 執行下列命令。使用您自己的資訊取代 # 取代並取代並排 1、*slc\_vol1* 和 *file1*。

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -  
path /file1
```

使用 ONTAPCLI 啟動 SnapLock 合規磁碟區中所有檔案的法務保存

使用 ONTAPCLI 啟動 SnapLock 合規磁碟區中所有檔案的法務保存

- 執行下列命令。使用您自己的資訊取代 # 取代並取代的 1 和 *slc\_vol1*。

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -  
path /
```

使用 ONTAPCLI 結束 SnapLock 合規磁碟區中檔案的法務保存

使用 ONTAPCLI 結束 SnapLock 合規磁碟區中檔案的法務保存

- 執行下列命令。使用您自己的資訊取代 # 取代並取代並排 1、*slc\_vol1* 和 *file1*。

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -  
path /file1
```



**Note**

建議您在發出法務保存時-operation-status，使用 `snaplock legal-hold show` 命令監控，以確保它不會失敗。

使用 ONTAPCLI 結束 SnapLock 合規磁碟區中所有檔案的法務保存

使用 ONTAPCLI 結束 SnapLock 合規磁碟區中所有檔案的法務保存

- 執行下列命令。使用您自己的資訊取代 # 取代並取代的 1 和 `slc_vol1`。

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -  
path /
```

**Note**

建議您在發出法務保存時-operation-status，使用 `snaplock legal-hold show` 命令監控，以確保它不會失敗。

NetApp 文件中心的相關命令：

- [snaplock 法務保存中止](#)
- [snaplock 法務保存傾印檔案](#)
- [snaplock 法務保存傾印訴訟](#)
- [snaplock legal-hold show](#)

## 使用 複寫您的資料 FlexCache

FlexCache 是 NetApp ONTAP's 遠端快取功能，可讓資料集更接近用戶端，進而改善存取效能並降低成本。它可簡化檔案分佈並降低 WAN 成本。當您建立 FlexCache 磁碟區時，最初只會從原始檔案系統複製中繼資料。這種方法比完整資料複本更快且更節省空間，只耗用一小部分的儲存容量。

## FlexCache 的運作方式

FlexCache 磁碟區是稀疏填入的快取，可讓您存取儲存在原始磁碟區中的資料。快取可以位於不同的、選擇性的遠端檔案系統中。不會從原始伺服器磁碟區複製所有資料，只會視需要 FlexCache 複製資料。FlexCache 磁碟區最適合不常變更資料的讀取密集型工作流程，因為原始伺服器資料的任何變更都需要重新整理快取。

您可以在下列組態中使用 FlexCache 搭配 FSx for ONTAP：

| 原始磁碟區             | FlexCache volume  |
|-------------------|-------------------|
| 內部部署 NetApp ONTAP | FSx for OnTAP     |
| FSx for OnTAP     | 內部部署 NetApp ONTAP |
| FSx for OnTAP     | FSx for OnTAP     |

## FlexCache 寫入模式

FlexCache 磁碟區支援兩種寫入操作的操作模式：全寫模式和回寫模式。

在預設模式中，寫入會從快取轉送到原始磁碟區。在資料遞交至原始磁碟區的儲存體，且原始伺服器確認寫入回快取之前，不會向用戶端確認寫入操作。由於每次寫入都必須周遊快取和原始伺服器之間的網路，因此此模式的延遲比回寫模式高。

在 9.15.1 ONTAP 中推出的回寫模式中，寫入會遞交至快取位置的儲存體，並立即確認給用戶端。然後，資料會以非同步方式寫入原始磁碟區。此模式可讓寫入以接近本機的速度執行，進而大幅改善分散式工作負載的效能。

針對需要低延遲快取寫入的大量寫入工作負載，使用回寫模式。針對對延遲不敏感的讀取密集型工作負載，或當您的原始檔案系統有超過 10 個 FlexCache 原始磁碟區時，請使用全寫式模式。

## FlexCache 磁碟區建立概觀

建立 FlexCache 磁碟區包含下列步驟：

- 收集來源和目的地邏輯界面 (LIFs)
- 在原始伺服器和快取檔案系統之間建立叢集對等互連
- 建立儲存虛擬機器 (SVM) 互連關係

- 建立FlexCache磁碟區並選取寫入模式
- 將FlexCache磁碟區掛載到您的用戶端

如需詳細說明，請參閱 [建立FlexCache](#)。

## 建立FlexCache

使用下列程序，您將在 Amazon FSx for NetApp ONTAP 檔案系統上建立FlexCache磁碟區，該磁碟區由內部部署NetApp ONTAP叢集中的原始磁碟區提供支援。

### 使用 ONTAP CLI

您將使用 ONTAP CLI 在 FSx for ONTAP 檔案系統上建立和管理FlexCache組態。

這些程序中的命令會針對叢集、SVM 和磁碟區 使用以下別名：

- Cache\_ID – 快取叢集的 ID（格式為 FSxIdabcdef1234567890a）
- Origin\_ID – 原始叢集的 ID
- CacheSVM – 快取 SVM 名稱
- OriginSVM – 原始伺服器 SVM 名稱
- OriginVol – 原始磁碟區名稱
- CacheVol – FlexCache磁碟區名稱

本節中的程序使用以下 CLI NetApp ONTAP 命令。

- [network interfaces show](#)
- [cluster peer](#) 命令
- [volume flexcache create](#)

### 先決條件

在您開始使用下列各節中的程序之前，請確定您符合下列先決條件：

- 來源和目的地檔案系統是在相同的 VPC 中連接，或在使用 Amazon VPC AWS Transit Gateway AWS Direct Connect、或對等的網路中連接 AWS VPN。如需詳細資訊，請參閱《Amazon VPC 對等互連指南》中的 [從內存取資料 AWS 雲端](#)和什麼是 VPC 對等互連？。 <https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>

- FSx for ONTAP 檔案系統的 VPC 安全群組具有傳入和傳出規則，允許 ICMP 以及連接埠 11104 和 11105 上的 TCP 用於叢集間端點 (LIFs)。
- 您已使用 SVM 建立 ONTAP 檔案系統的目的地 FSx，但尚未建立將用作 FlexCache 的磁碟區。如需詳細資訊，請參閱[建立檔案系統](#)。

## 記錄來源和目的地叢集間 LIFs

1. 對於做為目的地叢集的 FSx for ONTAP 檔案系統：
  - a. 開啟位於 <https://console.aws.amazon.com/fsx/> 的 Amazon FSx 主控台。
  - b. 選擇檔案系統，然後選擇目的地叢集 ONTAP 檔案系統的 FSx，以開啟檔案系統詳細資訊頁面。
  - c. 在管理中，尋找叢集間端點 - IP 地址，並記錄值。

### Note

對於橫向擴展檔案系統，每個高可用性 (HA) 對有兩個叢集間端點 IP 地址。

2. 對於內部部署來源叢集，請使用下列 CLI 命令擷取叢集間 LIF IP ONTAP 地址：

```
Origin::> network interface show -role intercluster
Logical                               Network
Vserver      Interface  Status    Address/Mask
-----
OriginSVM
              inter_1    up/up     10.0.0.36/24
              inter_2    up/up     10.0.1.69/24
```

3. 儲存 inter\_1 和 inter\_2 IP 地址。別名做為 OriginSVM origin\_inter\_1 和 origin\_inter\_2 參考，別名做為 CacheSVM cache\_inter\_1 和 參考 cache\_inter\_2。

## 在原始伺服器和快取之間建立叢集對等互連

使用 CLI [cluster peer create](#) ONTAP 命令在 Cache 和叢集上建立 Source 叢集對等關係。您將提供先前在[記錄來源和目的地叢集間 LIFs](#) 程序中儲存的叢集間 IP 地址。出現提示時，系統會要求您建立 *cluster-peer-passphrase* 在 Origin 叢集上建立叢集對等互連時需要輸入的。

1. 在叢集上設定 Cache 叢集對等互連（您的 FSx for ONTAP 檔案系統）。

- a. 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。*management\_endpoint\_ip* 將取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

- b. 使用下列命令，並記錄您建立的密碼。對於橫向擴展檔案系統，請提供每個 HA 對的 *inter\_1* 和 *inter\_2* IP 地址。

```
FSx-Cache::> cluster peer create -address-family ipv4 -peer-  
addrs origin_inter_1,origin_inter_2
```

Enter the passphrase: *cluster-peer-passphrase*

Confirm the passphrase: *cluster-peer-passphrase*

Notice: Now use the same passphrase in the "cluster peer create" command in the other cluster.

2. 使用下列命令在 *source* (內部部署) 叢集上設定叢集對等互連。您需要輸入在上一個步驟中建立的密碼短語，才能進行身分驗證。對於橫向擴展檔案系統，您需要為每個 HA 對提供叢集間 IP 地址。

```
Origin::> cluster peer create -address-family ipv4 -peer-  
addrs cache_inter_1,cache_inter_2
```

Enter the passphrase: *cluster-peer-passphrase*

Confirm the passphrase: *cluster-peer-passphrase*

3. 在 *source* 叢集上，使用下列命令，確認叢集對等互連已成功設定。在輸出中，Availability 應該設定為 Available。

```
Origin::> cluster peer show
```

| Peer Cluster Name | Availability | Authentication |
|-------------------|--------------|----------------|
| -----             | -----        | -----          |
| Cache_ID          | Available    | ok             |

如果輸出未顯示 Available，請在 *source* 和 *cache* 叢集上重複上述步驟。

## 設定儲存虛擬機器 (SVM) 對等互連

成功建立叢集對等互連之後，下一個步驟是使用 `vserver peer` 命令在快取叢集（快取）上建立 SVM 對等互連關係。下列程序中使用的其他別名如下：

- *CacheLocalName* – 在 cache SVM 上設定 SVM 對等互連時用來識別 origin SVM 的名稱。
- *OriginLocalName* – 在 origin SVM 上設定 SVM 對等互連時用來識別 cache SVM 的名稱。

1. 在 cache SVM 上，使用下列命令來建立 SVM 互連關係。

```
FSx-Cache::> vserver peer create -vserver CacheSVM -peer-vserver OriginSVM -peer-cluster Origin_ID -local-name OriginLocalName -application flexcache
```

2. 在來源叢集上，使用下列命令來接受 SVM 對等互連關係。

```
Origin::> vserver peer accept -vserver OriginSVM -peer-vserver CacheSVM -local-name CacheLocalName
```

3. 在來源叢集上，接受對等關係。

```
Origin::> vserver peer accept -vserver OriginSVM -peer-vserver CacheSVM -local-name CacheLocalName
```

4. 使用以下命令驗證 SVM 對等互連是否成功；Peer State 應在回應 `peered` 中將 設定為 。

```
Origin::> vserver peer show
```

| Vserver   | Peer Vserver | Peer State | Peering Cluster | Remote Applications |
|-----------|--------------|------------|-----------------|---------------------|
| OriginSVM | CacheSVM     | peered     | FSx-Cache       | flexcache           |

## 建立磁碟 FlexCache 區

成功建立 SVM 互連關係後，下一步是在快取 SVM 上建立 FlexCache 磁碟區。FlexCache 磁碟區必須是 FlexGroup。您也將為您的 FlexCache 磁碟區選擇操作模式。如需詳細資訊，請參閱 [FlexCache 寫入模式](#)。

1. 在快取叢集上，使用下列 ONTAP CLI 命令來建立您的 FlexCache 磁碟區。此範例會建立名為 *CacheVol* 的 2 TB FlexCache 磁碟區。

- 若要建立全寫 FlexCache 磁碟區，請使用下列命令。

```
FSx-Cache::> volume flexcache create -vserver CacheSVM -size 2t -volume CacheVol
               -origin-volume OriginVol -origin-vserver OriginSVM -junction-path /flexcache -
               aggr-list aggr1
```

- 若要建立回寫 FlexCache 磁碟區，請使用下列命令。

```
FSx-Cache::> volume flexcache create -vserver CacheSVM -size 2t -volume CacheVol
               -origin-volume OriginVol -origin-vserver OriginSVM -junction-path /flexcache -
               aggr-list aggr1 -is-writeback-enabled true
```

#### Note

您可以使用 `volume flexcache config modify -is-writeback-enabled {true|false}` 命令來修改寫入模式。使用此命令之前，請務必使用 `set -privilege advanced` 命令進入 ONTAP CLI 進階模式。

2. 驗證 FlexCache 磁碟區與原始磁碟區 FlexCache 之間的關係。

- 對於全 FlexCache 寫磁碟區，您的輸出看起來會與下列範例類似。

```
FSx-Cache::> volume flexcache show
```

| Vserver  | Volume   | Size  | Origin-Vserver | Origin-Volume | Origin-Cluster |
|----------|----------|-------|----------------|---------------|----------------|
| -----    | -----    | ----- | -----          | -----         | -----          |
| CacheSVM | CacheVol | 2TB   | OriginSVM      | OriginVol     | Origin         |

- 對於回 FlexCache 寫磁碟區，您的輸出看起來會類似下列範例。

```
FSx-Cache::> volume flexcache show
```

| Vserver   | Volume   | Size  | Origin-Vserver | Origin-Volume | Origin-Cluster |
|-----------|----------|-------|----------------|---------------|----------------|
| -----     | -----    | ----- | -----          | -----         | -----          |
| CacheSVM  | CacheVol | 2TB   | OriginSVM      | OriginVol     | Origin         |
| Writeback |          |       |                |               |                |

|          |          |     |           |           |        |
|----------|----------|-----|-----------|-----------|--------|
| CacheSVM | CacheVol | 2TB | OriginSVM | OriginVol | Origin |
| true     |          |     |           |           |        |

## 掛載磁碟FlexCache區

一旦FlexCache磁碟區變成可用，NFSv3, NFSv4 和 SMB 用戶端就可以掛載它。一旦掛載 FlexCache，用戶端就可以存取內部部署原始磁碟區上的整個資料集。

- 若要建立掛載點並掛載 FlexCache，請在用戶端上執行下列命令：

```
$ sudo mkdir -p /fsx/CacheVol
$ sudo mount -t nfs management.fs-01d2f606463087f6d.fsx.us-east-1.amazonaws.com:/
CacheVol /fsx/CacheVol
```

## 使用 複寫您的資料 NetApp SnapMirror

您可以使用 NetApp SnapMirror來排程 FSx for ONTAP 檔案系統的定期複寫往返第二個檔案系統。此功能適用於區域內和跨區域部署。

NetApp SnapMirror 無論您是在 中複寫兩個 Amazon FSx 檔案系統 AWS，還是在內部部署之間複寫，都會以高速複寫資料，因此您可以取得跨ONTAP系統的高可用性和快速資料複寫 AWS。複寫可以每隔 5 分鐘排程一次，但應根據 RPOs（復原點目標）、RTOs（復原時間目標）和效能考量仔細選擇間隔。

當您將資料複寫至NetApp儲存系統並持續更新次要資料時，您的資料會保持最新狀態，並隨時保持可用狀態。不需要外部複寫伺服器。如需使用 NetApp SnapMirror複寫資料的詳細資訊，請參閱 NetApp BlueXP [文件中的了解複寫服務](#)。

除了 CLI 和 REST API 之外，您還可以NetApp SnapMirror使用 Amazon FSx 主控台 AWS CLI、和 Amazon FSx API 建立的資料保護 (DP) NetApp ONTAP 目的地磁碟區。如需使用 Amazon FSx 主控台建立目的地磁碟區的資訊 AWS CLI，請參閱 [建立磁碟區](#)。

您可以使用 NetApp BlueXP或 ONTAP CLI 為您的檔案系統排程複寫。



 Note

SnapMirror 複寫有兩種類型：磁碟區層級 SnapMirror 和 SVM 災難復原 (SVMDR)。FSx for ONTAP 僅支援磁碟區層級 SnapMirror 複寫。StrictSync 不支援 Synchronous SnapMirror，包括。

## 使用 NetApp BlueXP 排程複寫

您可以使用 NetApp BlueXP 在 FSx for ONTAP 檔案系統上設定使用 SnapMirror 的複寫。如需詳細資訊，請參閱 NetApp BlueXP 文件中的在[系統之間複寫資料](#)。

## 使用 ONTAP CLI 排程複寫

您可以使用 ONTAP CLI 來設定排程的磁碟區複寫。如需詳細資訊，請參閱 NetApp ONTAP 文件中心的[管理 SnapMirror 磁碟區複寫](#)。

# AWS FSx for ONTAP 的計費和用量報告

AWS 為 FSx for ONTAP 提供兩種用量報告：

- AWS 帳單報告是您正在使用的所有活動的 AWS 服務 高階檢視，包括適用於 ONTAP 的 FSx。
- AWS 用量報告是特定服務的活動摘要，依小時、天或月彙總。它也包含用量圖表，提供 FSx for ONTAP 用量的圖形表示。

## Note

與其他相同 AWS 服務，FSx for ONTAP 只會向您收取使用費用。如需詳細資訊，請參閱 [Amazon FSx for NetApp ONTAP 定價](#)。

## 檢視 FSx for ONTAP 的 AWS 帳單報告

您可以在 AWS 帳單與成本管理 主控台的帳單頁面上檢視依服務列出的 AWS 用量和費用摘要。

檢視 AWS 帳單報告

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/costmanagement/> 開啟 AWS 帳單與成本管理 主控台。
2. 在導覽窗格中，選擇 Bills (帳單)。
3. 選擇帳單期間（例如，2024 年 8 月）。
4. 若要查看 Amazon FSx 費用，請在依服務收費索引標籤上，在依服務文字篩選欄位中輸入 FSx，然後展開 FSx 以檢視費用 AWS 區域。

FSx for ONTAP 檔案系統的費用會顯示在報告中的 Amazon FSx CreateFileSystem : ONTAP 項目下。

5. 若要下載 CSV 格式的詳細帳單報告，請選擇帳單頁面頂端的全部下載至 CSV。

如需 AWS 帳單的詳細資訊，請參閱 AWS Billing 《使用者指南》中的 [檢視帳單](#)。

帳單報告包含適用於 FSx for ONTAP 檔案系統的下列用量類型：

## First generation FSx for ONTAP file systems

| 收費類型                     | 單位     | 描述                                            |  |
|--------------------------|--------|-----------------------------------------------|--|
| ONTAP 單一可用區 SSD 儲存體      | GB-月   | 在第一代單一可用區域 ONTAP 檔案系統上佈建的 SSD 儲存量             |  |
| ONTAP 多可用區域 SSD 儲存體      | GB-月   | 在適用於 ONTAP 檔案系統的第一代多可用區域 FSx 上佈建的 SSD 儲存量     |  |
| ONTAP 單一可用區輸送量           | MBps-月 | 在適用於 ONTAP 檔案系統的第一代單一可用區域 FSx 上佈建的輸送量容量       |  |
| ONTAP 多可用區域輸送量           | MBps-月 | 在適用於 ONTAP 檔案系統的第一代多可用區域 FSx 上佈建的輸送量容量        |  |
| 佈建的 ONTAP 單一可用區 SSD IOPS | IOPS-月 | 適用於 ONTAP 檔案系統的第一代單一可用區域 FSx 上的佈建 SSD IOPS 數量 |  |
| 佈建的 ONTAP 多可用區域 SSD IOPS | IOPS-月 | 適用於 ONTAP 檔案系統的第一代多可用區域 FSx 上的佈建 SSD IOPS 數量  |  |

## Second generation FSx for ONTAP file systems

| 收費類型                      | 單位   | 描述                                         |  |
|---------------------------|------|--------------------------------------------|--|
| ONTAP Single-AZ-2 SSD 儲存體 | GB-月 | 在適用於 ONTAP 檔案系統的第二代單一可用區域 FSx 上佈建的 SSD 儲存量 |  |

| 收費類型                              | 單位     | 描述                                                    |
|-----------------------------------|--------|-------------------------------------------------------|
| ONTAP Multi-AZ-2 SSD 儲存體          | GB-月   | 在適用於 ONTAP 檔案系統的<br>第二代多可用區域 FSx 上佈<br>建的 SSD 儲存量     |
| ONTAP Single-AZ-2 輸送量             | MBps-月 | 在適用於 ONTAP 檔案系統的<br>第二代單一可用區域 FSx 上<br>佈建的輸送量容量       |
| ONTAP Multi-AZ-2 輸送量              | MBps-月 | 在適用於 ONTAP 檔案系統的<br>第二代多可用區域 FSx 上佈<br>建的輸送量容量        |
| 佈建的 ONTAP Single-AZ-2<br>SSD IOPS | IOPS-月 | 適用於 ONTAP 檔案系統的第<br>二代單一可用區域 FSx 上的<br>佈建 SSD IOPS 數量 |
| 佈建的 ONTAP Multi-AZ-2<br>SSD IOPS  | IOPS-月 | 適用於 ONTAP 檔案系統的第<br>二代多可用區域 FSx 上的佈<br>建 SSD IOPS 數量  |

## All FSx for ONTAP filesystems

| 收費類型                     | 單位   | 描述                                              |
|--------------------------|------|-------------------------------------------------|
| ONTAP 標準容量集區儲存           | GB-月 | FSx for ONTAP 檔案系統使<br>用的容量集區儲存量。               |
| ONTAP 備份儲存               | GB-月 | 用於備份的儲存容量                                       |
| SnapLock 用量              | GB-月 | SnapLock 磁碟區使用的儲存<br>容量                         |
| 讀取 ONTAP 標準容量集區儲<br>存的請求 | 作業   | 對 FSx for ONTAP 檔案系統<br>上的標準容量集區儲存提出的<br>讀取請求數量 |

| 收費類型                  | 單位 | 描述                                      |
|-----------------------|----|-----------------------------------------|
| 將請求寫入 ONTAP 標準容量集區儲存體 | 作業 | 對 FSx for ONTAP 檔案系統上的標準容量集區儲存提出的寫入請求數量 |

## 檢視適用於 ONTAP 的 FSx AWS 用量報告

AWS 提供比帳單報告更詳細的 FSx 用量報告。用量報告會依小時、日或月提供彙總用量資料，並依區域和用量類型列出操作。

### 檢視 AWS 用量報告

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/costmanagement/> 開啟 AWS 帳單與成本管理 主控台。
2. 在導覽窗格中選擇 Cost Explorer。
3. 在報告參數區段下，選擇報告的日期範圍和精細程度。
4. 將群組依據 > 維度設為 Service。
5. 在篩選條件 > 服務下，選擇 FSx
6. 選擇用量類型。如需適用於 ONTAP 用量類型的 FSx 清單，請參閱此程序後的表格。
7. 為您的報告進行任何其他篩選條件選擇。
8. 若要將報告詳細資訊下載至檔案，請選擇下載為 CSV。

下表列出 FSx for ONTAP 用量類型，可用來篩選報告以檢視 ONTAP 檔案系統的用量資料。如需使用 Cost Explorer 的詳細資訊，請參閱 AWS Cost Management 《使用者指南》中的[使用 分析成本和用量 AWS Cost Explorer](#)。

### First generation FSx for ONTAP file systems

| 用量類型                                | 單位   | 描述                                          |
|-------------------------------------|------|---------------------------------------------|
| <i>region</i> -Storage.SAZ_2N : SSD | GB-月 | 在適用於 ONTAP 檔案系統的第一代單一可用區域 FSx 上佈建的 SSD 儲存量。 |

| 用量類型                                     | 單位       | 描述                                                                      |
|------------------------------------------|----------|-------------------------------------------------------------------------|
| <i>region</i> -Storage.MAZ : SSD         | GB-月     | 在適用於 ONTAP 檔案系統的第一代多可用區域 FSx 上佈建的 SSD 儲存量。                              |
| <i>region</i> -ThroughputCapacity.SAZ_2N | MiBps-Mo | 在適用於 ONTAP 檔案系統的第一代單一可用區域 FSx 上佈建的輸送量容量。                                |
| <i>region</i> -ThroughputCapacity.MAZ    | MiBps-Mo | 在適用於 ONTAP 檔案系統的第一代多可用區域 FSx 上佈建的輸送量容量。                                 |
| <i>region</i> -ProvisionedSSDIOPS.SAZ_2N | IOPS-Mo  | 在適用於 ONTAP 檔案系統的第一代單一可用區域 FSx 上，每 GiB SSD 儲存體佈建超過 3 IOPS 的 SSD IOPS 數量。 |
| <i>region</i> -ProvisionedSSDIOPS.MAZ    | IOPS-Mo  | 在適用於 ONTAP 檔案系統的第一代多可用區域 FSx 上，每 GiB SSD 儲存體佈建超過 3 IOPS 的 SSD IOPS 數量。  |

## Second generation FSx for ONTAP file systems

| 用量類型                                 | 單位   | 描述                                          |
|--------------------------------------|------|---------------------------------------------|
| <i>region</i> -Storage.SAZ_2N2 : SSD | GB-月 | 在適用於 ONTAP 檔案系統的第二代單一可用區域 FSx 上佈建的 SSD 儲存量。 |
| <i>region</i> -Storage.MAZ2 : SSD    | GB-月 | 在適用於 ONTAP 檔案系統的第二代多可用區域 FSx 上佈建的 SSD 儲存量。  |

| 用量類型                                      | 單位       | 描述                                                                      |
|-------------------------------------------|----------|-------------------------------------------------------------------------|
| <i>region</i> -ThroughputCapacity.SAZ_2N2 | MiBps-Mo | 在適用於 ONTAP 檔案系統的第二代單一可用區域 FSx 上佈建的輸送量容量。                                |
| <i>region</i> -ThroughputCapacity.MAZ2    | MiBps-Mo | 在適用於 ONTAP 檔案系統的第二代多可用區域 FSx 上佈建的輸送量容量。                                 |
| <i>region</i> -ProvisionedSSDIOPS.SAZ_2N2 | IOPS-Mo  | 在適用於 ONTAP 檔案系統的第二代單一可用區域 FSx 上，每 GiB SSD 儲存體佈建超過 3 IOPS 的 SSD IOPS 數量。 |
| <i>region</i> -ProvisionedSSDIOPS.MAZ2    | IOPS-Mo  | 在適用於 ONTAP 檔案系統的第二代異地同步備份 FSx 上，每 GiB SSD 儲存體佈建超過 3 IOPS 的 SSD IOPS 數量。 |

#### All FSx for ONTAP file systems

| 用量類型                                     | 單位    | 描述                                          |
|------------------------------------------|-------|---------------------------------------------|
| <i>region</i> -Storage.SAZ_2N : CPoolStd | GB-Mo | 用於 ONTAP 檔案系統的第一代或第二代單一可用區域 FSx 的標準容量集區儲存量。 |
| <i>region</i> -Storage.MAZ : CPoolStd    | GB-Mo | 用於 ONTAP 檔案系統的第一代或第二代異地同步備份 FSx 的標準容量集區儲存量。 |
| <i>region</i> -BackupUsage               | GB-月  | 用於備份的儲存容量。                                  |
| <i>region</i> -SnaplockUsage             | GB-月  | 磁碟SnapLock區使用的儲存容量。                         |

| 用量類型                                            | 單位 | 描述                                              |
|-------------------------------------------------|----|-------------------------------------------------|
| <i>region</i> -Requests.SAZ_2N : C<br>PoolStdRd | 作業 | 對適用於 ONTAP 檔案系統的單一可用區域 FSx 上的標準容量集區儲存提出的讀取請求數量。 |
| <i>region</i> -Requests.SAZ_2N : C<br>PoolStdWr | 作業 | 對適用於 ONTAP 檔案系統的單一可用區域 FSx 上的標準容量集區儲存提出的寫入請求數量。 |
| <i>region</i> -Requests.MAZ : CPoo<br>IStdRd    | 作業 | 對適用於 ONTAP 檔案系統的多可用區域 FSx 上的標準容量集區儲存提出的讀取請求數量。  |
| <i>region</i> -Requests.MAZ : CPoo<br>IStdWr    | 作業 | 對適用於 ONTAP 檔案系統的多可用區域 FSx 上的標準容量集區儲存提出的寫入請求數量。  |



# 監控 Amazon FSx for NetApp ONTAP

您可以使用下列服務和工具來監控 Amazon FSx for NetApp ONTAP 用量和活動：

- Amazon CloudWatch – 您可以使用 Amazon CloudWatch 監控檔案系統，該系統會自動從 FSx for ONTAP 收集原始資料，並將其處理為可讀指標。這些統計資料會保留 15 個月的時間，以便您存取歷史資訊並查看檔案系統的運作狀態。您也可以根據指定期間內的指標設定警示，並根據您指定的閾值相關的指標值執行一或多個動作。
- ONTAP EMS 事件 – 您可以使用 ONTAP 事件管理系統 (EMS) 產生的事件來監控 FSx for ONTAP 檔案系統。EMS 事件是檔案系統中出現的通知，例如 iSCSI LUN 建立或自動調整磁碟區大小。
- NetApp Data Infrastructure Insights – 您可以使用 NetApp Data Infrastructure Insights 服務來監控 FSx for ONTAP 檔案系統的組態、容量和效能指標。您也可以根據指標條件建立提醒。
- NetApp Harvest 和 NetApp Grafana – 您可以使用 NetApp Harvest 和 NetApp Grafana 來監控 FSx for ONTAP 檔案系統。NetApp Harvest 透過從 FSx for ONTAP 檔案系統收集效能、容量和硬體指標來監控 ONTAP 檔案系統。Grafana 提供儀表板，其中會顯示收集的收成指標。
- AWS CloudTrail – 您可以使用 AWS CloudTrail 將 Amazon FSx 的所有 API 呼叫擷取為事件。這些事件提供 Amazon FSx 中使用者、角色或服務 AWS 所採取動作的記錄。

## 主題

- [使用 Amazon CloudWatch 監控](#)
- [監控 FSx 的 ONTAP EMS 事件](#)
- [使用資料基礎設施洞見進行監控](#)
- [使用 Harvest 和 Grafana 監控 ONTAP 檔案系統的 FSx](#)
- [使用 監控 FSx 的 ONTAP API 呼叫 AWS CloudTrail](#)

## 使用 Amazon CloudWatch 監控

您可以使用 Amazon CloudWatch 監控檔案系統，該系統會收集來自 Amazon FSx for NetApp ONTAP 的原始資料，並將其處理為可讀且幾近即時的指標。這些統計資料會保留 15 個月，以便您可以存取歷史資訊，以判斷檔案系統的運作狀態。根據預設，FSx for ONTAP 指標資料會在 1 分鐘的期間內自動傳送至 CloudWatch。如需 CloudWatch 的詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的[什麼是 Amazon CloudWatch？](#)。

**Note**

根據預設，FSx for ONTAP 會以 1 分鐘的期間將指標資料傳送至 CloudWatch，但下列指標會以 5 分鐘的間隔傳送：

- FileServerDiskThroughputBalance
- FileServerDiskIopsBalance

FSx for ONTAP 的 CloudWatch 指標分為四個類別，由用於查詢每個指標的維度定義。如需維度的詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的[維度](#)。

- 檔案系統指標：File-system-level效能和儲存容量指標。
- 檔案伺服器指標：File-server-level指標。
- 詳細檔案系統彙總指標：每個彙總的詳細檔案系統指標。
- 詳細的檔案系統指標：每個儲存層File-system-level儲存指標 (SSD 和容量集區)。
- 磁碟區指標：每個磁碟區的效能和儲存容量指標。
- 詳細磁碟區指標：依儲存層或資料類型（使用者、快照或其他）的磁碟區儲存容量指標。

FSx for ONTAP 的所有 CloudWatch 指標都會發佈至 CloudWatch 中的AWS/FSx命名空間。

## 主題

- [存取 CloudWatch 指標](#)
- [在 Amazon FSx 主控台中監控](#)
- [檔案系統指標](#)
- [第二代檔案系統指標](#)
- [磁碟區指標](#)

## 存取 CloudWatch 指標

您可以透過下列方式查看 Amazon FSx 的 Amazon CloudWatch 指標：FSx

- Amazon FSx 主控台
- Amazon CloudWatch 主控台

- CloudWatch 的 AWS Command Line Interface (AWS CLI)
- CloudWatch API

下列程序說明如何使用 Amazon FSx 主控台檢視檔案系統的 CloudWatch 指標。

使用 Amazon FSx 主控台檢視檔案系統的 CloudWatch 指標

1. 開啟 Amazon FSx 主控台，網址為 <https://console.aws.amazon.com/fsx/> : //www.。
2. 在左側導覽窗格中，選擇檔案系統，然後選擇您要檢視其指標的檔案系統。
3. 在摘要頁面上，從第二個面板選擇監控 & 效能，以檢視檔案系統指標的圖表。

監控與效能面板上有四個索引標籤。

- 選擇摘要（預設標籤）以顯示檔案系統活動的任何作用中警告、CloudWatch 警示和圖形。
- 選擇儲存以檢視儲存容量和使用率指標。
- 選擇效能以檢視檔案伺服器儲存效能指標。
- 選擇 CloudWatch 警示以檢視針對檔案系統設定的任何警示圖表。

下列程序說明如何使用 Amazon FSx 主控台檢視磁碟區的 CloudWatch 指標

使用 Amazon FSx 主控台檢視磁碟區的 CloudWatch 指標

1. 開啟 Amazon FSx 主控台，網址為 <https://console.aws.amazon.com/fsx/> : //https : //https : //https : //https : //
2. 在左側導覽窗格中，選擇磁碟區，然後選擇您要檢視其指標的磁碟區。
3. 在摘要頁面上，從第二個面板中選擇監控（預設索引標籤），以檢視磁碟區指標的圖形。

下列程序說明如何使用 Amazon CloudWatch 主控台檢視檔案系統的 CloudWatch 指標。Amazon CloudWatch

使用 Amazon CloudWatch 主控台檢視指標

1. 在檔案系統的摘要頁面上，從第二個面板中選擇監控和效能，以檢視檔案系統指標的圖表。
2. 從您要在 Amazon CloudWatch 主控台中檢視之圖形右上角的動作選單中選擇在指標中檢視。Amazon CloudWatch 這會在 Amazon CloudWatch 主控台中開啟指標頁面。

下列程序說明如何將 FSx for ONTAP 檔案系統指標新增至 Amazon CloudWatch 主控台儀表板。

將指標新增至 Amazon CloudWatch 主控台

1. 在 Amazon FSx 主控台的監控與效能面板中選擇一組指標 (摘要、儲存或效能)。
2. 選擇面板右上角的新增至儀表板。這會開啟 Amazon CloudWatch 主控台。
3. 從清單中選擇現有的 CloudWatch 儀表板，或建立新的儀表板。如需詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的[使用 Amazon CloudWatch 儀表板](#)。

下列程序說明如何使用 存取檔案系統的指標 AWS CLI。

從 存取指標 AWS CLI

- 使用 CloudWatch [list-metrics](#) CLI 命令搭配 `--namespace "AWS/FSx"` 參數。如需詳細資訊，請參閱 [AWS CLI 命令參考](#)。

下列程序說明如何使用 CloudWatch API 存取檔案系統的指標。

使用 CloudWatch API 存取指標

- 呼叫 [GetMetricStatistics](#) API 操作。如需詳細資訊，請參閱 [Amazon CloudWatch API 參考](#)。

## 在 Amazon FSx 主控台中監控

Amazon FSx 報告的 CloudWatch 指標提供 FSx for ONTAP 檔案系統和磁碟區的寶貴資訊。

主題

- [在 Amazon FSx 主控台中監控檔案系統指標](#)
- [在 Amazon FSx 主控台中監控磁碟區指標](#)
- [效能警告和建議](#)
- [建立 Amazon CloudWatch 警示以監控 Amazon FSx](#)

## 在 Amazon FSx 主控台中監控檔案系統指標

您可以使用 Amazon FSx 主控台中檔案系統儀表板上的監控與效能面板，來檢視下表所述的指標。如需詳細資訊，請參閱[存取 CloudWatch 指標](#)。

| 監控與效能   | 如何...                        | 圖表                 | 相關指標                                                                                                                                                                                                                                    |
|---------|------------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Summary | ...決定檔案系統上可用的儲存容量？           | 可用的主要儲存容量 (位元組)    | StorageCapacity {SSD} - StorageUsed {SSD}                                                                                                                                                                                               |
|         | ...決定檔案系統的總用戶端輸送量？           | 用戶端總輸送量 (位元組/秒)    | $\text{SUM}(\text{DataReadBytes} + \text{DataWriteBytes}) / \text{PERIOD}$ (以秒為單位)                                                                                                                                                      |
|         | ...決定檔案系統的總用戶端 IOPS？         | 用戶端 IOPS 總計 (操作/秒) | $\text{SUM}(\text{DataReadOperations} + \text{DataWriteOperations} + \text{MetadataOperations}) / \text{PERIOD}$ (以秒為單位)                                                                                                                |
|         | ...決定檔案系統的讀取、寫入和中繼資料操作的平均延遲？ | 平均延遲 (毫秒/操作)       | 平均讀取延遲： $\text{DataReadOperationTime} * 1000 / \text{DataReadOperations}$<br>平均寫入延遲： $\text{DataWriteOperationTime} * 1000 / \text{DataWriteOperations}$<br>平均中繼資料延遲： $\text{MetadataOperationTime} * 1000 / \text{MetadataOperations}$ |
|         | ...決定檔案系統上已使用和可用儲存容量的分佈？     | 儲存分佈               | 主要方案可用：StorageCapacity {SSD} - StorageUsed {SSD}                                                                                                                                                                                        |

| 監控與效能   | 如何...                            | 圖表                   | 相關指標                                                               |
|---------|----------------------------------|----------------------|--------------------------------------------------------------------|
| 儲存      |                                  |                      | 使用的主要方案 : StorageUsed {SSD}                                        |
|         |                                  |                      | 使用的容量集區 : StorageUsed {StandardCapacityPool }                      |
|         | ...決定儲存效率 ( 壓縮、重複資料刪除和壓縮 ) 的節省 ? | 節省儲存效率               | StorageEfficiencySavings                                           |
|         | ...決定有多少主要儲存可用 ?                 | 可用的主要儲存容量 ( 位元組 )    | StorageCapacity {SSD} - StorageUsed {SSD}                          |
|         | ...決定我的檔案系統已使用的主要儲存體百分比 ?        | 主要儲存容量使用率 ( 百分比 )    | $\text{StorageUsed \{SSD\} * 100 / \text{StorageCapacity \{SSD\}}$ |
| 檔案伺服器效能 | ...判斷我的檔案系統是否接近其網路輸送量限制 ?        | 網路輸送量 – 使用率 ( 百分比 )  | NetworkThroughputUtilization                                       |
|         | ...判斷我的檔案系統是否接近磁碟輸送量限制 ?         | 磁碟輸送量 – 使用率 ( 百分比 )  | FileServerDiskThroughputUtilization                                |
|         | ...判斷我的檔案系統是否已用盡磁碟輸送量的允許爆量額度 ?   | 磁碟輸送量 – 爆量平衡 ( 百分比 ) | FileServerDiskThroughputBalance                                    |

| 監控與效能 | 如何...                                      | 圖表                       | 相關指標                           |
|-------|--------------------------------------------|--------------------------|--------------------------------|
|       | ...判斷我的檔案系統是否接近其檔案伺服器的 SSD IOPS 限制？        | 磁碟 IOPS – 使用率（百分比）       | FileServerDiskIops Utilization |
|       | ...判斷我的檔案系統是否已用盡其檔案伺服器的磁碟 SSD IOPS 允許爆量額度？ | 磁碟 IOPS – 爆量平衡（百分比）      | FileServerDiskIops Balance     |
|       | ...決定檔案系統 CPU 的平均使用率？                      | CPU 使用率（百分比）             | CPUUtilization                 |
|       | ...判斷我的工作負載是否有效利用檔案系統的 RAM 和 NVMe 讀取快取？    | 快取命中率（百分比）               | FileServerCacheHit Ratio       |
| 磁碟效能  | ...判斷我的檔案系統是否接近其目前佈建的 SSD IOPS 容量？         | 磁碟 IOPS – 使用率 (SSD)（百分比） | DiskIopsUtilization            |

#### Note

我們建議您將任何效能相關維度的平均輸送量容量使用率，例如網路使用率、CPU 使用率和 SSD IOPS 使用率維持在 50% 以下。這可確保您有足夠的備用輸送量容量，以因應工作負載中的意外尖峰，以及任何背景儲存操作（例如儲存同步、資料分層或備份）。

## 在 Amazon FSx 主控台中監控磁碟區指標

您可以在 Amazon FSx 主控台中檢視磁碟區儀表板上的監控面板，以查看其他效能指標。如需詳細資訊，請參閱[存取 CloudWatch 指標](#)。

| 監控 | 如何...                      | 圖表                 | 相關指標                                                                                                                                                                                                                                            |
|----|----------------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | ...決定磁碟區的可用儲存容量？           | 可用的儲存容量            | StorageCapacity                                                                                                                                                                                                                                 |
|    | ...決定磁碟區的總用戶端輸送量？          | 用戶端總輸送量<br>(位元組/秒) | $\text{SUM}(\text{DataReadBytes} + \text{DataWriteBytes}) / \text{PERIOD}$ (以秒為單位)                                                                                                                                                              |
|    | ...決定磁碟區的總用戶端 IOPS？        | 用戶端 IOPS 總計 (操作/秒) | $\text{SUM}(\text{DataReadOperations} + \text{DataWriteOperations} + \text{MetadataOperations}) / \text{PERIOD}$ (以秒為單位)                                                                                                                        |
|    | ...決定有多少讀取和寫入操作來自或前往容量集區層？ | 容量集區 IOPS (操作/秒)   | 讀取操作：CapacityPoolReadOperations<br>寫入操作：CapacityPoolWriteOperations                                                                                                                                                                             |
|    | ...決定磁碟區讀取、寫入和中繼資料操作的平均延遲？ | 平均延遲 (毫秒/操作)       | 平均讀取延遲： $\text{DataReadOperationTime} * 1000 / \text{DataReadOperations}$<br><br>平均寫入延遲： $\text{DataWriteOperationTime} * 1000 / \text{DataWriteOperations}$<br><br>平均中繼資料延遲： $\text{MetadataOperationTime} * 1000 / \text{MetadataOperations}$ |



| 監控 | 如何...                     | 圖表             | 相關指標                          |
|----|---------------------------|----------------|-------------------------------|
|    |                           |                | ime * 1000/MetadataOperations |
|    | ...決定磁碟區上可用的檔案或索引數量？      | 可用的檔案 (inodes) | FilesCapacity - FilesUsed     |
|    | ...決定我的磁碟區上已使用和可用儲存容量的分佈？ | 儲存分佈           | StorageCapacity - StorageUsed |

## 效能警告和建議

每當其中一個指標接近或超過多個連續資料點的預定閾值時，FSx for ONTAP 會顯示 CloudWatch 指標的警告。這些警告為您提供可行的建議，您可以用來最佳化檔案系統的效能。

您可以在監控與效能儀表板的數個區域中存取警告。所有作用中或最近的 Amazon FSx 效能警告，以及針對處於 ALARM 狀態的檔案系統所設定的任何 CloudWatch 警示，都會出現在摘要區段的監控與效能面板中。警告也會顯示在顯示指標圖形的儀表板區段中。

您可以為任何 Amazon FSx 指標建立 CloudWatch 警示。如需詳細資訊，請參閱[建立 Amazon CloudWatch 警示以監控 Amazon FSx](#)。

### 使用效能警告來改善檔案系統效能

Amazon FSx 提供可行的建議，您可以用來最佳化檔案系統的效能。這些建議說明如何解決潛在的效能瓶頸。如果您預期活動會繼續，或對檔案系統的效能造成影響，您可以採取建議的動作。根據哪個指標已觸發警告，您可以透過增加檔案系統的輸送量容量或儲存容量來解決它，如下表所述。

| 儀表板區段 | 如果有此指標的警告 | 執行此作業                                                                                                                                                                    |
|-------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 儲存    | 主要儲存容量使用率 | <p>如果您的檔案系統尚未達到 SSD 儲存容量上限，請增加檔案系統的主要儲存容量。如需詳細資訊，請參閱<a href="#">更新儲存容量和佈建 IOPS</a>。</p> <p>如果您的檔案系統有多個 HA 對，且主要儲存容量使用率僅較高於檔案系統彙總的子集（構成主要儲存層的儲存集區），則您也可以重新平衡工作負載，讓您的主</p> |

| 儀表板區段   | 如果有此指標的警告 | 執行此作業                                                                                                                                                                                                                                                                        |
|---------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         |           | 要儲存容量使用率更平均分散到檔案系統。如需重新平衡工作負載的詳細資訊，請參閱 <a href="#">平衡跨 HA 對的工作負載</a> 。                                                                                                                                                                                                       |
| 檔案伺服器效能 | 網路輸送量     | 如果您的檔案系統尚未達到最大輸送量容量，請增加檔案系統的輸送量容量。如需更新輸送量容量的詳細資訊，請參閱 <a href="#">更新輸送量容量</a> 。                                                                                                                                                                                               |
|         | 磁碟輸送量     |                                                                                                                                                                                                                                                                              |
|         | 磁碟 IOPS   | 如果您的檔案系統有多個 HA 對，且只有一部分的檔案伺服器使用率很高，則您也可以重新平衡工作負載，以便工作負載更平均地利用每個檔案系統 HA 對的效能功能。如需重新平衡工作負載的詳細資訊，請參閱 <a href="#">平衡跨 HA 對的工作負載</a> 。                                                                                                                                            |
|         | CPU 使用率   |                                                                                                                                                                                                                                                                              |
| 磁碟效能    | 磁碟 IOPS   | <p>如果您的檔案系統尚未達到檔案系統目前輸送量容量的 SSD IOPS 上限，請增加 SSD IOPS。如需更新檔案系統佈建 IOPS 的詳細資訊，請參閱 <a href="#">更新儲存容量和佈建 IOPS</a>。</p> <p>如果您的檔案系統有多個 HA 對，而且您的磁碟 IOPS 使用率僅較高於檔案系統彙總的子集（構成主要儲存層的儲存集區），則您也可以重新平衡工作負載，以便在檔案系統中更平均地使用磁碟 IOPS。如需重新平衡工作負載的詳細資訊，請參閱 <a href="#">平衡跨 HA 對的工作負載</a>。</p> |

如需檔案系統效能的詳細資訊，請參閱 [Amazon FSx for NetApp ONTAP 效能](#)。

## 建立 Amazon CloudWatch 警示以監控 Amazon FSx

您可以建立 CloudWatch 警報，在警示變更狀態時傳送 Amazon Simple Notification Service (Amazon SNS) 訊息。警示會在您指定的期間監看單一指標。如有需要，警示接著會根據相對於指定閾值的指標值，在數個期間內執行一或多個動作。此動作是傳送到 Amazon SNS 主題或 Auto Scaling 政策的通知。

警示僅會針對持續狀態變更調用動作。CloudWatch 警示不會只因處於特定狀態就調用動作，狀態必須已變更並已維持一段指定的時間。您可以從 Amazon FSx 主控台或 Amazon CloudWatch 主控台建立警示。

下列程序說明如何使用 Amazon FSx 主控台、AWS Command Line Interface (AWS CLI) 和 API 建立警示。

### 使用 Amazon FSx 主控台設定警示

1. 開啟 Amazon FSx 主控台，網址為 <https://console.aws.amazon.com/fsx/> : //https : //https : //https : //https : ///
2. 在左側導覽窗格中，選擇檔案系統，然後選擇您要為其建立警示的檔案系統。
3. 在摘要頁面上，從第二個面板選擇監控 & 效能。
4. 選擇 CloudWatch 警示索引標籤。
5. 選擇建立 CloudWatch 警示。系統會將您重新導向至 CloudWatch 主控台。
6. 選擇選取指標。
7. 在指標區段中，選擇 FSx。
8. 選擇指標類別：
  - 檔案系統指標
  - 詳細檔案系統指標
  - 磁碟區指標
  - 詳細磁碟區指標
9. 選擇您要設定警示的指標，然後選擇選取指標。
10. 在條件區段中，選擇您想要警示的條件，然後選擇下一步。

#### Note

檔案系統維護期間，可能不會發佈指標。若要防止不必要的和誤導性的警示條件變更，以及設定警示，使其能夠彈性地處理遺失的資料點，請參閱《Amazon [CloudWatch 使用者指南](#)》中的設定 CloudWatch 警示如何處理遺失的資料。Amazon CloudWatch

11. 如果您希望 CloudWatch 在警示狀態啟動動作時傳送電子郵件或 Amazon SNS 通知給您，請選擇警示狀態觸發條件的警示狀態。

針對傳送通知至下列 SNS 主題，選擇 選項。如果您選擇 Create topic (建立主題)，您可以為新的電子郵件訂閱清單來設定名稱和電子郵件地址。此清單會儲存並顯示在欄位中供未來警示使用。選擇下一步。

 Note

如果您使用建立主題來建立新的 Amazon SNS 主題，電子郵件地址必須先經過驗證才會接收通知。電子郵件只有在警示進入警示狀態時才會傳送。如果此警示狀態在驗證電子郵件地址之前發生變更，就不會收到通知。

12. 填寫警示名稱和警示描述欄位，然後選擇下一步。
13. 在預覽和建立頁面上，檢閱您要建立的警示，然後選擇建立警示。

### 使用 CloudWatch 主控台設定警示

1. 透過 <https://console.aws.amazon.com/cloudwatch/> 開啟 CloudWatch 主控台。
2. 選擇建立警示以啟動建立警示精靈。
3. 請遵循中的程序，使用 Amazon FSx 主控台設定警示，從步驟 6 開始。

### 使用 設定警示 AWS CLI

- 呼叫 [put-metric-alarm](#) CLI 命令。如需詳細資訊，請參閱《AWS CLI 命令參考》<https://docs.aws.amazon.com/cli/latest/reference/>。

### 使用 CloudWatch API 設定警示

- 呼叫 [PutMetricAlarm](#) API 操作。如需詳細資訊，請參閱 [Amazon CloudWatch API 參考](#)。

## 檔案系統指標

您的 Amazon FSx for NetApp ONTAP 檔案系統指標會分類為檔案系統指標或詳細的檔案系統指標。

- 檔案系統指標是單一檔案系統的彙總效能和儲存指標，採用單一維度 `FileSystemId`。這些指標會測量檔案系統的網路效能和儲存容量使用量。
- 詳細的檔案系統指標會測量檔案系統的儲存容量，以及每個儲存層（例如 SSD 儲存和容量集區儲存）中所使用的儲存體。每個指標都包含 `FileSystemId`、`StorageTier` 和 `DataType` 維度。

請注意，Amazon FSx 何時將這些指標的資料點發佈至 CloudWatch：

- 對於使用率指標（名稱以使用率結尾的任何指標，例如 NetworkThroughputUtilization），每個作用中檔案伺服器或彙總的每個期間都會發出一個資料點。例如，Amazon FSx 會針對的每個作用中檔案伺服器發出每分鐘指標 FileServerDiskIopsUtilization，針對發出每分鐘指標 DiskIopsUtilization。
- 對於所有其他指標，每個期間都會發出單一資料點，對應於所有作用中檔案伺服器（例如 DataReadBytes 檔案伺服器指標）或所有彙總（例如 DiskReadBytes 儲存指標）的指標總值。

## 主題

- [網路 I/O 指標](#)
- [檔案伺服器指標](#)
- [磁碟 I/O 指標](#)
- [儲存容量指標](#)
- [詳細的檔案系統指標](#)

## 網路 I/O 指標

所有這些指標都採用一個維度 FileSystemId。

| 指標                           | 描述                                                                                                                                                                                                              |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NetworkThroughputUtilization | <p>檔案系統的網路輸送量使用率百分比。</p> <p>Average 統計資料是檔案系統在指定期間內的平均網路輸送量使用率。</p> <p>Minimum 統計資料是檔案系統在指定期間內的最低網路輸送量使用率。</p> <p>Maximum 統計資料是檔案系統在指定期間內的最高網路輸送量使用率。</p> <p>單位：百分比</p> <p>有效統計資料：Minimum、Average 和 Maximum</p> |

| 指標                   | 描述                                                                                                                                                 |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| NetworkSentBytes     | <p>檔案系統傳送的位元組數（網路 I/O）。</p> <p>Sum 統計資料是檔案系統在指定期間內傳送的位元組總數。</p> <p>若要計算任何統計資料的傳送輸送量（每秒位元組數），請將統計資料除以指定期間內的秒數。</p> <p>單位：位元組</p> <p>有效的統計資訊：Sum</p> |
| NetworkReceivedBytes | <p>檔案系統收到的位元組數（網路 I/O）。</p> <p>Sum 統計資料是檔案系統在指定期間內接收的位元組總數。</p> <p>若要計算任何統計資料的接收輸送量（每秒位元組數），請將統計資料除以指定期間內的秒數。</p> <p>單位：位元組</p> <p>有效的統計資訊：Sum</p> |
| DataReadBytes        | <p>從用戶端讀取到檔案系統的位元組數（網路 I/O）。</p> <p>Sum 統計資料是指定期間內與讀取操作相關聯的位元組總數。若要計算一段期間的平均輸送量（每秒位元組數），請將Sum統計資料除以指定期間內的秒數。</p> <p>單位：位元組</p> <p>有效的統計資訊：Sum</p>  |

| 指標                  | 描述                                                                                                                                              |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| DataWriteBytes      | <p>用戶端寫入檔案系統的位元組數（網路 I/O）。</p> <p>Sum 統計資料是指定期間內與寫入操作相關聯的位元組總數。若要計算一段期間的平均輸送量（每秒位元組數），請將Sum統計資料除以指定期間內的秒數。</p> <p>單位：位元組</p> <p>有效的統計資訊：Sum</p> |
| DataReadOperations  | <p>從用戶端讀取到檔案系統的讀取操作（網路 I/O）計數。</p> <p>Sum 統計資料是指定期間內發生的 I/O 操作總數。若要計算一段期間內每秒的平均讀取操作，請將Sum統計資料除以指定期間內的秒數。</p> <p>單位：計數</p> <p>有效的統計資訊：Sum</p>    |
| DataWriteOperations | <p>從用戶端寫入檔案系統的寫入操作（網路 I/O）計數。</p> <p>Sum 統計資料是指定期間內發生的 I/O 操作總數。若要計算期間每秒的平均寫入操作，請將Sum統計資料除以指定期間內的秒數。</p> <p>單位：計數</p> <p>有效的統計資訊：Sum</p>        |

| 指標                     | 描述                                                                                                                                                                              |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MetadataOperations     | <p>用戶端對檔案系統的中繼資料操作（網路 I/O）計數。</p> <p>Sum 統計資料是指定期間內發生的 I/O 操作總數。若要計算一段時間內每秒的平均中繼資料操作，請將Sum統計資料除以指定期間內的秒數。</p> <p>單位：計數</p> <p>有效的統計資訊：Sum</p>                                   |
| DataReadOperationTime  | <p>在檔案系統內用於讀取操作（網路 I/O）的用戶端存取檔案系統中資料的總時間總和。</p> <p>Sum 統計資料是讀取操作在指定期間內所花費的總秒數。若要計算一段時間的平均讀取延遲，請將Sum統計資料除以相同期間的SumDataReadOperations 指標。</p> <p>單位：秒</p> <p>有效的統計資訊：Sum</p>      |
| DataWriteOperationTime | <p>在檔案系統內用於從存取檔案系統中資料的用戶端完成寫入操作（網路 I/O）的總時間總和。</p> <p>Sum 統計資料是寫入操作在指定期間內所花費的秒總數。若要計算某段期間的平均寫入延遲，請將Sum統計資料除以相同期間的 SumDataWriteOperations 指標。</p> <p>單位：秒</p> <p>有效的統計資訊：Sum</p> |



| 指標                         | 描述                                                                                                                                                                                                       |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CapacityPoolReadBytes      | <p>從檔案系統的容量集區層讀取的位元組數（網路 I/O）。</p> <p>為了確保資料完整性，ONTAP 會在執行寫入操作後立即對容量集區執行讀取操作。</p> <p>Sum 統計資料是指定期間內從檔案系統的容量集區層讀取的位元組總數。若要計算每秒的容量集區位元組，請將Sum統計資料除以指定期間內的秒數。</p> <p>單位：位元組</p> <p>有效的統計資訊：Sum</p>          |
| CapacityPoolReadOperations | <p>檔案系統容量集區層的讀取操作（網路 I/O）數目。這會轉換為容量集區讀取請求。</p> <p>為了確保資料完整性，ONTAP 會在執行寫入操作後立即對容量集區執行讀取操作。</p> <p>Sum 統計資料是指定期間內來自檔案系統容量集區層的讀取操作總數。若要計算每秒的容量集區請求，請將Sum統計資料除以指定期間內的秒數。</p> <p>單位：計數</p> <p>有效的統計資訊：Sum</p> |

| 指標                          | 描述                                                                                                                                                                                                    |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CapacityPoolWriteBytes      | <p>寫入檔案系統的容量集區層的位元組數（網路 I/O）。</p> <p>為了確保資料完整性，ONTAP 會在執行寫入操作後立即對容量集區執行讀取操作。</p> <p>Sum 統計資料是寫入檔案系統容量集區層的位元組總數，在指定期間內寫入。若要計算每秒的容量集區位元組，請將Sum統計資料除以指定期間內的秒數。</p> <p>單位：位元組</p> <p>有效的統計資訊：Sum</p>      |
| CapacityPoolWriteOperations | <p>從容量集區層寫入檔案系統的寫入操作（網路 I/O）數目。這會轉換為寫入請求。</p> <p>為了確保資料完整性，ONTAP 會在執行寫入操作後立即對容量集區執行讀取操作。</p> <p>Sum 統計資料是指定期間內檔案系統容量集區層的寫入操作總數。若要計算每秒的容量集區請求，請將Sum統計資料除以指定期間內的秒數。</p> <p>單位：計數</p> <p>有效的統計資訊：Sum</p> |

## 檔案伺服器指標

所有這些指標都需要一個維度 FileSystemId。

| 指標             | 描述                  |
|----------------|---------------------|
| CPUUtilization | 檔案系統的 CPU 資源使用率百分比。 |

| 指標                                  | 描述                                                                                                                                                                                                                                         |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                     | <p>Average 統計資料是檔案系統在指定期間內的平均 CPU 使用率。</p> <p>Minimum 統計資料是檔案系統在指定期間內的最低 CPU 使用率。</p> <p>Maximum 統計資料是檔案系統在指定期間內的最高 CPU 使用率。</p> <p>單位：百分比</p> <p>有效統計資料：Average、Minimum和Maximum</p>                                                       |
| FileServerDiskThroughputUtilization | <p>檔案伺服器與主要層之間的磁碟輸送量，以輸送量容量決定的佈建限制百分比表示。</p> <p>Average 統計資料是檔案伺服器在指定期間內磁碟輸送量的平均使用率百分比。</p> <p>Minimum 統計資料是檔案伺服器在指定期間內磁碟輸送量的最低使用率百分比。</p> <p>Maximum 統計資料是檔案伺服器在指定期間內磁碟輸送量的最高使用率。</p> <p>單位：百分比</p> <p>有效統計資料：Average、Minimum和Maximum</p> |

| 指標                              | 描述                                                                                                                                                                                                                                 |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FileServerDiskThroughputBalance | <p>檔案伺服器與主要層之間磁碟輸送量的可用爆量額度百分比。這適用於佈建輸送量容量小於 512 MBps 的檔案系統。</p> <p>Average 統計資料是指定期間內可用的平均爆量餘額。</p> <p>Minimum 統計資料是指定期間內可用的最小爆量餘額。</p> <p>Maximum 統計資料是指定期間內可用的最大爆量餘額。</p> <p>單位：百分比</p> <p>有效統計資料：Average、Minimum和Maximum</p>    |
| FileServerDiskIopsBalance       | <p>檔案伺服器與主要層之間磁碟 IOPS 的可用爆量額度百分比。這適用於佈建輸送量容量小於 512 MBps 的檔案系統。</p> <p>Average 統計資料是指定期間內可用的平均爆量餘額。</p> <p>Minimum 統計資料是指定期間內可用的最小爆量餘額。</p> <p>Maximum 統計資料是指定期間內可用的最大爆量餘額。</p> <p>單位：百分比</p> <p>有效統計資料：Average、Minimum和Maximum</p> |

| 指標                            | 描述                                                                                                                                                                                                                                                  |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FileServerDiskIopsUtilization | <p>檔案伺服器的可用磁碟 IOPS 容量 IOPS 使用率百分比。</p> <p>Average 統計資料是檔案系統在指定期間內的平均磁碟 IOPS 使用率。</p> <p>Minimum 統計資料是檔案系統在指定期間內的最低磁碟 IOPS 使用率。</p> <p>Maximum 統計資料是檔案系統在指定期間內的最大磁碟 IOPS 使用率。</p> <p>單位：百分比</p> <p>有效統計資料：Average、Minimum和Maximum</p>                |
| FileServerCacheHitRatio       | <p>檔案系統 RAM 和 NVMe 快取中資料提供的所有讀取請求百分比。較高百分比表示檔案系統的讀取快取會提供更多讀取。</p> <p>單位：百分比</p> <p>Average 統計資料是檔案系統在指定期間內的平均快取命中百分比。</p> <p>Minimum 統計資料是檔案系統在指定期間內的最低快取命中百分比。</p> <p>Maximum 統計資料是檔案系統在指定期間內的最高快取命中百分比。</p> <p>有效統計資料：Average、Minimum和Maximum</p> |

## 磁碟 I/O 指標

所有這些指標都需要一個維度 FileSystemId。

| 指標                  | 描述                                                                                                                                                                          |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DiskReadBytes       | <p>從任何磁碟讀取到檔案系統主要層的位元組數 ( 磁碟 I/O)。</p> <p>Sum 統計資料是指定期間內從檔案系統讀取的位元組總數。</p> <p>若要計算任何統計資料的讀取磁碟輸送量 ( 每秒位元組數 ) , 請將Sum統計資料除以指定期間內的秒數。</p> <p>單位 : 位元組</p> <p>有效的統計資訊 : Sum</p> |
| DiskWriteBytes      | <p>從任何磁碟寫入檔案系統主要層的位元組數 ( 磁碟 I/O)。</p> <p>Sum 統計資料是指定期間內從檔案系統寫入的位元組總數。</p> <p>若要計算任何統計資料的寫入磁碟輸送量 ( 每秒位元組數 ) , Sum請將統計資料除以指定期間內的秒數。</p> <p>單位 : 位元組</p> <p>有效的統計資訊 : Sum</p>  |
| DiskIopsUtilization | <p>檔案伺服器和儲存磁碟區之間的磁碟 IOPS , 以主要層佈建磁碟 IOPS 限制的百分比表示。</p> <p>Average 統計資料是檔案系統在指定期間內的平均磁碟 IOPS 使用率。</p> <p>Minimum 統計資料是檔案系統在指定期間內的最低磁碟 IOPS 使用率。</p>                          |

| 指標                  | 描述                                                                                                          |
|---------------------|-------------------------------------------------------------------------------------------------------------|
|                     | <p>Maximum 統計資料是檔案系統在指定期間內的<br/>最大磁碟 IOPS 使用率。</p> <p>單位：百分比</p> <p>有效統計資料：Average、Minimum和<br/>Maximum</p> |
| DiskReadOperations  | <p>檔案系統主要層的讀取操作（磁碟 I/O）數目。</p> <p>Sum 統計資料是指定期間內主要層的讀取操作總<br/>數。</p> <p>單位：計數</p> <p>有效的統計資訊：Sum</p>        |
| DiskWriteOperations | <p>檔案系統主要層的寫入操作（磁碟 I/O）數目。</p> <p>Sum 統計資料是指定期間內主要層的寫入操作總<br/>數。</p> <p>單位：計數</p> <p>有效的統計資訊：Sum</p>        |

## 儲存容量指標

所有這些指標都需要一個維度 FileSystemId。

| 指標                       | 描述                                                                                                                      |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------|
| StorageEfficiencySavings | <p>從儲存效率功能（壓縮、重複資料刪除和壓<br/>縮）儲存的位元組。</p> <p>Average 統計資料是指定期間內平均儲存效<br/>率節省。若要計算儲存效率節省佔所有儲存<br/>資料的百分比，請在一分鐘的期間內，使用</p> |

| 指標          | 描述                                                                                                                                                                                                                                     |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             | <p>Sum 的 統計資料除StorageEfficiencySavings 以 StorageEfficiencySavings 和 StorageUsed 檔案系統指標的總和StorageUsed 。</p> <p>Minimum 統計資料是指定期間內節省的最小儲存效率。</p> <p>Maximum 統計資料是指定期間內節省的最大儲存效率。</p> <p>單位：位元組</p> <p>有效統計資料：Average、Minimum和Maximum</p> |
| StorageUsed | <p>檔案系統上主要 (SSD) 層和容量集區層上存放的實體資料總量。此指標包括節省儲存效率功能，例如資料壓縮和重複資料刪除。</p> <p>單位：位元組</p> <p>有效統計資料：Average、Minimum和Maximum</p>                                                                                                                |



| 指標                | 描述                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LogicalDataStored | <p>同時考量 SSD 層和容量集區層，存放在檔案系統上的邏輯資料總量。此指標包含快照和 FlexClones 的總邏輯大小，但不包含透過壓縮、壓縮和重複資料刪除來節省儲存效率。</p> <p>若要以位元組為單位計算儲存效率節省，請在 StorageUsed 指定期間取得 Average 的，並在 LogicalDataStored 相同期間從 Average 減去它。</p> <p>若要以總邏輯資料大小的百分比來計算儲存效率節省，StorageUsed 請在指定期間內取得 Average 的，並在 LogicalDataStored 相同期間從 Average 減去它。然後將差異除以 LogicalDataStored 相同期間的 Average。</p> <p>單位：位元組</p> <p>有效統計資料：Average、Minimum 和 Maximum</p> |

## 詳細的檔案系統指標

詳細的檔案系統指標是每個儲存層的詳細儲存使用率指標。詳細的檔案系統指標都有維度 FileSystemId、StorageTier 和 DataType。

- StorageTier 維度指出指標測量的儲存層，可能值為 SSD 和 StandardCapacityPool。
- DataType 維度指出指標測量的資料類型，可能的值為 All。

指定指標和維度鍵值對的每個唯一組合都有一列，其中包含該組合測量項目的描述。

| 指標                         | 描述                                                                                                                                                                                                                                                                                                      |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| StorageCapacityUtilization | <p>每個檔案系統彙總的儲存容量使用率。您每個檔案系統的彙總每分鐘都會發出一個指標。</p> <p>Average 統計資料是指定期間內檔案系統效能方案的平均儲存容量使用率。</p> <p>Minimum 統計資料是檔案系統效能層在指定期間內的最低儲存容量使用率。</p> <p>Maximum 統計資料是檔案系統效能層在指定期間內的最高儲存容量使用率。</p> <p>單位：百分比</p> <p>有效統計資料：Average、Minimum和Maximum</p>                                                               |
| StorageCapacity            | <p>主要 (SSD) 層的總儲存容量。</p> <p>單位：位元組</p> <p>有效的統計資訊：Maximum</p>                                                                                                                                                                                                                                           |
| StorageUsed                | <p>使用的實體儲存容量，以位元組為單位，特定於儲存層。此值包括節省儲存效率功能，例如資料壓縮和重複資料刪除。的有效維度值StorageTier 為 SSD和 StandardCapacityPool，對應至此指標測量的儲存層。此指標也需要具有值的 DataType維度All。</p> <p>Average、Minimum和 Maximum統計資料是指定期間內以位元組為單位的每層儲存耗用量。</p> <p>若要計算主要 (SSD) 儲存層的儲存容量使用率，請將這些統計資料除以MaximumStorageCapacity 相同期間的，其StorageTier 維度等於 SSD。</p> |

| 指標 | 描述                                                                                                                                                         |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>若要以位元組為單位計算主要 (SSD) 儲存層的可用儲存容量，請從MaximumStorageCapacity 相同期間的 減去任何這些統計資料，其維度StorageTier 等於 SSD。</p> <p>單位：位元組</p> <p>有效統計資料：Average、Minimum和Maximum</p> |

## 第二代檔案系統指標

FSx for ONTAP 第二代檔案系統提供下列指標。對於 指標，會針對每個 HA 對和每個彙總發出資料點（針對儲存使用率指標）。

### Note

如果您有具有多個 HA 對的檔案系統，您也可以使用[單一 HA 對檔案系統指標](#)和[磁碟區指標](#)。

### 主題

- [網路 I/O 指標](#)
- [檔案伺服器指標](#)
- [磁碟 I/O 指標](#)
- [詳細的檔案系統指標](#)

## 網路 I/O 指標

所有這些指標需要兩個維度，FileSystemId和FileServer。

- FileSystemId – 檔案系統 AWS 的資源 ID。
- FileServer – ONTAP 中檔案伺服器（或節點）的名稱（例如，FsxId01234567890abcdef-01）。奇數編號的檔案伺服器是偏好的檔案伺服器（也就是，除非檔案系統容錯移轉至次要檔案伺服器，否則它們會服務流量），而偶數編號的檔案伺服器是次要檔

案伺服器（也就是，只有在其合作夥伴無法使用時，才會提供流量）。因此，次要檔案伺服器通常比偏好的檔案伺服器顯示較少的使用率。

| 指標                           | 描述                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NetworkThroughputUtilization | <p>網路輸送量使用率佔檔案系統可用網路輸送量的百分比。此指標相當於 檔案系統一個 HA 對網路輸送量容量的最大值NetworkSentBytes 和NetworkReceivedBytes 百分比。此指標會考慮所有流量，包括背景任務（例如 SnapMirror、分層和備份）。您每個檔案系統的檔案伺服器每分鐘都會發出一個指標。</p> <p>Average 統計資料是指定期間內指定檔案伺服器的平均網路輸送量使用率。</p> <p>Minimum 統計資料是指定期間內指定檔案伺服器一分鐘內的最低網路輸送量使用率。</p> <p>Maximum 統計資料是指定期間內指定檔案伺服器一分鐘內的最高網路輸送量使用率。</p> <p>單位：百分比</p> <p>有效統計資料：Average、Minimum和Maximum</p> |
| NetworkSentBytes             | <p>檔案系統傳送的位元組數（網路 IO）。此指標會考慮所有流量，包括背景任務（例如 SnapMirror、分層和備份）。您每個檔案系統的檔案伺服器每分鐘都會發出一個指標。</p> <p>Sum 統計資料是指定檔案伺服器在指定期間內透過網路傳送的位元組總數。</p> <p>Average 統計資料是指定檔案伺服器在指定期間內透過網路傳送的平均位元組數。</p>                                                                                                                                                                                       |

| 指標 | 描述                                                                                                                                                                                                        |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>Minimum 統計資料是指定檔案伺服器在指定期間內透過網路傳送的最低位元組數。</p> <p>Maximum 統計資料是指定檔案伺服器在指定期間內透過網路傳送的最大位元組數。</p> <p>若要計算任何統計資料的傳送輸送量（每秒位元組數），請將統計資料除以指定期間內的秒數。</p> <p>單位：位元組</p> <p>有效統計資料：Sum、Minimum、Average和Maximum</p> |

| 指標                   | 描述                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NetworkReceivedBytes | <p>檔案系統收到的位元組數（網路 IO）。此指標會考慮所有流量，包括背景任務（例如 SnapMirror、分層和備份）。您每個檔案系統的檔案伺服器每分鐘都會發出一個指標。</p> <p>Sum 統計資料是指定檔案伺服器在指定期間內透過網路接收的位元組總數。</p> <p>Average 統計資料是指定檔案伺服器在指定期間內每分鐘透過網路接收的平均位元組數。</p> <p>Minimum 統計資料是指定檔案伺服器在指定期間內每分鐘透過網路接收的最低位元組數。</p> <p>Maximum 統計資料是指定檔案伺服器在指定期間內每分鐘透過網路接收的最高位元組數。</p> <p>若要計算任何統計資料的接收輸送量（每秒位元組數），請將統計資料除以期間的秒數。</p> <p>單位：位元組</p> <p>有效統計資料：Sum、Minimum、Average 和 Maximum</p> |

## 檔案伺服器指標

所有這些指標需要兩個維度，FileSystemId 和 FileServer。

| 指標             | 描述                                                                                             |
|----------------|------------------------------------------------------------------------------------------------|
| CPUUtilization | <p>檔案系統的 CPU 資源使用率百分比。您每個檔案系統的檔案伺服器每分鐘都會發出一個指標。</p> <p>Average 統計資料是檔案系統在指定期間內的平均 CPU 使用率。</p> |

| 指標                                  | 描述                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                     | <p>Minimum 統計資料是指定期間內指定檔案伺服器的最低 CPU 使用率。</p> <p>Maximum 統計資料是指定期間指定檔案伺服器的最高 CPU 使用率。</p> <p>單位：百分比</p> <p>有效統計資料：Average、Minimum和Maximum</p>                                                                                                                                                                                                                                               |
| FileServerDiskThroughputUtilization | <p>檔案伺服器與彙總之間的磁碟輸送量，以輸送量容量決定的佈建限制百分比表示。此指標會考慮所有流量，包括背景任務（例如 SnapMirror、分層和備份）。此指標相當於 檔案系統一個 HA 對之檔案伺服器磁碟輸送量容量的 DiskReadBytes 和 DiskWriteBytes 總和百分比。您每個檔案系統的檔案伺服器每分鐘都會發出一個指標。</p> <p>Average 統計資料是指定期間指定檔案伺服器的平均檔案伺服器磁碟輸送量使用率。</p> <p>Minimum 統計資料是指定期間內指定檔案伺服器的最低檔案伺服器磁碟輸送量使用率。</p> <p>Maximum 統計資料是指定期間內指定檔案伺服器的最高檔案伺服器磁碟輸送量使用率。</p> <p>單位：百分比</p> <p>有效統計資料：Average、Minimum和Maximum</p> |

| 指標                            | 描述                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FileServerDiskIopsUtilization | <p>檔案伺服器的可用磁碟 IOPS 容量 IOPS 使用率，以磁碟 IOPS 限制的百分比表示。這與不同DiskIopsUtilization 之處在於，磁碟 IOPS 的使用率超出檔案伺服器可處理的最大值，而不是佈建的磁碟 IOPS。此指標會考慮所有流量，包括背景任務（例如 SnapMirror、分層和備份）。您每個檔案系統的檔案伺服器每分鐘都會發出一個指標。</p> <p>Average 統計資料是指定期間內指定檔案伺服器的平均磁碟 IOPS 使用率。</p> <p>Minimum 統計資料是指定期間內指定檔案伺服器的最低磁碟 IOPS 使用率。</p> <p>Maximum 統計資料是指定期間內指定檔案伺服器的最高磁碟 IOPS 使用率。</p> <p>單位：百分比</p> <p>有效統計資料：Average、Minimum和Maximum</p> |



| 指標                      | 描述                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FileServerCacheHitRatio | <p>針對每個 HA 對（例如，HA 對中的作用中檔案伺服器），由檔案系統 RAM 或 NVMe 快取中資料提供的所有讀取請求百分比。較高百分比表示快取讀取與總讀取的比率較高。會考慮所有 I/O，包括背景任務（例如 SnapMirror、分層和備份）。您每個檔案系統的檔案伺服器每分鐘都會發出一個指標。</p> <p>單位：百分比</p> <p>Average 統計資料是檔案系統在指定期間內其中一個 HA 對的平均快取命中率。</p> <p>Minimum 統計資料是檔案系統在指定期間內其中一個 HA 對的最低快取命中率。</p> <p>Maximum 統計資料是檔案系統在指定期間內其中一個 HA 對的最高快取命中率。</p> <p>有效統計資料：Average、Minimum和Maximum</p> |

## 磁碟 I/O 指標

所有這些指標需要兩個維度，FileSystemId和Aggregate。

- FileSystemId – 檔案系統 AWS 的資源 ID。
- Aggregate – 檔案系統的效能層包含多個儲存集區，稱為彙總。每個 HA 對都有一個彙總。例如，彙總aggr1映射至 HA 對中的檔案伺服器 FsxId01234567890abcdef-01（作用中檔案伺服器）和檔案伺服器 FsxId01234567890abcdef-02（次要檔案伺服器）。

| 指標            | 描述                                          |
|---------------|---------------------------------------------|
| DiskReadBytes | 從此彙總讀取的 64 位元組數（磁碟 IO）。此指標會考慮所有流量，包括背景任務（例如 |

| 指標 | 描述                                                                                                                                                                                                                                                                                                                                      |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>SnapMirror、分層和備份 )。您每個檔案系統的彙總每分鐘都會發出一個指標。</p> <p>Sum 統計資料是指定期間內每分鐘從指定彙總讀取的位元組總數。</p> <p>Average 統計資料是指定期間內每分鐘從指定彙總讀取的平均位元組數。</p> <p>Minimum 統計資料是指定期間內每分鐘從指定彙總讀取的最低位元組數。</p> <p>Maximum 統計資料是指定期間內每分鐘從指定彙總讀取的最高位元組數。</p> <p>若要計算任何統計資料的讀取磁碟輸送量 ( 每秒位元組數 )，請將統計資料除以期間的秒數。</p> <p>單位：位元組</p> <p>有效統計資料：Sum、Minimum、Average和Maximum</p> |

| 指標             | 描述                                                                                                                                                                                                                                                                                                                                                                               |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DiskWriteBytes | <p>從任何磁碟寫入此彙總的位元組數（磁碟 IO）。此指標會考慮所有流量，包括背景任務（例如 SnapMirror、分層和備份）。您每個檔案系統的彙總每分鐘都會發出一個指標。</p> <p>Sum 統計資料是寫入指定彙總的位元組總數，在指定期間內。</p> <p>Average 統計資料是指定期間內每分鐘寫入給指定彙總的平均位元組數。</p> <p>Minimum 統計資料是指定期間內每分鐘寫入給指定彙總的最低位元組數。</p> <p>Maximum 統計資料是指定期間內每分鐘寫入給指定彙總的最高位元組數。</p> <p>若要計算任何統計資料的寫入磁碟輸送量（每秒位元組數），請將統計資料除以指定期間內的秒數。</p> <p>單位：位元組</p> <p>有效統計資料：Sum、Minimum、Average和Maximum</p> |

| 指標                  | 描述                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DiskIopsUtilization | <p>一個彙總的磁碟 IOPS 使用率，以彙總磁碟 IOPS 限制的百分比表示（即檔案系統的總 IOPS 除以檔案系統的 HA 對數）。這與不同FileServerDiskIopsUtilization之處在於，這是佈建磁碟 IOPS 相對於您佈建 IOPS 限制的使用率，而不是檔案伺服器支援的最大磁碟 IOPS（即每個 HA 對所設定的輸送量容量所決定）。此指標會考慮所有流量，包括背景任務（例如 SnapMirror、分層和備份）。您每個檔案系統的彙總每分鐘都會發出一個指標。</p> <p>Average 統計資料是指定期間內指定彙總的平均磁碟 IOPS 使用率。</p> <p>Minimum 統計資料是指定期間內指定彙總的最低磁碟 IOPS 使用率。</p> <p>Maximum 統計資訊 ii 指定期間內指定彙總的最高磁碟 IOPS 使用率。</p> <p>單位：百分比</p> <p>有效統計資料：Minimum、Average和Maximum</p> |

| 指標                 | 描述                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DiskReadOperations | <p>此彙總的讀取操作（磁碟 IO）數目。此指標會考慮所有流量，包括背景任務（例如 SnapMirror、分層和備份）。您每個檔案系統的彙總每分鐘都會發出一個指標。</p> <p>Sum 統計資料是指定彙總在指定期間內執行的讀取操作總數。</p> <p>Average 統計資料是指定彙總在指定期間內每分鐘執行的平均讀取操作數。</p> <p>Minimum 統計資料是指定彙總在指定期間內每分鐘執行的最低讀取操作數目。</p> <p>Maximum 統計資料是指定彙總在指定期間內每分鐘執行的最高讀取操作數目。</p> <p>若要計算期間內的平均磁碟 IOPS，請使用 Average 統計資料並將結果除以 60（秒）。</p> <p>單位：計數</p> <p>有效統計資料：Sum、Minimum、Average 和 Maximum</p> |

| 指標                  | 描述                                                                                                                                                                                                                                                                      |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DiskWriteOperations | <p>此彙總的寫入操作（磁碟 IO）數目。此指標會考慮所有流量，包括背景任務（例如 SnapMirror、分層和備份）。您每個檔案系統的彙總每分鐘都會發出一個指標。</p> <p>Sum 統計資料是指定彙總在指定期間內執行的寫入操作總數。</p> <p>Average 統計資料是指定彙總在指定期間內每分鐘執行的平均寫入操作數。</p> <p>若要計算期間內的平均磁碟 IOPS，請使用 Average 統計資料並將結果除以 60（秒）。</p> <p>單位：計數</p> <p>有效統計資料：Sum和 Average</p> |

## 詳細的檔案系統指標

詳細的檔案系統指標是每個儲存層的詳細儲存使用率指標。詳細的檔案系統指標具有 FileSystemId、StorageTier和 DataType維度，或 FileSystemId、DataType、StorageTier和 Aggregate維度。

- 未提供Aggregate維度時，指標適用於整個檔案系統。StorageUsed 和 StorageCapacity指標每分鐘都有單一資料點，對應於檔案系統的總消耗儲存體（每個儲存層）和總儲存體容量（適用於 SSD 層）。同時，StorageCapacityUtilization指標每分鐘會針對每個彙總發出一個指標。
- 提供Aggregate維度時，指標會用於每個彙總。

維度的意義如下：

- FileSystemId – 檔案系統 AWS 的資源 ID。
- Aggregate – 檔案系統的效能層包含多個儲存集區，稱為彙總。每個 HA 對都有一個彙總。例如，彙總aggr1映射到 HA 對中的檔案伺服器 FsxId01234567890abcdef-01（作用中檔案伺服器）和檔案伺服器 FsxId01234567890abcdef-02（次要檔案伺服器）。

- **StorageTier** – 指出指標測量的儲存層，可能的值為 SSD 和 StandardCapacityPool。
- **DataType** – 指出指標測量的資料類型，可能的值為 All。

指定指標和維度鍵值對的每個唯一組合都有一列，其中包含該組合測量項目的描述。

| 指標                         | 描述                                                                                                                                                                                                                              |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| StorageCapacityUtilization | <p>指定檔案系統彙總的儲存容量使用率。您每個檔案系統的彙總每分鐘都會發出一個指標。</p> <p>Average 統計資料是指定期間內指定彙總的平均儲存容量使用率。</p> <p>Minimum 統計資料是指定期間內指定彙總的儲存容量使用率下限。</p> <p>Maximum 統計資料是指定期間內指定彙總的儲存容量使用率上限。</p> <p>單位：百分比</p> <p>有效統計資料：Minimum、Average 和 Maximum</p> |
| StorageCapacity            | <p>指定檔案系統彙總的儲存容量。您每個檔案系統的彙總每分鐘都會發出一個指標。</p> <p>Average 統計資料是指定期間內指定彙總的平均儲存容量。</p> <p>Minimum 統計資料是指定期間內指定彙總的儲存容量下限。</p> <p>Maximum 統計資料是指定期間內指定彙總的儲存容量上限。</p> <p>單位：位元組</p>                                                     |

| 指標          | 描述                                                                                                                                                                                                                                                                                                                                                   |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             | 有效統計資料：Minimum、Average和Maximum                                                                                                                                                                                                                                                                                                                       |
| StorageUsed | <p>使用的實體儲存容量，以位元組為單位，特定於儲存層。此值包括節省儲存效率功能，例如資料壓縮和重複資料刪除。的有效維度值StorageTier 為 SSD和 StandardCapacityPool ，對應至此指標測量的儲存層。您每個檔案系統的彙總每分鐘都會發出一個指標。</p> <p>Average 統計資訊是指定儲存層在指定期間內由指定彙總耗用的平均實體儲存容量。</p> <p>Minimum 統計資訊是指定儲存層在指定期間內由指定彙總耗用的實體儲存容量下限。</p> <p>Maximum 統計資訊是指定儲存層在指定期間內由指定彙總耗用的實體儲存容量上限。</p> <p>單位：位元組</p> <p>有效統計資料：Minimum、Average和Maximum</p> |

## 磁碟區指標

您的 Amazon FSx for NetApp ONTAP 檔案系統可以有一或多個存放資料的磁碟區。每個磁碟區都有一組 CloudWatch 指標，分類為磁碟區指標或詳細磁碟區指標。

- 磁碟區指標是每個磁碟區的效能和儲存體指標，需要兩個維度，FileSystemId而VolumeId會FileSystemId映射至磁碟區所屬的檔案系統。
- 詳細磁碟區指標是per-storage-tier的指標，這些指標會使用 StorageTier 維度（可能的值為 SSD和 StandardCapacityPool）測量每個層的儲存體耗用量Snapshot，並使用 DataType維度（可能的值為 User、和）測量每個資料類型的儲存體耗用量Other。這些指標具有 FileSystemId、StorageTier、VolumeId和 DataType維度。



## 主題

- [網路 I/O 指標](#)
- [儲存容量指標](#)
- [詳細磁碟區指標](#)

## 網路 I/O 指標

所有這些指標需要兩個維度，FileSystemId和 VolumeId。

| 指標                 | 描述                                                                                                                                            |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| DataReadBytes      | <p>用戶端從磁碟區讀取的位元組數（網路 I/O）。</p> <p>Sum 統計資料是指定期間內與讀取操作相關聯的位元組總數。若要計算期間的平均輸送量（每秒位元組數），請將Sum統計資料除以指定期間內的秒數。</p> <p>單位：位元組</p> <p>有效的統計資訊：Sum</p> |
| DataWriteBytes     | <p>用戶端寫入磁碟區的位元組數（網路 I/O）。</p> <p>Sum 統計資料是指定期間內與寫入操作相關聯的位元組總數。若要計算期間的平均輸送量（每秒位元組數），請將Sum統計資料除以指定期間內的秒數。</p> <p>單位：位元組</p> <p>有效的統計資訊：Sum</p>  |
| DataReadOperations | <p>用戶端在磁碟區上的讀取操作（網路 I/O）數目。</p> <p>Sum 統計資料是指定期間內讀取操作的總數。若要計算期間每秒的平均讀取操作，請將Sum統計資料除以指定期間內的秒數。</p>                                             |

| 指標                    | 描述                                                                                                                                                                      |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <p>單位：計數</p> <p>有效的統計資訊：Sum</p>                                                                                                                                         |
| DataWriteOperations   | <p>用戶端在磁碟區上的寫入操作（網路 I/O）數目。</p> <p>Sum 統計資料是指定期間內寫入操作的總數。若要計算期間每秒的平均寫入操作，請將Sum統計資料除以指定期間內的秒數。</p> <p>單位：計數</p> <p>有效的統計資訊：Sum</p>                                       |
| MetadataOperations    | <p>用戶端從中繼資料活動到磁碟區的 I/O 操作（網路 I/O）數目。</p> <p>Sum 統計資料是指定期間內中繼資料操作的總數。若要計算一段時間內每秒的平均中繼資料操作，請將Sum統計資料除以指定期間內的秒數。</p> <p>單位：計數</p> <p>有效的統計資訊：Sum</p>                       |
| DataReadOperationTime | <p>從存取磁碟區中資料的用戶端讀取操作（網路 I/O）在磁碟區內花費的總時間總和。</p> <p>Sum 統計資料是讀取操作在指定期間內所花費的總秒數。若要計算期間的平均讀取延遲，請將Sum統計資料除以相同期間的SumDataReadOperations 指標。</p> <p>單位：秒</p> <p>有效的統計資訊：Sum</p> |

| 指標                     | 描述                                                                                                                                                                                   |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DataWriteOperationTime | <p>在磁碟區中完成寫入操作（網路 I/O）所花費的總時間總和，此寫入操作來自存取磁碟區中資料的用戶端。</p> <p>Sum 統計資料是寫入操作在指定期間內所花費的總秒數。若要計算期間的平均寫入延遲，請將Sum統計資料除以相同期間的 Sum DataWriteOperations 指標。</p> <p>單位：秒</p> <p>有效的統計資訊：Sum</p> |
| MetadataOperationTime  | <p>磁碟區中用於從存取磁碟區中資料的用戶端完成中繼資料操作（網路 I/O）的總時間總和。</p> <p>Sum 統計資料是讀取操作在指定期間內所花費的總秒數。若要計算期間的平均延遲，請將統計資料除以SumMetadataOperations 相同期間的 Sum。</p> <p>單位：秒</p> <p>有效的統計資訊：Sum</p>              |

| 指標                         | 描述                                                                                                                                                                                                       |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CapacityPoolReadBytes      | <p>從磁碟區的容量集區層讀取的位元組數（網路 I/O）。</p> <p>為了確保資料完整性，ONTAP 會在執行寫入操作後立即對容量集區執行讀取操作。</p> <p>Sum 統計資料是指定期間內從磁碟區容量集區層讀取的位元組總數。若要計算每秒的容量集區位元組，請將Sum統計資料除以指定期間內的秒數。</p> <p>單位：位元組</p> <p>有效的統計資訊：Sum</p>             |
| CapacityPoolReadOperations | <p>來自磁碟區容量集區層的讀取操作（網路 I/O）數目。這會轉換為容量集區讀取請求。</p> <p>為了確保資料完整性，ONTAP 會在執行寫入操作後立即對容量集區執行讀取操作。</p> <p>Sum 統計資料是指定期間內來自磁碟區容量集區層的讀取操作總數。若要計算每秒的容量集區請求，請將Sum統計資料除以指定期間內的秒數。</p> <p>單位：計數</p> <p>有效的統計資訊：Sum</p> |

| 指標                          | 描述                                                                                                                                                                                                 |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CapacityPoolWriteBytes      | <p>寫入磁碟區容量集區層的位元組數（網路 I/O）。</p> <p>為了確保資料完整性，ONTAP 會在執行寫入操作後立即對容量集區執行讀取操作。</p> <p>Sum 統計資料是寫入磁碟區容量集區層的位元組總數，在指定的期間內。若要計算每秒的容量集區位元組，請將Sum統計資料除以指定期間內的秒數。</p> <p>單位：位元組</p> <p>有效的統計資訊：Sum</p>       |
| CapacityPoolWriteOperations | <p>從容量集區層到磁碟區的寫入操作（網路 I/O）數目。這會轉換為寫入請求。</p> <p>為了確保資料完整性，ONTAP 會在執行寫入操作後立即對容量集區執行讀取操作。</p> <p>Sum 統計資料是指定期間內磁碟區容量集區層的寫入操作總數。若要計算每秒的容量集區請求，請將Sum統計資料除以指定期間內的秒數。</p> <p>單位：計數</p> <p>有效的統計資訊：Sum</p> |

## 儲存容量指標

所有這些指標需要兩個維度，FileSystemId和 VolumeId。

| 指標              | 描述              |
|-----------------|-----------------|
| StorageCapacity | 磁碟區的大小，以位元組為單位。 |

| 指標                         | 描述                                                       |
|----------------------------|----------------------------------------------------------|
|                            | 單位：位元組<br><br>有效的統計資訊：Maximum                            |
| StorageUsed                | 磁碟區使用的邏輯儲存容量。<br><br>單位：位元組<br><br>有效的統計資訊：Average       |
| StorageCapacityUtilization | 磁碟區的儲存容量使用率。<br><br>單位：百分比<br><br>有效的統計資訊：Average        |
| FilesUsed                  | 磁碟區上使用的檔案（檔案或索引的數量）。<br><br>單位：計數<br><br>有效的統計資訊：Average |
| FilesCapacity              | 可在磁碟區上建立的索引總數。<br><br>單位：計數<br><br>有效的統計資訊：Maximum       |

## 詳細磁碟區指標

詳細的磁碟區指標需要的維度比磁碟區指標更多，可讓您更精細地測量資料。所有詳細磁碟區指標都有維度 `FileSystemId`、`StorageTier`、`VolumeId`和 `DataType`。

- `StorageTier` 維度指出指標測量的儲存層，可能的值為 `All`、`SSD`和 `StandardCapacityPool`。
- `DataType` 維度指出指標測量的資料類型，可能的值為 `All`、`User`、`Snapshot`和 `Other`。

下表定義列出維度的 `StorageUsed` 指標測量。

| 指標                         | 描述                                                                                                                                                                                                                                                                                                                              |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| StorageUsed                | <p>使用的邏輯空間量，以位元組為單位。此指標會根據此指標使用的維度，測量不同類型的空間耗用。將 StorageTier 設定為 SSD 或 StandardCapacityPool，並將 DataType 設定為 All，此指標會分別測量 SSD 和容量集區層此磁碟區的邏輯空間使用量。將 DataType 維度設定為 User、Snapshot 或 Other，並將 StorageTier 設定為 All，此指標會測量每種個別資料類型的邏輯空間用量。Snapshot 資料耗用包括快照預留，預設是磁碟區大小的 5%。</p> <p>單位：位元組</p> <p>有效統計資料：Minimum、Average 和 Maximum</p> |
| StorageCapacityUtilization | <p>磁碟區已使用實體磁碟空間的百分比。</p> <p>單位：百分比</p> <p>有效的統計資訊：Maximum</p>                                                                                                                                                                                                                                                                   |

## 監控 FSx 的 ONTAP EMS 事件

您可以使用 NetApp ONTAP 的原生事件管理系統 (EMS) 監控 FSx 的 ONTAP 檔案系統事件。您可以使用 NetApp ONTAP CLI 檢視這些事件。

### 主題

- [EMS 事件概觀](#)
- [檢視 EMS 事件](#)
- [將 EMS 事件轉送至 Syslog 伺服器](#)

## EMS 事件概觀

EMS 事件會自動產生通知，在 FSx for ONTAP 檔案系統中發生預先定義的條件時提醒您。這些通知會通知您，以便您可以防止或修正可能導致較大問題的問題，例如儲存虛擬機器 (SVM) 身分驗證問題或完整磁碟區。

根據預設，事件會記錄在事件管理系統日誌中。使用 EMS，您可以監控事件，例如使用者密碼變更、FlexGroup 內接近完整容量的組份、邏輯單位號碼 (LUN) 已手動上線或離線，或磁碟區自動調整大小。

如需 ONTAP EMS 事件的詳細資訊，請參閱 NetApp [ONTAP 文件中心中的 ONTAP EMS 參考](#)。若要顯示事件類別，請使用文件的左側導覽窗格。

### Note

FSx for ONTAP 檔案系統只能使用一些 ONTAP EMS 訊息。若要檢視可用的 ONTAP EMS 訊息清單，請使用 NetApp ONTAP CLI [事件目錄 show](#) 命令。

EMS 事件描述包含事件名稱、嚴重性、可能的原因、日誌訊息和修正動作，可協助您決定如何回應。例如，當磁碟區的自動調整大小失敗時，會發生 [wafl.vol.autoSize.fail](#) 事件。根據事件描述，修正動作是在設定自動調整大小時增加磁碟區的大小上限。

## 檢視 EMS 事件

使用 NetApp ONTAP CLI [事件日誌 show](#) 命令來顯示事件日誌的內容。如果您在檔案系統上具有 fsxadmin 角色，即可使用此命令。命令語法如下所示：

```
event log show [event_options]
```

首先列出最新的事件。根據預設，此命令會顯示具有下列資訊的 ALERT、EMERGENCY 和 ERROR 嚴重性層級事件：

- 時間 – 事件的時間。
- 節點 – 事件發生的節點。
- 嚴重性 – 事件的嚴重性層級。若要顯示 NOTICE、INFORMATIONAL 或 DEBUG 嚴重性層級事件，請使用 `-severity` 選項。
- 事件 – 事件名稱和訊息。



若要顯示事件的詳細資訊，請使用下表所列的一或多個事件選項。

| 事件選項                             | 描述                                                                                                                                                                                                                                                                       |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -detail                          | 顯示其他事件資訊。                                                                                                                                                                                                                                                                |
| -detailtime                      | 以反向時間順序顯示詳細事件資訊。                                                                                                                                                                                                                                                         |
| -instance                        | 顯示所有欄位的詳細資訊。                                                                                                                                                                                                                                                             |
| -node <i>nodename</i>   local    | 顯示您指定節點的事件清單。使用此選項搭配 -seqnum 顯示詳細資訊。                                                                                                                                                                                                                                     |
| -seqnum <i>sequence_number</i>   | 選取符合序列中此數字的事件。使用 搭配 -node 顯示詳細資訊。                                                                                                                                                                                                                                        |
| -time <i>MM/DD/YYYY HH:MM:SS</i> | <p>選取在此特定時間發生的事件。使用格式：MM/DD/YY YY HH : MM : SS 【+- HH : MM】。您可以在兩個時間陳述式之間使用 .. 運算子來指定時間範圍。</p> <pre>event log show - time "04/17/2023 05:55:00".."04/17/ 2023 06:10:00"</pre> <p>比較時間值是相對於執行 命令時的目前時間。下列範例顯示如何僅顯示最後一分鐘內發生的事件：</p> <pre>event log show -time &gt;1m</pre> |

| 事件選項                                    | 描述                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                         | 此選項的月份和日期欄位不是零填充。這些欄位可以是單一數字；例如 4/1/2023 06:45:00。                                                                                                                                                                                                                                                                |
| <code>-severity <i>sev_level</i></code> | <p>選取符合 <i>sev_level</i> 值的事件，其必須是下列其中一項：</p> <ul style="list-style-type: none"><li>• EMERGENCY – 中斷</li><li>• ALERT – 單一故障點</li><li>• ERROR – 降級</li><li>• NOTICE – 資訊</li><li>• INFORMATIONAL – 資訊</li><li>• DEBUG – 偵錯資訊</li></ul> <p>若要顯示所有事件，請指定嚴重性，如下所示：</p> <pre>event log show -severity &lt;=DEBUG</pre> |

| 事件選項                                            | 描述                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-ems-severity <i>ems_sev_level</i></code> | <p>選取符合 <i>ems_sev_level</i> 值的事件，其必須為下列其中一項：</p> <ul style="list-style-type: none"> <li>• <code>NODE_FAULT</code> – 偵測到資料損毀或節點無法提供用戶端服務。</li> <li>• <code>SVC_FAULT</code> – 偵測到暫時性的服務損失，通常是暫時性軟體故障。</li> <li>• <code>NODE_ERROR</code> – 偵測到未立即導致致命的硬體錯誤。</li> <li>• <code>SVC_ERROR</code> – 偵測到未立即導致死亡的軟體錯誤。</li> <li>• <code>WARNING</code> – 未指出故障的高優先順序訊息。</li> <li>• <code>NOTICE</code> – 未指出故障的正常優先順序訊息。</li> <li>• <code>INFO</code> – 不表示故障的低優先順序訊息。</li> <li>• <code>DEBUG</code> – 除錯訊息。</li> <li>• <code>VAR</code> – 在執行時間選取具有變數嚴重性的訊息。</li> </ul> <p>若要顯示所有事件，請指定嚴重性，如下所示：</p> <pre>event log show -ems-severity &lt;=DEBUG</pre> |
| <code>-source <i>text</i></code>                | <p>選取符合 <i>##</i> 值的事件。來源通常是軟體模組。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| 事件選項                                               | 描述                                                             |
|----------------------------------------------------|----------------------------------------------------------------|
| <code>-message-name</code> <i>message_name</i>     | 選取符合 <i>message_name</i> 值的事件。訊息名稱是描述性的，因此依訊息名稱篩選輸出會顯示特定類型的訊息。 |
| <code>-event</code> <i>text</i>                    | 選取符合##值的事件。event 欄位包含事件的完整文字，包括任何參數。                           |
| <code>-kernel-generation-num</code> <i>integer</i> | 選取符合##值的事件。只有來自核心的事件具有核心產生數字。                                  |
| <code>-kernel-sequence-num</code> <i>integer</i>   | 選取符合##值的事件。只有來自核心的事件具有核心序號。                                    |
| <code>-action</code> <i>text</i>                   | 選取符合##值的事件。action 欄位說明如果有的話，您必須採取哪些修正動作來修正情況。                  |
| <code>-description</code> <i>text</i>              | 選取符合##值的事件。description 欄位說明事件發生的原因及其意義。                        |
| <code>-filter-name</code> <i>filter_name</i>       | 選取符合 <i>filter_name</i> 值的事件。只有符合此值的現有篩選條件所包含的事件才會顯示。          |
| <code>-fields</code> <i>fieldname</i> , ...        | 表示命令輸出也包含指定的欄位。您可以使用 <code>-fields ?</code> 來選擇您要指定的欄位。        |

## 檢視 EMS 事件

- 若要將 SSH 插入檔案系統的 NetApp ONTAP CLI，請遵循 Amazon FSx for NetApp ONTAP 使用者指南 [使用 NetApp ONTAP CLI](#) 一節中記錄的步驟。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

- 使用 `event log show` 命令來顯示事件日誌的內容。

```
::> event log show
Time                Node                Severity            Event
-----
6/30/2023 13:54:19  node1              NOTICE            vifmgr.portup: A link up event was
received on node node1, port e0a.
6/30/2023 13:54:19  node1              NOTICE            vifmgr.portup: A link up event was
received on node node1, port e0d.
```

如需 `event log show` 命令傳回之 EMS 事件的相關資訊，請參閱 NetApp [ONTAP 文件中心中的 ONTAP EMS 參考](#)。

## 將 EMS 事件轉送至 Syslog 伺服器

您可以設定 EMS 事件，將通知轉送至 Syslog 伺服器。EMS 事件轉送用於即時監控檔案系統，以判斷和隔離各種問題的根本原因。如果您的環境尚未包含事件通知的 Syslog 伺服器，您必須先建立一個伺服器。DNS 必須在檔案系統上設定，才能解析 Syslog 伺服器名稱。

### Note

您的 Syslog 目的地必須位於檔案系統使用的主要子網路中。

## 設定 EMS 事件將通知轉送至 Syslog 伺服器

- 若要將 SSH 插入檔案系統的 NetApp ONTAP CLI，請遵循 Amazon FSx for NetApp ONTAP 使用者指南 [使用 NetApp ONTAP CLI](#) 一節中記錄的步驟。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

- 使用 [事件通知目的地建立](#) 命令來建立類型的事件通知目的地 `syslog`，指定下列屬性：

- *dest\_name* – 要建立的通知目的地名稱 (例如 syslog-ems)。事件通知目的地名稱長度必須為 2 到 64 個字元。有效字元包括下列 ASCII 字元：A-Z、a-z、0-9、"\_" 和 "-"。名稱的開頭和結尾必須是：A-Z、a-z 或 0-9。
- *syslog\_name* – 傳送 Syslog 訊息的 Syslog 伺服器主機名稱或 IP 地址。
- *transport\_protocol* – 用來傳送事件的通訊協定：
  - udp-unencrypted – 無安全性的使用者資料包通訊協定。這是預設通訊協定。
  - tcp-unencrypted – 無安全性的傳輸控制通訊協定。
  - tcp-encrypted – 具有 Transport Layer Security (TLS) 的傳輸控制通訊協定。指定此選項時，FSx for ONTAP 會透過驗證其憑證來驗證目的地主機的身分。
- *port\_number* – 傳送 Syslog 訊息的 Syslog 伺服器連接埠。預設值 syslog-port 參數取決於 syslog-transport 參數的設定。如果 syslog-transport 設定為 tcp-encrypted，syslog-port 則預設值為 6514。如果 syslog-transport 設定為 tcp-unencrypted，則 syslog-port 具有預設值 601。否則，預設連接埠會設為 514。

```
::> event notification destination create -name dest_name -syslog syslog_name -
syslog-transport transport_protocol -syslog-port port_number
```

3. 使用 [事件通知建立](#) 命令，為事件篩選條件定義的一組事件建立新的通知，傳送至上一個步驟中建立的通知目的地，並指定下列屬性：

- *node\_name* – 事件篩選條件的名稱。包含在事件篩選條件中的事件會轉送至 -destinations 參數中指定的目的地。
- *dest\_name* – 傳送事件通知的現有通知目的地名稱。

```
::> event notification create -filter-name filter_name -destinations dest_name
```

4. 如果您選取 TCP 做為 *transport\_protocol*，您可以使用 event notification destination check 命令產生測試訊息，並驗證您的設定是否有效。使用 命令指定下列屬性：

- *node\_name* – 節點的名稱 (例如 FsxId07353f551e6b557b4-01)。
- *dest\_name* – 傳送事件通知的現有通知目的地名稱。

```
::> set diag
```

```
::*> event notification destination check -node node_name -destination-  
name dest_name
```

## 使用資料基礎設施洞見進行監控

NetApp Data Infrastructure Insights ( 先前稱為 Cloud Insights) 是一種 NetApp 服務，可用來監控 Amazon FSx for NetApp ONTAP 檔案系統，以及其他 NetApp 儲存解決方案。透過 Data Infrastructure Insights，您可以監控組態、容量和效能指標，以了解工作負載的趨勢，並規劃未來的效能和儲存容量需求。您也可以根據可與現有工作流程和生產力工具整合的指標條件來建立提醒。

### Note

具有多個 HA 對的第二代檔案系統不支援 Data Infrastructure Insights。

Data Infrastructure Insights 提供：

- 指標和日誌的廣度 – 收集組態、容量和效能指標。透過預先定義的儀表板、警示和報告，了解工作負載的趨勢。
- 使用者分析和勒索軟體保護 – 透過 Cloud Secure 和 ONTAP 快照，您可以稽核、偵測、停止和修復使用者錯誤和勒索軟體的事件。
- SnapMirror 報告 – 了解您的 SnapMirror 關係，並設定複寫問題的提醒。
- 容量規劃 – 了解現場部署工作負載的資源需求，協助您將工作負載遷移至更有效率的 FSx for ONTAP 組態。您也可以使用這些洞見來規劃 FSx for ONTAP 部署何時需要更多效能或容量。

如需詳細資訊，請參閱 NetApp ONTAP 產品[文件中的資料基礎設施洞見](#)文件。

## 使用 Harvest 和 Grafana 監控 ONTAP 檔案系統的 FSx

NetApp Harvest 是一種開放原始碼工具，用於從 ONTAP 系統收集效能和容量指標，並與 FSx for ONTAP 相容。您可以使用 Harvest 搭配 Grafana 進行開放原始碼監控解決方案。

### Harvest 和 Grafana 入門

下一節詳細說明如何設定和設定 Harvest 和 Grafana，以測量 FSx for ONTAP 檔案系統的效能和儲存容量使用率。

您可以使用 Harvest 和 來監控 Amazon FSx for NetApp ONTAP 檔案系統 Grafana。透過從 FSx for ONTAP 檔案系統收集效能、容量和硬體指標來 NetApp Harvest 監控 ONTAP 資料中心。Grafana 提供儀表板，其中會顯示收集的 Harvest 指標。

## 支援的 Harvest 儀表板

Amazon FSx for NetApp ONTAP 會公開一組不同於內部部署 的指標 NetApp ONTAP。因此，fsx 目前僅支援使用 標記的下列 out-of-the-box Harvest 儀表板與 FSx for ONTAP 搭配使用。這些儀表板中的某些面板可能缺少不支援的資訊。

- 收成：中繼資料
- ONTAP：cDOT
- ONTAP：叢集
- ONTAP：合規
- ONTAP：資料中心
- ONTAP：資料保護快照
- ONTAP：LUN
- ONTAP：節點
- ONTAP：Qtree
- ONTAP：安全性
- ONTAP：SnapMirror
- ONTAP：SVM
- ONTAP：磁碟區

FSx for ONTAP 支援下列 Harvest 儀表板，但在 中預設不會啟用 Harvest。

- ONTAP：FlexCache
- ONTAP：FlexGroup
- ONTAP：NFS 用戶端
- ONTAP：NFSv4 Storepool 監視器
- ONTAP：NFS 故障診斷
- ONTAP：SMB
- ONTAP：工作負載



## 不支援的Harvest儀表板

FSx for ONTAP 不支援下列Harvest儀表板。

- ONTAP：彙總
- ONTAP：磁碟
- ONTAP：外部服務操作
- ONTAP：File Systems Analytics (FSA)
- ONTAP：運作狀態
- ONTAP：MetroCluster
- ONTAP：Power
- ONTAP：層架
- ONTAP：S3 物件存放區

## AWS CloudFormation 範本

若要開始使用，您可以部署 AWS CloudFormation 範本，自動啟動執行 Harvest 和 Grafana 的 Amazon EC2 執行個體。作為 AWS CloudFormation 範本的輸入，您可以指定檔案系統fsxadmin的使用者和 Amazon FSx 管理端點，這些端點將新增為此部署的一部分。部署完成後，您可以登入 Grafana 儀表板來監控您的檔案系統。

此解決方案使用 AWS CloudFormation 自動部署 Harvest 和 Grafana 解決方案。範本會建立 Amazon EC2 Linux 執行個體，並安裝 Harvest 和 Grafana 軟體。若要使用此解決方案，請下載 [fsx-ontap-harvest-grafana.template](#) AWS CloudFormation 範本。

### Note

實作此解決方案會產生相關聯 AWS 服務的帳單。如需詳細資訊，請參閱這些服務的定價詳細資訊頁面。

## Amazon EC2 執行個體類型

設定範本時，您會提供 Amazon EC2 執行個體類型。NetApp 的執行個體大小建議取決於您監控的檔案系統數量，以及您選擇收集的指標數量。使用預設組態，對於您監控的每個 10 個檔案系統，NetApp 建議：

- CPU：2 個核心
- 記憶體：1 GB
- 磁碟：500 MB（主要由日誌檔案使用）

以下是一些範例組態和您可以選擇的 t3 執行個體類型。

| 檔案系統  | CPU   | Disk    | 執行個體類型     |
|-------|-------|---------|------------|
| 10 以下 | 2 個核心 | 500 MB  | t3.micro   |
| 10–40 | 4 個核心 | 1000 MB | t3.xlarge  |
| 40+   | 8 個核心 | 2000 MB | t3.2xlarge |

如需 Amazon EC2 執行個體類型的詳細資訊，請參閱《Amazon EC2 使用者指南》中的 [一般用途執行個體](#)。

## 執行個體連接埠規則

當您設定 Amazon EC2 執行個體時，請確定連接埠 3000 和 9090 已開放給 Amazon EC2 Harvest 和 Grafana 執行個體所在的安全群組的傳入流量。由於啟動的執行個體會透過 HTTPS 連線至端點，因此需要解析端點，而該端點需要連接埠 53 TCP/UDP 才能用於 DNS。此外，若要到達端點，它需要連接埠 443 TCP 才能進行 HTTPS 和網際網路存取。

## 部署程序

下列程序會設定和部署 Harvest/Grafana 解決方案。部署大約需要五分鐘的時間。開始之前，您必須在 AWS 帳戶中的 Amazon Virtual Private Cloud (Amazon VPC) 中執行 FSx for ONTAP 檔案系統，以及下列範本的參數資訊。如需建立檔案系統的詳細資訊，請參閱 [建立檔案系統](#)。

### 啟動 Harvest/Grafana 解決方案堆疊

1. 下載 [fsx-ontap-harvest-grafana.template](#) AWS CloudFormation 範本。如需建立 AWS CloudFormation 堆疊的詳細資訊，請參閱 AWS CloudFormation 《使用者指南》中的 [在 AWS CloudFormation 主控台上建立堆疊](#)。

**Note**

根據預設，此範本會在美國東部（維吉尼亞北部）AWS 區域啟動。您必須在可使用 Amazon FSx AWS 區域的中啟動此解決方案。如需詳細資訊，請參閱中的 [Amazon FSx 端點和配額](#) AWS 一般參考。

2. 對於 參數，請檢閱範本的參數，並根據檔案系統的需求修改它們。此解決方案使用下列預設值。

| 參數            | 預設       | 描述                                                                                                                                                                                                                                                                                    |
|---------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| InstanceType  | t3.micro | <p>Amazon EC2 執行個體類型。以下是 t3 執行個體類型。</p> <ul style="list-style-type: none"><li>• t3.micro</li><li>• t3.small</li><li>• t3.medium</li><li>• t3.large</li><li>• t3.xlarge</li><li>• t3.2xlarge</li></ul> <p>如需此參數允許之 Amazon EC2 執行個體類型值的完整清單，請參閱 fsx-ontap-harvest-grafana.template。</p> |
| KeyPair       | 無預設值     | 用來存取 Amazon EC2 執行個體的金鑰對。                                                                                                                                                                                                                                                             |
| SecurityGroup | 無預設值     | Harvest/Grafana 執行個體的安全群組 ID。除了連接埠 53 和 443 之外，請確定傳入連接埠 3000 和 9090 已開啟您要用來存取 Grafana 儀表板的用戶端。                                                                                                                                                                                        |

| 參數               | 預設                                                            | 描述                                                                                                                           |
|------------------|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| 子網路類型            | 無預設值                                                          | 指定子網路類型，public或private。將public子網路用於必須連接到網際網路的資源，並將私有子網路用於不會連接到網際網路的資源。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 <a href="#">子網路類型</a> 。 |
| 子網路              | 無預設值                                                          | 指定與 Amazon FSx for NetApp ONTAP 檔案系統偏好的子網路相同的子網路。您可以在 Amazon FSx 主控台的 FSx for ONTAP 檔案系統詳細資訊頁面的網路與安全索引標籤中找到檔案系統的偏好子網路 ID     |
| LatestLinuxAmild | /aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2 | 特定中 Amazon Linux 2 AMI 的最新版本 AWS 區域。                                                                                         |
| FSxEndPoint      | 無預設值                                                          | 檔案系統的管理端點 IP 地址。您可以在 Amazon FSx 主控台的 FSx for ONTAP 檔案系統詳細資訊頁面的管理索引標籤中找到檔案系統的管理端點 IP 地址。                                      |
| SecretName       | 無預設值                                                          | AWS Secrets Manager 包含檔案系統fsxadmin使用者密碼的秘密名稱。這是您在建立檔案系統時所提供的密碼。                                                              |

### 3. 選擇 Next (下一步)。

4. 針對選項，選擇下一步。
5. 針對檢閱，檢閱並確認設定。您必須選取確認範本建立 IAM 資源的核取方塊。
6. 選擇建立以部署堆疊。

您可以在狀態欄的 AWS CloudFormation 主控台中檢視堆疊的狀態。您應該會在大約五分鐘內看到 CREATE\_COMPLETE 狀態。

## 登入 Grafana

部署完成後，請使用您的瀏覽器登入 Amazon EC2 執行個體 IP 和連接埠 3000 的 Grafana 儀表板：

```
http://EC2_instance_IP:3000
```

出現提示時，請使用 Grafana 預設使用者名稱 (admin) 和密碼 (pass)。我們建議您在登入後立即變更密碼。

如需詳細資訊，請參閱 GitHub 上的 [NetApp Harvest](#) 頁面。

## 針對 Harvest 和 Grafana 進行故障診斷

如果您遇到 Harvest 和 Grafana 儀表板中提及的任何遺失資料，或無法透過 FSx for ONTAP 設定 Harvest 和 Grafana，請檢查下列主題是否有潛在解決方案。

### 主題

- [SVM 和磁碟區儀表板空白](#)
- [CloudFormation 堆疊會在逾時後復原](#)

## SVM 和磁碟區儀表板空白

如果 AWS CloudFormation 堆疊部署成功，並且可以聯絡 Grafana，但 SVM 和磁碟區儀表板空白，請使用下列程序來疑難排解您的環境。您需要對部署 Harvest 和 Grafana 的 Amazon EC2 執行個體進行 SSH 存取。

1. Amazon EC2 執行個體中的 SSH，您的 Harvest 和 Grafana 用戶端正在其上執行。

```
[~]$ ssh ec2-user@ec2_ip_address
```

## 2. 使用下列命令來開啟 `harvest.yml` 檔案和：

- 確認已為您的 FSx for ONTAP 執行個體建立項目，做為 Cluster-2。
- 確認使用者名稱和密碼的項目與您的 `fsxadmin` 登入資料相符。

```
[ec2-user@ip-ec2_ip_address ~]$ sudo cat /home/ec2-user/harvest_install/harvest/harvest.yml
```

## 3. 如果密碼欄位為空白，請在編輯器中開啟 檔案，並使用 `fsxadmin` 密碼更新檔案，如下所示：

```
[ec2-user@ip-ec2_ip_address ~]$ sudo vi /home/ec2-user/harvest_install/harvest/harvest.yml
```

## 4. 確保 `fsxadmin` 使用者登入資料以下列格式存放在 Secrets Manager 中，以供任何未來部署使用，`fsxadmin_password` 並以您的密碼取代。

```
{"username" : "fsxadmin", "password" : "fsxadmin_password"}
```

## CloudFormation 堆疊會在逾時後復原

如果您無法成功部署 CloudFormation 堆疊，且其正在轉返並發生錯誤，請使用下列程序來解決問題。您需要對 CloudFormation 堆疊部署的 EC2 執行個體進行 SSH 存取。

1. 重新部署 CloudFormation 堆疊，確保停用自動復原。
2. Amazon EC2 執行個體中的 SSH，您的 Harvest 和 Grafana 用戶端正在其上執行。

```
[~]$ ssh ec2-user@ec2_ip_address
```

## 3. Verify 表示已成功使用下列命令啟動 Docker 容器。

```
[ec2-user@ip-ec2_ip_address ~]$ sudo docker ps
```

在回應中，您應該會看到五個容器，如下所示：

| CONTAINER ID  | IMAGE                 | COMMAND                  | CREATED           |
|---------------|-----------------------|--------------------------|-------------------|
| 6b9b3f2085ef  | rahulguptajss/harvest | "bin/poller --config..." | 8 minutes ago     |
| Restating (1) | 20 seconds ago        |                          | harvest_cluster-2 |

```

3cf3e3623fde  rahulguptajss/harvest  "bin/poller --config..."  8 minutes ago  Up
About a minute                                harvest_cluster-1
708f3b7ef6f8  grafana/grafana        "/run.sh"                8 minutes ago  Up
8 minutes                                0.0.0.0:3000->3000/tcp  harvest_grafana
0febee61cab7  prom/alertmanager      "/bin/alertmanager -..."  8
minutes ago  Up 8 minutes                                0.0.0.0:9093->9093/tcp
harvest_prometheus_alertmanager
1706d8cd5a0c  prom/prometheus        "/bin/prometheus --c..."  8 minutes ago  Up
8 minutes                                0.0.0.0:9090->9090/tcp  harvest_prometheus

```

4. 如果 Docker 容器未執行，請檢查/var/log/cloud-init-output.log檔案中是否有失敗，如下所示。

```

[ec2-user@ip-ec2_ip_address ~]$ sudo cat /var/log/cloud-init-output.log
PLAY [Manage Harvest]
*****

TASK [Gathering Facts] *****
ok: [localhost]

TASK [Verify images] *****
failed: [localhost] (item=prom/prometheus) => {"ansible_loop_var": "item",
"changed": false, "item": "prom/prometheus",
"msg": "Error connecting: Error while fetching server API version: ('Connection
aborted.', ConnectionResetError(104, 'Co
nnection reset by peer'))"}
failed: [localhost] (item=prom/alertmanager) => {"ansible_loop_var": "item",
"changed": false, "item": "prom/alertmanag
er", "msg": "Error connecting: Error while fetching server API version: ('Connection
aborted.', ConnectionResetError(104,
'Connection reset by peer'))"}
failed: [localhost] (item=rahulguptajss/harvest) => {"ansible_loop_var": "item",
"changed": false, "item": "rahulguptajs
s/harvest", "msg": "Error connecting: Error while fetching server API version:
('Connection aborted.', ConnectionResetEr
ror(104, 'Connection reset by peer'))"}
failed: [localhost] (item=grafana/grafana) => {"ansible_loop_var": "item",
"changed": false, "item": "grafana/grafana",
"msg": "Error connecting: Error while fetching server API version: ('Connection
aborted.', ConnectionResetError(104, 'Co
nnection reset by peer'))"}

PLAY RECAP *****

```

```
localhost : ok=1 changed=0 unreachable=0 failed=1
skipped=0 rescued=0 ignored=0
```

5. 如果失敗，請執行下列命令來部署 Harvest 和 Grafana 容器。

```
[ec2-user@ip-ec2_ip_address ~]$ sudo su
[ec2-user@ip-ec2_ip_address ~]$ cd /home/ec2-user/harvest_install
[ec2-user@ip-ec2_ip_address ~]$ /usr/local/bin/ansible-playbook
manage_harvest.yml
[ec2-user@ip-ec2_ip_address ~]$ /usr/local/bin/ansible-playbook
manage_harvest.yml --tags api
```

6. 透過執行 `sudo docker ps` 並連線至您的 Harvest 和 Grafana URL，驗證容器已成功啟動。

## 使用 監控 FSx 的 ONTAP API 呼叫 AWS CloudTrail

Amazon FSx 已與 整合 AWS CloudTrail，此服務提供 Amazon FSx AWS 中使用者、角色或服務所採取動作的記錄。CloudTrail 會將 Amazon FSx for NetApp ONTAP 的所有 Amazon FSx API 呼叫擷取為事件。擷取的呼叫包括從 Amazon FSx 主控台和從程式碼呼叫到 Amazon FSx API 操作的呼叫。

如果您建立線索，您可以啟用 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 Amazon FSx 的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台的事件歷史記錄檢視最新事件。您可以使用 CloudTrail 收集的資訊，判斷對 Amazon FSx 提出的請求。您還可以判斷提出請求的來源 IP 地址、提出請求的人員和時間以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱 [「AWS CloudTrail 使用者指南」](#)。

## CloudTrail 中的 Amazon FSx 資訊

當您建立 AWS 帳戶時，您的帳戶會啟用 CloudTrail。當 API 活動在 Amazon FSx 中發生時，該活動會記錄在 CloudTrail 事件中，以及事件歷史記錄中的其他服務 AWS 事件。您可以在 AWS 帳戶中檢視、搜尋和下載最近的事件。如需詳細資訊，請參閱 [「使用 CloudTrail 事件歷史記錄檢視事件」](#)。

若持續記錄您 AWS 帳戶中的事件，包括 Amazon FSx 的事件，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。根據預設，當您在主控台中建立追蹤時，追蹤會套用至所有 AWS 區域。追蹤會記錄 AWS 分割區中所有 AWS 區域的事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析 CloudTrail 日誌中收集的事件資料並對其採取行動。如需詳細資訊，請參閱《AWS CloudTrail 使用者指南》中的以下主題：

- [為您的 建立追蹤 AWS 帳戶](#)



- [AWS 服務與 CloudTrail Logs 的整合](#)
- [設定 CloudTrail 的 Amazon SNS 通知](#)
- [接收多個區域的 CloudTrail 日誌檔案](#)和[接收多個帳戶的 CloudTrail 日誌檔案](#)

CloudTrail 會記錄所有 Amazon FSx [API 呼叫](#)。例如，對 CreateFileSystem 和 TagResource 操作的呼叫都會在 CloudTrail 日誌檔案中產生項目。

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

- 請求是否使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出。
- 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《使用者指南》中的 [CloudTrail userIdentity 元素](#)。AWS CloudTrail

## 了解 Amazon FSx 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔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。

下列範例顯示的 CloudTrail 日誌項目，示範從主控台建立之檔案系統標籤時的 TagResource 操作。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:sts::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-11-14T22:36:07Z"
      }
    }
  },
  }
```

```

    "eventTime": "2018-11-14T22:36:07Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789"
    },
    "responseElements": null,
    "requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
    "eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": "111122223333"
}

```

下列範例顯示的 CloudTrail 日誌項目，示範從主控台刪除之檔案系統標籤時的 UntagResource 動作。

```

{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "111122223333",
        "arn": "arn:aws:sts::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T23:40:54Z"
            }
        }
    },
    "eventTime": "2018-11-14T23:40:54Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "UntagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {

```

```
    "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-  
ab12cd34ef56gh789"  
  },  
  "responseElements": null,  
  "requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",  
  "eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",  
  "eventType": "AwsApiCall",  
  "apiVersion": "2018-03-01",  
  "recipientAccountId": "111122223333"  
}
```

# 在 FSx for ONTAP 中使用 Microsoft Active Directory

Amazon FSx 可與 Microsoft Active Directory 搭配使用，以與您現有的環境整合。Active Directory 是 Microsoft 目錄服務，用於儲存網路上物件的相關資訊，並協助管理員和使用者尋找和使用此資訊。這些物件通常包含共用資源，例如檔案伺服器、網路使用者和電腦帳戶。

您可以選擇將 FSx for ONTAP 儲存虛擬機器 (SVMs) 加入 Active Directory 網域，以提供使用者身分驗證和檔案和資料夾層級存取控制。伺服器訊息區塊 (SMB) 用戶端接著可以使用其在 Active Directory 中的現有使用者身分來驗證自己並存取 SVM 磁碟區。您的使用者可以使用現有的身分來控制對個別檔案和資料夾的存取。此外，您可以將現有的檔案和資料夾及其安全存取控制清單 (ACL) 組態遷移至 Amazon FSx，而不需進行任何修改。

如果 Microsoft Active Directory 網域基礎設施無法使用，您可以在 SVM 的工作群組中設定伺服器訊息區塊 (SMB) 伺服器，做為將 SVM 加入 Microsoft Active Directory 的替代方案。如需詳細資訊，請參閱[在工作群組中設定 SMB 伺服器](#)。

當您將 Amazon FSx for NetApp ONTAP 加入 Active Directory 時，您可以單獨將檔案系統的 SVMs 加入 Active Directory。這表示您可以有一個檔案系統，其中包含一些已加入 Active Directory 的 SVMs，以及其他未加入 Active Directory SVMs。

SVM 加入 Active Directory 之後，您可以更新下列 Active Directory 組態屬性：

- DNS 伺服器 IP 地址
- 自我管理的 Active Directory 服務帳戶使用者名稱和密碼

## 主題

- [將 SVM 加入自我管理 Microsoft AD 的先決條件](#)
- [使用 Active Directory 的最佳實務](#)
- [將 SVMs 加入 Microsoft Active Directory 的運作方式](#)
- [管理 SVM Active Directory 組態](#)

## 將 SVM 加入自我管理 Microsoft AD 的先決條件

將 FSx for ONTAP SVM 加入自我管理的 Microsoft AD 網域之前，請確定您的 Active Directory 和網路符合下列各節中所述的要求。

## 主題

- [內部部署 Active Directory 需求](#)
- [網路組態需求](#)
- [Active Directory 服務帳戶需求](#)

## 內部部署 Active Directory 需求

請確定您已擁有可加入 SVM 的內部部署或其他自我管理 Microsoft AD。此 Active Directory 應具有下列組態：

- Active Directory 網域控制站網域功能層級位於 Windows Server 2000 或更高版本。
- Active Directory 使用的網域名稱不是單一標籤網域 (SLD) 格式。Amazon FSx 不支援 SLD 網域。
- 如果您已經定義 Active Directory 網站，請確定與 FSx for ONTAP 檔案系統相關聯的 VPC 子網路已定義在相同的 Active Directory 網站中，而且 VPC 子網路與 Active Directory 網站上的子網路之間不存在衝突。

### Note

如果您使用的是 AWS Directory Service，FSx for ONTAP 不支援將 SVMs 加入 Simple Active Directory。

## 網路組態需求

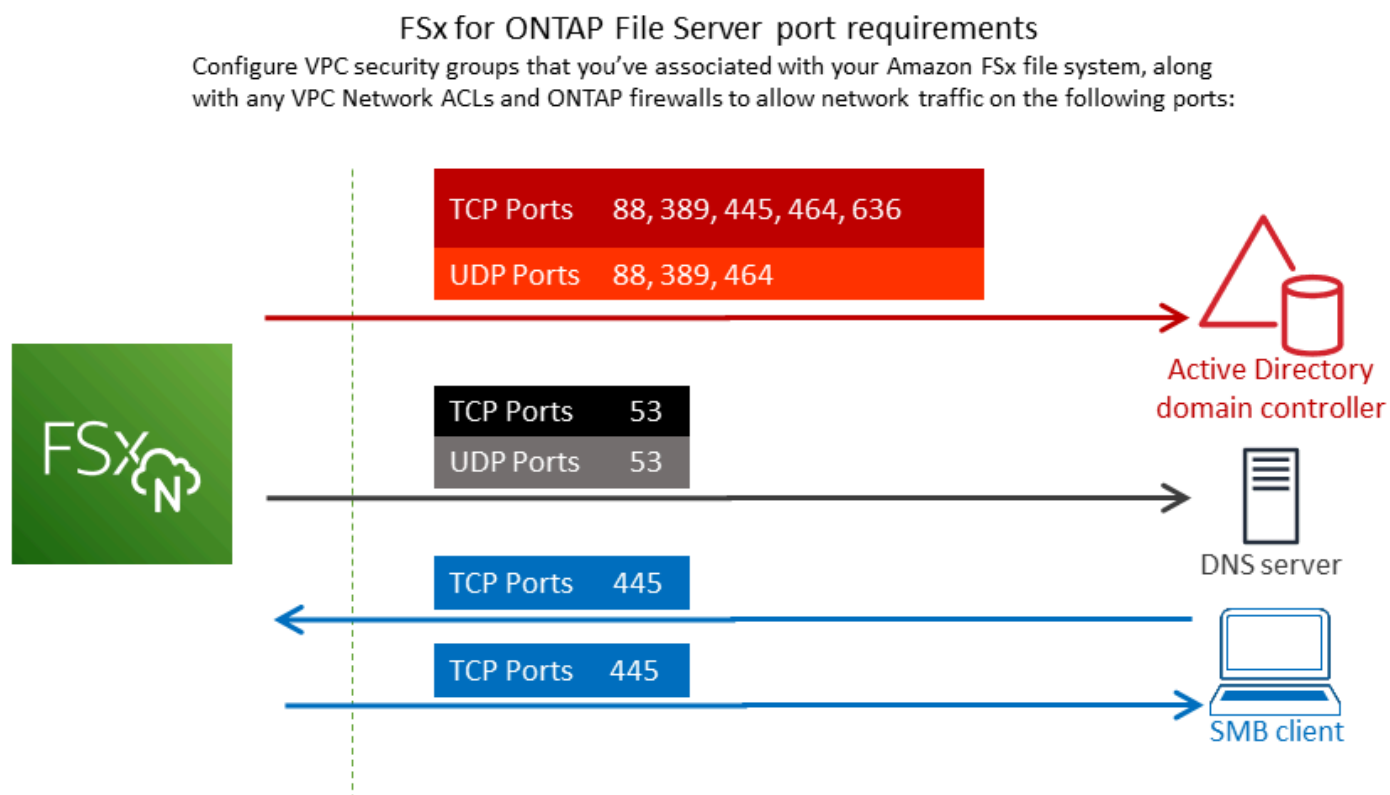
請確定您已備妥下列網路組態，並提供相關資訊。

### Important

若要讓 SVM 加入 Active Directory，您需要確保本主題中記錄的連接埠允許 SVM 上所有 Active Directory 網域控制器與兩個 iSCSI IP 地址 (iscsi\_1 和 iscsi\_2 邏輯界面 (LIFs)) 之間的流量。

- DNS 伺服器 and Active Directory 網域控制站 IP 地址。
- 使用 [AWS Direct Connect](#)、[AWS VPN](#) 或 建立檔案系統和自我管理 Active Directory 的 Amazon VPC 之間的連線 [AWS Transit Gateway](#)。

- 建立檔案系統之子網路的安全群組和 VPC 網路 ACLs 必須允許連接埠上的流量，並依照下圖所示的指示。



下表說明每個連接埠的角色。

| 通訊協定    | 連接埠 | 角色                              |
|---------|-----|---------------------------------|
| TCP/UDP | 53  | 網域名稱系統 (DNS)                    |
| TCP/UDP | 88  | Kerberos 身分驗證                   |
| TCP/UDP | 389 | 輕量型目錄存取通訊協定 (LDAP)              |
| TCP     | 445 | 目錄服務 SMB 檔案共用                   |
| TCP/UDP | 464 | 變更/設定密碼                         |
| TCP     | 636 | 透過 TLS/SSL 的輕量型目錄存取通訊協定 (LDAPS) |

- 這些流量規則也應該鏡像到套用至每個 Active Directory 網域控制站、DNS 伺服器、FSx 用戶端和 FSx 管理員的防火牆上。

#### Important

雖然 Amazon VPC 安全群組要求僅以啟動網路流量的方向開啟連接埠，但大多數 Windows 防火牆和 VPC 網路 ACLs 要求雙向開啟連接埠。

## Active Directory 服務帳戶需求

請確定您的自我管理 Microsoft AD 中有一個服務帳戶，該帳戶已委派將電腦加入網域的許可。服務帳戶是自我管理 Active Directory 中已委派特定任務的使用者帳戶。

至少，服務帳戶必須在您加入 SVM 的 OU 中委派下列許可：

- 能夠重設密碼
- 限制帳戶讀取和寫入資料的能力
- 能夠在電腦物件上設定 msDS-SupportedEncryptionTypes 屬性
- 驗證寫入 DNS 主機名稱的能力
- 已驗證能夠寫入服務主體名稱
- 建立和刪除電腦物件的能力
- 驗證讀取和寫入帳戶限制的能力

這些代表將電腦物件加入 Active Directory 所需的最低許可集。如需詳細資訊，請參閱 Windows Server 文件主題 [錯誤：當被委派控制的非管理員使用者嘗試將電腦加入網域控制器時，存取會遭拒](#)。

若要進一步了解如何建立具有正確許可的服務帳戶，請參閱 [將許可委派給您的 Amazon FSx 服務帳戶](#)。

#### Important

Amazon FSx 需要在整個 Amazon FSx 檔案系統生命週期內擁有有效的服務帳戶。Amazon FSx 必須能夠完整管理檔案系統，並執行需要它才能將資源取消加入和重新加入 Active Directory 網域的任務。這些任務包括取代失敗的檔案系統或 SVM，或修補 NetApp ONTAP

軟體。使用 Amazon FSx 將您的 Active Directory 組態資訊保持在最新狀態，包括服務帳戶憑證。如需進一步了解，請參閱 [使用 Amazon FSx 保持 Active Directory 組態的更新](#)。

如果這是您第一次使用 AWS 和 FSx for ONTAP，請務必在啟動 Active Directory 整合之前完成初始設定步驟。如需詳細資訊，請參閱[設定 FSx for ONTAP](#)。

#### Important

建立 SVMs 之後，請勿移動 Amazon FSx 在 OU 中建立的電腦物件，或是在 SVM 加入時刪除 Active Directory。這樣做會導致您的 SVMs 設定錯誤。

## 使用 Active Directory 的最佳實務

以下是將 Amazon FSx for NetApp ONTAP SVMs 加入自我管理的 Microsoft Active Directory 時應考慮的一些建議和準則。請注意，建議將這些作為最佳實務，但並非必要。

### 將許可委派給您的 Amazon FSx 服務帳戶

請務必使用所需的最低許可來設定您提供給 Amazon FSx 的服務帳戶。此外，將組織單位 (OU) 與其他網域控制站問題分開。

若要將 Amazon FSx SVMs 加入您的網域，請確定服務帳戶已委派許可。網域管理員群組的成員具有足夠的許可來執行此任務。不過，最佳實務是使用只有執行此作業所需的最低許可的服務帳戶。下列程序示範如何僅委派將 FSx for ONTAP SVMs 加入網域所需的許可。

在已加入目錄且已安裝 Active Directory 使用者和電腦 MMC 嵌入的機器上執行此程序。

為您的 Microsoft Active Directory 網域建立服務帳戶

1. 請確定您以 Microsoft Active Directory 網域的網域管理員身分登入。
2. 開啟 Active Directory 使用者和電腦 MMC 嵌入。
3. 在任務窗格中，展開網域節點。
4. 尋找並開啟您要修改之 OU 的內容（按一下滑鼠右鍵）選單，然後選擇委派控制。
5. 在控制委派精靈頁面上，選擇下一步。
6. 選擇新增，為選取的使用者和群組新增特定使用者或特定群組，然後選擇下一步。



7. 在 Tasks to Delegate (要委派的任務) 頁面上，選擇 Create a custom task to delegate (建立要委派的自訂任務)，然後選擇 Next (下一步)。
8. 選擇僅資料夾中的下列物件，然後選擇電腦物件。
9. 選擇在此資料夾中建立選取的物件，以及在此資料夾中刪除選取的物件。然後選擇下一步。
10. 在顯示這些許可下，確保已選取一般和屬性特定。
11. 針對許可，選擇下列項目：
  - 重設密碼
  - 讀取和寫入帳戶限制
  - 驗證寫入 DNS 主機名稱
  - 驗證寫入服務主體名稱
  - 寫入 msDS-SupportedEncryptionTypes
12. 選擇 Next (下一步)，然後選擇 Finish (完成)。
13. 關閉 Active Directory 使用者和電腦 MMC 嵌入。

 Important

建立 SVMs 之後，請勿移動 Amazon FSx 在 OU 中建立的電腦物件。這樣做會導致您的 SVMs 設定錯誤。

## 使用 Amazon FSx 保持 Active Directory 組態的更新

若要讓 Amazon FSx SVMs 持續可用，請在變更自我管理 AD 設定時更新 SVM 的自我管理 Active Directory (AD) 組態。

例如，假設您的 AD 使用以時間為基礎的密碼重設政策。在此情況下，一旦重設密碼，請務必使用 Amazon FSx 更新服務帳戶密碼。若要這樣做，請使用 Amazon FSx 主控台、Amazon FSx API 或 AWS CLI。同樣地，如果 Active Directory 網域的 DNS 伺服器 IP 地址變更，一旦發生變更，就會使用 Amazon FSx 更新 DNS 伺服器 IP 地址。

如果更新的自我管理 AD 組態發生問題，SVM 狀態會切換到設定錯誤。此狀態會在主控台、API 和 CLI 的 SVM 描述旁顯示錯誤訊息和建議的動作。如果 SVM 的 AD 組態發生問題，請務必針對組態屬性採取建議的修正動作。如果問題已解決，請確認 SVM 的狀態變更為已建立。

如需詳細資訊，請參閱 [使用 AWS Management Console](#)、[AWS CLI](#)、[和 API 更新現有的 SVM Active Directory 組態](#) 和 [使用 ONTAP CLI 修改 Active Directory 組態](#)。

## 使用安全群組來限制 VPC 內的流量

若要限制虛擬私有雲端 (VPC) 中的網路流量，您可以在 VPC 中實作最低權限的原則。換句話說，您可以將許可限制為所需的最低許可。若要這樣做，請使用安全群組規則。如需進一步了解，請參閱 [Amazon VPC 安全群組](#)。

## 為您的檔案系統的網路介面建立傳出安全群組規則

為了提高安全性，請考慮使用傳出流量規則設定安全群組。這些規則應僅允許傳出流量傳送到自我管理 AD 網域控制站，或在子網路或安全群組內。將此安全群組套用至與 Amazon FSx 檔案系統彈性網路介面相關聯的 VPC。如需進一步了解，請參閱 [使用 Amazon VPC 的檔案系統存取控制](#)。

## 將 SVMs 加入 Microsoft Active Directory 的運作方式

您的組織可能會使用 Active Directory 管理身分和裝置，無論是內部部署還是雲端。使用 FSx for ONTAP，您可以透過下列方式將 SVMs 直接加入現有的 Active Directory 網域：

- 在建立時將新的 SVMs 加入 Active Directory：
  - 使用 Amazon FSx 主控台中的標準建立選項來建立新的 FSx for ONTAP 檔案系統，您可以將預設 SVM 加入自我管理 Active Directory。如需詳細資訊，請參閱 [建立檔案系統（主控台）](#)。
  - 使用 Amazon FSx 主控台 AWS CLI 或 Amazon FSx API 在現有的 FSx for ONTAP 檔案系統上建立新的 SVM。如需詳細資訊，請參閱 [建立儲存虛擬機器 \(SVM\)](#)。
- 將現有 SVMs 加入 Active Directory：
  - 使用 AWS CLI AWS Management Console 和 API 將 SVM 加入 Active Directory，並在初次嘗試加入失敗時重新嘗試將 SVM 加入 Active Directory。您也可以為已加入 Active Directory SVMs 更新一些 Active Directory 組態屬性。如需詳細資訊，請參閱 [管理 SVM Active Directory 組態](#)。
  - 使用 NetApp ONTAP CLI 或 REST API 加入、重新嘗試加入和取消加入 SVM Active Directory 組態。如需詳細資訊，請參閱 [使用 NetApp CLI 更新 SVM Active Directory 組態](#)。

### Important

- 如果您使用 Microsoft DNS 做為預設 DNS 服務，Amazon FSx 只會註冊 SVM 的 DNS 記錄。如果您使用第三方 DNS，則必須在建立 Amazon FSx SVMs 之後手動設定 DNS 項目。

- 如果您使用 AWS Managed Microsoft AD，則必須指定群組，例如 AWS 委派 FSx 管理員、AWS 委派管理員，或具有委派 OU 許可的自訂群組。

當您將 FSx for ONTAP SVM 直接加入自我管理的 Active Directory 時，SVM 會位於相同的 Active Directory 樹系 (Active Directory 組態中包含網域、使用者和電腦的最上層邏輯容器)，以及與您的使用者和現有資源相同的 Active Directory 網域，包括現有的檔案伺服器。

## 將 SVM 加入 Active Directory 時所需的資訊

無論您選擇的 API 操作為何，在將 SVM 加入 Active Directory 時，您都必須提供 Active Directory 的下列相關資訊：

- 要為 SVM 建立之 Active Directory 電腦物件的 NetBIOS 名稱。這是 Active Directory 中 SVM 的名稱，在您的 Active Directory 中必須是唯一的。請勿使用主網域的 NetBIOS 名稱。NetBIOS 名稱不能超過 15 個字元。
- Active Directory 的完整網域名稱 (FQDN)。FQDN 不能超過 255 個字元。

### Note

FQDN 不能是單一標籤網域 (SLD) 格式。Amazon FSx 不支援 SLD 網域。

- 您網域的 DNS 伺服器或網域主機最多三個 IP 地址。

DNS 伺服器 IP 地址和 Active Directory 網域控制站 IP 地址可以在任何 IP 地址範圍內，但以下除外：

- 與 Amazon Web Services 擁有的 IP 地址衝突的 IP 地址 AWS 區域。如需依區域的 AWS IP 地址清單，請參閱 [AWS IP 地址範圍](#)。
- 下列 CIDR 區塊範圍中的 IP 地址：198.19.0.0/16
- 將 SVM 加入 Active Directory 網域時，Amazon FSx 使用之 Active Directory 網域上服務帳戶的使用者名稱和密碼。如需服務帳戶需求的詳細資訊，請參閱 [Active Directory 服務帳戶需求](#)。
- (選用) 您加入 SVM 之網域中的組織單位 (OU)。

### Note

如果您將 SVM 加入 AWS Directory Service Active Directory，則必須提供預設 OU 內的 OU，該 OU 會為相關的目錄物件 AWS Directory Service 建立 AWS。這是

因為 AWS Directory Service 不提供 Active Directory 預設 OU Computers 的存取權。例如，如果您的 Active Directory 網域是 `example.com`，您可以指定下列 OU：OU=Computers,OU=example,DC=example,DC=com。

- (選用) 您要委派授權給的網域群組，以在檔案系統上執行管理動作。例如，此網域群組可能會管理 Windows SMB 檔案共用、取得檔案和資料夾的擁有權等。如果您未指定此群組，Amazon FSx 預設會將此授權委派給 Active Directory 網域中的網域管理員群組。

## 管理 SVM Active Directory 組態

本節說明如何使用 AWS Management Console、AWS CLI、FSx API 和 ONTAP CLI 來執行下列動作：

- 將現有的 SVM 加入 Active Directory
- 修改現有的 SVM Active Directory 組態
- 從 Active Directory SVMs

若要從 Active Directory 移除 SVM，您必須使用 NetApp ONTAP CLI。

### 主題

- [使用 AWS Management ConsoleAWS CLI 和 API 將 SVMs 加入 Active Directory](#)
- [使用 AWS Management ConsoleAWS CLI、和 API 更新現有的 SVM Active Directory 組態](#)
- [使用 NetApp CLI 更新 SVM Active Directory 組態](#)

## 使用 AWS Management ConsoleAWS CLI 和 API 將 SVMs 加入 Active Directory

使用下列程序將現有的 SVM 加入 Active Directory。在此程序中，SVM 尚未加入 Active Directory。

將 SVM 加入 Active Directory (AWS Management Console)

1. 在 Amazon FSx 主控台開啟 <https://console.aws.amazon.com/fsx/>。
2. 選擇您要加入 Active Directory 的 SVM：
  - 在左側導覽窗格中，選擇檔案系統，然後選擇具有您要更新之 SVM 的 ONTAP 檔案系統。
  - 選擇儲存虛擬機器索引標籤。

–或–

- 若要顯示所有可用 SVMs 的清單，請在左側導覽窗格中展開 ONTAP，然後選擇儲存虛擬機器。AWS 區域 隨即顯示 中您帳戶中所有 SVMs 的清單。

從清單中選擇您要加入 Active Directory 的 SVM。

- 在 SVM 摘要面板的右上角，選擇動作 > 加入/更新 Active Directory。將 SVM 加入 Active Directory 視窗隨即出現。
- 針對您要加入 SVM 的 Active Directory，輸入下列資訊：
  - 要為 SVM 建立之 Active Directory 電腦物件的 NetBIOS 名稱。這是 Active Directory 中 SVM 的名稱，在您的 Active Directory 中必須是唯一的。請勿使用主網域的 NetBIOS 名稱。NetBIOS 名稱不能超過 15 個字元。
  - Active Directory 的完整網域名稱 (FQDN)。網域名稱不能超過 255 個字元。
  - DNS 伺服器 IP 地址 – 網域 DNS 伺服器的 IPv4 地址。
  - 服務帳戶使用者名稱 – 現有 Active Directory 中服務帳戶的使用者名稱。請勿包含網域字首或尾碼。例如，對於 EXAMPLE\ADMIN，請僅使用 ADMIN。
  - 服務帳戶密碼 – 服務帳戶的密碼。
  - 確認密碼 – 服務帳戶的密碼。
  - (選用) 組織單位 (OU) – 您要加入 SVM 的組織單位辨別路徑名稱。
  - 委派檔案系統管理員群組 – Active Directory 中可管理檔案系統的群組名稱。

如果您使用的是 AWS AWS Managed Microsoft AD，則必須指定群組，例如委派的 FSx 管理員、AWS 委派的管理員，或具有委派 OU 許可的自訂群組。

如果您要加入自我管理的 Active Directory，請使用 Active Directory 中的 群組名稱。預設群組為 Domain Admins。

- 選擇加入 Active Directory，使用您提供的組態將 SVM 加入 Active Directory。

將 SVM 加入 Active Directory (AWS CLI)

- 若要將 FSx for ONTAP SVM 加入 Active Directory，請使用 [update-storage-virtual-machine](#) CLI 命令（或同等的 [UpdateStorageVirtualMachine](#) API 操作），如下列範例所示。

```
aws fsx update-storage-virtual-machine \  
  --storage-virtual-machine-id svm-abcdef0123456789a\  
  --ad-username ADMIN \  
  --ad-password 'P@ssw0rd' \  
  --ad-domain FQDN \  
  --ad-ou-path 'OU=Example,DC=example,DC=com' \  
  --ad-group-name 'Example Admins' \  
  --ad-forest FQDN \  
  --ad-forest-ip FQDN
```

```
--active-directory-configuration
SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
  OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com", \
  FileSystemAdministratorsGroup="FSxAdmins",UserName="FSxService",\
  Password="password", \
  DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

成功建立儲存虛擬機器後，Amazon FSx 會以 JSON 格式傳回其描述，如下列範例所示。

```
{
  "StorageVirtualMachine": {
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    },
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddresses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddresses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddresses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddresses": ["198.19.0.5", "198.19.0.6"]
      }
    }
  }
}
```

```

    },
    "Iscsi": {
      "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com",
      "IpAddresses": ["198.19.0.7", "198.19.0.8"]
    }
  },
  "FileSystemId": "fs-0123456789abcdef0",
  "Lifecycle": "CREATED",
  "Name": "vol1",
  "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/fs-0123456789abcdef0/svm-abcdef0123456789a",
  "StorageVirtualMachineId": "svm-abcdef0123456789a",
  "Subtype": "default",
  "Tags": [],
}
}

```

## 使用 AWS Management Console、AWS CLI、和 API 更新現有的 SVM Active Directory 組態

使用下列程序更新已加入 Active Directory 之 SVM 的 Active Directory 組態。

### 更新 SVM Active Directory 組態 (AWS Management Console)

1. 開啟 Amazon FSx 主控台，網址為 <https://console.aws.amazon.com/fsx/> : //。
2. 選擇要更新的 SVM，如下所示：
  - 在左側導覽窗格中，選擇檔案系統，然後選擇具有您要更新之 SVM 的 ONTAP 檔案系統。
  - 選擇儲存虛擬機器索引標籤。

–或–

  - 若要顯示所有可用的 SVMs 清單，請在左側導覽窗格中展開 ONTAP，然後選擇儲存虛擬機器。

從清單中選取要更新的 SVM。
3. 在 SVM 摘要面板上，選擇動作 > 加入/更新 Active Directory。更新 SVM Active Directory 組態視窗隨即出現。



4. 您可以在此視窗中更新下列 Active Directory 組態屬性。
  - DNS 伺服器 IP 地址 – 網域 DNS 伺服器的 IPv4 地址。
  - 服務帳戶使用者名稱 – 現有 Active Directory 中服務帳戶的使用者名稱。請勿包含網域字首或尾碼。對於 EXAMPLE\ADMIN，請使用 ADMIN。
  - 服務帳戶密碼 – Active Directory 服務帳戶的密碼。
5. 輸入更新之後，請選擇更新 Active Directory 以進行變更。

使用下列程序更新已加入 Active Directory 之 SVM 的 Active Directory 組態。

#### 更新 SVM Active Directory 組態 (AWS CLI)

- 若要使用 AWS CLI 或 API 更新 SVM 的 Active Directory 組態，請使用 [update-storage-virtual-machine](#) CLI 命令（或同等的 [UpdateStorageVirtualMachine](#) API 操作），如下列範例所示。

```
aws fsx update-storage-virtual-machine \
  --storage-virtual-machine-id svm-abcdef0123456789a\
  --active-directory-configuration \
  SelfManagedActiveDirectoryConfiguration='{UserName="FSxService",\
  Password="password", \
  DnsIps=["10.0.1.18"]}'
```

## 使用 NetApp CLI 更新 SVM Active Directory 組態

您可以使用 NetApp ONTAP CLI 將 SVM 加入和退出 Active Directory，以及修改現有的 SVM Active Directory 組態。

### 使用 ONTAP CLI 將 SVM 加入 Active Directory

您可以使用 ONTAP CLI 將現有的 SVMs 加入 Active Directory，如下列程序所述。即使您的 SVM 已加入 Active Directory，您也可以執行此操作。

1. 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。將 **management\_endpoint\_ip** 取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```



如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

2. 透過提供完整目錄 DNS 名稱 (corp.example.com) 和至少一個 DNS 伺服器 IP 地址，為您的 Active Directory 建立 DNS 項目。

```
::>vserver services name-service dns create -vserver svm_name -
domains corp.example.com -name-servers dns_ip_1, dns_ip_2
```

若要驗證與 DNS 伺服器的連線，請執行下列命令。將 *svm\_name* 取代為您自己的資訊。

```
FsxId0ae30e5b7f1a50b6a::>vserver services name-service dns check -vserver svm_name
```

| Vserver  | Name Server   | Name Server<br>Status | Status Details          |
|----------|---------------|-----------------------|-------------------------|
| svm_name | 172.31.14.245 | up                    | Response time (msec): 0 |
| svm_name | 172.31.25.207 | up                    | Response time (msec): 1 |

2 entries were displayed.

3. 若要將 SVM 加入 Active Directory，請執行下列命令。請注意，您必須指定 Active Directory 中尚未存在 computer\_name 的，並提供的目錄 DNS 名稱-domain。針對 -OU，輸入您希望 SVM 加入的 OUs，以及 DC 格式的完整 DNS 名稱。

```
::>vserver cifs create -vserver svm_name -cifs-server computer_name -
domain corp.example.com -OU OU=Computers,OU=example,DC=corp,DC=example,DC=com
```

若要驗證 Active Directory 連線的狀態，請執行下列命令：

```
::>vserver cifs check -vserver svm_name
```

```

Vserver : svm_name
  Cifs NetBIOS Name : svm_netBIOS_name
    Cifs Status : Running
      Site : Default-First-Site-Name
Node Name      DC Server Name  DC Server IP   Status   Status Details
-----
FsxId0ae30e5b7f1a50b6a-01
  corp.example.com
                                172.31.14.245   up        Response time (msec): 5
FsxId0ae30e5b7f1a50b6a-02
  corp.example.com
```

```
172.31.14.245    up    Response time (msec): 20
2 entries were displayed.
```

- 如果您在此聯結後無法存取共用，請判斷您用來存取共用的帳戶是否具有許可。例如，如果您使用預設Admin帳戶（委派管理員）搭配 AWS 受管 Active Directory，則必須在 ONTAP 中執行下列命令。netbios\_domain 對應至 Active Directory 的網域名稱（對於 corp.example.com，此處netbios\_domain使用的是 example）。

```
FsxId0123456789a::>vserver cifs users-and-groups local-group add-members -vserver
svm_name -group-name BUILTIN\Administrators -member-names netbios_domain\admin
```

## 使用 ONTAP CLI 修改 Active Directory 組態

您可以使用 ONTAP CLI 來修改現有的 Active Directory 組態。

- 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。將 *management\_endpoint\_ip* 取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

- 執行下列命令來暫時關閉 SVM 的 CIFS 伺服器：

```
FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
```

- 如果您需要修改 Active Directory 的 DNS 項目，請執行下列命令：

```
::>vserver services name-service dns modify -vserver svm_name -
domains corp.example.com -name-servers dns_ip_1,dns_ip_2
```

您可以使用 `vserver services name-service dns check -vserver svm_name` 命令驗證 Active Directory DNS 伺服器的連線狀態。

```
::>vserver services name-service dns check -vserver svm_name

Name Server
Vserver      Name Server  Status      Status Details
-----
svmciad      dns_ip_1     up           Response time (msec): 1
```

```
svmciad      dns_ip_2      up      Response time (msec): 1
2 entries were displayed.
```

4. 如果您需要修改 Active Directory 組態本身，您可以使用下列命令來變更現有的欄位，取代：

- *computer\_name*，如果您想要修改 SVM 的 NetBIOS（機器帳戶）名稱。
- *domain\_name*，如果您想要修改網域名稱。這應與本節的步驟 3 () 中所述的 DNS 網域項目對應 corp.example.com。
- *organizational\_unit*，如果您想要修改 OU (OU=Computers, OU=example, DC=corp, DC=example, DC=com)。

您需要重新輸入您用來將此裝置加入 Active Directory 的 Active Directory 登入資料。

```
::>vserver cifs modify -vserver svm_name -cifs-server computer_name -
domain domain_name -OU organizational_unit
```

您可以使用 `vserver cifs check -vserver svm_name` 命令來驗證 Active Directory 連線的連線狀態。

5. 當您完成修改 Active Directory 和 DNS 組態時，請執行下列命令讓 CIFS 伺服器恢復：

```
::>vserver cifs modify -vserver svm_name -status-admin up
```

## 使用 NetApp ONTAP CLI 從 SVM 取消加入 Active Directory

NetApp ONTAP CLI 也可用來依照下列步驟，從 Active Directory 中取消加入 SVM：

1. 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。將 *management\_endpoint\_ip* 取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

2. 執行下列命令，刪除從 Active Directory 中取消加入裝置的 CIFS 伺服器。若要讓 ONTAP 刪除您 SVM 的機器帳戶，請提供您最初用來將 SVM 加入 Active Directory 的登入資料。

```
FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
```

3. 如果您需要修改 Active Directory 的 DNS 項目，請執行下列命令：

```
FsxId0123456789a::vserver cifs delete -vserver svm_name
```

In order to delete an Active Directory machine account for the CIFS server, you must supply the name and password of a Windows account with sufficient privileges to remove computers from the "CORP.AEXAMPLE.COM" domain.

Enter the user name: *user\_name*

Enter the password:

Warning: There are one or more shares associated with this CIFS server  
Do you really want to delete this CIFS server and all its shares? {y|n}: *y*

4. 執行下列命令來刪除 Active Directory 的 DNS 伺服器：

```
::vserver services name-service dns delete -vserver svm_name
```

如果您看到如下所示的警告 - 指示dns應該移除為 ns-switch- 而且您不打算將此裝置重新加入 Active Directory，您可以移除ns-switch項目。

Warning: "DNS" is present as one of the sources in one or more ns-switch databases but no valid DNS configuration was found for Vserver  
"svm\_name". Remove "DNS" from ns-switch using the "vserver services name-service ns-switch" command. Configuring "DNS" as a source  
in the ns-switch setting when there is no valid configuration can cause protocol access issues.

5. (選用) 執行下列命令dns來移除 ns-switch的項目。驗證來源順序，然後修改以移除hosts資料庫dns的項目，sources使其僅包含列出的其他來源。在此範例中，唯一的其他來源是 files。

```
::>vserver services name-service ns-switch show -vserver svm_name -database hosts
```

```

Vserver: svm_name
Name Service Switch Database: hosts
Name Service Source Order: files, dns
```

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts  
-sources files
```

6. (選用) 將資料庫主機sources的 修改為僅包含 , 以移除dns項目files。

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts  
-sources files
```

# 遷移至 Amazon FSx for NetApp ONTAP

下列各節提供如何將現有 NetApp ONTAP 檔案系統遷移至 Amazon FSx for NetApp ONTAP 的相關資訊。

## Note

如果您打算使用 All 分層政策將資料遷移到容量集區層，請記住檔案中繼資料一律存放在 SSD 層，而且所有新的使用者資料都會先寫入 SSD 層。當資料寫入 SSD 層時，背景分層程序會開始將資料分層至容量集區儲存體，但分層程序並非立即進行，且會耗用網路資源。您需要調整 SSD 層的大小，以考量檔案中繼資料 (3-7% 的使用者資料大小)，做為使用者資料的緩衝區，然後再將其分層到容量集區儲存。建議您不要超過 SSD 層的 80% 使用率。

遷移資料時，請務必使用 [CloudWatch File 系統指標](#) 監控您的 SSD 層，以確保其填充速度不會超過層處理程序將資料移至容量集區儲存體的速度。

## 主題

- [使用 NetApp SnapMirror 遷移至 FSx for ONTAP](#)
- [使用 遷移至 FSx for ONTAP AWS DataSync](#)

## 使用 NetApp SnapMirror 遷移至 FSx for ONTAP

您可以使用 NetApp SnapMirror 將 NetApp ONTAP 檔案系統遷移至 Amazon FSx for NetApp ONTAP。

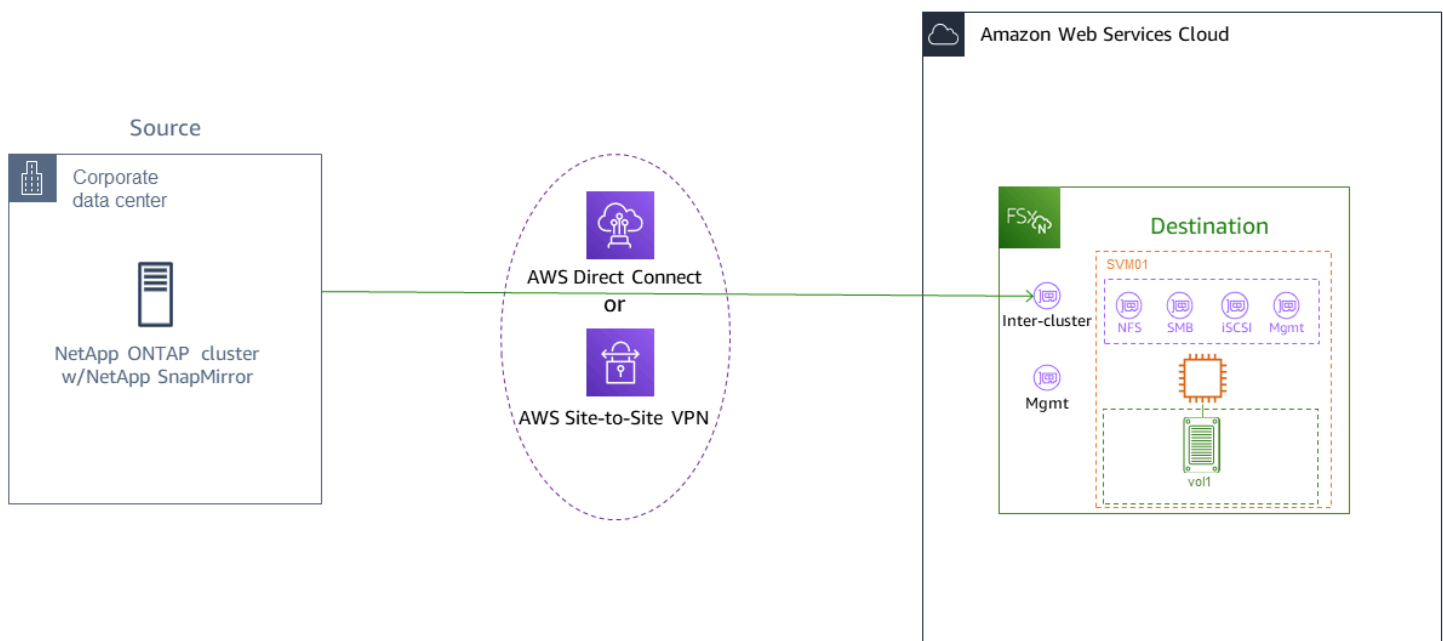
NetApp SnapMirror 會在兩個 ONTAP 檔案系統之間使用區塊層級複寫，將資料從指定的來源磁碟區複寫到目的地磁碟區。建議使用 SnapMirror 將內部部署 NetApp ONTAP 檔案系統遷移至 FSx for ONTAP。NetApp SnapMirror 的區塊層級複寫快速且高效，即使檔案系統具有下列特性：

- 複雜的目錄結構
- 超過 5,000 萬個檔案
- 非常小的檔案大小（以 KB 為單位）

當您使用 SnapMirror 遷移到 FSx for ONTAP 時，已刪除重複資料和壓縮資料會保留在這些狀態，從而縮短傳輸時間並減少遷移所需的頻寬量。遷移到目的地磁碟區時，來源 ONTAP 磁碟區上存在的快照會保留。將內部部署 NetApp ONTAP 檔案系統遷移至 FSx for ONTAP 涉及下列高階任務：

1. 在 Amazon FSx 中建立目的地磁碟區。
2. 收集來源和目的地邏輯界面 (LIFs)。
3. 在來源和目的地檔案系統之間建立叢集對等。
4. 建立 SVM 對等互連關係。
5. 建立 SnapMirror 關係。
6. 維護更新的目的地叢集。
7. 切換到 FSx for ONTAP 檔案系統。

下圖說明本節所述的遷移案例。



## 主題

- [開始之前](#)
- [建立目的地磁碟區](#)
- [記錄來源和目的地叢集間 LIFs](#)
- [在來源和目的地之間建立叢集對等](#)
- [建立 SVM 對等互連關係](#)
- [建立 SnapMirror 關係](#)
- [將資料傳輸至 FSx for ONTAP 檔案系統](#)
- [切換至 Amazon FSx](#)

## 開始之前

開始使用下列各節所述的程序之前，請確定您符合下列先決條件：

- FSx for ONTAP 會將用戶端流量優先於背景任務，包括資料分層、儲存效率和備份。遷移資料時，作為一般最佳實務，我們建議您監控 SSD 層的容量，以確保其使用率不超過 80%。您可以使用 [CloudWatch File 系統指標](#) 來監控 SSD 層的使用率。如需詳細資訊，請參閱 [磁碟區指標](#)。
- 如果您在遷移資料時將目的地磁碟區的資料分層政策設定為 `ALL`，所有檔案中繼資料都會存放在主要 SSD 儲存層。無論磁碟區的資料分層政策為何，檔案中繼資料一律存放在 SSD 型主要層。我們建議您假設主要層：容量集區層儲存容量的比率為 1：10。
- 來源和目的地檔案系統是在相同的 VPC 中連接，或位於使用 Amazon VPC 對等互連的網路中，傳輸閘道 AWS Direct Connect 或 AWS VPN。如需詳細資訊，請參閱《Amazon VPC 對等指南》中的 [從內存取資料 AWS 雲端](#) 和什麼是 VPC 對等互連？。 <https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>
- FSx for ONTAP 檔案系統的 VPC 安全群組具有傳入和傳出規則，允許 ICMP 以及連接埠 443、10000、11104 和 11105 上的 TCP，適用於叢集間端點 (LIFs)。
- 在建立 SnapMirror 資料保護關係之前，請確認來源和目的地磁碟區正在執行相容的 NetApp ONTAP 版本。如需詳細資訊，請參閱 NetApp 的 [ONTAP 使用者文件中適用於 SnapMirror 關係的相容 ONTAP 版本](#)。此處顯示的程序使用來源的現場部署 NetApp ONTAP 檔案系統。
- 您的內部部署（來源）NetApp ONTAP 檔案系統包含 SnapMirror 授權。
- 您已使用 SVM 建立 ONTAP 檔案系統的目的地 FSx，但尚未建立目的地磁碟區。如需詳細資訊，請參閱 [建立檔案系統](#)。

這些程序中的命令使用以下叢集、SVM 和磁碟區別名：

- *FSx-Dest* – 目的地 (FSx) 叢集的 ID（格式為 FSxIdabcdef1234567890a）。
- *OnPrem-Source* – 來源叢集的 ID。
- *DestSVM* – 目的地 SVM 名稱。
- *SourceSVM* – 來源 SVM 名稱。
- 來源和目的地磁碟區名稱都是 `vol1`。

### Note

FSx for ONTAP 檔案系統在所有 ONTAP CLI 命令中稱為叢集。



本節中的程序使用以下 NetApp ONTAP CLI 命令。

- [磁碟區建立](#) 命令
- [叢集](#) 命令
- [vserver 對等](#) 命令
- [snapmirror](#) 命令

您將使用 NetApp ONTAP CLI 在 FSx for ONTAP 檔案系統上建立和管理 SnapMirror 組態。如需詳細資訊，請參閱[使用 NetApp ONTAP CLI](#)。

## 建立目的地磁碟區

除了 NetApp ONTAP CLI 和 REST API 之外，您還可以使用 Amazon FSx 主控台 AWS CLI、和 Amazon FSx API 建立資料保護 (DP) 目的地磁碟區。如需使用 Amazon FSx 主控台建立目的地磁碟區的相關資訊 AWS CLI，請參閱 [建立磁碟區](#)。

### Note

ONTAP 當目的地磁碟區的分層政策為 `all` 時，不會保留在目的地 DP 磁碟區中來源處達到的後置處理壓縮節省。為了保持程序後壓縮節省，您應該將目的地磁碟區分層政策設定為 `auto` 並在目的地檔案系統上啟用 `inactive-data-compression`，以在目的地重新套用程序後壓縮節省。

在下列程序中，您將使用 NetApp ONTAP CLI 在 FSx for ONTAP 檔案系統上建立目的地磁碟區。您需要檔案系統管理連接埠 `fsxadmin` 的密碼和 IP 地址或 DNS 名稱。

1. 使用您在建立檔案系統時設定的使用者 `fsxadmin` 和密碼，使用目的地檔案系統建立 SSH 工作階段。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. 在儲存容量至少等於來源磁碟區的儲存容量的目的地叢集上建立磁碟區。使用 `-type DP` 將其指定為 SnapMirror 關係的目的地。

如果您計劃使用資料分層，我們建議您將 `-tiering-policy` 設定為 `all`。這可確保您的資料立即傳輸到容量集區儲存，並防止 SSD 層的容量不足。遷移後，您可以切換 `-tiering-policy` 到 `auto`。

**Note**

無論磁碟區的資料分層政策為何，檔案中繼資料一律存放在 SSD 型主要層。

```
FSx-Dest::> vol create -vserver DestSVM -volume vol1 -aggregate aggr1 -size 1g -
type DP -tiering-policy all
```

## 記錄來源和目的地叢集間 LIFs

SnapMirror 使用叢集間邏輯界面 (LIFs)，每個介面都有唯一的 IP 地址，以促進來源和目的地叢集之間的資料傳輸。

1. 對於 ONTAP 檔案系統的目的地 FSx，您可以透過導覽至檔案系統詳細資訊頁面上的管理索引標籤，從 Amazon FSx 主控台擷取叢集間端點 - IP 地址。
2. 對於來源 NetApp ONTAP 叢集，請使用 ONTAP CLI 擷取叢集間 LIF IP 地址。執行以下命令：

```
OnPrem-Source::> network interface show -role intercluster
```

| Logical<br>Vserver | Interface | Status | Network<br>Address/Mask |
|--------------------|-----------|--------|-------------------------|
| FSx-Dest           | inter_1   | up/up  | 10.0.0.36/24            |
|                    | inter_2   | up/up  | 10.0.1.69/24            |

**Note**

對於第二代單一可用區檔案系統，每個高可用性 (HA) 對有兩個叢集間 IP 地址。儲存這些值以供稍後使用。

儲存 inter\_1 和 inter\_2 IP 地址。它們在 中以 FSx-Dest dest\_inter\_1 和 的形式參考，dest\_inter\_2 而以 source\_inter\_1 和 OnPrem-Source 的形式參考 source\_inter\_2。

## 在來源和目的地之間建立叢集對等

透過提供叢集間 IP 地址，在目的地叢集上建立叢集對等關係。您也需要建立密碼短語，當您在來源叢集上建立叢集對等互連時，需要輸入密碼短語。

1. 使用下列命令在目的地叢集上設定對等互連。對於第二代單一可用區檔案系統，您需要提供每個叢集間 IP 地址。

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-  
addrs source_inter_1,source_inter_2
```

Enter the passphrase:

Confirm the passphrase:

Notice: Now use the same passphrase in the "cluster peer create" command in the other cluster.

2. 接著，在來源叢集上建立叢集對等關係。您需要輸入您在上方建立的密碼短語，才能進行身分驗證。對於第二代單一可用區檔案系統，您需要提供每個叢集間 IP 地址。

```
OnPrem-Source::> cluster peer create -address-family ipv4 -peer-  
addrs dest_inter_1,dest_inter_2
```

Enter the passphrase:

Confirm the passphrase:

3. 使用來源叢集上的下列命令，確認對等互連是否成功。在輸出中，Availability 應該設定為 Available。

```
OnPrem-Source::> cluster peer show
```

| Peer Cluster Name | Availability | Authentication |
|-------------------|--------------|----------------|
| FSx-Dest          | Available    | ok             |

## 建立 SVM 對等互連關係

建立叢集對等時，下一個步驟是對 SVMs 對等。使用 `vserver peer` 命令在目的地叢集 (FSx-Dest) 上建立 SVM 對等互連關係。下列命令中使用的其他別名如下：

- DestLocalName – 這是在來源 SVM 上設定 SVM 對等時用來識別目的地 SVM 的名稱。

- **SourceLocalName** – 這是在目的地 SVM 上設定 SVM 對等時用來識別來源 SVM 的名稱。

1. 使用下列命令，在來源和目的地 SVM 之間建立 SVMs 對等互連關係。

```
FSx-Dest::> vservers peer create -vservers DestSVM -peer-vservers SourceSVM -peer-cluster OnPrem-Source -applications snapmirror -local-name SourceLocalName
```

```
Info: [Job 207] 'vservers peer create' job queued
```

2. 接受來源叢集上的對等關係：

```
OnPrem-Source::> vservers peer accept -vservers SourceSVM -peer-vservers DestSVM -local-name DestLocalName
```

```
Info: [Job 211] 'vservers peer accept' job queued
```

3. 使用下列命令驗證 SVM 對等互連狀態；Peer State 應該在回應peered中設定為。

```
OnPrem-Source::> vservers peer show
```

|         | Peer     | Peer   | Peer     | Peering      | Remote  |
|---------|----------|--------|----------|--------------|---------|
| Vserver | Vserver  | State  | Cluster  | Applications | Vserver |
| -----   | -----    | -----  | -----    | -----        | -----   |
| svm01   | destsvm1 | peered | FSx-Dest | snapmirror   | svm01   |

## 建立 SnapMirror 關係

現在您已對來源和目的地 SVMs 建立對等，後續步驟是在目的地叢集上建立和初始化 SnapMirror 關係。

### Note

建立並初始化 SnapMirror 關係後，目的地磁碟區會變成唯讀，直到關係中斷為止。

- 使用 `snapmirror create` 命令在目的地叢集上建立 SnapMirror 關係。snapmirror create 命令必須從目的地 SVM 使用。

您可以選擇使用 `-throttle` 來設定 SnapMirror 關係的最大頻寬（以 kB/秒為單位）。

```
FSx-Dest::> snapmirror create -source-path SourceLocalName:vol1 -destination-path DestSVM:vol1 -vserver DestSVM -throttle unlimited
```

```
Operation succeeded: snapmirror create for the relationship with destination "DestSVM:vol1".
```

## 將資料傳輸至 FSx for ONTAP 檔案系統

現在您已建立 SnapMirror 關係，您可以將資料傳輸到目的地檔案系統。

1. 您可以在目的地檔案系統上執行下列命令，將資料傳輸至目的地檔案系統。

### Note

執行此命令後，SnapMirror 會開始將資料快照從來源磁碟區傳輸至目的地磁碟區。

```
FSx-Dest::> snapmirror initialize -destination-path DestSVM:vol1 -source-path SourceLocalName:vol1
```

2. 如果您正在遷移正在使用的資料，則需要更新目的地叢集，使其與您的來源叢集保持同步。若要對目的地叢集執行一次性更新，請執行下列命令。

```
FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
```

3. 您也可以在完成遷移之前，先排程每小時或每日更新，並將用戶端移至 FSx for ONTAP。您可以使用 [snapmirror modify](#) 命令建立 SnapMirror 更新排程。

```
FSx-Dest::> snapmirror modify -destination-path DestSVM:vol1 -schedule hourly
```

## 切換至 Amazon FSx

若要準備轉換至 FSx for ONTAP 檔案系統，請執行下列動作：

- 中斷所有寫入來源叢集的用戶端的連線。
- 執行最終的 SnapMirror 傳輸，以確保剪下時不會遺失資料。

- 中斷 SnapMirror 關係。
- 將所有用戶端連接到 FSx for ONTAP 檔案系統。

1. 為了確保來源叢集中的所有資料都傳輸到 FSx for ONTAP 檔案系統，請執行最終 Snapmirror 傳輸。

```
FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
```

2. 確認 Mirror State 設定為 Snapmirrored，且 Relationship Status 設定為 Idle，以確保資料遷移已完成Idle。您也應該確保Last Transfer End Timestamp日期如預期，如上次傳輸至目的地磁碟區的時間所示。
3. 執行下列命令以顯示 SnapMirror 狀態。

```
FSx-Dest::> snapmirror show -fields state,status,last-transfer-end-timestamp
```

| Source Path | Destination Path | Mirror State | Relationship Status | Last Transfer End Timestamp |
|-------------|------------------|--------------|---------------------|-----------------------------|
| Svm01:vol1  | svm02:DestVol    | Snapmirrored | Idle                | 09/02 09:02:21              |

4. 使用 snapmirror quiesce命令停用任何未來的 SnapMirror 傳輸。

```
FSx-Dest::> snapmirror quiesce -destination-path DestSVM:vol1
```

5. Quiesced 使用 確認 Relationship Status 已變更為 snapmirror show。

```
FSx-Dest::> snapmirror show
```

| Source Path     | Destination Path | Mirror State | Relationship Status |
|-----------------|------------------|--------------|---------------------|
| sourcesvm1:vol1 | svm01:DestVol    | Snapmirrored | Quiesced            |

6. 在遷移期間，目的地磁碟區為唯讀。若要啟用讀取/寫入，您需要中斷 SnapMirror 關係並切換到 FSx for ONTAP 檔案系統。使用以下命令中斷 SnapMirror 關係。

```
FSx-Dest::> snapmirror break -destination-path DestSVM:vol1
```

```
Operation succeeded: snapmirror break for destination "DestSVM:vol1".
```

7. 一旦 SnapMirror 複寫完成且您中斷了 SnapMirror 關係，您就可以掛載磁碟區，讓資料可用。

```
FSx-Dest::> vol mount -vserver fsx -volume vol1 -junction-path /vol1
```

磁碟區現在可供完全遷移至目的地磁碟區的資料使用。磁碟區也可供用戶端讀取和寫入。如果您先前 tiering-policy 將此磁碟區的設定為 all，您可以將其變更為 auto 或，snapshot-only。您的資料會根據存取模式在儲存層之間自動轉換。若要讓用戶端和應用程式可存取此資料，請參閱[存取 FSx for ONTAP 資料](#)。

## 使用 遷移至 FSx for ONTAP AWS DataSync

我們建議使用在 FSx for ONTAP 檔案系統與非 ONTAP 檔案系統之間 AWS DataSync 傳輸資料，包括 FSx for Lustre、FSx for OpenZFS、FSx for Windows File Server、Amazon EFS、Amazon S3 和內部部署檔案器。如果您要在 FSx for ONTAP 和 NetApp ONTAP 之間傳輸檔案，建議您使用 [NetApp SnapMirror](#)。AWS DataSync 是一種資料傳輸服務，可簡化、自動化和加速透過網際網路或，在自我管理的儲存系統和 AWS 儲存服務之間移動和複寫資料 AWS Direct Connect。DataSync 可以傳輸您的檔案系統資料和中繼資料，例如擁有權、時間戳記和存取許可。

您可以使用 DataSync 在兩個 FSx for ONTAP 檔案系統之間傳輸檔案，也可以將資料移至不同 AWS 區域或 AWS 帳戶中的檔案系統。您也可以將 DataSync 與 FSx for ONTAP 檔案系統用於其他任務。例如，您可以執行一次性資料遷移、定期擷取分散式工作負載的資料，以及排程複寫以進行資料保護和復原。

在 DataSync 中，位置是 FSx for ONTAP 檔案系統的端點。如需特定傳輸案例的資訊，請參閱 AWS DataSync 《使用者指南》中的[使用位置](#)。

### Note

如果您打算使用 All 分層政策將資料遷移到容量集區層，請記住檔案中繼資料一律存放在 SSD 層，而且所有新的使用者資料都會先寫入 SSD 層。當資料寫入 SSD 層時，背景分層程序會開始將資料分層至容量集區儲存體，但分層程序並非立即進行，且會耗用網路資源。您需要調整 SSD 層的大小，以考量檔案中繼資料 (3-7% 的使用者資料大小)，做為使用者資料的緩衝區，然後再將其分層到容量集區儲存。建議您不要超過 80% 的 SSD 使用率。

遷移資料時，請務必使用 [CloudWatch File 系統指標](#) 監控您的 SSD 層，以確保其填充速度不會超過層處理程序將資料移至容量集區儲存體的速度。您也可以將 DataSync 傳輸調節至低於分層發生速率的速率，以確保您的 SSD 層不會超過 80% 的使用率。例如，對於輸送量容量至少為 512 MBps 的檔案系統，200 MBps 限流通常會平衡資料傳輸和資料分層速率。

## 先決條件

若要將資料遷移至 FSx for ONTAP 設定，您需要符合 DataSync 需求的伺服器 and 網路。若要進一步了解，請參閱 AWS DataSync 使用者指南中的 [DataSync 需求](#)。

## 使用 DataSync 遷移檔案的基本步驟

使用 DataSync 將檔案從來源傳輸到目的地包含下列基本步驟：

- 在您的環境中下載和部署代理程式並啟用它（如果在兩者之間傳輸則不需要 AWS 服務）。
- 建立來源和目的地位置。
- 建立任務。
- 執行任務以將檔案從來源傳輸至目的地。

如需詳細資訊，請參閱《AWS DataSync 使用者指南》中的以下主題：

- [自我管理儲存與之間的資料傳輸 AWS](#)
- [為 Amazon FSx for NetApp ONTAP 建立位置](#)



# Amazon FSx for NetApp ONTAP 的安全性

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

安全性是 AWS 與您之間의 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 中執行 AWS 服務的基礎設施 AWS 雲端。AWS 也為您提供可安全使用的服務。作為[AWS 合規計畫](#)的一部分，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 Amazon FSx for NetApp ONTAP 的合規計畫，請參閱[AWS 合規計畫的服務範圍](#)。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您了解如何在使用 Amazon FSx 時套用共同責任模型。下列主題說明如何設定 Amazon FSx 以符合您的安全與合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 Amazon FSx 資源。

## 主題

- [Amazon FSx for NetApp ONTAP 中的資料保護](#)
- [Amazon FSx for NetApp ONTAP 的身分和存取管理](#)
- [AWS Amazon FSx for OpenZFS 的 受管政策](#)
- [使用 Amazon VPC 的檔案系統存取控制](#)
- [Amazon FSx for NetApp ONTAP 的合規驗證](#)
- [Amazon FSx for NetApp ONTAP 和界面 VPC 端點 \(AWS PrivateLink\)](#)
- [Amazon FSx for NetApp ONTAP 中的彈性](#)
- [Amazon FSx for NetApp ONTAP 中的基礎設施安全性](#)
- [將 NetApp ONTAP Vscan 與 FSx for ONTAP 搭配使用](#)
- [ONTAP 角色和使用者](#)

## Amazon FSx for NetApp ONTAP 中的資料保護

AWS [共同責任模型](#)適用於 Amazon FSx for NetApp ONTAP 中的資料保護。如此模型所述，AWS 負責保護執行所有的 全球基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同

時負責所使用 AWS 服務的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱[資料隱私權常見問答集](#)。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的[AWS 共同的責任模型](#)和[GDPR](#) 部落格文章。

基於資料保護目的，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 Amazon FSx 或使用 AWS 服務主控台、API AWS CLI 或其他 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。

## FSx for ONTAP 中的資料加密

Amazon FSx for NetApp ONTAP 支援靜態資料加密和傳輸中資料的加密。建立 Amazon FSx 檔案系統時，會自動啟用靜態資料加密。如果您使用輕量型目錄存取通訊協定 (LDAP) 存取加入 Active Directory 或網域的儲存虛擬機器 (SVM) 中的資料，Amazon FSx for NetApp ONTAP 支援透過 NFS 和 SMB 通訊協定傳輸中的 Kerberos 型加密。

### 使用加密時

如果您的組織受限於需要加密靜態資料和中繼資料的公司或法規政策，您的資料會自動靜態加密。我們也建議您使用傳輸中資料的加密來掛載檔案系統，以啟用傳輸中資料的加密。

如需使用 Amazon FSx for NetApp ONTAP 進行資料加密的詳細資訊，請參閱[靜態資料加密](#)和[加密傳輸中的資料](#)。

## 靜態資料加密

所有 Amazon FSx for NetApp ONTAP 檔案系統和備份都會使用 () 管理 AWS Key Management Service 的金鑰進行靜態加密 AWS KMS。資料會在寫入檔案系統之前自動加密，並在讀取時自動解密。所有備份都會在建立時自動加密，並在備份還原至新磁碟區時自動解密。這些程序由 Amazon FSx 透明處理，因此您不需要修改應用程式。

Amazon FSx 使用業界標準的 AES-256 加密演算法來加密靜態 Amazon FSx 資料和中繼資料。如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的[密碼編譯基礎](#)。

### Note

AWS 金鑰管理基礎設施使用聯邦資訊處理標準 (FIPS) 140-2 核准的密碼編譯演算法。基礎設施符合國家標準技術研究所 (NIST) 800-57 的建議。

## Amazon FSx 如何使用 AWS KMS

Amazon FSx 與 整合 AWS KMS 以進行金鑰管理。Amazon FSx 使用 KMS 金鑰來加密您的檔案系統和任何磁碟區備份。您可以選擇用來加密和解密檔案系統和磁碟區備份（資料和中繼資料）的 KMS 金鑰。您可以啟用、停用或撤銷此 KMS 金鑰的授予。此 KMS 金鑰可以是下列兩種類型之一：

- AWS 受管 KMS 金鑰 – 這是預設 KMS 金鑰，可免費使用。
- 客戶受管 KMS 金鑰 – 這是最靈活的 KMS 金鑰，因為您可以設定其金鑰政策和授予多個使用者或服務。如需建立 KMS 金鑰的詳細資訊，請參閱 AWS Key Management Service [《開發人員指南》中的建立金鑰](#)。

### Important

Amazon FSx 僅接受對稱加密 KMS 金鑰。您無法搭配 Amazon FSx 使用非對稱 KMS 金鑰。

如果您使用客戶管理的 KMS 金鑰做為檔案資料加密和解密的 KMS 金鑰，您可以啟用金鑰輪換。啟用金鑰輪換時，AWS KMS 每年會自動輪換金鑰一次。此外，使用客戶管理的 KMS 金鑰，您可以選擇何時停用、重新啟用、刪除或撤銷對 KMS 金鑰的存取權。如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的[輪換 AWS KMS keys](#)和[啟用和停用金鑰](#)。

## 的 Amazon FSx 金鑰政策 AWS KMS

金鑰政策是控制對 KMS 金鑰之存取的主要方式。如需金鑰政策的詳細資訊，請參閱《開發人員指南》中的[在 中使用金鑰政策 AWS KMS](#)。AWS Key Management Service 以下清單說明 Amazon FSx 針對靜態檔案系統和備份所支援的所有相關 AWS KMS 許可：

- kms:Encrypt：(選用) 將純文字加密為加密文字。此許可會納入預設的金鑰政策中。
- kms:Decrypt：(必要) 對密文進行解密。加密文字是先前已加密的純文字。此許可會納入預設的金鑰政策中。
- kms:ReEncrypt – (選用) 使用新的 加密伺服器端的資料 AWS KMS key，而不會公開用戶端資料的純文字。資料會先解密，然後重新加密。此許可會納入預設的金鑰政策中。
- kms:GenerateDataKeyWithoutPlaintext – (必要) 傳回以 KMS 金鑰加密的資料加密金鑰。此許可會納入 kms:GenerateDataKey\* 下預設的金鑰政策中。
- kms:CreateGrant：(必要) 將授予新增至金鑰，以指定誰可以使用金鑰和使用條件。授予是金鑰政策的備用許可機制。如需授權的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的[使用授權](#)。此許可會納入預設的金鑰政策中。
- kms:DescribeKey – (必要) 提供指定 KMS 金鑰的詳細資訊。此許可會納入預設的金鑰政策中。
- kms:ListAliases：(選用) 列出帳戶中所有金鑰別名。當您使用 主控台 建立加密的檔案系統時，此許可會填入 KMS 金鑰清單。我們建議您使用此許可，以提供最佳使用者體驗。此許可會納入預設的金鑰政策中。

## 加密傳輸中的資料

本主題說明在 FSx for ONTAP 檔案系統和連線用戶端之間傳輸時，可用於加密檔案資料的不同選項。它也提供指引，協助您選擇最適合工作流程的加密方法。

所有流 AWS 區域 經 AWS 全球網路的資料都會在實體層自動加密，再離開 AWS 安全的設施。可用區域之間的所有流量都會加密。額外的加密層，包括本節列出的加密層，提供額外的保護。如需有關 如何為資料流經 AWS 區域、可用區域和執行個體 AWS 提供保護的詳細資訊，請參閱《Amazon Elastic Compute Cloud Linux 執行個體使用者指南》中的[傳輸中加密](#)。

Amazon FSx for NetApp ONTAP 支援下列方法來加密 FSx for ONTAP 檔案系統和連線用戶端之間的傳輸中資料：

- 在支援 Amazon EC2 [Linux](#) 和 [Windows](#) 執行個體類型上執行的所有支援通訊協定和用戶端上自動 Nitro 型加密。

- NFS 和 SMB 通訊協定的 Kerberos 型加密。
- NFS、iSCSI 和 SMB 通訊協定的 IPsec 型加密

所有支援用於加密傳輸中資料的方法都使用產業標準 AES-256 密碼編譯演算法，以提供企業強度加密。

## 主題

- [選擇加密傳輸中資料的方法](#)
- [使用 AWS Nitro System 加密傳輸中的資料](#)
- [使用 Kerberos 型加密來加密傳輸中的資料](#)
- [使用 IPsec 加密加密傳輸中的資料](#)
- [啟用傳輸中資料的 SMB 加密](#)
- [使用 PSK 身分驗證設定 IPsec](#)
- [使用憑證身分驗證設定 IPsec](#)

## 選擇加密傳輸中資料的方法

本節提供的資訊可協助您決定哪種支援的傳輸中加密最適合您的工作流程。當您探索以下各節中詳細說明的支援選項時，請參閱本節。

選擇加密 FSx for ONTAP 檔案系統和連線用戶端之間傳輸中資料的方式時，需要考慮幾個因素。這些因素包括：

- 您的 FSx for ONTAP 檔案系統正在其中執行 AWS 區域的。
- 用戶端執行所在的執行個體類型。
- 用戶端存取您檔案系統的位置。
- 網路效能需求。
- 您要加密的資料通訊協定。
- 如果您使用的是 Microsoft Active Directory。

## AWS 區域

檔案系統在 中執行 AWS 區域的 會決定您是否可以使用 Amazon Nitro 型加密。如需詳細資訊，請參閱[使用 AWS Nitro System 加密傳輸中的資料](#)。

## 用戶端執行個體類型

如果存取檔案系統的用戶端正在任何支援的 Amazon EC2 Mac、[Linux](#) 或 [Windows](#) 執行個體類型上執行，且您的工作流程符合使用 Nitro 型加密的所有其他需求，則可以使用 Amazon [Nitro 型加密](#)。使用 Kerberos 或 IPsec 加密沒有任何用戶端執行個體類型需求。

## 用戶端位置

用戶端存取檔案系統位置相關資料的位置會影響哪些傳輸中加密方法可供使用。如果用戶端和檔案系統位於相同的 VPC，您可以使用任何支援的加密方法。如果用戶端和檔案系統位於對等 VPCs 中，只要流量不會通過虛擬網路裝置或服務，例如傳輸閘道，也是如此。如果用戶端不在相同或對等 VPC 中，或者流量透過虛擬網路裝置或服務傳遞，則 Nitro 型加密不是可用的選項。

## 網路效能

使用 Amazon Nitro 型加密不會影響網路效能。這是因為支援的 Amazon EC2 執行個體會利用基礎 Nitro System 硬體的卸載功能，自動加密執行個體之間的傳輸中流量。

使用 Kerberos 或 IPsec 加密會影響網路效能。這是因為這兩種加密方法都是以軟體為基礎的，這需要用戶端和伺服器使用運算資源來加密和解密傳輸中流量。

## 資料通訊協定

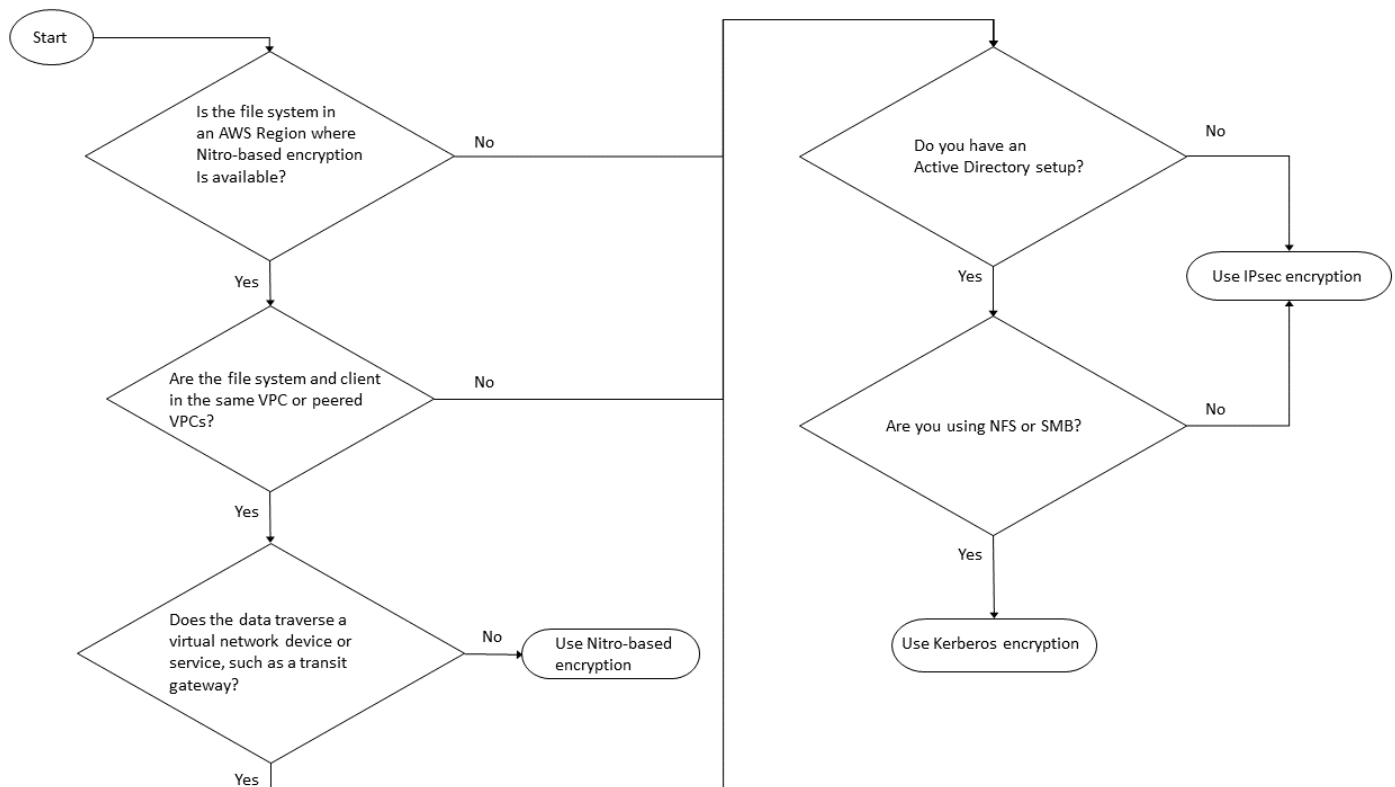
您可以使用 Amazon Nitro 型加密和 IPsec 加密搭配所有支援的通訊協定 – NFS、SMB 和 iSCSI。您可以使用 Kerberos 加密搭配 NFS 和 SMB 通訊協定（搭配 Active Directory）。

## Active Directory

如果您使用的是 Microsoft Active Directory，您可以透過 NFS 和 SMB 通訊協定使用 [Kerberos 加密](#)。

使用下圖協助您決定要使用的傳輸中加密方法。





當下列所有條件都適用於您的工作流程時，IPsec 加密是唯一可用的選項：

- 您正在使用 NFS、SMB 或 iSCSI 通訊協定。
- 您的工作流程不支援使用 Amazon Nitro 型加密。
- 您未使用 Microsoft Active Directory 網域。

## 使用 AWS Nitro System 加密傳輸中的資料

使用 Nitro 型加密，當存取檔案系統的用戶端在 中支援的 Amazon EC2 [Linux](#) 或 [Windows](#) 執行個體類型上執行時，傳輸中的資料會自動加密，AWS 區域 該類型可在 FSx for ONTAP 上使用。

使用 Amazon Nitro 型加密不會影響網路效能。這是因為支援的 Amazon EC2 執行個體會利用基礎 Nitro System 硬體的卸載功能，自動加密執行個體之間的傳輸中流量。

當支援的用戶端執行個體類型位於相同 AWS 區域 VPC 中或與檔案系統 VPC 對等的 VPC 中時，會自動啟用 Nitro 型加密。此外，如果用戶端位於對等 VPC 中，則資料無法周遊虛擬網路裝置或服務（例如傳輸閘道），以便自動啟用 Nitro 型加密。如需 Nitro 型加密的詳細資訊，請參閱適用於 [Linux](#) 或 [Windows](#) 執行個體類型的 Amazon EC2 使用者指南中的傳輸中加密一節。

下表詳細說明可使用 Nitro 型加密 AWS 區域 的。

## 支援 Nitro 型加密

| 產生                   | 部署類型            | AWS 區域                                                                   |
|----------------------|-----------------|--------------------------------------------------------------------------|
| 第一代檔案系統 <sup>1</sup> | 單一可用區 1 多個可用區 1 | 美國東部（維吉尼亞北部）、美國東部（俄亥俄）、美國西部（奧勒岡）、歐洲（愛爾蘭）                                 |
| 第二代檔案系統              | 單一可用區 2 多可用區 2  | 美國東部（維吉尼亞北部）、美國東部（俄亥俄）、美國西部（加利佛尼亞北部）、美國西部（奧勒岡）、歐洲（法蘭克福）、歐洲（愛爾蘭）、亞太區域（雪梨） |

<sup>1</sup> 2022 年 11 月 28 日當天或之後建立的第一代檔案系統支援所列中的 Nitro 型傳輸中加密 AWS 區域。

如需可使用 FSx for ONTAP AWS 區域之的詳細資訊，請參閱 [Amazon FSx for NetApp ONTAP 定價](#)。

如需 FSx for ONTAP 檔案系統效能規格的詳細資訊，請參閱 [輸送量容量對效能的影響](#)。

## 使用 Kerberos 型加密來加密傳輸中的資料

如果您使用的是 Microsoft Active Directory，您可以透過 NFS 和 SMB 通訊協定使用 Kerberos 型加密，為[加入 Microsoft Active Directory 的 SVMs](#) 子磁碟區加密傳輸中資料。

## 使用 Kerberos 透過 NFS 加密傳輸中的資料

NFSv3 和 NFSv4 通訊協定支援使用 Kerberos 加密傳輸中的資料。若要針對 NFS 通訊協定使用 Kerberos 啟用傳輸中加密，請參閱 NetApp ONTAP 文件中心中的[搭配使用 Kerberos 與 NFS 以提高安全性](#)。

## 使用 Kerberos 透過 SMB 加密傳輸中的資料

在支援 SMB 通訊協定 3.0 或更新版本的運算執行個體上映射的檔案共用支援透過 SMB 通訊協定傳輸中的資料加密。這包括 Microsoft Windows Server 2012 和更新版本以及 Microsoft Windows 8 和更新



版本的所有 Microsoft Windows 版本。啟用時，FSx for ONTAP 會在您存取檔案系統時，使用 SMB 加密自動加密傳輸中的資料，而不需要您修改應用程式。

FSx for ONTAP SMB 支援 128 和 256 位元加密，這取決於用戶端工作階段請求。如需不同加密層級的說明，請參閱 NetApp ONTAP 文件中心的[使用 CLI 設定管理 SMB 的 SMB 伺服器最低身分驗證安全層級一節](#)。

#### Note

用戶端決定加密演算法。NTLM 和 Kerberos 身分驗證都使用 128 和 256 位元加密。FSx for ONTAP SMB Server 接受所有標準 Windows 用戶端請求，而精細控制是由 Microsoft 群組政策或登錄檔設定處理。

您可以使用 ONTAP CLI 來管理 FSx for ONTAP SVMs 和磁碟區的傳輸中加密設定。若要存取 NetApp ONTAP CLI，請在要在傳輸中加密的 SVM 上建立 SSH 工作階段，如中所述[使用 CLI ONTAP 管理 SVMs](#)。

如需如何在 SVM 或磁碟區上啟用 SMB 加密的說明，請參閱[啟用傳輸中資料的 SMB 加密](#)。

## 使用 IPsec 加密加密傳輸中的資料

FSx for ONTAP 支援在傳輸模式下使用 IPsec 通訊協定，以確保資料在傳輸期間持續安全和加密。IPsec 為所有支援的 IP end-to-end 流量 – NFS、iSCSI 和 SMB 通訊協定，提供用戶端與 FSx for ONTAP 檔案系統之間的端對端傳輸中資料加密。使用 IPsec 加密，您可以在 FSx for ONTAP SVM 之間建立 IPsec 通道，而 FSx for ONTAP SVM 設定為啟用 IPsec，以及在存取資料的連線用戶端上執行 IPsec 用戶端。

我們建議您在從不支援 [Nitro 型](#) 加密的用戶端存取您的資料時，以及如果您的用戶端和 SVMs 未加入以 Kerberos 型加密所需的 Active Directory 時，使用 IPsec 透過 NFS、SMB 和 iSCSI 通訊協定加密傳輸中的資料。當您的 iSCSI 用戶端不支援 Nitro 型加密時，IPsec 加密是唯一可用於加密 iSCSI 流量傳輸中資料的選項。

對於 IPsec 身分驗證，您可以使用預先共用金鑰 (PSKs) 或憑證。如果您使用的是 PSK，您使用的 IPsec 用戶端必須支援具有 PSK 的網際網路金鑰交換版本 2 (IKEv2)。在 FSx for ONTAP 和用戶端上設定 IPsec 加密的高層級步驟如下：

1. 在檔案系統上啟用和設定 IPsec。
2. 在用戶端上安裝和設定 IPsec
3. 為多個用戶端存取設定 IPsec

如需如何使用 PSK 設定 IPsec 的詳細資訊，請參閱 NetApp ONTAP 文件中心的[透過線路加密設定 IP 安全性 \(IPsec\)](#)。

如需如何使用憑證設定 IPsec 的詳細資訊，請參閱[使用憑證身分驗證設定 IPsec](#)。

## 啟用傳輸中資料的 SMB 加密

根據預設，當您建立 SVM 時，SMB 加密會關閉。您可以啟用個別共用所需的 SMB 加密，或在 SVM 上啟用該 SVM 上所有共用所需的 SMB 加密。

### Note

在 SVM 或共用上啟用所需的 SMB 加密時，不支援加密的 SMB 用戶端無法連線至該 SVM 或共用。

## 要求 SVM 上傳入 SMB 流量的 SMB 加密

使用下列程序，使用 CLI 在 SVM 上要求 SMB NetApp ONTAP 加密。

1. 若要使用 SSH 連線至 SVM 管理端點，請使用您建立 SVM 時設定的使用者名稱 `vsadmin` 和 `vsadmin` 密碼。如果您未設定 `vsadmin` 密碼，請使用使用者名稱 `fsxadmin` 和 `fsxadmin` 密碼。您可以使用管理端點 IP 地址或 DNS 名稱，從與檔案系統位於相同 VPC 的用戶端 SSH 進入 SVM。

```
ssh vsadmin@svm-management-endpoint-ip-address
```

具有範例值的 命令：

```
ssh vsadmin@198.51.100.10
```

使用管理端點 DNS 名稱的 SSH 命令：

```
ssh vsadmin@svm-management-endpoint-dns-name
```

使用範例 DNS 名稱的 SSH 命令：

```
ssh vsadmin@management.svm-abcdef01234567892fs-08fc3405e03933af0.fsx.us-east-2.aws.com
```

Password: **vsadmin-password**

This is your first recorded login.  
FsxIdabcdef01234567892::~>

2. 使用 [vserver cifs security modify](#) NetApp ONTAP CLI 命令來要求 SMB 加密傳入 SMB 流量到 SVM。

```
vserver cifs security modify -vserver vserver_name -is-smb-encryption-required true
```

3. 若要停止對傳入 SMB 流量要求 SMB 加密，請使用下列命令。

```
vserver cifs security modify -vserver vserver_name -is-smb-encryption-required false
```

4. 若要查看 SVM 上的目前is-smb-encryption-required設定，請使用 CLI [vserver cifs security show](#) NetApp ONTAP 命令：

```
vserver cifs security show -vserver vs1 -fields is-smb-encryption-required

vserver  is-smb-encryption-required
-----  -----
vs1      true
```

如需在 SVM 上管理 SMB 加密的詳細資訊，請參閱 NetApp ONTAP [文件中心的在 SMB 伺服器上設定必要的 SMB 加密，以透過 SMB 進行資料傳輸](#)。

在磁碟區上啟用 SMB 加密

使用下列程序，使用 CLI 在共享上啟用 SMB NetApp ONTAP 加密。

1. 建立 SVM 管理端點的安全 Shell (SSH) 連線，如中所述[使用 CLI ONTAP 管理 SVMs](#)。
2. 使用下列 NetApp ONTAP CLI 命令建立新的 SMB 共享，並在存取此共享時需要 SMB 加密。

```
vserver cifs share create -vserver vserver_name -share-name share_name -  
path share_path -share-properties encrypt-data
```

如需詳細資訊，請參閱 CLI NetApp ONTAP 命令手冊頁面[vserver cifs share create](#)中的。

3. 若要在現有的 SMB 共享上要求 SMB 加密，請使用下列命令。

```
vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties encrypt-data
```

如需詳細資訊，請參閱 CLI NetApp ONTAP 命令手冊頁面[vserver cifs share create](#)中的。

4. 若要關閉現有 SMB 共用的 SMB 加密，請使用下列命令。

```
vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties encrypt-data
```

如需詳細資訊，請參閱 CLI NetApp ONTAP 命令手冊頁面[vserver cifs share properties remove](#)中的。

5. 若要查看 SMB 共享上的目前is-smb-encryption-required設定，請使用下列 CLI NetApp ONTAP 命令：

```
vserver cifs share properties show -vserver vserver_name -share-name share_name -fields share-properties
```

如果命令傳回的其中一個屬性是 encrypt-data 屬性，則該屬性指定存取此共用時必須使用 SMB 加密。

如需詳細資訊，請參閱 CLI NetApp ONTAP 命令手冊頁面[vserver cifs share properties show](#)中的。

## 使用 PSK 身分驗證設定 IPsec

如果您使用 PSK 進行身分驗證，則在 FSx for ONTAP 和用戶端上設定 IPsec 加密的步驟如下：

1. 在檔案系統上啟用和設定 IPsec。
2. 在用戶端上安裝和設定 IPsec
3. 為多個用戶端存取設定 IPsec

如需使用 PSK 設定 IPsec 的詳細資訊，請參閱NetApp ONTAP文件中心的[透過線路加密設定 IP 安全性 \(IPsec\)](#)。

## 使用憑證身分驗證設定 IPsec

下列主題提供在 FSx for ONTAP 檔案系統和執行 Libreswan IPsec 的用戶端上使用憑證驗證設定 IPsec 加密的指示。此解決方案使用 AWS Private Certificate Authority AWS Certificate Manager 和 來建立私有憑證授權單位和產生憑證。

在 FSx for ONTAP 檔案系統和連線用戶端上使用憑證身分驗證來設定 IPsec 加密的高階步驟如下：

1. 擁有發行憑證的憑證授權單位。
2. 產生和匯出檔案系統和用戶端的 CA 憑證。
3. 在用戶端執行個體上安裝憑證並設定 IPsec。
4. 在檔案系統上安裝憑證並設定 IPsec。
5. 定義安全政策資料庫 (SPD)。
6. 為多個用戶端存取設定 IPsec。

### 建立和安裝 CA 憑證

對於憑證身分驗證，您需要從 FSx for ONTAP 檔案系統的憑證授權單位，以及將存取檔案系統上資料的用戶端，產生並安裝憑證。下列範例使用 AWS Private Certificate Authority 來設定私有憑證授權單位，並產生要在檔案系統和用戶端上安裝的憑證。使用 AWS Private Certificate Authority，您可以建立根和次級憑證授權單位 (CAs 的完全 AWS 託管階層，以供組織內部使用。此程序有五個步驟：

1. 使用 建立私有憑證授權機構 (CA) AWS Private CA
2. 在私有 CA 上發行並安裝根憑證
3. 為您的檔案系統和用戶端請求來自 AWS Certificate Manager 的私有憑證
4. 匯出檔案系統和用戶端的憑證。

如需詳細資訊，請參閱 AWS Private Certificate Authority 《使用者指南》中的[私有 CA 管理](#)。

### 建立根私有 CA

1. 建立 CA 時，您必須在您提供的檔案中指定 CA 組態。下列命令使用 Nano 文字編輯器來建立 `ca_config.txt` 檔案，指定下列資訊：
  - 演算法的名稱
  - CA 用來簽署的簽署演算法
  - X.500 主旨資訊

```
$ > nano ca_config.txt
```

文字編輯器隨即出現。

2. 使用 CA 的規格編輯 檔案。

```
{
  "KeyAlgorithm":"RSA_2048",
  "SigningAlgorithm":"SHA256WITHRSA",
  "Subject":{"
    "Country":"US",
    "Organization":"Example Corp",
    "OrganizationalUnit":"Sales",
    "State":"WA",
    "Locality":"Seattle",
    "CommonName":"*.ec2.internal"
  }
}
```

3. 儲存並關閉檔案，結束文字編輯器。如需詳細資訊，請參閱 AWS Private Certificate Authority 《使用者指南》中的[建立 CA 的程序](#)。
4. 使用 [create-certificate-authority](#) AWS Private CA CLI 命令來建立私有 CA。

```
~/home > aws acm-pca create-certificate-authority \
  --certificate-authority-configuration file://ca_config.txt \
  --certificate-authority-type "ROOT" \
  --idempotency-token 01234567 --region aws-region
```

如果成功，此命令會輸出 CA 的 Amazon Resource Name (ARN)。

```
{
  "CertificateAuthorityArn": "arn:aws:acm-pca:aws-region:111122223333:certificate-
  authority/12345678-1234-1234-1234-123456789012"
}
```

為您的私有根 CA 建立和安裝憑證 (AWS CLI)

1. 使用 AWS CLI 命令產生憑證簽署請求 [get-certificate-authority-csr](#) (CSR)。

```
$ aws acm-pca get-certificate-authority-csr \
  --certificate-authority-arn arn:aws:acm-pca:aws-region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
  --output text \
  --endpoint https://acm-pca.aws-region.amazonaws.com \
  --region eu-west-1 > ca.csr
```

產生的檔案 `ca.csr` 為以 base64 格式編碼的 PEM 檔案，其外觀如下。

```
-----BEGIN CERTIFICATE-----
MIICiTCcAFICCCQD6m7oRw0uX0jANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAGTAldBMRAwDgYDVQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6
b24xZDASBgNVBASTC0lBTSBDb25zb2x1MRIwEAYDVQQDEw1UZXR0Q21sYWx1ZAd
BgkqhkiG9w0BCQEWEG5vb251QGftYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI1MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAGTAldBMRAwDgYD
VQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6b24xZDASBgNVBASTC0lBTSBDb25z
b2x1MRIwEAYDVQQDEw1UZXR0Q21sYWx1ZAdBgkqhkiG9w0BCQEWEG5vb251QGft
YXpvbi5jb20wZGZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvYsWtC2XADZ4nB+BLygVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITx0USQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb30hjZnzcvcQAaRHhd1QWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJI1J00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp3780D8uTs7fLvJx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimv3rrszlaEXAMPLE=
-----END CERTIFICATE-----
```

如需詳細資訊，請參閱 AWS Private Certificate Authority 《使用者指南》中的[安裝根 CA 憑證](#)。

2. 使用 [issue-certificate](#) AWS CLI 命令在您的私有 CA 上發行和安裝根憑證。

```
$ aws acm-pca issue-certificate \
  --certificate-authority-arn arn:aws:acm-pca:aws-region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
  --csr file://ca.csr \
  --signing-algorithm SHA256WITHRSA \
  --template-arn arn:aws:acm-pca::template/RootCACertificate/V1 \
  --validity Value=3650,Type=DAYS --region aws-region
```

3. 使用 [get-certificate](#) AWS CLI 命令下載根憑證。

```
$ aws acm-pca get-certificate \
```

```
--certificate-authority-arn arn:aws:acm-pca:aws-region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
--certificate-arn arn:aws:acm-pca:aws-region:486768734100:certificate-authority/12345678-1234-1234-1234-123456789012/certificate/
abcdef0123456789abcdef0123456789 \
--output text --region aws-region > rootCA.pem
```

4. 使用 [import-certificate-authority-certificate](#) AWS CLI 命令在您的私有 CA 上安裝根憑證。

```
$ aws acm-pca import-certificate-authority-certificate \
--certificate-authority-arn arn:aws:acm-pca:aws-region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
--certificate file://rootCA.pem --region aws-region
```

## 產生和匯出檔案系統和用戶端憑證

1. 使用 [request-certificate](#) AWS CLI 命令來請求要在檔案系統和用戶端上使用的 AWS Certificate Manager 憑證。

```
$ aws acm request-certificate \
--domain-name *.ec2.internal \
--idempotency-token 12345 \
--region aws-region \
--certificate-authority-arn arn:aws:acm-pca:aws-region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012
```

如果請求成功，則會傳回已發行憑證的 ARN。

2. 為了安全起見，您必須在匯出私有金鑰時為其指派密碼短語。建立密碼短語並將其存放在名為 `passphrase.txt` 的檔案中。
3. 使用 [export-certificate](#) AWS CLI 命令匯出先前發行的私有憑證。匯出的檔案包含憑證、憑證鏈，以及與內嵌在憑證中的公有金鑰相關聯的加密私有 2048 位元 RSA 金鑰。為了安全起見，您必須在匯出私有金鑰時為其指派密碼短語。下列範例適用於 Linux EC2 執行個體。

```
$ aws acm export-certificate \
--certificate-arn arn:aws:acm:aws-region:111122223333:certificate/12345678-1234-1234-1234-123456789012 \
--passphrase $(cat passphrase.txt | base64) --region aws-region >
exported_cert.json
```



4. 使用下列jq命令，從JSON回應中擷取私有金鑰和憑證。

```
$ passphrase=$(cat passphrase.txt | base64)
cat exported_cert.json | jq -r .PrivateKey > prv.key

cat exported_cert.json | jq -r .Certificate > cert.pem
```

5. 使用下列openssl命令從JSON回應解密私有金鑰。輸入命令後，系統會提示您輸入密碼短語。

```
$ openssl rsa -in prv.key -passin pass:$passphrase -out decrypted.key
```

在 Amazon Linux 2 用戶端上安裝和設定 Libreswan IPsec

下列各節提供在執行 Amazon Linux 2 的 Amazon EC2 執行個體上安裝和設定 Libreswan IPsec 的說明。

安裝和設定 Libreswan

1. 使用 SSH 連線至 EC2 執行個體。如需如何執行此操作的特定指示，請參閱《Amazon Elastic Compute Cloud [Linux 執行個體使用者指南](#)》中的[使用 SSH 用戶端連線至 Linux 執行個體](#)。
2. 執行下列命令來安裝 libreswan：

```
$ sudo yum install libreswan
```

3. (選用) 在後續步驟中驗證 IPsec 時，如果沒有這些設定，可能會標記這些屬性。建議您先在沒有這些設定的情況下測試您的設定。如果您的連線有問題，請返回此步驟並進行下列變更。

安裝完成後，請使用您偏好的文字編輯器，將下列項目新增至 /etc/sysctl.conf 檔案。

```
net.ipv4.ip_forward=1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.lo.accept_redirects = 0
net.ipv4.conf.lo.send_redirects = 0
net.ipv4.conf.all.rp_filter = 0
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.eth0.rp_filter = 0
```

儲存變更並結束文字編輯器。

4. 套用變更。

```
$ sudo sysctl -p
```

5. 驗證 IPsec 組態。

```
$ sudo ipsec verify
```

確認您Libreswan安裝的 版本正在執行中。

6. 初始化 IPsec NSS 資料庫。

```
$ sudo ipsec checknss
```

### 在用戶端上安裝憑證

1. 將您為用戶端[產生的憑證](#)複製到 EC2 執行個體上的工作目錄。您
2. 將先前產生的憑證匯出為與 相容的格式libreswan。

```
$ openssl pkcs12 -export -in cert.pem -inkey decrypted.key \  
-certfile rootCA.pem -out certkey.p12 -name fsx
```

3. 匯入重新格式化的金鑰，並在出現提示時提供密碼短語。

```
$ sudo ipsec import certkey.p12
```

4. 使用偏好的文字編輯器建立 IPsec 組態檔案。

```
$ sudo cat /etc/ipsec.d/nfs.conf
```

將下列項目新增至組態檔案：

```
conn fsxn  
    authby=rsasig  
    left=172.31.77.6  
    right=198.19.254.13  
    auto=start  
    type=transport
```

```
ikev2=insist
keyexchange=ike
ike=aes256-sha2_384;dh20
esp=aes_gcm_c256
leftcert=fsx
lefttrsasigkey=%cert
leftid=%fromcert
rightid=%fromcert
righttrsasigkey=%cert
```

在檔案系統上設定 IPsec 後，您會在用戶端上啟動 IPsec。

在檔案系統上設定 IPsec

本節提供在 FSx for ONTAP 檔案系統上安裝憑證，以及設定 IPsec 的說明。

在檔案系統上安裝憑證

1. 將根憑證 (rootCA.pem)、用戶端憑證 (cert.pem) 和解密的金鑰 (decrypted.key) 檔案複製到您的檔案系統。您需要知道憑證的密碼短語。
2. 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。*management\_endpoint\_ip* 將取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

3. cat 在用戶端（而非檔案系統上）上使用來列出 cert.pem 和 decrypted.key 檔案的內容 rootCA.pem，讓您可以複製每個檔案的輸出，並在下列步驟中出現提示時貼上。

```
$ > cat cert.pem
```

複製憑證內容。

4. 除非已安裝憑證，否則您必須將所有在交互身分驗證期間使用的 CA 憑證，包括 ONTAP 端和用戶端 CAs，安裝到 ONTAP 憑證管理（如同 ONTAP 自我簽署根 CA 的情況）。

使用 security certificate install NetApp CLI 命令來安裝用戶端憑證，如下所示：

```
FSxID123:: > security certificate install -vserver dr -type client -cert-name  
ipsec-client-cert
```

Please enter Certificate: Press <Enter> when done

貼上您先前複製cert.pem的檔案內容，然後按 Enter 鍵。

Please enter Private Key: Press <Enter> when done

貼上 decrypted.key 檔案的內容，然後按 Enter 鍵。

Do you want to continue entering root and/or intermediate certificates {y|n}:

輸入 n 以完成輸入用戶端憑證。

5. 建立並安裝憑證以供 SVM 使用。此憑證的發行者 CA 必須已安裝至 IPsec ONTAP並新增至 IPsec。 IPsec

使用下列命令來安裝根憑證。

```
FSxID123:: > security certificate install -vserver dr -type server-ca -cert-name  
ipsec-ca-cert
```

Please enter Certificate: Press <Enter> when done

貼上 rootCA.pem 檔案的內容，然後按 Enter 鍵。

6. 若要確保在身分驗證期間安裝的 CA 位於 IPsec CA 搜尋路徑中，請使用「安全 ipsec ca-certificate add」命令將ONTAP憑證管理 CAs 新增至 IPsec 模組。

輸入下列命令來新增根憑證。

```
FSxID123:: > security ipsec ca-certificate add -vserver dr -ca-certs ipsec-ca-cert
```

7. 輸入下列命令，在安全政策資料庫 (SPD) 中建立所需的 IPsec 政策。

```
security ipsec policy create -vserver dr -name policy-name -local-ip-  
subnets 198.19.254.13/32 -remote-ip-subnets 172.31.0.0/16 -auth-method PKI -action
```

```
ESP_TRA -cipher-suite SUITEB_GCM256 -cert-name ipsec-client-cert -local-identity
"CN=*.ec2.internal" -remote-identity "CN=*.ec2.internal"
```

8. 使用下列命令來顯示檔案系統的 IPsec 政策以進行確認。

```
FSxID123:: > security ipsec policy show -vserver dr -instance
```

```

                Vserver: dr
                Policy Name: promise
                Local IP Subnets: 198.19.254.13/32
                Remote IP Subnets: 172.31.0.0/16
                Local Ports: 0-0
                Remote Ports: 0-0
                Protocols: any
                Action: ESP_TRA
                Cipher Suite: SUITEB_GCM256
                IKE Security Association Lifetime: 86400
                IPsec Security Association Lifetime: 28800
                IPsec Security Association Lifetime (bytes): 0
                Is Policy Enabled: true
                Local Identity: CN=*.ec2.internal
                Remote Identity: CN=*.ec2.internal
                Authentication Method: PKI
                Certificate for Local Identity: ipsec-client-cert
```

## 在用戶端上啟動 IPsec

現在 IPsec 已在 FSx for ONTAP 檔案系統和用戶端上設定，您可以在用戶端上啟動 IPsec。

1. 使用 SSH 連線至您的用戶端系統。
2. 啟動 IPsec。

```
$ sudo ipsec start
```

3. 檢查 IPsec 的狀態。

```
$ sudo ipsec status
```

4. 在您的檔案系統上掛載磁碟區。

```
$ sudo mount -t nfs 198.19.254.13:/benchmark /home/ec2-user/acm/dr
```

## 5. 透過在 FSx for ONTAP 檔案系統上顯示加密連線來驗證 IPsec 設定。

```
FSxID123:: > security ipsec show-ikesa -node FsxId123
FsxId08ac16c7ec2781a58::> security ipsec show-ikesa -node FsxId08ac16c7ec2781a58-01
```

| Vserver | Policy Name        | Local Address | Remote Address | Initiator-SPI    | State       |
|---------|--------------------|---------------|----------------|------------------|-------------|
| dr      | <i>policy-name</i> | 198.19.254.13 | 172.31.77.6    | 551c55de57fe8976 | ESTABLISHED |
| fsx     | <i>policy-name</i> | 198.19.254.38 | 172.31.65.193  | 4fd3f22c993e60c5 | ESTABLISHED |

2 entries were displayed.

### 為多個用戶端設定 IPsec

當少數用戶端需要利用 IPsec 時，為每個用戶端使用單一 SPD 項目就已足夠。不過，當數百甚至數千個用戶端需要利用 IPsec 時，我們建議您使用 IPsec 多個用戶端組態。

FSx for ONTAP 支援跨多個網路將多個用戶端連接到啟用 IPsec 的單一 SVM IP 地址。您可以使用 subnet 組態或 Allow all clients 組態來完成此操作，如下列程序所述：

### 使用子網路組態為多個用戶端設定 IPsec

若要允許特定子網路上的所有用戶端（例如 192.168.134.0/24）使用單一 SPD 政策項目連線到單一 SVM IP 地址，您必須 remote-ip-subnets 以子網路形式指定。此外，您必須指定具有正確用戶端身分 remote-identity 的欄位。

#### Important

使用憑證身分驗證時，每個用戶端都可以使用自己的唯一憑證或共用憑證進行身分驗證。FSx for ONTAP IPsec 會根據本機信任存放區上安裝的 CAs 檢查憑證的有效性。FSx for ONTAP 也支援憑證撤銷清單 (CRL) 檢查。

- 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。*management\_endpoint\_ip* 將取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

2. 使用 CLI `security ipsec policy create` NetApp ONTAP 命令，如下所示，將##值取代為您的特定值。

```
FsxId123456::> security ipsec policy create -vserver svm_name -name policy_name \
  -local-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 \
  -local-ports 2049 -protocols tcp -auth-method PSK \
  -cert-name my_nfs_server_cert -local-identity ontap_side_identity \
  -remote-identity client_side_identity
```

使用 允許所有用戶端組態為多個用戶端設定 IPsec

若要允許任何用戶端，無論其來源 IP 地址為何，連線到已啟用 SVM IPsec 的 IP 地址，請在指定 `remote-ip-subnets` 欄位時使用 `0.0.0.0/0` 萬用字元。

此外，您必須指定具有正確用戶端身分 `remote-identity` 的欄位。對於憑證身分驗證，您可以輸入 ANYTHING。

此外，使用 `0.0.0.0/0` 萬用字元時，您必須設定要使用的特定本機或遠端連接埠號碼。例如，NFS 連接埠 2049。

1. 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。*management\_endpoint\_ip* 將取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

2. 使用 `security ipsec policy create` NetApp ONTAP CLI 命令，如下所示，將##值取代為您的特定值。

```
FsxId123456::> security ipsec policy create -vserver svm_name -name policy_name \
  -local-ip-subnets 192.168.134.34/32 -remote-ip-subnets 0.0.0.0/0 \
  -local-ports 2049 -protocols tcp -auth-method PSK \
  -cert-name my_nfs_server_cert -local-identity ontap_side_identity \
  -local-ports 2049 -remote-identity client_side_identity
```

# Amazon FSx for NetApp ONTAP 的身分和存取管理

AWS Identity and Access Management (IAM) 是一種 AWS 服務，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證（登入）和授權（具有許可）來使用 Amazon FSx 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](#)
- [Amazon FSx for NetApp ONTAP 如何與 IAM 搭配使用](#)
- [Amazon FSx for NetApp ONTAP 的身分型政策範例](#)
- [對 Amazon FSx for NetApp ONTAP 身分和存取進行故障診斷](#)
- [使用 Amazon FSx 的服務連結角色](#)
- [搭配 Amazon FSx 使用標籤](#)

## 目標對象

您使用 AWS Identity and Access Management (IAM) 的方式會有所不同，取決於您在 Amazon FSx 中執行的工作。

服務使用者 – 如果您使用 Amazon FSx 服務來執行任務，您的管理員會為您提供所需的登入資料和許可。當您使用更多 Amazon FSx 功能來執行工作時，您可能需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取 Amazon FSx 中的功能，請參閱 [對 Amazon FSx for NetApp ONTAP 身分和存取進行故障診斷](#)。

服務管理員 – 如果您在公司負責 Amazon FSx 資源，您可能擁有 Amazon FSx 的完整存取權。您的任務是判斷服務使用者應存取哪些 Amazon FSx 功能和資源。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步了解貴公司如何搭配 Amazon FSx 使用 IAM，請參閱 [Amazon FSx for NetApp ONTAP 如何與 IAM 搭配使用](#)。

IAM 管理員 – 如果您是 IAM 管理員，建議您了解撰寫政策以管理 Amazon FSx 存取的詳細資訊。若要檢視您可以在 IAM 中使用的 Amazon FSx 身分型政策範例，請參閱 [Amazon FSx for NetApp ONTAP 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 帳戶根使用者身分、IAM 使用者身分或擔任 IAM 角色來驗證（登入 AWS）。

您可以使用透過身分來源提供的登入資料，以聯合身分 AWS 身分登入。AWS IAM Identity Center (IAM Identity Center) 使用者、您公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料，都是聯合身分的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使用聯合 AWS 身分存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱 AWS 登入 [《使用者指南》中的如何登入您的 AWS 帳戶](#)。

如果您以 AWS 程式設計方式存取，AWS 會提供軟體開發套件 (SDK) 和命令列界面 (CLI)，以使用您的登入資料以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱《IAM 使用者指南》中的[適用於 API 請求的 AWS Signature 第 4 版](#)。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如，AWS 建議您使用多重驗證 (MFA) 來提高帳戶的安全性。如需更多資訊，請參閱《AWS IAM Identity Center 使用者指南》中的[多重要素驗證](#)和《IAM 使用者指南》中的[IAM 中的 AWS 多重要素驗證](#)。

### AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取帳戶中的所有 AWS 服務和資源。此身分稱為 AWS 帳戶 Theroot 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，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

根據最佳實務，要求人類使用者，包括需要管理員存取權的使用者，使用聯合身分提供者 AWS 服務來使用臨時憑證來存取。

聯合身分是您企業使用者目錄、Web 身分提供者、AWS Directory Service、Identity Center 目錄，或 AWS 服務是透過身分來源提供的登入資料存取的任何使用者。當聯合身分存取時 AWS 帳戶，它們會擔任角色，而角色會提供臨時登入資料。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連接並同步到您自己的身分來源中的一組使用者 AWS 帳戶和群組，以便

在所有和應用程式中使用。如需 IAM Identity Center 的詳細資訊，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](#)是中的身分 AWS 帳戶，具有單一人員或應用程式的特定許可。建議您盡可能依賴臨時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 [IAM 使用者指南](#)中的為需要長期憑證的使用案例定期輪換存取金鑰。

[IAM 群組](#)是一種指定 IAM 使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供臨時憑證。如需更多資訊，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](#)是中具有特定許可 AWS 帳戶的身分。它類似 IAM 使用者，但不與特定的人員相關聯。若要暫時在中擔任 IAM 角色 AWS Management Console，您可以從[使用者切換至 IAM 角色（主控台）](#)。您可以透過呼叫 AWS CLI 或 AWS API 操作或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱《IAM 使用者指南》中的[擔任角色的方法](#)。

使用臨時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱《[IAM 使用者指南](#)》中的為第三方身分提供者 (聯合) 建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的[許可集](#)。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。不過，對於某些 AWS 服務，您可以直接將政策連接到資源 (而不是使用角色做為代理)。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](#)。

- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
- 轉送存取工作階段 (FAS) – 當您使用 IAM 使用者或角色在其中執行動作時 AWS，您會被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫的委託人許可 AWS 服務，結合 AWS 服務 請求向下游服務提出請求。只有在服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱 [《轉發存取工作階段》](#)。
- 服務角色 – 服務角色是服務擔任的 [IAM 角色](#)，可代表您執行動作。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權給 AWS 服務](#)。
- 服務連結角色 – 服務連結角色是一種連結至 的服務角色類型 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 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。
- 在 Amazon EC2 上執行的應用程式 – 您可以使用 IAM 角色來管理在 EC2 執行個體上執行之應用程式的臨時登入資料，以及提出 AWS CLI 或 AWS API 請求。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體描述檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得臨時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的[使用 IAM 角色來授予許可權給 Amazon EC2 執行個體上執行的應用程式](#)。

## 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。政策是 中的物件，AWS 當與身分或資源相關聯時，會定義其許可。當委託人（使用者、根使用者或角色工作階段）發出請求時，會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策會以 JSON 文件 AWS 的形式存放在 中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的 [JSON 政策概觀](#)。

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。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。

預設情況下，使用者和角色沒有許可。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。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該政策的使用者可以從 AWS Management Console AWS CLI、或 API AWS 取得角色資訊。

## 身分型政策

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](#)。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管政策是獨立的政策，您可以連接到中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受管政策和客戶受管政策。如需了解如何在受管政策及內嵌政策之間選擇，請參閱《IAM 使用者指南》中的[在受管政策和內嵌政策間選擇](#)。

## 資源型政策

資源型政策是連接到資源的 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。

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用來自 IAM 的 AWS 受管政策。

## 存取控制清單 (ACL)

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。

Amazon S3 AWS WAF 和 Amazon VPC 是支援 ACLs 的服務範例。如需進一步了解 ACL，請參閱 Amazon Simple Storage Service 開發人員指南中的[存取控制清單 \(ACL\) 概觀](#)。

## 其他政策類型

AWS 支援其他較不常見的政策類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交

集。會在 Principal 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的 [IAM 實體許可界限](#)。

- 服務控制政策 (SCPs) – SCPs 是 JSON 政策，可指定中組織或組織單位 (OU) 的最大許可 AWS Organizations。AWS Organizations 是一種用於分組和集中管理您企業擁有 AWS 帳戶之多個的服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 會限制成員帳戶中實體的許可，包括每個實體 AWS 帳戶根使用者。如需 Organizations 和 SCP 的詳細資訊，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) - RCP 是 JSON 政策，可用來設定您帳戶中資源的可用許可上限，採取這種方式就不需要更新附加至您所擁有的每個資源的 IAM 政策。RCP 會限制成員帳戶中資源的許可，並可能影響身分的有效許可，包括 AWS 帳戶根使用者，無論它們是否屬於您的組織。如需 Organizations 和 RCPs 的詳細資訊，包括支援 RCPs AWS 服務的清單，請參閱 AWS Organizations 《使用者指南》中的 [資源控制政策 \(RCPs\)](#)。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過撰寫程式的方式建立角色或聯合使用者的暫時工作階段時，做為參數傳遞。所產生工作階段的許可會使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南中的 [工作階段政策](#)。

## 多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要了解如何 AWS 在涉及多個政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的 [政策評估邏輯](#)。

## Amazon FSx for NetApp ONTAP 如何與 IAM 搭配使用

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

您可以搭配 Amazon FSx for NetApp ONTAP 使用的 IAM 功能

| IAM 功能                | Amazon FSx 支援 |
|-----------------------|---------------|
| <a href="#">身分型政策</a> | 是             |
| <a href="#">資源型政策</a> | 否             |



| IAM 功能                         | Amazon FSx 支援 |
|--------------------------------|---------------|
| <a href="#">政策動作</a>           | 是             |
| <a href="#">政策資源</a>           | 是             |
| <a href="#">政策條件索引鍵</a>        | 是             |
| <a href="#">ACL</a>            | 否             |
| <a href="#">ABAC (政策中的標籤)</a>  | 是             |
| <a href="#">臨時憑證</a>           | 是             |
| <a href="#">轉送存取工作階段 (FAS)</a> | 是             |
| <a href="#">服務角色</a>           | 否             |
| <a href="#">服務連結角色</a>         | 是             |

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

## Amazon FSx 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。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。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](#)。

## Amazon FSx 的身分型政策範例

若要檢視 Amazon FSx 身分型政策的範例，請參閱 [Amazon FSx for NetApp ONTAP 的身分型政策範例](#)。

## Amazon FSx 中的資源型政策

支援資源型政策：否

## Amazon FSx 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。政策動作通常具有與相關聯 AWS API 操作相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看 Amazon FSx 動作的清單，請參閱《服務授權參考》中的 [Amazon FSx 定義的動作](#)。

Amazon FSx 中的政策動作在動作之前使用下列字首：

```
fsx
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

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

若要檢視 Amazon FSx 身分型政策的範例，請參閱 [Amazon FSx for NetApp ONTAP 的身分型政策範例](#)。

## Amazon FSx 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。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 [Amazon Resource Name \(ARN\)](#) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (\*) 來表示陳述式適用於所有資源。

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

若要查看 Amazon FSx 資源類型及其 ARNs，請參閱《服務授權參考》中的 [Amazon FSx 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 [Amazon FSx 定義的動作](#)。

若要檢視 Amazon FSx 身分型政策的範例，請參閱 [Amazon FSx for NetApp ONTAP 的身分型政策範例](#)。

## Amazon FSx 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 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用 [條件運算子](#) 的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵，AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，會使用邏輯 OR 操作 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 [IAM 政策元素：變數和標籤](#)。

AWS 支援全域條件金鑰和服務特定的條件金鑰。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 Amazon FSx 條件索引鍵的清單，請參閱《服務授權參考》中的 [Amazon FSx 的條件索引鍵](#)。若要了解您可以使用條件金鑰的動作和資源，請參閱 [Amazon FSx 定義的動作](#)。

若要檢視 Amazon FSx 身分型政策的範例，請參閱 [Amazon FSx for NetApp ONTAP 的身分型政策範例](#)。



## Amazon FSx 中的存取控制清單 (ACLs)

支援 ACL：否

## 使用 Amazon FSx 的屬性型存取控制 (ABAC)

支援 ABAC (政策中的標籤)：是

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在 AWS 中，這些屬性稱為標籤。您可以將標籤連接到 IAM 實體（使用者或角色）和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

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 \(ABAC\)](#)。

如需標記 Amazon FSx 資源的詳細資訊，請參閱 [標記 Amazon FSx 資源](#)。

若要檢視身分型政策範例，以根據該資源上的標籤來限制存取資源，請參閱 [使用標籤來控制對 Amazon FSx 資源的存取](#)。

## 搭配 Amazon FSx 使用暫時登入資料

支援臨時憑證：是

當您使用臨時登入資料登入時，有些 AWS 服務 無法運作。如需其他資訊，包括哪些 AWS 服務 使用臨時登入資料，請參閱《[AWS 服務 IAM 使用者指南](#)》中的使用 IAM 的。

如果您 AWS Management Console 使用使用者名稱和密碼以外的任何方法登入，則使用臨時登入資料。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立臨時登入資料。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱《IAM 使用者指南》中的 [從使用者切換至 IAM 角色 \(主控台\)](#)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱 [IAM 中的暫時性安全憑證](#)。

## 轉送 Amazon FSx 的存取工作階段

支援轉寄存取工作階段 (FAS)：是

當您使用 IAM 使用者或角色在 中執行動作時 AWS，您會被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，結合 AWS 服務 請求向下游服務提出請求。只有在服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱[轉發存取工作階段](#)。

## Amazon FSx 的服務角色

支援服務角色：否

## Amazon FSx 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 Amazon FSx 服務連結角色的詳細資訊，請參閱 [使用 Amazon FSx 的服務連結角色](#)。

## Amazon FSx for NetApp ONTAP 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 Amazon FSx 資源的許可。他們也無法使用 AWS Management Console、AWS Command Line Interface (AWS CLI) 或 AWS API 來執行任務。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。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

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 Amazon FSx 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 [Amazon FSx 的動作、資源和條件索引鍵](#)。

### 主題

- [政策最佳實務](#)
- [使用 Amazon FSx 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 Amazon FSx 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 AWS 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》[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_credentials\\_mfa\\_configure-api-require.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html) 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 Amazon FSx 主控台

若要存取 Amazon FSx for NetApp ONTAP 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 Amazon FSx 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 Amazon FSx 主控台，也請將 AmazonFSxConsoleReadOnlyAccess 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](#)。

您可以在 中查看 AmazonFSxConsoleReadOnlyAccess 和其他 Amazon FSx 受管服務政策[AWS Amazon FSx for OpenZFS 的 受管政策](#)。

## 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": "*"
    }
  ]
}
```

```
}
```

## 對 Amazon FSx for NetApp ONTAP 身分和存取進行故障診斷

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

### 主題

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

### 我無權在 Amazon FSx 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 fsx:*GetWidget* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
fsx: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 fsx:*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 Amazon FSx。

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。

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

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

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

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

## 我想要允許以外的人員 AWS 帳戶 存取我的 Amazon FSx 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 Amazon FSx 是否支援這些功能，請參閱 [Amazon FSx for NetApp ONTAP 如何與 IAM 搭配使用](#)。
- 若要了解如何提供您擁有 AWS 帳戶 的資源存取權，請參閱《[IAM 使用者指南](#)》中的在您擁有 AWS 帳戶 的另一個 中為 IAM 使用者提供存取權。
- 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](#)。

## 使用 Amazon FSx 的服務連結角色

Amazon FSx 使用 AWS Identity and Access Management (IAM) [服務連結角色](#)。服務連結角色是直接連結至 Amazon FSx 的唯一 IAM 角色類型。服務連結角色是由 Amazon FSx 預先定義，並包含該服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓您更輕鬆地設定 Amazon FSx，因為您不必手動新增必要的許可。Amazon FSx 會定義其服務連結角色的許可，除非另有定義，否則只有 Amazon FSx 可以擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

您必須先刪除服務連結角色的相關資源，才能將其刪除。這可保護您的 Amazon FSx 資源，因為您不會不小心移除存取資源的許可。

如需關於支援服務連結角色的其他服務的資訊，請參閱[可搭配 IAM 運作的 AWS 服務](#)，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (是) 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。



## Amazon FSx 的服務連結角色許可

Amazon FSx 使用名為 `AWSServiceRoleForAmazonFSx` 的服務連結角色 – 在您的帳戶中執行特定動作，例如為 VPC 中的檔案系統建立彈性網路界面，以及在 CloudWatch 中發佈檔案系統和磁碟區指標。

如需此政策的更新，請參閱 [AmazonFSxServiceRolePolicy](#)

許可詳細資訊

許可詳細資訊

`AWSServiceRoleForAmazonFSx` 角色許可是由 `AmazonFSxServiceRolePolicy` AWS 受管政策所定義。`AWSServiceRoleForAmazonFSx` 具有下列許可：

### Note

所有 Amazon FSx 檔案系統類型都會使用 `AWSServiceRoleForAmazonFSx`；某些列出的許可不適用於 FSx for ONTAP。

- `ds` – 允許 Amazon FSx 檢視、授權和取消授權 AWS Directory Service 目錄中的應用程式。
- `ec2` – 允許 Amazon FSx 執行下列動作：
  - 檢視、建立和取消關聯與 Amazon FSx 檔案系統相關聯的網路介面。
  - 檢視與 Amazon FSx 檔案系統相關聯的一或多個彈性 IP 地址。
  - 檢視與 Amazon FSx 檔案系統相關聯的 Amazon VPCs、安全群組和子網路。
  - 為所有可與 VPC 搭配使用的安全群組提供增強型安全群組驗證。
  - 建立許可，讓 AWS 授權的使用者在網路界面上執行特定操作。
- `cloudwatch` – 允許 Amazon FSx 在 AWS/FSx 命名空間下將指標資料點發佈至 CloudWatch。
- `route53` – 允許 Amazon FSx 將 Amazon VPC 與私有託管區域建立關聯。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateFileSystem",
      "Effect": "Allow",
      "Action": [
```

```

        "ds:AuthorizeApplication",
        "ds:GetAuthorizedApplicationDetails",
        "ds:UnauthorizeApplication",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeAddresses",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVPCs",
        "ec2:DisassociateAddress",
        "ec2:GetSecurityGroupsForVpc",
        "route53:AssociateVPCWithHostedZone"
    ],
    "Resource": "*"
},
{
    "Sid": "PutMetrics",
    "Effect": "Allow",
    "Action": [
        "cloudwatch:PutMetricData"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringEquals": {
            "cloudwatch:namespace": "AWS/FSx"
        }
    }
},
{
    "Sid": "TagResourceNetworkInterface",
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:network-interface/*"
    ],

```



```

        "Condition": {
            "StringEquals": {
                "ec2:CreateAction": "CreateNetworkInterface"
            },
            "ForAllValues:StringEquals": {
                "aws:TagKeys": "AmazonFSx.FileSystemId"
            }
        }
    },
    {
        "Sid": "ManageNetworkInterface",
        "Effect": "Allow",
        "Action": [
            "ec2:AssignPrivateIpAddresses",
            "ec2:ModifyNetworkInterfaceAttribute",
            "ec2:UnassignPrivateIpAddresses"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:network-interface/*"
        ],
        "Condition": {
            "Null": {
                "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
            }
        }
    },
    {
        "Sid": "ManageRouteTable",
        "Effect": "Allow",
        "Action": [
            "ec2:CreateRoute",
            "ec2:ReplaceRoute",
            "ec2>DeleteRoute"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:route-table/*"
        ],
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
            }
        }
    }
}
]

```

```
}
```

此政策的任何更新都會在 [中說明 AWS 受管政策的 Amazon FSx 更新](#)。

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的 [服務連結角色許可](#)。

## 為 Amazon FSx 建立服務連結角色

您不需要手動建立一個服務連結角色。當您在 AWS Management Console、IAM CLI 或 IAM API 中建立檔案系統時，Amazon FSx 會為您建立服務連結角色。

### Important

此服務連結角色可以顯示在您的帳戶，如果您於其他服務中完成一項動作時，可以使用支援此角色的功能。若要進一步了解，請參閱 [我的 IAM 帳戶中出現的新角色](#)。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您建立檔案系統時，Amazon FSx 會再次為您建立服務連結角色。

## 編輯 Amazon FSx 的服務連結角色

Amazon FSx 不允許您編輯 AWSServiceRoleForAmazonFSx 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需更多資訊，請參閱 IAM 使用者指南中的 [編輯服務連結角色](#)。

## 刪除 Amazon FSx 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。不過，您必須先刪除所有檔案系統和備份，才能手動刪除服務連結角色。

### Note

如果您嘗試刪除資源時，Amazon FSx 服務正在使用該角色，則刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

## 使用 IAM 手動刪除服務連結角色

使用 IAM 主控台、IAM CLI 或 IAM API 來刪除 AWSServiceRoleForAmazonFSx 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[刪除服務連結角色](#)。

## Amazon FSx 服務連結角色支援的區域

Amazon FSx 支援在提供服務的所有區域中使用服務連結角色。如需詳細資訊，請參閱 [AWS 區域與端點](#)。

## 搭配 Amazon FSx 使用標籤

您可以使用標籤來控制對 Amazon FSx 資源的存取，以及實作屬性型存取控制 (ABAC)。若要在建立期間將標籤套用至 Amazon FSx 資源，使用者必須具有特定 AWS Identity and Access Management (IAM) 許可。

### 在建立期間授予標籤資源的許可

透過一些建立資源的 Amazon FSx API 動作，您可以在建立資源時指定標籤。您可以使用這些資源標籤來實作屬性型存取控制 (ABAC)。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS ?](#)。

若要讓使用者在建立資源時加上標籤，他們必須具有使用建立資源之動作的許可，例如 `fsx:CreateFileSystem`、`fsx:CreateStorageVirtualMachine` 或 `fsx:CreateVolume`。如果在資源建立動作中指定標籤，IAM 會對 `fsx:TagResource` 動作執行額外的授權，以驗證使用者是否具有建立標籤的許可。因此，使用者必須同時具備使用 `fsx:TagResource` 動作的明確許可。

下列範例政策允許使用者建立檔案系統和儲存虛擬機器 (SVMs)，並在建立特定 期間將標籤套用至它們 AWS 帳戶。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateFileSystem",
        "fsx:CreateStorageVirtualMachine",
        "fsx:TagResource"
      ],
      "Resource": [
        "arn:aws:fsx:region:account-id:file-system/*",
        "arn:aws:fsx:region:account-id:file-system/*/storage-virtual-machine/*"
      ]
    }
  ]
}
```

```
}  
]  
}
```

同樣地，以下政策允許使用者在特定檔案系統上建立備份，並在備份建立期間將任何標籤套用至備份。

```
{  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "fsx:CreateBackup"  
      ],  
      "Resource": "arn:aws:fsx:region:account-id:file-system/file-system-id*"  
    },  
    {  
      "Effect": "Allow",  
      "Action": [  
        "fsx:TagResource"  
      ],  
      "Resource": "arn:aws:fsx:region:account-id:backup/*"  
    }  
  ]  
}
```

只有在資源建立 `fsx:TagResource` 動作期間套用標籤時，才會評估動作。因此，如果請求中未指定標籤，則具有建立資源許可（假設沒有標記條件）的使用者不需要使用 `fsx:TagResource` 動作的許可。然而，若該使用者試圖建立具有標籤的資源卻未具備使用 `fsx:TagResource` 動作的許可，則該請求會失敗。

如需標記 Amazon FSx 資源的詳細資訊，請參閱 [標記 Amazon FSx 資源](#)。如需使用標籤控制 Amazon FSx 資源存取的詳細資訊，請參閱 [使用標籤來控制對 Amazon FSx 資源的存取](#)。

## 使用標籤來控制對 Amazon FSx 資源的存取

若要控制對 Amazon FSx 資源和動作的存取，您可以根據標籤使用 IAM 政策。您可以透過兩個方式提供控制：

- 您可以根據這些資源上的標籤來控制對 Amazon FSx 資源的存取。
- 您可以控制在 IAM 請求條件中傳遞的標籤。

如需有關如何使用標籤來控制 AWS 資源存取的資訊，請參閱《IAM 使用者指南》中的[使用標籤控制存取](#)。如需在建立時標記 Amazon FSx 資源的詳細資訊，請參閱[在建立期間授予標籤資源的許可](#)。如需標記資源的詳細資訊，請參閱[標記 Amazon FSx 資源](#)。

### 根據資源的標籤控制存取

若要控制使用者或角色可以在 Amazon FSx 資源上執行的動作，您可以在資源上使用標籤。例如，您可能想要根據資源上標籤的金鑰值組，允許或拒絕檔案系統資源上的特定 API 操作。

#### Example 範例政策 – 僅在使用特定標籤時建立檔案系統

此政策允許使用者建立檔案系統，只有在它們使用特定標籤鍵/值對標記時，在此範例中為 key=Department、value=Finance。

```
{
  "Effect": "Allow",
  "Action": [
    "fsx:CreateFileSystem",
    "fsx:TagResource"
  ],
  "Resource": "arn:aws:fsx:region:account-id:file-system/*",
  "Condition": {
    "StringEquals": {
      "aws:RequestTag/Department": "Finance"
    }
  }
}
```

#### Example 範例政策 – 僅建立具有特定標籤之 NetApp ONTAP 磁碟區的 Amazon FSx 備份

此政策允許使用者僅針對以鍵值對 key=Department、標記的 ONTAP 磁碟區建立 FSx 備份 value=Finance。備份是使用標籤 建立的 Department=Finance。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateBackup"
      ],

```

```

    "Resource": "arn:aws:fsx:region:account-id:volume/*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/Department": "Finance"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "fsx:TagResource",
      "fsx:CreateBackup"
    ],
    "Resource": "arn:aws:fsx:region:account-id:backup/*",
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/Department": "Finance"
      }
    }
  }
]
}

```

### Example 範例政策 – 從具有特定標籤的備份建立具有特定標籤的磁碟區

此政策允許使用者建立Department=Finance僅從使用 標記的備份中標記的磁碟區Department=Finance。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateVolumeFromBackup",
        "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:volume/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/Department": "Finance"
        }
      }
    }
  ]
}

```

```

    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "fsx:CreateVolumeFromBackup"
    ],
    "Resource": "arn:aws:fsx:region:account-id:backup/*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/Department": "Finance"
      }
    }
  }
]
}

```

### Example 範例政策 – 刪除具有特定標籤的檔案系統

此政策允許使用者僅刪除以 標記的檔案系統Department=Finance。如果他們建立最終備份，則必須使用 標記Department=Finance。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx>DeleteFileSystem"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Department": "Finance"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:backup/*",

```

```

        "Condition": {
            "StringEquals": {
                "aws:RequestTag/Department": "Finance"
            }
        }
    ]
}

```

### Example 範例政策 – 刪除具有特定標籤的磁碟區

此政策允許使用者僅刪除以 標記的磁碟區Department=Finance。如果他們建立最終備份，則必須使用 標記Department=Finance。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:DeleteVolume"
      ],
      "Resource": "arn:aws:fsx:region:account-id:volume/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Department": "Finance"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:backup/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/Department": "Finance"
        }
      }
    }
  ]
}

```



# AWS Amazon FSx for OpenZFS 的 受管政策

AWS 受管政策是由 AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住，AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的[客戶管理政策](#)，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新受 AWS 管政策中定義的許可，則更新會影響政策連接的所有主體身分（使用者、群組和角色）。當新的 AWS 服務啟動或新的 API 操作可用於現有服務時，AWS 最有可能更新 AWS 受管政策。

如需詳細資訊，請參閱《IAM 使用者指南》中的[AWS 受管政策](#)。

## AmazonFSxServiceRolePolicy

允許 Amazon FSx 代表您管理 AWS 資源。如需進一步了解，請參閱[使用 Amazon FSx 的服務連結角色](#)。

## AWS 受管政策：AmazonFSxDeleteServiceLinkedRoleAccess

您不得將 AmazonFSxDeleteServiceLinkedRoleAccess 連接到 IAM 實體。此政策會連結至服務，並僅用於該服務的服務連結角色。您無法連接、取消連接、修改或刪除此政策。如需詳細資訊，請參閱[使用 Amazon FSx 的服務連結角色](#)。

此政策授予管理許可，允許 Amazon FSx 刪除其 Amazon S3 存取的服務連結角色，僅供 Amazon FSx for Lustre 使用。

### 許可詳細資訊

此政策包含中的許可iam，允許 Amazon FSx 檢視、刪除和檢視 FSx Service Linked Roles for Amazon S3 存取的刪除狀態。

若要檢視此政策的許可，請參閱《AWS 受管政策參考指南》中的[AmazonFSxDeleteServiceLinkedRoleAccess](#)。

## AWS 受管政策：AmazonFSxFullAccess

您可以將 AmazonFSxFullAccess 連接至您的 IAM 實體。Amazon FSx 也會將此政策連接至允許 Amazon FSx 代表您執行動作的服務角色。

提供 Amazon FSx 的完整存取權和相關 AWS 服務的存取權。

### 許可詳細資訊

此政策包含以下許可。

- `fsx` – 允許主體完整存取以執行所有 Amazon FSx 動作，但除外 `BypassSnaplockEnterpriseRetention`。
- `ds` – 允許主體檢視 AWS Directory Service 目錄的相關資訊。
- `ec2`
  - 允許主體在指定的條件下建立標籤。
  - 為所有可與 VPC 搭配使用的安全群組提供增強型安全群組驗證。
- `iam` – 允許原則代表使用者建立 Amazon FSx 服務連結角色。這是必要的，以便 Amazon FSx 可以代表使用者管理 AWS 資源。
- `firehose` – 允許主體將記錄寫入 Amazon Data Firehose。這是必要的，以便使用者可以透過傳送稽核存取日誌到 Firehose 來監控 FSx for Windows File Server 檔案系統存取。
- `logs` – 允許主體建立日誌群組、日誌串流，以及將事件寫入日誌串流。這是必要的，讓使用者可以透過傳送稽核存取日誌到 CloudWatch Logs 來監控 FSx for Windows File Server 檔案系統存取。

若要檢視此政策的許可，請參閱《AWS 受管政策參考指南》中的 [AmazonFSxFullAccess](#)。

## AWS 受管政策：AmazonFSxConsoleFullAccess

您可將 `AmazonFSxConsoleFullAccess` 政策連接到 IAM 身分。

此政策會授予管理許可，以允許完整存取 Amazon FSx 並透過存取相關 AWS 服務 AWS Management Console。

### 許可詳細資訊

此政策包含以下許可。

- `fsx` – 允許主體在 Amazon FSx 管理主控台中執行所有動作，但除外 `BypassSnaplockEnterpriseRetention`。
- `cloudwatch` – 允許主體在 Amazon FSx 管理主控台中檢視 CloudWatch 警示和指標。
- `ds` – 允許主體列出 AWS Directory Service 目錄的相關資訊。

- ec2
  - 允許主體在路由表上建立標籤、列出網路介面、路由表、安全群組、子網路以及與 Amazon FSx 檔案系統相關聯的 VPC。
  - 允許主體為所有可與 VPC 搭配使用的安全群組提供增強型安全群組驗證。
  - 允許主體檢視與 Amazon FSx 檔案系統相關聯的彈性網路介面。
- kms – 允許主體列出 AWS Key Management Service 金鑰的別名。
- s3 – 允許主體列出 Amazon S3 儲存貯體中的部分或全部物件（最多 1000 個）。
- iam – 准許建立服務連結角色，以允許 Amazon FSx 代表使用者執行動作。

若要檢視此政策的許可，請參閱《AWS 受管政策參考指南》中的 [AmazonFSxConsoleFullAccess](#)。

## AWS 受管政策：AmazonFSxConsoleReadOnlyAccess

您可將 AmazonFSxConsoleReadOnlyAccess 政策連接到 IAM 身分。

此政策會授予 Amazon FSx 和相關 AWS 服務的唯讀許可，讓使用者可以在 中檢視這些服務的相關資訊 AWS Management Console。

### 許可詳細資訊

此政策包含以下許可。

- fsx – 允許主體在 Amazon FSx 管理主控台中檢視 Amazon FSx 檔案系統的相關資訊，包括所有標籤。
- cloudwatch – 允許主體在 Amazon FSx 管理主控台中檢視 CloudWatch 警示和指標。
- ds – 允許主體在 Amazon FSx 管理主控台中檢視 AWS Directory Service 目錄的相關資訊。
- ec2
  - 允許主體在 Amazon FSx FSx 管理主控台中檢視與 Amazon FSx 檔案系統相關聯的網路介面、安全群組、子網路和 VPC。
  - 允許主體為所有可與 VPC 搭配使用的安全群組提供增強型安全群組驗證。
  - 允許主體檢視與 Amazon FSx 檔案系統相關聯的彈性網路介面。
- kms – 允許主體在 Amazon FSx 管理主控台中檢視 AWS Key Management Service 金鑰的別名。
- log – 允許主體描述與發出請求的帳戶相關聯的 Amazon CloudWatch Logs 日誌群組。這是必要的，以便主體可以檢視 FSx for Windows File Server 檔案系統的現有檔案存取稽核組態。

- `firehose` – 允許主體描述與提出請求的帳戶相關聯的 Amazon Data Firehose 交付串流。這是必要的，以便主體可以檢視 FSx for Windows File Server 檔案系統的現有檔案存取稽核組態。

若要檢視此政策的許可，請參閱《AWS 受管政策參考指南》中的 [AmazonFSxConsoleReadOnlyAccess](#)。

## AWS 受管政策：AmazonFSxReadOnlyAccess

您可將 AmazonFSxReadOnlyAccess 政策連接到 IAM 身分。

- `fsx` – 允許主體在 Amazon FSx 管理主控台中檢視 Amazon FSx 檔案系統的相關資訊，包括所有標籤。
- `ec2` – 為所有可與 VPC 搭配使用的安全群組提供增強型安全群組驗證。

若要檢視此政策的許可，請參閱《AWS 受管政策參考指南》中的 [AmazonFSxReadOnlyAccess](#)。

## AWS 受管政策的 Amazon FSx 更新

檢視自此服務開始追蹤 Amazon FSx AWS 受管政策更新以來的詳細資訊。如需此頁面變更的自動提醒，請訂閱 Amazon FSx 頁面上的 RSS 摘要 [Amazon FSx for NetApp ONTAP 的文件歷史記錄](#)。

| 變更                                                  | 描述                                                                                                  | 日期              |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------|-----------------|
| <a href="#">AmazonFSxConsoleFullAccess</a> – 更新現有政策 | Amazon FSx 新增了新的許可， <code>fsx:CreateAndAttachS3AccessPoint</code> 允許主體建立 S3 並將其連接到 FSx 磁碟區。         | 2025 年 4 月 14 日 |
| <a href="#">AmazonFSxConsoleFullAccess</a> – 更新現有政策 | Amazon FSx 新增了新的許可， <code>fsx:DescribeS3AccessPointAttachments</code> 允許主體在中列出 AWS 帳戶中的所有 S3 AWS 區域 | 2025 年 4 月 14 日 |
| <a href="#">AmazonFSxConsoleFullAccess</a> – 更新現有政策 | Amazon FSx 新增了 <code>fsx:UpdateS3Access</code>                                                      | 2025 年 4 月 14 日 |

| 變更                                                       | 描述                                                                                    | 日期              |
|----------------------------------------------------------|---------------------------------------------------------------------------------------|-----------------|
|                                                          | PointAttachments 允許主體修改現有 S3 的新許可。                                                    |                 |
| <a href="#">AmazonFSxConsoleFullAccess</a> – 更新現有政策      | Amazon FSx 新增了 fsx:DetachAndDeleteS3AccessPoint 允許主體刪除 S3 的新許可。                       | 2025 年 4 月 14 日 |
| <a href="#">AmazonFSxFullAccess</a> – 更新現有政策             | Amazon FSx 新增了新的許可，fsx:CreateAndAttachS3AccessPoint 允許主體建立 S3 並將其連接到 FSx 磁碟區。         | 2025 年 4 月 14 日 |
| <a href="#">AmazonFSxFullAccess</a> – 更新現有政策             | Amazon FSx 新增了新的許可，fsx:DescribeS3AccessPointAttachments 允許主體在中列出 AWS 帳戶中的所有 S3 AWS 區域 | 2025 年 4 月 14 日 |
| <a href="#">AmazonFSxFullAccess</a> – 更新現有政策             | Amazon FSx 新增了 fsx:UpdateS3AccessPointAttachments 允許主體修改現有 S3 的新許可。                   | 2025 年 4 月 14 日 |
| <a href="#">AmazonFSxFullAccess</a> – 更新現有政策             | Amazon FSx 新增了 fsx:DetachAndDeleteS3AccessPoint 允許主體刪除 S3 的新許可。                       | 2025 年 4 月 14 日 |
| <a href="#">AmazonFSxConsoleReadOnlyAccess</a> – 更新至現有政策 | Amazon FSx 新增了新的許可，ec2:DescribeNetworkInterfaces 允許主體檢視與其檔案系統相關聯的彈性網路介面。              | 2025 年 2 月 25 日 |

| 變更                                                       | 描述                                                                                               | 日期             |
|----------------------------------------------------------|--------------------------------------------------------------------------------------------------|----------------|
| <a href="#">AmazonFSxConsoleFullAccess</a> – 更新現有政策      | Amazon FSx 新增了新的許可， <code>ec2:DescribeNetworkInterfaces</code> 允許主體檢視與其檔案系統相關聯的彈性網路介面。           | 2025 年 2 月 7 日 |
| <a href="#">AmazonFSxServiceRolePolicy</a> – 更新至現有政策     | Amazon FSx 新增了新的許可， <code>ec2:GetSecurityGroupsForVpc</code> 允許主體為所有可與 VPC 搭配使用的安全群組提供增強型安全群組驗證。 | 2024 年 1 月 9 日 |
| <a href="#">AmazonFSxReadOnlyAccess</a> – 更新現有政策         | Amazon FSx 新增了新的許可， <code>ec2:GetSecurityGroupsForVpc</code> 允許主體為所有可與 VPC 搭配使用的安全群組提供增強型安全群組驗證。 | 2024 年 1 月 9 日 |
| <a href="#">AmazonFSxConsoleReadOnlyAccess</a> – 更新至現有政策 | Amazon FSx 新增了新的許可， <code>ec2:GetSecurityGroupsForVpc</code> 允許主體為所有可與 VPC 搭配使用的安全群組提供增強型安全群組驗證。 | 2024 年 1 月 9 日 |
| <a href="#">AmazonFSxFullAccess</a> – 更新現有政策             | Amazon FSx 新增了新的許可， <code>ec2:GetSecurityGroupsForVpc</code> 允許主體為所有可與 VPC 搭配使用的安全群組提供增強型安全群組驗證。 | 2024 年 1 月 9 日 |
| <a href="#">AmazonFSxConsoleFullAccess</a> – 更新至現有政策     | Amazon FSx 新增了新的許可， <code>ec2:GetSecurityGroupsForVpc</code> 允許主體為所有可與 VPC 搭配使用的安全群組提供增強型安全群組驗證。 | 2024 年 1 月 9 日 |

| 變更                                                   | 描述                                                                   | 日期               |
|------------------------------------------------------|----------------------------------------------------------------------|------------------|
| <a href="#">AmazonFSxFullAccess</a> – 更新現有政策         | Amazon FSx 新增了新的許可，讓使用者能夠為 FSx for OpenZFS 檔案系統執行跨區域和跨帳戶資料複寫。        | 2023 年 12 月 20 日 |
| <a href="#">AmazonFSxConsoleFullAccess</a> – 更新現有政策  | Amazon FSx 新增了新的許可，讓使用者能夠為 FSx for OpenZFS 檔案系統執行跨區域和跨帳戶資料複寫。        | 2023 年 12 月 20 日 |
| <a href="#">AmazonFSxFullAccess</a> – 更新現有政策         | Amazon FSx 新增了新許可，讓使用者能夠執行 FSx for OpenZFS 檔案系統的隨需磁碟區複寫。             | 2023 年 11 月 26 日 |
| <a href="#">AmazonFSxConsoleFullAccess</a> – 更新至現有政策 | Amazon FSx 新增了新許可，讓使用者能夠執行 FSx for OpenZFS 檔案系統的隨需磁碟區複寫。             | 2023 年 11 月 26 日 |
| <a href="#">AmazonFSxFullAccess</a> – 更新現有政策         | Amazon FSx 新增了新的許可，讓使用者能夠檢視、啟用和停用 FSx for ONTAP 多可用區域檔案系統的共用 VPC 支援。 | 2023 年 11 月 14 日 |
| <a href="#">AmazonFSxConsoleFullAccess</a> – 更新現有政策  | Amazon FSx 新增了新的許可，讓使用者能夠檢視、啟用和停用 FSx for ONTAP 多可用區域檔案系統的共用 VPC 支援。 | 2023 年 11 月 14 日 |
| <a href="#">AmazonFSxFullAccess</a> – 更新現有政策         | Amazon FSx 新增了新的許可，以允許 Amazon FSx 管理 FSx for OpenZFS 多可用區域檔案系統的網路組態。 | 2023 年 8 月 9 日   |



| 變更                                                              | 描述                                                                                             | 日期              |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------|-----------------|
| <a href="#">AWS 受管政策：AmazonFSxServiceRolePolicy</a> – 更新至現有政策   | Amazon FSx 修改了現有的cloudwatch:PutMetricData 許可，以便 Amazon FSx 將 CloudWatch 指標發佈到AWS/FSx命名空間。      | 2023 年 7 月 24 日 |
| <a href="#">AmazonFSxFullAccess</a> – 更新現有政策                    | Amazon FSx 已更新政策以移除fsx:*許可並新增特定fsx動作。                                                          | 2023 年 7 月 13 日 |
| <a href="#">AmazonFSxConsoleFullAccess</a> – 更新現有政策             | Amazon FSx 已更新政策以移除fsx:*許可並新增特定fsx動作。                                                          | 2023 年 7 月 13 日 |
| <a href="#">AmazonFSxConsoleReadOnlyAccess</a> – 更新現有政策         | Amazon FSx 新增了新的許可，讓使用者能夠在 Amazon FSx FSx 主控台中檢視 FSx for Windows File Server 檔案系統的增強效能指標和建議動作。 | 2022 年 9 月 21 日 |
| <a href="#">AmazonFSxConsoleFullAccess</a> – 更新至現有政策            | Amazon FSx 新增了新的許可，讓使用者能夠在 Amazon FSx FSx 主控台中檢視 FSx for Windows File Server 檔案系統的增強效能指標和建議動作。 | 2022 年 9 月 21 日 |
| <a href="#">AmazonFSxReadOnlyAccess</a> – 開始追蹤政策                | 此政策會授予所有 Amazon FSx 資源和與其關聯之任何標籤的唯讀存取權。                                                        | 2022 年 2 月 4 日  |
| <a href="#">AmazonFSxDeleteServiceLinkedRoleAccess</a> – 開始追蹤政策 | 此政策會授予管理許可，允許 Amazon FSx 刪除其 Amazon S3 存取的服務連結角色。                                              | 2022 年 1 月 7 日  |



| 變更                                                      | 描述                                                                                                                                             | 日期             |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| <a href="#">AmazonFSxServiceRolePolicy</a><br>– 更新至現有政策 | Amazon FSx 新增了新的許可，以允許 Amazon FSx 管理 Amazon FSx for NetApp ONTAP 檔案系統的網路組態。                                                                    | 2021 年 9 月 2 日 |
| <a href="#">AmazonFSxFullAccess</a> – 更新現有政策            | Amazon FSx 新增了新的許可，以允許 Amazon FSx 在 EC2 路由表上為範圍縮小的呼叫建立標籤。                                                                                      | 2021 年 9 月 2 日 |
| <a href="#">AmazonFSxConsoleFullAccess</a> – 更新至現有政策    | Amazon FSx 新增了允許 Amazon FSx 建立 Amazon FSx for NetApp ONTAP 多可用區域檔案系統的許可。                                                                       | 2021 年 9 月 2 日 |
| <a href="#">AmazonFSxConsoleFullAccess</a> – 更新現有政策     | Amazon FSx 新增了新的許可，以允許 Amazon FSx 在 EC2 路由表上為範圍縮小的呼叫建立標籤。                                                                                      | 2021 年 9 月 2 日 |
| <a href="#">AmazonFSxServiceRolePolicy</a><br>– 更新至現有政策 | Amazon FSx 新增了允許 Amazon FSx 描述和寫入 CloudWatch Logs 日誌串流的許可。<br><br>這是必要的，讓使用者可以使用 CloudWatch Logs 檢視 FSx for Windows File Server 檔案系統的檔案存取稽核日誌。 | 2021 年 6 月 8 日 |

| 變更                                                      | 描述                                                                                                                                                              | 日期             |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| <a href="#">AmazonFSxServiceRolePolicy</a><br>– 更新至現有政策 | <p>Amazon FSx 新增了允許 Amazon FSx 描述和寫入 Amazon Data Firehose 交付串流的許可。</p> <p>這是必要的，讓使用者可以使用 Amazon Data Firehose 檢視 FSx for Windows File Server 檔案系統的檔案存取稽核日誌。</p> | 2021 年 6 月 8 日 |
| <a href="#">AmazonFSxFullAccess</a> – 更新現有政策            | <p>Amazon FSx 新增了新的許可，允許主體描述和建立 CloudWatch Logs 日誌群組、日誌串流，以及將事件寫入日誌串流。</p> <p>這是必要的，以便主體可以使用 CloudWatch Logs 檢視 FSx for Windows File Server 檔案系統的檔案存取稽核日誌。</p>  | 2021 年 6 月 8 日 |
| <a href="#">AmazonFSxFullAccess</a> – 更新現有政策            | <p>Amazon FSx 新增了新的許可，允許主體描述記錄並將其寫入 Amazon Data Firehose。</p> <p>這是必要的，讓使用者可以使用 Amazon Data Firehose 檢視 FSx for Windows File Server 檔案系統的檔案存取稽核日誌。</p>          | 2021 年 6 月 8 日 |

| 變更                                                       | 描述                                                                                                                                                                    | 日期             |
|----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| <a href="#">AmazonFSxConsoleFullAccess</a> – 更新現有政策      | <p>Amazon FSx 新增了新的許可，允許主體描述與提出請求的帳戶相關聯的 Amazon CloudWatch Logs 日誌群組。</p> <p>這是必要的，以便主體在設定 FSx for Windows File Server 檔案系統的檔案存取稽核時，可以選擇現有的 CloudWatch Logs 日誌群組。</p> | 2021 年 6 月 8 日 |
| <a href="#">AmazonFSxConsoleFullAccess</a> – 更新現有政策      | <p>Amazon FSx 新增了新的許可，允許主體描述與提出請求的帳戶相關聯的 Amazon Data Firehose 交付串流。</p> <p>這是必要的，以便主體在設定 FSx for Windows File Server 檔案系統的檔案存取稽核時，可以選擇現有的 Firehose 交付串流。</p>          | 2021 年 6 月 8 日 |
| <a href="#">AmazonFSxConsoleReadOnlyAccess</a> – 更新至現有政策 | <p>Amazon FSx 新增了新的許可，允許主體描述與提出請求的帳戶相關聯的 Amazon CloudWatch Logs 日誌群組。</p> <p>這是必要的，以便主體可以檢視 FSx for Windows File Server 檔案系統的現有檔案存取稽核組態。</p>                          | 2021 年 6 月 8 日 |

| 變更                                                       | 描述                                                                                                                                  | 日期             |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|----------------|
| <a href="#">AmazonFSxConsoleReadOnlyAccess</a> – 更新至現有政策 | Amazon FSx 新增了新的許可，允許主體描述與提出請求的帳戶相關聯的 Amazon Data Firehose 交付串流。<br><br>這是必要的，以便主體可以檢視 FSx for Windows File Server 檔案系統的現有檔案存取稽核組態。 | 2021 年 6 月 8 日 |
| Amazon FSx 開始追蹤變更                                        | Amazon FSx 開始追蹤其 AWS 受管政策的變更。                                                                                                       | 2021 年 6 月 8 日 |

## 使用 Amazon VPC 的檔案系統存取控制

您可以使用其中一個端點的 DNS 名稱或 IP 地址存取 Amazon FSx for NetApp ONTAP 檔案系統和 SVMs，視其存取類型而定。DNS 名稱會映射至 VPC 中檔案系統或 SVM 彈性網路界面的私有 IP 地址。只有關聯 VPC 內的資源，或是透過 AWS Direct Connect 或 VPN 與關聯 VPC 連線的資源，才能透過 NFS、SMB 或 iSCSI 通訊協定存取檔案系統中的資料。如需詳細資訊，請參閱《[Amazon VPC 使用者指南](#)》中的[什麼是 Amazon VPC](#)？。

### Warning

您不得修改或刪除與檔案系統相關聯的彈性網路界面 (s)。修改或刪除網路界面可能會導致 VPC 和檔案系統之間的連線永久中斷。

## Amazon VPC 安全群組

安全群組可做為 FSx for ONTAP 檔案系統的虛擬防火牆，以控制傳入和傳出流量。傳入規則控制傳入至檔案系統的流量，傳出規則控制來自檔案系統的傳出流量。當您建立檔案系統時，您可以指定在其中建立的 VPC，並套用該 VPC 的預設安全群組。您可以將規則新增至每個安全群組，以允許流量進出其相關聯的檔案系統和 SVMs。您可隨時修改安全群組規則。新的和修改過的規則會自動套用至與安全群組相關聯的所有資源。當 Amazon FSx 決定是否允許流量到達資源時，它會評估與資源相關聯的所有安全群組的所有規則。

若要使用安全群組來控制對 Amazon FSx 檔案系統的存取，請新增傳入和傳出規則。傳入規則控制傳入流量，傳出規則控制來自檔案系統的傳出流量。請確定您的安全群組中有正確的網路流量規則，將 Amazon FSx 檔案系統的檔案共用映射至支援的運算執行個體上的資料夾。

如需安全群組規則的詳細資訊，請參閱《Amazon EC2 使用者指南》中的[安全群組規則](#)。Amazon EC2

## 建立 VPC 安全群組

### 建立 Amazon FSx 的安全群組

1. 開啟位於 <https://console.aws.amazon.com/ec2> 的 Amazon EC2 主控台。
2. 在導覽窗格中，選擇 Security Groups (安全群組)。
3. 選擇 Create Security Group (建立安全群組)。
4. 指定安全群組的名稱和描述。
5. 針對 VPC，選擇與檔案系統相關聯的 Amazon VPC，在該 VPC 內建立安全群組。
6. 對於傳出規則，允許所有連接埠上的所有流量。
7. 將下列規則新增至安全群組的傳入連接埠。對於來源欄位，您應該選擇自訂，並輸入與需要存取 FSx for ONTAP 檔案系統的執行個體相關聯的安全群組或 IP 地址範圍，包括：
  - 透過 NFS、SMB 或 iSCSI 存取檔案系統中資料的 Linux、Windows 和/或 macOS 用戶端。
  - 您將對等至檔案系統的任何 ONTAP 檔案系統/叢集（例如，使用 SnapMirror、SnapVault 或 FlexCache）。
  - 您將用來存取 ONTAP REST API、CLI 或 ZAPIs 的任何用戶端（例如，Harvest/Grafana 執行個體、NetApp Connector 或 NetApp BlueXP）。

| 通訊協定    | 連接埠 | 角色                               |
|---------|-----|----------------------------------|
| 所有 ICMP | 全部  | Ping 執行個體                        |
| SSH     | 22  | SSH 存取叢集管理 LIF 或節點管理 LIF 的 IP 地址 |
| TCP     | 111 | NFS 的遠端程序呼叫                      |
| TCP     | 135 | CIFS 的遠端程序呼叫                     |
| TCP     | 139 | CIFS 的 NetBIOS 服務工作階段            |

| 通訊協定 | 連接埠     | 角色                                             |
|------|---------|------------------------------------------------|
| TCP  | 161-162 | 簡易網路管理通訊協定 (SNMP)                              |
| TCP  | 443     | ONTAP REST API 存取叢集管理 LIF 或 SVM 管理 LIF 的 IP 地址 |
| TCP  | 445     | 使用 NetBIOS 架構透過 TCP 的 Microsoft SMB/CIFS       |
| TCP  | 635     | NFS 掛載                                         |
| TCP  | 749     | Kerberos                                       |
| TCP  | 2049    | NFS 伺服器協助程式                                    |
| TCP  | 3260    | 透過 iSCSI 資料 LIF 存取 iSCSI                       |
| TCP  | 4045    | NFS 鎖定協助程式                                     |
| TCP  | 4046    | NFS 的網路狀態監控                                    |
| TCP  | 10000   | 網路資料管理通訊協定 (NDMP) 和 NetApp SnapMirror 叢集間通訊    |
| TCP  | 11104   | NetApp SnapMirror 叢集間通訊的管理                     |
| TCP  | 11105   | 使用叢集間 LIFs SnapMirror 資料傳輸                     |
| UDP  | 111     | NFS 的遠端程序呼叫                                    |
| UDP  | 135     | CIFS 的遠端程序呼叫                                   |
| UDP  | 137     | CIFS 的 NetBIOS 名稱解析                            |
| UDP  | 139     | CIFS 的 NetBIOS 服務工作階段                          |
| UDP  | 161-162 | 簡易網路管理通訊協定 (SNMP)                              |
| UDP  | 635     | NFS 掛載                                         |
| UDP  | 2049    | NFS 伺服器協助程式                                    |

| 通訊協定 | 連接埠  | 角色          |
|------|------|-------------|
| UDP  | 4045 | NFS 鎖定協助程式  |
| UDP  | 4046 | NFS 的網路狀態監控 |
| UDP  | 4049 | NFS 配額通訊協定  |

8. 將安全群組新增至檔案系統的彈性網路界面。

### 不允許存取檔案系統

若要暫時禁止從所有用戶端存取檔案系統，您可以移除與檔案系統彈性網路界面相關聯的所有安全群組，並將其取代為沒有傳入/傳出規則的群組。

## Amazon FSx for NetApp ONTAP 的合規驗證

若要了解 是否 AWS 服務 在特定合規計劃的範圍內，請參閱[AWS 服務 合規計劃範圍內](#)然後選擇您感興趣的合規計劃。如需一般資訊，請參閱 [AWS Compliance Programs](#)。

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

您使用 時的合規責任 AWS 服務 取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。AWS 提供下列資源來協助合規：

- [安全合規與治理](#) - 這些解決方案實作指南內容討論了架構考量，並提供部署安全與合規功能的步驟。
- [HIPAA 合格服務參考](#) - 列出 HIPAA 合格服務。並非所有 AWS 服務 都符合 HIPAA 資格。
- [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 客戶合規指南](#) - 透過合規的角度了解共同責任模型。本指南摘要說明跨多個架構（包括國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 保護 AWS 服務 和映射指南至安全控制的最佳實務。
- 《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](#) - 這 AWS 服務 可讓您全面檢視其中的安全狀態 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱「[Security Hub 控制參考](#)」。

- [Amazon GuardDuty](#) – 這會監控您的環境是否有可疑和惡意活動，以 AWS 服務 偵測對您 AWS 帳戶、工作負載、容器和資料的潛在威脅。GuardDuty 可滿足特定合規架構所規定的入侵偵測需求，以協助您因應 PCI DSS 等各種不同的合規需求。
- [AWS Audit Manager](#) – 這 AWS 服務 可協助您持續稽核 AWS 用量，以簡化您管理風險和符合法規和業界標準的方式。

## Amazon FSx for NetApp ONTAP 和介面 VPC 端點 (AWS PrivateLink)

您可以將 Amazon FSx 設定為使用介面 VPC 端點，以改善 VPC 的安全狀態。介面 VPC 端點採用 [AWS PrivateLink](#) 技術，可讓您在沒有網際網路閘道、NAT 裝置、VPN 連接或 AWS Direct Connect 連線的情況下私下存取 Amazon FSx APIs。VPC 中的執行個體不需要公有 IP 地址，即可與 Amazon FSx APIs 通訊。VPC 和 Amazon FSx 之間的流量不會離開 AWS 網路。

每個介面 VPC 端點由子網路中的一或多個彈性網路界面表示。網路界面提供私有 IP 地址，做為 Amazon FSx API 流量的進入點。Amazon FSx 支援使用 IPv4 和雙堆疊 (IPv4 和 IPv6) IP 地址類型設定的 VPC 端點。如需詳細資訊，請參閱《Amazon [VPC 使用者指南](#)》中的[建立介面 VPC 端點](#)。

### Amazon FSx 介面 VPC 端點的考量事項

為 Amazon FSx 設定介面 VPC 端點之前，請務必檢閱《Amazon [VPC 使用者指南](#)》中的[介面 VPC 端點屬性和限制](#)。

您可以從 VPC 呼叫任何 Amazon FSx API 操作。例如，您可以從 VPC 內呼叫 CreateFileSystem API，以建立 FSx for ONTAP 檔案系統。如需 Amazon FSx APIs 的完整清單，請參閱《Amazon FSx API 參考》中的[動作](#)。

### VPC 對等互連考量

您可以使用 VPCs 對等互連，透過介面 VPC 端點將其他 VPC 連接至 VPC。VPC 對等互連是兩個 VPC 之間的網路連線。您可以在自己的兩個 VPC 之間建立 VPCs 對等互連，或在另一個 VPC 中建立 VPC AWS 帳戶。VPCs 也可以是兩個不同的 AWS 區域。

對等 VPCs 之間的流量會保留在 AWS 網路上，而不會周遊公有網際網路。一旦 VPCs 對等互連，兩個 VPCs 中的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體等資源可以透過其中一個 VPCs 中建立的介面 VPC 端點存取 Amazon FSx API。



## 為 Amazon FSx API 建立介面 VPC 端點

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface () 為 Amazon FSx API 建立 VPC 端點AWS CLI。如需詳細資訊，請參閱《Amazon [VPC 使用者指南](#)》中的建立介面 VPC 端點。

若要為 Amazon FSx 建立介面 VPC 端點，請使用下列其中一項：

- **com.amazonaws.*region*.fsx** – 建立 Amazon FSx API 操作的端點。
- **com.amazonaws.*region*.fsx-fips** – 為 Amazon FSx API 建立符合[聯邦資訊處理標準 \(FIPS\) 140-2](#) 的端點。

若要使用私有 DNS 選項，您必須設定 VPC 的 `enableDnsHostnames` 和 `enableDnsSupport` 屬性。如需詳細資訊，請參閱《Amazon [VPC 使用者指南](#)》中的檢視和更新 VPC 的 DNS 支援。

AWS 區域 在中國除外，如果您為端點啟用私有 DNS，您可以使用 VPC 端點的預設 DNS 名稱向 Amazon FSx 提出 API 請求 AWS 區域，例如 `fsx.us-east-1.amazonaws.com`。對於中國（北京）和中國（寧夏）AWS 區域，您可以 `fsx-api.cn-northwest-1.amazonaws.com.cn` 分別使用 `fsx-api.cn-north-1.amazonaws.com.cn` 和使用 VPC 端點提出 API 請求。

如需詳細資訊，請參閱《Amazon [VPC 使用者指南](#)》中的透過介面 VPC 端點存取服務。

## 為 Amazon FSx 建立 VPC 端點政策

若要控制對 Amazon FSx API 的存取，您可以將 AWS Identity and Access Management (IAM) 政策連接至 VPC 端點。此政策會指定以下項目：

- 可執行動作的主體。
- 可執行的動作。
- 可供執行動作的資源。

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的[使用 VPC 端點控制對服務的存取](#)。

## Amazon FSx for NetApp ONTAP 中的彈性

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 提供多個實體隔離和隔離的可用區域，這些可用區域與低延遲、高輸送量和高備援聯網連接。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

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，Amazon FSx 還提供數種功能，以協助支援您的資料彈性和備份需求。

## 備份和還原

Amazon FSx 會在 Amazon FSx for NetApp ONTAP 檔案系統中建立並儲存磁碟區的自動備份。Amazon FSx 會在 Amazon FSx for NetApp ONTAP 檔案系統的備份時段建立磁碟區的自動備份。Amazon FSx 會根據您指定的備份保留期來儲存磁碟區的自動備份。您也可以透過建立使用者起始的備份來手動備份磁碟區。您可以隨時使用指定為來源的備份建立新的磁碟區，以還原磁碟區備份。

如需詳細資訊，請參閱[使用磁碟區備份保護您的資料](#)。

## 快照

Amazon FSx 會建立 Amazon FSx for NetApp ONTAP 磁碟區的快照副本。快照副本提供保護，防止最終使用者意外刪除或修改磁碟區中的檔案。如需詳細資訊，請參閱[使用快照保護您的資料](#)。

## 可用區域

Amazon FSx for NetApp ONTAP 檔案系統旨在提供資料的持續可用性，即使伺服器發生故障也一樣。每個檔案系統都由至少一個可用區域中的兩個檔案伺服器提供支援，每個伺服器都有自己的儲存體。Amazon FSx 會自動複寫您的資料，以防止其發生元件故障、持續監控硬體故障，並在發生故障時自動取代基礎設施元件。檔案系統會自動視需要容錯移轉和回復（通常在 60 秒內），而用戶端會自動容錯移轉和回復檔案系統。

### 多可用區域檔案系統

Amazon FSx for NetApp ONTAP 檔案系統在可用區域之間 AWS 具有高可用性和耐用性，即使在無法使用可用區域的情況下，也能持續提供資料的可用性。

如需詳細資訊，請參閱[可用性、耐用性和部署選項](#)。

### 單一可用區檔案系統

Amazon FSx for NetApp ONTAP 檔案系統在單一 AWS 可用區域內具有高可用性和耐用性，旨在當個別檔案伺服器或磁碟故障時，在該可用區域內提供持續可用性。

如需詳細資訊，請參閱[可用性、耐用性和部署選項](#)。

# Amazon FSx for NetApp ONTAP 中的基礎設施安全性

Amazon FSx for NetApp ONTAP 是受管服務，受到 AWS 全球網路安全的保護。如需 AWS 安全服務以及 如何 AWS 保護基礎設施的相關資訊，請參閱[AWS 雲端安全](#)。若要使用基礎設施安全最佳實務來設計您的 AWS 環境，請參閱安全支柱 AWS Well-Architected Framework 中的[基礎設施保護](#)。

您可以使用 AWS 發佈的 API 呼叫，透過網路存取 Amazon FSx。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。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。

## 將 NetApp ONTAP Vscan 與 FSx for ONTAP 搭配使用

您可以使用 NetApp ONTAP's Vscan 功能來執行支援的第三方防毒軟體。如需詳細資訊，請參閱下列每個支援解決方案的資源。

- Deep Instinct – [Vscan 合作夥伴解決方案](#)和 [Deep Instinct 文件](#)<sup>1</sup>
- SentinelOne – [Vscan 合作夥伴解決方案](#)和 [SentinelOne Singularity Cloud Data Security](#)
- Symantec – [Vscan 合作夥伴解決方案](#)和 [Symantec 保護引擎](#)
- Trellix ( 先前為 McAfee) – [Vscan 合作夥伴解決方案](#)和 [Trellix 產品文件](#)
- Trend Micro – [Vscan 合作夥伴解決方案](#)

### Note

<sup>1</sup> 您必須登入 Deep Instinct 的入口網站以檢視其文件。

## ONTAP 角色和使用者

NetApp ONTAP 包含強大且可擴展的角色型存取控制 (RBAC) 功能。ONTAP角色會在使用 CLI 和 REST API ONTAP 時定義使用者功能和權限。每個角色都會定義不同層級的管理功能和權限。您可

以將角色指派給使用者，以便在使用 ONTAP REST API 和 CLI 時控制其對 FSx for ONTAP 資源的存取。FSx for ONTAP 檔案系統使用者和儲存虛擬機器 (SVM) 使用者有個別可用的 ONTAP 角色。

當您建立 FSx for ONTAP 檔案系統時，預設 ONTAP 使用者會在檔案系統層級和 SVM 層級建立。您可以建立其他檔案系統和 SVM 使用者，也可以建立其他 SVM 角色，以滿足組織的需求。本章說明 ONTAP 使用者和角色，並提供建立其他使用者和 SVM 角色的詳細程序。

## 檔案系統管理員角色和使用者

預設 ONTAP 檔案系統使用者為 `fsxadmin`，其具有指派給該使用者 `fsxadmin` 的角色。您可以指派給檔案系統使用者的兩個預先定義角色，如下所示：

- **fsxadmin**- 具有此角色的管理員在 ONTAP 系統中擁有不受限制的權限。他們可以設定 FSx for ONTAP 檔案系統上可用的所有檔案系統和 SVM 層級資源。
- **fsxadmin-readonly**- 具有此角色的管理員可以在檔案系統層級檢視所有項目，但無法進行任何變更。

此角色非常適合與監控應用程式搭配使用，例如，NetApp Harvest 因為它具有所有可用資源及其屬性的唯讀存取權，但無法對其進行任何變更。

您可以建立其他檔案系統使用者，並將 `fsxadmin` 或 `fsxadmin-readonly` 角色指派給他們。您無法建立新的角色或修改現有的角色。如需詳細資訊，請參閱 [為檔案系統和 SVM 管理建立新的 ONTAP 使用者](#)。

下表說明檔案系統管理員角色對 CLI 和 REST API ONTAP 命令和命令目錄的存取層級。

| 角色名稱                           | 存取層級 | 前往下列命令或命令目錄                                                         |
|--------------------------------|------|---------------------------------------------------------------------|
| <code>fsxadmin</code>          | 全部   | FSx for ONTAP 中提供的所有命令目錄                                            |
| <code>fsxadmin-readonly</code> | 全部   | <code>security login password</code><br><br>僅適用於管理自己的使用者帳戶本機密碼和金鑰資訊 |
|                                | 無    | <code>security</code>                                               |

| 角色名稱 | 存取層級 | 前往下列命令或命令目錄                |
|------|------|----------------------------|
|      | 唯讀   | FSx for ONTAP 中可用的所有其他命令目錄 |

## SVM 管理員角色和使用者

每個 SVM 都有單獨的身分驗證網域，並且可以由自己的管理員獨立管理。對於檔案系統上的每個 SVM，預設使用者是 vsadmin，其預設會指派 vsadmin 角色。除了 vsadmin 角色之外，還有其他預先定義的 SVM 角色，提供可指派給 SVM 使用者的縮小範圍許可。您也可以建立自訂角色，提供符合您組織需求的存取控制層級。

SVM 管理員的預先定義角色及其功能如下所示：

| 角色名稱           | 功能                                                                                                                                                                                                                                                                                                                    |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vsadmin        | <ul style="list-style-type: none"> <li>• 管理您的使用者帳戶、本機密碼和金鑰資訊</li> <li>• 管理磁碟區，磁碟區移動除外</li> <li>• 管理配額、qtrees、快照複本和檔案</li> <li>• 管理 LUNs</li> <li>• 執行 SnapLock 操作，特殊權限刪除除外</li> <li>• 設定通訊協定：NFS、SMB 和 iSCSI</li> <li>• 設定服務：DNS、LDAP 和 NIS</li> <li>• 監控作業</li> <li>• 監控網路連線和網路界面</li> <li>• 監控 SVM 的運作狀態</li> </ul> |
| vsadmin-volume | <ul style="list-style-type: none"> <li>• 管理您的使用者帳戶、本機密碼和金鑰資訊</li> <li>• 管理磁碟區，包括磁碟區移動</li> <li>• 管理配額、qtrees、快照複本和檔案</li> <li>• 管理 LUNs</li> <li>• 設定通訊協定：NFS、SMB 和 iSCSI</li> <li>• 設定服務：DNS、LDAP 和 NIS</li> <li>• 監控網路界面</li> </ul>                                                                                 |

| 角色名稱             | 功能                                                                                                                                                                                                                                                                   |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <ul style="list-style-type: none"> <li>• 監控 SVM 的運作狀態</li> </ul>                                                                                                                                                                                                     |
| vsadmin-protocol | <ul style="list-style-type: none"> <li>• 管理您的使用者帳戶、本機密碼和金鑰資訊</li> <li>• 管理 LUNs</li> <li>• 設定通訊協定：NFS、SMB 和 iSCSI</li> <li>• 設定服務：DNS、LDAP 和 NIS</li> <li>• 監控網路界面</li> <li>• 監控 SVM 的運作狀態</li> </ul>                                                                |
| vsadmin-backup   | <ul style="list-style-type: none"> <li>• 管理您的使用者帳戶、本機密碼和金鑰資訊</li> <li>• 管理 NDMP 操作</li> <li>• 進行還原的磁碟區讀取/寫入</li> <li>• 管理 SnapMirror 關係和快照副本</li> <li>• 檢視磁碟區和網路資訊</li> </ul>                                                                                        |
| vsadmin-snaplock | <ul style="list-style-type: none"> <li>• 管理您的使用者帳戶、本機密碼和金鑰資訊</li> <li>• 管理磁碟區，磁碟區移動除外</li> <li>• 管理配額、qtrees、快照複本和檔案</li> <li>• 執行 SnapLock 操作，包括特殊權限刪除</li> <li>• 設定通訊協定：NFS 和 SMB</li> <li>• 設定服務：DNS、LDAP 和 NIS</li> <li>• 監控作業</li> <li>• 監控網路連線和網路界面</li> </ul> |
| vsadmin-readonly | <ul style="list-style-type: none"> <li>• 管理您的使用者帳戶、本機密碼和金鑰資訊</li> <li>• 監控 SVM 的運作狀態</li> <li>• 監控網路界面</li> <li>• 檢視磁碟區和 LUNs</li> <li>• 檢視 服務和通訊協定</li> </ul>                                                                                                       |

如需如何建立新的 SVM 角色的詳細資訊，請參閱 [建立 SVM 角色](#)。

## 使用 Active Directory 驗證ONTAP使用者

您可以驗證 Windows Active Directory 網域使用者對 FSx for ONTAP 檔案系統和 SVM 的存取。您必須執行下列任務，Active Directory 帳戶才能存取您的檔案系統：

- 您需要設定 Active Directory 網域控制站對 SVM 的存取。

您用來將設定為 Active Directory 網域控制站存取的閘道或通道的 SVM 必須啟用 CIFS、加入 Active Directory 或兩者。如果您未啟用 CIFS 且僅將通道 SVM 加入 Active Directory，請確定 SVM 已加入您的 Active Directory。如需詳細資訊，請參閱[將 SVMs加入 Microsoft Active Directory 的運作方式](#)。

- 您需要啟用 Active Directory 網域使用者帳戶才能存取檔案系統。

您可以為存取 CLI 或 REST API 的 Windows 網域使用者使用密碼身分驗證或 SSH ONTAP 公有金鑰身分驗證。

如需說明如何使用為檔案系統和 SVM 管理員設定 Active Directory 身分驗證的程序，請參閱[為 ONTAP使用者設定 Active Directory 身分驗證](#)。

## 為檔案系統和 SVM 管理建立新的ONTAP使用者

每個ONTAP使用者都與 SVM 或檔案系統相關聯。具有 fsxadmin角色的檔案系統使用者可以使用 CLI 命令建立新的 SVM [security login create](#) ONTAP 角色和使用者。

security login create 命令會為管理公用程式建立登入方法。登入方法包含使用者名稱、應用程式（存取方法）和身分驗證方法。使用者名稱可以與多個應用程式建立關聯。它可以選擇性地包含存取控制角色名稱。如果使用 Active Directory、LDAP 或 NIS 群組名稱，則登入方法會將存取權授予屬於指定群組的使用者。如果使用者是安全登入資料表中佈建的多個群組的成員，則該使用者將存取針對個別群組授權的命令組合清單。

如需如何建立新ONTAP使用者的資訊，請參閱[建立 ONTAP 使用者](#)。

### 主題

- [建立 ONTAP 使用者](#)
- [建立 SVM 角色](#)
- [為ONTAP使用者設定 Active Directory 身分驗證](#)
- [設定公有金鑰身分驗證](#)
- [更新檔案系統和 SVM 角色的密碼需求](#)



- [更新fsxadmin帳戶密碼失敗](#)

## 建立 ONTAP 使用者

### 建立新的 SVM 或檔案系統使用者 (ONTAP CLI)

只有具有 fsxadmin 角色的檔案系統使用者可以建立新的 SVM 和檔案系統使用者。

1. 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。*management\_endpoint\_ip* 將取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

2. 使用 `security login create` ONTAP CLI 命令在 FSx for ONTAP 檔案系統或 SVM 上建立新的使用者帳戶。

在範例中插入預留位置的資料，以定義下列必要屬性：

- `-vserver` – 指定您要建立新 SVM 角色或使用者的 SVM 名稱。如果您要建立檔案系統角色或使用者，請不要指定 SVM。
- `-user-or-group-name` – 指定登入方法的使用者名稱或 Active Directory 群組名稱。Active Directory 群組名稱只能使用 domain 身分驗證方法和 `ontapi` 和 `ssh` 應用程式來指定。
- `-application` – 指定登入方法的應用程式。可能的值包括 `http`、`ontapi` 和 `ssh`。
- `-authentication-method` – 指定登入的身分驗證方法。可能的值包括以下：
  - `domain` – 用於 Active Directory 身分驗證
  - `password` – 用於密碼身分驗證
  - `publickey` – 公有金鑰身分驗證的使用者
- `-role` – 指定登入方法的存取控制角色名稱。在檔案系統層級，唯一可以指定的角色是 `fsxadmin`。

(選用) 您也可以搭配 命令使用下列一或多個參數：

- `[-comment]` – 使用 來包含使用者帳戶的符號或註解。例如 **Guest account**。長度上限為 128 個字元。



- `[-second-authentication-method {none|publickey|password|nsswitch}]` – 指定第二要素驗證方法。您可以指定下列方法：
  - `password` – 用於密碼身分驗證
  - `publickey` – 用於公有金鑰身分驗證
  - `nsswitch` – 用於 NIS 或 LDAP 身分驗證
  - `none` – 如果您未指定預設值

```
Fsx0123456::> security login create -vserver vserver_name -user-or-group-name user_or_group_name -application login_application -authentication-method auth_method -role role_or_account_name
```

下列命令會使用 SSH 搭配密碼來登入，`new_fsxadmin`以指派`fsxadmin-readonly`的角色建立新的檔案系統使用者。出現提示時，請為使用者提供密碼。

```
Fsx0123456::> security login create -user-or-group-name new_fsxadmin -application ssh -authentication-method password -role fsxadmin-readonly
```

```
Please enter a password for user 'new_fsxadmin':  
Please enter it again:
```

```
Fsx0123456::>
```

3. 下列命令會使用 `vsadmin_readonly`角色在 SVM `new_vsadmin` 上建立新的 `fsx` SVM 使用者，設定為使用 SSH 搭配密碼登入。出現提示時，請為使用者提供密碼。

```
Fsx0123456::> security login create -vserver fsx -user-or-group-name new_vsadmin -application ssh -authentication-method password -role vsadmin-readonly
```

```
Please enter a password for user 'new_vsadmin':  
Please enter it again:
```

```
Fsx0123456::>
```

4. 下列命令會建立新的唯讀檔案系統使用者`harvest2-user`，供 NetApp Harvest 應用程式用來收集效能和容量指標。如需詳細資訊，請參閱[使用 Harvest 和 Grafana 監控 ONTAP 檔案系統的 FSx](#)。

```
Fsx0123456::> security login create -user-or-group-name harvest2-user -application
ssh -role fsxadmin-readonly -authentication-method password
```

檢視所有檔案系統和 SVM 使用者的資訊

- 使用下列命令來檢視檔案系統和 SVMs 的所有登入資訊。

```
Fsx0123456::> security login show
```

Vserver: Fsx0123456

| User/Group<br>Name | Application | Authentication<br>Method | Role Name         | Acct<br>Locked | Second<br>Authentication<br>Method |
|--------------------|-------------|--------------------------|-------------------|----------------|------------------------------------|
| autosupport        | console     | password                 | autosupport       | no             | none                               |
| fsxadmin           | http        | password                 | fsxadmin          | no             | none                               |
| fsxadmin           | ontapi      | password                 | fsxadmin          | no             | none                               |
| fsxadmin           | ssh         | password                 | fsxadmin          | no             | none                               |
| fsxadmin           | ssh         | publickey                | fsxadmin          | -              | none                               |
| new_fsxadmin       | ssh         | password                 | fsxadmin-readonly | no             | none                               |

Vserver: fsx

| User/Group<br>Name | Application | Authentication<br>Method | Role Name        | Acct<br>Locked | Second<br>Authentication<br>Method |
|--------------------|-------------|--------------------------|------------------|----------------|------------------------------------|
| new_vsadmin        | ssh         | password                 | vsadmin-readonly | no             | none                               |
| vsadmin            | http        | password                 | vsadmin          | yes            | none                               |
| vsadmin            | ontapi      | password                 | vsadmin          | yes            | none                               |
| vsadmin            | ssh         | password                 | vsadmin          | yes            | none                               |

10 entries were displayed.

```
Fsx0123456::>
```

## 建立 SVM 角色

您建立的每個 SVM 都有一個預設 SVM 管理員，該管理員會指派預先定義的 vsadmin 角色。除了一組 [預先定義的 SVM 角色](#) 之外，您還可以建立新的 SVM 角色。如果您需要為 SVM 建立新角色，請使

用 `security login role create` ONTAP CLI 命令。此命令可供具有 `fsxadmin` 角色的檔案系統管理員使用。

## 建立新的 SVM 角色 (ONTAP CLI)

1. 您可以使用 [security login role create](#) ONTAP CLI 命令建立新的 SVM 角色：

```
Fsx0123456::> security login role create -vserver vs1.example.com -role vol_role -  
cmddirname volume
```

2. 在命令中指定下列必要參數：

- `-vserver` SVM 的名稱
- `-role` – 角色的名稱。
- `-cmddirname` – 角色授予存取權的命令或命令目錄。以雙引號括住命令子目錄名稱。例如 "volume snapshot"。輸入 `DEFAULT` 以指定所有命令目錄。

3. (選用) 您也可以將下列任何參數新增至命令：

- `-vserver` – 與該角色相關聯的 SVM 名稱。
- `-access` – 角色的存取層級。對於命令目錄，這包括：
  - `none` – 拒絕存取命令目錄中的命令。這是自訂角色的預設值。
  - `readonly` – 准許存取命令目錄中的 `show` 命令及其子目錄。
  - `all` – 授予對命令目錄及其子目錄中所有命令的存取權。若要授予或拒絕對內部命令的存取，您必須指定命令目錄。

對於非內部命令（結尾不是 `create`、`delete`、`modify` 或的命令 `show`）：

- `none` – 拒絕存取命令目錄中的命令。這是自訂角色的預設值。
- `readonly` – 不適用。請勿使用。
- `all` – 授予命令的存取權。
- `-query` – 用來篩選存取層級的查詢物件，以命令的有效選項或命令目錄中命令的形式指定。以雙引號括住查詢物件。

4. 執行 `security login role create` 命令。

下列命令會為 `vs1.example.com` Vserver 建立名為 "admin" 的存取控制角色。角色具有「磁碟區」命令的所有存取權，但僅限於「彙總0」彙總內。

```
Fsx0123456::>security login role create -role admin -cmddirname volume -query "-aggr aggr0" -access all -vserver vs1.example.com
```

## 為ONTAP使用者設定 Active Directory 身分驗證

使用 ONTAP CLI 為ONTAP檔案系統和 SVM 使用者設定使用 Active Directory 身分驗證。

您必須是具有 fsxadmin角色的檔案系統管理員，才能使用此程序中的命令。

### 為ONTAP使用者設定 Active Directory 身分驗證 (ONTAP CLI)

此程序中的命令可供具有 fsxadmin角色的檔案系統使用者使用。

1. 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。*management\_endpoint\_ip* 將取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

2. 使用如下所示的 [security login domain-tunnel create](#) 命令來建立網域通道，以驗證 Windows Active Directory 使用者。將 *svm\_name* 取代為您用於網域通道的 SVM 名稱。

```
FsxId0123456::> security login domain-tunnel create -vserver svm_name
```

3. 使用 [security login create](#) 命令建立將存取檔案系統的 Active Directory 網域使用者帳戶。

在 命令中指定下列必要參數：

- -vserver – 使用 CIFS 設定並加入 Active Directory 的 SVM 名稱。它將用作通道，向檔案系統驗證 Active Directory 網域使用者的身分。將建立新角色或使用者。
- -user-or-group-name – 登入方法的使用者名稱或 Active Directory 群組名稱。Active Directory 群組名稱只能使用domain身分驗證方法和ontapissh應用程式來指定。
- -application – 登入方法的應用程式。可能的值包括 http、ontapi 和 ssh。
- -authentication-method – 用於登入的身分驗證方法。可能的值包括以下：
  - domain – 用於 Active Directory 身分驗證
  - password – 用於密碼身分驗證

- `publickey` – 用於公有金鑰身分驗證
- `-role` – 登入方法的存取控制角色名稱。在檔案系統層級，唯一可以指定的角色是 `-role fsxadmin`。

下列範例會CORP\Admin建立filesystem1檔案系統的 Active Directory 網域使用者帳戶。

```
FSxId012345::> security login create -vserver filesystem1 -username CORP\Admin -  
application ssh -authmethod domain -role fsxadmin
```

下列範例會使用公有金鑰身分驗證建立CORP\Admin使用者帳戶。

```
FSxId0123456ab::> security login create -user-or-group-name "CORP\Admin" -  
application ssh -authentication-method publickey -role fsxadmin  
Warning: To use public-key authentication, you must create a public key for user  
"CORP\Admin".
```

使用下列命令為CORP\Admin使用者建立公有金鑰：

```
FSxId0123456ab::> security login publickey create -username "CORP  
\Admin" -publickey "ecdsa-sha2-nistp256 SECRET_STRING_HERE_IS_REDACTED=  
cwaltham@b0be837a91bf.ant.amazon.com"
```

使用 SSH 搭配 Active Directory 登入資料登入檔案系統

- 如果您選擇 `-application` 類型，以下範例示範如何使用 Active Directory 登入資料ssh將 SSH 傳送至您的檔案系統。的格式username為 "domain-name\user-name"，這是您在建立帳戶時提供的網域名稱和使用者名稱，以反斜線分隔並以引號括住。

```
FSx0123456::> ssh "CORP\user"@management.fs-abcdef01234567892.fsx.us-east-2.aws.com
```

當系統提示您輸入密碼時，請使用 Active Directory 使用者的密碼。

## 設定公有金鑰身分驗證

若要啟用 SSH 公有金鑰驗證，您必須先產生 SSH 金鑰，並使用 `security login publickey create` 命令將其與管理員帳戶建立關聯。這可讓帳戶存取 SVM。`security login publickey create` 命令接受下列參數。

| 參數                         | 描述                                                                    |
|----------------------------|-----------------------------------------------------------------------|
| <code>-vserver</code> (選用) | 帳戶存取的 SVM 名稱。如果您要為檔案系統使用者設定 SSH 公有金鑰身分驗證，請勿包含 <code>-vserver</code> 。 |
| <code>-username</code>     | 帳戶的使用者名稱。預設值 <code>admin</code> 是叢集管理員的預設名稱。                          |
| <code>-index</code>        | 公有金鑰的索引號碼。如果金鑰是為帳戶建立的第一個金鑰，則預設值為 0。否則，預設值會比帳戶的最高現有索引號碼多一個。            |
| <code>-publickey</code>    | OpenSSH 公有金鑰。以雙引號括住索引鍵。                                               |
| <code>-role</code>         | 指派給帳戶的存取控制角色。                                                         |
| <code>-comment</code> (選用) | 公有金鑰的描述性文字。以雙引號括住文字。                                                  |

下列範例會將公有金鑰與 SVM `svmadmin` 的 SVM 管理員帳戶建立關聯 `svm01`。公有金鑰已指派索引號碼 5。

```
Fsx0123456::> security login publickey create -vserver svm01 -username svmadmin
-index 5 -publickey "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAsPH64CYbUsDQCdW22JnK6J/
vU9upnKzd2zAk9C1f7YaWRUAFNs2Qe5lUmQ3ldi8AD0Vfbr5T6HZPCixNAIzaFciDy7hgnmdj9eNGedGr/
JNrftQbLD1hZybX
+72DpQB0tYWBhe6eDJ1oPLobZBGfMlPXh8VjeU44i7W4+s0hG0E=tsmith@publickey.example.com"
```

### Important

您必須是 SVM 或檔案系統管理員才能執行此任務。

## 更新檔案系統和 SVM 角色的密碼需求

您可以使用 CLI 命令更新檔案系統或 SVM [security login role config modify](#) ONTAP 角色的密碼需求。此命令僅適用於具有 fsxadmin 角色的檔案系統管理員帳戶。修改密碼需求時，如果有任何具有該角色的現有使用者將受到變更影響，系統會發出警告。

對於在 fsx SVM 上具有 vsadmin-readonly 角色的使用者，下列範例會將長度下限密碼需求修改為 12 個字元。在此範例中，有具有此角色的現有使用者。

```
FsxId0123456::> security login role config modify -role vsadmin-readonly -vserver fsx -  
passwd-minlength 12
```

由於現有使用者，系統會顯示下列警告：

```
Warning: User accounts with this role exist. Modifications to the username/password  
restrictions on this role could result in non-compliant user  
accounts.
```

```
Do you want to continue? {y|n}:
```

```
FsxId0123456::>
```

## 更新 fsxadmin 帳戶密碼失敗

當您更新 fsxadmin 使用者的密碼時，如果不符合檔案系統上設定的密碼要求，您可能會收到錯誤。您可以使用 CLI 或 REST API `security login role config show` ONTAP 命令來檢視密碼需求。

檢視檔案系統或 SVM 角色的密碼需求

- 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。*management\_endpoint\_ip* 將取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

- `security login role config show` 命令會傳回檔案系統或 SVM 角色的密碼需求。

```
FsxId0123456:> security login role config show -role fsxadmin -
fields password_requirement_fields
```

針對 `-fields` 參數，指定下列任何或所有項目：

- `passwd-minlength` – 密碼的長度下限。
- `passwd-min-special-chars` – 密碼中的特殊字元數目下限。
- `passwd-min-lowercase-chars` – 密碼中的小寫字元數下限。
- `passwd-min-uppercase-chars` – 密碼中的大寫字元數下限。
- `passwd-min-digits` – 密碼中的位數下限。
- `passwd-alphanum` – 包含或排除英數字元的相關資訊。
- `passwd-expiry-time` – 密碼過期時間。
- `passwd-expiry-warn-time` – 密碼過期警告時間。

3. 執行下列命令以查看所有密碼需求：

```
FsxId0123456:> security login role config show -role fsxadmin -fields passwd-
minlength, passwd-min-special-chars, passwd-min-lowercase-chars, passwd-min-
digits, passwd-alphanum, passwd-expiry-time, passwd-expiry-warn-time, passwd-min-
uppercase-chars
```

| vserver      | role     | passwd-minlength | passwd-alphanum | passwd-min-special-chars | passwd-expiry-time | passwd-min-lowercase-chars | passwd-min-uppercase-chars | passwd-min-digits | passwd-expiry-warn-time |
|--------------|----------|------------------|-----------------|--------------------------|--------------------|----------------------------|----------------------------|-------------------|-------------------------|
| FsxId0123456 | fsxadmin | 3                | enabled         | 0                        | 0                  | 0                          | 0                          | unlimited         | unlimited               |



## 配額

接下來，您可以了解使用 Amazon FSx for NetApp ONTAP 時的配額。

### 主題

- [您可以提高的配額](#)
- [每個檔案系統的資源配額](#)

## 您可以提高的配額

以下是 AWS 帳戶 AWS 區域您可以增加的每個 Amazon FSx for NetApp ONTAP 配額。

| 資源             | 預設        | 描述                                                                  |
|----------------|-----------|---------------------------------------------------------------------|
| ONTAP 檔案系統     | 100       | 您可以在此帳戶中建立的 Amazon FSx for NetApp ONTAP 檔案系統數目上限。                   |
| ONTAP SSD 儲存容量 | 524 , 288 | 此帳戶中所有 Amazon FSx for NetApp ONTAP 檔案系統的 SSD 儲存容量上限（以 GiB 為單位）。     |
| ONTAP 輸送量容量    | 10,240    | 此帳戶中所有 Amazon FSx for NetApp ONTAP 檔案系統的輸送量容量上限 (MBps)。             |
| ONTAP SSD IOPS | 1,000,000 | 此帳戶中所有 Amazon FSx for NetApp ONTAP 檔案系統的 SSD IOPS 數量上限。             |
| ONTAP 備份       | 10,000    | 您可以在 中擁有的所有 Amazon FSx for NetApp ONTAP 檔案系統的使用者起始磁碟區備份數量上限 AWS 帳戶。 |

## 請求提高配額

1. 開啟 [AWS 支援](#) 頁面，若必要請登入，然後選擇 Create case (建立案例)。
2. 針對建立案例，選擇帳戶和帳單支援。
3. 在案例詳細資訊面板中，執行下列項目：
  - 針對類型選擇帳戶。
  - 針對類別選擇其他帳戶問題。
  - 針對主題輸入 **Amazon FSx for NetApp ONTAP service limit increase request**。
  - 提供請求的詳細描述，包括：
    - 如果您想要增加的 FSx 配額，以及如果知道，您想要增加的值。
    - 您尋求提高配額的原因。
    - 您要請求增加的每個檔案系統的檔案系統 ID 和區域。
4. 提供您偏好的聯絡選項，然後選擇提交。

## 每個檔案系統的資源配額

下表列出 中每個檔案系統的 Amazon FSx for NetApp ONTAP 資源配額 AWS 區域。

| 資源          | 每個檔案系統的限制                                                                                                                                             |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSD 儲存容量下限  | 每個高可用性 (HA) 對 1,024 GiB                                                                                                                               |
| SSD 儲存容量上限  | <ul style="list-style-type: none"> <li>• 第二代單一可用區檔案系統：每個 HA 對 512 TiB，最多 1 PiB</li> <li>• 第二代異地同步備份檔案系統：512 TiB</li> <li>• 第一代檔案系統：192 TiB</li> </ul> |
| SSD IOPS 上限 | 第二代檔案系統： <ul style="list-style-type: none"> <li>• 單一可用區每個 HA 對 200,000 個（最多 12 對）</li> <li>• 異地同步備份總計 200,000</li> </ul>                              |

| 資源      | 每個檔案系統的限制                                                                                                                                                                                                                                                                                                                                          |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | <p>第一代檔案系統：</p> <ul style="list-style-type: none"> <li>• 美國東部（俄亥俄）區域、美國東部（維吉尼亞北部）區域、美國西部（奧勒岡）區域和歐洲（愛爾蘭）為 160,000</li> <li>• 在所有其他 <a href="#">FSx for ONTAP 可用 AWS 區域的情況下為 80,000</a></li> </ul>                                                                                                                                                   |
| 最小輸送量   | <ul style="list-style-type: none"> <li>• 第二代檔案系統 (1 個 HA 對)：384 MBps</li> <li>• 第二代檔案系統 (2 個或更多 HA 對)：每個 HA 對 1,536 MBps</li> <li>• 第一代檔案系統：128 MBps</li> </ul>                                                                                                                                                                                    |
| 最大輸送量   | <p>第二代檔案系統：</p> <ul style="list-style-type: none"> <li>• 單一可用區 73,728 MBps<sup>1</sup></li> <li>• 異地同步備份 6,144 MBps</li> </ul> <p>第一代檔案系統：</p> <ul style="list-style-type: none"> <li>• 美國東部（俄亥俄）區域、美國東部（維吉尼亞北部）區域、美國西部（奧勒岡）區域和歐洲（愛爾蘭）為 4,096 MBps<sup>2</sup></li> <li>• 在<a href="#">所有其他 FSx for ONTAP 可用 AWS 區域的情況下為 2,048 MBps</a></li> </ul> |
| 磁碟區數量上限 | <ul style="list-style-type: none"> <li>• 第二代檔案系統 (1 個 HA 對)：500</li> <li>• 第二代檔案系統 (2 個或更多 HA 對)：1,000</li> <li>• 第一代檔案系統：500</li> </ul>                                                                                                                                                                                                           |

| 資源                             | 每個檔案系統的限制                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 快照數量上限                         | 每個磁碟區 1,023 <sup>個3</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 備份數量上限                         | 每個磁碟區 4,091 <sup>個4</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SVMs 數量上限                      | <p>具有一個 HA 對的第二代檔案系統：</p> <ul style="list-style-type: none"> <li>• 6 (384 MBps 的輸送量容量)</li> <li>• 6 (768 MBps 的輸送量容量)</li> <li>• 14 (1,536 MBps 的輸送量容量)</li> <li>• 14 (3,072 MBps 的輸送量容量)</li> <li>• 24 (6,144 MBps 的輸送量容量)</li> </ul> <p>具有 2–12 個 HA 對的第二代檔案系統：</p> <ul style="list-style-type: none"> <li>• 5</li> </ul> <p>第一代檔案系統：</p> <ul style="list-style-type: none"> <li>• 6 (128 MBps 輸送量)</li> <li>• 6 (256 MBps 輸送量)</li> <li>• 14 (512 MBps 輸送量)</li> <li>• 14 (1,024 MBps 輸送量)</li> <li>• 24 (2,048 MBps 輸送量)</li> <li>• 24 (4,096 MBps 輸送量)</li> </ul> |
| 標籤數量上限                         | 50                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 自動備份的最長保留期間                    | 90 天                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 使用者啟動備份的最長保留期間                 | 無保留限制                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 每個檔案系統支援的路由數量上限                | 50 <sup>5</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 每個檔案伺服器的用戶端連線數目上限 <sup>6</sup> | 100,000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

**Note**

- <sup>1</sup> 在具有 12 個 HA 對的第二代單一可用區檔案系統上 (每個 HA 對 6,144 MBps)。如需詳細資訊，請參閱[管理高可用性 \(HA\) 對](#)。
- <sup>2</sup> 若要佈建 4 Gbps 的輸送量容量，您的 FSx for ONTAP 第一代檔案系統需要支援的 SSD IOPS 上限 (160,000) 和至少 5,120 GiB 的 SSD 儲存容量組態 AWS 區域。如需哪些 AWS 區域支援 4,096 MBps 輸送量的詳細資訊，請參閱[輸送量容量對效能的影響](#)。
- <sup>3</sup> 您可以隨時為每個磁碟區儲存最多 1,023 個快照。達到此限制後，您必須先刪除現有的快照，才能建立新的磁碟區快照。
- <sup>4</sup> 您可以隨時為每個磁碟區儲存最多 4,091 個備份。達到此限制後，您必須先刪除現有的備份，才能建立新的磁碟區備份。
- <sup>5</sup> 您可以隨時為每個檔案系統設定最多 50 個路由。達到此限制後，您必須先刪除現有的路由，才能設定新的路由。檔案系統擁有的路由數量取決於其擁有的 SVMs 數量，以及與其相關聯的路由表數量。您可以使用下列方程式來判斷檔案系統的現有路由數量： $(1 + \text{檔案系統中SVMs數量}) * (\text{與檔案系統關聯的路由表})$ 。
- <sup>6</sup> 用戶端連線定義為特定檔案伺服器的單一 TCP 連線。檔案系統中每個 HA 對有一個作用中的檔案伺服器。用戶端可以有多个 TCP 連線至檔案伺服器。例如，如果用戶端使用多路徑。

# 對 Amazon FSx for NetApp ONTAP 進行故障診斷

使用下列各節來協助疑難排解 FSx for ONTAP 檔案系統。

## 主題

- [您的檔案系統處於 MISCONFIGURED 狀態](#)
- [您無法存取您的檔案系統](#)
- [您的儲存虛擬機器 \(SVM\) 處於 MISCONFIGURED 狀態](#)
- [您無法將儲存虛擬機器 \(SVM\) 加入 Active Directory](#)
- [您無法刪除儲存虛擬機器或磁碟區](#)
- [您的磁碟區處於 MISCONFIGURED 狀態](#)
- [您的磁碟區儲存容量不足](#)
- [由於磁碟區容量不足，您的備份失敗](#)
- [故障診斷網路問題](#)

## 您的檔案系統處於 MISCONFIGURED 狀態

檔案系統處於 MISCONFIGURED 狀態有許多潛在原因，每個系統都有自己的解析度，如下所示。

## 主題

- [VPC 擁有者帳戶已停用異地同步備份 VPC 共用](#)
- [您無法在多可用區檔案系統上建立新的 SVM](#)
- [檔案系統的 SSD 儲存層已滿 90%](#)

## VPC 擁有者帳戶已停用異地同步備份 VPC 共用

共用 VPC 子網路 AWS 帳戶 中參與者建立的異地同步備份檔案系統將進入 MISCONFIGURED 狀態，原因如下：

- 共用 VPC 子網路的擁有者帳戶已停用 FSx for ONTAP 檔案系統的多可用區域 VPC 共用支援。
- 擁有者帳戶已停止共用 VPC 子網路。

如果擁有者帳戶已停止共用 VPC 子網路，您會在該檔案系統的主控台中看到下列訊息：

The vpc ID `vpc-012345abcde` does not exist

若要解決此問題，您必須聯絡與您共用 VPC 子網路的擁有者帳戶。如需詳細資訊，請參閱 [在共用子網路中建立 FSx for ONTAP 檔案系統](#) 以取得詳細資訊。

## 您無法在多可用區檔案系統上建立新的 SVM

對於共用 VPC AWS 帳戶 中參與者建立的異地同步備份檔案系統，由於下列其中一個原因，您將無法建立新的 SVM：

- 共用 VPC 子網路的擁有者帳戶已停用 FSx for ONTAP 檔案系統的多可用區域 VPC 共用支援。
- 擁有者帳戶已停止共用 VPC 子網路。

若要解決此問題，您必須聯絡與您共用 VPC 子網路的擁有者帳戶。如需詳細資訊，請參閱 [在共用子網路中建立 FSx for ONTAP 檔案系統](#) 以取得詳細資訊。

## 檔案系統的 SSD 儲存層已滿 90%

您的單一可用區或多可用區檔案系統的 SSD 儲存層目前已滿 90%。我們建議您持續不超過 SSD 儲存層的 80% 使用率。如果您在檔案系統的下一個維護時段之前未釋放 SSD 儲存層中的空間，FSx for ONTAP 會在修補操作期間暫時降低檔案系統的輸送量。這是為了確保背景維護程序可以在合理的期間內完成。若要避免這種情況，請將 SSD 儲存層的使用率降低到 90% 以下。您可以透過多種方式降低 SSD 使用率，包括：

- 增加檔案系統的 SSD 儲存容量。
- 透過刪除不需要的資料。
- 透過刪除不需要的磁碟區快照。

如需詳細資訊，請參閱[管理儲存容量](#)。

## 您無法存取您的檔案系統

本節說明與無法存取您的檔案系統相關的問題和解決方案。

### 主題

- [您的多可用區檔案系統缺少路由表標籤](#)

- [您的檔案系統有超過 50 個路由](#)
- [您的檔案系統缺少一或多個檔案伺服器的路由](#)
- [檔案系統的彈性網路界面已修改或刪除](#)
- [已刪除連接至檔案系統彈性網路界面的彈性 IP 地址](#)
- [檔案系統的 VPC 安全群組缺少必要的傳入規則](#)
- [運算執行個體的 VPC 安全群組缺少必要的傳出規則](#)
- [運算執行個體的子網路不會使用任何與檔案系統相關聯的路由表](#)
- [Amazon FSx 無法更新使用 建立的異地同步備份檔案系統的路由表 AWS CloudFormation](#)
- [無法從另一個 VPC 中的用戶端透過 iSCSI 存取檔案系統](#)
- [擁有的帳戶已停止共用 VPC 子網路](#)
- [無法透過 NFS、SMB、ONTAP CLI 或 ONTAP REST API 從另一個 VPC 或內部部署中的用戶端存取檔案系統](#)

## 您的多可用區檔案系統缺少路由表標籤

Amazon FSx 會使用標籤型身分驗證來管理多可用區域檔案系統的 VPC 路由表。與您的檔案系統相關聯的一或多個路由表目前缺少這些路由表標籤。這些路由表會以 標記Key: AmazonFSx; Value: ManagedByAmazonFSx。如果您在下一個維護時段之前未手動新增這些標籤，則與缺少標籤的路由表相關聯的子網路中的任何用戶端都會在修補操作期間暫時無法存取檔案系統。若要避免這種情況，請手動新增缺少的路由表標籤。

如需詳細資訊，請參閱[更新檔案系統](#)。

## 您的檔案系統有超過 50 個路由

您的檔案系統目前有超過 50 個與其相關聯的路由。如果您在檔案系統下一個排定的維護時段之前未移除其中一些路由，容錯移轉程序可能需要比平常更長的時間。若要避免這種情況，請將路由數量減少到 50 以下。以下是您可以採取的步驟，以減少與檔案系統相關聯的路由數量：

- 刪除任何多餘的路由
- 減少與檔案系統相關聯的 SVMs 數量
- 減少與檔案系統相關聯的路由表數量

如需詳細資訊，請參閱[更新檔案系統](#)及[刪除儲存虛擬機器 \(SVM\)](#)。



## 您的檔案系統缺少一或多個檔案伺服器的路由

您的檔案系統目前缺少一或多個檔案伺服器的路由，且現有的路由表沒有足夠的空間來新增路由表項目。如果您在檔案系統下一個排定的維護時段之前未新增缺少的路由，任何連線的用戶端都會在修補操作期間中斷連線。若要避免這種情況，請新增缺少的路由。

如需詳細資訊，請參閱[更新檔案系統及配額](#)。

## 檔案系統的彈性網路界面已修改或刪除

您不得修改或刪除任何檔案系統的彈性網路界面。修改或刪除網路界面可能會導致虛擬私有雲端 (VPC) 與檔案系統之間的連線永久中斷。建立新的檔案系統，請勿修改或刪除 Amazon FSx 網路介面。如需詳細資訊，請參閱[使用 Amazon VPC 的檔案系統存取控制](#)。

## 已刪除連接至檔案系統彈性網路界面的彈性 IP 地址

Amazon FSx 不支援從公有網際網路存取檔案系統。Amazon FSx 會自動分離任何彈性 IP 地址，這是可從網際網路連線的公有 IP 地址，而該公有 IP 地址會連接到檔案系統的彈性網路界面。如需詳細資訊，請參閱[支援的用戶端](#)。

## 檔案系統的 VPC 安全群組缺少必要的傳入規則

檢閱 中指定的傳入規則[Amazon VPC 安全群組](#)，並確保與您檔案系統相關聯的安全群組具有對應的傳入規則。

## 運算執行個體的 VPC 安全群組缺少必要的傳出規則

檢閱 中指定的傳出規則[Amazon VPC 安全群組](#)，並確保與運算執行個體相關聯的安全群組具有對應的傳出規則。

## 運算執行個體的字網路不會使用任何與檔案系統相關聯的路由表

FSx for ONTAP 會建立端點來存取 VPC 路由表中的檔案系統。我們建議您將檔案系統設定為使用與用戶端所在子網路相關聯的所有 VPC 路由表。根據預設，Amazon FSx 會使用 VPC 的主要路由表。您可以選擇性地為 Amazon FSx 指定一或多個路由表，以便在建立檔案系統時使用。

如果您可以 ping 檔案系統的叢集間端點，但無法 ping 檔案系統的管理端點（如需[檔案系統資源](#)詳細資訊，請參閱），您的用戶端可能不會位於與其中一個檔案系統的路由表相關聯的子網路中。若要

存取您的檔案系統，請將其中一個檔案系統的路由表與用戶端的子網路建立關聯。如需更新檔案系統 Amazon VPC 路由表的相關資訊，請參閱 [更新檔案系統](#)。

## Amazon FSx 無法更新使用 建立的異地同步備份檔案系統的路由表 AWS CloudFormation

Amazon FSx 會使用標籤型身分驗證來管理多可用區域檔案系統的 VPC 路由表。這些路由表會以標記 Key: AmazonFSx; Value: ManagedByAmazonFSx。使用 建立或更新 FSx for ONTAP 多可用區檔案系統時，AWS CloudFormation 建議您手動新增 Key: AmazonFSx; Value: ManagedByAmazonFSx 標籤。

如果您無法連線到多可用區檔案系統，請檢查與檔案系統相關聯的 VPC 路由表是否已標記 Key: AmazonFSx; Value: ManagedByAmazonFSx。如果不是，則 Amazon FSx 無法更新這些路由表，以在發生容錯移轉事件時，將管理和資料連接埠的浮動 IP 地址路由到作用中的檔案伺服器。如需更新檔案系統 Amazon VPC 路由表的相關資訊，請參閱 [更新檔案系統](#)。

## 無法從另一個 VPC 中的用戶端透過 iSCSI 存取檔案系統

若要從另一個 VPC 中的用戶端透過網際網路小型電腦系統介面 (iSCSI) 通訊協定存取檔案系統，您可以設定 Amazon VPC 對等互連，或在 AWS Transit Gateway 與您的檔案系統相關聯的 VPC 與用戶端所在的 VPC 之間設定。如需詳細資訊，請參閱《Amazon Virtual Private Cloud 指南》中的 [建立和接受 VPC 互連連線](#)。

## 擁有的帳戶已停止共用 VPC 子網路

如果您在已與您共用的 VPC 子網路中建立檔案系統，擁有的帳戶可能已停止共用 VPC 子網路。

如果擁有者帳戶已停止共用 VPC 子網路，您會在該檔案系統的主控台中看到下列訊息：

```
The vpc ID vpc-012345abcde does not exist
```

您需要聯絡擁有的帳戶，讓他們可以與您重新共用子網路。

## 無法透過 NFS、SMB、ONTAP CLI 或 ONTAP REST API 從另一個 VPC 或內部部署中的用戶端存取檔案系統

若要從另一個 VPC 或內部部署中的用戶端透過網路檔案系統 (NFS)、伺服器訊息區塊 (SMB) 或 NetApp ONTAP CLI 和 REST API 存取檔案系統，您必須使用與檔案系統相關聯的 VPC 與用戶端所在的網路 AWS Transit Gateway 之間設定路由。如需詳細資訊，請參閱 [存取 FSx for ONTAP 資料](#)。

## 您的儲存虛擬機器 (SVM) 處於 MISCONFIGURED 狀態

儲存虛擬機器進入 MISCONFIGURED 狀態有許多潛在原因，每個都具有自己的解析度，如下所示。

### 您的 SVM 具有離線磁碟區

您的檔案系統包含處於離線狀態的磁碟區。我們建議您持續讓磁碟區保持線上狀態。如果您在檔案系統下一個維護時段之前未上線此磁碟區，Amazon FSx 會在修補操作期間暫時上線此磁碟區。若要避免這種情況，請上線或刪除磁碟區。

若要讓離線磁碟區恢復上線，請使用 [volume online](#) ONTAP CLI 命令，如下列範例所示。如果只有一個 SVM (Vserver)，則不需要指定 `-vserver` 參數。

```
FsxID-abcdef123456:~> volume online -volume volume_name -vserver svm_name  
  
Volume 'vs1:vol1' is now online.
```

### 您的 SVM 具有具有 iSCSI LUN 或 NVMe/TCP 命名空間的離線磁碟區

您的檔案系統包含處於受限狀態的磁碟區。我們建議您持續讓磁碟區保持線上狀態。如果您在檔案系統下一個維護時段之前未上線此磁碟區，Amazon FSx 會在修補操作期間暫時上線此磁碟區。若要避免這種情況，請上線或刪除磁碟區。

若要讓離線磁碟區恢復上線，請使用 [volume online](#) ONTAP CLI 命令，如下列範例所示。如果只有一個 SVM (Vserver)，則不需要指定 `-vserver` 參數。

```
FsxID-abcdef123456:~> volume online -volume volume_name -vserver svm_name  
  
Volume 'vs1:vol1' is now online.
```

## 您無法將儲存虛擬機器 (SVM) 加入 Active Directory

如果您無法將 SVM 加入 Active Directory (AD)，請先檢閱 [將 SVMs 加入 Microsoft Active Directory 的運作方式](#)。下列各節列出防止 SVM 加入 Active Directory 的常見問題，包括針對每個情況產生的錯誤訊息。

### 主題

- [SVM NetBIOS 名稱與主網域的 NetBIOS 名稱相同。](#)

- [SVM 已加入另一個 Active Directory](#)
- [Amazon FSx 無法連線至 Active Directory 網域控制站，因為 SVM 的 NetBIOS 名稱已在使用中](#)
- [Amazon FSx 無法與您的 Active Directory 網域控制站通訊](#)
- [由於連接埠需求或服務帳戶許可未滿足，Amazon FSx 無法連線至您的 Active Directory](#)
- [Amazon FSx 無法連線至 Active Directory 網域控制站，因為服務帳戶登入資料無效](#)
- [由於服務帳戶登入資料不足，Amazon FSx 無法連線至 Active Directory 網域控制站](#)
- [Amazon FSx 無法與您的 Active Directory DNS 伺服器或網域控制站通訊](#)
- [由於 Active Directory 網域名稱無效，Amazon FSx 無法與您的 Active Directory 通訊。](#)
- [服務帳戶無法存取 SVM Active Directory 組態中指定的管理員群組](#)
- [Amazon FSx 無法連線至 Active Directory 網域控制站，因為指定的組織單位不存在或無法存取](#)

## SVM NetBIOS 名稱與主網域的 NetBIOS 名稱相同。

將 SVM 加入自我管理 Active Directory 失敗，並顯示下列錯誤訊息：

Amazon FSx 無法與您的 Active Directory 建立連線。這是因為您指定的伺服器名稱是主網域的 NetBIOS 名稱。若要修正此問題，請為 SVM 選擇與主網域的 NetBIOS 名稱不同的 NetBIOS 名稱。然後重新嘗試將 SVM 加入 Active Directory。

若要解決此問題，請遵循中所述的程序[使用 AWS Management ConsoleAWS CLI 和 API 將 SVMs 加入 Active Directory](#)，重新嘗試將 SVM 加入 AD。請確定您的 SVM 使用 NetBIOS Active Directory 主網域的名稱不同的 NetBIOS 名稱。

## SVM 已加入另一個 Active Directory

將 SVM 加入 Active Directory 失敗，並顯示下列錯誤訊息：

Amazon FSx 無法建立與 Active Directory 的連線。這是因為 SVM 已加入網域。若要將此 SVM 加入不同的網域，您可以使用 ONTAP CLI 或 REST API 從 Active Directory 中取消加入此 SVM。然後重新嘗試將 SVM 加入不同的 Active Directory。

若要解決問題，請執行下列動作：

1. 使用 NetApp ONTAP CLI 從目前的 Active Directory 中取消加入 SVM。如需詳細資訊，請參閱[使用 NetApp ONTAP CLI 從 SVM 取消加入 Active Directory](#)。

2. 請遵循中所述的程序[使用 AWS Management ConsoleAWS CLI 和 API 將 SVMs 加入 Active Directory](#)，重新嘗試將 SVM 加入新的 AD。

## Amazon FSx 無法連線至 Active Directory 網域控制站，因為 SVM 的 NetBIOS 名稱已在使用中

建立加入自我管理 AD 的 SVM 失敗，並顯示下列錯誤訊息：

Amazon FSx 無法與您的 Active Directory 建立連線。這是因為您指定的 NetBIOS（電腦）名稱已在 Active Directory 中使用。若要修正此問題，請為不在 Active Directory 中使用的 SVM 選擇 NetBIOS 名稱。請指定 NetBIOS（電腦），然後重新嘗試將 SVM 加入 Active Directory。

若要解決此問題，請遵循中所述的程序[使用 AWS Management ConsoleAWS CLI 和 API 將 SVMs 加入 Active Directory](#)，重新嘗試將 SVM 加入 AD。確保您為 SVM 使用唯一且尚未在 Active Directory 中使用的 NetBIOS 名稱。

## Amazon FSx 無法與您的 Active Directory 網域控制站通訊

將 SVM 加入自我管理 AD 失敗，並顯示下列錯誤訊息：

Amazon FSx 無法與您的 Active Directory 通訊。若要修正此問題，請確定 Amazon FSx 與您的網域控制站之間允許網路流量。然後重新嘗試將 SVM 加入 Active Directory。

要解決此問題，請依照下列步驟：

1. 檢閱中所述的需求[網路組態需求](#)，並進行必要的變更，以啟用 Amazon FSx 和 AD 之間的網路通訊。
2. 一旦 Amazon FSx 能夠與您的 AD 通訊，請遵循中所述的程序[使用 AWS Management ConsoleAWS CLI 和 API 將 SVMs 加入 Active Directory](#)，並再次嘗試將 SVM 加入您的 AD。

## 由於連接埠需求或服務帳戶許可未滿足，Amazon FSx 無法連線至您的 Active Directory

將 SVM 加入自我管理 AD 失敗，並顯示下列錯誤訊息：

Amazon FSx 無法與您的 Active Directory 建立連線。這是因為不符合 Active Directory 的連接埠需求，或是所提供的服務帳戶沒有使用指定組織單位將儲存虛擬機器加入網域的許可。若要修正此問題，



請在解決連接埠和服務帳戶的任何許可問題後更新儲存虛擬機器的 Active Directory 組態，如 Amazon FSx 使用者指南中所述。

要解決此問題，請依照下列步驟：

1. 檢閱中所述的需求[網路組態需求](#)，並進行必要的變更以符合聯網需求，並確保在必要的連接埠上啟用通訊
2. 檢閱 中所述的服務帳戶需求[Active Directory 服務帳戶需求](#)。確保服務帳戶具有使用指定組織單位將 SVM 加入 AD 網域所需的委派許可。
3. 變更連接埠許可或服務帳戶後，請遵循中所述的程序[使用 AWS Management ConsoleAWS CLI 和 API 將 SVMs 加入 Active Directory](#)，並再次嘗試將 SVM 加入 AD。

## Amazon FSx 無法連線至 Active Directory 網域控制站，因為服務帳戶登入資料無效

將 SVM 加入自我管理 Active Directory 失敗，並顯示下列錯誤訊息：

Amazon FSx 無法與您的 Active Directory 網域控制站建立連線，因為提供的服務帳戶登入資料無效。若要修正此問題，請使用有效的服務帳戶更新儲存虛擬機器的 Active Directory 組態。

若要解決此問題，請使用中所述的程序[使用 AWS Management ConsoleAWS CLI、和 API 更新現有的 SVM Active Directory 組態](#)來更新 SVM 的服務帳戶登入資料。輸入服務帳戶使用者名稱時，請務必只包含使用者名稱（例如 ServiceAcct），且不要包含任何網域字首（例如 corp.com \ServiceAcct）或網域尾碼（例如）ServiceAcct@corp.com。輸入服務帳戶使用者名稱時，請勿使用辨別名稱 (DN)（例如 CN=ServiceAcct,OU=example,DC=corp,DC=com）。

## 由於服務帳戶登入資料不足，Amazon FSx 無法連線至 Active Directory 網域控制站

將 SVM 加入自我管理 Active Directory 失敗，並顯示下列錯誤訊息：

Amazon FSx 無法與您的 Active Directory 網域控制站 (Active Directory) 建立連線。這是因為 Active Directory 的連接埠需求未滿足，或提供的服務帳戶沒有將儲存虛擬機器加入具有指定組織單位之網域的許可。

若要解決此問題，請確定您已將所需的許可委派給您提供的服務帳戶。服務帳戶必須能夠在您加入檔案系統的網域中建立和刪除 OU 中的電腦物件。服務帳戶至少也需要具有執行下列動作的許可：

- 重設密碼
- 限制帳戶讀取和寫入資料
- 驗證寫入 DNS 主機名稱的能力
- 已驗證能夠寫入服務主體名稱
- 能夠建立和刪除電腦物件
- 驗證讀取和寫入帳戶限制的能力

如需建立具有正確許可之服務帳戶的詳細資訊，請參閱 [Active Directory 服務帳戶需求](#) 和 [將許可委派給您的 Amazon FSx 服務帳戶](#)。

## Amazon FSx 無法與您的 Active Directory DNS 伺服器或網域控制站通訊

將 SVM 加入自我管理 Active Directory 失敗，並顯示下列錯誤訊息：

Amazon FSx 無法與您的 Active Directory 通訊。這是因為 Amazon FSx 無法連線到您網域提供的 DNS 伺服器或網域控制站。若要修正此問題，請使用有效的 DNS 伺服器更新儲存虛擬機器的 Active Directory 組態，以及允許流量從儲存虛擬機器流向網域控制器的聯網組態。

若要解決此問題，請使用下列程序：

1. 如果只有 Active Directory 中的某些網域控制站可以連線，例如由於地理限制或防火牆，您可以新增偏好的網域控制站。使用此選項，Amazon FSx 會嘗試聯絡偏好的網域控制站。使用 [vserver cifs domain preferred-dc add](#) NetApp ONTAP CLI 命令新增偏好的網域控制站，如下所示：
  - a. 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。*management\_endpoint\_ip* 將取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

- b. 輸入下列命令，其中：
  - -vserver vservice\_name 指定儲存虛擬機器 (SVM) 名稱。
  - -domain domain\_name 指定指定網域控制站所屬網域的完整 Active Directory 名稱 (FQDN)。

- `-preferred-dc IP_address,...` 會依偏好順序，指定偏好網域控制站的一或多個 IP 地址，做為逗號分隔清單。

```
FsxId123456789::> vservers cifs domain preferred-dc add -vservers vservers_name -
domain domain_name -preferred-dc IP_address, ...+
```

下列命令會將網域控制站 172.17.102.25 和 172.17.102.24 新增至 SVM vs1 上 SMB 伺服器用來管理 `cifs.lab.example.com` 網域外部存取的偏好網域控制站清單。

```
FsxId123456789::> vservers cifs domain preferred-dc add -vservers vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

2. 檢查您的網域控制器是否可以使用 DNS 解析。使用 [vservers services access-check dns forward-lookup](#) NetApp ONTAP CLI 命令，根據指定的 DNS 伺服器或 vservers 的 DNS 組態來傳回主機名稱的 IP 地址。
  - a. 若要存取 ONTAP CLI，請執行下列命令，在 Amazon FSx for NetApp ONTAP 檔案系統或 SVM 的管理連接埠上建立 SSH 工作階段。`management_endpoint_ip` 將取代為檔案系統管理連接埠的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

如需詳細資訊，請參閱[使用 CLI ONTAP 管理檔案系統](#)。

- b. 使用下列命令進入 ONTAP CLI 進階模式。

```
FsxId123456789::> set adv
```

- c. 輸入下列命令，其中：
- `-vservers vservers_name` 指定儲存虛擬機器 (SVM) 名稱。
  - `-hostname host_name` 指定要在 DNS 伺服器上查詢的主機名稱。
  - `-node node_name` 指定執行命令的節點名稱。
  - `-lookup-type` 指定要在 DNS 伺服器上查詢的 IP 地址類型，預設值為 `all`。

```
FsxId123456789::> vservers services access-check dns forward-lookup \
-vservers vservers_name -node node_name \
```



```
-domains domain_name -name-servers dns_server_ip_address \  
-hostname host_name
```

3. 檢閱將 SVM 加入 AD 時[所需的資訊](#)。
4. 將 SVM 加入 AD 時，請檢閱[聯網需求](#)。
5. 使用中所述的程序[網路組態需求](#)，使用 AD DNS 伺服器的正確 IP 地址來更新 SVM 的 AD 組態。

由於 Active Directory 網域名稱無效，Amazon FSx 無法與您的 Active Directory 通訊。

將 SVM 加入自我管理 Active Directory 失敗，並顯示下列錯誤訊息：

Amazon FSx 偵測到提供的 FQDN 無效。若要修正此問題，請使用符合組態要求的 FQDN 來更新儲存虛擬機器的 Active Directory 組態。

若要解決此問題，請使用下列程序：

1. 檢閱 中描述的內部部署 Active Directory [將 SVM 加入 Active Directory 時所需的資訊](#) 網域名稱要求 確定您嘗試加入的 AD 符合該要求。
2. 使用中所述的程序[使用 AWS Management ConsoleAWS CLI 和 API 將 SVMs 加入 Active Directory](#)，然後重新嘗試將 SVM 加入 AD。請務必針對 AD 網域的 FQDN 使用正確的格式。

## 服務帳戶無法存取 SVM Active Directory 組態中指定的管理員群組

將 SVM 加入自我管理 Active Directory 失敗，並顯示下列錯誤訊息：

Amazon FSx 無法套用您的 Active Directory 組態。這是因為您提供的管理員群組不存在或無法存取您提供的服務帳戶。若要修正此問題，請確定您的聯網組態允許從 SVM 到 Active Directory 網域控制站 (DNS) 和 DNS 伺服器的流量。然後，更新 SVM 的 Active Directory 組態，提供 Active Directory 的 DNS 伺服器，並在網域中指定管理員群組，供提供的服務帳戶存取。

要解決此問題，請依照下列步驟：

1. 檢閱[提供網域群組](#)以對 SVM 執行管理動作的相關資訊。請確定您使用的是 AD 網域管理員群組的正確名稱。
2. 使用中所述的程序[使用 AWS Management ConsoleAWS CLI 和 API 將 SVMs 加入 Active Directory](#)，然後重新嘗試將 SVM 加入 AD。

## Amazon FSx 無法連線至 Active Directory 網域控制站，因為指定的組織單位不存在或無法存取

將 SVM 加入自我管理 Active Directory 失敗，並顯示下列錯誤訊息：

Amazon FSx 無法與您的 Active Directory 建立連線。這是因為您指定的組織單位不存在或無法存取提供的服務帳戶。若要修正此問題，請更新儲存虛擬機器的 Active Directory 組態，指定服務帳戶具有加入許可的組織單位。

要解決此問題，請依照下列步驟：

1. 檢閱將 [SVM 加入 AD 的先決條件](#)。
2. 檢閱將 SVM 加入 AD 時[所需的資訊](#)。
3. 使用[此程序](#)搭配正確的組織單位，重新嘗試將 SVM 加入 AD。

## 您無法刪除儲存虛擬機器或磁碟區

每個 FSx for ONTAP 檔案系統可以包含一或多個儲存虛擬機器 (SVMs)，而每個 SVM 可以包含一或多個磁碟區。刪除資源時，您必須先確保已刪除其所有子項。例如，在刪除 SVM 之前，您必須先刪除 SVM 中的所有非根磁碟區。

### Important

您只能使用 Amazon FSx 主控台、API 和 CLI 刪除儲存虛擬機器。如果磁碟區已啟用 Amazon FSx 備份，您只能使用 Amazon FSx 主控台、API 或 CLI 刪除磁碟區。

為了協助保護您的資料和組態，Amazon FSx 在某些情況下會防止刪除 SVMs 和磁碟區。如果您嘗試刪除 SVM 或磁碟區，但您的刪除請求未成功，Amazon FSx 會在 AWS 主控台 AWS Command Line Interface (AWS CLI) 和 API 中提供資源未刪除原因的相關資訊。解決刪除失敗的原因之後，您可以重試刪除請求。

### 主題

- [識別刪除失敗](#)
- [SVM 刪除：無法存取路由表](#)
- [SVM 刪除：對等關係](#)
- [SVM 或磁碟區刪除：SnapMirror](#)

- [SVM 刪除：啟用 Kerberos 的 LIF](#)
- [SVM 刪除：其他原因](#)
- [磁碟區刪除：FlexCache 關係](#)

## 識別刪除失敗

當您刪除 Amazon FSx SVM 或磁碟區時，通常會在資源從 Amazon FSx 主控台、CLI 和 API 消失之前，看到資源Lifecycle的狀態轉換為 DELETING 長達幾分鐘。

如果您嘗試刪除資源，且其Lifecycle狀態從 轉換為 DELETING，然後轉返 CREATED，則此行為表示資源未成功刪除。在此情況下，Amazon FSx 會在CREATED生命週期狀態旁的主控台中報告提醒圖示。選擇提醒圖示會顯示刪除失敗的原因，如下列範例所示。

### Lifecycle state



### Lifecycle transition message

Cannot delete storage virtual machine while it has non-root volumes.

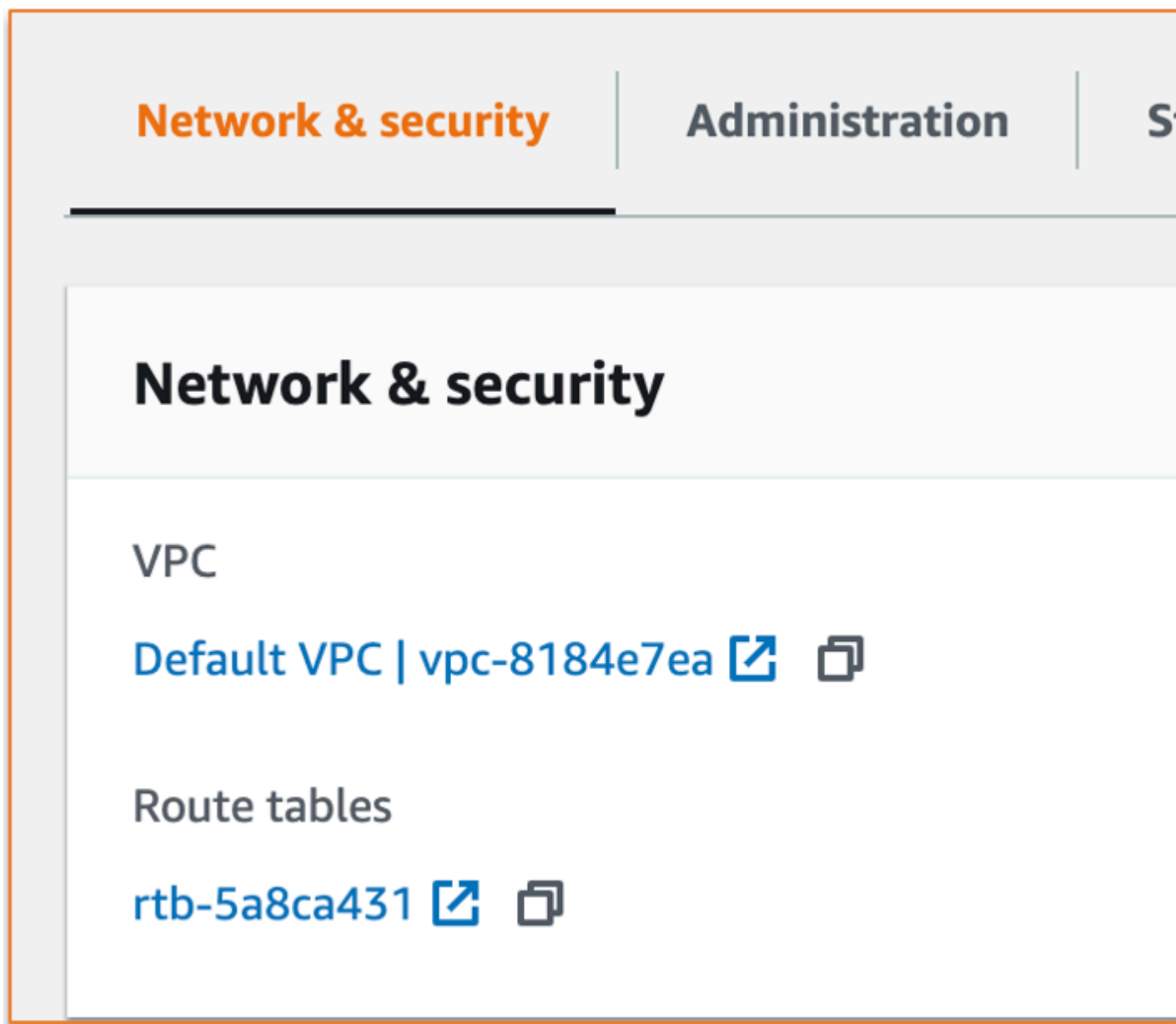
下列各節提供 Amazon FSx 防止 SVM 和磁碟區刪除的最常見原因，並提供如何解決這些問題的step-by-step說明。

## SVM 刪除：無法存取路由表

每個 FSx for ONTAP 檔案系統都會建立一或多個路由表項目，以提供自動容錯移轉和跨可用區域容錯。根據預設，這些路由表項目會在您 VPC 的預設路由表中建立。您可以選擇指定一或多個可建立 FSx for ONTAP 介面的非預設路由表。Amazon FSx 會使用 AmazonFSx 標籤來標記與檔案系統相關聯的每個路由表，如果移除此標籤，可能會導致 Amazon FSx 無法刪除資源。如果發生這種情況，您會看到下列 LifecycleTransitionReason：

Amazon FSx is unable to complete the requested storage virtual machine operation because of an inability to access one or more of the route tables associated with your file system. Please contact ##.

您可以在 Amazon FSx 主控台中找到檔案系統的路由表，方法是導覽至網路與安全索引標籤下方的檔案系統的摘要頁面：



選擇路由表連結會帶您前往路由表。接著，確認與您檔案系統相關聯的每個路由表都已標記此鍵/值對：

Key: AmazonFSx

Value: ManagedByAmazonFSx

| Tags                             |                    |
|----------------------------------|--------------------|
| <input type="text"/> Search tags |                    |
| Key                              | Value              |
| Name                             | Default            |
| AmazonFSx                        | ManagedByAmazonFSx |

如果此標籤不存在，請重新建立，然後嘗試再次刪除 SVM。

## SVM 刪除：對等關係

如果您嘗試刪除屬於對等關係的 SVM 或磁碟區，您必須先刪除對等關係，才能刪除 SVM 或磁碟區。此要求可防止對等 SVMs 運作狀態不佳。如果您的 SVM 因為對等關係而無法刪除，您會看到以下 LifecycleTransitionReason：

Amazon FSx 無法刪除儲存虛擬機器，因為它是 SVM 對等關係或轉換對等關係的一部分。請刪除關係並重試。

您可以透過 ONTAP CLI 刪除 SVM 對等關係。若要存取 ONTAP CLI，請遵循中的步驟[使用 CLI 管理檔案系統](#)。使用 ONTAP CLI，採取下列步驟。

1. 使用以下命令檢查 SVM 對等關係。*svm\_name* 將取代為 SVM 的名稱。

```
FsxId123456789::> vserver peer show -vserver svm_name
```

如果此命令成功，您會看到類似以下的輸出：

| Vserver         | Peer Vserver | Peer State | Peer Cluster           | Peering Applications | Remote Vserver |
|-----------------|--------------|------------|------------------------|----------------------|----------------|
| <i>svm_name</i> | test2        | peered     | FsxId02d81fef0d84734b6 | snapmirror           | fsxDest        |
| <i>svm_name</i> | test3        | peered     | FsxId02d81fef0d84734b6 | snapmirror           | fsxDest        |

2 entries were displayed.

2. 使用以下命令刪除每個 SVM 對等關係。將 *svm\_name*、和 取代 *remote\_svm\_name* 為您的實際值。

```
FsxId123456789abcdef::> vserver peer delete -vserver svm_name -peer-  
vserver remote_svm_name
```

如果此命令成功，您會看到下列輸出：

```
Info: 'vserver peer delete' command is successful.
```

## SVM 或磁碟區刪除：SnapMirror

如同在未先刪除對等關係的情況下，無法刪除具有對等關係的 SVM（請參閱[SVM 刪除：對等關係](#)），在未先刪除 SnapMirror 關係的情況下，無法刪除具有 SnapMirror 關係的 SVM。若要刪除 SnapMirror 關係，請使用 ONTAP CLI 在 SnapMirror 關係的目的地檔案系統上採取下列步驟。若要存取 ONTAP CLI，請遵循中的步驟[使用 CLI ONTAP 管理檔案系統](#)。

### Note

Amazon FSx 備份使用 SnapMirror 來建立檔案系統磁碟區的point-in-time增量備份。您無法在 ONTAP CLI 中刪除備份的此 SnapMirror 關係。不過，當您透過 AWS CLI、API 或主控台刪除磁碟區時，此關係會自動刪除。

1. 使用下列命令，在目的地檔案系統上列出您的 SnapMirror 關係。*svm\_name* 將取代為 SVM 的名稱。

```
FsxId123456789abcdef::> snapmirror show -vserver svm_name
```

如果此命令成功，您會看到類似以下的輸出：

| Source Path         | Destination Type | Path            | Mirror State | Relationship Status | Total Progress | Healthy | Last Updated |
|---------------------|------------------|-----------------|--------------|---------------------|----------------|---------|--------------|
| sourceSvm:sourceVol | XDP              | destSvm:destVol | Snapmirrored | Idle                | -              | true    | -            |

2. 在目的地檔案系統上執行下列命令，以刪除您的 SnapMirror 關係。

```
FsxId123456789abcdef::> snapmirror release -destination-path destSvm:destVol -
source-path sourceSvm:sourceVol -force true
```

## SVM 刪除：啟用 Kerberos 的 LIF

如果您嘗試刪除已啟用 Kerberos 的邏輯界面 (LIF) 的 SVM，您必須先在該 LIF 上停用 Kerberos，才能刪除 SVM。

您可以透過 ONTAP CLI 在 LIF 上停用 Kerberos。若要存取 ONTAP CLI，請遵循中的步驟[使用 CLI 管理檔案系統](#)。

1. 使用下列命令，在 ONTAP CLI 中進入診斷模式。

```
FsxId123456789abcdef::> set diag
```

當系統提示您繼續時，請輸入 **y**。

```
Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y
```

2. 檢查哪些界面已啟用 Kerberos。 *svm\_name* 將取代為 SVM 的名稱。

```
FsxId123456789abcdef::> kerberos interface show -vserver svm_name
```

如果此命令成功，您會看到類似以下的輸出：

```
(vserver nfs kerberos interface show)
      Logical
Vserver  Interface      Address      Kerberos SPN
-----  -
svm_name  nfs_smb_management_1
                               10.19.153.48   enabled
5 entries were displayed.
```

3. 使用以下命令停用 Kerberos LIF。 *svm\_name* 將取代為 SVM 的名稱。您需要提供用來將此 SVM 加入 Active Directory 的 Active Directory 使用者名稱和密碼。

```
FsxId123456789abcdef::> kerberos interface disable -vserver svm_name -lif
nfs_smb_management_1
```

如果此命令成功，您會看到下列輸出。提供您用來將此 SVM 加入 Active Directory 的 Active Directory 使用者名稱和密碼。當系統提示您繼續時，請輸入 **y**。

```
(vserver nfs kerberos interface disable)
Username: admin
Password: *****

Warning: This command deletes the service principal name from the machine account
on the KDC.
Do you want to continue? {y|n}: y

Disabled Kerberos on LIF "nfs_smb_management_1" in Vserver "svm_name".
```

4. 使用以下命令，確認 SVM 上的 Kerberos 已停用。*svm\_name* 將取代為 SVM 的名稱。

```
FsxId123456789abcdef::> kerberos interface show -vserver svm_name
```

如果此命令成功，您會看到類似以下的輸出：

```
(vserver nfs kerberos interface show)
Logical
Vserver      Interface      Address      Kerberos SPN
-----
svm_name    nfs_smb_management_1
                                10.19.153.48  disabled
5 entries were displayed.
```

5. 如果介面顯示為 disabled，請嘗試透過 CLI、API AWS 或主控台再次刪除 SVM。

如果您無法使用上述命令刪除 LIF，您可以使用下列命令強制刪除 Kerberos LIF。*svm\_name* 將取代為 SVM 的名稱。

#### Important

下列命令可以在 Active Directory 上綁定 SVM 的電腦物件。



```
FsxId123456789abcdef:> kerberos interface disable -vserver svm_name -lif  
nfs_smb_management_1 -force true
```

如果此命令成功，您會看到類似以下的輸出。當系統提示您繼續時，請輸入 **y**。

```
(vserver nfs kerberos interface disable)  
  
Warning: Kerberos configuration for LIF "nfs_smb_management_1" in Vserver  
"svm_name" will be deleted.  
The corresponding account on the KDC will not be deleted. Do you want to continue?  
{y|n}: y
```

## SVM 刪除：其他原因

FSx for ONTAP SVMs 在加入 Active Directory 時，會在 Active Directory 中建立電腦物件。在某些情況下，您可能想要使用 ONTAP CLI 手動從 Active Directory 退出 SVM。若要存取 ONTAP CLI，請遵循中的步驟[使用 CLI ONTAP 管理檔案系統](#)，使用 fsxadmin 登入資料在檔案系統層級登入 ONTAP CLI。使用 ONTAP CLI，採取下列步驟從 Active Directory 中退出 SVM。

### Important

此程序可以在 Active Directory 上綁定 SVM 的電腦物件。

1. 使用下列命令，在 ONTAP CLI 中輸入進階模式。

```
FsxId123456789abcdef:> set adv
```

執行此命令後，您會看到此輸出。輸入 **y** 以繼續。

```
Warning: These advanced commands are potentially dangerous; use them only when  
directed to do so by NetApp personnel.  
Do you want to continue? {y|n}: y
```

2. 使用下列命令刪除 Active Directory 的 DNS。*svm\_name* 將取代為 SVM 的名稱。

```
FsxId123456789abcdef:> vservers services name-service dns dynamic-update record
delete -vservers svm_name -lif nfs_smb_management_1
```

 Note

如果 DNS 記錄已刪除或 DNS 伺服器無法連線，則此命令會失敗。如果發生這種情況，請繼續下一個步驟。

3. 使用以下命令停用 DNS。*svm\_name* 將取代為 SVM 的名稱。

```
FsxId123456789abcdef:> vservers services name-service dns dynamic-update modify -
vservers svm_name -is-enabled false -use-secure false
```

如果此命令成功，您會看到下列輸出：

```
Warning: DNS updates for Vserver "svm_name" are now disabled.
Any LIFs that are subsequently modified or deleted
can result in a stale DNS entry on the DNS server,
even when DNS updates are enabled again.
```

4. 從 Active Directory 取消加入裝置。*svm\_name* 將取代為 SVM 的名稱。

```
FsxId123456789abcdef:> vservers cifs delete -vservers svm_name
```

執行此命令後，您會看到下列輸出，其中 *CORP.EXAMPLE.COM* 會取代為您的網域名稱。出現提示時，輸入您的使用者名稱和密碼。當系統詢問您是否要刪除伺服器時，請輸入 **y**。

```
In order to delete an Active Directory machine account for the CIFS server,
you must supply the name and password of a Windows account with sufficient
privileges to remove computers from the "CORP.EXAMPLE.COM" domain.
Enter the user name: admin
Enter the password:
Warning: There are one or more shares associated with this CIFS server
Do you really want to delete this CIFS server and all its shares? {y|n}: y
Warning: Unable to delete the Active Directory computer account for this CIFS
server.
Do you want to continue with CIFS server deletion anyway? {y|n}: y
```

## 磁碟區刪除：FlexCache 關係

除非您先刪除快取關係，否則無法刪除屬於 FlexCache 關係原始磁碟區的磁碟區。若要判斷哪些磁碟區具有 FlexCache 關係，您可以使用 ONTAP CLI。若要存取 ONTAP CLI，請遵循中的步驟[使用 CLI 管理檔案系統](#)。

1. 使用以下命令檢查 FlexCache 關係。

```
FsxId123456789abcdef::> volume flexcache origin show-caches
```

2. 使用以下命令刪除任何快取關係。將 *dest\_svm\_name*、和 取代 *dest\_vol\_name* 為您的實際值。

```
FsxId123456789abcdef::> volume flexcache delete -vserver dest_svm_name -  
volume dest_vol_name
```

3. 刪除快取關係之後，請嘗試再次透過 AWS CLI、API 或主控台刪除 SVM。

## 您的磁碟區處於 MISCONFIGURED 狀態

ONTAP 磁碟區進入 MISCONFIGURED 狀態有許多潛在原因，如下列主題所述。

### 您的磁碟區已滿 98%

您的檔案系統目前包含超過 98% 已滿的磁碟區。我們建議您持續不超過 95% 的磁碟區使用率。如果您在檔案系統下一個維護時段之前沒有釋放磁碟區中的空間，Amazon FSx 會停用磁碟區上的機會鎖定，中斷任何現有的「封鎖」。修補程序完成後，Amazon FSx 會重新啟用磁碟區上的封鎖。若要避免這種情況，請將磁碟區的儲存容量使用率降低至低於 98%。達成此目標的一些方法包括：

- 增加磁碟區的大小。
- 刪除不需要的資料。
- 刪除不需要的快照。

如需詳細資訊，請參閱 [更新儲存容量](#) 和 [刪除快照](#)。

## 您的離線磁碟區具有 iSCSI LUN 或 NVMe/TCP 命名空間

您的檔案系統目前託管處於離線狀態的磁碟區，且該磁碟區包含 iSCSI LUN 或 NVMe/TCP 命名空間，或兩者。我們建議您持續將磁碟區保持在線上。如果您在檔案系統下一個維護時段之前未上線此磁碟區，Amazon FSx 會在修補操作期間暫時上線此磁碟區。若要避免這種情況，請上線或刪除磁碟區。

若要讓離線磁碟區恢復上線，請使用 [volume online](#) ONTAP CLI 命令，如下列範例所示。如果只有一個 SVM (Vserver)，則不需要指定 `-vserver` 參數。

```
FsxID-abcdef123456:> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

## 離線磁碟區是FlexCache原始伺服器

您的檔案系統包含處於離線狀態的 FlexCache 原始磁碟區。我們建議您持續將磁碟區保持在線上。如果您在檔案系統下一個維護時段之前未上線此磁碟區，Amazon FSx 會在修補操作期間暫時上線此磁碟區。在此期間，資料可能會與快取磁碟區中的資料一起寫回 FlexCache 原始磁碟區。若要避免這種情況，請上線或刪除磁碟區。

若要讓離線磁碟區恢復上線，請使用 [volume online](#) ONTAP CLI 命令，如下列範例所示。如果只有一個 SVM (Vserver)，則不需要指定 `-vserver` 參數。

```
FsxID-abcdef123456:> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

## 離線磁碟區是SnapMirror關係的一部分

您的檔案系統目前託管處於離線狀態的磁碟區，且該磁碟區是 SnapMirror 來源或目的地。我們建議您持續將磁碟區保持在線上。如果您在檔案系統下一個維護時段之前未上線此磁碟區，Amazon FSx 會在修補操作期間暫時上線此磁碟區，並暫停 SnapMirror 關係。在此期間，資料可能會與來源磁碟區中的資料一起寫入 SnapMirror 目的地 SnapMirror 磁碟區。若要避免這種情況，請上線或刪除磁碟區。

若要讓離線磁碟區恢復上線，請使用 [volume online](#) ONTAP CLI 命令，如下列範例所示。如果只有一個 SVM (Vserver)，則不需要指定 `-vserver` 參數。

```
FsxID-abcdef123456:> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

## 您的受限磁碟區包含 iSCSI LUN 或 NVMe/TCP 命名空間

您的檔案系統目前託管處於受限狀態的磁碟區，且該磁碟區包含 iSCSI LUN、NVMe/TCP 命名空間或兩者。我們建議您持續將磁碟區保持在線上。如果您在檔案系統下一個維護時段之前未上線此磁碟區，Amazon FSx 會在修補操作期間暫時上線此磁碟區。若要避免這種情況，請上線或刪除磁碟區。

若要讓離線磁碟區恢復上線，請使用 [volume online](#) ONTAP CLI 命令，如下列範例所示。如果只有一個 SVM (Vserver)，則不需要指定 `-vserver` 參數。

```
FsxID-abcdef123456:> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

## 您的限制磁碟區是 FlexCache 原始伺服器

您的檔案系統包含處於受限狀態的 FlexCache 原始磁碟區。我們建議您持續將磁碟區保持在線上。如果您在檔案系統下一個維護時段之前未上線此磁碟區，Amazon FSx 會在修補操作期間暫時上線此磁碟區。在此期間，資料可能會與快取磁碟區中的資料一起寫回 FlexCache 原始磁碟區。若要避免這種情況，請上線或刪除磁碟區。

若要讓離線磁碟區恢復上線，請使用 [volume online](#) ONTAP CLI 命令，如下列範例所示。如果只有一個 SVM (Vserver)，則不需要指定 `-vserver` 參數。

```
FsxID-abcdef123456:> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

## 您的受限磁碟區是 SnapMirror 關係的一部分

您的檔案系統目前託管處於受限狀態的磁碟區，且該磁碟區是 SnapMirror 來源或目的地。我們建議您持續將磁碟區保持在線上。如果您在檔案系統下一個維護時段之前未上線此磁碟區，Amazon FSx 會在修補操作期間暫時上線此磁碟區，並暫停 SnapMirror 關係。在此期間，資料可能會與來源磁碟區中的資料一起寫入 SnapMirror 目的地 SnapMirror 磁碟區。若要避免這種情況，請上線或刪除磁碟區。

若要讓離線磁碟區恢復上線，請使用 [volume online](#) ONTAP CLI 命令，如下列範例所示。如果只有一個 SVM (Vserver)，則不需要指定 `-vserver` 參數。

```
FsxID-abcdef123456:> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

# 您的磁碟區儲存容量不足

如果您磁碟區的空間不足，您可以使用此處顯示的程序來診斷和解決這種情況。

## 主題

- [判斷磁碟區儲存容量的使用方式](#)
- [增加磁碟區的儲存容量](#)
- [使用磁碟區自動調整大小](#)
- [檔案系統的主要儲存體已滿](#)
- [刪除快照](#)
- [增加磁碟區的檔案容量上限](#)

## 判斷磁碟區儲存容量的使用方式

您可以使用 `volume show-space` NetApp ONTAP CLI 命令，查看磁碟區的儲存容量使用情形。此資訊可協助您決定如何回收或節省磁碟區儲存容量。如需詳細資訊，請參閱[監控磁碟區的儲存容量（主控台）](#)。

## 增加磁碟區的儲存容量

您可以使用 Amazon FSx 主控台 AWS CLI 和 Amazon FSx API 來增加磁碟區的儲存容量。如需使用增加的容量更新磁碟區的詳細資訊，請參閱[更新磁碟區](#)。

或者，您可以使用 `volume modify` NetApp ONTAP CLI 命令來增加磁碟區的儲存容量。如需詳細資訊，請參閱[變更磁碟區的儲存容量（主控台）](#)。

## 使用磁碟區自動調整大小

您可以使用磁碟區自動調整大小，讓磁碟區在達到使用的空間閾值時，自動成長至指定的大小。您可以使用 `volume autosize` NetApp ONTAP CLI 命令，為 FSx for ONTAP 的預設磁碟區類型 FlexVol 磁碟區類型執行此操作。FSx 如需詳細資訊，請參閱[啟用自動調整大小](#)。

## 檔案系統的主要儲存體已滿

如果您的 FSx for ONTAP 檔案系統的主要儲存已滿，您無法將任何其他資料新增至檔案系統中的磁碟區，即使磁碟區顯示其有足夠的可用儲存容量。您可以在 Amazon FSx 主控台的檔案系統詳細資訊頁面上的監控與效能索引標籤中，檢視可用的主要儲存容量。如需詳細資訊，請參閱[監控 SSD 儲存體使用率](#)。

若要解決此問題，您可以增加檔案系統主要儲存層的大小。如需詳細資訊，請參閱[更新檔案系統 SSD 儲存體和 IOPS](#)。

## 刪除快照

您的磁碟區預設會使用預設快照政策來啟用快照。快照會存放在磁碟區根目錄的 `.snapshot` 目錄中。您可以透過下列方式管理與快照相關的磁碟區儲存容量：

- [手動刪除快照](#) – 透過手動刪除快照來回收儲存容量。
- [建立快照自動刪除政策](#) – 建立比預設快照政策更積極刪除快照的政策。
- [關閉自動快照](#) – 關閉自動快照以節省儲存容量。

當您刪除快照時，不會回收與您要刪除之快照大小相等的儲存量。您可以使用磁碟區快照運算可回收的 [-vserver CLI](#) ONTAP 命令，使用資料取代 `svm_name`、`vol_name` 和 `snapshot_name`，來查看刪除快照時可回收的儲存量。

```
fsid8970abc52::> volume snapshot compute-reclaimable -vserver svm_name -volume vol_name  
-snapshot snapshot_name  
A total of 667648 bytes can be reclaimed.
```

如需刪除快照和管理快照政策以節省儲存容量的詳細資訊，請參閱 [刪除快照](#)。

## 增加磁碟區的檔案容量上限

FSx for ONTAP 磁碟區在用盡可用節點或檔案指標的數量時，可能會耗盡檔案容量。根據預設，磁碟區上每 32KiB 磁碟區大小的可用節點數量為 1。如需詳細資訊，請參閱[磁碟區檔案容量](#)。

磁碟區中的索引數量會隨著磁碟區的儲存容量而增加，最高可達到 648 GiB 的閾值。根據預設，儲存容量為 648 GiB 或更多的磁碟區都有相同數量的 Inodes，即 21，251，126。若要檢視磁碟區的最大檔案容量，請參閱 [監控磁碟區的檔案容量](#)。

如果您建立大於 648 GiB 的磁碟區，並且想要擁有超過 21，251，126 個索引，則必須手動增加磁碟區上的檔案數量上限。如果您的磁碟區用完儲存容量，您可以檢查其最大檔案容量。如果接近其檔案容量，您可以手動增加。如需詳細資訊，請參閱[若要增加磁碟區上的檔案數量上限 \(ONTAP CLI\)](#)。

## 由於磁碟區容量不足，您的備份失敗

磁碟區的自動每日備份失敗，並顯示下列訊息：



Amazon FSx could not create a backup of your volume because the backup snapshot was deleted.

由於磁碟區上的可用儲存容量不足，因此自動每日備份會失敗。若要緩解此條件，您需要釋放磁碟區的儲存容量。您可以根據您的情況，使用下列一或多個選項來完成此操作：

- [增加磁碟區的儲存容量](#)
- [增加磁碟區的快照保留](#)
- [停用快照自動刪除](#)
- [請勿使用 ONTAP CLI 刪除備份快照](#)

## 故障診斷網路問題

如果您遇到網路問題，您可以使用此處顯示的程序來診斷問題。

### 您想要擷取封包追蹤

封包追蹤是透過 layer 驗證封包路徑到其目的地的程序。您可以使用下列 CLI NetApp ONTAP 命令控制封包追蹤程序：

- `network tcpdump start` – 開始封包追蹤
- `network tcpdump show` – 顯示目前正在執行的封包追蹤
- `network tcpdump stop` – 停止執行中的封包追蹤

這些命令可供在檔案系統上具有 `fsxadmin` 角色的使用者使用。

從檔案系統擷取封包追蹤

1. 若要在檔案系統的 NetApp ONTAP CLI 中 SSH，請遵循 Amazon FSx for NetApp ONTAP 使用者指南中 [使用 NetApp ONTAP CLI](#) 一節所述的步驟。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. 使用下列命令，在 ONTAP CLI 中輸入診斷權限層級。

```
::> set diag
```



當系統提示您繼續時，請輸入 y。

```
Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y
```

3. 識別檔案系統上您要儲存封包追蹤的位置。磁碟區必須上線，且必須掛載在具有有效連接路徑的命名空間中。使用下列命令來檢查符合這些條件的磁碟區：

```
::*> volume show -junction-path !- -fields junction-path
vserver volume    junction-path
-----
fsx      test_vol1 /test_vol1
fsx      test_vol2 /test_vol2
fsx      test_vol2 /test_vol3
```

4. 使用最低必要引數啟動追蹤。取代以下項目：

- 將 *node\_name* 取代為節點的名稱（例如，FsxId01234567890abcdef-01）。
- 將 *svm\_name* 取代為儲存虛擬機器的名稱（例如 fsx）。
- 將 *junction\_path\_name* 取代為磁碟區的名稱（例如 test-vol1）。

```
::*> debug network tcpdump start -node node_name -ipspace Default -pass-through "-i
e0e -w /clus/svm_name/junction_path_name"
Info: Started network trace on interface "e0e"
Warning: Snapshots should be disabled on the tcpdump destination volume while
packet traces are occurring. Use the
"volume modify -snapshot-policy none -vserver fsx -volume test_vol1" command to
disable Snapshots on the
tcpdump destination volume.
```

#### Important

封包追蹤只能在 e0e 介面和 Default IP 空間中擷取。在 FSx for ONTAP 中，所有網路流量都會使用 e0e 介面。

使用封包追蹤時，請記住下列事項：

- 啟動封包追蹤時，您必須包含要存放追蹤檔案的路徑，格式為：`/clus/svm_name/junction-path-name`
- 或者，提供封包追蹤的檔案名稱。如果未指定 `filter_name`，則會以 `node-name_port-name_yyyymmdd_hhmmss.trc` 格式自動產生
- 如果指定滾動追蹤，則 `filter_name` 的尾碼會加上數字，指出輪換序列中的位置。
- ONTAP CLI 也接受下列選用引-pass-through數：

```
-B, --buffer-size=<KiB>
-c <number_of_packets>
-C <file_size-mB>
-F <filter_expression_filename>
-G <rotate_seconds>
--time-stamp-precision {micro|nano}
-Q, --direction {in|out|inout}
-s, --snapshot-length=<bytes>
-U, --packet-buffered
-W <rotate_file_count>
<filter-expression>
```

- 如需篩選條件表達式的資訊，請參閱 [pcap-filter\(7\) man 頁面](#)。

## 5. 檢視進行中追蹤：

```
::*> debug network tcpdump show
Node                IPspace  Port      Filename
-----
FsxId123456789abcdef-01  Default  e0e       /clus/fsx/test_vol1/
FsxId123456789abcdef-01_e0e_20230605_181451.trc
```

## 6. 停止追蹤：

```
::*> debug network tcpdump stop -node FsxId123456789abcdef-01 -ipspace Default -
port e0e
Info: Stopped network trace on interface "e0e"
```

## 7. 返回管理員權限層級：

```
::*> set -priv admin
::>
```

## 8. 存取封包追蹤。

您的封包追蹤會存放在您使用 `debug network tcpdump start` 命令指定的磁碟區中，並且可以透過 NFS 匯出或與該磁碟區對應的 SMB 共用存取。

如需擷取封包追蹤的詳細資訊，請參閱 [《》中的如何使用 ONTAP 9.10+ 中的偵錯網路傾印](#)。NetApp Knowledge Base

# Amazon FSx for NetApp ONTAP 的文件歷史記錄

- API 版本：2018-03-01
- 文件最近更新時間：2025 年 6 月 9 日

下表說明 Amazon FSx NetApp ONTAP 使用者指南的重要變更。如需有關文件更新的通知，您可以訂閱 RSS 摘要。

| 變更                                                             | 描述                                                                                                                                               | 日期              |
|----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <a href="#">FSx for ONTAP 支援 Amazon Elastic VMware Service</a> | FSx for ONTAP 現在可以用作 Amazon EVS 的外部資料存放區。如需詳細資訊，請參閱 <a href="#">搭配使用 Amazon Elastic VMware Service 與 FSx for ONTAP</a> 。                         | 2025 年 6 月 9 日  |
| <a href="#">已新增其他 AWS 區域 支援</a>                                | 適用於 ONTAP 檔案系統的第二代（多可用區域 2 和單一可用區域 2）FSx 現已在亞太區域（東京）和亞太區域（孟買）提供。如需詳細資訊，請參閱 <a href="#">可用性依據 AWS 區域</a> 。                                        | 2025 年 6 月 2 日  |
| <a href="#">針對回FlexCache寫模式新增的支援</a>                           | FSx for ONTAP 磁碟區現在支援回FlexCache寫模式。如需詳細資訊，請參閱 <a href="#">使用 複寫資料FlexCache</a> 。                                                                 | 2025 年 5 月 28 日 |
| <a href="#">Amazon FSx 已更新 AmazonFSxFullAccess AWS 受管政策</a>    | <a href="#">AmazonFSxFullAccess</a> 受管政策已更新，以新增 fsx:CreateAndAttachS3AccessPoint、fsx:DescribeS3AccessPointAttachments、fsx:UpdateS3AccessPointAtt | 2025 年 5 月 28 日 |

chments, 和 fsx:DetachAndDeleteS3AccessPoint 許可。

[Amazon FSx 已更新 AmazonFSxConsoleFullAccess AWS 受管政策](#)

[AmazonFSxConsoleFullAccess](#) 受管政策已更新, 以新增 fsx:CreateAndAttachS3AccessPoint 、 fsx:DescribeS3AccessPointAttachments fsx:UpdateS3AccessPointAttachments, 和 fsx:DetachAndDeleteS3AccessPoint 許可。

2025 年 5 月 28 日

[已新增其他 AWS 區域 支援](#)

FSx for ONTAP 檔案系統現可於亞太區域 ( 泰國 ) 和墨西哥 ( 中部 ) 使用。如需詳細資訊, 請參閱[可用性依據 AWS 區域](#)。

2025 年 5 月 8 日

[現在支援自治勒索軟體防護 \(ARP\)](#)

FSx for ONTAP 現在支援監控和防禦勒索軟體和惡意軟體攻擊的 NetApp AI 驅動功能 ARP。如需詳細資訊, 請參閱[使用自動勒索軟體防護來保護您的資料](#)

2025 年 4 月 7 日

[FSx for ONTAP 使用者指南中的新主題說明如何在工作群組中設定 SMB 伺服器](#)

[在工作群組中設定 SMB 伺服器](#)描述如何在 SVM 上設定工作群組中的 SMB 伺服器, 作為將 SVM 加入 Microsoft Active Directory 的替代方案。

2025 年 3 月 4 日

|                                                                        |                                                                                                                                                     |                 |
|------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <a href="#">Amazon FSx 已更新 AmazonFSxConsoleReadOnlyAccess AWS 受管政策</a> | Amazon FSx 已更新 AmazonFSxConsoleReadOnlyAccess 政策來新增 ec2:DescribeNetworkInterfaces 許可。如需詳細資訊，請參閱 <a href="#">AmazonFSx ConsoleReadOnlyAccess</a> 政策。 | 2025 年 2 月 25 日 |
| <a href="#">現在支援其他 Harvest 儀表板</a>                                     | FSx for ONTAP 現在支援其他 Harvest 儀表板，包括預設未啟用的儀表板。也新增了 FSx for ONTAP 不支援的儀表板清單。如需詳細資訊，請參閱 <a href="#">使用 Harvest 和 Grafana 監控 ONTAP 檔案系統的 FSx</a> 。      | 2025 年 2 月 18 日 |
| <a href="#">新的 FSx for ONTAP 帳單和用量報告主題已新增至 FSx for ONTAP 使用者指南</a>     | <a href="#">AWS FSx for ONTAP 的帳單和用量報告</a> 主題說明如何在 AWS 帳單與成本管理 主控台中存取 FSx for ONTAP 檔案系統的用量報告帳單。它還在兩個報告中提供 FSx for ONTAP 特有的所有用量類型。                 | 2025 年 2 月 13 日 |
| <a href="#">新增對 Amazon FSx 雙堆疊 VPC 介面端點的支援</a>                         | 您現在可以使用 IPv4 和 IPv6 IP 地址和 DNS 名稱為 Amazon FSx 建立雙堆疊 VPC 介面端點。如需詳細資訊，請參閱適用於 <a href="#">ONTAP 的 FSx 和界面 VPC 端點</a> 。                                 | 2025 年 2 月 7 日  |
| <a href="#">新增對雙堆疊 API 端點的支援</a>                                       | 用於建立和管理檔案系統的 Amazon FSx 服務 API 具有新的雙堆疊端點。如需詳細資訊，請參閱《Amazon FSx API 參考》中的 API <a href="#">端點</a> 。                                                   | 2025 年 2 月 7 日  |

|                                                                    |                                                                                                                                            |                  |
|--------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| <a href="#">Amazon FSx 已更新 AmazonFSxConsoleFullAccess AWS 受管政策</a> | Amazon FSx 已更新 AmazonFSxConsoleFullAccess 政策來新增 ec2:DescribeNetworkInterfaces 許可。如需詳細資訊，請參閱 <a href="#">AmazonFSxConsoleFullAccess</a> 政策。 | 2025 年 2 月 7 日   |
| <a href="#">發佈新主題，使用 複寫資料 FlexCache</a>                            | 已發佈新主題，說明如何使用 FlexCache 將內部部署 ONTAP 檔案系統中的資料複寫至 FSx for ONTAP 檔案系統。如需詳細資訊，請參閱 <a href="#">使用 FlexCache 複寫資料</a> 。                          | 2024 年 12 月 19 日 |
| <a href="#">新增對第二代檔案系統的支援</a>                                      | 您現在可以建立第二代單一可用區和多可用區檔案系統。單一高可用性 (HA) 對現在可提供高達 6 GBps 的輸送量容量和 200,000 個 SSD IOPS。如需詳細資訊，請參閱 <a href="#">高可用性 (HA) 對</a> 。                   | 2024 年 7 月 9 日   |
| <a href="#">新增支援從備份還原磁碟區讀取資料</a>                                   | 您現在可以掛載具有檔案資料的唯讀存取權的磁碟區，同時從第二代檔案系統的備份還原。如需詳細資訊，請參閱 <a href="#">將備份還原至新磁碟區</a> 。                                                            | 2024 年 7 月 9 日   |
| <a href="#">新增在第二代檔案系統上調整輸送量容量的支援</a>                              | 您現在可以在建立後調整第二代檔案系統的輸送量容量。如需詳細資訊，請參閱 <a href="#">管理輸送量容量</a> 。                                                                              | 2024 年 7 月 9 日   |

### [新增支援將 HA 對新增至第二代單一可用區檔案系統](#)

您現在可以在建立後將 HA 對新增至第二代單一可用區檔案系統。第二代單一可用區檔案系統總共可以有 12 個 HA 對。如需詳細資訊，請參閱[新增高可用性 \(HA\) 對](#)。

2024 年 7 月 9 日

### [新增支援透過 TCP \(NVMe/TCP\) 通訊協定的非揮發性 Memory Express](#)

您現在可以在 Amazon FSx for NetApp ONTAP 檔案系統上使用 NVMe/TCP 通訊協定進行資料傳輸。如需詳細資訊，請參閱[使用區塊儲存協定](#)

2024 年 7 月 9 日

### [新增檔案系統管理使用者 fsxadmin-readonly 角色的支援](#)

fsxadmin-readonly 角色現在可供 ONTAP 檔案系統管理使用者使用，可用於檔案系統監控應用程式，例如 NetApp Harvest。如需詳細資訊，請參閱[檔案系統管理員角色和使用者](#)。

2024 年 4 月 30 日

### [新增支援 Windows 網域管理使用者的 SSH 公有金鑰身分驗證](#)

您現在可以搭配 Active Directory 網域檔案系統和 SVM 使用者使用 SSH 公有金鑰身分驗證。如需詳細資訊，請參閱[設定 ONTAP 使用者的 Active Directory 身分驗證](#)。

2024 年 4 月 30 日



## [在橫向擴展檔案系統中新增 12 個 HA 對的支援](#)

Amazon FSx for NetApp ONTAP 新增了對橫向擴展檔案系統中 12 個 HA 對的支援。具有 12 個 HA 對的檔案系統可在 12 個高可用性 (HA) 對中提供高達 72 GBps 的輸送量和 2,400,000 SSD IOPS。如需詳細資訊，請參閱[高可用性 \(HA\) 對](#)和 [Amazon FSx for NetApp ONTAP 效能](#)。

2024 年 3 月 4 日

## [新增雲端寫入模式的支援](#)

Amazon FSx for NetApp ONTAP 新增對磁碟區的雲端寫入模式的支援。如需詳細資訊，請參閱[在磁碟區上啟用雲端寫入模式](#)。

2024 年 2 月 6 日

## [新增使用 備份 FlexGroup 磁碟區的支援 AWS Backup](#)

您現在可以使用 AWS Backup 在 FSx for ONTAP 檔案系統上備份和還原 FlexGroup 磁碟區。如需詳細資訊，請參閱[搭配使用 AWS Backup 與 Amazon FSx](#)。

2024 年 1 月 11 日

## [Amazon FSx 已更新 AmazonFSxFullAccess、AmazonFSxConsoleFullAccess、AmazonFSxReadOnlyAccess、AmazonFSxConsoleReadOnlyAccess 和 AmazonFSxServiceRolePolicy AWS 受管政策](#)

Amazon FSx 已更新 AmazonFSxFullAccess、AmazonFSxConsoleFullAccess、AmazonFSxReadOnlyAccess、AmazonFSxConsoleReadOnlyAccess 和 AmazonFSxServiceRolePolicy 政策以新增 ec2:GetSecurityGroupsForVpc 許可。如需詳細資訊，請參閱 [Amazon FSx AWS 受管政策的更新](#)。

2024 年 1 月 9 日

|                                                                                          |                                                                                                                                                                                               |                  |
|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| <a href="#">Amazon FSx 已更新 AmazonFSxFullAccess 和 AmazonFSxConsoleFullAccess AWS 受管政策</a> | Amazon FSx 已更新 AmazonFSxFullAccess 和 AmazonFSxConsoleFullAccess 政策來新增ManageCrossAccountDataReplication 動作。如需詳細資訊，請參閱 <a href="#">Amazon FSx AWS 受管政策的更新</a> 。                                 | 2023 年 12 月 20 日 |
| <a href="#">新增橫向擴展指標的支援</a>                                                              | FSx for ONTAP 現在為具有多個 HA 對的檔案系統提供 Amazon CloudWatch 指標。如需詳細資訊，請參閱 <a href="#">橫向擴展檔案系統指標</a> 。                                                                                                | 2023 年 11 月 26 日 |
| <a href="#">新增橫向擴展檔案系統的支援</a>                                                            | Amazon FSx for NetApp ONTAP 新增了對橫向擴展檔案系統的支援，可在六個高可用性 (HA) 對中提供高達 36 GBps 的輸送量容量和 1,200,000 SSD IOPS。如需詳細資訊，請參閱 <a href="#">高可用性 (HA) 對</a> 和 <a href="#">Amazon FSx for NetApp ONTAP 效能</a> 。 | 2023 年 11 月 26 日 |
| <a href="#">新增 FlexGroup 磁碟區的支援</a>                                                      | Amazon FSx for NetApp ONTAP 新增 FlexGroup 磁碟區的支援。如需詳細資訊，請參閱 <a href="#">磁碟區樣式</a> 。                                                                                                            | 2023 年 11 月 26 日 |

## [新增多可用區域檔案系統的共用 VPC 支援](#)

參與者帳戶現在可以在與其共用的 VPC 中建立多可用區域檔案系統。擁有者帳戶可以在 Amazon FSx 主控台、CLI 和 API 中管理此功能。如需詳細資訊，請參閱在[共用子網路中建立 FSx for ONTAP 檔案系統](#)

2023 年 11 月 26 日

## [Amazon FSx 已更新 AmazonFSxFullAccess 和 AmazonFSxConsoleFullAccess AWS 受管政策](#)

Amazon FSx 已更新 AmazonFSxFullAccess 和 AmazonFSxConsoleFullAccess 政策以新增 fsx:CopySnapshotAndUpdateVolume 許可。如需詳細資訊，請參閱 [Amazon FSx AWS 受管政策的更新](#)。

2023 年 11 月 26 日

## [Amazon FSx 已更新 AmazonFSxFullAccess 和 AmazonFSxConsoleFullAccess AWS 受管政策](#)

Amazon FSx 已更新 AmazonFSxFullAccess 和 AmazonFSxConsoleFullAccess 政策，以新增 fsx:DescribeSharedVPCConfiguration 和 fsx:UpdateSharedVPCConfiguration 許可。如需詳細資訊，請參閱 [Amazon FSx AWS 受管政策的更新](#)。

2023 年 11 月 14 日

## [新增建立其他 ONTAP 角色和使用者的支援](#)

Amazon FSx for NetApp ONTAP 現在支援建立其他 ONTAP 角色和使用者，以在使用 ONTAP CLI 和 REST API 時定義使用者功能和權限。如需詳細資訊，請參閱 [Amazon FSx for NetApp ONTAP 中的角色和使用者](#)。

2023 年 9 月 6 日

### [新增對其他 CloudWatch 指標和增強型監控儀表板的支援](#)

FSx for ONTAP 現在提供額外的效能指標和增強型監控儀表板，以提高檔案系統活動的可見性。如需詳細資訊，請參閱[使用 CloudWatch 監控](#)。

2023 年 8 月 17 日

### [Amazon FSx 已更新 AmazonFSxServiceRolePolicy AWS 受管政策](#)

Amazon FSx 已更新 AmazonFSxServiceRolePolicy 中的cloudwatch:PutMetricData 許可。如需詳細資訊，請參閱[Amazon FSx AWS 受管政策的更新](#)。

2023 年 7 月 24 日

### [新增直接使用 NetApp System Manager 的支援](#)

您可以System Manager直接從管理 FSx for ONTAP 檔案系統 NetApp BlueXP。如需詳細資訊，請參閱[搭配使用 NetApp System Manager 與 BlueXP](#)。

2023 年 7 月 13 日

### [新增監控 EMS 事件的支援](#)

您可以使用 NetAPP ONTAP 的原生 來監控 FSx 的 ONTAP 檔案系統事件Events Management System (EMS)。您可以使用 NetApp ONTAP CLI 檢視 EMS 事件。如需詳細資訊，請參閱[監控 FSx for ONTAP EMS 事件](#)。

2023 年 7 月 13 日

### [新增 的支援 SnapLock](#)

FSx for ONTAP 現在支援 SnapLock磁碟區。SnapLock 可讓您將檔案轉換為寫入、讀取許多 (WORM) 狀態，進而防止在指定的保留期間內修改或刪除檔案。FSx for ONTAP 支援 SnapLock 的合規和企業保留模式。如需詳細資訊，請參閱[使用 SnapLock](#)。

2023 年 7 月 13 日

### [新增對傳輸中資料的 IPsec 加密的支援](#)

FSx for ONTAP 現在支援使用 IPsec 加密來加密檔案系統和連線用戶端之間傳輸中的資料。如需詳細資訊，請參閱[使用 PSK 身分驗證設定 IPsec](#) 和[使用憑證身分驗證設定 IPsec](#)。

2023 年 7 月 13 日

### [磁碟區大小上限已增加](#)

FSx for ONTAP 將磁碟區的大小上限從 100 TB 更新為 300 TB。如需詳細資訊，請參閱[開啟磁碟區自動調整大小](#)。

2023 年 7 月 13 日

### [Amazon FSx 已更新 AmazonFSxFullAccess AWS 受管政策](#)

Amazon FSx 已更新 AmazonFSxFullAccess 政策，以移除 fsx:\* 許可並新增特定 fsx 動作。如需詳細資訊，請參閱 [AmazonFSxFullAccess](#) 政策。

2023 年 7 月 13 日

### [Amazon FSx 已更新 AmazonFSxConsoleFullAccess AWS 受管政策](#)

Amazon FSx 已更新 AmazonFSxConsoleFullAccess 政策，以移除 fsx:\* 許可並新增特定 fsx 動作。如需詳細資訊，請參閱 [AmazonFSxConsoleFullAccess](#) 政策。

2023 年 7 月 13 日

### [新增將現有儲存虛擬機器加入 Active Directory 的支援](#)

您可以使用 AWS CLI 和 API 將現有的儲存虛擬機器加入 Active Directory。如需詳細資訊，請參閱將 [SVM 加入 Active Directory](#)。

2023 年 6 月 13 日

### [針對單一可用區檔案系統新增的 NVMe 讀取快取支援](#)

NVMe 讀取快取現在支援 2022 年 11 月 28 日之後建立的單一可用區檔案系統，在美國東部（俄亥俄）區域、美國東部（維吉尼亞北部）區域、美國西部（奧勒岡）區域和歐洲（愛爾蘭）中具有至少 2 GBps 的輸送量。如需詳細資訊，請參閱[部署類型對效能的影響](#)。

2022 年 11 月 28 日

### [新增使用 VPC 內 IP 地址範圍建立多可用區域檔案系統的支援](#)

您現在可以透過指定 VPC IP 地址範圍內的端點，為 ONTAP 檔案系統建立異地同步備份 FSx。如需詳細資訊，請參閱[建立 FSx for ONTAP 檔案系統](#)。

2022 年 11 月 28 日

### [新增在多可用區域檔案系統上更新 VPC 路由表的支援](#)

您現在可以將新的 VPC 路由表與現有適用於 ONTAP 檔案系統的異地同步備份 FSx 建立關聯（新增），或從現有的適用於 ONTAP 檔案系統的異地同步備份 FSx 取消關聯（移除）現有 VPC 路由表。如需詳細資訊，請參閱[更新檔案系統](#)。

2022 年 11 月 28 日

### [新增支援使用 AWS Nitro System 加密傳輸中的資料](#)

從美國東部（俄亥俄）區域、美國東部（維吉尼亞北部）區域、美國西部（奧勒岡）區域和歐洲（愛爾蘭）支援的 Amazon EC2 執行個體存取時，傳輸中的資料會自動加密。如需詳細資訊，請參閱[使用 AWS Nitro System 加密傳輸中的資料](#)。

2022 年 11 月 28 日

### 新增建立 DP 磁碟區的支援

您現在可以使用 Amazon FSx 主控台 AWS CLI 或 Amazon FSx API 建立 DP（資料保護）磁碟區。當您想要遷移或保護單一磁碟區的資料時，您可以使用 DP 磁碟區做為 NetApp SnapMirror 或 SnapVault 關係的目的地。如需詳細資訊，請參閱[磁碟區類型](#)。

2022 年 11 月 28 日

### 新增將磁碟區標籤複製到備份的支援

您現在可以在 AWS CLI 或 Amazon FSx API CopyTagsToBackups 中啟用，以自動將標籤從磁碟區複製到備份。如需詳細資訊，請參閱[將標籤複製到備份](#)。

2022 年 11 月 28 日

### 新增選擇快照政策的支援

您現在可以在使用 Amazon FSx 主控台或 Amazon FSx API 建立或更新磁碟區時 AWS CLI，從三個內建快照政策中進行選擇。您也可以選取在 ONTAP CLI 或 REST API 中建立的自訂快照政策。如需詳細資訊，請參閱[快照政策](#)。

2022 年 11 月 28 日

### 新增對其他檔案系統輸送量容量選項的支援

FSx for ONTAP 現在支援 4,096 MBps 的輸送量容量，適用於 2022 年 11 月 28 日之後在美國東部（俄亥俄）區域、美國東部（維吉尼亞北部）區域、美國西部（奧勒岡）區域和歐洲（愛爾蘭）建立的檔案系統。如需詳細資訊，請參閱[輸送量容量對效能的影響](#)。

2022 年 11 月 28 日

### [新增對其他 SSD IOPS 的支援](#)

FSx for ONTAP 現在支援 160,000 SSD IOPS，適用於 2022 年 11 月 28 日之後在美國東部（俄亥俄）區域、美國東部（維吉尼亞北部）區域、美國西部（奧勒岡）區域和歐洲（愛爾蘭）建立的檔案系統。如需詳細資訊，請參閱[輸送量容量對效能的影響](#)。

2022 年 11 月 28 日

### [新增使用 FSx for ONTAP 做為 VMware Cloud on 外部資料存放區的支援 AWS](#)

您可以使用 FSx for ONTAP 作為 VMware Cloud on AWS Software-Defined Data Centers (SDDCs) 的外部資料存放區。這項新增的支援提供彈性，可獨立於 VMware Cloud on AWS 工作負載的運算資源來擴展或縮減儲存體。如需詳細資訊，請參閱[搭配使用 VMware Cloud 與 FSx for ONTAP](#)。

2022 年 8 月 30 日

### [自動增加檔案系統的儲存容量](#)

當使用過的 SSD 儲存容量超過您指定的閾值時，使用 AWS 開發的可自訂 AWS CloudFormation 範本自動增加檔案系統的儲存容量。如需詳細資訊，請參閱[動態增加 SSD 儲存容量](#)。

2022 年 6 月 3 日

### [Amazon FSx 現在已與 整合 AWS Backup](#)

除了使用原生 Amazon FSx 備份之外，您現在可以使用 AWS Backup 備份和還原 FSx 檔案系統。如需詳細資訊，請參閱[搭配使用 AWS Backup 與 Amazon FSx](#)。

2022 年 5 月 18 日



### [新增單一可用區域 ONTAP 檔案系統部署的支援](#)

您可以為 ONTAP 檔案系統建立單一可用區域 FSx，其設計旨在提供單一可用區域 (AZ) 內的高可用性和耐用性。如需詳細資訊，請參閱[選擇檔案系統部署](#)。

2022 年 4 月 13 日

### [新增 AWS PrivateLink 介面 VPC 端點的支援](#)

您現在可以使用介面 VPC 端點從 VPC 存取 Amazon FSx API，而無需透過網際網路傳送流量。如需詳細資訊，請參閱[Amazon FSx 和介面 VPC 端點](#)。

2022 年 4 月 5 日

### [新增修改現有 ONTAP 檔案系統輸送量容量的支援](#)

您現在可以修改現有 ONTAP 檔案系統可用的輸送量容量。如需詳細資訊，請參閱[管理輸送量容量](#)。

2022 年 3 月 30 日

### [新增對 SSD 儲存容量和佈建 IOPS 擴展的支援](#)

您現在可以隨著儲存和 IOPS 需求的變化，增加現有 FSx for ONTAP 檔案系統的 SSD 儲存容量和佈建 IOPS。如需詳細資訊，請參閱[管理儲存容量和佈建 IOPS](#)。

2022 年 1 月 25 日

### [新增對 Amazon CloudWatch 指標的支援](#)

您可以使用 Amazon CloudWatch 監控您的檔案系統，它會從 FSx for ONTAP 收集原始資料，並將其處理為可讀且近乎即時的指標。如需詳細資訊，請參閱[使用 Amazon CloudWatch 進行監控](#)。

2022 年 1 月 19 日

### [新增對其他檔案系統輸送量選項的支援](#)

FSx for ONTAP 現在支援 128 MBps 和 256 MBps 的檔案系統輸送量選項。如需詳細資訊，請參閱[輸送量容量對效能的影響](#)。

2021 年 11 月 30 日

### [Amazon FSx for NetApp ONTAP 現已正式推出](#)

FSx for ONTAP 是一項全受管服務，可在 NetApp 的 ONTAP 檔案系統上提供高度可靠、可擴展、高效能且功能豐富的檔案儲存。它提供 NetApp 檔案系統的熟悉功能、效能、功能和 APIs，以及全受管 AWS 服務的靈活性、可擴展性和簡單性。

2021 年 9 月 2 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。