aws

使用者指南

FSx for OnTAP

FSx for OnTAP: 使用者指南

Table of Contents

什麼是適用於 NetApp ONTAP 的 Amazon FSx？

Amazon FSx for NetApp ONTAP 是一種全受管服務，提供以熱門 ONTAP 檔案系統為基礎的高度可靠、可擴展、高效能和功能豐富 NetApp的檔案儲存。FSx for ONTAP 結合了 NetApp 檔案系統熟悉的功能、效能、功能和 API 作業，以及完全受控的靈活性、可擴充性和簡易性。 AWS 服務

適用於 ONTAP 的 FSx 提供功能豐富、快速且彈性的共用檔案儲存空間，可從內部部署或內部部署執行的 Linux、Windows 和 macOS 運算執行個體進行廣泛存取。 AWS 適用於 ONTAP 的 FSx 提供低於一毫秒延遲的高效能固態硬碟 (SSD) 儲存裝置。使用 FSx for ONTAP，您可以為工作負載達到 SSD 等級的效能，同時只需支付一小部分資料的 SSD 儲存費用。

使用 FSx for ONTAP 管理資料會比較容易，因為只要按一下按鈕，就能快照、複製和複製檔案。此外，FSx for ONTAP 會自動將您的資料分層到成本較低的彈性儲存，從而減少佈建或管理容量的需求。

FSx for ONTAP 也提供高可用性與耐用性的儲存裝置，並提供完全受控的備份功能，並支援跨區域災難復原。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性和防毒應用程式。

對於內部部署 ONTAP 使用 NetApp ONTAP 的客戶而言，FSx for ONTAP 是一個理想的解決方案，可讓您從內部部署移轉、備份或成組分解檔案型應用程式， AWS 而無需變更應用程式程式碼或管理資料的方式。

FSx for ONTAP 是一項完全受控的服務，可讓您更輕鬆地在雲端中啟動和擴充可靠、高效能且安全的共用檔案儲存空間。使用適用於 ONTAP 的 FSx，您不再需要擔心：

- 設定和佈建檔案伺服器和儲存磁碟區
- 複製資料
- 安裝和修補檔案伺服器軟體
- 偵測並解決硬體故障
- 管理容錯移轉和容錯回復
- 手動執行備份

適用於 ONTAP 的 FSx 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

適用於 ONTAP 的 FSx 功能

使用 FSx for ONTAP，您可以獲得具有下列功能的完全受控檔案儲存解決方案：

- Support 單一命名空間中的 PB 級資料集
- 每個檔案系統每秒最高可達數十 GB 的輸送量
- 使用網路檔案系統 (NFS)、伺服器訊息區 (SMB) 及網際網路小型電腦系統介面 (iSCSI) 通訊協定，進行多重通訊協定存取資料
- 高可用性和耐用的異地同步備份和單一同步備份部署
- 自動資料分層功能，根據您的存取模式，自動將不常存取的資料轉換至成本較低的儲存層，藉此降低儲存成本
- 資料壓縮、重複資料刪除和壓縮功能，可減少儲存耗用量
- Support NetApp 的 SnapMirror 複製功能
- Support NetApp 的內部部署快取解決方案： NetApp 全域檔案快取和 FlexCache
- Support 使用原生 AWS 或 NetApp 工具以及 API 作業的存取和管理
  - AWS Management Console、 AWS Command Line Interface (AWS CLI) 和軟體開發套件
  - NetApp 開啟 CLI、休息 API 和藍運算式
- Support 下列資料保護與安全性功能：
  - 使用加密文件系統數據和靜態備份 AWS KMS keys
  - 使用中小企業 Kerberos 工作階段金鑰加密傳輸中的資料
  - 按需防毒掃描
  - 使用 Microsoft 活動目錄驗證和授權
  - 檔案存取稽核
  - NetAppSnapLockWORM 功能，支援合規性和企業磁碟區

安全性與資料保護

Amazon FSx 提供多層級的安全性和合規性，以協助保護您的資料。它會使用您在 AWS Key Management Service (AWS KMS) 中管理的金鑰自動加密檔案系統和備份中的靜態資料。您也可以使用適用於 NFS 和 SMB 用戶端的 Kerberos 來加密傳輸中的資料。

Amazon FSx 已經過評估符合下列標準：

- 國際標準組織
- 支付卡產業資料安全標準 (PCI DSS)
- 系統與組織控制 (SOC) 認證
- 1996 年的《Health 保險可攜性與責任法案》

如需詳細資訊，請參閱 適 NetApp 用於 ONTAP 的 Amazon FSx 中的資料保護。

Amazon FSx 也提供下列層級的存取控制：

- 在檔案系統層級，Amazon FSx 透過使用 Amazon 虛擬私有雲端 (Amazon VPC) 安全群組提供存取控制。
- 在 API 層級，Amazon FSx 透過使用 AWS Identity and Access Management (IAM) 存取政策提供存取控制。
- 為了在檔案和資料夾層級提供存取控制，Amazon FSx 支援 Unix 許可、NFS 存取控制清單 (ACL) 和 NTFS ACL。當您將 Amazon FSx 加入作用中目錄時，存取檔案系統的使用者可以使用其使用中目錄登入資料進行驗證。

為了讓您可以查看使用者在 Amazon FSx 資源上採取的動作，Amazon FSx 與之整合 AWS CloudTrail 以監控和記錄您的 Amazon FSx API 呼叫。如需詳細資訊，請參閱 使用 FSx 誌記錄用於 ONTAP API 調用AWS CloudTrail。

此外，Amazon FSx 透過高耐用性的檔案系統備份來保護您的資料。Amazon FSx 會執行每日自動備份，而且您可以隨時進行額外備份。如需詳細資訊，請參閱 保護您的資料。

開發管理系統的 FSx 訂價

我們會根據下列類別向您收取檔案系統費用：

- 固態硬碟儲存容量 (每 GB 每月或 GB-月)

- 您佈建的固態硬碟 IOPS 以上三個 IOPS/GB (每個 IOPS)
- 輸送量容量 (每秒百萬位元組 [MBps]-月)
- 容量集區儲存體耗用量 (每 GB-月)
- 容量集區要求 (每次讀取和寫入)
- Backup 儲存體耗用量 (每 GB-月)

如需有關服務相關定價和費用的詳細資訊，請參閱 Amazon FSx 瞭解 NetApp ONTAP 定價。

安裝管理論壇的 FSx

如果您在使用 Amazon FSx 時遇到問題，請使用 FSx 進行 ONTAP 討論區來取得解答。

您是第一次使用 Amazon FSx 嗎？

如果您是 Amazon FSx 的首次使用者，建議您依序閱讀下列各節：

1. 如果您不熟悉 AWS，請參閱為 ONTAP 設定 FSx若要設定 AWS 帳戶.
2. 如果您已準備好建立第一個 Amazon FSx 檔案系統，請依照中開始使用適 NetApp 用於 ONTAP 的 Amazon FSx的指示進行。
3. 如需有關效能的詳細資訊，請參閱適用於 NetApp ONTAP 性能的 Amazon FSx。
4. 如需 Amazon FSx 安全性詳細資訊，請參閱適 NetApp 用於 ONTAP 的 Amazon FSx 中的安全性。
5. 如需有關 Amazon FSx API 的資訊，請參閱 Amazon FSx 應用程式介面參考。

適用於 NetApp ONTAP 的 Amazon FSx 如何運作

本主題介紹適用於 NetApp ONTAP 檔案系統的 Amazon FSx 主要功能及其運作方式，並提供詳細說明、重要實作詳細資訊和 step-by-step 組態程序各節的連結。

主題

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 ONTAP 叢集。 NetApp 您可以為檔案系統指定固態硬碟 (SSD) 儲存容量和輸送量容量，然後選擇建立檔案系統的 Amazon 虛擬私有雲 (VPC)。如需詳細資訊，請參閱 管理 ONTAP 檔案系統的 FSx。

您的檔案系統可以有一到 12 個高可用性 (HA) 配對，視其組態而定。HA 配對由作用中-待命組態中的兩個檔案伺服器組成。具有單一 HA 配對的檔案系統稱為向上擴充檔案系統。具有多個 HA 配對的檔案系統稱為向外延展檔案系統。如需詳細資訊，請參閱 高可用性 (HA) 配對。

儲存虛擬機器

儲存區虛擬機器 (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 位址與 SVM 進行介面。如需詳細資訊，請參閱 管理 SVM。

您可以將 SVM 加入 Microsoft 活動目錄以進行文件訪問身份驗證和授權。如需詳細資訊，請參閱 使用 FSx 中的 Microsoft 活動目錄進行 ONTAP。

磁碟區

適用於 ONTAP 磁碟區的 FSx 是用於組織和分組資料的虛擬資源。磁碟區是儲存在 SVM 上的邏輯容器，儲存在其中的資料會耗用檔案系統上的實體儲存容量。

建立磁碟區時，您可以設定其大小，這會決定您可以在其中儲存的實體資料量，而不論資料儲存在哪個儲存層。您也可以設定磁碟區類型，RW (可讀寫) 或 DP (資料保護)。DP 磁碟區是唯讀的，可用作 NetApp SnapMirror 或 SnapVault 關係中的目的地。

適用於 ONTAP 磁碟區的 FSx 是精簡佈建的，這表示它們只會耗用儲存容量來儲存在其中的資料。使用精簡佈建磁碟區時，不會預先保留儲存容量。相反，存儲是根據需要動態分配的。刪除磁碟區或 LUN 中的資料時，可用空間會釋放回檔案系統。例如，您可以在配置 10 TiB 可用儲存容量的檔案系統上建立三個 10 TiB 磁碟區，只要儲存在三個磁碟區中的資料總量不超過 10 TiB 即可。實際儲存在磁碟區上的資料量會計入您的整體儲存容量使用量。如需詳細資訊，請參閱 管理安裝磁碟區的 FSx。

儲存層

ONTAP 檔案系統的 FSx 有兩個儲存層：主要儲存和容量集區儲存。主要儲存裝置是佈建、可擴充的高效能 SSD 儲存裝置，專為資料集的使用中部分而打造。容量集區儲存是完全彈性的儲存層，可擴充至 PB 級，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耗用儲存層的容量。如需詳細資訊，請參閱 適用於 ONTAP 儲存層的 FSx。

資料分層

資料分層是指 Amazon FSx for NetApp ONTAP 自動在 SSD 和容量集區儲存層之間移動資料的程序。每個磁碟區都有一個分層政策，用於控制當資料變為非作用中 (冷) 時，是否將資料移至容量層。磁碟區的分層原則冷卻期決定資料變為非作用中 (冷) 的時間。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、壓縮和刪除重複)，以減少資料消耗的儲存容量。儲存效率功能可減少 SSD 儲存、容量集區儲存空間和備份中的資料佔用空間。在不犧牲效能的情況下，一般用途的檔案共用工作負載可節省 65% 的儲存容量，是 SSD 和容量集區儲存層的壓縮、重複資料刪除和壓縮。如需詳細資訊，請參閱 提供 ONTAP 儲存效率的 FSx。

針對 ONTAP 檔案系統存取儲存在 FSx 上的資料

您可以透過 NFS (v3、v4、4.1 版、第 4.2 版) 和中小企業通訊協定，同時從多個 Linux、視窗或 macOS 用戶端存取 FSx 上的資料。您也可以使用 iSCSI (區塊) 通訊協定存取資料。如需詳細資訊，請參閱 存取 資料。

管理安排資源的 FSx

您可以透過數種方式與您的 FSx 進行 ONTAP 檔案系統互動，並管理其資源。您可以使用 AWS 和 ONTAP 管理工具來管理您的 FSx 的 NetApp ONTAP 資源：

- AWS 管理工具
  - 該 AWS Management Console
  - 該 AWS Command Line Interface （ AWS CLI ）
  - Amazon FSx API 和開發套件
  - AWS CloudFormation
- NetApp 管理工具：
  - NetApp 藍運算
  - NetApp ONTAP CLI
  - 在 NetApp ONTAP 休息 API

如需更多詳細資訊，請參閱 管理資源。

為 ONTAP 設定 FSx

第一次使用 Amazon FSx 之前，請先完成下列任務：

1. 註冊一個 AWS 帳戶
2. 建立具有管理權限的使用者

主題

註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

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

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   當您註冊一個時 AWS 帳戶，將創建AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。安全性最佳做法是將管理存取權指派給使用者，並僅使用 root 使用者來執行需要 root 使用者存取權的工作。

AWS 註冊過程完成後，會向您發送確認電子郵件。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。

建立具有管理權限的使用者

註冊後，請保護您的 AWS 帳戶 AWS 帳戶根使用者 AWS IAM Identity Center、啟用和建立系統管理使用者，這樣您就不會將 root 使用者用於日常工作。

保護您的 AWS 帳戶根使用者

1. 選擇 Root 使用者並輸入您的 AWS 帳戶 電子郵件地址，以帳戶擁有者身分登入。AWS Management Console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)。

   如需指示，請參閱《IAM 使用者指南》中的為 AWS 帳戶 根使用者啟用虛擬 MFA 裝置 (主控台)。

建立具有管理權限的使用者

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 身分中心中，將管理存取權授予使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的自學課程，請參閱《使用指南》IAM Identity Center 目錄中的「以預設值設定使用AWS IAM Identity Center 者存取」。

以具有管理權限的使用者身分登入

- 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 身分中心使用者登入的說明，請參閱使用AWS 登入 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

1. 在 IAM 身分中心中，建立遵循套用最低權限許可的最佳做法的權限集。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「建立權限集」。

2. 將使用者指派給群組，然後將單一登入存取權指派給群組。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「新增群組」。

下一步驟

若要開始使用 FSx 進行 ONTAP，請參閱開始使用適 NetApp 用於 ONTAP 的 Amazon FSx如需建立 Amazon FSx 資源的說明。

開始使用適 NetApp 用於 ONTAP 的 Amazon FSx

了解如何開始在 NetApp ONTAP 上使用 Amazon FSx。此入門練習包括以下步驟。

主題

步驟 1：為 NetApp ONTAP 檔案系統建立 Amazon FSx

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適用於 NetApp ONTAP 檔案系統的 Amazon FSx，請使用快速建立選項。

[快速建立] 選項可建立具有單一高可用性組 (HA)、單一儲存區虛擬機器 (SVM) 和單一磁碟區的檔案系統。「快速建立」選項可將此檔案系統設定為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，您可以視需要建立額外的 SVM 和磁碟區，包括加入作用中目錄的 SVM，以允許透過伺服器訊息區 (SMB) 通訊協定從 Windows 和 macOS 用戶端存取。

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，請參閱為 ONTAP 檔案系統建立 FSx。

建立 檔案系統

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 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，針對 NetApp ONTAP 選擇 Amazon FSx，然後選擇 [下一步]。便會顯示「建立 ONTAP 檔案系統」頁面。
4. 針對「建立方式」，選擇「快速建立」
5. 在「快速組態」區段中，對於檔案系統名稱-選用，請輸入檔案系統的名稱。當您命名檔案系統時，尋找和管理檔案系統會比較容易。您最多可以使用 256 個 Unicode 字母、空格和數字，再加上下列特殊字元：+ - (連字號) =。 _ (下劃線) ：/
6. 對於部署類型，請選擇異地同步備份或單一可用

    - 異地同步備份檔案系統會複寫您的資料，同 AWS 區域時支援跨多個可用區域的容錯移轉。
    - 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 可用性與持久性。

7. 對於 SSD 儲存容量，請指定檔案系統的儲存容量 (以 GiB) 為單位。請輸入介於範圍內的任何整數。如果您需要更多 SSD 儲存容量，可以使用標準建立。如需詳細資訊，請參閱 若要建立檔案系統 (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 4,096 MBps)。如果您需要更多輸送量容量，可以使用標準建立。

9. 對於 V irtual Private Cloud (VPC) (VPC)，請選擇您要與檔案系統建立關聯的 Amazon VPC。

10. 若要取得儲存效率，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] 將其關閉。

11. (僅限異地同步備份) 端點 IP 位址範圍會指定建立用於存取檔案系統之端點的 IP 位址範圍。

    選擇端點 IP 位址範圍的快速建立選項：

    - 來自虛擬私人雲端的未配置 IP 位址範圍 — 選擇此選項可讓 Amazon FSx 使用 VPC 主要 CIDR 範圍中的最後 64 個 IP 位址作為檔案系統的端點 IP 位址範圍。請注意，如果您多次選擇此選項，此範圍會在多個檔案系統之間共用。

      > **Note**
      >
      > - 您建立的每個檔案系統會使用此範圍內的兩個 IP 位址，一個用於叢集，另一個用於第一個 SVM。第一個和最後一個 IP 位址也會保留。對於每個額外的 SVM，檔案系統就會耗用另一個 IP 位址。例如，裝載 10 個 SVM 的檔案系統會使用 11 個 IP 位址。其他檔案系統以相同的方式運作。它們會使用兩個初始 IP 位址，再加上每個額外的 SVM 一個。使用相同 IP 位址範圍 (每個具有單一 SVM) 的檔案系統數目上限為 31。
      > - 如果子網路正在使用 VPC 主要 CIDR 範圍中任何一個最後 64 個 IP 位址，則此選項會呈現灰色。

    - 虛擬私人雲端以外的浮動 IP 位址範圍 — 選擇此選項可讓 Amazon FSx 使用 198.19.x.0/24 位址範圍，這個位址範圍尚未被具有相同 VPC 和路由表的任何其他檔案系統使用。

    您也可以在 [標準建立] 選項中指定自己的 IP 位址範圍。

12. 選擇下一步，然後檢閱 [建立 ONTAP 檔案系統] 頁面上的檔案系統組態。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)。

快速建立會建立具有一個 SVM (已命名fsx) 和一個磁碟區 (已命名vol1) 的檔案系統。磁碟區的結合路徑/vol1和容量集區分層原則為 Auto (會自動將 31 天未存取的任何資料分層至成本較低的容量集區儲存體)。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的服務管理 AWS KMS 金鑰在靜態時加密。

步驟 2：從 Amazon EC2 Linux 執行個體掛載檔案系統

您可以從亞馬遜彈性運算雲端 (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。

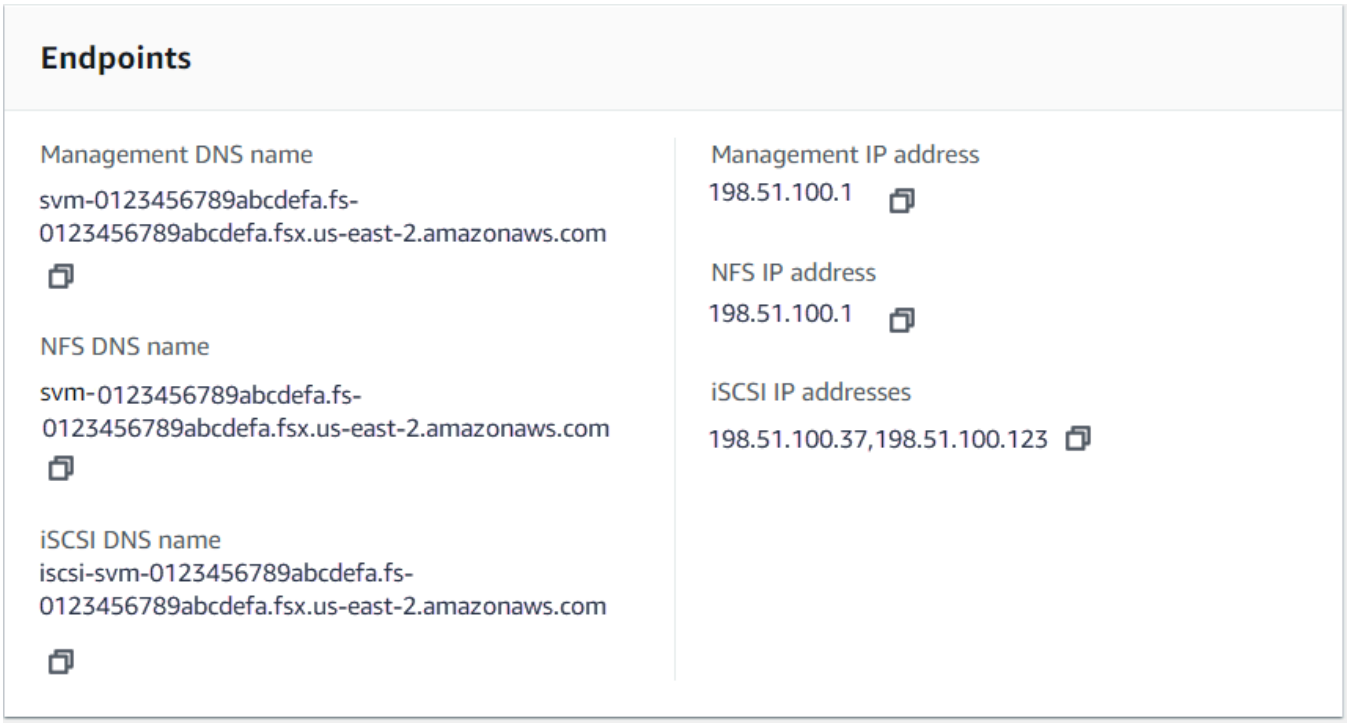
從 Amazon EC2 掛載您的檔案系統

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，該執行個體與您的檔案系統位於相同的虛擬私有雲端 (VPC) 中。如需有關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. Connect 到您的 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 Connect 到 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，然後使用適當的登入資料登入。
5. 使用下列命令，在 Amazon EC2 執行個體上建立一個目錄，做為磁碟區的掛接點。在下列範例中，使用您自己的資訊取代*###*。

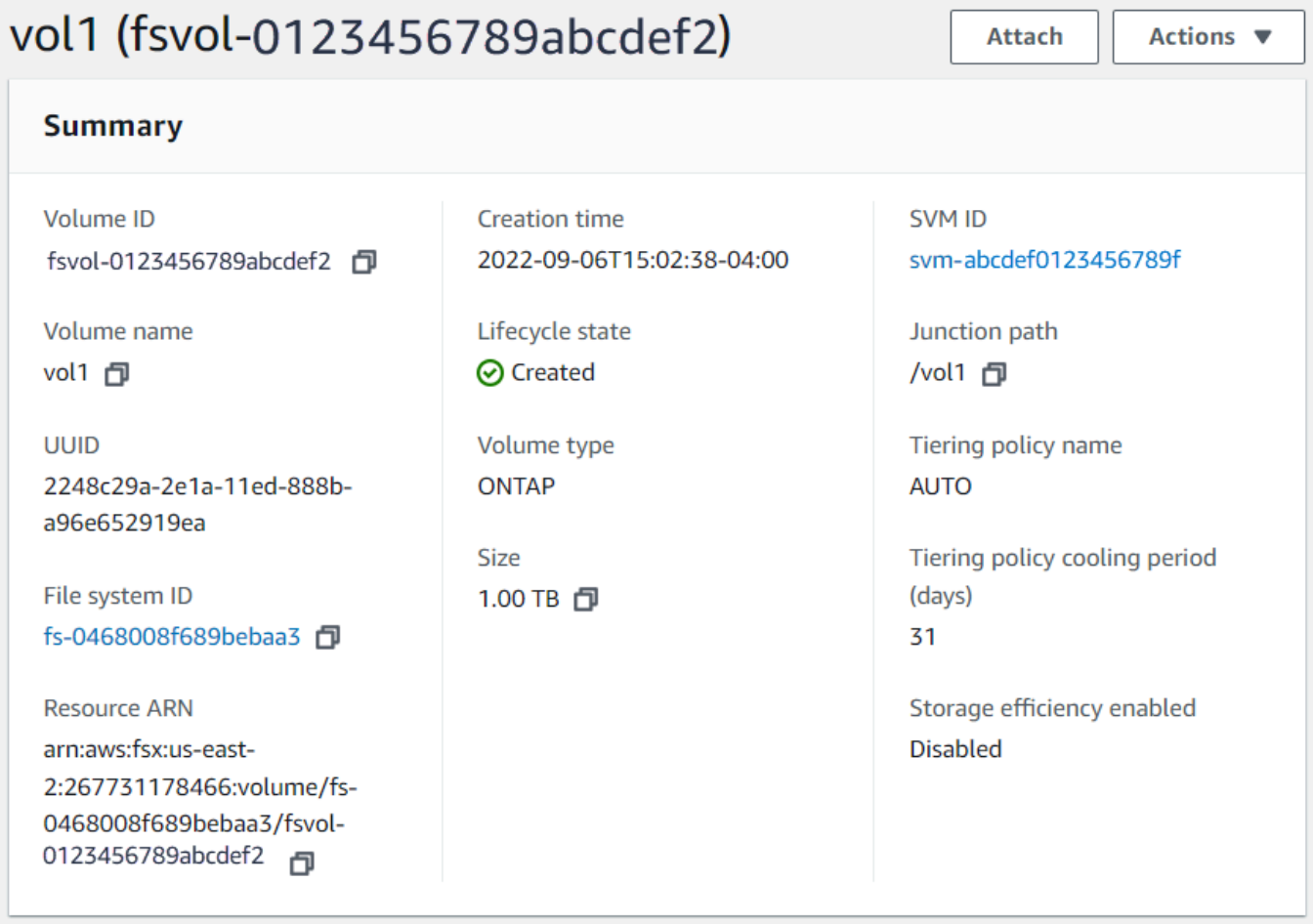
   ```
   $ sudo mkdir /mount-point
   ```

6. 將適用於 NetApp ONTAP 檔案系統的 Amazon FSx 掛載到您建立的目錄。使用類似於以下範例的mount指令。在下列範例中，以您自己的資訊取代下列預留位置值。

   - *nfs_version*— 您使用的 NFS 版本；適用於 ONTAP 的 FSx 支援版本 3、4.0、4.1 和 4.2 版本。
   - *nfs-dns-name*— 存在您要掛接之磁碟區之儲存區虛擬機器 (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，然後選擇要掛接的磁碟區所在的 SVM。您可以在「端點」面板上找到 NFS DNS 名稱，如下圖所示。



- *volume-junction-path*— 您要安裝的磁碟區的結合路徑。您可以在 Amazon FSx 主控台中 [磁碟區詳細資料] 頁面的 [摘要] 面板中找到磁碟區的結合路徑，如下圖所示。



- *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 EC2 執行個體疑難排解。

步驟 3：清除資源

完成這個練習之後，您應該依照下列步驟清理您的資源並保護您的 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執行個體。
2. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
3. 在 Amazon FSx 主控台上，刪除非 SVM 根磁碟區之 ONTAP 磁碟區的所有 FSx。如需詳細資訊，請參閱 刪除磁碟區。
4. 刪除所有適用於 ONTAP SVM 的 FSx。如需詳細資訊，請參閱 刪除儲存區虛擬機器 (SVM)。
5. 在 Amazon FSx 主控台上，刪除您的檔案系統。刪除檔案系統時，會自動刪除所有自動備份。但是，您仍然必須刪除任何手動創建的備份。以下步驟概述了此過程。

   a. 從主控台儀表板中，選擇您為本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. Amazon FSx 刪除檔案系統時，儀表板中的狀態會變更為「刪除」。刪除檔案系統後，該檔案系統將不再出現在儀表板中。任何自動備份都會隨檔案系統一起刪除。
   f. 現在，您可以刪除任何手動為文件系統創建的備份。在左側導覽中，選擇「備份」。
   g. 從儀表板中，選擇與您刪除的檔案系統具有相同檔案系統 ID 的任何備份，然後選擇 [刪除備份]。如果您已建立備份，請務必保留最終備份。
   h. 刪除備份」對話方塊隨即開啟。保持選取要刪除之備份 ID 的核取方塊，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都會一併刪除，以及您選擇刪除的任何手動備份。

存取 資料

您可以在現場部署環境中使用各種支援的用戶端和方法存取 AWS 雲端 Amazon FSx 檔案系統。

每個 SVM 都有四個端點，可用來存取資料或使用 NetApp ONTAP CLI 或 REST API 來管理 SVM：

- `Nfs`— 用於使用網路檔案系統 (NFS) 通訊協定進行連線
- `Smb`— 用於使用服務訊息區 (SMB) 通訊協定進行連線 (如果您的 SVM 已加入 Active Directory，或您正在使用工作群組。)
- `Iscsi`— 用於使用網際網路小型電腦系統介面 (iSCSI) 通訊協定進行連線 (僅適用於向上擴充的檔案系統)。
- `Management`— 用於使用 NetApp ONTAP CLI 或 API 或藍運算式管理 SVM NetApp

主題

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。它透過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 (SMB) 通訊協定 (包括 2.0、3.0 和 3.1.1) 的存取，以及網際網路小型電腦系統介面 (iSCSI) 通訊協定來達成此目的。

> **Important**
>
> Amazon FSx 不支援從公用網際網路存取檔案系統。Amazon FSx 會自動分離任何可從網際網路存取的公有 IP 位址 (連接至檔案系統的彈性網路界面) 的彈性 IP 位址。

下列 AWS 運算執行個體可與 ONTAP 的 FSx 搭配使用：

- Amazon Elastic Compute Cloud (Amazon EC2) 執行 Linux 執行個體，並支援 NFS 或中小企業、Microsoft 視窗和 MacOS。如需詳細資訊，請參閱 掛載磁碟區。
- Amazon Elastic Container Service (Amazon ECS) 碼頭集裝箱在 Amazon EC2 視窗和 Linux 實例。如需詳細資訊，請參閱 搭配 FSx 搭配 ONTAP 使用 Amazon 彈性容器服務。
- Amazon Elastic Kubernetes Service — 若要進一步了解，請參閱 Amazon EKS 使用者指南中的適用於 NetApp ONTAP CSI 驅動程式的 Amazon FSx。
- 紅帽 OpenShift 服務 AWS (ROSA) — 若要瞭解更多資訊，請參閱什麼是 Red Hat OpenShift 服務 AWS？ 在 AWS 使用者指南中的 Red Hat OpenShift 服務中。
- Amazon WorkSpaces 實例。如需詳細資訊，請參閱 將 Amazon WorkSpaces 與 FSx 一起使用 ONTAP。
- Amazon AppStream 2.0 實例。
- AWS Lambda — 如需詳細資訊，請參閱 AWS 部落格文章啟用 Amazon FSx 的無伺服器工作負載中小企業存取。
- 在 VMware 雲端 AWS 環境中執行的虛擬機器 (VM)。如需詳細資訊，請參閱將適用於 NetApp ONTAP 的 Amazon FSX 設定為外部儲存裝置和 VMware 雲端 AWS 與 Amazon FSX (適用於 NetApp ON TAP) 部署指南。

掛載完成後，ONTAP 檔案系統的 FSx 會顯示為 NFS 和 SMB 上的本機目錄或磁碟機代號，提供完全受控的共用網路檔案儲存，最多可供數千個用戶端同時存取。iSCSI LUN 可當作區塊裝置存取。

從內部存取資料 AWS

每個 Amazon FSx 檔案系統都與 Virtual Private Cloud (VPC) (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 VPC 存取您的檔案系統，這些 VPC 可以位於不同 AWS 帳戶或 AWS 區域. 除了下列章節中描述的存取 FSx for ONTAP 資源的需求之外，您還需要確保已設定檔案系統的 VPC 安全性群組，以便資料和管理流量可以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。

主題

- 從相同 VPC 中存取資料
- 從部署 VPC 外部存取資料

從相同 VPC 中存取資料

當您建立適用於 NetApp ONTAP 檔案系統的 Amazon FSx 時，請選取該系統所在的 Amazon VPC。與適用於 NetApp ONTAP 檔案系統的 Amazon FSx 相關聯的所有 SVM 和磁碟區也位於相同的 VPC 中。掛接磁碟區時，如果掛載磁碟區的檔案系統和用戶端位於相同的 VPC 中 AWS 帳戶，並且您可以使用 SVM 的 DNS 名稱和磁碟區結合或 SMB 共用 (視用戶端而定)。如需詳細資訊，請參閱 掛載磁碟區。

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中，或異地同步備份檔案系統的偏好子網路，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，然後選擇要掛接其磁碟區的 ONTAP 檔案系統，子網路或偏好的子網路 (異地同步備份) 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 以外的 AWS 位置存取 ONTAP 檔案系統端點的 FSx。

存取異地同步備份檔案系統上的 NFS、SMB 和 ONTAP 管理端點

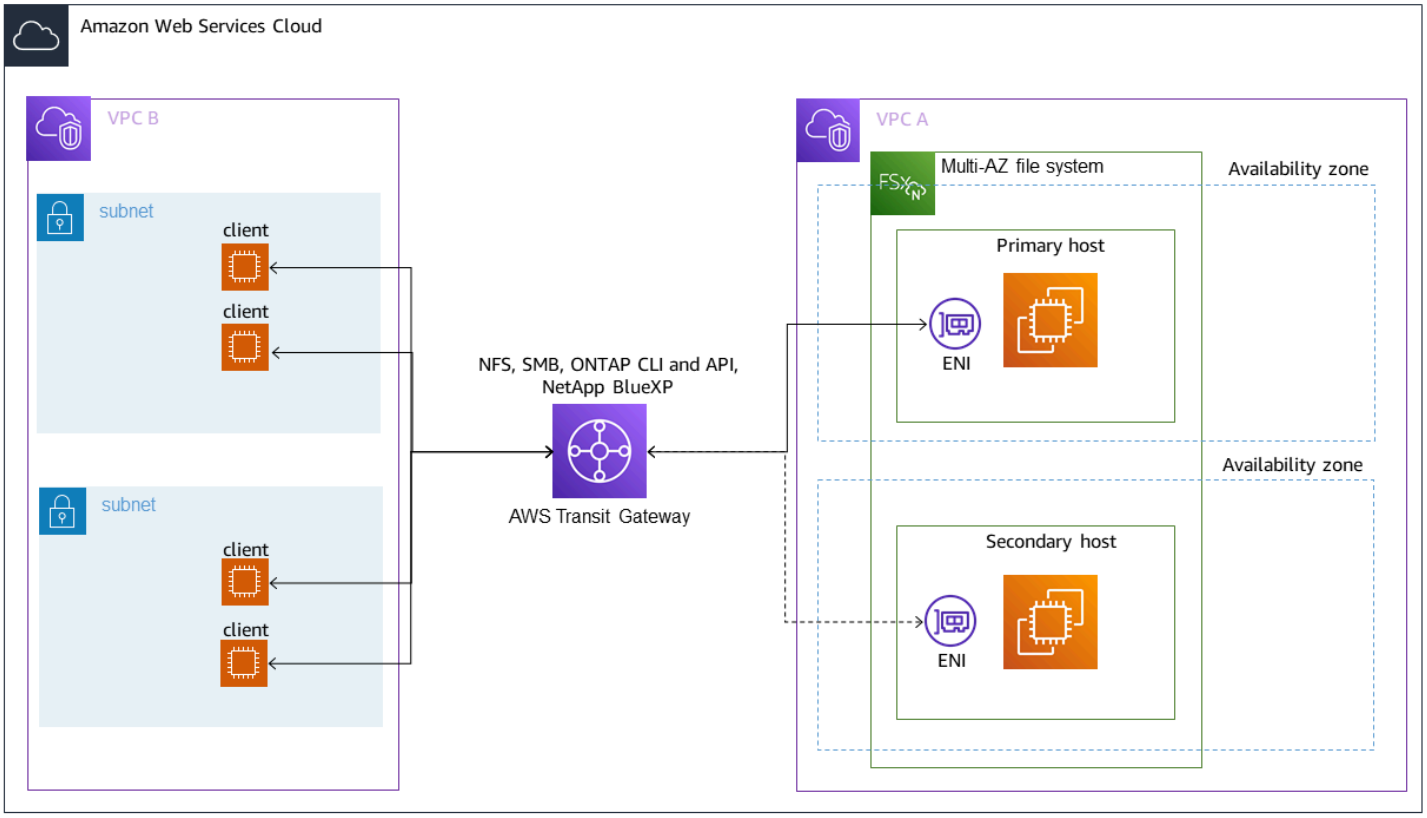
適用於 ONTAP 異地同步備份檔案系統的 Amazon FSX 上的 NFS、SMB 和 NetApp ONTAP 管理端點使用浮動網際網路通訊協定 (IP) 位址，因此連線的用戶端可在容錯移轉事件期間順暢地在偏好和備用檔案伺服器之間轉換。如需容錯移轉的詳細資訊，請參閱 適用於 ONTAP 的 FSx 的容錯移轉程序。

這些浮動 IP 位址是在您與檔案系統相關聯的 VPC 路由表中建立的，並且位於您可以在建立期間指定的`EndpointIpAddressRange`檔案系統內。根據檔案系統的建立方式，`EndpointIpAddressRange`會使用下列位址範圍：

- 依預設，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 範圍中最後 64 個 IP 位址。`EndpointIpAddressRange`
- `EndpointIpAddressRange`依預設，使用 AWS CLI 或 Amazon FSx API 建立的異地同步備份檔案系統會使用位`198.19.0.0/16`址區塊內的 IP 位址範圍。

僅AWS Transit Gateway支援路由至浮動 IP 位址，也稱為傳遞對等。VPC 對等互連 AWS Direct Connect，且 AWS VPN 不支援傳遞對等。因此，您必須使用 Transit Gateway 才能從檔案系統 VPC 以外的網路存取這些介面。

下圖說明如何使用 Transit Gateway，以進行 NFS、SMB 或管理存取異地同步備份檔案系統的異地同步備份檔案系統，這些檔案系統與正在存取 VPC 的用戶端不同。



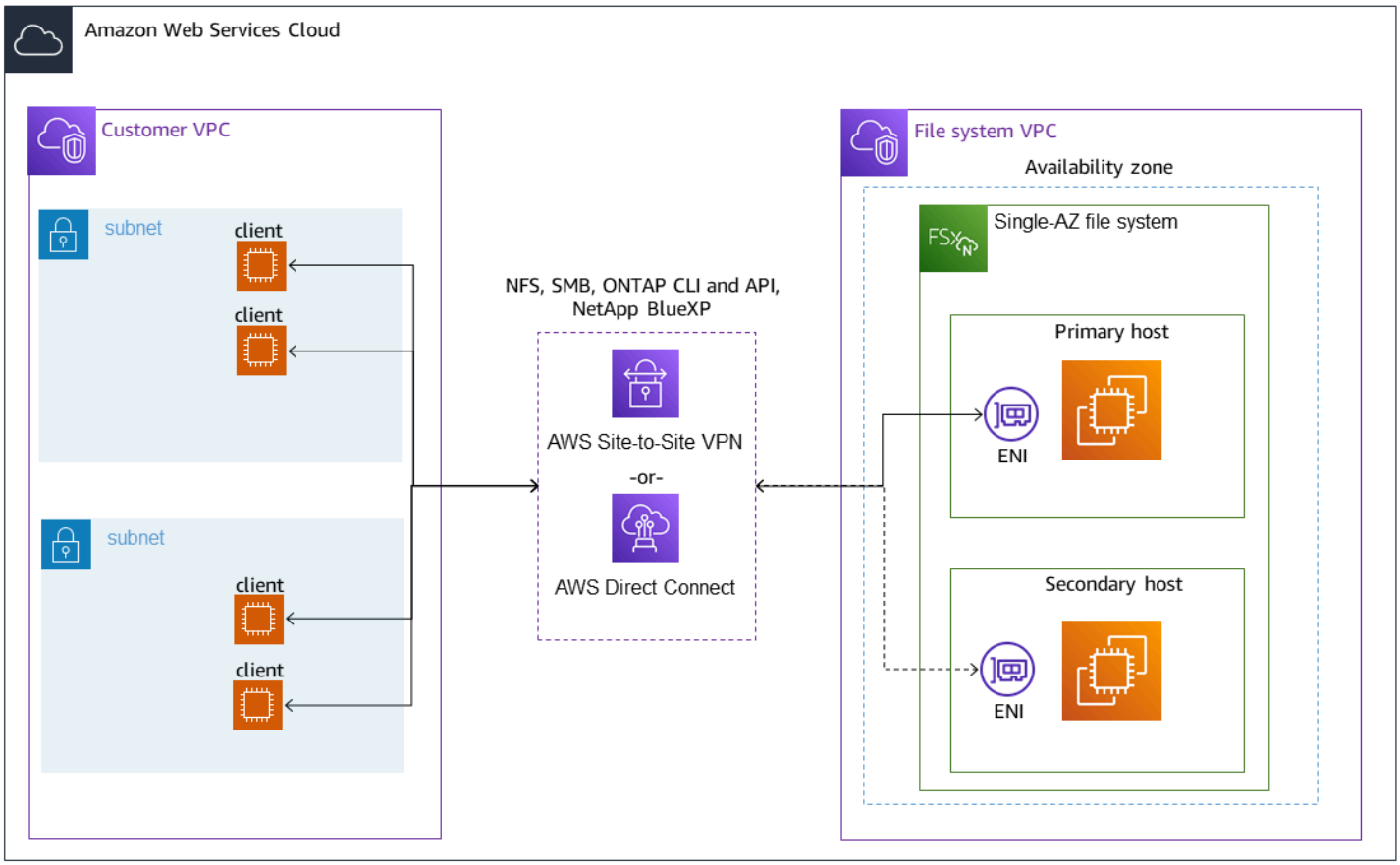
> **Note**
>
> 確保您使用的所有路由表都與異地同步備份檔案系統相關聯。這樣做有助於防止容錯移轉期間無法使用。如需將 Amazon VPC 路由表與檔案系統相關聯的資訊，請參閱。更新檔案系統

如需何時需要使用 Transit Gateway 存取 ONTAP 檔案系統 FSx 的相關資訊，請參閱。何時需要 Transit Gateway ?

針對單一可用區檔案系統存取 NFS、中小企業或 ONTAP CLI 和 API

用於透過 NFS 或 SMB 存取 ONTAP 單一可用區檔案系統的 FSx，以及使用 ONTAP CLI 或 REST API 管理檔案系統的端點，都是作用中檔案伺服器 ENI 上的次要 IP 位址。次要 IP 位址位於 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，或不需要。 AWS VPN AWS Transit Gateway

下圖說明如何使用 AWS VPN 或用 AWS Direct Connect 於 NFS、SMB 或管理存取單一可用區檔案系統，這些檔案系統位於與存取 VPC 不同的用戶端。



何時需要 Transit Gateway？

異地同步備份檔案系統是否需要 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 來存取異地同步備份檔案系統。

資料存取	需要 Transit Gateway 嗎？
透過 NFS、中小企業或 NetApp ONTAP REST API、CLI 或藍運算式存取 FSx	僅當： • 從對等 (例如內部部署) 網路存取，以及 • 您不是透過 NetApp FlexCache 或全域檔案快取執行個體存取 FSx
透過 iSCSI 存取資料	否
將 SVM 加入作用中目錄	否

資料存取	需要 Transit Gateway 嗎？
SnapMirror	否
FlexCache 快取	否
全域檔案快取	否

使用設定路由 AWS Transit Gateway

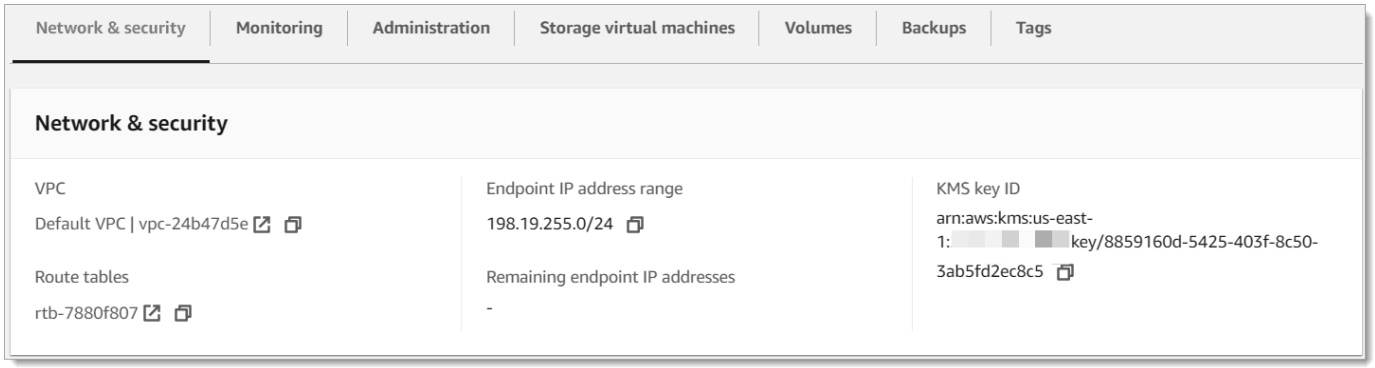
如果您的異地同步備份檔案系統超出 VPC `EndpointIPAddressRange` 的 CIDR 範圍，則需要在中設定其他路由，才能從對等網路或內 AWS Transit Gateway 部部署網路存取檔案系統。

> **Important**
>
> 若要使用 Transit Gateway 閘道存取異地同步備份檔案系統，必須在路由表與您的檔案系統相關聯的子網路中建立每個 Transit Gateway 的附件。

> **Note**
>
> 對於位於 VPC IP 位址範圍內的單一可用區檔案系統或異地同步備份檔案系統`EndpointIPAddressRange`，不需要額外的 Transit Gateway 組態。

若要使用來設定路由 AWS Transit Gateway

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 選擇要從對等網路設定存取權的 ONTAP 檔案系統的 FSx。
3. 在「網路與安全性」中，複製端點 IP 位址範圍。



4. 新增路由至「Transit Gateway」，將目的地為此 IP 位址範圍的流量路由至檔案系統的 VPC。如需詳細資訊，請參閱使用 Amazon VPC 傳輸閘道中的傳輸閘道。
5. 確認您可以從對等網路存取您的 FSx for ONTAP 檔案系統。

若要將路由表新增至您的檔案系統，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 中解析。若要從其他網路掛接磁碟區或連線至管理連接埠，您必須使用端點的 IP 位址。這些 IP 位址不會隨時間變更。

在部署 VPC 以外存取 iSCSI 或叢集間端點

您可以使用 VPC 對等互連，也可 AWS Transit Gateway 以從檔案系統的部署 VPC 外部存取檔案系統的 iSCSI 或叢集間端點。您可以使用 VPC 對等互連，在 VPC 之間路由 iSCSI 和叢集間流量。VPC 對等連線是兩個 VPC 之間的網路連線，可用來使用私有 IPv4 位址來路由它們之間的流量。您可以使用 VPC 對等連接相同 AWS 區域 或不同的 VPC。 AWS 區域如需 VPC 對等互連的詳細資訊，請參閱什麼是 V PC 對等互連？ 在 Amazon VPC 對等指南。

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；下列各節提供更具體的使用案例準則。除了下面列出的從現場部署存取 ONTAP 資源的不同 FSx 的任何要求之外，您還需要確保檔案系統的 VPC 安全群組允許資料在檔案系統和用戶端之間流動；如需必要的連接埠清單，請參閱 Amazon V PC 安全群組。

從內部部署存取 NFS、中小型企業或 ONTAP CLI 或 REST API 端點

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

存取異地同步備份檔案系

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 從現場部署網路存取異地同步備份檔案系統。為了支援異地同步備份檔案系統跨 AZ 的容錯移轉，Amazon FSx 針對 NFS、SMB 和 ONTAP 管理端點所使用的介面使用浮動 IP 地址。由於 NFS、SMB 和管理端點使用浮動 IP，因此您必須搭配使用AWS Transit Gateway AWS Direct Connect 或 AWS VPN 從內部部署網路存取這些介面。用於這些介面的浮動 IP 位址位於您在建立異地同步備份檔案系統時指定的 IP 位址。`EndpointIpAddressRange`如果您是從 Amazon FSx 主控台建立檔案系統，Amazon FSx 預設會從 VPC 的主要 CIDR 範圍中選擇最後 64 個 IP 位址，做為檔案系統的端點 IP 位址範圍。如果您是從 AWS CLI 或 Amazon FSx API 建立檔案系統，根據預設，Amazon FSx 會從 IP 位址範圍內選擇一個 `198.19.0.0/16` IP 位址範圍。浮動 IP 位址可用於在需要容錯移轉的情況下，將用戶端無縫轉換至待命檔案系統。如需詳細資訊，請參閱 適用於 ONTAP 的 FSx 的容錯移轉程序。

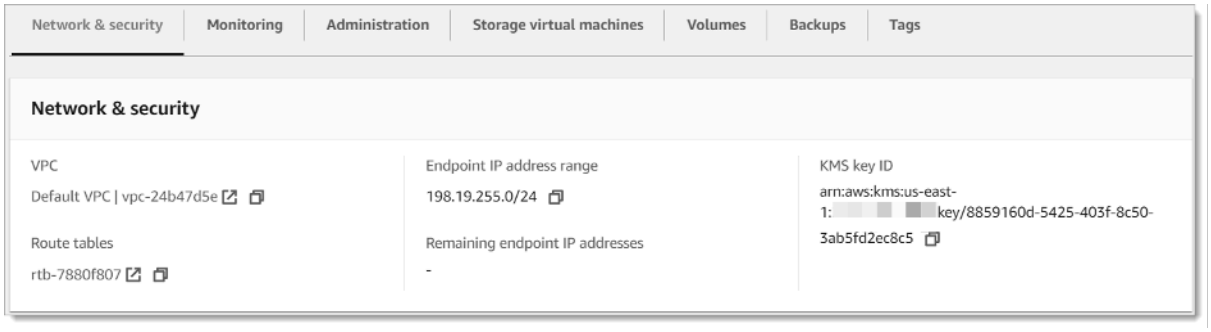
> **Important**
>
> 若要使用 Transit Gateway 閘道存取異地同步備份檔案系統，必須在路由表與您的檔案系統相關聯的子網路中建立每個 Transit Gateway 的附件。

若要設 AWS Transit Gateway 定從 VPC 外部存取

如果您的異地同步備份檔案系統超出 VPC `EndpointIPAddressRange` 的 CIDR 範圍，則需要在中設定其他路由，才能從對等網路或內 AWS Transit Gateway 部部署網路存取檔案系統。

> **Note**
>
> 對於位於 VPC IP 位址範圍內的單一可用區檔案系統或異地同步備份檔案系統`EndpointIPAddressRange`，不需要額外的 Transit Gateway 組態。

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 選擇要從對等網路設定存取權的 ONTAP 檔案系統的 FSx。
3. 在「網路與安全性」中，複製端點 IP 位址範圍。



4. 新增路由至「Transit Gateway」，將目的地為此 IP 位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 傳輸閘道使用者指南中的使用 Transit Gateway 道。
5. 確認您可以從對等網路存取您的 FSx for ONTAP 檔案系統。

> **Important**
>
> 若要使用 Transit Gateway 閘道存取異地同步備份檔案系統，必須在路由表與您的檔案系統相關聯的子網路中建立每個 Transit Gateway 的附件。

若要將路由表新增至您的檔案系統，請參閱更新檔案系統。

存取單一可用區檔案系統

單一可用 AWS Transit Gateway 區檔案系統不存在用於從內部部署網路存取資料的要求。單一可用區檔案系統部署在單一子網路中，不需要浮動 IP 位址即可在節點之間提供容錯移轉。相反地，您在單一可用區檔案系統上存取的 IP 位址會在檔案系統的 VPC CIDR 範圍內實作為次要 IP 位址，讓您無需從其他網路存取資料。 AWS Transit Gateway

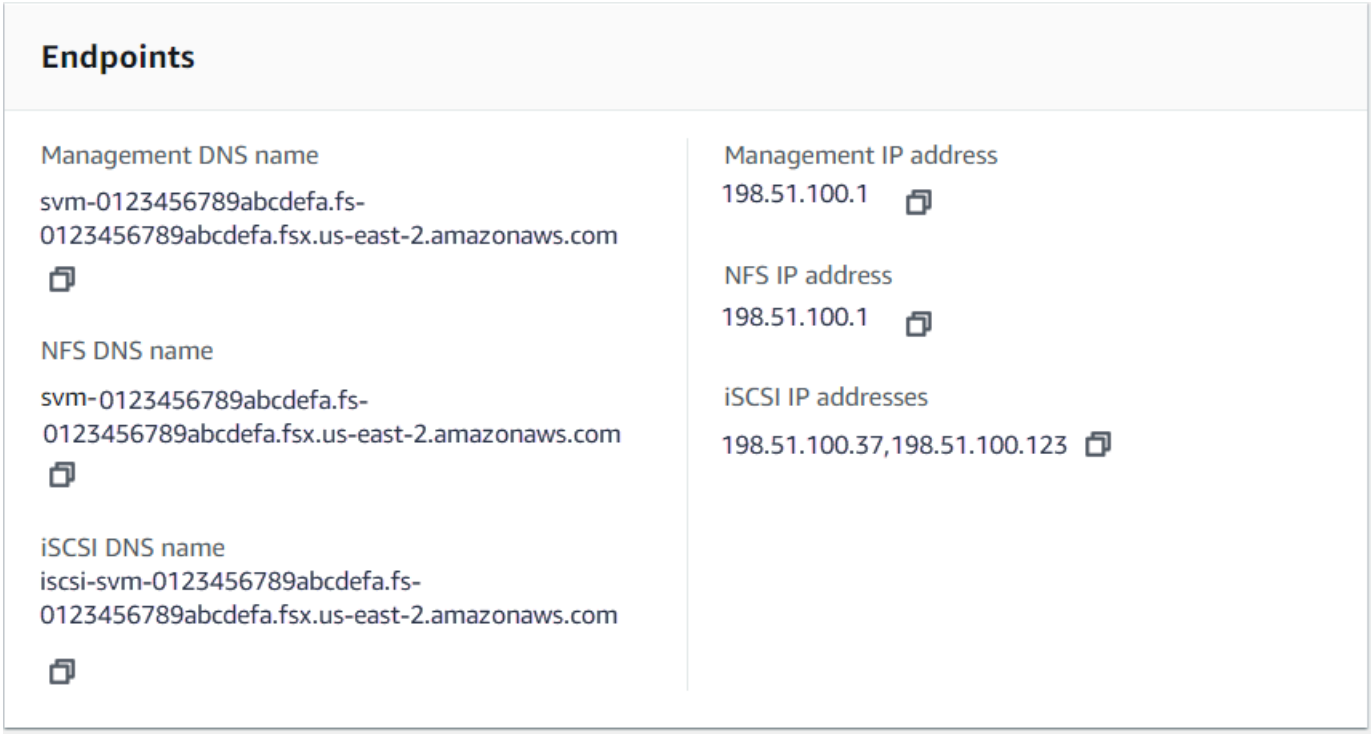
從內部部署存取叢集間端點

適用於 ONTAP 的叢集間端點 FSx 專用於 ONTAP 檔案系統之間的複寫流量，包括內部部 NetApp 署與 NetApp ONTAP 的 FSx 之間的複寫流量。複寫流量包括 SnapMirror不同檔案系統的儲存虛擬機器 (SVM) 與磁碟區之間的 FlexClone關係，以及 NetApp 全域檔案快取。 FlexCache叢集間端點也會用於作用中目錄流量。

由於當您為 ONTAP 檔案系統建立 FSx 時，檔案系統的叢集間端點會使用位於 VPC CIDR 範圍內的 IP 位址，因此您不需要使用 Transit Gateway 來路由內部部署與內部部署之間的叢集間流量。 AWS 雲端但是，內部部署用戶端仍必須使用 AWS VPN 或 AWS Direct Connect 建立與 VPC 的安全連線。

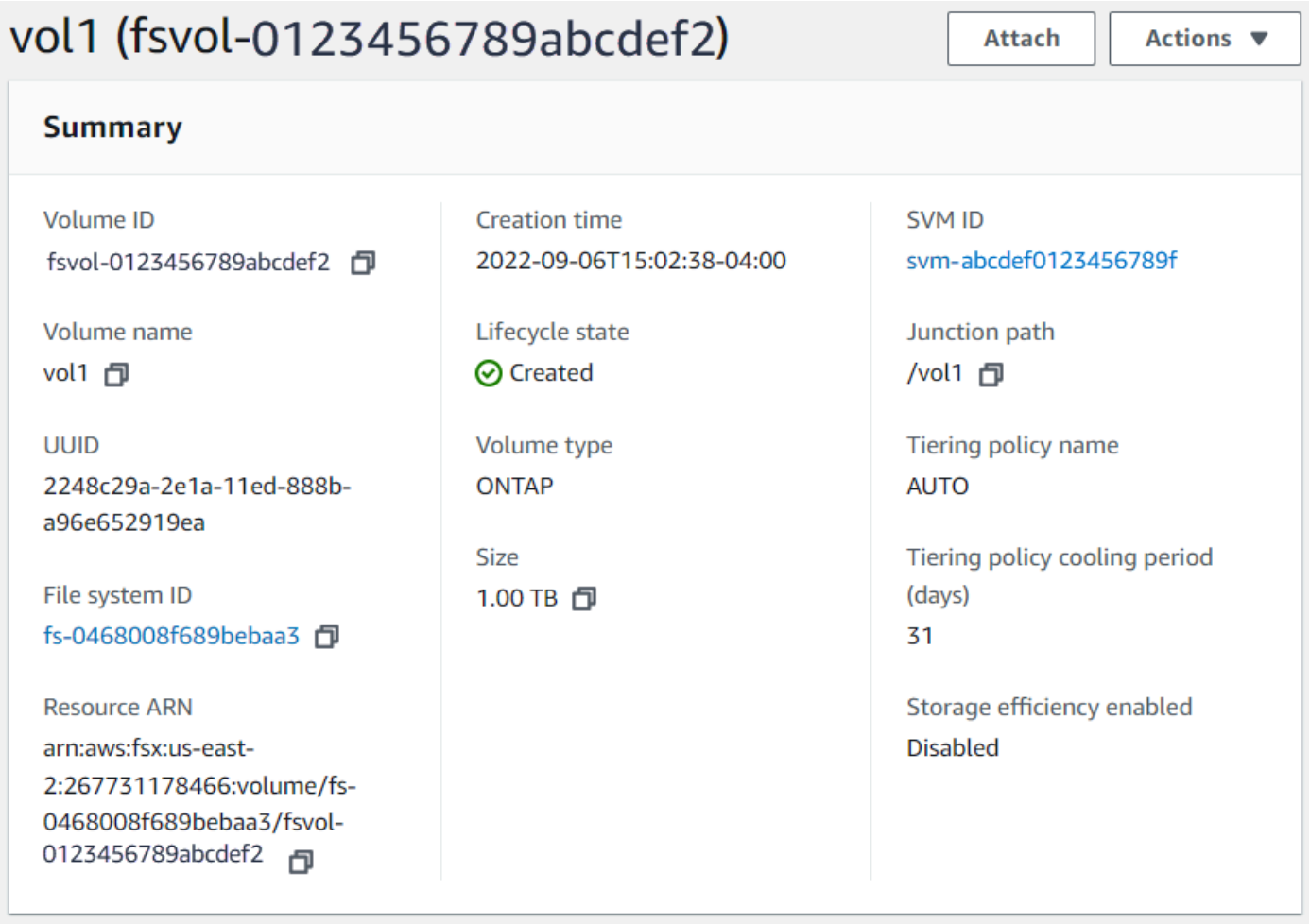
掛載磁碟區

您可以透過在用戶端上掛載磁碟區來存取 FSx for ONTAP 中的資料。本節中的命令使用建立磁碟區來掛接或連接磁碟區之 SVM 的 DNS 名稱或 IP 位址。您可以在 Amazon FSx 主控台中找到 SVM 的 DNS 名稱和 IP 位址，方法是選擇 ONTAP > 儲存虛擬機器，或在檔案系統的檔案系統詳細資料頁面的儲存虛擬機器索引標籤上 (如下圖所示)。



或者，您可以在 DescribeStorageVirtualMachinesAPI 操作的響應中找到它們。

您可以在磁碟區詳細資料頁面的摘要面板上的 Amazon FSx 主控台中找到磁碟區的結合路徑，如下圖所示。



主題

- 掛載在客戶端
- 安裝在 Microsoft 視窗用戶端
- 掛載於 macOS 用戶端

掛載在客戶端

我們建議您要連接 Linux 用戶端的 SVM 磁碟區具有UNIX或mixed的安全性樣式設定。如需詳細資訊，請參閱 管理安裝磁碟區的 FSx。

> **Note**
>
> 根據預設，適用於 ONTAP NFS 掛載的 FSx 為裝載。hard若要確保容錯移轉發生時順利進行，我們建議您使用預設hard掛載選項。

若要在 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，該執行個體與檔案系統位於相同的 VPC 中。

   如需有關啟動 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. Connect 到您的 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 Connect 到 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，然後使用適當的登入資料登入。
5. 在 EC2 執行個體上建立一個目錄以掛接 SVM 磁碟區，如下所示：

   ```
   sudo mkdir /fsx
   ```
6. 使用下列指令將磁碟區掛接到您剛建立的目錄：

   ```
   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-01234567890abdef0.fs-01234567890abcdef1.fsx.us-
   east-1.amazonaws.com:/vol1 /fsx
   ```

   您也可以使用 SVM 的 IP 位址 SVM 來取代其 DNS 名稱。我們建議您使用 DNS 名稱來掛載用戶端以向外延展檔案系統，因為這有助於確保您的用戶端在檔案系統的高可用性 (HA) 配對之間取得平衡。

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

   > **Note**
   >
   > 對於向外延展檔案系統，parallel NFS (pNFS) 通訊協定預設為啟用，預設會用於掛接 NFS v4.1 或更新版本之磁碟區的任何用戶端。

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適用於 ONTAP 磁碟區的 FSx，請使用檔案。/etc/fstab/etc/fstab 檔案包含檔案系統的資訊，在執行個體啟動期間執行的指令mount -a會掛載中列出的檔案系統/etc/fstab。

> **Note**
>
> 適用於 ONTAP 檔案系統的 FSx 不支援/etc/fstab在 Amazon EC2 Mac 執行個體上使用的自動掛接。

> **Note**
>
> 在更新 EC2 執行個體的/etc/fstab檔案之前，請確定您已經建立了適用於 ONTAP 檔案系統的 FSx。如需詳細資訊，請參閱 為 ONTAP 檔案系統建立 FSx。

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. 建立將用來掛載 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 Tab 字元。它應該顯示為一行，沒有換行符。

```
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 位址。最後三個參數表示 NFS 選項（我們設置為默認值），轉儲文件系統和文件系統檢查（這些通常不使用，因此我們將它們設置為 0）。

5. 儲存對檔案所做的變更。
6. 現在，使用下面的命令掛載文件共享。下次系統啟動時，資料夾將自動掛載。

```
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接 ONTAP 磁碟區。

安裝在 Microsoft 視窗用戶端

本節說明如何透過執行 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，請檢閱下列需求。

此程序假設用戶端和檔案系統位於相同的 VPC 和 AWS 帳戶。如果用戶端位於內部部署或不同的 VPC AWS 帳戶、或中 AWS 區域，此程序也假設您已使用 AWS Transit Gateway 或使用私人安全通道設定 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 通訊協定將磁碟區附加到 Windows 用戶端。

必要條件

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 加入作用中目錄的詳細資訊，請參閱管理適用於 ONTAP 儲存區虛擬機器的 FSx。如需使用工作群組的詳細資訊，請參閱NetApp 文件中心的工作群組概觀中的設定 SMB 伺服器。
- 您要連接的磁碟區的安全性樣式設定為NTFS或mixed。如需詳細資訊，請參閱 管理安裝磁碟區的 FSx。

使用 SMB 和作用中目錄在 Windows 用戶端上附加 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 Microsoft 視窗的 Amazon EC2 執行個體，該執行個體與檔案系統位於相同的 VPC 中，並加入與磁碟區的 SVM 相同的 Microsoft 活動目錄。

   如需有關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 加入作用中目錄的詳細資訊，請參閱管理適用於 ONTAP 儲存區虛擬機器的 FSx。

3. Connect 到您的 Amazon EC2 視窗執行個體。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的連線到 Windows 執行個體。

4. 開啟命令提示。

5. 執行下列命令。取代以下項目：

   - 更換為任何可用`Z:`的磁碟機代號。
   - 取代`DNS_NAME`為磁碟區 SVM 之 SMB 端點的 DNS 名稱或 IP 位址。
   - `SHARE_NAME`以 SMB 共用的名稱取代。`C$`是 SVM 命名空間根目錄的預設 SMB 共用，但您不應該掛載它，因為它會將儲存空間公開到根磁碟區，而且可能會造成安全性和服務中斷。您應該提供要掛載的 SMB 共用名稱，而不是`C$`。如需建立 SMB 共用的詳細資訊，請參閱管理中小企業股。

   ```
   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 位址，而不是其 DNS 名稱。我們建議您使用 DNS 名稱來掛載用戶端以向外延展檔案系統，因為這有助於確保您的用戶端在檔案系統的高可用性 (HA) 配對之間取得平衡。

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

掛載於 macOS 用戶端

本節說明如何透過執行 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 AWS 帳戶。如果用戶端位於內部部署 AWS 帳戶 或 AWS 區域不同的 VPC 中， AWS Direct Connect 或者您已使用. AWS Transit Gateway 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 通訊協定將磁碟區附加至 Mac 用戶端。

若要使用 SMB 在 macOS 用戶端上掛接 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 macOS 的 Amazon EC2 Mac 執行個體，該執行個體與檔案系統位於相同的 VPC 中。

   如需有關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. Connect 到您的 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 Connect 到 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，然後使用適當的登入資料登入。
5. 在 EC2 執行個體上建立目錄以掛接磁碟區，如下所示：

   ```
   sudo mkdir /fsx
   ```
6. 使用下列指令掛接磁碟區。

   ```
   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 位址，而不是其 DNS 名稱。我們建議您使用 DNS 名稱來掛載用戶端以向外延展檔案系統，因為這有助於確保您的用戶端在檔案系統的高可用性 (HA) 配對之間取得平衡。

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

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

若要使用 NFS 在 macOS 用戶端上掛接 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，該執行個體與檔案系統位於相同的 VPC 中。

   如需有關啟動 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. Connect 到您的 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 Connect 到 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，將 FSx for ONTAP 磁碟區掛載到 Linux EC2 執行個體上：

   ```
   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-01234567890abdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /
   fsxontap
   ```

   您也可以使用 SVM 的 IP 位址 SVM 來取代其 DNS 名稱。我們建議您使用 DNS 名稱來掛載用戶端以向外延展檔案系統，因為這有助於確保您的用戶端在檔案系統的 HA 配對之間保持平衡。

   ```
   sudo mount -t nfs -o nfsvers=4.1 198.51.100.1:/vol1 /fsxontap
   ```
5. 使用下列指令將磁碟區掛接到剛才建立的目錄。

   ```
   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-01234567890abdef0.fs-01234567890abcdef1.fsx.us-
east-1.amazonaws.com:/vol1 /fsx
```

您也可以使用 SVM 的 IP 位址 SVM 來取代其 DNS 名稱。我們建議您使用 DNS 名稱來掛載用戶端以向外延展檔案系統，因為這有助於確保您的用戶端在檔案系統的高可用性 (HA) 配對之間取得平衡。

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

iSCSI 載

適用於 NetApp ONTAP 的 Amazon FSx 可透過 iSCSI (網際網路小型電腦系統介面) 通訊協定提供共用區塊儲存支援。您可以透過佈建 LUN (邏輯單位編號) 並將它們對應至啟動器群組 (igroups)，從而將區塊儲存體公開給 Linux 和 Windows 主機來啟用 iSCSI 儲存區。

> **Note**
>
> ONTAP 向外延展檔案系統的 FSx 不支援 iSCSI 通訊協定，這些檔案系統是具有多個高可用性 (HA) 對檔案伺服器的檔案系統。

主題

將 iSCSI 連接至用戶端

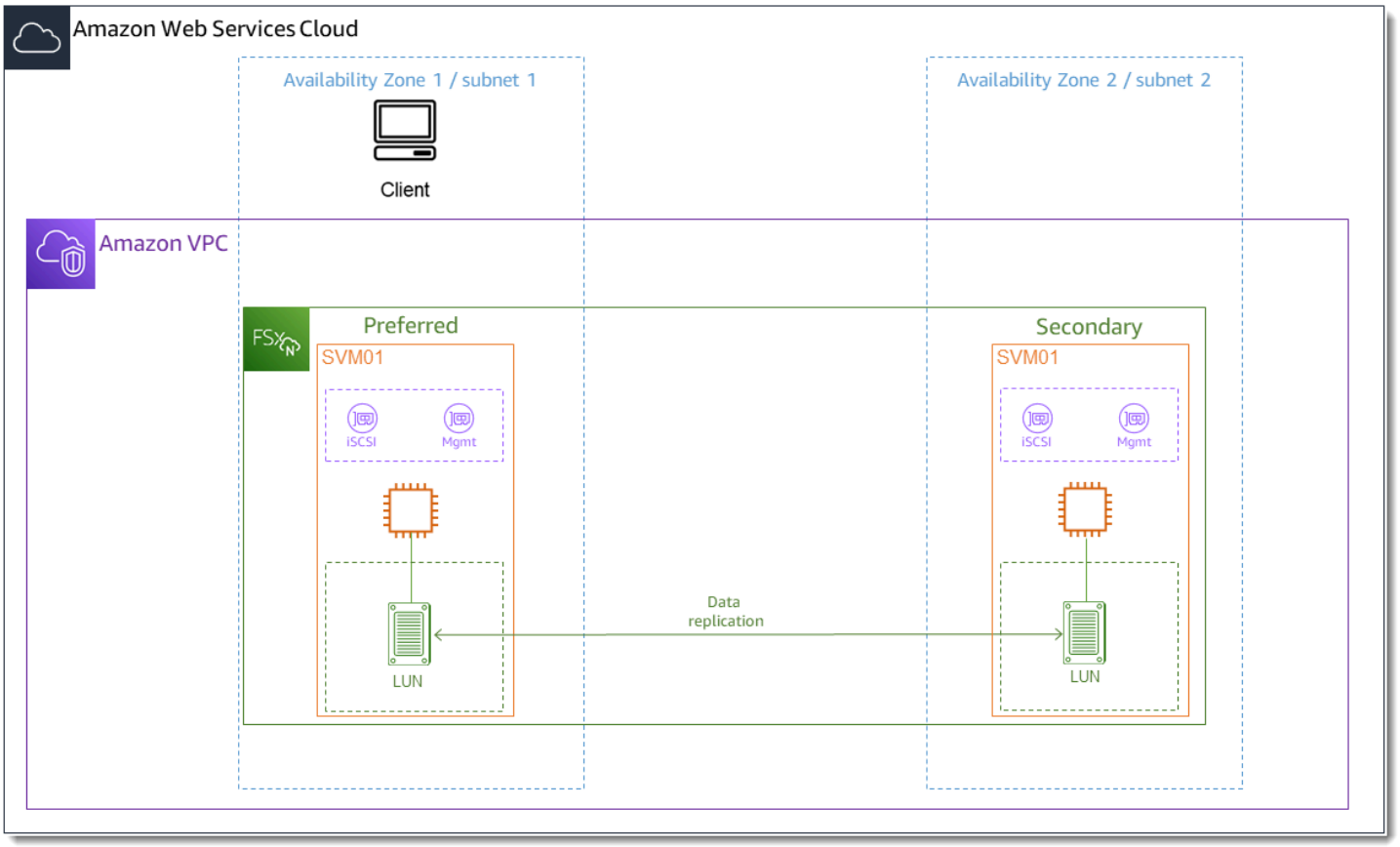
這些程序中顯示的範例使用下列設定：

- 已經建立掛載至 Linux 主機的 iSCSI 磁碟區。如需詳細資訊，請參閱 建立一 iSCSI。
- 掛接 iSCSI LUN 的 Linux 主機是執行 Amazon Linux 2 Amazon 機器映像 (AMI) 的亞馬遜 EC2 執行個體。它具有設定為允許輸入和輸出流量的 VPC 安全群組，如中使用 Amazon VPC 進行檔案系統存取控制所述。

- 適用於 ONTAP 檔案系統的 Linux 主機和 FSx 位於相同的 VPC 和. AWS 帳戶如果主機位於另一個 VPC 中，您可以使用 VPC 對等互連或 AWS Transit Gateway 授與其他 VPC 存取磁碟區 iSCSI 端點。如需詳細資訊，請參閱 從部署 VPC 外部存取資料。

  如果您使用執行不同 Linux AMI 的 EC2 執行個體，主機上安裝的部分公用程式可能已預先安裝，而且您可能會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 AMI 也有效。

  我們建議 EC2 執行個體與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

- 在用戶端上安裝及設定 iSCSI
- 在 FSx 上設定適用於 ONTAP 檔案系統的 iSCSI
- 在您的用戶端上掛載 iSCSI 磁碟

在用戶端上安裝及設定 iSCSI

若要安裝 iSCSI 用戶端

1. 確認`iscsi-initiator-utils`並已安裝`device-mapper-multipath`在您的 Linux 設備上。使用安全殼層用戶端 Connect 至您的 Linux 執行個體。如需詳細資訊，請參閱使用安全殼層 Connect 到 Linux 執行個體。
2. 使用以下命令安裝 `multipath` iSCSI 用戶端。如果您想要在檔案伺服器之間自動容錯移轉，則需要進行安`multipath`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`檔案中的取代逾時值設定為值，`5`而不是使用預設值`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，您可能必須使用以下命令：

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

5. 使用以下命令確認服務正在運行。

```
~$ 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
```

若要在您的用戶端上設定 iSCSI

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

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

2. 使用下列命令判斷 Linux 主機的啟動器名稱。啟動器名稱的位置取決於您的 iSCSI 公用程式。如果使用`iscsi-initiator-utils`，初始器名稱位於檔案`/etc/iscsi/initiatorname.iscsi`中。

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

   系統以初始器名稱回應。

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

在 FSx 上設定適用於 ONTAP 檔案系統的 iSCSI

1. 使用 NetApp 下列指令，Connect 至您在其上建立 iSCSI LUN 的 FSx 適用於 ONTAP 檔案系統上的 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 指令lun igroup create建立初始器群組 (`igroup`)。啟動器群組對應至 iSCSI LUN，並控制哪些啟動器 (用戶端) 可以存取 LUN。取代`host_initiator_name`為您在上一個程序中擷取的 Linux 主機中的初始器名稱。

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

   如果您要讓對應至此 igroup 的 LUN 可供多台主機使用，您可以指定多個初始器名稱，並以逗號分隔。如需詳細資訊，請參閱 NetApp ONTAP 文件中心的 LUN 測試建立。

3. 使用以下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
--------- ------------ -------- -------- ------------------------------------
svm_name  igroup_name  iscsi    linux    iqn.1994-05.com.redhat:abcdef12345
```

4. 此步驟假設您已經建立了一個 iSCSI LUN。如果尚未執行，請參建立一 iSCSI閱以取得相 step-by-step 關說明。

使用指定下列屬性，從您建立的 LUN 建立對應至您建立的 lun mapping createigroup：

- *svm_name*— 提供 iSCSI 目標的儲存區虛擬機器名稱。主機會使用此值連線到 LUN。
- *vol_name*— 裝載 LUN 的磁碟區名稱。
- *lun_name*— 您指派給 LUN 的名稱。
- *igroup_name*— 初始器群組的名稱。
- *lun_id*— LUN ID 整數是特定於對應，而不是 LUN 本身。igroup 中的初始器會使用此值，作為邏輯單位編號在存取儲存裝置時使用此值作為初始器。

```
::> 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指令確認 LUN 已建立、連線和對應。

```
::> 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
 --------- ------------------------------- ------------------------ --------
 --------
 svm_name  /vol/vol_name/lun_name          6c5742314e5d52766e796150 online   mapped
```

儲存serial_hex值 (在此範例中為6c5742314e5d52766e796150)，您將在稍後的步驟中使用該值，為區塊裝置建立易記的名稱。

6. 使用此network interface show -vserver命令擷取您在其中建立 iSCSI LUN 之 SVM 的位址iscsi_1和iscsi_2介面。

```
::> 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 位址iscsi_1為172.31.0.143和iscsi_2是172.31.21.81。

在您的用戶端上掛載 iSCSI 磁碟

1. 在您的 Linux 用戶端上，使用下列指令來探索使用iscsi_1的 IP 位址 *ICSI* _1_IP 的目標 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對應target_initiator於偏好可用區域中 iSCSI LUN 的。

2. (選擇性) 您可以使用建立其他工作階段target_initiator。對於單一流程流量，Amazon EC2 的頻寬限制為每秒 5 GB (約 625 MB/秒)，但是您可以建立多個工作階段，從單一用戶端提高檔案系統的輸送量。如需詳細資訊，請參閱 Amazon 彈性運算雲端 Linux 執行個體使用者指南中的 Amazon EC2 執行個體網路頻寬。

   下列命令會在每個可用區域中的每個 ONTAP 節點為每個啟動器建立 8 個工作階段，讓用戶端能夠將最高 40 Gb/s (5,000 MB) 的彙總輸送量驅動到 iSCSI LUN。

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

3. 登入目標初始器。您的 iSCSI LUN 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.
   ```

   上面的輸出被截斷；您應該在每個文件服務器上看到每個會話的一個Login successful響應Logging in和一個響應。在每個節點有 4 個會話的情況下，將有 8 個Logging in和 8 個Login successful響應。

4. 使用下列命令，透過顯示dm-multipath具有多個原則的單一 LUN，以確認是否已識別並合併 iSCSI 工作階段。應該有相同數量的設備被列為active和那些列為enabled.

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

   在輸出中，磁碟名稱格式化為dm-xyz，其中xyz為整數。如果沒有其他多重路徑磁碟，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到 Linux 用戶端。它位於路徑下方/dev/*dm-xyz*。您不應將此路徑用於管理目的，而是使用路徑下的符號連結/dev/mapper/*wwid*，其中*wwid*是 LUN 的唯一識別碼，在不同裝置間保持一致。在下一個步驟中，您將提供易記的名稱，以*wwid*便將其與其他多重路徑磁碟區分開來。

為您的區塊裝置提供易記的名稱

1. 若要為您的裝置提供易記的名稱，請在/etc/multipath.conf檔案中建立別名。若要這麼做，請使用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：

   - 以您在在 FSx 上設定適用於 ONTAP 檔案系統的 iSCSI程序中儲存的值取serial_hex代。
   - 如範例所示，3600a0980將前置字元加入至serial_hex值。這是適用於 ONTAP 的 Amazon FSx 使用的 NetApp ONTAP 發行版的唯一序言。 NetApp
   - 以您要在裝置上使用的易記名稱取device_name代。

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

作為替代方法，您可以將以下腳本複製並保存為 bash 文件，例如multipath_alias.sh. 您可以使用 sudo 權限執行指令碼，取代 *serial_hex* (不含 3600a0980 前置詞) 以及您個別*device_name*的序號和所需的易記名稱。此指令碼會搜尋/etc/multipath.conf檔案中未註

解的multipaths區段。如果存在，它會在該部分附加一個multipath條目；否則，它將創建一個新的multipaths部分，其中包含塊設備的multipath條目。

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

若要磁碟分割 LUN

下一步是使用格式化和分割 LUN fdisk。

1. 使用以下命令來驗證您的路徑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。依照顯示的順序輸入選項。請注意，此Last sector值會因 iSCSI LUN 的大小而有所不同 (此範例中為 10GB)。您可以使用小於最後一個磁區的值來建立多個分割區 (20971519在此範例中)。

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

fsdisk互動式提示隨即開始。

```
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.
```

輸入後w，您的新分區/dev/mapper/*partition_name*變為可用。*#####*

#<device_name><partition_number>具有格式。 1被用作上一個步驟中fdisk指令中使用的分割區號碼。

3. 使用/dev/mapper/*partition_name*作為路徑建立您的檔案系統。

```
~$ 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
```

若要在 Linux 用戶端上掛載 LUN

1. 建立目錄 *directory_path* 做為檔案系統的掛載點。

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

2. 使用下列指令掛載檔案系統。

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

3. (選擇性) 您可以將掛載目錄的擁有權變更為使用者。*username*以您的使用者名稱取代。

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

4. (選擇性) 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!
```

您已經在 Linux 用戶端上成功建立並掛接了一個 iSCSI LUN。

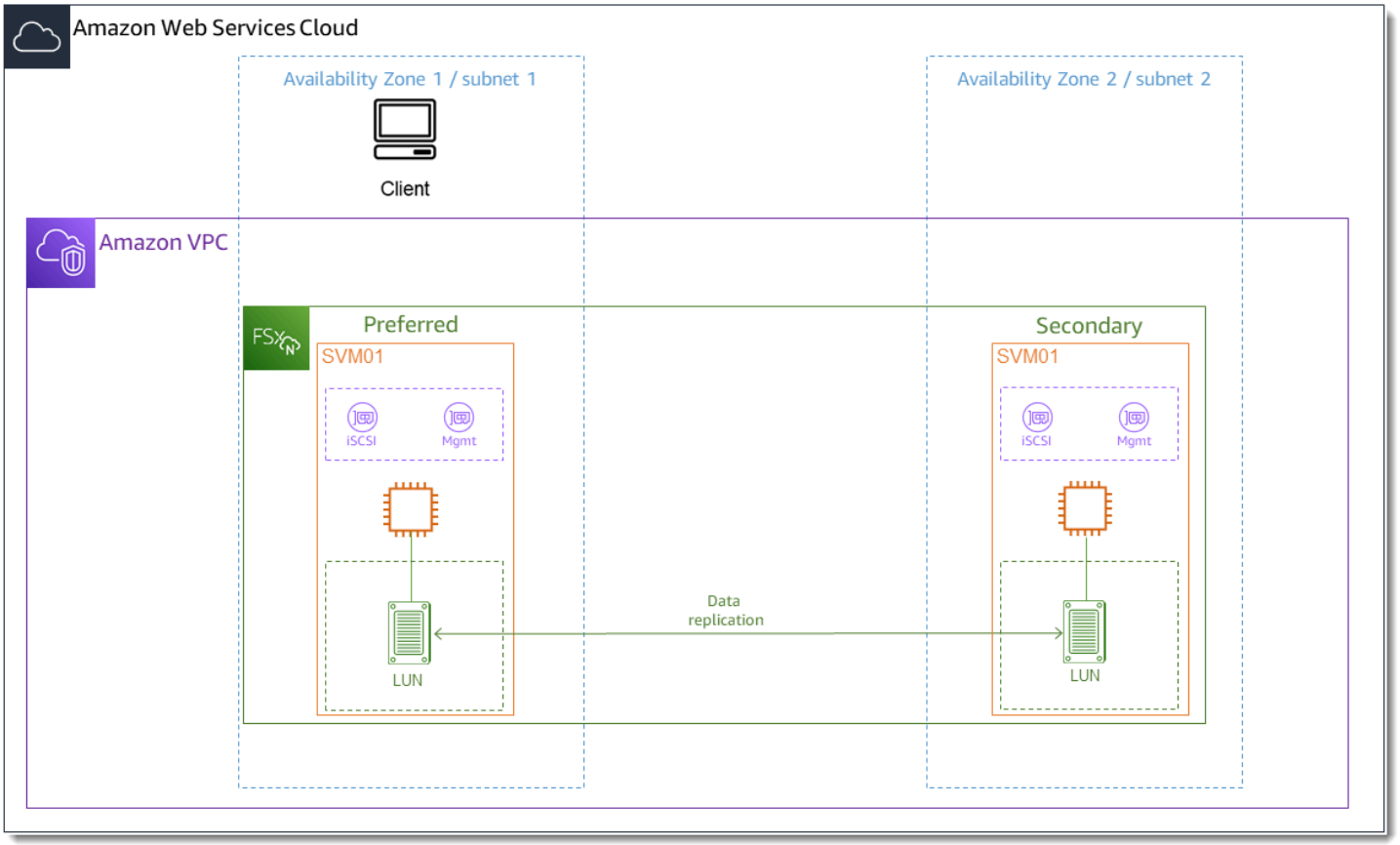
將 iSCSI LUN 掛載到視窗用戶端

這些程序中顯示的範例使用下列設定：

- 已經建立掛載至 Windows 主機的 iSCSI 磁碟區。如需詳細資訊，請參閱 建立一 iSCSI。
- 正在掛載 iSCSI LUN 的 Microsoft 視窗主機是一個 Amazon EC2 實例，運行 Microsoft 視窗服務器 2019 Amazon 機器映像（AMI）。它具有設定為允許輸入和輸出流量的 VPC 安全群組，如中使用 Amazon VPC 進行檔案系統存取控制所述。

  您可能在設定中使用不同的 Microsoft 視窗 AMI。
- 用戶端和檔案系統位於相同的 VPC 和 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 授與其他 VPC 存取 iSCSI 端點。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

- 在用戶端上設定 iSCSI
- 在 FSx 上設定適用於 ONTAP 檔案系統的 iSCSI
- 在視窗用戶端上掛載 iSCSI 磁碟

- 驗證您的 iSCSI 組態

在用戶端上設定 iSCSI

1. 使用視窗遠端桌面連線至您要掛接 iSCSI LUN 的視窗用戶端。如需詳細資訊，請參閱 Amazon 彈性運算雲端使用者指南中的使用 RDP Connect 到 Windows 執行個體。
2. PowerShell 以系統管理員身分開啟視窗。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。您將使用這個值，在您的 FSx 上使用 ONTAP CLI 來設定適用於 ONTAP 檔案系統的 NetApp iSCSI 時。

```
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-IO` (MPIO)。使用下列命令：

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

5. `Multipath-IO`安裝完成後，請重新啟動 Windows 執行個體。將 Windows 執行個體保持開啟狀態，以便在接下來的一節中執行掛載 iSCSI LUN 的步驟。

在 FSx 上設定適用於 ONTAP 檔案系統的 iSCSI

1. 使用 NetApp 下列指令，Connect 至您在其上建立 iSCSI LUN 的 FSx 適用於 ONTAP 檔案系統上的 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建立啟動器群組，或。igroup啟動器群組對應至 iSCSI LUN，並控制哪些啟動器 (用戶端) 可以存取 LUN。取代host_initiator_name為您在上一個程序中擷取的 Windows 主機中的初始器名稱。

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

如果要讓對應至此的 LUN 可igroup供多台主機使用，您可以指定多個以逗號分隔的初始器名稱。如需詳細資訊，請參閱 lun igroup createNetApp ONTAP 文件中心。

3. 使用下列命令確認已成功建立：igroup

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

系統會以下列輸出回應：

```
Vserver    Igroup        Protocol OS Type  Initiators
---------  ------------  -------- -------- ------------------------------------
svm_name   igroup_name   iscsi    windows  iqn.1994-05.com.windows:abcdef12345
```

在建igroup立之後，您就可以建立 LUN 並將它們對應至. igroup

4. 此步驟假設您已經建立了一個 iSCSI LUN。如果尚未執行，請參建立一 iSCSI閱以取得相 step-by-step 關說明。

建立從 LUN 到新磁碟的 LUN 對應igroup。

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

5. 使用下列指令確認 LUN 已建立、連線及對應：

```
::> lun show -path /vol/vol_name/lun_name
Vserver     Path                            State   Mapped   Type     Size
---------   ------------------------------- ------- -------- -------- --------
svm_name    /vol/vol_name/lun_name          online  mapped   windows  10GB
```

您現在可以在 Windows 執行個體上新增 iSCSI 目標了。

6. 使用下列命令擷取 SVM 的iscsi_1和iscsi_2介面的 IP 位址：

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

```
            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 位址iscsi_1為172.31.0.143和iscsi_2是172.31.21.81。

在視窗用戶端上掛載 iSCSI 磁碟

1. 在 Windows 執行個體上，以系統管理員身分開啟 PowerShell 終端機。
2. 您將建立可執行下列動作的.ps1指令碼：
   - 連線至每個檔案系統的 iSCSI 介面。
   - 為 iSCSI 新增及設定 MPIO。
   - 為每個 iSCSI 連線建立 8 個工作階段，這可讓用戶端向 iSCSI LUN 磁碟機高達 40 Gb/s (5,000 MB/秒) 的彙總輸送量。擁有 8 個工作階段可確保單一用戶端能夠為 ONTAP 輸送量容量提供最高層級 FSx 的 4,000 MB/s 輸送量容量。您可以選擇性地將工作階段數目變更為較高或較低的工作階段數目 (每個工作階段最多可提供 625 MB/s 的輸送量)，方法是1..8將#Establish iSCSI connection步驟中的 for 迴圈修改為另一個上限。如需詳細資訊，請參閱 Amazon EC2 執行個體網路頻寬，其中的 Amazon 彈性運算雲端使用者指南適用於 Windows 執行個體。

   將下列指令集複製到檔案中以建立指.psl令碼。

   - 將iscsi_1和iscsi_2取代為您在上一個步驟中擷取的 IP 位址。
   - ec2_ip以您的 Windows 執行個體的 IP 位址取代。

```
#iSCSI IP addresses for Preferred and Standby subnets
$TargetPortalAddresses = @("iscsi_1","iscsi_2")

#iSCSI Initator IP Address (Local node IP address)
$LocaliSCSIAddress = "ec2_ip"

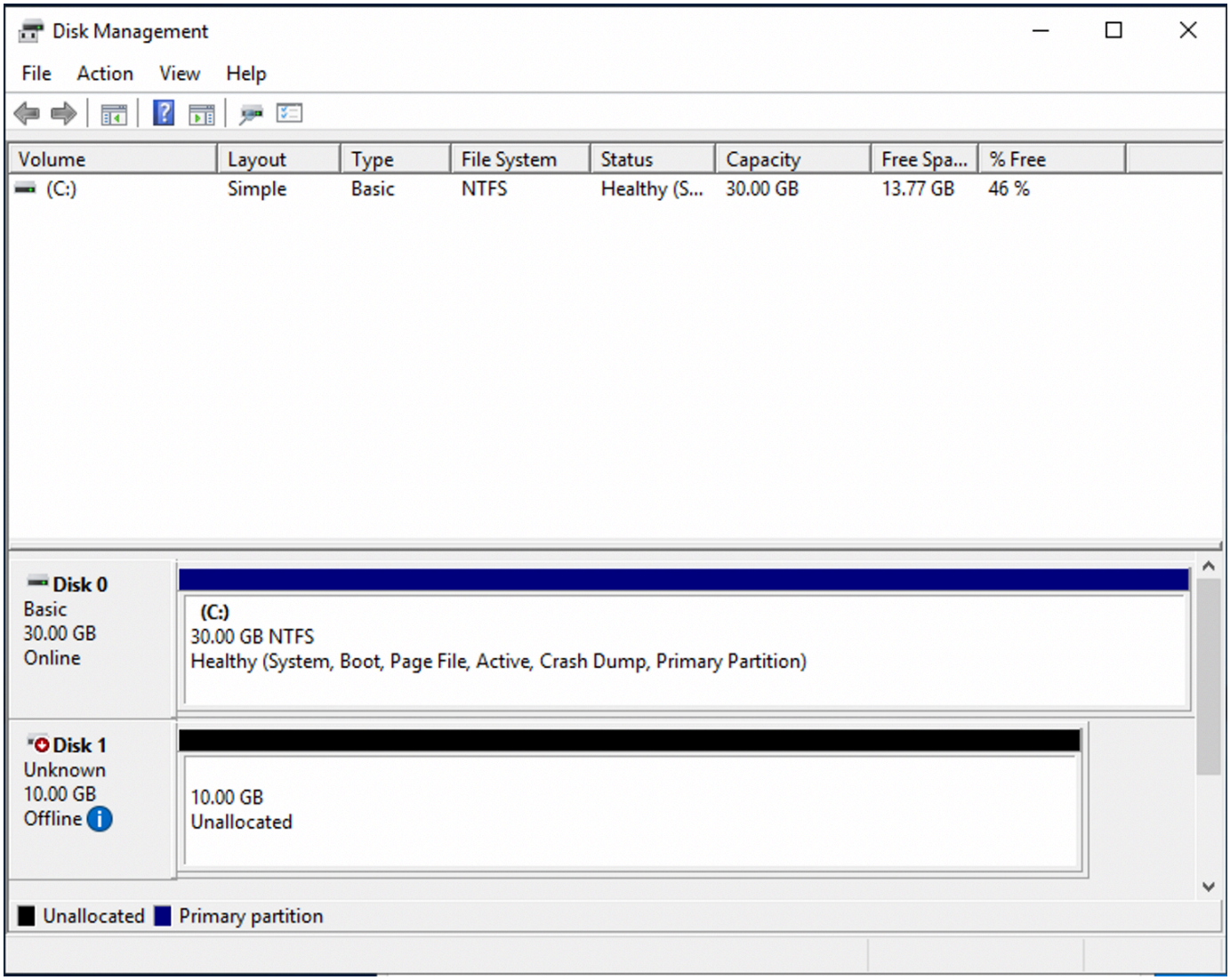
#Connect to FSx for NetApp ONTAP file system
Foreach ($TargetPortalAddress in $TargetPortalAddresses) {
New-IscsiTargetPortal -TargetPortalAddress $TargetPortalAddress -
TargetPortalPortNumber 3260 -InitiatorPortalAddress $LocaliSCSIAddress
}

#Add MPIO support for iSCSI
New-MSDSMSupportedHW -VendorId MSFT2005 -ProductId iSCSIBusType_0x9

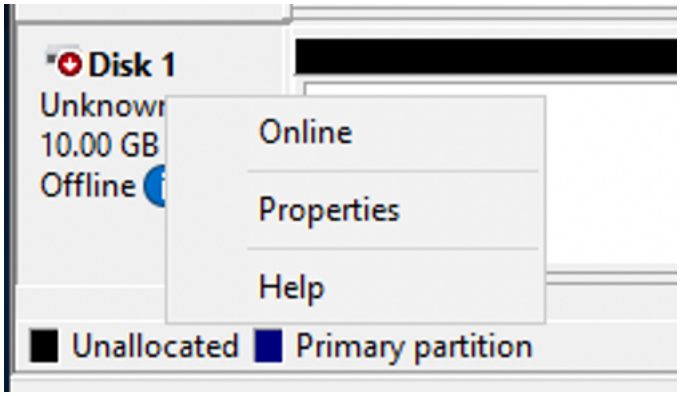
#Establish iSCSI connection
1..8 | %{Foreach($TargetPortalAddress in $TargetPortalAddresses)
{Get-IscsiTarget | Connect-IscsiTarget -IsMultipathEnabled $true -
TargetPortalAddress $TargetPortalAddress -InitiatorPortalAddress $LocaliSCSIAddress
 -IsPersistent $true}}

#Set the MPIO Policy to Round Robin
Set-MSDSMGlobalDefaultLoadBalancePolicy -Policy RR
```

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



4. 找出未配置的磁碟這是 iSCSI LUN。在此範例中，磁碟 1 是 iSCSI 磁碟。它處於離線狀態。



將游標置於磁碟 1 上方，然後按一下滑鼠右鍵，然後選擇「線上」，使磁碟區上

> **Note**
>
> 您可以修改儲存區域網路 (SAN) 原則，讓新磁碟區自動上線。如需詳細資訊，請參閱 Microsoft 視窗伺服器命令參考中的 SAN 原則。

5. 若要初始化磁碟，請將游標放在磁碟 1 上按一下滑鼠右鍵，然後選擇「初始化」 這時系統顯示「初始化」 選擇確定初始化磁碟。
6. 像平常一樣格式化磁盤。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

我們提供了一個指令碼來檢查您的 iSCSI 設定是否已正確設定。此指令碼會檢查參數，例如工作階段計數、節點分配和多重路徑 I/O (MPIO) 狀態。下列工作說明如何安裝和使用指令碼。

若要驗證您的 iSCSI 組態

1. 開啟視窗 PowerShell 視窗。
2. 使用以下命令下載腳本。

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

3. 使用下列命令展開 zip 檔案。

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

4. 使用下列命令執行指令碼。

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

5. 檢閱輸出以瞭解組態的目前狀態。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.

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
```

將 FSx 與其他服務搭配使用 AWS

除了 Amazon EC2 之外，您還可以搭配磁碟區使用其他 AWS 服務來存取資料。

主題

- 將 Amazon WorkSpaces 與 FSx 一起使用 ONTAP
- 搭配 FSx 搭配 ONTAP 使用 Amazon 彈性容器服務
- 將 VMware 雲端與 FSx 搭配使用

將 Amazon WorkSpaces 與 FSx 一起使用 ONTAP

FSx for ONTAP 可以與 Amazon 一起使用， WorkSpaces 以提供共享的網絡連接存儲（NAS）或存儲 Amazon 帳戶的漫遊配置文件。 WorkSpaces 透過 WorkSpaces 執行個體連線至 SMB 檔案共用之後，使用者就可以在檔案共用上建立和編輯檔案。

下列程序說明如何將 Amazon FSx 與 Amazon WorkSpaces 搭配使用，提供漫遊設定檔和主資料夾存取一致的體驗，並為 Windows 和 Linux 使用 WorkSpaces 者提供共用團隊資料夾。如果您是 Amazon 的新手 WorkSpaces，可以按照 Amazon WorkSpaces 管理指南中的 WorkSpaces 快速設置入門中的說明創建您的第一個 Amazon WorkSpaces 環境。

主題

- 提供漫遊設定檔支援
- 提供共用資料夾以存取常用檔案

提供漫遊設定檔支援

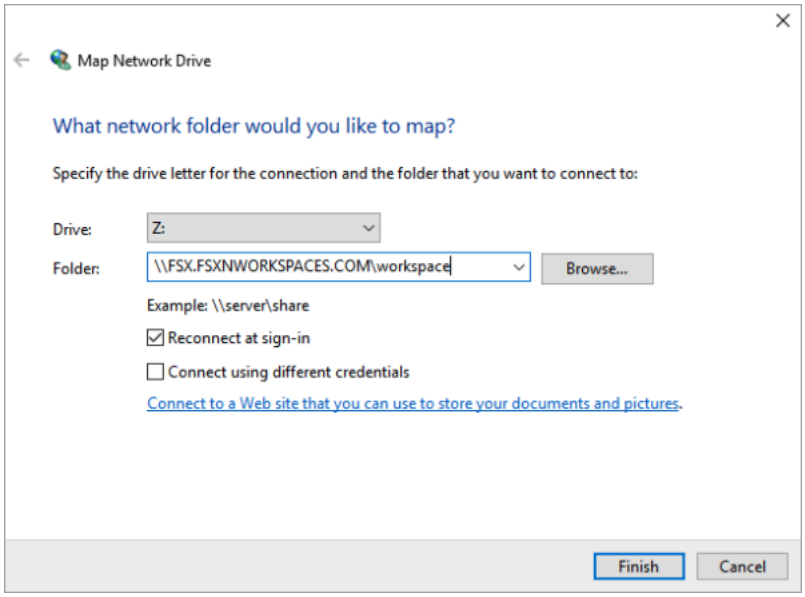
您可以使用 Amazon FSx 為組織中的使用者提供漫遊設定檔支援。使用者將擁有僅存取其漫遊設定檔的權限。資料夾將會使用使用中的目錄群組原則自動連線。使用漫遊設定檔時，使用者登出 Amazon FSx 檔案共用時會儲存使用者的資料和桌面設定，以便在不同的 WorkSpaces 執行個體之間共用文件和設定，並使用 Amazon FSx 每日自動備份自動備份來自動備份。

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 主控台為 ONTAP 檔案系統建立 FSx。如需詳細資訊，請參閱若要建立檔案系統 (主控台)。

   > **Important**
   >
   > ONTAP 檔案系統的每個 FSx 都有一個端點 IP 位址範圍，可從中建立與檔案系統相關聯的端點。對於異地同步備份檔案系統，適用於 ONTAP 的 FSx 會從 198.19.0.0/16 中選擇預設的未使用 IP 位址範圍作為端點 IP 位址範圍。此 IP 位址範圍也可用 WorkSpaces 於管理流量範圍，如《Amazon 管理指南》中的《IP 位址和連接埠需求 WorkSpaces 》 WorkSpaces中所述。因此，若要從 ONTAP 檔案系統存取異地同步備份 FSX WorkSpaces，您必須選取與 198.19.0.0/16 不重疊的端點 IP 位址範圍。

2. 如果您沒有將儲存區虛擬機器 (SVM) 加入至作用中目錄，請立即建立一個虛擬機器。例如，您可以佈建名為的 SVM，`fsx`並將NTFS安全性樣式設定為。如需詳細資訊，請參閱建立儲存區虛擬機器 (主控台)。
3. 為您的 SVM 建立磁碟區。例如，您可以建立名為的磁碟區，`fsx-vol`該磁碟區會繼承 SVM 根磁碟區的安全性樣式。如需詳細資訊，請參閱若要建立FlexVol磁碟區 (主控台)。
4. 在磁碟區上建立 SMB 共用。例如，您可以在磁碟區`workspace`上建立名為的共用`fsx-vol`，並在其中建立名為的資料夾`profiles`。如需詳細資訊，請參閱管理中小企業股。
5. 從執行 Windows 伺服器的 Amazon EC2 執行個體或從. WorkSpace 如需詳細資訊，請參閱存取資料。
6. 您可以將您的共用`Z:\`對應到 Windows WorkSpaces 執行個體上：



步驟 2：將 ONTAP 檔案共用的 FSx 連結至使用者帳戶

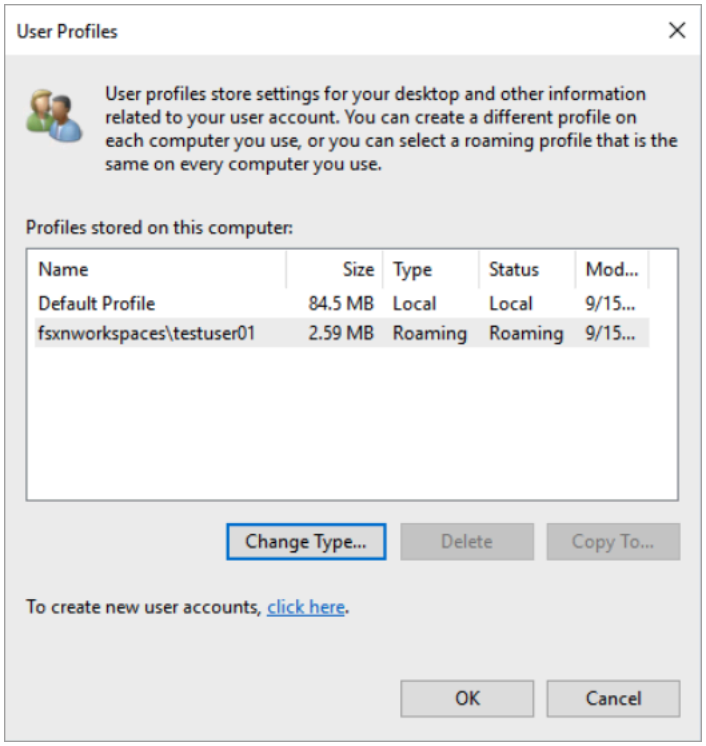
1. 在您的測試使用者上 WorkSpace，選擇「視窗」>「系統」>「進階系統設定」。
2. 在 [系統內容] 中，選取 [進階] 索引標籤並按 [使用者設定檔] 區段中的 [設定] 按鈕 登入的使用者的設定檔類型為。`Local`
3. 從登出測試使用者 WorkSpace。
4. 將測試使用者設定為在 Amazon FSx 檔案系統上擁有漫遊設定檔。在管理員中 WorkSpaces，開啟 PowerShell 主控台並使用類似下列範例的命令 (它會使用您先前在步驟 1 中建立的`profiles`資料夾)：

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

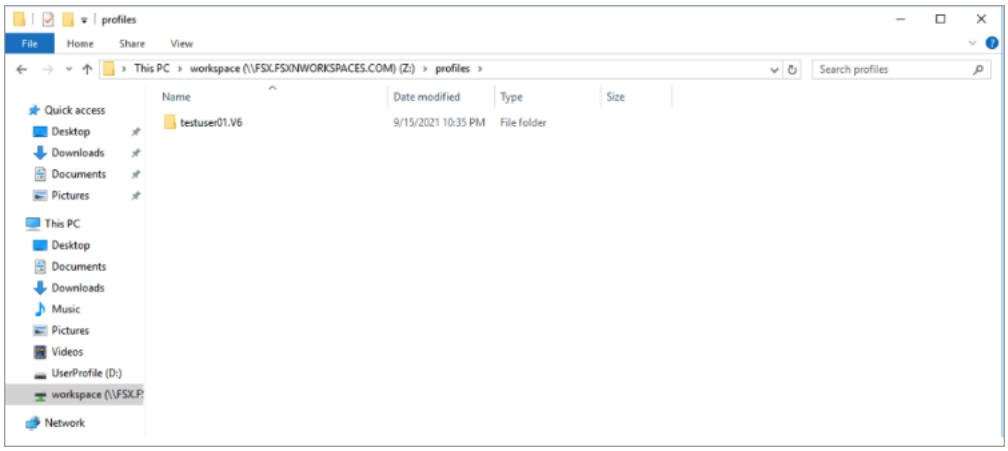
   例如：

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

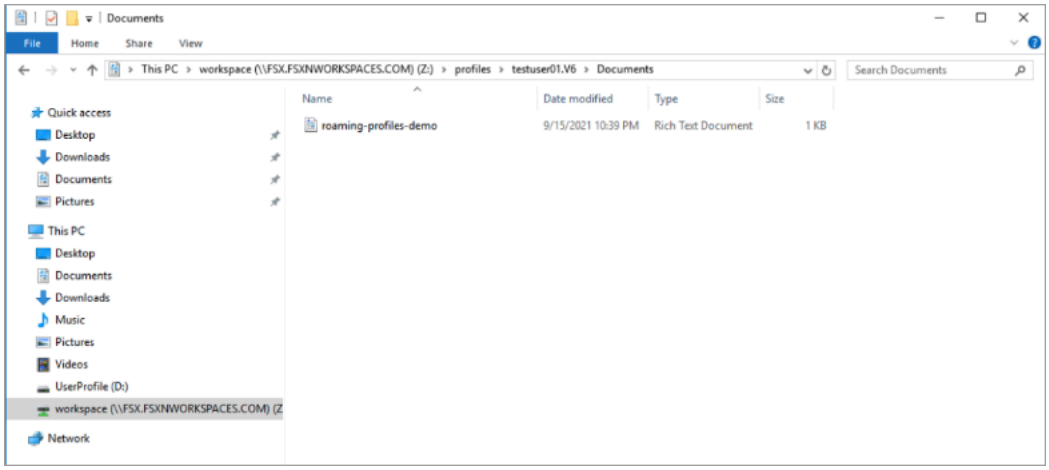
5. 登入測試使用者 WorkSpace。
6. 在 [系統內容] 中，選取 [進階] 索引標籤並按 [使用者設定檔] 區段中的 [設定] 按鈕 登入的使用者的設定檔類型為。`Roaming`



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



8. 在測試用戶的文件`Documents`夾中創建文檔
9. 從他們的測試使用者登出 WorkSpace。
10. 如果您以測試使用者的身分重新登入並瀏覽至他們的設定檔存放區，您將會看到您建立的文件。

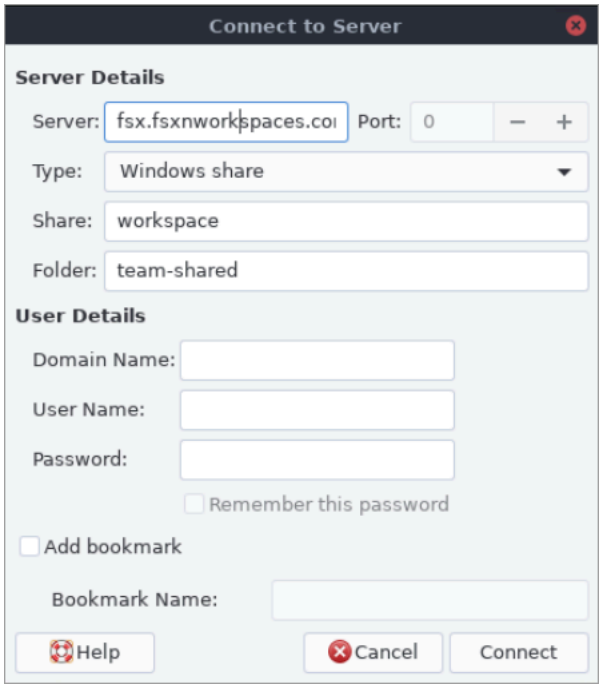


提供共用資料夾以存取常用檔案

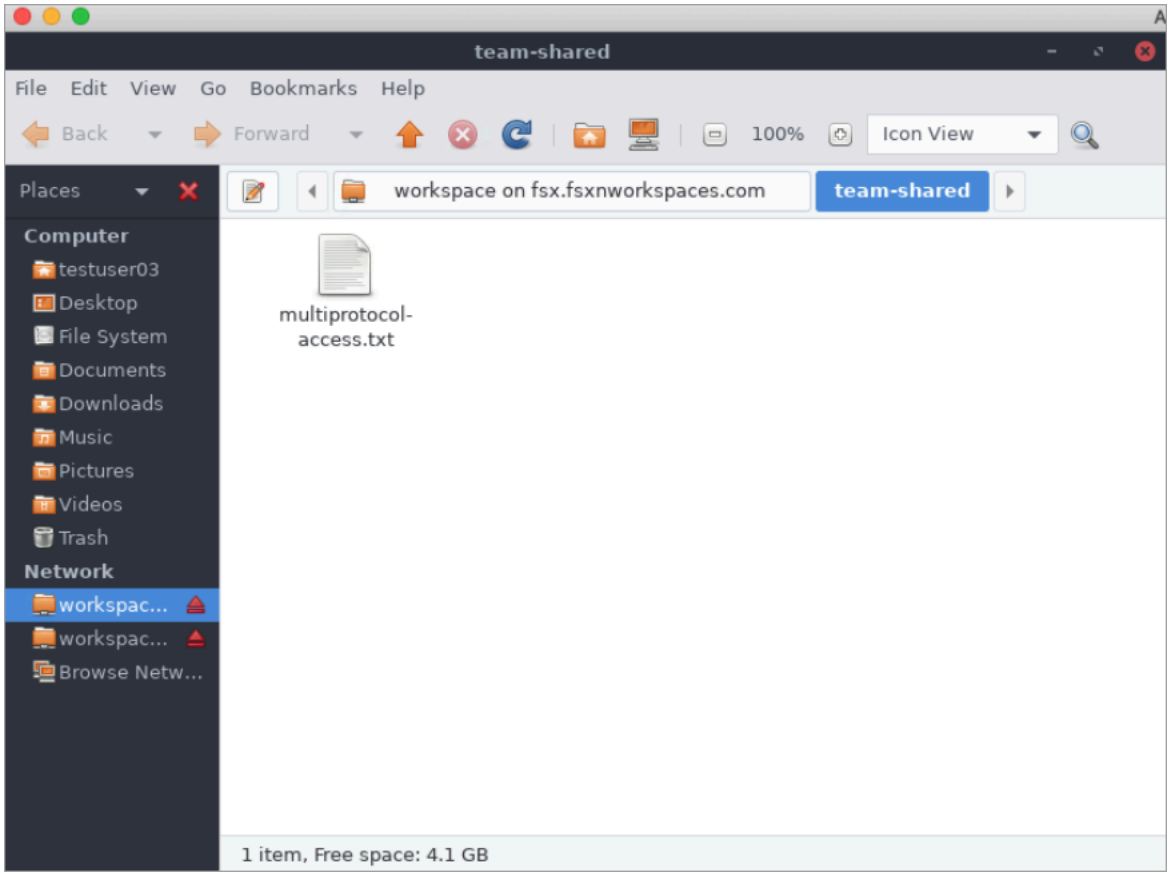
您可以使用 Amazon FSx 為組織中的使用者提供共用資料夾。共用資料夾可用來儲存使用者社群所使用的檔案，例如所有使用者所需的示範檔案、程式碼範例和說明手冊。一般而言，您有針對共用資料夾對應的磁碟機；不過，因為對應磁碟機會使用字母，因此您可以擁有的共用數目有限制。此程序會建立 Amazon FSx 共用資料夾，不需要磁碟機代號即可使用，讓您在指派共用給團隊時有更大的彈性。

若要從 Linux 和視窗掛載共用資料夾以進行跨平台存取 WorkSpaces

1. 從工作列中，選擇「位置」>「Connect 至伺服器」。
   a. 對於「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 而言 WorkSpace，如果您的 Linux 與 Amazon FSx 共享位於相同的網域，WorkSpace 則不需要輸入使用者詳細資訊。
   f. 選擇連線。



2. 建立連線之後，您可以`team-shared`在 SMB 共用中看到名為的共用資料夾 (在此範例中命名) `workspace`。



搭配 FSx 搭配 ONTAP 使用 Amazon 彈性容器服務

您可以從 Amazon EC2 Linux 或 Windows 執行個體上的 Amazon Elastic Container Service (Amazon ECS) 碼頭容器存取您的 NetApp ONTAP 檔案系統的亞馬遜 FSx。

安裝在 Amazon ECS Linux 容器

1. 使用適用於 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 彈性容器服務開發人員指南中的建立叢集。
2. 在 EC2 執行個體上建立一個目錄以掛接 SVM 磁碟區，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，將 FSx for ONTAP 磁碟區掛載到 Linux EC2 執行個體上：

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

4. 使用下列指令掛接磁碟區：

   ```
   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-01234567890abdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /
   fsxontap
   ```

   您也可以使用 SVM 的 IP 位址 SVM，而不是它的 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 容器定義中新增下列屬性`volumes`和`mountPoints`容器屬性。將其取代為適`sourcePath`用於 ONTAP 檔案系統的 FSx 中的掛載點和目錄。

   ```
   {
       "volumes": [
           {
   ```

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

安裝在 Amazon ECS 視窗容器

1. 使用適用於 Windows 容器的 EC2 視窗 + 網路叢集範本建立 ECS 叢集。如需詳細資訊，請參閱 Amazon 彈性容器服務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 視窗叢集，並對應 SMB 共用。

   啟動已加入您使用中目錄網域的 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 全域對應，以便將 SMB 共用對應至磁碟機。替換您的 FSx 檔案系統和共用名稱的 netbios 或 DNS 名稱以下的值。掛接在 Linux EC2 執行個體上的 NFS 磁碟區第 1 卷會在 FSx 檔案系統上設定為 CIFS 共用連結。

   ```
   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 全域對應：

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

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

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

```
        }
    ],
    .
    .
    .
}
```

將 VMware 雲端與 FSx 搭配使用

您可以使用適用於 ONTAP 的 FSx 做為 VMware 雲端上 AWS 軟體定義的資料中心 (SDDC) 的外部資料存放區。如需詳細資訊，請參閱將適用於 NetApp ONTAP 的 Amazon FSX 設定為外部儲存裝置和 VMware 雲端 AWS 與 Amazon FSX (適用於 NetApp ON TAP) 部署指南。

可用性與持久性

Amazon FSx for NetApp ONTAP 使用兩種部署類型：單一可用區和異地同步備份，提供不同層級的可用性和耐久性。本主題說明每種部署類型的可用性和耐久性功能，以協助您選擇適合工作負載的部署類型。如需服務可用性 SLA (服務等級協議) 的相關資訊，請參閱 Amazon FSx 服務水準協議。

主題

選擇檔案系統部署類型

以下各節說明單一可用區和異地同步備份檔案系統部署類型的可用性和耐久性功能。

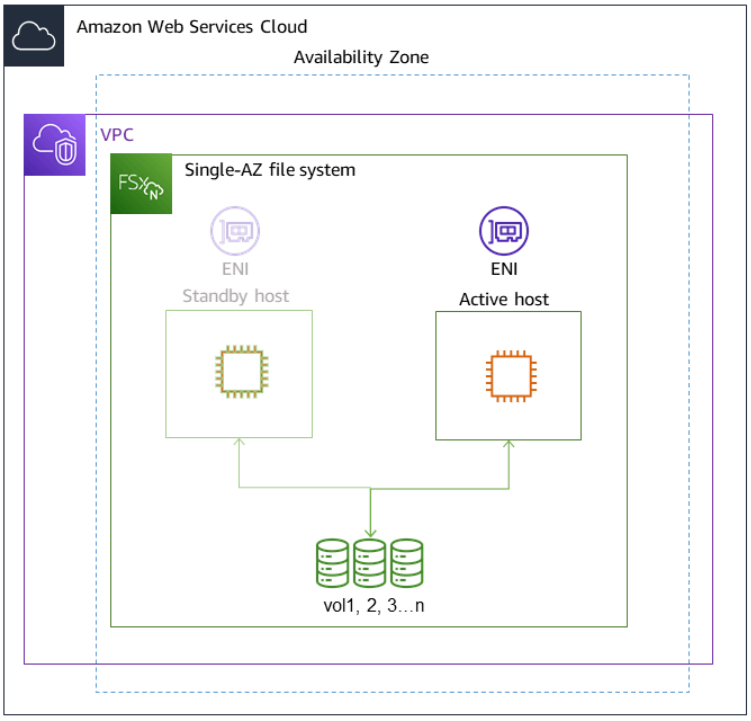
單一可用區部署類型

當您建立單一可用區檔案系統時，Amazon FSx 會在作用中-待命組態中自動佈建一對至十二對檔案伺服器，每對的作用中和待命檔案伺服器都位於中單一可用區域內的個別容錯網域中。 AWS 區域在規劃的檔案系統維護或任何作用中檔案伺服器的意外服務中斷期間，Amazon FSx 會自動且獨立地容錯移轉該高可用性 (HA) 配對到待命檔案伺服器，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替換基礎設施元件。為了達到高耐久性，Amazon FSx 會在可用區域內自動複寫您的資料，以保護資料免於元件故障。此外，您還可以選擇設定檔案系統資料的每日自動備份。這些備份儲存在多個可用區域，以便為所有備份資料提供異地同步備份復原。

單一可用區檔案系統專為不需要異地同步備份檔案系統資料恢復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的解決方案，或者只複寫單一可用區域內的資料 AWS 區域，以儲存在內部部署或其他內部部署中的資料的次要副本。

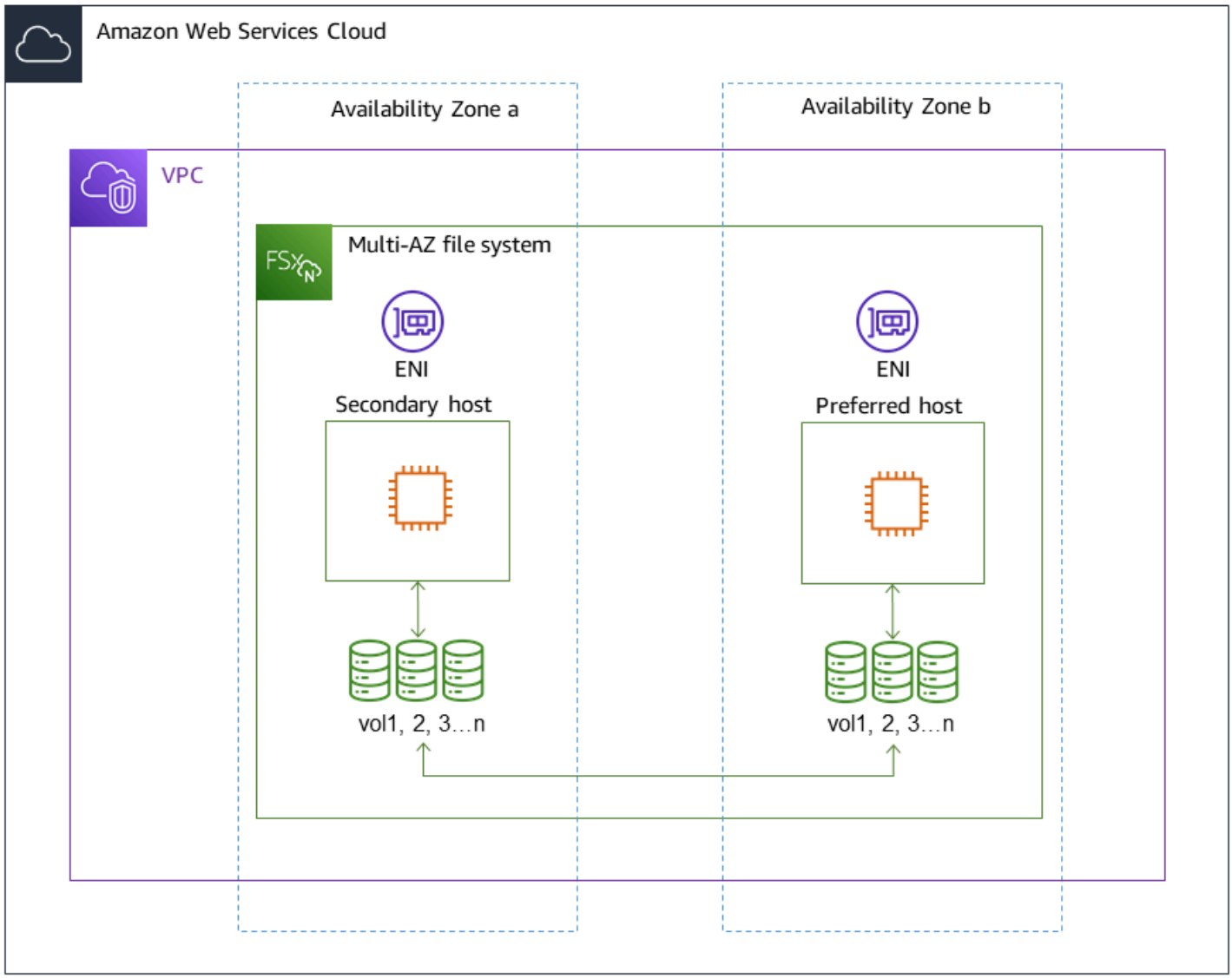
下圖說明 ONTAP 單一可用區檔案系統的 FSx 架構。



異地同步備份部署型

異地同步備份檔案系統支援單一可用區檔案系統的所有可用性和耐久性功能。此外，即使在可用區域無法使用的情況下，它們也能為資料提供持續可用性。異地同步備份部署具有單一 HA 對檔案伺服器，待命檔案伺服器部署在與作用中檔案伺服器不同 AWS 區域的可用區域中。寫入檔案系統的任何變更都會跨可用區域同步複寫到待命區域。

異地同步備份檔案系統專為使用案例而設計，例如需要高可用性才能共用 ONTAP 檔案資料，並且需要跨可用區域內建複寫進行儲存的關鍵業務生產工作負載。下圖說明 ONTAP 異地同步備份檔案系統的 FSx 架構。



適用於 ONTAP 的 FSx 的容錯移轉程序

如果發生下列任何一種情況，單一可用區和異地同步備份檔案系統會自動容錯移轉指定的 HA 配對，從慣用或作用中的檔案伺服器到待命檔案伺服器：

- 首選或活動的文件服務器變為不可用
- 檔案系統的輸送量容量已變更
- 偏好或使用中的檔案伺服器會經過計劃的維護
- 發生可用區域中斷 (僅異地同步備份檔案系統)

> **Note**
>
> 對於向外延展檔案系統，每個 HA 配對的容錯移轉行為都是獨立的。如果某個 HA 配對的偏好檔案伺服器無法使用，則只有該 HA 配對會容錯移轉至其待命檔案伺服器。

當從某個檔案伺服器容錯移轉至另一個檔案伺服器時，新的使用中檔案伺服器會自動開始為該 HA 配對提供所有檔案系統讀取和寫入要求。對於異地同步備份檔案系統，當偏好的檔案伺服器完全復原並可用時，Amazon FSx 會自動故障回復，容錯回復通常在 60 秒內完成。對於單一同步備份和異地同步備份檔案系統，容錯移轉通常在 60 秒內完成，從偵測到使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。由於用戶端透過 NFS 或 SMB 存取資料時所使用的端點 IP 位址保持不變，因此容錯移轉對 Linux、Windows 和 macOS 應用程式而言是透明的，這些應用程式會繼續執行檔案系統作業，而無需手動介入。

若要確保針對 ONTAP 單一可用區和異地同步備份檔案系統連線到 FSx 的用戶端，容錯移轉是透明的，請參閱。從內部存取資料 AWS

在檔案系統上測試容錯移轉

您可以修改其輸送量容量，在向上擴充的檔案系統上測試容錯移轉。修改檔案系統的輸送量容量時，Amazon FSx 會依序切換檔案系統的檔案伺服器。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，檔案系統會自動故障回到新的主要伺服器，而 Amazon FSx 則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。如需修改檔案系統輸送量容量和監視要求進度的詳細資訊，請參閱管理輸送量容量。

網路資源

本節說明單一可用區和異地同步備份檔案系統所耗用的網路資源。

子網

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在其中建立檔案系統的可用區域。建立異地同步備份檔案系統時，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的不同 AWS 區域可用區域中。如需有關 Amazon VPC 的詳細資訊，請參閱什麼是 Amazon V PC？ 在 Amazon Virtual Private Cloud 用戶指南中。

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

文件系统弹性网络接口

對於單一可用區檔案系統，Amazon FSx 會在您與檔案系統關聯的子網路中佈建兩個彈性網路界面 (ENI)。對於異地同步備份檔案系統，Amazon FSx 還佈建兩個 ENI，每個與檔案系統關聯的子網路中各一個。用戶端會使用 elastic network interface 與您的 Amazon FSx 檔案系統進行通訊。雖然網路界面屬於您帳戶 VPC 的一部分，但仍視為 Amazon FSx 的服務範圍內。異地同步備份檔案系統使用浮動網際網路通訊協定 (IP) 位址，以便連線的用戶端在容錯移轉事件期間順暢地在偏好和待命檔案伺服器之間

> **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 與檔案系統之間的連線永久中斷。
> - 與檔案系統相關聯的彈性網路介面會自動建立路由，並將其新增至預設 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 ONTAP 檔案系統部署類型之每個 FSx 的子網路、elastic network interface 和 IP 位址資源：

	單一可用區 (向上擴充)	單一可用區 (向外擴充)	異地同步備份 (向上擴充)
子網路數目	1	1	2
彈性網路介面數	2	每 HA 對 2 個	2
每個 ENI 的 IP 位址數	1 + 檔案系統中的 SVM 數量	HA 配對計數 + HA 配對計數乘以檔案系統中的 SVM 數目	1 + 檔案系統中的 SVM 數量

	單一可用區 (向上擴充)	單一可用區 (向外擴充)	異地同步備份 (向上擴充)
VPC 路由表路由數量	N/A	N/A	1 + 檔案系統中的 SVM 數量

建立檔案系統或 SVM 之後，在刪除檔案系統之前，其 IP 位址不會變更。

> **Important**
>
> Amazon FSx 不支援從公用網際網路存取檔案系統或公開檔案系統。Amazon FSx 會自動分離任何可從網際網路存取的公有 IP 位址 (連接至檔案系統的彈性網路界面) 的彈性 IP 位址。

管理儲存容量

Amazon FSx for NetApp ONTAP 提供許多儲存相關功能，可讓您用來管理檔案系統上的儲存容量。

主題

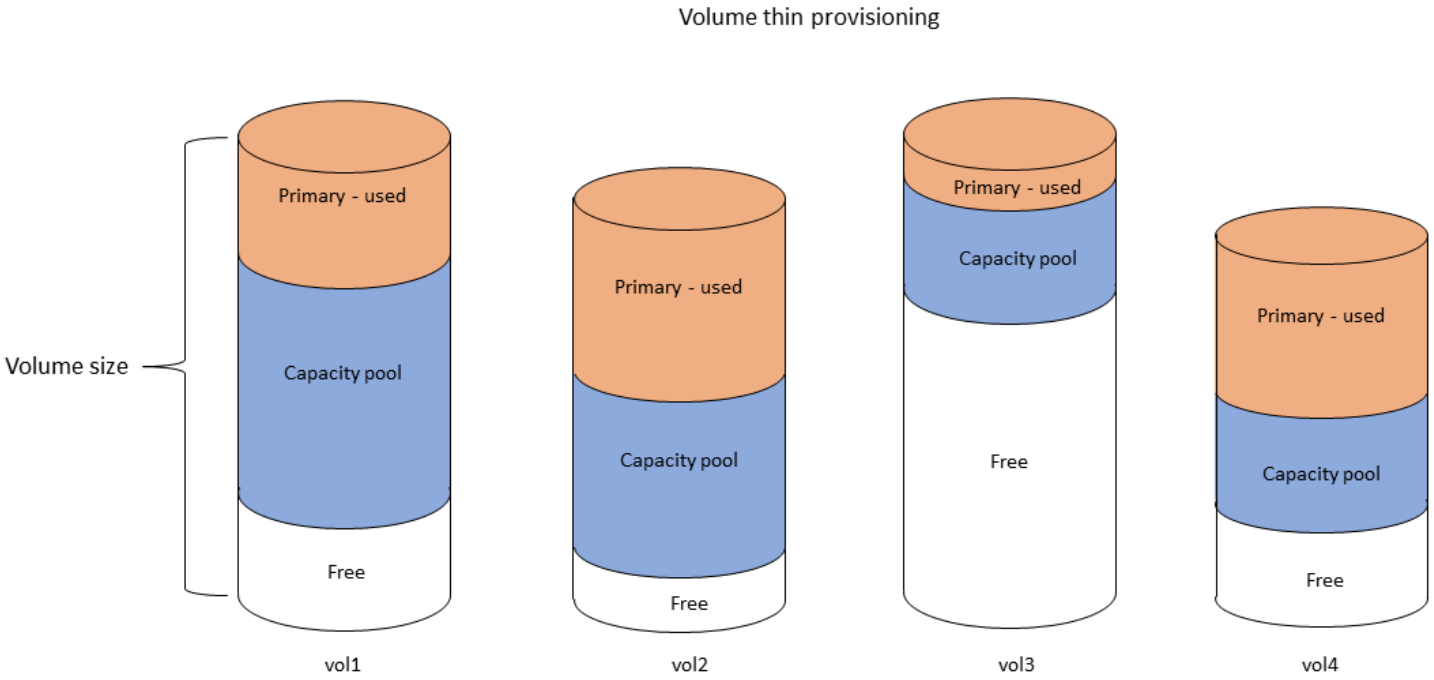
適用於 ONTAP 儲存層的 FSx

儲存層是適用於 NetApp ONTAP 檔案系統之 Amazon FSx 的實體儲存媒體。適用於 ONTAP 的 FSx 提供下列儲存層：

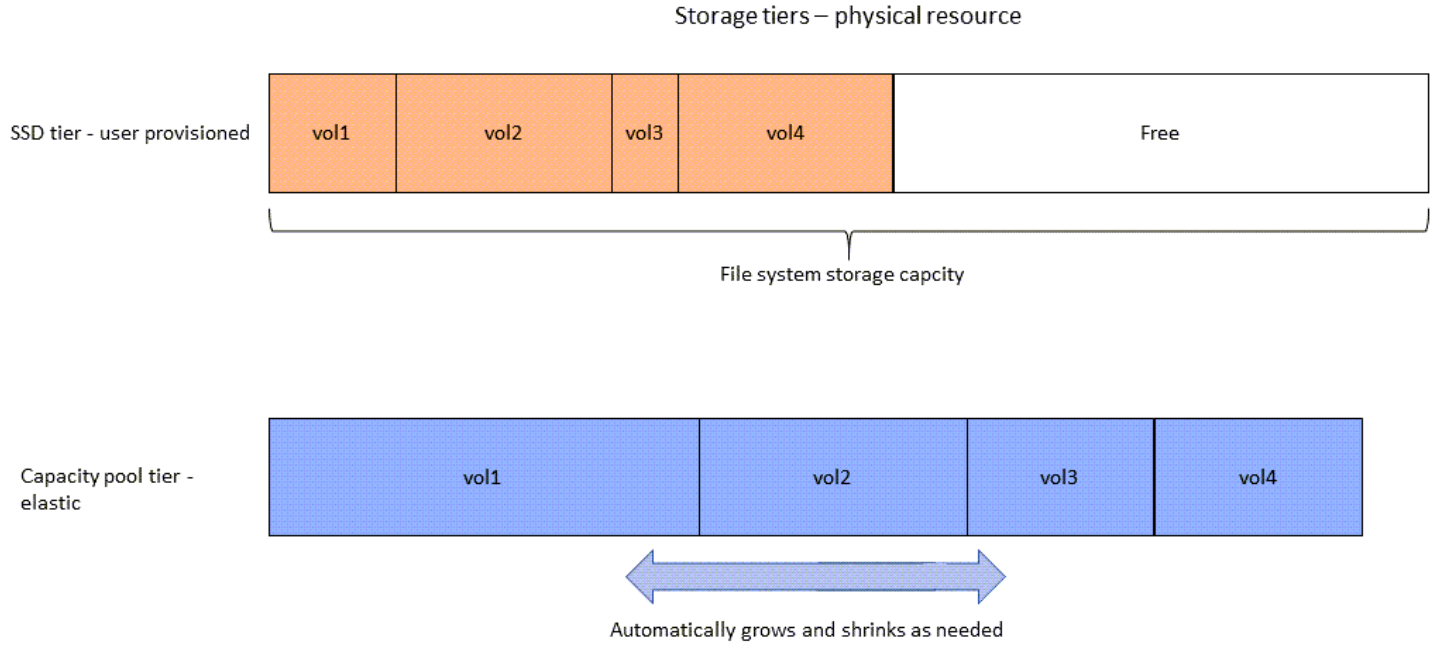
- SSD 層：使用者佈建的高效能固態硬碟 (SSD) 儲存裝置，專為資料集的使用中部分而打造。
- 容量集區層：全彈性儲存裝置，可自動擴充至 PB 規模，並針對不常存取的資料進行成本最佳化。

ONTAP 磁碟區的 FSx 是一種虛擬資源，與資料夾類似，不會消耗儲存容量。您儲存的資料 (以及消耗實體儲存空間) 存放在磁碟區內。當您建立磁碟區時，您可以指定磁碟區的大小 — 您可以在建立磁碟區後進行修改。適用於 ONTAP 磁碟區的 FSx 是精簡佈建的，且不會事先保留檔案系統儲存。而是視需要動態配置 SSD 和容量集區儲存。您在磁碟區層級設定的分層原則會決定儲存在 SSD 層中的資料是否以及何時轉換至容量集區層。

下圖說明針對檔案系統中 ONTAP 磁碟區在多個 FSx 上配置的資料範例。



下圖說明上圖中四個磁碟區中的資料如何使用檔案系統的實體儲存容量。



您可以選擇最符合檔案系統上每個磁碟區需求的分層原則，以降低儲存成本。如需詳細資訊，請參閱磁碟區資料分層。

選擇適當的檔案系統 SSD 儲存容量

為 FSx for ONTAP 檔案系統選擇固態硬碟儲存容量時，您需要謹記下列事項，這些事項會影響可用於儲存資料的 SSD 儲存容量：

- 保留給 NetApp ONTAP 軟體開銷的儲存容量。
- 文件元數據
- 最近寫入的資料
- 您打算儲存在 SSD 儲存裝置上的檔案，無論是尚未達到冷卻期間的資料，還是您最近讀取的資料已擷取回 SSD。

SSD 儲存裝置的使用方式

您檔案系統的 SSD 儲存空間會用於 NetApp ONTAP 軟體 (額外負荷)、檔案中繼資料和資料的組合。

NetApp ONTAP 软件开销

與其他 NetApp ONTAP 檔案系統一樣，最多 16% 的檔案系統 SSD 儲存容量會保留用於 ONTAP 額外負荷，這表示它無法用於儲存您的檔案。ONTAP 開銷的分配方式如下：

- 11% 保留給 NetApp ONTAP 軟體使用。對於具有 30 TB 以上 SSD 儲存容量的檔案系統，將保留 6%。
- 5% 會保留給彙總快照，這是同步兩個檔案系統檔案伺服器之間的資料所需的彙總快照。

文件元數據

文件元數據通常消耗文件所消耗的存儲容量的 3-7%。這個百分比取決於平均檔案大小 (較小的平均檔案大小需要較多的中繼資料)，以及節省檔案的儲存空間效率。請注意，檔案中繼資料不會因為節省儲存效率而受益。您可以使用下列準則來估算檔案系統中繼資料使用的 SSD 儲存容量。

平均檔案大小	中繼資料大小 (以檔案資料的百分比表示)
4 KB	7%
8 KB	3.5%
32 KB 或更大	1-3%

針對您計劃在容量集區層上儲存的檔案中繼資料調整所需的 SSD 儲存容量大小時，我們建議您針對計劃儲存在容量集區層上的每 10 GiB 資料，使用 1 GiB SSD 儲存的保守比例。

儲存在 SSD 層的檔案資料

除了使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一開始都會寫入 SSD 層，然後才會連結至容量集區儲存體。無論磁碟區的分層政策為何，都是如此，但使用傳輸資料 SnapMirror 至已設定所有資料分層政策的磁碟區除外。

只要 SSD 層使用率低於 90%，就會在 SSD 層中快取容量集區層的隨機讀取。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

我們建議您持續不要超過 SSD 儲存層的 80% 使用率。對於向外延展檔案系統，我們還建議您持續不要超過任何檔案系統彙總的 80% 使用率。這些建議與對 ONTAP NetApp 的建議一致。由於檔案系統的 SSD 層也可用於容量集區層的暫存寫入，以及從容量集區層隨機讀取，因此存取模式的任何突然變更都會快速導致 SSD 層的使用率增加。

在 90% SSD 使用率下，從容量集區層讀取的資料不會再快取至 SSD 層，因此任何寫入檔案系統的新資料都會保留剩餘的 SSD 容量。這會導致從容量集區層重複讀取相同的資料，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 層使用率達到或高於 98% 時，所有分層功能都會停止。如需詳細資訊，請參閱 分層臨界值。

提供 ONTAP 儲存效率的 FSx

NetApp ONTAP 提供區塊層級的儲存效率功能，包括壓縮、壓縮和重複資料刪除功能，可為一般檔案共用節省高達 65% 的儲存容量，而不會犧牲效能。

適用於 NetApp ONTAP 的 Amazon FSx 也支援其他 ONTAP 功能，可為您節省空間，包括快照、精簡佈建和磁碟區。 FlexClone

儲存效率功能預設不會啟用。您可以啟用它們，如下所示：

- 當您建立檔案系統時，在 SVM 的根磁碟區上。
- 當您建立新磁碟區時。
- 修改現有磁碟區時。

若要檢視啟用儲存效率的檔案系統上節省的儲存空間量，請參閱檢視節省的儲存效率。

計算節省儲存效率

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. FlexClones 這些量度具有單一維度FileSystemId。如需詳細資訊，請參閱 檔案系統度量。

- 若要計算以位元組為單位的StorageUsed儲存體效率節省，請取指定期間內的平均值，並從相同期間的LogicalDataStored平均值中減去。
- 若要以邏輯資料總大小的百分比計算儲存效率節省的情況，請取Average出指定StorageUsed時段內的指定期間，然後從相Average同期間減去。LogicalDataStored然後在同一時期除LogicalDataStored以差異。Average

SSD 固態硬碟大小

假設您要為不常存取 80% 資料的應用程式儲存 100 TiB 的資料。在這個案例中，80% (80 TB) 的資料會自動分層至容量集區層，而剩餘的 20% (20 TB) 則會保留在 SSD 儲存體中。基於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 的固態硬碟儲存容量，以儲存 20 TiB 的主動存取資料。您佈建的 SSD 儲存容量也必須將 ONTAP 軟體儲存額外負荷納入 16%，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 儲存裝置。對於剩餘的 80 TiB 不常存取的資料，您也將使用 28 TiB 的容量集區儲存體。

檔案系統儲存容量與 IOPS

當您建立適用於 ONTAP 檔案系統的 FSx 時，您必須指定 SSD 層的儲存容量。對於向外延展檔案系統，您指定的儲存容量會平均分散在每個高可用性 (HA) 配對的儲存池中；這些儲存集區稱為彙總。

對於您佈建的每個 GiB SSD 儲存，Amazon FSx 會為檔案系統自動佈建每秒 3 個 SSD 輸入/輸出作業 (IOPS)，每個檔案系統最多可達 160,000 個 SSD IOPS。對於向外延展檔案系統，SSD IOPS 會平均分散在每個檔案系統的彙總中。您可以選擇在每 GiB 的自動 3 SSD IOPS 之上，指定佈建的固態硬碟 IOPS 等級。如需有關可為 FSx 佈建 ONTAP 檔案系統之最大固態硬碟 IOPS 數目的詳細資訊，請參閱。輸送量容量對效能的影響

主題

更新檔案系統固態硬碟儲存和 IOPS

當您需要為資料集的使用中部分提供額外儲存空間時，可以增加適用於 NetApp ONTAP 檔案系統的 Amazon FSx 固態硬碟儲存容量。使用 Amazon FSx 主控台、Amazon FSx API 或 AWS Command Line Interface (AWS CLI) 來增加固態硬碟儲存容量。如需詳細資訊，請參閱 修改 SSD 儲存容量和佈建的 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 儲存容量可供您使用之後，我們會向您收費。如需有關定價的詳細資訊，請參閱 Amazon FSx 瞭解 NetApp ONTAP 定價資訊。

增加儲存容量後，Amazon FSx 會在背景執行儲存優化程序，以重新平衡資料。對於大多數檔案系統而言，儲存最佳化需要幾個小時，而且對工作負載效能的明顯影響最小。

您可以隨時使用 Amazon FSx 主控台、CLI 和 API 追蹤儲存優化程序的進度。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 時需要考量的幾個重要事項：

- 儲存容量只會增加 — 您只能增加檔案系統的 SSD 儲存容量；您無法降低儲存容量。
- 儲存容量下限增加 — 每次增加 SSD 儲存容量必須至少為檔案系統目前 SSD 儲存容量的 10%，最多可達到檔案系統組態的最大 SSD 儲存容量。
- (僅限向外延展) 儲存容量分攤 — 您為檔案系統選擇的新儲存容量或 SSD IOPS 會平均分散在每個檔案系統的彙總中。
- 間隔時間增加 — 在修改 SSD 儲存容量、佈建 IOPS 或檔案系統的輸送量容量之後，您必須等待至少六個小時，才能再次在相同檔案系統上修改這些組態。這有時被稱為冷卻時間。

- 佈建 IOPS 模式 — 對於佈建的 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 固態硬碟儲存容量 3 個佈建的固態硬碟 IOPS，最高可達您檔案系統組態的最大 SSD IOPS。

    > **Note**
    >
    > 如需有關可為 FSx 佈建 ONTAP 檔案系統之最大固態硬碟 IOPS 數目的詳細資訊，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 的數目，其數目必須大於或等於每 GiB 的 SSD 儲存容量 3 IOPS。如果您選擇佈建較高層級的 IOPS，您需要支付該月內佈建率高於包含費率的平均 IOPS 費用，以 IOPS 月為單位。

如需有關定價的詳細資訊，請參閱 Amazon FSx 瞭解 NetApp ONTAP 定價資訊。

何時增加 SSD 儲存容量

如果您的可用 SSD 層儲存空間不足，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 層對於資料集的使用中部分而言已經過小。

若要監控檔案系統上可用的可用儲存空間量，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 監控 CloudWatch。

> **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，並且有容量可供其他資料使用。對於向外延展檔案系統，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。

如需檔案系統 SSD 儲存體的使用方式，以及為檔案中繼資料和作業軟體保留多少 SSD 儲存空間的詳細資訊，請參閱選擇適當的檔案系統 SSD 儲存容量。

監控 SSD 儲存使用率

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。 CloudWatch 您可以使用 Amazon 監控儲存容量使用率，並設定警示，以便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 80% 的儲存容量使用率。這樣可以確保正確分層功能，並為新數據提供開銷。如果您的 SSD 儲存層持續高於 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 更新檔案系統固態硬碟儲存和 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。可用的 SSD 儲存容量圖表顯示一段時間內檔案系統上可用的 SSD 儲存容量。儲存區分佈圖顯示檔案系統的整體儲存容量目前如何分佈在 3 個類別上：

- 容量集區層
- 固態硬碟層級-可用
- 固態硬碟層-已使用

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

監控檔案系統可用的 SSD 階層儲存容量 (主控台)

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 在左側導覽欄中選擇 [檔ONTAP案系統]，然後選擇您要檢視其儲存容量資訊的檔案系統。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 [儲存空間]。顯示每個彙總圖形的可用主要儲存容量和儲存容量使用率。

建立檔案系統儲存容量使用率警示

建議您持續不要超過平均 SSD 儲存容量使用率 80%。有時 SSD 儲存使用率峰值高於 80% 是可以接受的。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空間，而不會遇到問題。下列程序說明如何建立 CloudWatch 警示，以便在檔案系統的 SSD 儲存使用率接近 80% 時發出警示。

建立檔案系統 SCU 警示

您可以使用`StorageCapacityUtilization`量度建立警示，當 ONTAP 檔案系統的一或多個 FSx 達到儲存使用率閾值時觸發。

1. 開啟主 CloudWatch 控台，網址為 https://console.aws.amazon.com/cloudwatch/。

2. 在左側導覽窗格的 [警報] 下，選擇 [所有鬧鐘]。然後，選擇「建立鬧鐘」。在「建立警示」精靈中，選擇 「選取量度」。
3. 在圖形總管中，選擇多重來源查詢索引標籤。
4. 在查詢建置器中，選擇下列項目：

   - 針對「命名空間」，選取 AWS/FSx > 詳細的檔案系統測量結果。
   - 對於「測量結果名稱」，選取 MAX (StorageCapacityUtilization)。
   - 對於「篩選依據」，您可以選擇性地依據其 ID 包含或排除特定檔案系統。如果您將 [篩選依據] 保留空白，當任何檔案系統超過警示的儲存容量使用率閾值時，就會觸發警示。
   - 將其餘選項保留空白，然後選擇「圖形查詢」。
5. 選擇選取指標。回到精靈的「度量」區段中，為您的量度提供「標籤」。我們建議將期限保持在 5 分鐘。
6. 在「條件」下，選擇「靜態」臨界值類型 (每當您的量度大於/等於 80 時)。
7. 選擇「下一步」以移至「設定動作」 頁面。

若要設定警示動作

您可以設定各種動作，讓警報在達到您設定的閾值時觸發。在此範例中，我們選擇了 Simple Notification Service (SNS) 主題，但您可以在 Amazon 使用 CloudWatch 者指南中的使用 Amazon CloudWatch 警示中了解其他動作。

1. 在「通知」區段中，選擇要在警示處於ALARM狀態時通知的 SNS 主題。您可以選擇現有主題或建立新主題。您將收到訂閱通知，您必須先確認，然後才會收到電子郵件地址的警報通知。
2. 選擇下一步。

完成鬧鐘

請依照下列指示完成建立 CloudWatch 鬧鐘的程序。

1. 在 [新增名稱和說明] 頁面上，提供警示名稱，並選擇性地提供說明，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 [建立鬧鐘]。

檢視節省的儲存效率

啟用後，您可以在 Amazon FSx 主控台、Amazon 主控台和 ONTAP CloudWatch CLI 中查看節省了多少儲存容量。

若要檢視節省的儲存效率 (主控台)

針對用於 ONTAP 檔案系統的 FSx 主控台，Amazon FSx 主控台顯示的儲存效率節省成本包括和節省的成本。 FlexClones SnapShots

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 從檔案系統清單中選擇您要檢視儲存效率節省的 ONTAP 檔案系統 FSx。
3. 在檔案系統詳細資料頁面的第二個面板上，選擇 [監視與效能] 索引標籤中的 [摘要]。
4. 儲存空間效率節省圖表會顯示您以邏輯資料大小的百分比和實體位元組來節省多少空間。

若要檢視儲存效率節省 (ONTAPCLI)

您可以看到壓縮、壓縮和重複資料刪除所節省的儲存效率，而不會受到快照的影響，並且FlexClones使用 CLI 執行`storage aggregate show-efficiency`命令。ONTAP如需詳細資訊，請參閱NetApp ONTAP文件中心的儲存彙總顯示效率。

1. 若要存取 NetApp ONTAP CLI，請執行下列命令，在適用於 NetApp ONTAP 檔案系統的 Amazon FSx 管理連接埠上建立安全殼層工作階段。取代*`management_endpoint_ip`*為檔案系統管理連接埠的 IP 位址。

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

   如需詳細資訊，請參閱 使用 ONTAP CLI 管理檔案系統。
2. 該storage aggregate show-efficiency命令顯示有關所有聚合的存儲效率的信息。存儲效率顯示在四個不同級別：

   - 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
```

修改 SSD 儲存容量和佈建的 IOPS

您可以增加檔案系統的 SSD 儲存，並使用 Amazon FSx 主控台、和 API 來增加或減少佈建 SSD IOPS 的 AWS CLI數量。

更新檔案系統 (主控台) 的 SSD 儲存容量或佈建的 IOPS

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檔案系統。在 [檔案系統] 清單中，選取您要更新固態硬碟儲存容量和 SSD IOPS 的 ONTAP 檔案系統的 FSx。
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 儲存容量值旁邊的 [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 (2,048 GiB per HA pair)	4,506 GiB (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：
   - 若要以目前值的百分比變更方式輸入新的 SSD 儲存容量，請選擇 [百分比]。
   - 若要在 GiB 中輸入新值，請選擇「絕對」。
6. 根據輸入類型，輸入「所需增加百分比」的值。
   - 在「百分比」中，輸入增加百分比值。此值必須至少比目前值大 10%。
   - 對於「絕對」，請輸入以 GiB 為單位的新值，最大允許值為 196,608 GiB。
7. 針對佈建的 SSD IOPS，您有兩個選項可以修改檔案系統佈建的 SSD IOPS 數目：
   - 如果您希望 Amazon FSx 自動擴展您的固態硬碟 IOPS，以維持每 GiB 固態硬碟儲存容量 3 個佈建的固態硬碟 IOPS (最多可達 160,000 個)，請選擇「自動」。
   - 如果您要指定 SSD IOPS 的數量，請選擇使用者佈建。輸入 IOPS 的絕對數量，至少是 SSD 儲存層 GiB 數量的三倍，小於或等於 160,000。

> **Note**
>
> 如需有關可為 FSx 佈建 ONTAP 檔案系統之最大固態硬碟 IOPS 數目的詳細資訊，請參閱。輸送量容量對效能的影響

8. 選擇更新。

> **Note**
>
> 提示底部會顯示新 SSD 儲存容量和 SSD IOPS 的組態預覽。對於向外延展檔案系統，也會顯示每個 HA-PAIR 配對的值。

為檔案系統 (CLI) 更新固態硬碟儲存容量和佈建的 IOPS

若要更新適用於 ONTAP 檔案系統之 FSx 的 SSD 儲存容量和佈建的 IOPS，請使用 AWS CLI 命令update-file-system或對等UpdateFileSystem的 API 動作。使用您的值設定下列參數：

- 設定`--file-system-id`為您要更新之檔案系統的 ID。
- 若要增加 SSD 儲存容量，`--storage-capacity`請設定目標儲存容量值，該值必須至少比目前值大 10%。

- 若要修改佈建的 SSD IOPS，請使用內`--ontap-configuration DiskIopsConfiguration`容。此屬性有兩個參數，`Iops`並且`Mode`：
  - 如果您要指定已佈建 IOPS 的數目，請使用 `Iops=`*`number_of_IOPS`* (最多 160,000 個) 和。`Mode=USER_PROVISIONED`IOPS 值必須大於或等於要求之 SSD 儲存容量的三倍。如果您沒有增加儲存容量，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 自動增加您的固態硬碟 IOPS，請使用`Mode=AUTOMATIC`且不要使用此`Iops`參數。Amazon FSx 會針對佈建的固態硬碟儲存容量，每一 GiB 自動維護 3 個固態硬碟 IOPS (最多可達 160,000 個)。

> **Note**
>
> 如需有關可為 FSx 佈建 ONTAP 檔案系統之最大固態硬碟 IOPS 數目的詳細資訊，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 儲存空間增加至 2000 GiB，並將使用者佈建的固態硬碟 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}'
```

若要監視更新進度，請使用指describe-file-systems AWS CLI 令。在輸出中查找`AdministrativeActions`部分。

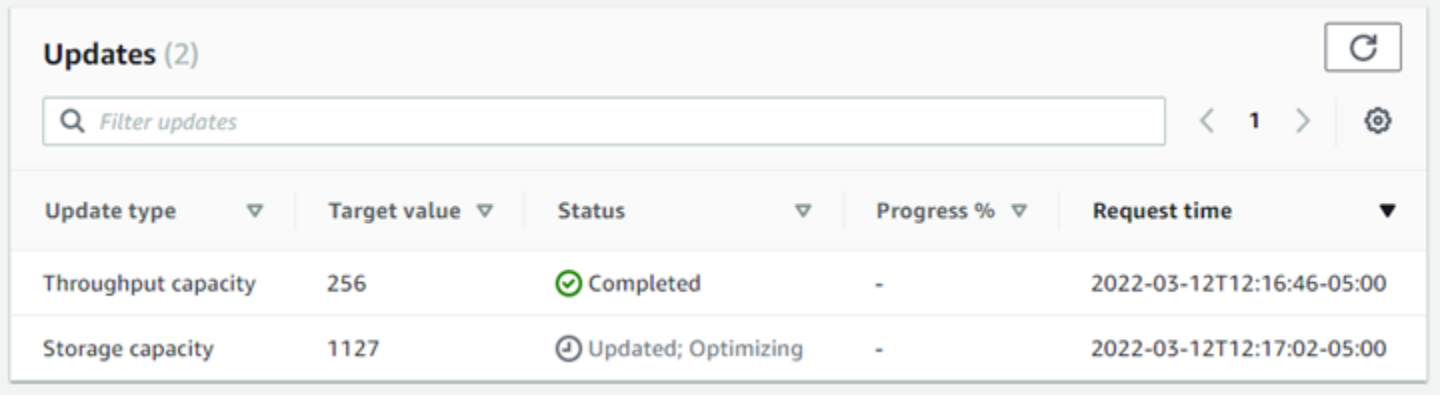
如需詳細資訊，請參閱 Amazon FSx AdministrativeAction中的 NetApp ONTAP API 參考資料。

監控儲存容量和 IOPS 更新

您可以使用 Amazon FSx 主控台、CLI 和 API 監控固態硬碟儲存容量和 IOPS 更新的進度。

若要監視儲存和 IOPS 更新 (主控台)

在 FSx for ONTAP 檔案系統之 [檔案系統詳細資料] 頁面上的 [更新] 索引標籤中，您可以檢視每種更新類型的 10 個最新更新。



針對 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 擴展要求的模式和 IOPS 值。

目標值

您指定用來將檔案系統的 SSD 儲存容量或 IOPS 更新為的值。

狀態

更新的目前狀態。可能的值如下：

- 擱置中 — Amazon FSx 已收到更新要求，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 增加了檔案系統的 SSD 儲存容量。儲存最佳化程序現在會在背景中重新平衡資料。
- 已完成 — 更新已順利完成。
- 失敗 — 更新要求失敗。選擇問號 (?) 以查看詳細資訊。

進度%

以完成百分比顯示儲存體最佳化程序的進度。

請求時間

Amazon FSx 收到更新動作要求的時間。

若要監視儲存區和 IOPS 更新 (CLI)

您可以使用describe-file-systems AWS CLI 命令和 DescribeFileSystemsAPI 作業來檢視和監視檔案系統 SSD 儲存容量增加的要求。AdministrativeActions陣列會列出每個管理動作類型的 10 個最新更新動作。當您增加檔案系統的 SSD 儲存容量時，會產生兩個AdministrativeActions動作：a FILE_SYSTEM_UPDATE 和一個STORAGE_OPTIMIZATION動作。

下列範例顯示 describe-file-systems CLI 命令回應的摘錄。檔案系統具有擱置中的管理動作，可將固態硬碟儲存容量增加至 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，並將新的較大儲存磁碟新增至檔案系統。檔案系統可使用新儲存區時，FILE_SYSTEM_UPDATE狀態會變更為UPDATED_OPTIMIZING。儲存容量會顯示更大的新值，而 Amazon FSx 則開始處理STORAGE_OPTIMIZATION管理動作。下列 describe-file-systems CLI 命令回應摘錄會顯示此行為。

ProgressPercent屬性會顯示儲存區最佳化程序的進度。成功完成儲存最佳化程序之後，FILE_SYSTEM_UPDATE動作的狀態會變更為COMPLETED，且STORAGE_OPTIMIZATION動作不再顯示。

```
"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"
    }
]
```

如果儲存區容量或 IOPS 更新要求失敗，FILE_SYSTEM_UPDATE動作的狀態會變更為FAILED，如下列範例所示。FailureDetails屬性會提供失敗的相關資訊。

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586373915.697,
        "Status": "FAILED",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
            }
        },
        "FailureDetails": {
            "Message": "failure-message"
        }
    }
```

```
]
```

動態增加 SSD 儲存容量

當使用的 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來動態增加 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、基於此閾值的 Amazon CloudWatch 警示，以及增加檔案系統儲存容量的 AWS Lambda 功能。

解決方案會自動部署所有必要的元件，並使用下列參數：

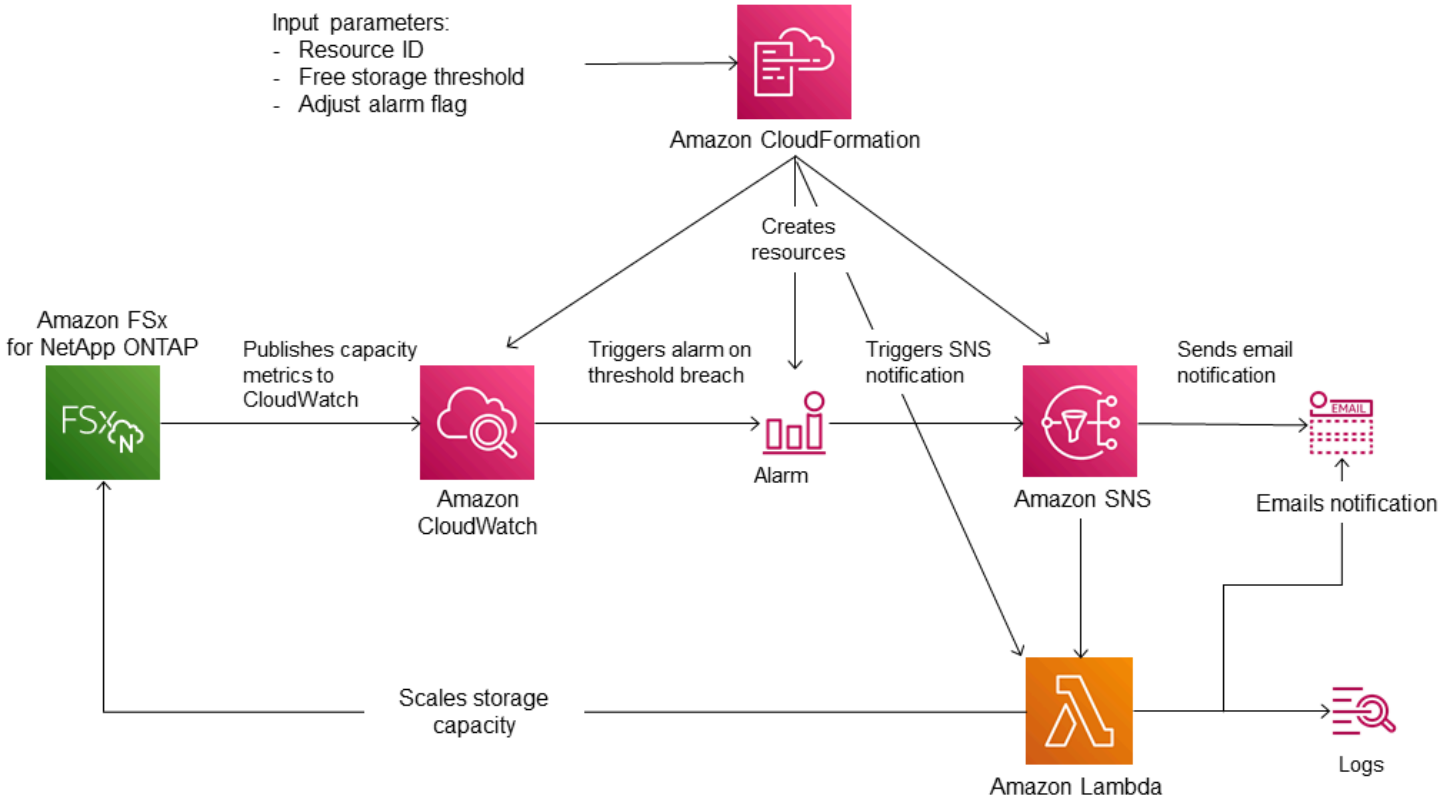
- 您的 FSx 代表 ONTAP 檔案系統識別碼。
- 使用的 SSD 存儲容量閾值（數值）。這是觸發 CloudWatch 警報的百分比。
- 儲存容量增加的百分比 (%)。
- 用來接收擴展通知的電子郵件地址。

主題

- 架構概觀
- AWS CloudFormation 範本
- 使用自動化部署 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，以及所有必要的 AWS Identity and Access Management (IAM) 角色。IAM 角色授予 Lambda 函數呼叫 Amazon FSx API 作業的權限。
2. CloudWatch 當檔案系統已使用的儲存容量超過指定閾值時觸發警示，並將訊息傳送至 Amazon SNS 佇列。只有當檔案系統的已使用容量連續超過臨界值 5 分鐘時，才會觸發警示。
3. 然後，解決方案會觸發訂閱此 Amazon SNS 主題的 Lambda 函數。
4. Lambda 函數會根據指定的增加百分比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. Lambda 函數作業的原始 CloudWatch 警示狀態和結果會傳送至 Amazon SNS 佇列。

若要接收有關作為回應 CloudWatch 警示所執行動作的通知，您必須按照訂閱確認電子郵件中提供的連結確認 Amazon SNS 主題訂閱。

AWS CloudFormation 範本

此解決方案 AWS CloudFormation 使用自動化部署元件，這些元件用於自動增加 ONTAP 檔案系統的 FSx 儲存容量。若要使用此解決方案，請下載 F SxOntapDynamicStorageScaling 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加以修改。

FileSystemId

無預設值。您要自動增加儲存容量之檔案系統的 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臨界值，以檔案系統目前儲存容量的百分比 (%) 指定。當使用的儲存體超過此臨界值時，檔案系統會被視為具有較低的可用儲存容量。

EmailAddress

無預設值。指定要用於 SNS 訂閱的電子郵件地址，並接收儲存容量閾值警示。

PercentIncrease

預設值為 20%。指定儲存容量的增加量，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，就會嘗試一次儲存擴展。如果您的 SSD 儲存容量使用率在嘗試進行儲存擴展作業之後仍然高於臨界值，則不會再嘗試進行儲存擴展操作。

最大值 B SxSizeinGi

預設值為 指定 SSD 儲存裝置支援的最大儲存容量。

使用自動化部署 AWS CloudFormation

下列程序會設定並部署 AWS CloudFormation 堆疊，以自動增加 ONTAP 檔案系統 FSx 的儲存容量。部署需要幾分鐘的時間。如需有關建立 CloudFormation 堆疊的詳細資訊，請參閱《使用指南》中的〈在 AWS CloudFormation 主控台上建立堆疊AWS CloudFormation〉。

> **Note**
>
> 實作此解決方案會產生相關 AWS 服務的費用。如需詳細資訊，請參閱這些服務的定價詳細資料頁面。

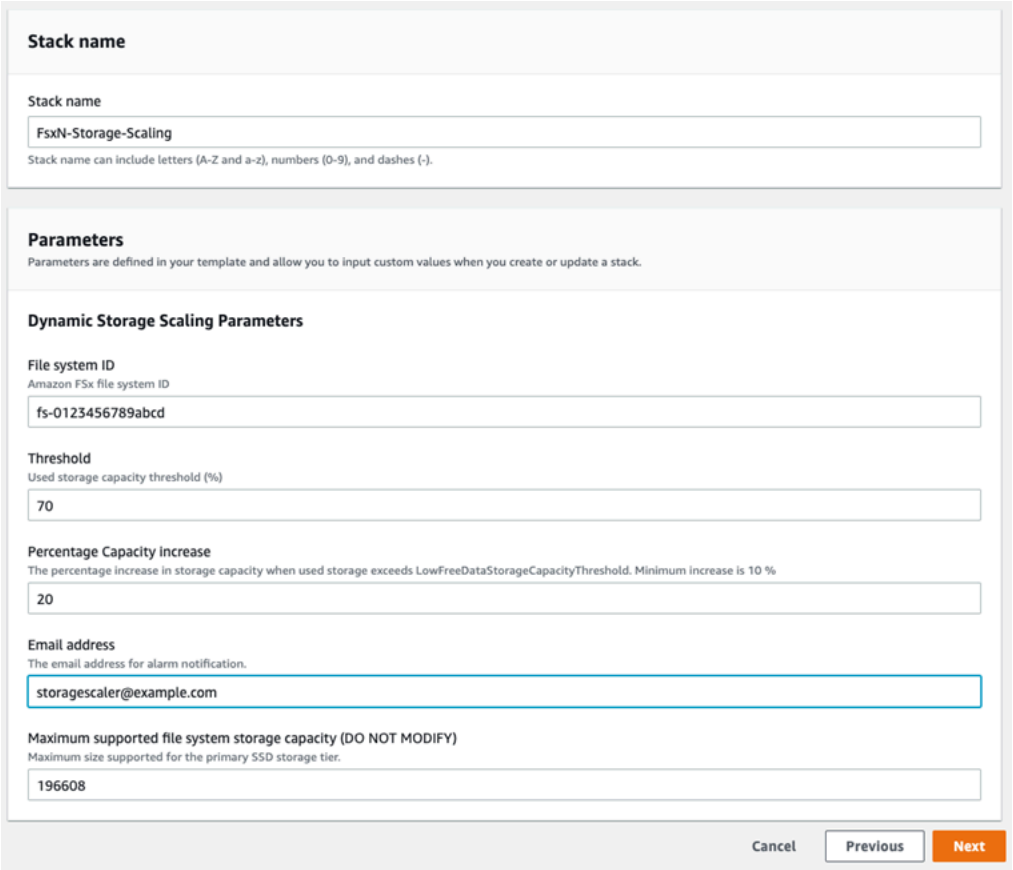
在開始之前，您必須具有在您的 Amazon Virtual Private Cloud (Amazon VPC) 中執行的 Amazon FSx 檔案系統的識別碼。 AWS 帳戶如需建立 Amazon FSx 資源的詳細資訊，請參閱開始使用適 NetApp 用於 ONTAP 的 Amazon FSx。

啟動自動儲存容量增加解決方案堆疊

1. 下載 F SxOntapDynamicStorageScaling AWS CloudFormation 範本。

   > **Note**
   >
   > Amazon FSx 目前僅在特定 AWS 區域提供。您必須在提供 Amazon FSx 的 AWS 區域啟動此解決方案。如需詳細資訊，請參閱. AWS 一般參考

2. 在 AWS CloudFormation 主控台中，選擇 [建立堆疊] > [使用新資源]。
3. 選擇模板已準備就緒。在「指定範本」區段中，選擇「上傳範本檔案」，然後上傳您下載的範本。
4. 在指定堆疊詳細資料中，輸入自動儲存容量增加解決方案的值。



5. 輸入堆疊名稱。
6. 對於「參數」，請檢閱範本的參數並加以修改，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. 輸入自訂解決方案所需的 [選項] 設定，然後選擇 [下一步]。
8. 對於「檢閱」，請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 AWS CloudFormation 主控台的 [狀態] 欄中檢視堆疊的狀態。您應該會在幾分鐘內看到「建立 _ 完成」狀態。

更新堆疊

建立堆疊之後，您可以使用相同的範本並為參數提供新值來更新堆疊。如需詳細資訊，請參閱《AWS CloudFormation 使用指南》中的「直接更新堆疊」。

磁碟區儲存容量

FSx for ONTAP 磁碟區是用於分組資料、決定資料儲存方式以及決定資料存取權的類型的虛擬資源。磁碟區 (如資料夾) 本身不會耗用檔案系統儲存容量。只有儲存在磁碟區中的資料會消耗 SSD 儲存空間，而且視磁碟區的分層原則而定，容量集區儲存。您可以在建立磁碟區時設定磁碟區的大小，之後也可以變更其大小。您可以使用 AWS Management Console、和 API 和 ONTAP CLI 來監視 AWS CLI 和管理 FSx 的 ONTAP 磁碟區的儲存容量。

主題

磁碟區資料分層

適用於 NetApp ONTAP 檔案系統的 Amazon FSx 具有兩個儲存層：主要儲存和容量集區儲存。主要儲存裝置是佈建、可擴充的高效能 SSD 儲存裝置，專為資料集的使用中部分而打造。容量集區儲存是一種完全彈性的儲存層，可擴充至 PB 級，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原則、冷卻期間和臨界值設定，自動分層到容量集區儲存層。下列各節說明ONTAP磁碟區分層原則，以及用來決定何時將資料分層至容量集區的臨界值。

磁碟區分層政策

您可以選擇檔案系統上每個磁碟區的分層原則，以決定如何將 FSx 用於 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。您可以從下列其中一個原則中選擇決定哪些資料 (如果有的話) 會分層至容量集區儲存體。

> **Note**
>
> 分層可以將檔案資料和快照資料移至容量集區層。不過，檔案中繼資料一律保留在 SSD 層上。如需詳細資訊，請參閱 SSD 儲存裝置的使用方式。

- 自動 — 此原則會將所有冷資料 (使用者資料和快照) 移至容量集區層。資料的冷卻速率由原則的冷卻期決定，預設為 31 天，可設定為 2-183 天之間的值。當基礎冷資料區塊隨機讀取 (如典型的檔案存取) 時，會將它們變成熱並寫入主要儲存層。當冷資料區塊依序讀取 (例如透過防毒掃描) 時，它們會保持冷卻狀態，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 — 此原則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原則的冷卻期間，預設為 2 天，且可設定為 2-183 天之間的值。讀取冷快照資料時，會將其設為熱並寫入主要儲存層。這是使用 Amazon FSx API 或 NetApp ONTAP CLI 建立磁碟區時的預設政策。 AWS CLI
- 全部 — 此原則會將所有使用者資料和快照資料標示為冷，並將其儲存在容量集區層中。讀取資料區塊時，資料區塊會保持冷卻狀態，而且不會寫入主要儲存層。當資料寫入具有全部分層原則的磁碟區時，資料一開始仍會寫入 SSD 儲存層，並透過背景處理程序分層至容量集區。請注意，檔案中繼資料一律保留在 SSD 層。
- 無 — 此原則會將磁碟區的所有資料保留在主要儲存層，並防止其移至容量集區儲存體。如果您在使用任何其他原則後將磁碟區設定為此原則，只要您的 SSD 使用率低於 90%，容量集區儲存體中的磁碟區中的現有資料就會由背景處理程序移至 SSD 儲存體。故意讀取資料或修改磁碟區的雲端擷取政策，可加快背景程序的速度。如需詳細資訊，請參閱 雲端擷取政策。

最佳作法是移轉計劃長期儲存在容量集區儲存體中的資料時，建議您在磁碟區上使用自動分層原則。使用自動分層功能，資料會在移至容量集區層之前，儲存在 SSD 儲存層至少 2 天 (根據磁碟區的冷卻週期)。將 SSD 儲存資料保留至少 2 天，讓 ONTAP 能夠執行處理後壓縮和重複資料刪除功能，當資料分層到容量集區時，這些資料會保留下來。ONTAP 只會針對 SSD 儲存裝置上的資料執行處理後壓縮

和重複資料刪除，因此選取此原則可協助您節省最多的長期儲存空間。您也可以最大限度地提高磁碟區建立的第一個備份的傳輸速度，因為正在備份的資料位於 SSD 儲存裝置上。

如需設定或修改磁碟區分層原則的詳細資訊，請參閱設定磁碟區的分層政策。

分層冷卻週期

磁碟區的分層冷卻期間會設定 SSD 層中資料標示為冷卻所需的時間量。冷卻期間適用於`Auto`和`Snapshot-only`分層策略。您可以將冷卻週期設定為 2—183 天範圍內的值。如需設定冷卻週期的更多資訊，請參閱設定最低冷卻天數。

資料會在冷卻期到期後 24 至 48 小時分層。分層是消耗網路資源的背景處理序，而且優先順序低於面向用戶端的要求。當有正在進行的客戶端面向請求時，分層活動會被限制。

雲端擷取政策

磁碟區的雲端擷取政策會設定條件，以指定何時允許從容量集區層讀取的資料提升至 SSD 層。當雲端擷取政策設定為以外的任何內容時`Default`，此原則會覆寫磁碟區分層原則的擷取行為。磁碟區可以具有下列其中一個雲端擷取政策：

- 預設 — 此原則會根據磁碟區的基礎分層原則擷取分層資料。這是所有磁碟區的預設雲端擷取政策。
- 永不 — 此原則永遠不會擷取分層資料，無論讀取是連續還是隨機讀取。這類似於將磁碟區的分層政策設定為 [全部]，不同之處在於您可以將它與其他原則 (自動、僅限 Snapshot) 搭配使用，以根據最短冷卻週期而非立即分層資料。
- 讀取時 — 此原則會擷取所有用戶端導向資料讀取的分層資料。使用 [全部分層] 原則時，此原則沒有任何作用。
- 升級 — 此原則會標示容量集區中的所有磁碟區資料，以便擷取至 SSD 層。資料會在每日背景分層掃描器下次執行時標記。對於具有週期性工作負載不常執行，但在執行時需要 SSD 層效能的應用程式，此原則非常有益。使用 [全部分層] 原則時，此原則沒有任何作用。

如需有關設定磁碟區雲端擷取政策的資訊，請參閱設定磁碟區的雲端擷取政策。

分層臨界值

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。下列臨界值會根據檔案系統的 SSD 儲存容量使用量設定分層行為，如上所述。如需如何監控磁碟區 SSD 儲存層之容量使用率的相關資訊，請參閱監控磁碟區儲存容量。

> **Note**
>
> 建議您不要超過 SSD 儲存層 80% 的儲存容量使用率。對於向外延展檔案系統，此建議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。這樣可以確保正確分層功能，並為新數據提供開銷。如果您的 SSD 儲存層持續高於 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 更新檔案系統固態硬碟儲存和 IOPS。

FSx for ONTAP 使用下列儲存容量閾值來管理磁碟區的分層：

- <= 50% SSD 儲存層使用率 — 在此臨界值時，SSD 儲存層被視為未充分利用，而且只有使用全部分層原則的磁碟區才會將資料分層到容量集區儲存體。具有自動和僅快照政策的磁碟區不會以此閾值分層資料。
- > 50% SSD 儲存層使用率 — 具有自動和僅限快照分層原則的磁碟區會根據分層最小冷卻天數設定來分層資料。預設設定為 31 天。
- >= 90% SSD 儲存層使用率 — 在此閾值下，Amazon FSx 會優先考慮保留 SSD 儲存層中的空間。使用自動和僅限快照原則讀取磁碟區時，容量集區層中的冷資料不會再移至 SSD 儲存層。
- >= 98% SSD 儲存層使用率 — 當 SSD 儲存層使用率達到或高於 98% 時，所有分層功能都會停止。您可以繼續讀取儲存層，但無法寫入層。

快照與磁碟區儲存容量

快照是 NetApp ONTAP 磁碟區的 Amazon FSx 在某個時間點的唯讀映像檔。快照提供保護，防止意外刪除或修改磁碟區中的檔案。透過快照，您的使用者可以輕鬆檢視和還原先前快照中的個別檔案或資料夾。

快照與您的系統數據一起存儲，並且它們消耗了 Firle 系統的存儲容量。不過，快照只會針對自上次快照以來變更的部分而消耗儲存容量。快照不包含在備份系統磁碟區中。

根據預設，磁碟區上的快照會使用預設快照原則啟用快照。快照儲存在磁碟區根`.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：

- 快照原則 — 選取內建快照原則，或選擇您在 ONTAP CLI 或 REST API 中建立的自訂原則。
- 手動刪除快照 — 手動刪除快照以回收儲存容量。
- 建立快照自動刪除策略 — 建立刪除比預設快照策略更多快照的策略。
- 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。

磁碟區檔案容量

適用於 NetApp ONTAP 磁碟區的 Amazon FSx 具有檔案指標，可用來儲存檔案中繼資料，例如檔案名稱、上次存取時間、權限、大小，以及做為資料區塊的指標。這些文件指針被稱為 inodes，並且每個卷具有 inode 的數量，這被稱為卷文件容量的數量有限的容量。當磁碟區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。

磁碟區可以包含的檔案系統物件 (檔案、目錄、快照副本) 的數目取決於磁碟區有多少個 Inode。磁碟區中的 inode 數量會隨磁碟區的儲存容量 (以及磁碟區成分的磁碟區成分數目) 相同增加。FlexGroup根據預設，儲存容量為 648 GiB 或以上的FlexVol磁碟區 (或FlexGroup成分) 都具有相同數量的索引節點：21,251,126。如果您建立的磁碟區大於 648 GiB，並且希望其具有超過 21,251,126 個索引節點，則必須手動增加最大的索引節點 (檔案) 數量。如需檢視磁碟區檔案數目上限的詳細資訊，請參閱檢視磁碟區的檔案容量。

每 32 KiB 的磁碟區儲存容量，磁碟區上的預設節點數目為 1 個 inode，磁碟區大小為 648 GiB。對於 1 GiB 磁碟區：

磁碟區大小 (以位元組為單位) × (1 個檔案 ÷ 節點大小 (位元組) = 檔案的最大數量

1 個檔案 × (1 個檔案 ÷ 0 個位元組) = 32,768 個檔案

您可以增加磁碟區可包含的最大 inode 數目，每 4 KiB 的儲存容量最多可增加 1 個 inode。如果是 1 GiB 磁碟區。這會將節點或檔案的最大數目從 32,768 增加到 262,144：

1 個檔案 × (1 個檔案 ÷ 4 個位元組) = 2 個檔案

ONTAP 磁碟區的 FSx 最多可以有 20 億個節點。

如需變更磁碟區可儲存的檔案數目上限的資訊，請參閱增加磁碟區上的檔案數目上限。

更新磁碟區的儲存容量

您可以使用 AWS Management Console、 AWS CLI 和 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已使用的儲存容量閾值時自動增加或縮小。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 主控台和 API 來增加或減少磁碟區的儲存容量。 AWS CLI如需詳細資訊，請參閱 更新磁碟區。

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

若要修改磁碟區的大小 (ONTAP CLI)

1. 若要存取 NetApp ONTAP CLI，請執行下列命令，在適用於 NetApp ONTAP 檔案系統的 Amazon FSx 管理連接埠上建立安全殼層工作階段。取代*management_endpoint_ip*為檔案系統管理連接埠的 IP 位址。

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

   如需詳細資訊，請參閱 使用 ONTAP CLI 管理檔案系統。

2. 使用 volume modify ONTAP CLI 指令修改磁碟區的儲存容量。運行以下命令，使用您的數據代替以下值：

   - *svm_name*以建立磁碟區之儲存區虛擬機器 (SVM) 的名稱取代。
   - 以您要重新調整大小的磁碟區名稱取*vol_name*代。
   - 以格式*vol_size*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
   ```

啟用自動調整磁碟區

磁碟區自動調整大小，以便磁碟區在達到已使用的空間臨界值時自動成長到指定的大小。您可以使用 ONTAP CLI 指令針對 FlexVol 磁碟區類型 (適用於 ONTAP 的 FSx 的預設磁碟區類型) 執行volume autosize此動作。

若要啟用磁碟區自動調整大小 (ONTAP CLI)

1. 若要存取 NetApp ONTAP CLI，請執行下列命令，在適用於 NetApp ONTAP 檔案系統的 Amazon FSx 管理連接埠上建立安全殼層工作階段。取代*management_endpoint_ip*為檔案系統管理連接埠的 IP 位址。

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

   如需詳細資訊，請參閱 使用 ONTAP CLI 管理檔案系統。

2. 如圖所示使用volume autosize指令，取代下列值：

   - *svm_name*以建立磁碟區的 SVM 名稱取代。
   - 以您要調整大小的磁碟區名稱取*vol_name*代。
   - 以已使*grow_threshold*用的空間百分比值取代 (例如90)，磁碟區會自動增加大小 (最大*max_size*值)。
   - 取代*max_size*為磁碟區可以成長到的最大大小。使用格式 *integer*[KB|MB|GB|TB|PB]；例如，300TB。最大尺寸為 300 TB。預設值為磁碟區大小的 120%。
   - 將 *min_size* 替換為卷將縮小到的最小大小。使用與##########
   - 將 shrink *_threshold* 取代為磁碟區將自動縮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
```

監控磁碟區儲存容量

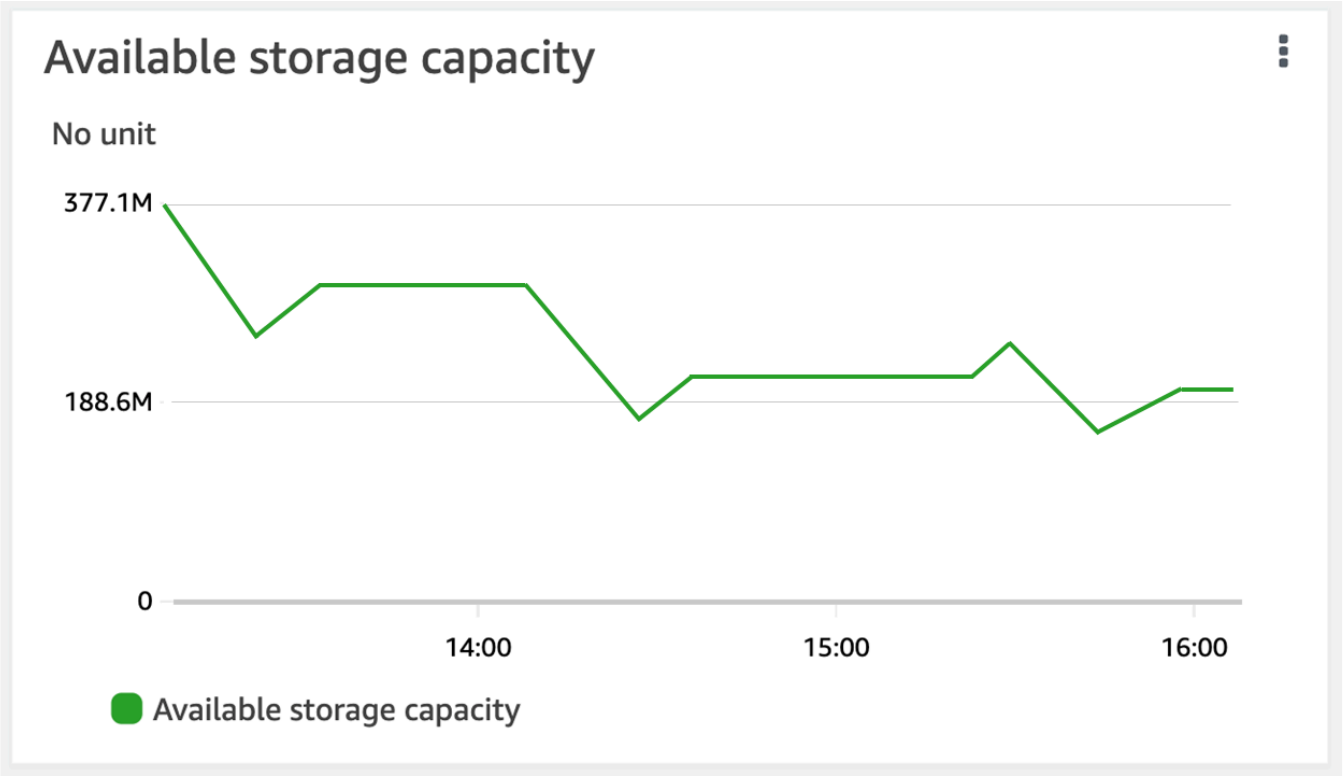
您可以在 AWS Management Console、 AWS CLI和 NetApp ONTAP CLI 中檢視磁碟區的可用儲存區及其儲存區分佈。

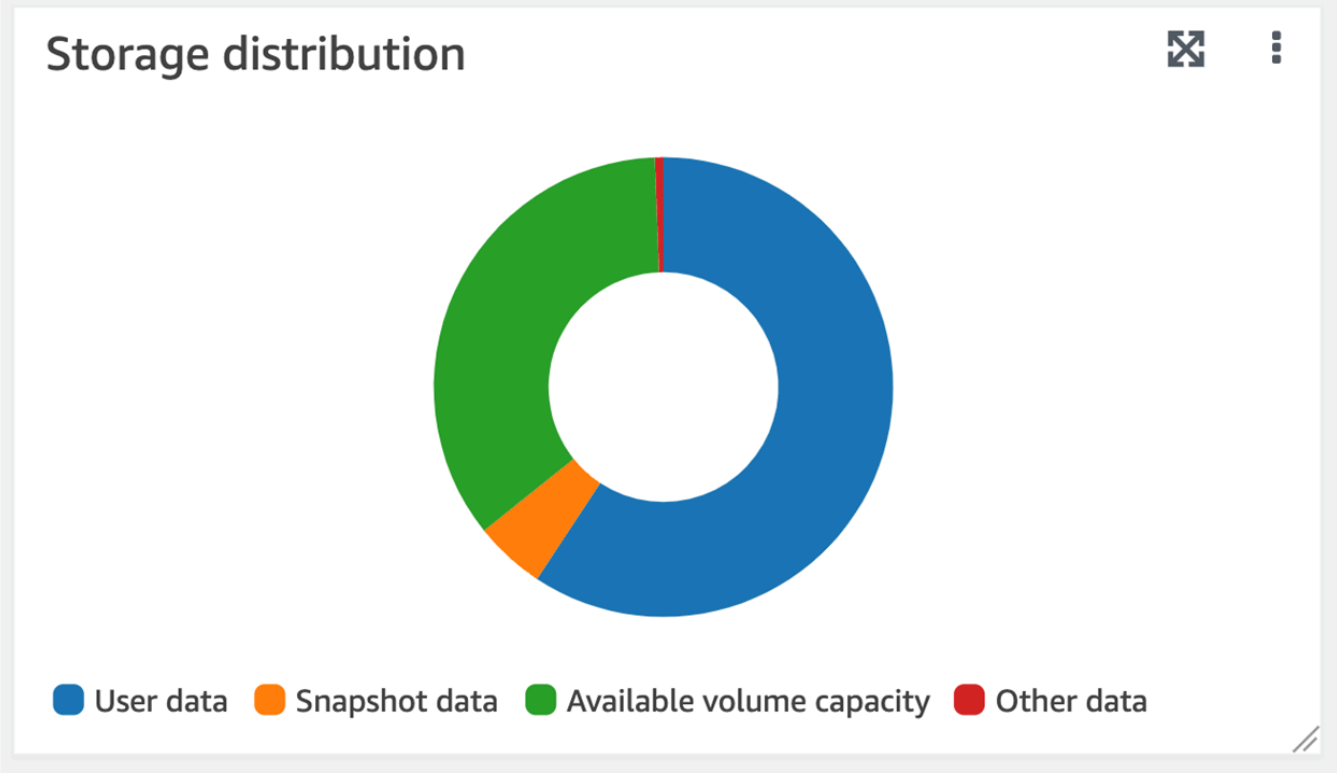
監視磁碟區的儲存容量 (主控台)

可用的儲存空間圖表會顯示磁碟區隨時間變化的可用儲存容量。儲存區分佈圖顯示磁碟區的儲存容量目前分佈在 4 個類別上的方式：

- 使用者資料
- 快照資料
- 可用磁碟區容量
- 其他數據

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 在左側導覽欄中選擇 [磁碟區]，然後選擇您要檢視其儲存容量資訊的 ONTAP 磁碟區。便會顯示磁碟區詳細資訊頁面
3. 在第二個面板中，選擇監控標籤。會顯示「可用的儲存體」和「儲存體」分佈圖，以及其他數個圖形。


Available storage capacity
No unit
377.1M
188.6M
0
14:00
15:00
16:00
Available storage capacity


Storage distribution
User data
Snapshot data
Available volume capacity
Other data

若要監視磁碟區的儲存容量 (ONTAPCLI)

您可以使用 `volume show-space` ONTAP CLI 命令來監視磁碟區儲存容量的使用情況。如需詳細資訊，請參閱NetApp ONTAP文件volume show-space中心中的。

1. 若要存取 NetApp ONTAP CLI，請執行下列命令，在適用於 NetApp ONTAP 檔案系統的 Amazon FSx 管理連接埠上建立安全殼層工作階段。取代*management_endpoint_ip*為檔案系統管理連接埠的 IP 位址。

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

   如需詳細資訊，請參閱 使用 ONTAP CLI 管理檔案系統。

2. 透過發出下列指令來檢視磁碟區的儲存容量使用量，取代下列值：

   - *svm_name*以建立磁碟區的 SVM 名稱取代。
   - 以您要設定資料分層原則之磁碟區的名稱取*vol_name*代。

   ```
   ::> volume show-space -vserver svm_name -volume vol_name
   ```

   如果命令成功，您將看到類似以下內容的輸出：

   ```
   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%
   ```

此指令的輸出會顯示不同類型資料在此磁碟區上佔用的實體空間量。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並Snapshot Reserve消耗組合 90% 的磁碟區容量。

Snapshot Reserve顯示保留用於儲存快照副本的磁碟空間量。如果快照複製儲存體超過保留空間，它會溢出到檔案系統中，而這個數量會顯示在下Snapshot Spill方。

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。

對於磁 FlexVol 碟區類型 (ONTAP 磁碟區 FSx 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項功能。

設定磁碟區的分層政策

您可以使用 AWS Management Console、 AWS CLI 和 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原則 (主控台)

使用下列程序，使用修改磁碟區的資料分層原則。 AWS Management Console

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 [磁碟區]，然後選擇您要修改其資料分層原則的 ONTAP 磁碟區。
3. 從動作下拉式功能表中選擇更新磁碟區。會出現 [更新磁碟區] 視窗。
4. 對於容量集區分層原則，請選擇磁碟區的新原則。如需詳細資訊，請參閱 磁碟區分層政策。
5. 選擇 [更新]，將新原則套用至磁碟區。

若要設定磁碟區的分層原則 (CLI)

- 使用更新磁碟區 CLI 命令 (相當於 Amazon FSx API 動作) UpdateVolume修改磁碟區的分層政策。下列 CLI 命令範例會將磁碟區的資料分層原則設定為。SNAPSHOT_ONLY

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

對於成功的要求，系統會以磁碟區描述回應。

```
{
    "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"
    }
}
```

若要修改磁碟區的分層原則 (ONTAP CLI)

您可以使用 `volume modify` ONTAP CLI 命令來設定磁碟區的分層原則。如需詳細資訊，請參閱 `volume modify` NetApp ONTAP 文件中心。

1. 若要存取 NetApp ONTAP CLI，請執行下列命令，在適用於 NetApp ONTAP 檔案系統的 Amazon FSx 管理連接埠上建立安全殼層工作階段。取代*management_endpoint_ip*為檔案系統管理連接埠的 IP 位址。

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

   如需詳細資訊，請參閱 使用 ONTAP CLI 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. 使用下列命令修改磁碟區資料分層原則，取代下列值：

   - *svm_name*以建立磁碟區的 SVM 名稱取代。
   - 以您要設定資料分層原則之磁碟區的名稱取*vol_name*代。
   - 以所需*tiering_policy*的原則取代。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
```

設定最低冷卻天數

磁碟區的最小冷卻天數可設定用來判斷哪些資料處於溫暖狀態以及哪些資料為冷的臨界值。您可以使用 AWS CLI 和 API 和 ONTAP CLI 來設定磁碟區的最小冷卻天數。

若要設定磁碟區的最小冷卻天數 (CLI)

- 使用更新磁碟區 CLI 命令 (UpdateVolume這是相當於 Amazon FSx API 動作) 來修改磁碟區組態。下列 CLI 命令範例會將磁碟區設定CoolingPeriod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}
```

系統會回應成功要求的磁碟區說明。

```
{
```

```
    "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"
    }
}
```

若要設定磁碟區的最小冷卻天數 (ONTAP CLI)

使用 `volume modify` ONTAP CLI 指令來設定現有磁碟區的最小冷卻天數。如需詳細資訊，請參閱 `volume modify` NetApp ONTAP 文件中心。

1. 若要存取 NetApp ONTAP CLI，請執行下列命令，在適用於 NetApp ONTAP 檔案系統的 Amazon FSx 管理連接埠上建立安全殼層工作階段。取代*management_endpoint_ip*為檔案系統管理連接埠的 IP 位址。

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

   如需詳細資訊，請參閱 使用 ONTAP CLI 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. 使用下列指令來變更磁碟區的分層最小冷卻天數，並取代下列值：

   - *svm_name*以建立磁碟區的 SVM 名稱取代。
   - 取代*vol_name*為您要設定冷卻天數的體積名稱。
   - 用所需*cooling_days*的 2-183 之間的整數替換。

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

   系統會針對成功的要求回應如下。

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

設定磁碟區的雲端擷取政策

使用 `volume modify` ONTAP CLI 命令為現有磁碟區設定雲端擷取政策。如需詳細資訊，請參閱 `volume modify` NetApp ONTAP 文件中心。

若要設定磁碟區的雲端擷取政策 (ONTAP CLI)

1. 若要存取 NetApp ONTAP CLI，請執行下列命令，在適用於 NetApp ONTAP 檔案系統的 Amazon FSx 管理連接埠上建立安全殼層工作階段。取代*management_endpoint_ip*為檔案系統管理連接埠的 IP 位址。

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

   如需詳細資訊，請參閱 使用 ONTAP CLI 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. 使用下列命令來設定磁碟區的雲端擷取政策，取代下列值：

   - *svm_name*以建立磁碟區的 SVM 名稱取代。
   - 取代*vol_name*為您要設定雲端擷取政策的磁碟區名稱。
   - 取代*retrieval_policy*為所需的值，可以是default、on-read、never、或promote。

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

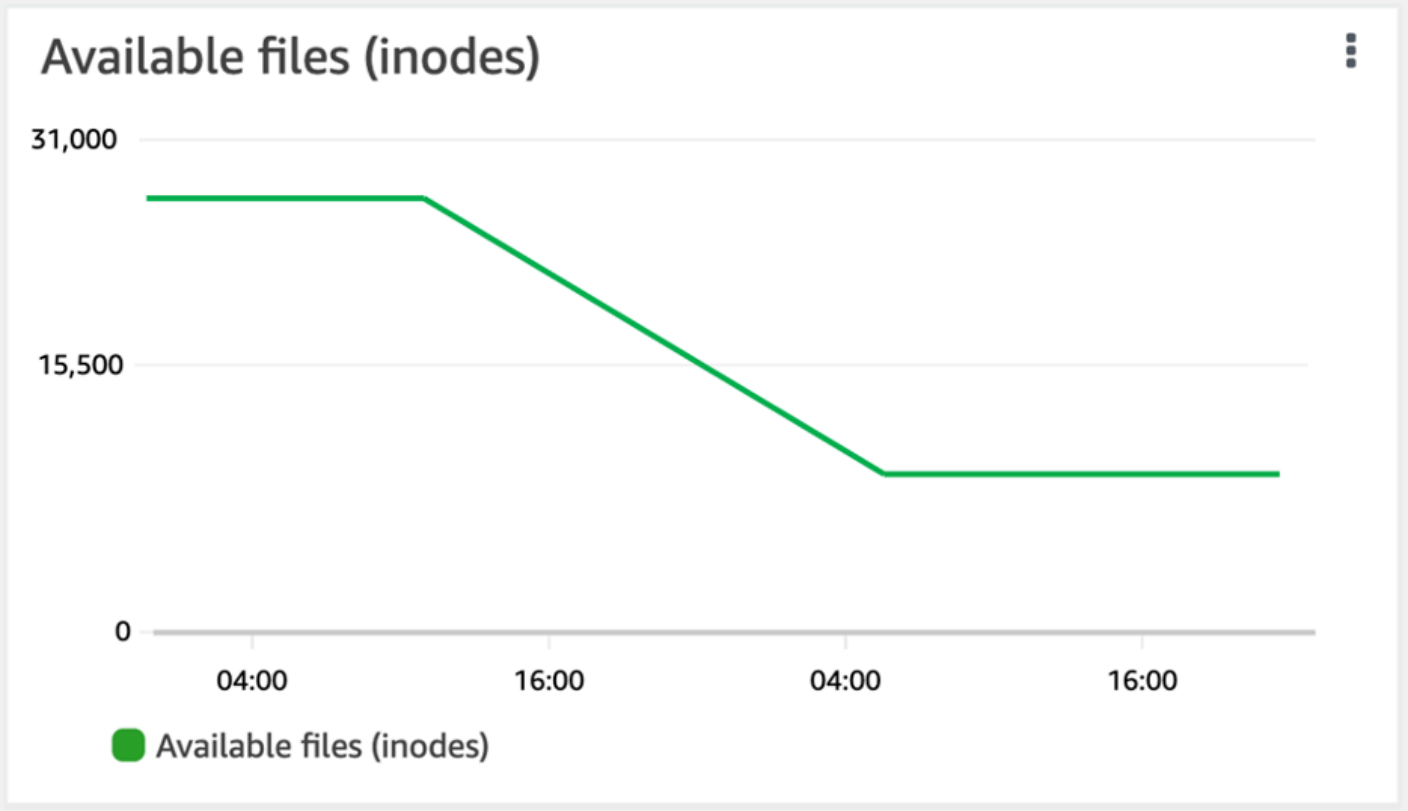
   系統會針對成功的要求回應如下。

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

檢視磁碟區的檔案容量

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。

- 體 CloudWatch 積指標FilesCapacity和FilesUsed.
- 在 Amazon FSx 主控台中，瀏覽至磁碟區監控索引標籤中的可用檔案 (inode) 圖表。下圖顯示磁碟區上隨時間而減少的可用檔案 (inode)。



增加磁碟區上的檔案數目上限

當可用的節點或檔案指標數量用盡時，ONTAP 磁碟區的 FSx 可能會耗盡檔案容量。

增加磁碟區上的檔案數目上限 (ONTAPCLI)

您可以使用 `volume modify` ONTAP CLI 命令增加磁碟區上的檔案數目上限。如需詳細資訊，請參閱 NetApp ONTAP文件`volume modify`中心中的。

1. 若要存取 NetApp ONTAP CLI，請執行下列命令，在適用於 NetApp ONTAP 檔案系統的 Amazon FSx 管理連接埠上建立安全殼層工作階段。取代*management_endpoint_ip*為檔案系統管理連接埠的 IP 位址。

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

   如需詳細資訊，請參閱 使用 ONTAP CLI 管理檔案系統。

2. 根據使用案例執行以下其中一項操作。替換*svm_name*你*vol_name*的價值觀。

- 若要將磁碟區設定為永遠具有最大可用檔案數目 (inode)，請執行下列步驟：

  1. 使用下列命令在 ONTAP CLI 中進入進階模式。

     ```
     ::> set adv
     ```

  2. 運行此命令後，您將看到此輸出。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
     ```

  3. 輸入下列指令，永遠使用磁碟區上的檔案數目上限：

     ```
     ::> volume modify -vserver svm_name -volume vol_name -files-set-maximum true
     ```

- 若要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，請使用下列指令：

  ```
  ::> volume modify -vserver svm_name -volume vol_name -files max_number_files
  ```

啟用磁碟區的雲端寫入模式

使用 volume modify ONTAP CLI 命令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 volume modify NetApp ONTAP 文件中心。

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此功能。
- 磁碟區必須是讀寫 (RW) 磁碟區。
- 磁碟區必須具有 [全部分層] 原則。如需修改磁碟區分層原則的詳細資訊，請參閱設定磁碟區的分層政策。

雲端寫入模式對於移轉等情況很有幫助，例如，使用 NFS 通訊協定將大量資料傳輸到檔案系統。

若要設定磁碟區的雲端寫入模式 (ONTAP CLI)

1. 若要存取 NetApp ONTAP CLI，請執行下列命令，在適用於 NetApp ONTAP 檔案系統的 Amazon FSx 管理連接埠上建立安全殼層工作階段。取代*management_endpoint_ip*為檔案系統管理連接埠的 IP 位址。

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

   如需詳細資訊，請參閱 使用 ONTAP CLI 管理檔案系統。

2. 使用下列命令進入 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
   ```

3. 使用下列指令來設定磁碟區的雲端寫入模式，取代下列值：

   - *svm_name*以建立磁碟區的 SVM 名稱取代。
   - 取代*vol_name*為您要設定雲端寫入模式的磁碟區名稱。
   - 取代*vol_cw_mode*`true`為在磁碟區上啟用雲端寫入模式或`false`停用它。

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

   系統會針對成功的要求回應如下。

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

保護您的資料

除了自動複寫檔案系統資料以確保高耐久性之外，Amazon FSx 還提供下列選項，以進一步保護儲存在檔案系統上的資料：

- 原生 Amazon FSx 備份可支援您在 Amazon FSx 中的備份保留和合規需求。您還可以用 AWS Backup 來集中管理、自動化和保護雲端 AWS 服務 中的備份。
- 快照可讓使用者輕鬆還原檔案變更，並透過將檔案還原至舊版本來比較檔案版本。
- 將 Amazon FSx 檔案系統複寫到第二個檔案系統，以提供資料保護和復原。啟用時，複寫會自動排程進行。
- SnapLock可將檔案轉換為「一次寫入多讀」(WORM) 狀態，以保護檔案，防止在指定的保留期間內進行修改或刪除。

主題

使用備份

使用 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由使用者啟動的備份。ONTAP 備份的 FSx 是每個磁碟區，因此每個備份僅包含特定磁碟區中的資料。Amazon FSx 備份具有高度耐用性和增量功能。

所有 Amazon FSx 備份 (每日自動備份和使用者啟動的備份) 都是增量備份。這表示只會儲存最近一次備份後，磁碟區上已變更的資料。如此可將建立備份所需的時間和備份所需的儲存時間降至最低，藉由不複製資料來節省儲存成本。刪除備份時，只會移除該備份專屬的資料。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，以有效地還原檔案系統磁碟區的 point-in-time 快照。

為磁碟區建立定期備份是有助於支援資料保留和合規性需求的最佳作法。無論是建立備份、從備份還原或刪除備份，都能輕鬆使用 Amazon FSx 備份。

Amazon FSx 支援使用`OntapVolumeType`的 `RW` (讀寫) 備份ONTAPFlexVol磁碟區 (在所有檔案系統上) 和FlexGroup磁碟區。

> **Note**
>
> Amazon FSx 不支援備份資料保護 (DP) 磁碟區、負載共用 (LS) 磁碟區或目標磁碟區。FlexCache

每個檔案系統和每個磁碟區可儲存的備份數量有限制。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。

主題

備份的運作方式

Amazon FSx 備份使用快照 (即磁碟區的唯讀映像) 來維持備份之間的增量。 point-in-time每次進行備份時，Amazon FSx 都會先拍攝磁碟區的快照。備份快照會儲存在您的磁碟區中，並佔用 SSD 儲存層的空間。Amazon FSx 接著會將此快照與先前的備份快照 (如果有的話) 進行比較，並且只將變更的資料複製到備份中。

如果之前沒有備份快照，則最新備份快照的全部內容都會複製到備份中。成功擷取最新的備份快照後，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，直到進行下一次備份 (當程序重複執行時) 為止。為了最佳化備份儲存成本，請ONTAP保留磁碟區在備份中節省的儲存效率。

Amazon FSx 無法備份離線的磁碟區。

儲存需求

若要備份磁碟區，您的磁碟區和檔案系統都必須有足夠的可用 SSD 儲存容量來儲存備份快照。建立備份快照時，快照耗用的額外儲存容量不會導致磁碟區超過 98% SSD 儲存使用率。如果發生這種情況，備份將失敗。您可以隨時增加磁碟區或檔案系統的 SSD 儲存空間，以確保備份不會中斷。

使用自動每日備份

建立檔案系統時，預設會啟用檔案系統磁碟區的自動每日備份功能。您可以隨時為檔案系統啟用或停用自動每日備份。在每日備份時段期間進行自動每日備份，這是在您建立檔案系統時自動設定的。您可以隨時修改每日備份時段。對於使用磁碟區以獲得更佳備份效能的應用程式，建議您選擇一天中的每日備份時間，該時間不在正常作業時間。如需詳細資訊，請參閱 Backup 與還原效能。

您可以在建立檔案系統時或隨時在主控台中將自動每日備份的保留期設定為 1 到 90 天之間。預設的每日自動備份保留期為 30 天。服務會在保留期間到期後刪除自動每日備份。您可以使用 CLI 或 API 將保留期設定為 0 到 90 天之間；將其設定為 0 會關閉自動每日備份。

每日備份時段和備份保留期是檔案系統層級的設定，適用於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 來變更檔案系統的備份時段和備份保留期，以及開啟或關閉自動每日備份。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。如需詳細資訊，請參閱 備份和離線磁碟區。

> **Note**
>
> 自動每日備份的最長保留期為 90 天，但您建立的使用者啟動的備份 (包括使用建立的備份) 會永久保留 AWS Backup，除非您或 AWS Backup 服務將其刪除。

您可以使用主控台、CLI 和 API 手動刪除每日自動備份。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。最終備份將永久保留，除非您將其刪除。如需詳細資訊，請參閱刪除備份。

使用使用者啟動的備份

使用 Amazon FSx，您可以隨時使用、和 API 手動備份檔案系統的磁碟區。 AWS Management Console AWS CLI您的使用者啟動的備份是相對於可能為磁碟區建立的其他備份的增量備份，並永久保留，除非您刪除它們。即使在您刪除磁碟區或建立備份的檔案系統之後，仍會保留使用者起始的備

份。您只能使用 Amazon FSx 主控台、API 或 CLI 刪除使用者啟動的備份。它們永遠不會被 Amazon FSx 自動刪除。如需詳細資訊，請參閱 刪除備份。

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 備份和離線磁碟區。

將標籤複製到備份

使用 CLI 或 API 建立或更新磁碟區時，您可以啟用自動CopyTagsToBackups將磁碟區上的任何標記複製到其備份。不過，如果您在建立使用者啟動的備份時新增任何標記 (包括在使用主控台時命名備份)，即使已啟用，服務也不會從磁碟區複製標記。CopyTagsToBackups

Backup 與還原效能

有多種因素可能會影響備份和還原作業的效能。Backup 和還原作業是背景處理程序，這表示它們的優先順序相對於用戶端 IO 作業較低。用戶端 IO 作業包括 NFS、CIFS 和 iSCSI 資料的讀取和寫入。所有背景處理程序 (包括備份與還原作業) 僅使用檔案系統輸送量容量中未使用的部分，而且可能需要幾分鐘到幾小時的時間才能完成，具體取決於備份的大小和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設定檔。當大部分資料位於 SSD 儲存裝置時，建議您建立磁碟區的第一個備份。包含大多數小文件的數據集通常具有較低的性能相比，大多包含大部分大小的文件的數據集相比。這是因為處理大量小型檔案比處理較少的大型檔案，會耗用更多的 CPU 週期和網路額外負荷。

一般而言，在備份 SSD 儲存層中儲存的資料時，您可以預期下列備份速率：

- 多個並發備份中包含大型文件的 750 Mbps。
- 多個並發備份中包含大多數小文件的 100 Mbps。

通常，您可以期待以下恢復率：

- 在包含大型檔案的多個並行還原中進行 250 Mbps。
- 在包含大多數小檔案的並行還原中包含 100 Mbps。

AWS Backup 與 Amazon FSx 一起使用

AWS Backup 為 NetApp ONTAP 磁碟區備份 Amazon FSx，是一種簡單且符合成本效益的方式來保護您的資料。 AWS Backup 是一種統一的備份服務，旨在簡化備份的建立、還原和刪除作業，同時提供更好的報告和稽核功能。 AWS Backup 可以更輕鬆地制定集中式備份策略，以實現法律、法規和專

業合規性。 AWS Backup 同時提供一個集中的位置，讓您可以執行下列作業，讓保護 AWS 儲存磁碟區、資料庫和檔案系統變得更加簡單：

- 設定及稽核您要備份的 AWS 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 的內置備份功能。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，相對於您對磁碟區進行的任何其他 Amazon FSx 備份 (使用者啟動或自動備份)，並提供與透過 Amazon FSx 主控台進行的備份相同的還原選項。如果您使用 AWS Backup 來管理這些備份，您將獲得額外的功能，例如每小時一次建立排程備份的能力。您可以新增額外的防禦層，藉由將備份儲存在 Vault 中，以保護備份不受意外或惡意刪除的影響。 AWS Backup

由建立的備份視 AWS Backup 為使用者啟動的備份，它們會計入使用者啟動的 Amazon FSx 備份配額中。如需詳細資訊，請參閱 您可以提高的配額。您可以在 Amazon FSx 主控台、CLI 和 API AWS Backup 中檢視和還原由建立的備份。不過，您無法刪除 AWS Backup 在 Amazon FSx 主控台、CLI 或 API 中建立的備份。如需詳細資訊，請參閱開AWS Backup發人員指南 AWS Backup中的入門。

AWS Backup 無法備份離線的磁碟區。

將備份還原至新磁碟區

您可以將磁碟區備份還原至新磁碟區，並使用主控台、CLI 或 API 有效地還原磁碟區的 point-in-time 快照。

還原備份時，所有資料會先寫入 SSD 儲存層，然後服務會根據您為還原的磁碟區設定的分層原則，將資料分層至容量集區儲存體。將備份還原至具有分層原則的磁碟區時`All`，定期背景處理程序會將資料分層至容量集區。將備份還原至分層原則為`Snapshot Only`或的磁碟區時`Auto`，如果檔案系統的 SSD 使用率大於 50%，且冷卻速率是由分層原則的冷卻期間決定，則資料會分層到容量集區。

當您在具有與原始檔案系統不同數FlexGroup量的高可用性 (HA) 配對的檔案系統上還原磁碟區備份時，Amazon FSx 可能會新增其他組成磁碟區以確保組成分均勻分佈。

step-by-step 如需將備份還原至新磁碟區的指示，請參閱將備份還原至新磁碟區。

> **Note**
>
> 還原的磁碟區永遠具有與原始磁碟區相同的磁碟區型式。還原時無法變更音量樣式。

刪除備份

您可以刪除磁碟區的自動每日備份和使用者啟動的備份。刪除備份是永久且無法復原的動作。刪除備份中的任何資料也會被刪除。除非您確定 future 來不再需要該備份，否則請勿刪除備份。如需如何刪除備份的指示，請參閱刪除備份。

您無法在 Amazon FSx 主控台 AWS Backup、CLI 或 API 中刪除由建立且具有類型AWS Backup的備份。如需刪除由建立之備份的相關資訊 AWS Backup，請參閱 AWS Backup 開發人員指南中的刪除備份。

如果磁碟區離線，則無法刪除磁碟區的備份。如需詳細資訊，請參閱 備份和離線磁碟區。

> **Important**
>
> 請勿刪除磁碟區上的通用快照，因為它是用來維持備份之間的增量。刪除磁碟區上的通用快照會導致下一次備份是整個磁碟區，而不僅僅是增量備份。

備份和離線磁碟區

如果磁碟區離線，則無法建立或刪除磁碟區備份。使用 `volume show`ONTAPCLI 命令判斷磁碟區的目前狀態和狀態。

若要使離線磁碟區恢復線上狀態，請使用 `volume online`ONTAPCLI 命令，如下列範例所示：

```
::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

建立使用者啟動的備份

下列程序說明如何使用 Amazon FSx 主控台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 備份和離線磁碟區。

建立使用者啟動的磁碟區備份 (主控台)

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 瀏覽至 [檔案系統]，然後選擇您要備份磁碟區的ONTAP檔案系統。

3. 選擇磁碟區索引標籤。
4. 選擇您要備份的音量。
5. 從 [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。Backup 名稱最多可包含 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)。

您現在已經建立了其中一個檔案系統磁碟區的備份。您可以在 Amazon FSx 主控台中找到所有備份的表格，方法是在左側導覽中選擇備份。您可以搜尋備份的名稱，以及僅顯示相符結果的表格篩選器。

當您按照此程序所述建立使用者啟動的備份時，它會具有類型`USER_INITIATED`，並且在完全可用之前具有`CREATING`狀態。

將備份還原至新磁碟區

下列程序說明如何使用和將 ONTAP 備份的 FSx 還原至新磁碟區。 AWS Management Console AWS CLI

將磁碟區備份還原至新磁碟區 (主控台)

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 在瀏覽窗格中，選擇 [備份]，然後選擇您要還原的 ONTAP 磁碟區備份 FSx。
3. 在右上角的 [動作] 功能表中，選擇 [還原備份]。便會顯示 [從備份建立磁碟區] 頁面。
4. 從下拉式功能表中選擇您要還原備份的 ONTAP 檔案系統和儲存虛擬機器的 FSx。
5. 在 [磁碟區詳細資料] 底下，有幾個選項。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。
6. 在磁碟區大小中，輸入介於 20—314572800 範圍內的任何整數，以指定以 MB (MB) 為單位的大小。
7. 對於磁碟區類型，請選擇讀寫 (RW) 來建立可讀取和可寫入的磁碟區，或選擇資料保護 (DP) 來建立唯讀且可用作或關係目的地的磁碟區。NetApp SnapMirror SnapVault如需詳細資訊，請參閱 磁碟區類型。
8. 對於「結合路徑」，請在檔案系統中輸入要掛載磁碟區的位置。例如，名稱必須有前導正斜線/`vol3`。
9. 若要取得儲存效率，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 提供 ONTAP 儲存效率的 FSx。

10. 對於磁碟區安全性樣式，請選擇 [Unix (Linux)]、[NTFS] 或 [混合]。磁碟區的安全性樣式會決定是否為 NTFS 或 UNIX ACL 提供多重通訊協定存取的偏好設定。多重通訊協定存取不需要混合模式，只建議進階使用者使用。
11. 對於快照政策，請選擇磁碟區的快照政策。如需快照原則的詳細資訊，請參閱快照政策。

    如果您選擇 [自訂原則]，則必須在 [自訂原則] 欄位中指定原則的名稱。自訂原則必須已存在於 SVM 或檔案系統中。您可以使用 ONTAP CLI 或 REST API 建立自訂快照原則。如需詳細資訊，請參閱NetApp ONTAP產品文件中的建立快照原則。
12. 對於分層策略冷卻期間，有效值為 2-183 天。磁碟區的分層原則冷卻期間定義了尚未存取的資料被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策略。
13. 在 [進階] 區段中，對於 [SnapLock組態]，您可以保留預設的 [停用] 設定，或選擇 [啟用] 來設定SnapLock磁碟區。如需有關設定SnapLock Compliance磁碟區或磁碟區的SnapLock Enterprise詳細資訊，請參閱建立SnapLock符合性磁碟區和建立SnapLock企業磁碟區。如需 SnapLock 的相關資訊，請參閱 保護您的資料 SnapLock。
14. 選擇 [確認] 以建立磁碟區。

將磁碟區備份還原至新磁碟區 (CLI)

使用 create-volume-from-backupCLI 命令或等效的 CreateVolumeFromBackupAPI 指令，將磁碟區備份還原至新磁碟區。

- ```
  $ aws fsx create-volume-from-backup --backup-id backup-08e6fc1133fff3532 \
        --name demo --ontap-configuration JunctionPath=/demo, SizeInMegabytes=100000,
   \
        StorageVirtualMachineId=svm-0f04a9c7c27e1908b, TieringPolicy={Name=ALL}
  ```

  成功請求的系統響應：

  ```
  {
        "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",

        }
    }
```

刪除備份

您可以使用 Amazon FSx 主控台、CLI 和 API 刪除自動每日備份和使用者啟動的備份，如下列程序所述。

若要刪除使用建立的備份 AWS Backup，請參閱 AWS Backup 開發人員指南中的刪除備份。

刪除備份原則 (主控台)

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 在控制台儀表板中，從左側導航中選擇「備份」。
3. 從 [備份] 表格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 是您要刪除的備份。
5. 確認已勾選要刪除之備份的核取方塊。
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刪除，且無法復原。

若要刪除備份 (CLI)

- 使用刪除備份 CLI 命令或對等的 DeleteBackup API 動作來刪除 ONTAP 磁碟區備份的 FSx，如下列範例所示。

```
$ aws fsx delete-backup --backup-id backup-a0123456789abcdef
```

系統回應包含要刪除之備份的 ID 及其生命週期狀態，並DELETED指出要求已成功。

```
{
    "BackupId": "backup-a0123456789abcdef",
    "Lifecycle": "DELETED"
}
```

使用快照

快照是 NetApp ONTAP 磁碟區的 Amazon FSx 在某個時間點的唯讀映像檔。快照提供保護，防止意外刪除或修改磁碟區中的檔案。透過快照，您的使用者可以輕鬆檢視和還原先前快照中的個別檔案或資料夾，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以來發生變更的資料，這些資料會消耗系統的 SSD 儲存容量。快照不包含在任何磁碟區備份中。根據預設，磁碟區會使用default快照原則啟用快照。快照儲存在磁碟區根.snapshot目錄中。您可以在任何時間點，每個磁碟區最多儲存 1,023 個快照。達到此限制後，您必須先刪除現有的快照，然後才能建立磁碟區的新快照。

主題

- 快照政策
- 還原個別檔案和資料夾
- 從快照還原檔案
- 刪除快照
- 建立快照自動刪除政策
- 刪除快照
- 停用自動快照
- 快照保留
- 更新磁碟區的快照保留

快照政策

快照政策定義了系統如何為磁碟區建立快照。此原則會指定建立快照的時間、要保留多少個複本，以及命名方式。適用於 ONTAP 的 FSx 有三種內建快照原則：

- `default`
- `default-1weekly`
- `none`

依預設，每個磁碟區都與檔案系統的`default`快照原則相關聯。我們建議對大多數工作負載使用此原則。

此`default`原則會依照下列排程自動建立快照，並刪除最舊的快照複本，以便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**
>
> 快照時間是以檔案系統的時區為基礎，預設為國際標準時間 (UTC)。如需變更時區的相關資訊，請參閱 Sup NetApp port 文件中的顯示和設定系統時區。

此`default-1weekly`原則的運作方式與`default`原則相同，不同之處在於它只會保留每週排程中的一個快照。

此原`none`則不會建立任何快照。您可以將此原則指派給磁碟區，以防止擷取自動快照。

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原則。您可以在 Amazon FSx 主控台、或 Amazon FSx API 中建立或更新磁碟區時選擇快照政策。 AWS CLI如需詳細資訊，請參閱 建立磁碟區 及 更新磁碟區。

還原個別檔案和資料夾

使用 Amazon FSx 檔案系統上的快照，您的使用者可以快速還原個別檔案或資料夾的先前版本。這樣做可讓他們復原儲存在共用檔案系統上的已刪除或變更的檔案。他們在沒有管理員協助的情況下直接在桌面上以自助方式執行此操作。這種自助式方法可提高生產力並減少管理工作量

Linux 和 macOS 用戶端可以檢視磁碟區根`.snapshot`目錄中的快照。Windows 用戶端可以在 [Windows 檔案總管`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

若要從快照還原檔案 (Linux 和 macOS 用戶端)

1. 如果原始檔案仍然存在，而您不希望快照中的檔案覆寫該檔案，請使用 Linux 或 macOS 用戶端重新命名原始檔案，或將其移至其他目錄。
2. 在目`.snapshot`錄中，找出包含要還原之檔案版本的快照集。
3. 將檔案從目`.snapshot`錄複製到檔案原本存在的目錄中。

若要從快照還原檔案 (Windows 用戶端)

Windows 用戶端上的使用者可以使用熟悉的 Windows 檔案總管介面將檔案還原到舊版本。

1. 若要還原檔案，使用者請選擇要還原的檔案，然後從內容選單中選擇 [還原舊版] (按一下滑鼠右鍵)。
2. 然後，使用者可以從「舊版」清單中檢視和還原先前的版本。

快照中的資料是唯讀的。如果您想對「以前的版本」標簽中列出的文件和文件夾進行修改，那么您必須將要修改的文件和文件夾的拷貝保存到可寫入位置，并對拷貝進行修改。

刪除快照

快照只會耗用自上次快照以來已變更之磁碟區上資料的儲存容量。因此，如果您的工作負載快速寫入資料，來自舊資料的快照可能會佔用大量磁碟區的儲存容量。

例如，`volume show-space`ONTAPCLI 命令輸出會顯示 140 KB 的`User Data`。不過，在刪除使用者資料之`User Data`前，磁碟區有 9.8 GB 的空間。即使您已刪除磁碟區中的檔案，快照仍可能會參

考舊的使用者資料。正因為如此，Snapshot Reserve並Snapshot Spill在前面的例子佔用總共 9.8 GB 的空間，即使有幾乎沒有在卷上的用戶數據。

若要釋放磁碟區上的空間，您可以刪除不再需要的舊快照。您可以建立快照自動刪除原則或手動刪除快照來執行此操作。刪除快照會刪除儲存在快照上的變更資料。

建立快照自動刪除政策

您可以建立政策，以便在磁碟區的可用空間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，為磁碟區建立自動刪除原則。

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*以建立磁碟區的 SVM 名稱取代。
- *vol_name*以磁碟區的名稱取代。

對於-trigger，指定下列其中一個值：

- volume— volume 如果您希望刪除快照的臨界值與總使用磁碟區容量臨界值相對應，請使用此選項。觸發刪除快照的已使用磁碟區容量閾值取決於磁碟區的大小，臨界值從已使用容量的百分之 85 至 98% 調整。較小的磁碟區有較小的臨界值，而較大的磁碟區則具有較大的臨界值。
- snap_reserve— 如snap_reserve果您想要根據快照保留中可保留的內容刪除快照，請使用此選項。

```
::> 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。

刪除快照

使用 volume snapshot deleteONTAPCLI 指令手動刪除快照，並將下列預留位置值取代為您的資料：

- *svm_name*以建立磁碟區的 SVM 名稱取代。
- *vol_name*以磁碟區的名稱取代。
- 以*snapshot_name*快照名稱取代。此指令支援的萬用字元 (*) *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。這些快照可用來維持備份之間的增量，不得使用此方法刪除。

```
FsxIdabcdef01234567892::> volume snapshot delete -vserver svm_name -volume vol_name -
snapshot snapshot_name
```

停用自動快照

自動快照會根據預設的快照原則為您的 FSx for ONTAP 檔案系統中的磁碟區啟用。如果您不需要資料的快照 (例如，如果您使用的是測試資料)，可以透過將磁碟區的快照政策設定為none使用 AWS Management Console、 AWS CLI 和 API 和 ONTAP CLI 來停用快照，如下列程序所述。

若要停用自動快照 (AWS 主控台)

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 瀏覽至檔案系統，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

   隨即顯示磁碟區目前設定的「更新磁碟區」對話方塊。
6. 針對 [快照] 原則，選擇 [無]。
7. 選擇 [更新] 以更新磁碟區。

若要停用自動快照 (AWS CLI)

- 使用更新磁碟區 AWS CLI 命令 (或等效的 UpdateVolumeAPI 命令) 將設定SnapshotPolicy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
```

若要停用自動快照 (ONTAPCLI)

將磁碟區的快照政策設定為使用none預設原則來關閉自動快照。

1. 使用 volume snapshot policy showONTAPCLI 命令顯示none原則。

```
::> snapshot policy show -policy none

Vserver: FsxIdabcdef01234567892
                         Number of Is
Policy Name              Schedules Enabled Comment
------------------------ --------- ------- ---------------------------------
none                               0 false   Policy for no automatic snapshots.
    Schedule               Count     Prefix                 SnapMirror Label
    ---------------------- -----     ---------------------- ------------------
    -                          -     -                      -
```

2. 使用 CII 命volume modifyONTAP令將磁碟區的快照原則設定none為停用自動快照。以您的資料取代下列預留位置值：

   - *svm_name*— 使用您的 SVM 的名稱。
   - *vol_name*— 使用您的卷的名稱。

   當系統提示您繼續時，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.
```

快照保留

快照備份保留會設定磁碟區儲存容量的特定百分比來儲存快照副本，預設值為 5%。快照備份保留必須有足夠的空間配置給快照複本，包括磁碟區備份。如果快照複本超過快照保留空間，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副本的磁碟空間百分比。

每當快照佔用 100% 以上的快照保留時，它們就會開始佔用主要 SSD 儲存空間。這個程序稱為快照溢出。當快照繼續佔用使用中的檔案系統空間時，檔案系統有變滿的風險。如果檔案系統因為快照溢滿而變滿，您只能在刪除足夠的快照後建立檔案。

當快照保留中的快照有足夠的可用磁碟空間時，從主要 SSD 層刪除檔案會釋放磁碟空間供新檔案使用，而參照這些檔案的快照複本只會耗用快照備份保留中的空間。

由於無法防止快照佔用大於快照保留量的磁碟空間 (快照保留)，因此請務必為快照保留足夠的磁碟空間，以便主要 SSD 層始終擁有可用空間來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 層刪除檔案並不會產生任何可用空間，因為新建立的快照也會參照所有資料。您必須刪除快照才能釋放儲存空間，才能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保留量。如需詳細資訊，請參閱 更新磁碟區的快照保留。

更新磁碟區的快照保留

您可以使用 NetApp ONTAP CLI 或 API 變更磁碟區上的快照保留量，如下列程序所述。

1. 若要存取 NetApp ONTAP CLI，請執行下列命令，在適用於 NetApp ONTAP 檔案系統的 Amazon FSx 管理連接埠上建立安全殼層工作階段。取代*management_endpoint_ip*為檔案系統管理連接埠的 IP 位址。

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

   如需詳細資訊，請參閱 使用 ONTAP CLI 管理檔案系統。
2. 使用 `snap reserve` ONTAP CLI 命令來變更用於快照副本保留的磁碟空間百分比。*vol_name*以磁碟區的名稱取代，以及 *percent* `with the percent of disk space you want to reserve for Snapshot copies.`

   ```
   ::> snap reserve vol_name 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%。

```
::> snap reserve vol1 25
```

排程複製使用 NetApp SnapMirror

您可以用 NetApp SnapMirror 來排定 ONTAP 檔案系統的 FSx 定期複製到第二個檔案系統，或從第二個檔案系統複製。此功能適用於區域內部署和跨區域部署。

NetApp SnapMirror 以高速複寫資料，因此無論您是在 AWS內部部署的兩個 Amazon FSx 檔案系統之間進行複寫，還是從現場部署複寫到 ONTAP 系統，都能獲得高資料可用性和快速資料複寫。 AWS雖然應該根據 RPO (復原點目標)、RTO (復原時間目標) 和效能考量仔細選擇間隔，但複寫的頻率可以每 5 分鐘排定一次。

當您將資料複製到 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，並在需要時保持可用狀態。不需要外部複寫伺服器。如需有關使用複寫資料 NetApp SnapMirror 的詳細資訊，請參閱 NetApp BlueExp 說明文件中的了解複寫服務。

除了 NetApp ONTAP CLI 和 REST API 之外，您還可以建立資料保護 (DP) 目的地磁碟區 AWS CLI，以便 NetApp SnapMirror使用 Amazon FSx 主控台、和 Amazon FSx API。如需使用 Amazon FSx 主控台建立目標磁碟區的相關資訊 AWS CLI，請參閱建立磁碟區。

您可以使用 NetApp BlueExp 或 NetApp ONTAP CLI 來排定檔案系統的複寫作業。

> **Note**
>
> SnapMirror複寫類型有兩種：磁碟區層級SnapMirror和 SVM 災難復原 (SVMDR)。FSx 僅支援 ONTAP 的磁碟區層級SnapMirror複寫。

使用 NetApp BlueExp 來排程複製

您可以使用 NetApp BlueExp SnapMirror 在您的 FSx 上針對 ONTAP 檔案系統設定複寫。如需詳細資訊，請參閱 NetApp BlueExp 說明文件中的在系統之間複製資料。

使用 NetApp ONTAP CLI 來排程複寫

您可以使用 NetApp ONTAP CLI 來設定排程的磁碟區複寫。如需相關資訊，請參閱 NetApp ONTAP 文件中心中的管理 SnapMirror 磁碟區複寫。

保護您的資料 SnapLock

SnapLock這項功能可讓您將檔案轉換為「一次寫入多讀」(WORM) 狀態，藉此保護檔案，防止在指定的保留期間內進行修改或刪除。您可以用SnapLock來符合法規遵循、保護關鍵業務資料免受勒索軟體攻擊，並為資料提供額外的保護層，防止資料遭到竄改或刪除。

適用於 NetApp ONTAP 的 Amazon FSx 支援合規性和企業保留模式。SnapLock如需詳細資訊，請參閱 SnapLock 合規 及 SnapLock企業。

您可以為在 2023 年 7 月 13 日或之後建立的 ONTAP 檔案系統，在 FSx 上建立SnapLock磁碟區。現有檔案系統將在即將到來的每週維護時段中獲得SnapLock支援。

主題

- SnapLock 的運作方式
- SnapLock 合規
- SnapLock企業
- 使用保留期 SnapLock
- 將檔案提交至 WORM 狀態
- 備份SnapLock磁碟區
- 刪除SnapLock磁碟區

SnapLock 的運作方式

SnapLock可防止檔案遭到刪除、變更或重新命名，協助您符合法規與管理目的。當您建立SnapLock磁碟區時，您會認可檔案寫入一次、讀取多個 (WORM) 儲存空間，並設定資料的保留期限。您的文件可以在指定的時間段內以不可擦除，不可寫入的狀態存儲，也可以無限期地存儲。

> **Important**
>
> 您必須指定磁碟區是否要在建立時使用SnapLock設定。非SnapLock磁碟區在建立之後無法轉換為SnapLock磁碟區。

保留模式

SnapLock具有兩種保留模式：合規性和企業。適用於 NetApp ONTAP 的 Amazon FSx 支持它們。它們具有不同的使用案例，並且某些功能不同，但它們都可以使用 WORM 模型保護您的資料不被修改或刪除。下表說明這些保留模式之間的一些相似性和差異。

SnapLock 功能	SnapLock 合規	SnapLock企業
描述	在合規性磁碟區上轉換為 WORM 的檔案，直到其保留期過期才能刪除。	授權使用者可以使用授權刪除功能，在其保留期到期之前刪除企業磁碟區上轉換為 WORM 的檔案。
使用案例	• 為了解決政府或行業特定的要求，例如美國證券交易委員會規則 17a-4 (f)、《美國國家財務委員會規則》第 4511 條以及美國商品期貨交易委員會 • 為了防止勒索軟件攻擊。	• 為了提高組織的數據完整性和內部合規性。 • 在使用「SnapLock符合性」之前測試保留設定。
自動提交	是	是
事件型保留 (EBR)*	是	是
合法持有*	是	否
特權刪除	否	是
卷追加模式	是	是
SnapLock稽核記錄磁碟區	是	是

* ONTAP CLI 和 REST API 支援 EBR 和法律保留作業。

SnapLock 管理員

您必須擁有SnapLock管理員權限才能對SnapLock磁碟區執行某些動作。 SnapLock管理員權限是在 ONTAP CLI 中的`vsadmin-snaplock`角色中定義的。您必須是叢集管理員，才能建立具有管理員角色的儲存區虛擬機器 (SVM) 管SnapLock理員帳戶。

您可以使用 ONTAP CLI 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、Q 樹狀結構、快照複本和檔案
- 執行SnapLock動作，包括特權刪除和法律保留
- 設定網路檔案系統 (NFS) 和伺服器訊息區 (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) 及網路資訊服務 (NIS) 服務
- 監控作業

下列程序詳細說明如何在 ONTAP CLI 中建立SnapLock系統管理員。您必須以叢集管理員身分登入安全連線，例如安全殼層通訊協定 (SSH)，才能執行此工作。

在 CLI 中使用 vsadmin 快照鎖定角色建立 SVM 管理員帳戶 ONTAP

- 執行下列命令。替換 *SVM_name* 並*SnapLockAdmin*用您自己的信息。

```
cluster1::> security login create -vserver SVM_name -user-or-group-
name SnapLockAdmin -application ssh -authentication-method password -role vsadmin-
snaplock
```

SnapLock稽核記錄磁碟區

SnapLock稽核記錄磁碟區包含SnapLock稽核記錄，其中包含事件的時間戳記，例如建立SnapLock系統管理員的時間、執行授權刪除作業的時間，或在檔案上設定「合法保留」時。SnapLock稽核記錄磁碟區是不可清除的事件記錄。

您必須在與磁碟區相同的 SVM 中建立SnapLock稽核記錄SnapLock磁碟區，才能執行下列動作：

- 開啟或關閉SnapLock企業磁碟區上的授權刪除。
- 對SnapLock合規性磁碟區中的檔案套用「法律保留」。

Warning

- SnapLock稽核記錄磁碟區的最短保留期限為六個月。在此保留期到期之前，即使磁碟區是在 SnapLock Enterprise 模式下建立，也無法刪除SnapLock稽核記錄磁碟區以及與其相關聯的 SVM 和檔案系統。
- 如果使用授權刪除檔案刪除，且其保留期間超過磁碟區的保留期限，則稽核記錄磁碟區會繼承檔案的保留期間。例如，如果使用授權刪除保留期為 10 個月的檔案，而稽核記錄磁碟區的保留期限為六個月，則稽核記錄磁碟區的保留期會延長至 10 個月。

SVM 中只能有一個使用中的SnapLock稽核記錄磁碟區，但 SVM 中的多個SnapLock磁碟區可共用該磁碟區。若要成功掛接SnapLock稽核記錄磁碟區，請將結合路徑設定為`/snaplock_audit_log`。沒有其他磁碟區可以使用此結合路徑，包括不是稽核記錄磁碟區的磁碟區。

您可以在SnapLock稽核記錄磁碟區根`/snaplock_log`目錄下的目錄中找到稽核記錄。有權限的刪除作業會記錄在`privdel_log`子目錄中。會登入「合法保留」開始與結束作業`/snaplock_log/legal_hold_logs/`。所有其他記錄檔都儲存在`system_log`子目錄中。

您可以使用 Amazon FSx 主控台、Amazon FSx API 以及 ONTAP CLI 和 REST API 建立SnapLock稽核日誌磁碟區。AWS CLI

Note

資料保護 (DP) 磁碟區無法做為SnapLock稽核記錄磁碟區使用。

下列程序說明如何在 Amazon FSx 主控台上建立SnapLock稽核日誌磁碟區。

若要建立SnapLock稽核日誌磁碟區，請使用 Amazon FSx 主控台

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 請遵循中建立新磁碟區的程序建立磁碟區。
3. 在「進階」段落中，對於「SnapLock 組態」，選擇啟用。

   選取此核取方塊以確認有關在磁碟區SnapLock上啟用的警告。
4. 針對 [稽核記錄檔量]，選擇 [啟用]

   請確定「結合」路徑已設定為`/snaplock_audit_log`。

5. 請遵循中建立新磁碟區的程序的其餘步驟建立磁碟區。
6. 選擇 [確認] 以建立磁碟區。

若要使用 Amazon FSx API 開啟SnapLock稽核日誌磁碟區，請`AuditLogVolume`在中使用. `CreateSnaplockConfiguration`

存取SnapLock磁碟區中的資料

您可以使用開放式檔案通訊協定 (例如 NFS 和 SMB) 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 保護的資料不會造成效能影響。

您可以在具有 NFS 和 SMB 的SnapLock磁碟區之間複製檔案，但它們不會在目的磁SnapLock碟區上保留其 WORM 屬性。您必須將複製的檔案重新提交至 WORM，以防止它們遭到修改或刪除。如需詳細資訊，請參閱 將檔案提交至 WORM 狀態。

您也可以使用複寫SnapLock資料SnapMirror，但來源磁碟區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，兩者都必須為 [相容性] 或 [企業])。

SnapLock 合規

適用於 NetApp ONTAP 的 Amazon FSx 支援SnapLock合規磁碟區。

使用SnapLock合規性

本節說明符合性保留模式的使用案例和考量事項。

SnapLock法規遵循的使用案例

您可以針對下列使用案例選擇合規性保留模式。

- 您可以使用SnapLock合規來處理政府或特定行業的要求，例如美國證券交易委員會規則 17a-4（f），FINRA 規則 4511 和美國商品期貨交易委員會法規 1.31。 SnapLock針對 NetApp ONTAP 的 Amazon FSx 合規經過評估是否符合這些任務和法規。Cohasset Associates如需詳細資訊，請參閱適用於 NetApp ONTAP 的 Amazon FSx 合規評估報告。
- 您可以使用「SnapLock法規遵循」來補充或增強全面的資料保護策略，以抵禦勒索軟體攻擊。

SnapLock符合性的考量

以下是有關合規性保留模式的一些重要事項。

- 在SnapLock合規性磁碟區上將檔案轉換為寫入一次、讀取多次 (WORM) 狀態之後，任何使用者都無法刪除該檔案的保留期限到期。
- 只有當磁碟區上所有 WORM 檔案的保留期間都過期，且 WORM 檔案已從磁碟區刪除時，才能刪除SnapLock符合性磁碟區。
- 您無法在建立之後重新命名SnapLock相容性磁碟區。
- 您可以用 SnapMirror 來複寫 WORM 檔案，但來源磁碟區和目標磁碟區必須具有相同的保留模式 (例如，兩者都必須為 [相容性])。
- 相容SnapLock性磁碟區無法轉換為SnapLock企業磁碟區，反之亦然。

建立SnapLock符合性磁碟區

您可以使用 Amazon FSx 主控台、Amazon FSx API 以AWS CLI及 ONTAP CLI 和 REST API 建立SnapLock合規磁碟區。

若要使用 Amazon FSx API 建立SnapLock合規磁碟區，請`SnaplockType`在中使用. `CreateSnaplockConfiguration`

下列程序說明如何在 Amazon FSx 主控台上建立SnapLock合規磁碟區。

在 Amazon FSx 主控台上建立SnapLock合規磁碟區

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 請遵循中建立新磁碟區的程序建立磁碟區。
3. 在「進階」段落中，對於「SnapLock 組態」，選擇啟用。

   選取此核取方塊以確認有關在磁碟區SnapLock上啟用的警告。
4. 針對 [保留模式]，選擇 [符合性
5. 在 [稽核記錄磁碟區] 中選擇 [啟用] 和 [停用]。

   如果選擇「啟用」，請確定「結合路徑」設定為`/snaplock_audit_log`。

   如需詳細資訊，請參閱 SnapLock稽核記錄磁碟區。
6. 針對「保留期間」，輸入「預設保留」、「最小保留」及「保留上限」的值。然後為每個單位選擇相應的單位。

   如需詳細資訊，請參閱 使用保留期 SnapLock。
7. 在「自動確認」中，選擇「啟用」和「停用」。

如果您選擇「啟用」，請在「自動確認」期間輸入值並選擇對應的「自動確認」單位。

您可以指定 5 分鐘到 10 年之間的值。

如需詳細資訊，請參閱 自動提交。

8. 對於磁碟區附加模式，請選擇 [啟用] 和 [停用]。

如需詳細資訊，請參閱 卷追加模式。

9. 請遵循中建立新磁碟區的程序的其餘步驟建立磁碟區。
10. 選擇 [確認] 以建立磁碟區。

SnapLock企業

適用於 NetApp ONTAP 的 Amazon FSx 支援SnapLock企業磁碟區。

使用SnapLock企業

本節說明企業保留模式的使用案例和考量事項。

SnapLock企業使用案例

您可以針對下列使用案例選擇企業保留模式。

- 您可以使用「SnapLock企業」來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性。
- 您可以使用 SnapLock Enterprise 來測試保留設定，然後再使用SnapLock符合性。

使用SnapLock企業的注意事項

以下是有關企業保留模式的一些重要事項。

- 您可以用SnapMirror來複寫 WORM 檔案，但來源磁碟區和目標磁碟區必須具有相同的保留模式 (例如，兩者都必須為 Enterprise)。
- SnapLock磁碟區無法從企業轉換為合規性，或從合規轉換為企業。
- SnapLock企業不支援「法律保留」。

特權刪除

「SnapLock企業」和「SnapLock規範遵循」之間的其中一個主要差異在於，SnapLock系統管理員可以開啟 SnapLock Enterprise 磁碟區上的授權刪除功能，以便在檔案的保留期限到期之前刪除檔案。系SnapLock統管理員是唯一可以從SnapLock企業磁碟區刪除檔案的使用者，且該磁碟區已放置有效保留原則。如需詳細資訊，請參閱 SnapLock 管理員。

您可以使用 Amazon FSx 主控台、Amazon FSx API 以及 ONTAP CLI 和 REST API 來開啟或關閉特權刪除。AWS CLI若要開啟授權刪除功能，您必須先在與磁碟區相同的 SVM 中建立SnapLock稽核記錄SnapLock磁碟區。如需詳細資訊，請參閱 SnapLock稽核記錄磁碟區。

若要使用 Amazon FSx API 開啟特權刪除功能，請`PrivilegedDelete`在中使用. `CreateSnaplockConfiguration`

下列程序說明如何在 Amazon FSx 主控台上開啟特權刪除功能。

在 Amazon FSx 主控台上開啟SnapLock企業磁碟區的授權刪除

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 請遵循中建立新磁碟區的程序建立磁碟區。
3. 在「進階」段落中，對於「SnapLock 組態」，選擇啟用。

   選取此核取方塊以確認有關在磁碟區SnapLock上啟用的警告。
4. 針對 [保留] 模式，選擇 [企業]
5. 針對「授權刪除」，選擇「啟用」
6. 請遵循中建立新磁碟區的程序的其餘步驟建立磁碟區。
7. 選擇 [確認] 以建立磁碟區。

> **Note**
>
> 您無法發出具有權限的 delete 命令來刪除一次寫入、讀取多個保留期限過期的 (WORM) 檔案。您可以在保留期間到期後發出正常的刪除作業。

您可以選擇永久關閉授權刪除，但此動作無法復原。如果永久關閉特權刪除，您就不需要有與SnapLock企業磁碟區相關聯的SnapLock稽核記錄磁碟區。

若要使用 Amazon FSx API 永久關閉授權刪除功能，請`PrivilegedDelete`在中使用. `CreateSnaplockConfiguration`

在 Amazon FSx 主控台上永久關閉SnapLock企業磁碟區上的授權刪除

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 請遵循中建立新磁碟區的程序建立磁碟區。
3. 在「進階」段落中，對於「SnapLock 組態」，選擇啟用。

   選取此核取方塊以確認有關在磁碟區SnapLock上啟用的警告。
4. 針對 [保留] 模式，選擇 [企業]
5. 針對「授權刪除」，選擇「永久停用」
6. 請遵循中建立新磁碟區的程序的其餘步驟建立磁碟區。
7. 選擇 [確認] 以建立磁碟區。

建立SnapLock企業磁碟區

您可以使用 Amazon FSx 主控台、Amazon FSx API 以AWS CLI及 ONTAP CLI 和其餘 API 建立SnapLock企業磁碟區。

若要使用 Amazon FSx API 建立SnapLock企業磁碟區，請`SnaplockType`在 `CreateSnaplockConfiguration`.

在 Amazon FSx 主控台上建立SnapLock企業磁碟區

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 請遵循中建立新磁碟區的程序建立磁碟區。
3. 在「進階」段落中，對於「SnapLock 組態」，選擇啟用。

   選取此核取方塊以確認有關在磁碟區SnapLock上啟用的警告。
4. 針對 [保留] 模式，選擇 [企業]
5. 在 [稽核記錄磁碟區] 中選擇 [啟用] 和 [停用]。

   如果選擇「啟用」，請確定「結合路徑」設定為`/snaplock_audit_log`。

   如需詳細資訊，請參閱 SnapLock稽核記錄磁碟區。

6. 針對「保留期間」，輸入「預設保留」、「最小保留」及「保留上限」的值。然後為每個單位選擇相應的單位。

   如需詳細資訊，請參閱 使用保留期 SnapLock。

7. 在「自動確認」中，選擇「啟用」和「停用」。

   如果您選擇「啟用」，請在「自動確認」期間輸入值並選擇對應的「自動確認」單位。

   您可以指定 5 分鐘到 10 年之間的值。

   如需詳細資訊，請參閱 自動提交。

8. 對於「授權刪除」，請選擇「啟用」、「停用」和「永久停用」。

   如需詳細資訊，請參閱 特權刪除。

9. 對於磁碟區附加模式，請選擇 [啟用] 和 [停用]。

   如需詳細資訊，請參閱 卷追加模式。

10. 請遵循中建立新磁碟區的程序的其餘步驟建立磁碟區。
11. 選擇 [確認] 以建立磁碟區。

略過企業模式

如果您使用的是 Amazon FSx 主控台或 Amazon FSx API，則必須擁有 IAM `fsx:BypassSnapLockEnterpriseRetention` 許可，才能刪除包含具有作用中保留政策之 WORM 檔案的SnapLock企業磁碟區。

如需詳細資訊，請參閱 刪除SnapLock磁碟區。

使用保留期 SnapLock

當您建立SnapLock磁碟區時，您可以設定磁碟區的預設保留期間，也可以設定寫入一次、明確讀取多個 (WORM) 檔案的保留期限。在保留期間，您無法刪除或修改受蠕蟲保護的檔案。保留期間是用來計算保留時間。例如，如果您在 2023 年 7 月 14 日午夜將檔案轉換為 WORM，並將保留期限設定為五年，則保留時間會延長到 2028 年 7 月 14 日午夜為止。

如需 WORM 的詳細資訊，請參閱將檔案提交至 WORM 狀態。

保留期政策

保留期間由您指定給下列參數的值決定：

- 預設保留期 — 指派給 WORM 檔案的預設保留期間 (如果您未提供明確的保留期間)。
- 最短保留期 — 可指定給 WORM 檔案的最短保留期。
- 最長保留期 — 可指派給 WORM 檔案的最長保留期間。

> **Note**
>
> 即使在保留期過後，您也無法修改 WORM 檔案。您只能將其刪除或設定新的保留期間，以再次開啟 WORM 防護。

您可以使用數個不同的時間單位來指定保留期間。下表列出支援的特定範圍。

Type	值	備註
秒鐘	0-65,535	
分鐘	0-65,535	
小時	0-24	
天	0-365	
月	0 -12	
年	0-100	
無限	-	永久保留檔案。 適用於 「預設保留」、「最大保留」和「最小保留」。
未指定 *	-	保留檔案，直到您設定保留期間為止。 僅適用於預設保留。

* 當您將檔案轉換為具有未指定保留期限的 WORM 時，系統會提供為SnapLock磁碟區設定的最短保留期限。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限。

過期的保留期

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限，以重新開啟 WORM 防護。WORM 檔案不會在保留期過期後自動刪除。您仍然無法修改 WORM 檔案的內容，即使其保留期已過。

設定SnapLock磁碟區的保留期

您可以使用 Amazon FSx 主控台、Amazon FSx API 以及 ONTAP CLI 和其餘 API 來設定SnapLock磁碟區的保留期間。AWS CLI

若要使用 Amazon FSx API 設定保留期間，請使用`SnaplockRetentionPeriod`組態。

下列程序說明如何在 Amazon FSx 主控台上設定保留期。

在 Amazon FSx 主控台上設定SnapLock磁碟區的保留期

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 請遵循中建立新磁碟區的程序建立磁碟區。
3. 在「進階」段落中，對於「SnapLock 組態」，選擇啟用。

   選取此核取方塊以確認有關在磁碟區SnapLock上啟用的警告。
4. 針對「保留期間」，輸入「預設保留」、「最小保留」及「保留上限」的值。然後為每個單位選擇相應的單位。
5. 請遵循中建立新磁碟區的程序的其餘步驟建立磁碟區。
6. 選擇 [確認] 以建立磁碟區。

將檔案提交至 WORM 狀態

本節討論如何將檔案轉換為一次寫入多次 (WORM) 狀態。它還討論了卷追加模式，這是一種將數據以增量方式寫入到受蠕蟲保護的文件的方法。

自動提交

如果檔案在您指定的一段時間內未修改，您可以使用自動認可將檔案轉換為 WORM。您可以使用 Amazon FSx 主控台、Amazon FSx API 以AWS CLI及 ONTAP CLI 和 REST API 開啟自動認可。

您可以指定 5 分鐘到 10 年之間的自動認可期間。下表列出支援的特定範圍。

單位	值
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 開啟自動認可，請使用`AutocommitPeriod`. `CreateSnaplockConfiguration`

下列程序說明如何在 Amazon FSx 主控台上開啟自動認可。

在 Amazon FSx 主控台上開啟自動認可

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 請遵循中建立新磁碟區的程序建立磁碟區。
3. 在「進階」段落中，對於「SnapLock 組態」，選擇啟用。

   選取此核取方塊以確認有關在磁碟區SnapLock上啟用的警告。
4. 針對「自動確認」，選擇「啟用」
5. 對於「自動確認」期間，輸入值並選擇對應的「自動確認」單位。

   您可以指定 5 分鐘到 10 年之間的值。
6. 請遵循中建立新磁碟區的程序的其餘步驟建立磁碟區。
7. 選擇 [確認] 以建立磁碟區。

卷追加模式

您無法修改受 WORM 保護的檔案中的現有資料。但是，SnapLock允許您使用可附加的文件來維護現有數據的保護。例如，您可以生成日誌文件或保留音頻或視頻流數據，同時以增量方式向它們寫入數據。您可以使用 Amazon FSx 主控台、Amazon FSx API 以及 ONTAP CLI 和 REST API 來AWS CLI開啟或關閉磁碟區附加模式。

更新磁碟區附加模式的需求

- 磁SnapLock碟區必須卸載。
- SnapLock磁碟區必須是空的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`VolumeAppendModeEnabled`在. `CreateSnaplockConfiguration`

下列程序說明如何在 Amazon FSx 主控台上開啟磁碟區附加模式。

在 Amazon FSx 主控台上開啟磁碟區附加模式

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 請遵循中建立新磁碟區的程序建立磁碟區。
3. 在「進階」段落中，對於「SnapLock 組態」，選擇啟用。

   選取此核取方塊以確認有關在磁碟區SnapLock上啟用的警告。
4. 針對磁碟區附加模式，選擇 [啟用]。
5. 請遵循中建立新磁碟區的程序的其餘步驟建立磁碟區。
6. 選擇 [確認] 以建立磁碟區。

事件型保留 (EBR)

您可以使用事件型保留 (EBR) 建立具有關聯保留期間的自訂原則。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`和指`snaplock event-retention apply`令將保留期設定為一年。使用 EBR 時，必須指定磁碟區、目錄或檔案。您在建立 EBR 原則時選取的保留期間會套用至指定路徑中的所有檔案。

EBR 受到 ONTAP CLI 和其他 API 的支援。

> **Note**
>
> ONTAP不支持帶有 FlexGroup 卷的 EBR。

下列程序說明如何建立、套用、修改及刪除 EBR 原則。您必須是SnapLock系統管理員 (具有vsadmin-snaplock角色) 才能在 ONTAP CLI 中完成這些工作。如需詳細資訊，請參閱 SnapLock 管理員。

若要在 CLI 中建立 EBR 原則 ONTAP

執行下列命令。用您自己的信息替換 *p1* 和 *#10 ##*。

```
vs1::> snaplock event-retention policy create -name p1 -retention-period "10 years"
```

若要在 CLI 中套用 EBR 原則 ONTAP

執行下列命令。用您自己的信息替換 *p1* 和 *slc*。如果您要指定 EBR 原則的特定路徑，可以在正斜線 (/) 之後新增路徑。否則，此命令會將 EBR 策略套用至磁碟區上的所有檔案。

```
vs1::> snaplock event-retention apply -policy-name p1 -volume slc -path /
```

若要在 CLI 中修改 EBR 原則 ONTAP

執行下列命令。用您自己的信息替換 *p1* 和 *#5 ##*。

```
vs1::> snaplock event-retention policy modify -name p1 -retention-period "5 years"
```

若要在 CLI 中刪除 EBR 原則 ONTAP

執行下列命令。用您自己的信息替換 *p1*。

```
vs1::> snaplock event-retention policy delete -name p1
```

「NetApp文件中心」中的相關指令：

- 快照鎖定事件保留中止
- 快照鎖定事件保留顯示虛擬伺服器

- 快照鎖定事件保留顯示
- 快照鎖定事件保留政策顯示

合法持有

您可以使用「合法保留」無限期保留 WORM 檔案。法律保留通常用於訴訟目的。在解除「法律保留」之前，無法刪除受「法律保留」限制的 WORM 檔案。

法律保留受 ONTAP CLI 和其他 API 支援。

> **Note**
>
> ONTAP不支援具有 FlexGroup 磁碟區的「法律保留」。

下列程序說明如何啟動和結束「法律保留」。您必須是SnapLock系統管理員 (具有vsadmin-snaplock角色) 才能在 ONTAP CLI 中完成這些工作。如需詳細資訊，請參閱 SnapLock 管理員。

使用 ONTAP CLI 對SnapLock合規性磁碟區中的檔案啟動「法律保留」

執行下列命令。*########## 1#slc_vol1 ### 1#*

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

使用 ONTAP CLI 對SnapLock合規性磁碟區中的所有檔案啟動法律保留

執行下列命令。用您自己的信息替換*## 1* 和 *slc_vol* 1。

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -path /
```

使用 ONTAP CLI 結束SnapLock合規性磁碟區中檔案的法律訴訟保留

執行下列命令。*########## 1#slc_vol1 ### 1#*

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

使用 ONTAP CLI 結束SnapLock合規性磁碟區中所有檔案的法律訴訟保留

執行下列命令。用您自己的信息替換*## 1* 和 *slc_vol* 1。

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -path /
```

> **Note**
>
> 我們建議您在發出法律保留時使-operation-status用snaplock legal-hold show命令監視，以確保它不會失敗。

「NetApp文件中心」中的相關指令：

- 快扣鎖法律保持中止
- 快照鎖法律保留轉儲文件
- 快照鎖法律保持傾倒訴訟
- 扣鎖法律保持秀

備份SnapLock磁碟區

您可以備份SnapLock磁碟區以獲得額外的資料保護。當您還原磁碟區時，SnapLock磁碟區的原始設定(例如預設保留、最小保留和最大保留量) 都會保留。也會保留一次寫入、讀取多個 (WORM) 設定和法律保留。

> **Note**
>
> 您無法備份SnapLock FlexGroup卷宗。

您可以將磁SnapLock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。

如需備份的詳細資訊，請參閱使用備份。

刪除SnapLock磁碟區

如果SnapLock符合性磁碟區上的所有寫入、讀取多個 (WORM) 檔案的保留期間都已過期，您可以刪除相容性磁碟區。

> **Note**
>
> 當您關閉包含SnapLock Enterprise或Compliance磁碟區AWS 帳戶的 FsX 時AWS，ONTAP 的 FSx 會暫停您的帳戶 90 天，且您的資料完整無缺。如果您沒有在 90 天內重新開啟帳戶，無論您的保留設定為何，都AWS會刪除包括SnapLock磁碟區中的資料在內的資料。

如果您有適當的權限，您可以隨時刪除SnapLock企業磁碟區。您必須是 Amazon FSx 管理員。此外，無論您使用的是 Amazon FSx 主控台還是 Amazon FSx API，您都必須擁有 IAM `fsx:BypassSnapLockEnterpriseRetention` IAM 許可，才能刪除包含含有效保留政策之 WORM 資料的SnapLock企業磁碟區。

> **Warning**
>
> SnapLock稽核記錄磁碟區的最短保留期限為六個月。在此保留期到期之前，您無法刪除SnapLock稽核記錄磁碟區、儲存區虛擬機器 (SVM) 或與 SVM 關聯的檔案系統 — 即使磁碟區是以企業模式建立的也一樣。SnapLock如需詳細資訊，請參閱 SnapLock稽核記錄磁碟區。

在 Amazon FSx 主控台上刪除SnapLock企業磁碟區

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 [磁碟區]。
3. 選擇您要刪除的磁碟區。
4. 在動作中，選擇刪除磁碟區。
5. 針對「略過 SnapLock 企業保留」，選擇「是」。
6. 在確認對話方塊中，為「建立最終備份」選擇下列其中一個選項：
   - 選擇 [是] 以進行磁碟區的最終備份。最終備份的名稱隨即顯示。
   - 如果您不想要磁碟區的最終備份，請選擇 [否]。系統會要求您確認磁碟區一旦刪除，就無法再使用自動備份。
7. 在確認刪除欄位**`delete`**中輸入確認磁碟區刪除。
8. 選擇刪除磁碟區。

使用 FSx 中的 Microsoft 活動目錄進行 ONTAP

Amazon FSx 與 Microsoft 活動目錄合作，與您現有的環境集成。Active Directory 是 Microsoft 目錄服務，用來儲存網路上物件的相關資訊，以及協助系統管理員和使用者尋找和使用這項資訊。這些物件通常包括共用資源，例如檔案伺服器和網路使用者和電腦帳戶。

您可以選擇性地將 FSx 用於 ONTAP 儲存區虛擬機器 (SVM) 加入您的 Active Directory 網域，以提供使用者驗證以及檔案和資料夾層級的存取控制。伺服器訊息區塊 (SMB) 用戶端接著就可以使用他們在 Active Directory 中現有的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) 組態移轉至 Amazon FSx，而無需進行任何修改。

當您將適用於 NetApp ONTAP 的 Amazon FSx 加入作用中目錄時，您可以獨立將檔案系統的 SVM 加入作用中目錄。這表示您可以擁有一個檔案系統，其中包含一些 SVM，這些 SVM 已加入至作用中目錄，以及其他非連結的 SVM。

將 SVM 加入作用中目錄之後，您可以更新下列作用中目錄組態屬性：

- DNS 伺服器 IP 位址
- 自我管理的作用中目錄服務帳戶使用者名稱

主題

- 將 SVM 加入自我管理的 Microsoft AD 的先決條件
- 使用活動目錄的最佳實踐
- 將 SVM 加入 Microsoft 活動目錄
- 管理 SVM 作用中目錄組態

將 SVM 加入自我管理的 Microsoft AD 的先決條件

在您將 FSx 適用於 ONTAP SVM 加入自我管理的 Microsoft AD 網域之前，請確定您的作用中目錄和網路符合下列各節所述的需求。

主題

- 內部部署作用中目錄
- 網路組態需求

- 作用中目錄服務帳戶需求

內部部署作用中目錄

請確定您已經擁有可加入 SVM 的內部部署或其他自行管理 Microsoft AD。此活動目錄應具有以下配置：

- 作用中目錄網域控制站網域功能層級為 Windows 伺服器 2000 或更高版本。
- 作用中目錄使用的網域名稱不是單一標籤網域 (SLD) 格式。Amazon FSx 不支持 SLD 域。
- 如果您已定義 Active Directory 站台，請確定 VPC 中與 ONTAP 檔案系統的 FSx 相關聯的子網路定義在相同的 Active Directory 站台中，而且您的 VPC 子網路與 Active Directory 站台上的子網路之間沒有衝突。

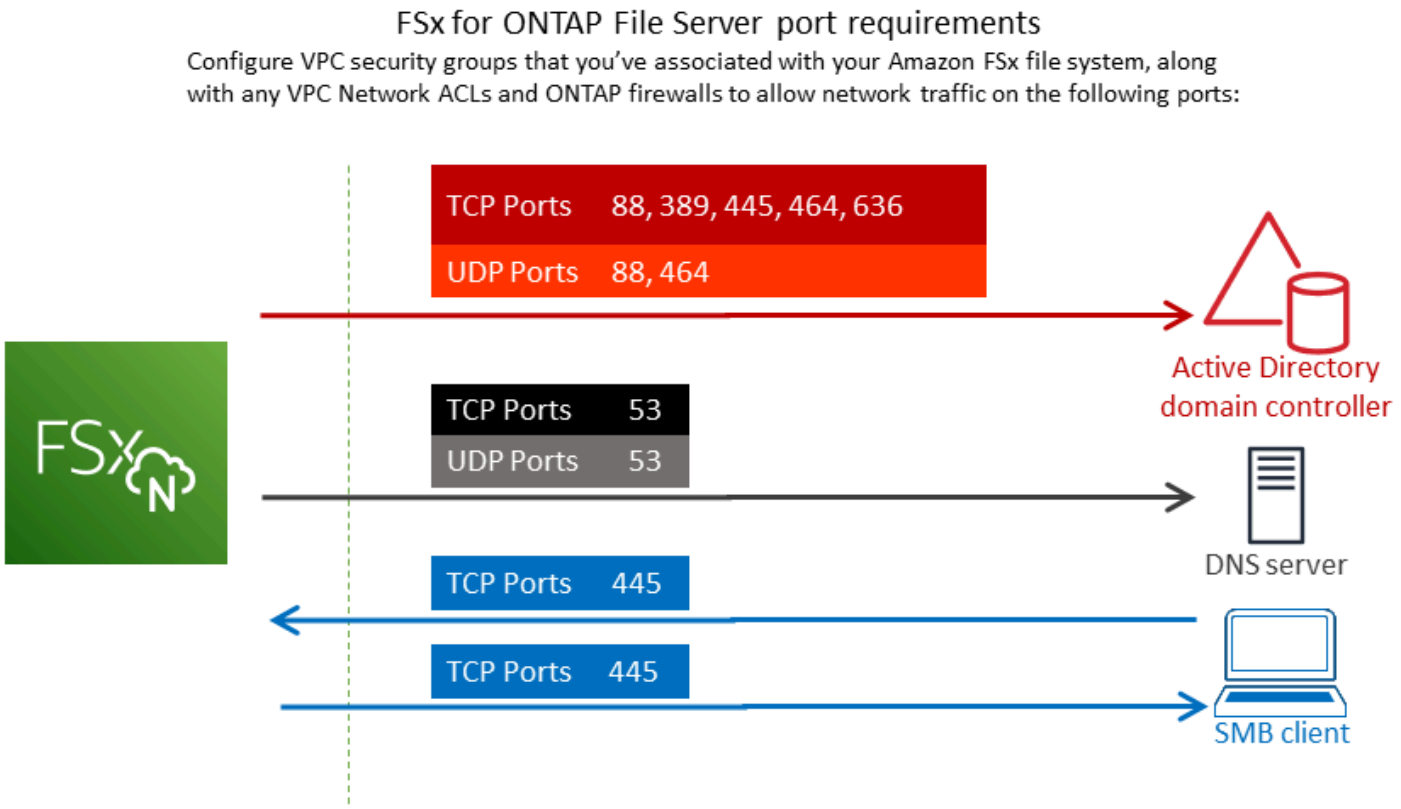
> **Note**
>
> 如果您正在使用 AWS Directory Service，則適用於 ONTAP 的 FSx 不支援將 SVM 加入簡易作用中目錄。

網路組態需求

請確定您有下列網路組態設定，以及可供您使用的相關資訊。

> **Important**
>
> 若要加入使用中目錄的 SVM，您必須確定本主題所述的連接埠允許 SVM 上的所有作用中目錄網域控制站和 iSCSI IP 位址 (iscsi_1 和 iscsi_2 邏輯介面 (LIF)) 之間的流量。

- DNS 伺服器和使用中目錄網域控制站的 IP 位址。
- 您正在建立檔案系統的 Amazon VPC 與使用AWS Direct Connect、AWS VPN或的自我管理作用中目錄之間的連線。AWS Transit Gateway
- 要建立檔案系統之子網路的安全性群組和 VPC Network ACL 必須允許連接埠上的流量，並按照下圖所示的方向執行。



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在適用於每個 Active Directory 網域控制站、DNS 伺服器、FSx 用戶端和 FSx 系統管理員的防火牆上。

> **Important**
>
> 雖然 Amazon VPC 安全群組要求連接埠只能以網路流量起始的方向開啟，但大多數 Windows 防火牆和 VPC 人雲端網路 ACL 都要求連接埠雙向開啟。

作用中目錄服務帳戶需求

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權限。服務帳戶是指已委派特定工作的自我管理 Active Directory 中的使用者帳戶。

至少，服務帳戶必須在您加入 SVM 的 OU 中委派下列權限：

- 能夠重置密碼
- 限制帳戶讀取和寫入資料的能力
- 能夠在計算機對象上設置`msDS-SupportedEncryptionTypes`屬性
- 已驗證寫入 DNS 主機名稱的能力
- 已驗證能夠寫入服務主體名稱
- 能夠創建和刪除計算機對象
- 經過驗證的讀取和寫入帳戶限制功能

這些代表將電腦物件加入您的 Active Directory 所需的最低權限集合。如需詳細資訊，請參閱 Windows Server 文件主題錯誤：已委派控制項的非系統管理員使用者嘗試將電腦加入網域控制站時，會拒絕存取。

若要進一步瞭解如何建立具有正確權限的服務帳戶，請參閱將許可委派給您的 Amazon FSx 服務帳戶。

> **Important**
>
> Amazon FSx 需要在 Amazon FSx 檔案系統整個生命週期內擁有有效的服務帳戶。Amazon FSx 必須能夠完全管理檔案系統，並執行要求其取消加入資源並將資源重新加入至您的作用中目錄網域的任務。這些工作包括取代失敗的檔案系統或 SVM，或修補 NetApp ONTAP 軟體。使用 Amazon FSx 讓您的作用中目錄組態資訊保持在最新狀態，包括服務帳戶登入資料。如需進一步了解，請參閱 使用 Amazon FSx 保持您的活動目錄配置更新。

如果這是您第一次使用 AWS 和 FSx 用於 ONTAP，請確定您已完成初始設定步驟，然後再開始進行 Active Directory 整合。如需詳細資訊，請參閱 為 ONTAP 設定 FSx。

> **Important**
>
> 建立 SVM 之後，請勿移動 Amazon FSx 在 OU 中建立的電腦物件，也不要在 SVM 加入時刪除您的作用中目錄。這樣做會導致您的 SVM 配置錯誤。

使用活動目錄的最佳實踐

這裡有一些建議和指導方針，您應該考慮將 Amazon FSx 的 NetApp ONTAP SVM 加入您的自我管理的 Microsoft 活動目錄。請注意，這些建議作為最佳實踐，但不是必需的。

將許可委派給您的 Amazon FSx 服務帳戶

確保以所需的最低許可設定您提供給 Amazon FSx 的服務帳戶。此外，請將組織單位 (OU) 與其他網域控制站問題分開。

若要將 Amazon FSx SVM 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擁有足夠的權限來執行此工作。不過，最佳作法是使用僅具有執行此操作所需最低權限的服務帳戶。下列程序示範如何僅將 FSx 的 ONTAP SVM 加入您的網域所需的權限委派給您的網域。

在已加入目錄且已安裝 Active Directory 使用者和電腦 MMC 嵌入式管理單元的電腦上執行此程序。

若要為您的 Microsoft 作用中目錄網域建立服務帳戶

1. 請確定您已以網域系統管理員身分登入您的 Microsoft 作用中目錄網域。
2. 開啟使用中目錄使用者和電腦 MMC 嵌入式管理單元。
3. 在工作窗格中，展開網域節點。
4. 找出並開啟您要修改之 OU 的內容 (按一下滑鼠右鍵) 功能表，然後選擇 [委派控制]。
5. 在 [委派控制精靈] 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. 選擇資料夾中的 [只有下列物件]，然後選擇 [電腦物件]。

9. 選擇在此資料夾中建立選取的物件，然後選擇刪除此資料夾中的選取物 然後選擇 Next（下一步）。
10. 在 [顯示這些權限] 下，確定已選取 [一般] 和 [特定屬性]。
11. 對於「權限」，請選擇下列項目：
    - 重設密碼
    - 讀取和寫入帳戶限制
    - 已驗證寫入 DNS 主機名稱
    - 已驗證的寫入服務主要名稱
    - 寫入 msDS-SupportedEncryptionTypes
12. 選擇 Next (下一步)，然後選擇 Finish (完成)。
13. 關閉使用中目錄使用者和電腦 MMC 嵌入式管理單元。

> **Important**
>
> 建立 SVM 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 SVM 配置錯誤。

使用 Amazon FSx 保持您的活動目錄配置更新

如需 Amazon FSx SVM 的不間斷可用性，請在變更自我管理 AD 設定時更新 SVM 的自我管理作用中目錄 (AD) 組態。

例如，假設您的 AD 使用以時間為基礎的密碼重設原則。在這種情況下，一旦密碼重設，請務必使用 Amazon FSx 更新服務帳戶密碼。若要這麼做，請使用 Amazon FSx 主控台、Amazon FSx API 或. AWS CLI 同樣地，如果您的作用中目錄網域的 DNS 伺服器 IP 位址變更，一旦發生變更，就會使用 Amazon FSx 更新 DNS 伺服器 IP 位址。

如果更新的自我管理 AD 組態發生問題，SVM 狀態會切換至 [設定錯誤]。此狀態會在主控台、API 和 CLI 中的 SVM 說明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更正動作。如果問題已解決，請確認 SVM 的狀態已變更為「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 使用中目錄組態 及 使用 ONTAP CLI 修改活動目錄配置。

使用安全群組限制 VPC 內的流量

若要限制虛擬私有雲 (VPC) 中的網路流量，您可以在 VPC 中實作最低權限原則。換句話說，您可以將權限限制為必要的最低權限。若要這麼做，請使用安全性群組規則。如需進一步了解，請參閱 Amazon VPC 安全群組。

為檔案系統的網路介面建立輸出安全性群組規則

為了提高安全性，請考慮使用輸出流量規則設定安全群組。這些規則應該只允許輸出流量到您自我管理的 AD 網域控制站或子網路或安全性群組內。將此安全群組套用至與 Amazon FSx 檔案系統 elastic network interface 相關聯的 VPC。如需進一步了解，請參閱使用 Amazon VPC 進行檔案系統存取控制。

將 SVM 加入 Microsoft 活動目錄

您的組織可能會使用 Active Directory 來管理身分識別和裝置，無論是內部部署還是在雲端。使用 FSx 適用於 ONTAP，您可以透過下列方式將 SVM 直接加入現有的使用中目錄網域：

- 在創建時將新的 SVM 加入活動目錄：
  - 使用 Amazon FSx 主控台中的標準建立選項，為 ONTAP 檔案系統建立新的 FSx，您可以將預設 SVM 加入自我管理的作用中目錄。如需詳細資訊，請參閱 若要建立檔案系統 (主控台)。
  - 使用 Amazon FSx 主控台或 Amazon FSx API AWS CLI，在 ONTAP 檔案系統的現有 FSx 上建立新的 SVM。如需詳細資訊，請參閱 建立儲存區虛擬機器。
- 將現有的 SVM 加入活動目錄：
  - 使用 AWS Management Console AWS CLI、和 API 將 SVM 加入作用中目錄，並在初次嘗試加入失敗時，重新嘗試將 SVM 加入作用中目錄。您也可以為已加入使用中目錄的 SVM 更新某些使用中目錄組態屬性。如需詳細資訊，請參閱 管理 SVM 作用中目錄組態。
  - 使用 NetApp ONTAP CLI 或 REST API 來加入、重新嘗試加入和取消加入 SVM 使用中目錄組態。如需詳細資訊，請參閱 使用 CLI 管理您的 SVM 使用中目錄組態 NetApp 。

> **Important**
>
> - 只有當您使用 Microsoft DNS 做為預設 DNS 服務時，Amazon FSx 才會註冊 SVM 的 DNS 記錄。如果您使用第三方 DNS，則必須在建立 Amazon FSx SVM 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 委派的 FSx 系統管理員、 AWS 委派管理員或具有委派 OU 權限的自訂群組。

當您將 ONTAP SVM 的 FSx 直接加入自我管理的作用中目錄時，SVM 會與您的使用者和現有資源 (包含網域、使用者和電腦的 Active Directory 組態中最上層的邏輯容器) 和使用者和現有資源 (包括現有檔案伺服器) 位於相同的 Active Directory 網域中。

將 SVM 加入作用中目錄時所需的資訊

將 SVM 加入作用中目錄時，無論您選擇的 API 作業為何，都必須提供下列有關作用中目錄的資訊：

- 要為您的 SVM 建立的作用中目錄電腦物件的 NetBIOS 名稱。這是活動目錄中的 SVM 的名稱，它在您的活動目錄中必須是唯一的。請勿使用家用網域的 NetBIOS 名稱。名 NetBIOS 能超過 15 個字元。
- 作用中目錄的完整網域名稱 (FQDN)。FQDN 不能超過 255 個字元。

> **Note**
>
> FQDN 不能使用單一標籤網域 (SLD) 格式。Amazon FSx 不支持 SLD 域。

- 您網域的 DNS 伺服器或網域主機最多三個 IP 位址。

  DNS 伺服器 IP 位址和使用中目錄網域控制站 IP 位址可以位於任何 IP 位址範圍內，但下列情況除外：

  - 與亞馬遜網絡服務擁有的 IP 地址衝突的 IP 地址。 AWS 區域如需依地區分類的 AWS IP 位址清單，請參閱 AWS IP 位址範圍。
  - 位於下列 CIDR 區塊範圍內的 IP 位址：
- 您活動目錄網域上的服務帳戶的使用者名稱和密碼，供 Amazon FSx 加入 SVM 到活動目錄網域時使用。如需服務帳戶需求的詳細資訊，請參閱作用中目錄服務帳戶需求。
- (選擇性) 您加入 SVM 的網域中的組織單位 (OU)。

> **Note**
>
> 如果您將 SVM 加入 AWS Directory Service Active Directory，您必須提供位於為相關目錄物件 AWS Directory Service 建立的預設 OU 內的 OU。 AWS這是因為 AWS Directory Service 不會提供存取您的作用中目錄的預設 `Computers`

OU。例如，如果您的作用中目錄網域是example.com，您可以指定下列OU：OU=Computers,OU=example,DC=example,DC=com。

- (選擇性) 您要委派權限，以便在檔案系統上執行管理動作的網域群組。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 作用中目錄組態

本節說明如何使用 AWS Management Console、 AWS CLI、FSx API 和 ONTAP CLI 執行下列作業：

- 將現有的 SVM 加入作用中目錄
- 修改現有的 SVM 作用中目錄組態
- 從活動目錄中刪除 SVM

若要從作用中目錄移除 SVM，您必須使用 NetApp ONTAP CLI。

主題

- 使用 AWS CLI 和 API 將 SVM 加入作用 AWS Management Console中目錄
- 使用 AWS Management Console、 AWS CLI和 API 更新現有的 SVM 使用中目錄組態
- 使用 CLI 管理您的 SVM 使用中目錄組態 NetApp

使用 AWS CLI 和 API 將 SVM 加入作用 AWS Management Console中目錄

使用下列程序將現有 SVM 加入作用中目錄。在此程序中，SVM 尚未加入作用中目錄。

將 SVM 加入作用中目錄 () AWS Management Console

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 選擇您要加入作用中目錄的 SVM：
   - 在左側導覽窗格中，選擇 [檔案系統]，然後選擇含有您要更新之 SVM 的 ONTAP 檔案系統。
   - 選擇儲存區虛擬機器索引標籤。

   — 或者 —

- 若要顯示所有可用 SVM 的清單，請在左側導覽窗格中展開 ONTAP，然後選擇 [儲存空間虛擬機器]。會顯示您帳戶中所有 SVM 的清 AWS 區域 單。

  從清單中選取要加入作用中目錄的 SVM。

3. 在「SVM 摘要」面板的右上角，選擇「動作」>「加入/更新作用中目錄」。[將 SVM 加入作用中目錄] 視窗隨即顯示。
4. 為您要加入 SVM 的作用中目錄輸入下列資訊：

   - 要為您的 SVM 建立的作用中目錄電腦物件的 NetBIOS 名稱。這是活動目錄中的 SVM 的名稱，它在您的活動目錄中必須是唯一的。請勿使用家用網域的 NetBIOS 名稱。名 NetBIOS 能超過 15 個字元。
   - 作用中目錄的完整網域名稱 (FQDN)。網域名稱不得超過 255 個字元。
   - DNS 伺服器 IP 位址 — 您網域的 DNS 伺服器的 IPv4 位址。
   - 服務帳戶使用者名稱 — 現有 Active Directory 中服務帳戶的使用者名稱。請勿包含網域前置字元或尾碼。例如`EXAMPLE\ADMIN`，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。
   - (選擇性) 組織單位 (OU) — 您要加入 SVM 的目標組織單位的辨別路徑名稱。
   - 委派檔案系統管理員群組 — 您 Active Directory 中可以管理您檔案系統的群組名稱。

     如果您正在使用 AWS Managed Microsoft AD，則必須指定群組，例如 AWS 委派的 FSx 系統管理員、 AWS 委派管理員或具有委派 OU 權限的自訂群組。

     如果您要加入自我管理的作用中目錄，請使用您的作用中目錄中的群組名稱。預設群組為`Domain Admins`。
5. 選擇加入使用中目錄，即可使用您提供的組態將 SVM 加入作用中目錄。

若要將 SVM 加入作用中目錄 (AWS CLI)

- 若要將 ONTAP SVM 的 FSx 加入作用中目錄，請使用 update-storage-virtual-machineCLI 命令 (或等效的 UpdateStorageVirtualMachineAPI 作業)，如下列範例所示。

```
aws fsx update-storage-virtual-machine \
  --storage-virtual-machine-id svm-abcdef0123456789a\
  --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之後，Amazon FSx 會以 JSON 格式傳回其說明，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",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
```

```
        "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["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 使用中目錄組態

使用下列程序來更新已加入作用中目錄之 SVM 的作用中目錄組態。

更新 SVM 使用中目錄組態 () 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]，然後選擇含有您要更新之 SVM 的 ONTAP 檔案系統。
   - 選擇儲存區虛擬機器索引標籤。

     — 或者 —

   - 若要顯示所有可用 SVM 的清單，請在左側導覽窗格中展開 ONTAP，然後選擇 [儲存空間虛擬機器]。

     從清單中選取您要更新的 SVM。
3. 在「SVM 摘要」面板上，選擇「動作」>「加入/更新作用中目錄」。更新 SVM 使用中目錄組態視窗隨即出現。
4. 您可以在此視窗中更新下列作用中目錄組態特性。

- DNS 伺服器 IP 位址 — 您網域的 DNS 伺服器的 IPv4 位址。
- 服務帳戶使用者名稱 — 現有 Active Directory 中服務帳戶的使用者名稱。請勿包含網域前置字元或尾碼。對於 `EXAMPLE\ADMIN`，請使用 `ADMIN`。
- 服務帳戶密碼 — 作用中目錄服務帳戶的密碼。

5. 輸入更新之後，請選擇 [更新作用中目錄] 以進行變更。

使用下列程序來更新已加入作用中目錄之 SVM 的作用中目錄組態。

更新 SVM 使用中目錄組態 () AWS CLI

- 若要使用 AWS CLI 或 API 更新 SVM 的使用中目錄組態，請使用 update-storage-virtual-machineCLI 命令 (或等效的 UpdateStorageVirtualMachineAPI 作業)，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 CLI 管理您的 SVM 使用中目錄組態 NetApp

您可以使用 NetApp ONTAP CLI 將 SVM 加入和取消加入作用中目錄，以及修改現有的 SVM 使用中目錄組態。

使用 ONTAP CLI 將 SVM 加入作用中目錄

您可以使用 ONTAP CLI 將現有的 SVM 加入作用中目錄，如下列程序所述。即使您的 SVM 已加入作用中目錄，您也可以執行此操作。

1. 若要存取 NetApp ONTAP CLI，請執行下列命令，在適用於 NetApp ONTAP 檔案系統的 Amazon FSx 管理連接埠上建立安全殼層工作階段。取代*management_endpoint_ip*為檔案系統管理連接埠的 IP 位址。

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

如需詳細資訊，請參閱 使用 ONTAP CLI 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 位址，為您的作用中目錄建立 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 DNS 伺服器的連線，請執行下列命令。用您自己的信息替換 *svm_name*。

```
FsxId0ae30e5b7f1a50b6a::>vserver services name-service dns check -vserver svm_name

                            Name Server
Vserver       Name Server     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 加入您的作用中目錄，請執行下列命令。請注意，您必須指定一computer_name個不存在於您的作用中目錄中，並提供的目錄 DNS 名稱-domain。針對-OU，輸入您要 SVM 加入的 OU，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
```

若要驗證您的作用中目錄連線的狀態，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.
```

4. 如果您在此加入後無法存取共享，請判斷您用來存取共享的帳戶是否具有權限。例如，如果您使用預設Admin帳戶 (委派的系統管理員) 搭配 AWS 受管理 Active Directory，您必須在 ONTAP 中執行下列命令。netbios_domain與您的活動目錄的域名相對應（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 修改活動目錄配置

您可以使用 ONTAP CLI 來修改現有的活動目錄配置。

1. 若要存取 NetApp ONTAP CLI，請執行下列命令，在適用於 NetApp ONTAP 檔案系統的 Amazon FSx 管理連接埠上建立安全殼層工作階段。取代*management_endpoint_ip*為檔案系統管理連接埠的 IP 位址。

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

如需詳細資訊，請參閱 使用 ONTAP CLI 管理檔案系統。

2. 執行下列命令以暫時關閉 SVM 的 CIFS 伺服器：

```
FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
```

3. 如果您需要修改作用中目錄的 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命令來驗證作用中目錄 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欄位，取代：

   - *####*，如果您想要修改 SVM 的 NetBIOS (機器帳戶) 名稱。
   - *##*，如果你想修改域的名稱。這應該與本節 (`corp.example.com`) 步驟 3 中所述的 DNS 網域項目相對應。
   - `organizational_unit`，如果您要修改 OU (`OU=Computers,OU=example,DC=corp,DC=example,DC=com`)。

   您將需要重新輸入您用來將此裝置加入作用中目錄的使用中目錄認證。

   ```
   ::>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`命令驗證活動目錄連接的連接狀態。

5. 當您完成修改作用中目錄和 DNS 組態時，請執行下列命令來備份 CIFS 伺服器：

   ```
   ::>vserver cifs modify -vserver svm_name -status-admin up
   ```

使用 ONTAP CLI 從 SVM 取消加入作用中目錄 NetApp

NetApp ONTAP CLI 也可以按照以下步驟用於從活動目錄取消加入 SVM：

1. 若要存取 NetApp ONTAP CLI，請執行下列命令，在適用於 NetApp ONTAP 檔案系統的 Amazon FSx 管理連接埠上建立安全殼層工作階段。取代*management_endpoint_ip*為檔案系統管理連接埠的 IP 位址。

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

   如需詳細資訊，請參閱 使用 ONTAP CLI 管理檔案系統。

2. 執行下列命令，從作用中目錄刪除未連接裝置的 CIFS 伺服器。若要讓 ONTAP 刪除 SVM 的機器帳戶，請提供您最初用來將 SVM 加入作用中目錄的認證。

   ```
   FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
   ```

3. 如果您需要修改作用中目錄的 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.ADEXAMPLE.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，以刪除作用中目錄的 DNS 伺服器：

```
::vserver services name-service dns delete -vserver svm_name
```

如果您看到類似下列的警告 (指出dns應該移除為)，ns-switch而且您不打算將此裝置重新加入 Active Directory，則可以移除這些項目。ns-switch

```
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. (選擇性) 執行下列命令dns來移除的ns-switch項目。驗證來源順序，然後修改以便只包含列出的其他來源，sources以移除hosts資料庫的dns項目。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. (選擇性) 修改僅包含的資料庫主機，以移除項目files。dns sources

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts
 -sources files
```

適用於 NetApp ONTAP 性能的 Amazon FSx

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

主題

ONTAP 檔案系統的 FSx 效能測量方式

檔案系統效能是根據其延遲、輸送量和每秒 I/O 作業數 (IOPS) 來衡量。

Latency (延遲)

Amazon FSx for NetApp ONTAP 可透過固態硬碟 (SSD) 儲存提供低於一毫秒的檔案操作延遲，以及容量集區儲存的延遲時間為數十毫秒。除此之外，Amazon FSx 在每個檔案伺服器上都有兩層讀取快取 (NVMe (非揮發性記憶體快速) 磁碟機和記憶體內部，可在您存取最頻繁讀取的資料時提供更低的延遲。

輸送量和 IOPS

每個 Amazon FSx 檔案系統可提供高達數千 GB 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 數量，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。

支援中小企業多通道與 NFS 連線

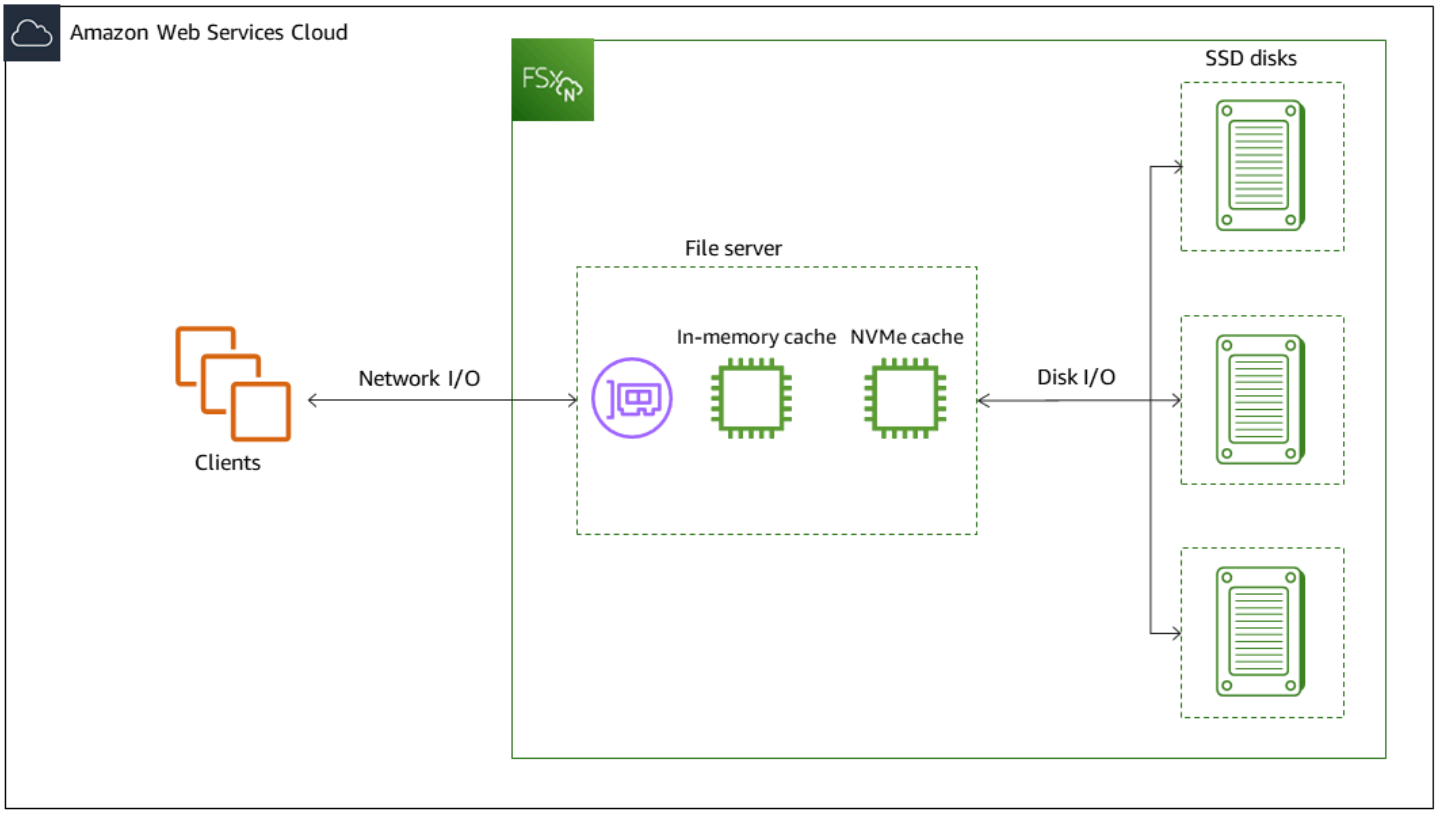
使用 Amazon FSx，您可以設定 SMB 多通道，在單一 SMB 工作階段中提供客戶ONTAP與用戶端之間的多個連線。SMB 多通道在用戶端與伺服器之間同時使用多個網路連線，以彙總網路頻寬，達到最大的使用率。如需使用 NetApp ONTAP CLI 設定 SMB 多通道的相關資訊，請參閱設定 SMB 多通道的效能和備援。

NFS 用戶端可以使用nconnect掛載選項，將多個 TCP 連線 (最多 16 個) 與單一 NFS 掛載相關聯。這類 NFS 用戶端會以循環配置資源的方式將檔案作業多工處理至多個 TCP 連線，因此可從可用的網路頻寬獲得更高的輸送量。支援 NFSv3 和 NFSv4 以上版本。nconnect Amazon EC2 執行個體網路頻寬說明全雙工每個網路流量頻寬限制為 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。請參閱您的 NFS 用戶端文件，以確認您的用戶端版本nconnect是否支援。如需有關NetApp ONTAP支援的詳細資訊nconnect，請參閱對 NFSv4 4.1 的ONTAP支援。

演出詳情

若要詳細瞭解適用於 NetApp ONTAP 效能模型的 Amazon FSx，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 (無論是存在於內部部署 AWS 或內部部署) 都可透過一或多個彈性網路介面 (ENI) 存取您的檔案系統。這些網路界面位於您與檔案系統建立關聯的 Amazon VPC 中。每個檔案系統 ENI 背後都有一個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的記憶體內快取和 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的 SSD 磁碟，代管您的檔案系統資料。

這些元件如下圖所示。



與這些架構元件 (網路界面、記憶體內快取、NVMe 快取和儲存磁碟區) 相對應，是適用於 NetApp ONTAP 檔案系統的 Amazon FSx 的主要效能特性，可判斷整體輸送量和 IOPS 效能。

- 網路 I/O 效能：用戶端與檔案伺服器之間的要求傳輸量 /IOPS (彙總)
- 檔案伺服器上的記憶體內快取和 NVMe 快取大小：可容納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要求傳輸量 /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、記憶體內和 NVMe 快取大小 — 完全取決於輸送量容量，而第三個 — 磁碟 I/O 效能 — 則由輸送量容量與 SSD IOPS 的組合決定。

以檔案為基礎的工作負載通常是尖峰，其特點是短暫而密集的高 I/O 時間，並且在突發之間有很多閒置時間。為了支援尖峰的工作負載，除了檔案系統全年無休的基準速度外，Amazon FSx 還提供網路 I/O 和磁碟 I/O 作業在一段時間內提升到更高速度的功能。Amazon FSx 使用網路 I/O 信用機制根據平均使用率分配輸送量和 IOPS — 檔案系統在輸送量和 IOPS 使用量低於其基準限制時會累積積分，並且可以在執行 I/O 作業時使用這些積分。

寫入作業使用的網路頻寬是讀取作業的兩倍。寫入作業必須在次要檔案伺服器上複寫，因此單一寫入作業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 (適用於 ONTAP) 建立兩種類型的檔案系統。具有單一高可用性 (HA) 對檔案伺服器的檔案系統稱為向上擴充檔案系統。具有多個 HA 配對的檔案系統稱為向外延展檔案系統。如需詳細資訊，請參閱 高可用性 (HA) 配對。

適用於 ONTAP 異地同步備份和單一可用區檔案系統的 FSx 可透過 SSD 儲存提供低於一毫秒的檔案作業延遲，而容量集區儲存則可提供數十毫秒的延遲。此外，符合下列需求的檔案系統還提供 NVMe 讀取快取，以減少讀取延遲並增加頻率讀取資料的 IOPS：

- 異地備份檔案系統
- 在 2022 年 11 月 28 日之後建立的單一可用區可用區向上擴充檔案系統，輸送量容量至少為 2 Gbps

下表顯示檔案系統可擴充至的輸送量容量，視高可用性 (HA) 配對的數量和可用性等因素而 AWS 區域定。

Scale-up

這些效能規格適用於向上擴充的檔案系統。

針對向上擴充檔案系統，每個 HA 配對 SSD 儲存的最大輸送量

	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)		提供適用於 ONTAP AWS 區域 的 FSx 的所有其他地方	
	讀取輸送量 (MBP)	寫入輸送量 (MBP)	讀取輸送量 (MBP)	寫入輸送量 (MBP)
單一可用區	4,096*	1,000	2,048	750
異地同步備份	4,096*	1,800	2,048	1,300

> **Note**
>
> * 若要佈建 4 Gbps 的輸送容量，您的檔案系統必須設定至少 5,120 GiB 的固態硬碟儲存容量和 160,000 個固態硬碟 IOPS。

Scale-out

這些效能規格適用於向外延展檔案系統。

針對向外擴充檔案系統，每個 HA 配對的 SSD 儲存最大輸送量

	讀取輸送量 (MBP)	寫入輸送量 (MBP)
單一可用區向外擴充	6,144*	1,100*

> **Note**
>
> * 每 HA 對 (最多 12 個)。如需詳細資訊，請參閱 高可用性 (HA) 配對。

儲存容量對效能的影響

您的檔案系統可達到的最大磁碟輸送量和 IOPS 層級為下列項目的較低：

- 檔案伺服器所提供的磁碟效能層級，根據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 數目所提供的磁碟效能等級

依預設，檔案系統的 SSD 儲存可提供下列磁碟輸送量和 IOPS 層級：

- 磁碟輸送量 (每 TiB 儲存裝置的 MBP)：768
- 磁碟 IOPS (每次儲存 TiB 的 IOP)：3,072

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容量。檔案系統的輸送量容量會決定網路 I/O 效能的等級，或是每個託管檔案系統的檔案伺服器可以透過網路向存取檔案的用戶端提供檔案資料的速度。更高的輸送量容量具有更多的記憶體和非揮發性記憶體快速 (NVMe) 儲存體，可快取每部檔案伺服器上的資料，以及每個檔案伺服器支援更高層級的磁碟 I/O 效能。

建立檔案系統時，您可以選擇性地佈建較高層級的 SSD IOPS。檔案系統可達到的最大 SSD IOPS 等級也取決於檔案系統的輸送量容量，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，以及基準和成組分解層次，以及對應的檔案伺服器上用於快取的記憶體量 AWS 區域。

Single-AZ (scale-up)

這些效能規格適用於指定的 2022 年 11 月 28 日之後建立的單一可用區擴充檔案系統。 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輸送量容量	網路輸送量容量 (MBP)		網絡 IOPS	記憶體內快取 (GB)	NVMe 讀取快取 (GB)	磁碟輸送量 (MBP)		固態硬碟 IOPS *	
	基準線	爆裂				基準線	爆裂	基準線	爆裂

FSx輸送量容量	網路輸送量容量 (MBP)		網絡 IOPS	記憶體內快取 (GB)	NVMe 讀取快取 (GB)	磁碟輸送量 (MBP)		固態硬碟 IOPS *	
128	188	1,500	數萬條基線	16	–	128	1,250	6,000	40,000
256	375	1,500		32	–	256	1,250	12,000	40,000
512	750	1,500	數十萬條基線	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**
>
> * 您的 SSD IOPS 只會在您存取未快取到檔案伺服器的記憶體內快取或 NVMe 快取中的資料時使用。

這些效能規格適用於提供 FSx for ONTAP 的所有其他單一 AWS 區域 可用區擴充檔案系統。

提供適用於 ONTAP FSx 的所有 AWS 區域 其他檔案系統的效能規格

FSx 輸送量容量	網路輸送量容量 (MBP)		網絡 IOPS	記憶體內快取 (GB)	磁碟輸送量 (MBP)		固態硬碟 IOPS *	
	基準線	爆裂			基準線	爆裂	基準線	爆裂
128	150	1,250	數萬條基線	16	128	600	6,000	18,750
256	300	1,250		32	256	600	12,000	18,750
512	625	1,250	數十萬條基線	64	512	600	18,750	–
1,024	1,500	–		128	1,024	–	40,000	–

FSx 輸送量容量	網路輸送量容量 (MBP)		網絡 IOPS	記憶體內快取 (GB)	磁碟輸送量 (MBP)		固態硬碟 IOPS *	
2,048	3,125	–		256	2,048	–	80,000	–

> **Note**
>
> * 您的 SSD IOPS 只會在您存取未快取到檔案伺服器的記憶體內快取或 NVMe 快取中的資料時使用。

Single-AZ (scale-out)

這些效能規格適用於向外延展檔案系統。

向外延展檔案系統的效能規格

FSx 輸送量容量	網路輸送量容量 (MBP)		網絡 IOPS	記憶體內快取 (GB)	磁碟輸送量 (MBP)		固態硬碟 IOPS *	
	基準線	爆裂			基準線	爆裂	基準線	爆裂
3,072**	6,250	–	數十萬條基線	128	3,072	–	100,000	–
6,144**	12,500	–		256	6,144	–	200,000	–

> **Note**
>
> * 您的 SSD IOPS 只會在您存取未快取到檔案伺服器的記憶體內快取或 NVMe 快取中的資料時使用。
> ** 每 HA 對 (最多 12 個)。如需詳細資訊，請參閱 高可用性 (HA) 配對。

Multi-AZ (scale-up)

這些效能規格適用於指定的 2022 年 11 月 28 日之後建立的異地同步備份擴充檔案系統。 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 輸送量容量	網路輸送量容量 (MBP)		網絡 IOPS	記憶體內快取 (GB)	NVMe 快取 (GB)	磁碟輸送量 (MBP)		固態硬碟 IOPS *	
	基準線	爆裂				基準線	爆裂	基準線	爆裂
128	188	1,500	數萬條基線	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	數十萬條基線	64	950	512	1,250	20,000	40,000
1,024	1,500	–		128	1,900	1,024	1,250	40,000	–
2,048	3,125	–		256	3,800	2,048	–	80,000	–
4,096	6,250	–		512	7,600	4,096	–	160,000	–

> **Note**
>
> * 您的 SSD IOPS 只會在您存取未快取到檔案伺服器的記憶體內快取或 NVMe 快取中的資料時使用。

這些效能規格適用於提供 FSx for ONTAP 的所有其他異 AWS 區域 地同步備份擴充檔案系統。

提供適用於 ONTAP FSx 的所有 AWS 區域 其他檔案系統的效能規格

FSx 輸送量容量	網路輸送量容量 (MBP)		網絡 IOPS	記憶體內快取 (GB)	NVMe 快取 (GB)	磁碟輸送量 (MBP)		固態硬碟 IOPS *	
	基準線	爆裂				基準線	爆裂	基準線	爆裂
128	150	1,250	數萬條基線	16	150	128	600	6,000	18,750
256	300	1,250		32	300	256	600	12,000	18,750
512	625	1,250	數十萬條基線	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**
>
> * 您的 SSD IOPS 只會在您存取未快取到檔案伺服器的記憶體內快取或 NVMe 快取中的資料時使用。

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。

配置 2 TiB SSD 儲存容量和 512 Mbps 輸送量容量的向上擴充檔案系統具有下列輸送量等級：

- 網路輸送量 — 625 MBps 基準線和 1,250 MBps 突增 (請參閱輸送量容量表格)
- 磁碟輸送量 — 512 MB 基準線和 600 兆比特突發。

因此，存取檔案系統的工作負載將能夠在檔案伺服器內快取和 NVMe 快取中快取的主動存取資料上執行的檔案作業，驅動高達 625 Mbps 的基準線和 1,250 MBPS 突發輸送量。

管理安裝專用資源的 FSx

使用 AWS Management Console AWS CLI、和 ONTAP CLI 和 API，您可以針對 ONTAP 資源的 FSx 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 (SVM)、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、密碼需求、SMB 和 iSCSI 通訊協定、網路可存取性

主題

管理 ONTAP 檔案系統的 FSx

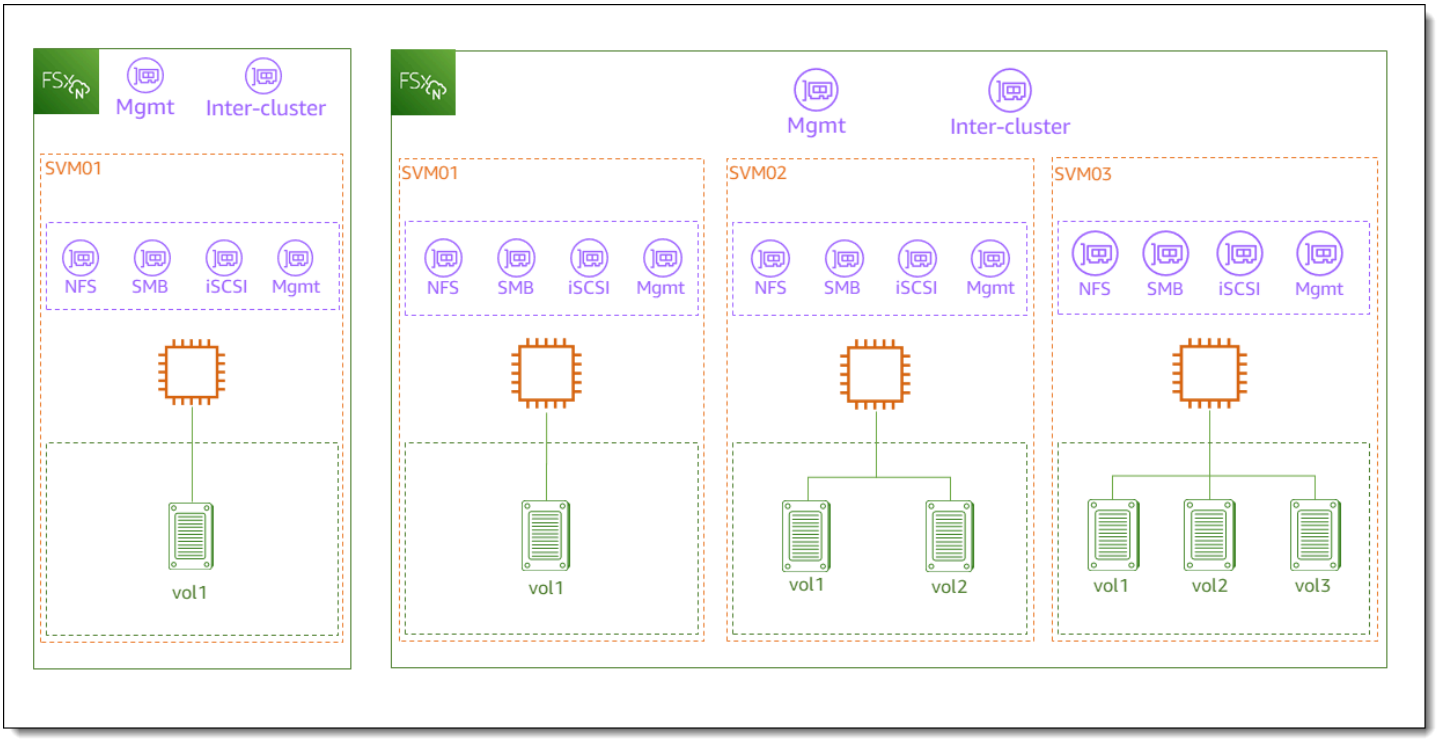
檔案系統是主要的 Amazon FSx 資源，類似於現場部署 ONTAP 叢集。您可以指定檔案系統的固態硬碟 (SSD) 儲存容量和輸送量容量，並選擇要在其中建立檔案系統的虛擬私有雲 (VPC)。每個檔案系統都有一個管理端點，您可以使用 ONTAP CLI 或 REST API 來管理資源和資料。

檔案系統資源

適用於 NetApp ONTAP 檔案系統的 Amazon FSx 由下列主要資源組成：

- 檔案系統本身的實體硬體，包括檔案伺服器和儲存媒體。
- 一或多個高可用性 (HA) 檔案伺服器配對，主控您的儲存區虛擬機器 (SVM)。向上擴充檔案系統具有一個 HA 配對，而向外延展檔案系統則具有兩個或多個 HA 配對。每個 HA 配對都有一個稱為彙總的儲存池。所有 HA 配對的彙總集合構成了您的 SSD 儲存層。
- 主控檔案系統磁碟區並擁有自己的認證和存取管理的一或多個儲存區虛擬機器 (SVM)。
- 一或多個磁碟區，可虛擬組織您的資料，並由您的用戶端掛接。

下圖說明具有單一 HA 配對之 ONTAP 檔案系統的向上擴充 FSx 架構，以及其主要資源之間的關係。左邊的 ONTAP 檔案系統 FSx 是最簡單的檔案系統，有一個 SVM 和一個磁碟區。右側的檔案系統具有多個 SVM，有些 SVM 具有多個磁碟區。檔案系統和 SVM 各有多個管理端點，而 SVM 也有資料存取端點。



為 ONTAP 檔案系統建立 FSx 時，您可以定義下列屬性：

- 部署類型 — 檔案系統的部署類型 (異地同步備份或單一可用區)。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，並提供向外延展的檔案系統。異地同步備份檔案系統也透過複寫您的資料並支援同一個內部多個可用區域的容錯移轉，提供額外的復原能力。 AWS 區域

- 儲存容量 — 這是固態硬碟儲存容量，向上擴充檔案系統最高可達 192 TB (TiB)，向外擴充檔案系統最高可達 1 個 PB 位元組 (PIB)。
- 固態硬碟 IOPS — 依預設，每 GB 的 SSD 儲存裝置包含三個 SSD IOPS (最高可達您的檔案系統組態支援的最大值)。您可以視需要選擇性佈建額外的 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 — 用於檔案系統建立的管理和資料存取端點的 VPC 和子網路。對於異地同步備份檔案系統，您還可以定義 IP 位址範圍和路由表。
- 加密 — 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使用 NetApp ONTAP CLI 和 REST API 來管理檔案系統。

您可以使用 ONTAP CLI 或 REST API 來管理 NetApp ONTAP 檔案系統的 FSx。您也可以在 Amazon FSx 檔案系統與其他 ONTAP 部署 (包括其他 Amazon FSx 檔案系統) 之間建 SnapVault 立關係 SnapMirror 或建立關係。ONTAP 檔案系統的每個 FSx 都具有下列檔案系統端點，可提供應用程式存取 NetApp 權：

- 管理 — 使用此端點透過安全殼層 (SSH) 存取 NetApp ONTAP CLI，或將 NetApp ONTAP REST API 與您的檔案系統搭配使用。
- 叢集間 — 使用或使用進行快取設定複製時，請使 NetApp SnapMirror 用此端點。 NetApp FlexCache

如需詳細資訊，請參閱 使用應用模組管理 ONTAP 資源的 FSx NetApp 及 排程複製使用 NetApp SnapMirror。

高可用性 (HA) 配對

ONTAP 檔案系統的每個 FSx 都由一或多個高可用性 (HA) 對的檔案伺服器提供支援，在作用中-待命組態中。在此組態中，有一個慣用的檔案伺服器會主動提供流量，而次要檔案伺服器則會在使用中伺服器無法使用時接管。適用於 ONTAP 向上擴充檔案系統的 FSx 由一對 HA 提供支援，可提供高達 4 Gbps 的輸送量容量和 16 萬個固態硬碟 IOP。適用於 ONTAP 水平擴充檔案系統的 FSx 由多達 12 個 HA 配對提供支援，可提供高達 72 Gbps 的輸送量容量和 2,400,000 個固態硬碟 IOPS (6 GBP 的輸送量容量和每個高可用性配對 20 萬個固態硬碟 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 儲存建議您應使用的 HA 配對數量。您也可以根據工作負載和效能需求，手動選擇 HA 配對的數量。如果您的檔案系統需求

滿足高達 4 Gbps 的輸送量容量和 160,000 SSD IOPS，以及多個 HA 配對 (如果您的工作負載需要更高等級的效能延展性)，建議您使用單一 HA 配對。

每個 HA 配對都有一個彙總，也就是實體磁碟的邏輯集合。

> **Note**
>
> 您無法將 HA 配對新增至現有的檔案系統。相反地，您可以使用、或將資料從備份還原至新檔案系統 SnapMirror AWS DataSync，在檔案系統之間移轉資料 (使用不同的 HA 配對)。

為 ONTAP 檔案系統建立 FSx

本節說明如何使用 Amazon FSx 主控台或 Amazon FSx API 為 ONTAP 檔案系統建立 FSx。 AWS CLI 您可以在您 AWS 帳戶 擁有的虛擬私有雲 (VPC) 中建立檔案系統，或在其他人與您共用的 VPC 中建立檔案系統。在您身為參與者的 VPC 中建立異地同步備份檔案系統時，需要考量一些事項。這些考量將在本主題中說明。

根據預設，當您從 Amazon FSx 主控台建立新檔案系統時，Amazon FSx 會自動建立包含單一儲存虛擬機器 (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，您可以選擇性地將 SVM 加入作用中目錄，以便透過伺服器訊息區 (SMB) 通訊協定從 Windows 和 macOS 用戶端存取。建立檔案系統之後，您可以視需要建立額外的 SVM 和磁碟區。

若要建立檔案系統 (主控台)

此程序會使用「標準建立」建立選項，為 ONTAP 檔案系統建立 FSx，其中包含您根據需求自訂的組態。如需有關使用「快速建立」(Quick create) 建立選項來快速建立具有預設組態參數集之檔案系統的資訊，請參閱步驟 1：為 NetApp ONTAP 檔案系統建立 Amazon FSx。

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
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 做為 NetApp ONTAP，然後選擇 [下一步]。
4. 在「建立方式」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：

- 在 [檔案系統名稱-選用] 中，輸入檔案系統的名稱。當您命名檔案系統時，尋找和管理檔案系統會比較容易。您最多可以使用 256 個 Unicode 字母、空格和數字，再加上下列特殊字元：+ - = 。 _ : /
- 對於部署類型，請選擇異地同步備份或單一可用
  - 異地同步備份檔案系統會複寫您的資料，同 AWS 區域時支援跨多個可用區域的容錯移轉。
  - 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。

    > **Note**
    >
    > 如果您想要建立具有兩個或多個高可用性 (HA) 配對 (最多 12 個) 的檔案系統，請選擇單一可用區。如需詳細資訊，請參閱 高可用性 (HA) 配對。

  如需詳細資訊，請參閱 可用性與持久性。
- 如需 SSD 儲存容量，請輸入檔案系統的儲存容量 (以 GB 為單位)。輸入介於 1,024 至 1,048,576 GiB 範圍內的任何整數 (最多 1 個百位元組 [PIB])。

  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。
- 針對佈建的 SSD IOPS，您有兩個選項可以為您的檔案系統佈建 IOPS 數目：
  - 如果您希望 Amazon FSx 自動佈建每 GiB 的固態硬碟儲存裝置 3 IOPS，請選擇自動 (預設值)。
  - 如果您要指定 IOPS 的數目，請選擇使用者佈建。每個檔案系統最多可佈建 200,000 個固態硬碟 IOPS。

    > **Note**
    >
    > 您可以在建立檔案系統之後增加佈建的 SSD IOPS。請記住，即使在佈建額外的 SSD IOPS 時，檔案系統可達到的最高等級也取決於檔案系統的輸送量容量。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輸送容量 (以每秒 MB) 為單位：
  - 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 高可用性 (HA) 配對。

輸送量容量是代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 適用於 NetApp ONTAP 性能的 Amazon FSx。

6. 在「網路」區段中，提供下列資訊：

- 對於 V irtual Private Cloud (VPC) (VPC)，請選擇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的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。
- 指定檔案伺服器的子網路。如果您要建立異地同步備份檔案系統，請同時為待命檔案伺服器選擇待命子網路。
- (僅限異地同步備份) 對於 VPC 路由表，請指定 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 使用標籤式身份驗證來管理異地同步備份檔案系統的這些路由表。這些路由表格以標籤`Key: AmazonFSx; Value: ManagedByAmazonFSx`。使用建立 ONTAP 異地同步備份檔案系統的 FSx 時， AWS CloudFormation 我們建議您手動新增標`Key: AmazonFSx; Value: ManagedByAmazonFSx`籤。

- (僅限異地同步備份) 端點 IP 位址範圍會指定建立用於存取檔案系統之端點的 IP 位址範圍。

端點 IP 位址範圍有三個選項：

- 來自 VPC 的未配置 IP 地址範圍 — Amazon FSx 從 VPC 的主要 CIDR 範圍中選擇最後 64 個 IP 地址，用作檔案系統的端點 IP 地址範圍。如果您多次選擇此選項，此範圍會在多個檔案系統之間共用。

> **Note**
>
> 如果子網路正在使用 VPC 主要 CIDR 範圍中任何一個最後 64 個 IP 位址，則此選項會呈現灰色。在此情況下，您仍然可以選擇 [輸入 IP 位址範圍] 選項，選擇 VPC 內位址範圍 (也就是不在主要 CIDR 範圍結尾的範圍或 VPC 次要 CIDR 的範圍)。

- 針對 [偏好的子網路]，指定檔案伺服器的子網路。如果您要建立異地同步備份檔案系統，請同時為待命檔案伺服器選擇待命子網路。
- (僅限異地同步備份) 對於 VPC 路由表，請指定 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 位址範圍會指定建立用於存取檔案系統之端點的 IP 位址範圍。

  端點 IP 位址範圍有三個選項：

  - 來自 VPC 的未配置 IP 地址範圍 — Amazon FSx 從 VPC 的主要 CIDR 範圍中選擇最後 64 個 IP 地址，用作檔案系統的端點 IP 地址範圍。如果您多次選擇此選項，此範圍會在多個檔案系統之間共用。

    > **Note**
    >
    > 如果子網路正在使用 VPC 主要 CIDR 範圍中任何一個最後 64 個 IP 位址，則此選項會呈現灰色。在此情況下，您仍然可以選擇 [輸入 IP 位址範圍] 選項，選擇 VPC 內位址範圍 (也就是不在主要 CIDR 範圍結尾的範圍或 VPC 次要 CIDR 的範圍)。

  - 虛擬私人雲端以外的浮動 IP 位址範圍 — Amazon FSx 選擇一個 198.19.x.0/24 位址範圍，這個位址範圍尚未被具有相同 VPC 和路由表的任何其他檔案系統使用。
  - 輸入 IP 位址範圍 — 您可以提供您自己選擇的 CIDR 範圍。您選擇的 IP 位址範圍可以在 VPC 的 IP 位址範圍內或之外，只要該範圍不與任何子網路重疊即可。

    > **Note**
    >
    > 請勿選擇落在下列 CIDR 範圍內的任何範圍，因為它們與 ONTAP 的 FSx 不相容：
    >
    > - 0.0.0/8
    > - 127.0.0.0/8
    > - 198.19.0.0/20
    > - 224.0.0.0/4
    > - 240.0.0/4
    > - 255.255.255/32

7. 在「安全性與加密」區段中，針對「加密金鑰」，選擇可保護檔案系統靜態資料的 AWS Key Management Service (AWS KMS) 加密金鑰。

8. 在檔案系統管理密碼中，輸入fsxadmin使用者的安全密碼。確認密碼。

   您可以使用使用fsxadmin者來管理您的檔案系統，使用 ONTAP CLI 和 REST API。如需fsxadmin使用者的詳細資訊，請參閱使用 ONTAP CLI 管理檔案系統。

9. 在 [預設儲存區虛擬機器組態] 區段中，提供下列資訊：

   - 在 [儲存區虛擬機器名稱] 欄位中，提供儲存區虛擬機器的名稱。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，您可以選擇性地選擇 [指定密碼] 並提供 SVM 使用者的vsadmin密碼。您可以使用使用vsadmin者來管理使用 ONTAP CLI 或其餘 API 的 SVM。如需vsadmin使用者的詳細資訊，請參閱使用 CLI 管理 SVM ONTAP。

     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使用fsxadmin者使用 ONTAP CLI 或 REST API 來管理檔案系統，但您無法使用 SVM 的使用vsadmin者執行相同的動作。
   - 在「作用中目錄」段落中，您可以將作用中目錄加入 SVM。如需詳細資訊，請參閱 使用 FSx 中的 Microsoft 活動目錄進行 ONTAP。

     如果您不想將 SVM 加入作用中目錄，請選擇不加入作用中目錄。

     如果您想要將 SVM 加入自我管理的 Active Directory 網域，請選擇 [加入作用中目錄]，並為您的作用中目錄提供下列詳細資料：

     - 要為您的 SVM 建立的作用中目錄電腦物件的 NetBIOS 名稱。名稱不能超過 15 個字元。
     - 您的活動目錄的完整網域名稱。網域名稱不能超過 255 個字元。
     - DNS 伺服器 IP 位址 — 您網域的網域名稱系統 (DNS) 伺服器的 IPv4 位址。
     - 服務帳戶使用者名稱 — 現有 Active Directory 中服務帳戶的使用者名稱。請勿包含網域前置字元或尾碼。
     - 服務帳戶密碼 — 服務帳戶的密碼。
     - 確認密碼 — 服務帳戶的密碼。
     - (選擇性) 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 — 您 Active Directory 中可以管理您檔案系統的群組名稱。

       如果您正在使用 AWS Managed Microsoft AD，則需要指定群組，例如 AWS 委派的 FSx 系統管理員、 AWS 委派管理員或具有委派 OU 權限的自訂群組。

       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，針對使用您的檔案系統建立的預設磁碟區提供下列資訊：

- 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。
- (僅限向上擴充檔案系統) 針對磁碟區樣式，請選擇FlexVol或FlexGroup。 FlexVol磁碟區是一般用途的磁碟區，大小最多可達 300 TiB。 FlexGroup磁碟區適用於高效能工作負載，大小最多可達 20 個 PIB。
- 在磁碟區大小中，輸入 800 GB (GiB) —2,000 PB (PIB) 範圍內的任何整數。
- 對於磁碟區類型，請選擇讀寫 (RW) 來建立可讀取和可寫入的磁碟區，或選擇資料保護 (DP) 來建立唯讀且可用作或關係目的地的磁碟區。NetApp SnapMirror SnapVault如需詳細資訊，請參閱 磁碟區類型。
- 對於「結合路徑」，請在檔案系統中輸入要掛載磁碟區的位置。例如，名稱必須有前導正斜線/vol3。
- 若要取得儲存效率，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 提供 ONTAP 儲存效率的 FSx。
- 對於磁碟區安全性樣式，請選擇磁碟區的 Unix (Linux)、NTFS 和混合。如需詳細資訊，請參閱磁碟區安全風格。
- 對於快照政策，請選擇磁碟區的快照政策。如需快照原則的詳細資訊，請參閱快照政策。

  如果您選擇 [自訂原則]，則必須在 [自訂原則] 欄位中指定原則的名稱。自訂原則必須已存在於 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原則。

11. 在 [預設磁碟區儲存分層] 區段中，對於容量集區分層原則，選擇磁碟區的儲存池分層原則，可以是 [自動] (預設值)、[僅快照]、[全部] 或 [無]。如需容量集區分層原則的詳細資訊，請參閱磁碟區分層政策。

    對於分層原則冷卻期間，如果您已將儲存分層設定為Auto和Snapshot-only原則。有效值為 2-183 天。磁碟區的分層原則冷卻期間定義了尚未存取的資料被標記為冷並移至容量集區儲存體之前的天數。

12. 在 Backup 與維護-選用中，您可以設定下列選項：

    - 對於每日自動備份，選擇啟用以進行每日自動備份。此選項預設為啟用。
    - 對於每日自動備份時段，請以協調世界時 (UTC) 設定一天中的時間，讓每日自動備份視窗開始。從此指定時間開始，視窗為 30 分鐘。此視窗無法與每週維護備份時段重疊。
    - 對於自動備份保留期，請設定要保留自動備份的 1-90 天之間。

- 對於「每週維護」時段，您可以設定希望維護時段開始的一週時間。第 1 天是星期一，2 是星期二，依此類推。從此指定時間開始，視窗為 30 分鐘。此視窗無法與每日自動備份視窗重疊。

13. 對於「標籤-選用」，您可以輸入金鑰和值，將標籤新增至檔案系統。標籤是區分大小寫的索引鍵值組，可協助您管理、篩選及搜尋檔案系統。

    選擇下一步。

14. 檢閱顯示在 Create file system (建立檔案系統) 頁面上的檔案系統組態。請注意您在建立檔案系統之後可以修改哪些檔案系統設定，以供參考。
15. 選擇 Create file system (建立檔案系統)。

若要建立檔案系統 (CLI)

- 若要為 ONTAP 檔案系統建立 FSx，請使用建立檔案系統 CLI 命令 (或等效的系CreateFile統 API 作業)，如下列範例所示。

```
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
```

成功建立檔案系統之後，Amazon FSx 會以 JSON 格式傳回檔案系統的說明，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，`create-file-system`CLI 命令和 `CreateFileSystem` API 作業不會建立預設 SVM 或磁碟區。若要建立 SVM，請參閱建立儲存區虛擬機器；若要建立磁碟區，請參閱建立磁碟區。

在共用子網路中為 ONTAP 檔案系統建立 FSx

VPC 共用可讓多個 AWS 帳戶 人在共用、集中管理的虛擬私有雲 (VPC) 中建立資源。在此模型中，擁有 VPC (擁有者) 的帳戶與屬於相同組織的其他帳戶 (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 單一可用區和異地同步備份檔案系統建立 FSx。若要建立異地同步備份檔案系統的參與者帳戶，擁有者帳戶還需要授與 Amazon FSx 權限，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 管理異地同步備份檔案系統的共用 VPC 支援。

> **Note**
>
> 參與者帳戶有責任與 VPC 擁有者協調，以防止建立任何將與參與者檔案系統的 VPC 內 CIDR 重疊的後續 VPC 子網路。如果子網路確實重疊，檔案系統的流量可能會中斷。

共用子網路需求和注意事項

將 ONTAP 檔案系統的 FSx 建立至共用子網路時，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 ONTAP 檔案系統的 FSx。
- 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所擁有的安全性群組來啟動資源。
- 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。擁有者帳戶可以看到參與者建立的安全性群組，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性群組，建立安全性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聯的資源。
- 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、修改和刪除異地同步備份檔案系統及其相關資源。此外，擁有者帳戶還必須授與 Amazon FSx 服務許可，才能代表參與者帳戶修改共用子網路中的路由表。如需更多資訊，請參閱管理異地同步備份檔案系統的共用 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 使用者指南中的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

與將要在共用子網路中建立 ONTAP 檔案系統 FSx 的參與者帳戶共用您的子網路時，您需要執行下列動作：

- VPC 擁有者必須使用 AWS Resource Access Manager 來與其他人安全地共用 VPC 和子網路。AWS 帳戶如需詳細資訊，請參閱 AWS Resource Access Manager 使用指南中的「共用 AWS 資源」。
- VPC 擁有者需要與參與者帳戶共用一或多個 VPC。如需詳細資訊，請參閱 Amazon 虛擬私有雲使用者指南中的與其他帳戶共用您的 VPC。
- 若要讓參與者帳戶為 ONTAP 異地同步備份檔案系統建立 FSx，VPC 擁有者還必須授予 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 ONTAP 異地同步備份檔案系統的 FSx 使用浮動 IP 位址，因此連線的用戶端可以在容錯移轉事件期間順暢地在偏好和待命檔案伺服器之間轉換。發生容錯移轉事件時，Amazon FSx 會更新與檔案系統相關聯的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。

管理異地同步備份檔案系統的共用 VPC 支援

擁有者帳戶可以管理參與者帳戶是否可以在 VPC 子網路中為 ONTAP 檔案系統建立異地同步備份 FSX，這些檔案系統擁有者已使用、和 API 與參與者共用 AWS Management Console AWS CLI，如以下各節所述。

管理異地同步備份檔案系統的 VPC 共用 (主控台)

開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。

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。
    - 若要為您共用的 VPC 子網路中的異地同步備份檔案系統啟用 VPC 共用，請選擇啟用參與者帳戶的路由表更新。
    - 若要在您擁有的所有 VPC 中停用異地同步備份檔案系統的 VPC 共用，請選擇停用參與者帳戶的路由表更新。顯示確認螢幕。

> **Important**
>
> 我們強烈建議您先刪除共用 VPC 中的參與者建立的異地同步備份檔案系統，然後再停用此功能。一旦功能被禁用，這些文件系統將進入一個MISCONFIGURED狀態，將有變得無法使用的風險。

3. 輸入**confirm**並選擇確認以禁用該功能。

管理異地同步備份檔案系統的 VPC 共用 ()AWS CLI

1. 若要檢視異地同步備份 VPC 共用的目前設定，請使用描述-共用-vpc-設定CLI 命令或等效的 API 命令，如下所示：DescribeSharedVpcConfiguration

```
$ aws fsx describe-shared-vpc-configuration
```

服務會回應成功的要求，如下所示：

```
{
    "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
}
```

2. 若要管理異地同步備份共用 VPC 組態，請使用更新共用-vpc-設定CLI 命令或等效的 API 命令。UpdateSharedVpcConfiguration下列範例會針對異地同步備份檔案系統啟用 VPC 共用。

```
$ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-participant-accounts true
```

服務會回應成功的要求，如下所示：

```
{
    "EnableFsxRouteTableUpdatesFromParticipantAccounts": "true"
}
```

3. 若要停用此功能，請EnableFsxRouteTableUpdatesFromParticipantAccounts將設定為false，如下列範例所示。

```
$ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-participant-accounts false
```

服務會回應成功的要求，如下所示：

```
{
    "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
}
```

更新檔案系統

本主題說明您可以更新現有檔案系統的哪些屬性，並提供使用主控台和 CLI 執行此操作的程序。

您可以使用 Amazon FSx 主控台和 Amazon FSx API，更新下列適用於 ONTAP 檔案系統屬性的 FSx： AWS CLI

- 每日自動備份。開啟或關閉自動每日備份、修改備份時段和備份保留期。如需備份的詳細資訊，請參閱使用自動每日備份。
- 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。如需維護時段的詳細資訊，請參閱使用 Amazon FSx 維護時段將效能最佳化。
- 檔案系統管理密碼。變更檔案系統`fsxadmin`使用者的密碼。您可以使用使用`fsxadmin`者來管理您的檔案系統，使用 ONTAP CLI 和 REST API。如需`fsxadmin`使用者的詳細資訊，請參閱使用 ONTAP CLI 管理檔案系統。
- Amazon VPC 路由表。透過適用於 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，以及用於存取 ONTAP CLI、API 和 BlueExp 的管理端點，使用與檔案系統關聯的 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異地同步備份檔案系統建立關聯，讓您即使網路不斷發展，也能設定哪些用戶端可以存取您的資料。您也可以從檔案系統中取消 (移除) 現有路由表格的關聯。

> **Note**
>
> Amazon FSx 使用標籤式身份驗證來管理異地同步備份檔案系統的 VPC 路由表。這些路由表格以標籤`Key: AmazonFSx; Value: ManagedByAmazonFSx`。使用建立或更新 ONTAP 異地同步備份檔案系統的 FSx 時，建 AWS CloudFormation 議您手動新增標`Key: AmazonFSx; Value: ManagedByAmazonFSx`籤。

更新檔案系統（主控台）

下列程序提供如何使用 ONTAP 檔案系統更新現有 FSx 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/。
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 ONTAP 檔案系統的 FSx。
3. 在頁面的第二個面板中選擇「備份」標籤。
4. 選擇更新。
5. 修改此檔案系統的每日自動備份設定。
6. 選擇儲存，以儲存變更。

若要更新每週維護時段

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
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 ONTAP 檔案系統的 FSx。
3. 在頁面的第二個面板中選擇「管理」標籤。
4. 在 [維護] 窗格中，選擇 [更新]。
5. 修改此檔案系統每週維護時間的時間。
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/。
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 ONTAP 檔案系統的 FSx。
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 管理員認證] 對話方塊中，於 ONTAP 系統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 [更新認證] 以儲存變更。

> **Note**
>
> 如果您收到錯誤訊息，指出新密碼不符合密碼需求，您可以使用 `security login role config show`ONTAPCLI 命令來檢視檔案系統上的密碼需求設定。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帳號密碼失敗。

更新異地同步備份檔案系統上的 VPC 路由表

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
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 ONTAP 檔案系統的 FSx。
3. 對於「動作」，選擇「管理路由表」。此選項僅適用於異地同步備份檔案系統。
4. 在「管理路由表」對話方塊中，執行下列任一項作業：
   - 若要建立新 VPC 路由表的關聯，請從關聯新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] 窗格中選取路由表格，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對 ONTAP 檔案系統的現有 FSx 進行更新。 AWS CLI

1. 若要更新 ONTAP 檔案系統 FSx 的組態，請使用更新檔案系統 CLI 命令 (或等效的UpdateFile系統 API 作業)，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. 若要停用每日自動備份，請將內AutomaticBackupRetentionDays容設定為 0。

```
aws fsx update-file-system \
```

```
    --file-system-id fs-0123456789abcdef0 \
    --ontap-configuration AutomaticBackupRetentionDays=0
```

刪除檔案系統

您可以使用 Amazon FSx 主控台、和 Amazon FSx API 和開發套件，刪除 ONTAP 檔案系統的 FSx。AWS CLI

若要刪除檔案系統：

- 使用控制台 — 按照中所述的程序進行操作步驟 3：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 SVM。然後使用刪除檔案系統 CLI 命令或系DeleteFile統 API 作業。

檢視檔案系統詳細資

您可以使用 Amazon FSx 主控台、、API 和支援的開發套件，檢視 FSx for ONTAP 檔案系統的 AWS CLI詳細組態資訊。 AWS

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」面板會顯示檔案系統的 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，以及可修改之屬性的編輯：
  - 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 — 檔案系統活動量度的高階摘要
    - 檔案系統儲存容量
    - 檔案伺服器與磁碟效能

    如需詳細資訊，請參閱 使用 Amazon 監控 CloudWatch。
  - 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的DNS名稱和IP位址。
    - 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 SVM 清單
- 檔案系統磁碟區清單
- Backup 設定 — 變更檔案系統的每日自動備份設定。
- 更新 — 顯示使用者對檔案系統配置進行的更新的狀態。
- 標籤 — 檢視、編輯、新增、移除標籤鍵：值配對。

- 使用 CLI 或 API — 使用描述檔案系統 CLI 命令或系統 API 作業。DescribeFile

FSx 表示 ONTAP 檔案系統狀態

您可以使用 Amazon FSx 主控台、 AWS CLI 指令描述檔案系統或 API 作業系統來檢視 Amazon FSx 檔案系統的狀態。DescribeFile

檔案系統狀態	描述
AVAILABLE	檔案系統已成功建立並可供使用。
CREATING	Amazon FSx 正在創建一個新的文件系統。
DELETING	Amazon FSx 正在刪除現有的檔案系統。
配置錯誤	檔案系統處於設定錯誤但可復原的狀態。
失敗	1. 檔案系統發生故障，Amazon FSx 無法復原。 2. 建立新檔案系統時，Amazon FSx 無法建立新的檔案系統。

管理適用於 ONTAP 儲存區虛擬機器的 FSx

在 ONTAP 的 FSx 中，磁碟區會託管在稱為儲存虛擬機器 (SVM) 的虛擬檔案伺服器上。SVM 是一種隔離的檔案伺服器，具有自己的管理認證和用於管理和存取資料的端點。當您存取 FSx for ONTAP 中的資料時，您的用戶端和工作站會使用 SVM 的端點 (IP 位址) 掛接由 SVM 主控的磁碟區、SMB 共用或 iSCSI LUN。

Amazon FSx 會在您的檔案系統上自動建立預設 SVM，當您使用. AWS Management Console您可以隨時使用主控台或 Amazon FSx API 和開發套件 AWS CLI，在檔案系統上建立額外的 SVM。您無法使用 ONTAP CLI 或其餘 API 來建立 SVM。

您可以將您的 SVM 加入到 Microsoft 活動目錄以進行文件訪問身份驗證和授權。如需詳細資訊，請參閱 使用 FSx 中的 Microsoft 活動目錄進行 ONTAP。

每個檔案系統的 SVM 數目上限

下表列出您可以為檔案系統建立的 SVM 數目上限。SVM 的最大數目取決於佈建的輸送容量量 (以每秒 MB 為單位)。

部署類型	輸送量容量 (MBPs)	每個檔案系統的 SVM 數目上限
單一可用區 (向上擴充) 和異地同步備份 (向上擴充)	128	6
	256	6
	512	14
	1,024	14
	2,048	24
	4,096	24
單一可用區 (向外擴充)	任何	5

主題

- 建立儲存區虛擬機器
- 更新儲存區虛擬機器
- 刪除儲存區虛擬機器 (SVM)
- 檢視儲存區虛擬機器組態詳細

建立儲存區虛擬機器

您可以使用 AWS Management Console、 AWS CLI和 API 為 ONTAP SVM 建立 FSx。

您可以為檔案系統建立的 SVM 數目上限，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 SVM 數目上限。

SVM 屬性

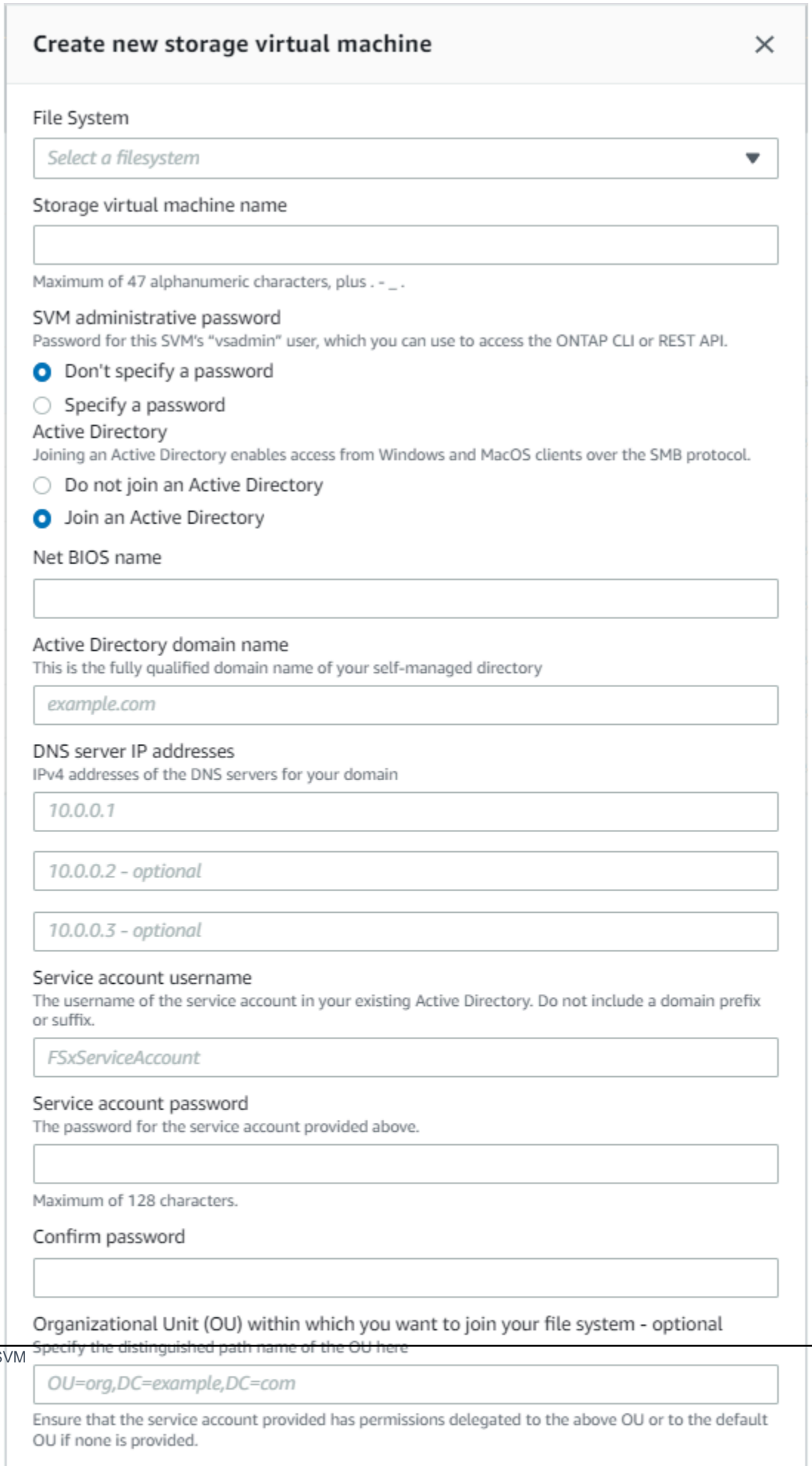
建立 SVM 時，您可以定義下列屬性：

- 它所屬的 ONTAP 檔案系統的 FSx。
- Microsoft 活動目錄（AD）配置 — 您可以選擇加入您的 SVM 到自我管理的 AD 進行身份驗證和訪問控制的 Windows 和 macOS 客戶端。如需詳細資訊，請參閱 使用 FSx 中的 Microsoft 活動目錄進行 ONTAP。
- 根磁碟區安全性樣式 — 設定根磁碟區安全性樣式 (Unix、NTFS 或混合)，以符合您用來存取 SVM 中資料的用戶端類型。如需詳細資訊，請參閱 磁碟區安全風格。
- SVM 管理密碼 — 您可以選擇性地設定 SVM 使用者的`vsadmin`密碼。如需詳細資訊，請參閱 使用 CLI 管理 SVM ONTAP。

建立儲存區虛擬機器 (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 [儲存區虛擬機器]。
3. 選擇 [建立新儲存區虛擬機器]。

   建立新的儲存區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. 對於檔案系統，請選擇要在其上建立儲存區虛擬機器的檔案系統。
5. 在 [儲存區虛擬機器名稱] 欄位中，提供儲存區虛擬機器的名稱。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，您可以選擇性地選擇 [指定密碼] 並提供此 SVM 使用者的vsadmin密碼。您可以使用使用vsadmin者來管理使用 ONTAP CLI 或其餘 API 的 SVM。如需vsadmin使用者的詳細資訊，請參閱使用 CLI 管理 SVM ONTAP。

   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使用fsxadmin者使用 ONTAP CLI 或 REST API 來管理您的檔案系統，但您無法使用 SVM 的使用vsadmin者執行相同的動作。
7. 對於活動目錄，您有以下選項：

   - 如果您沒有將檔案系統加入作用中目錄 (AD)，請選擇不要加入作用中目錄。
   - 如果您要將 SVM 加入自我管理的 AD 網域，請選擇 [加入作用中目錄]，並為 AD 提供下列詳細資料。如需詳細資訊，請參閱 將 SVM 加入自我管理的 Microsoft AD 的先決條件。
     - 要為您的 SVM 建立的作用中目錄電腦物件的 NetBIOS 名稱。名稱不能超過 15 個字元。這是活動目錄中此 SVM 的名稱。
     - 作用中目錄的完整網域名稱 (FQDN)。FQDN 不得超過 255 個字元。
     - DNS 伺服器 IP 位址 — 您網域的 DNS 伺服器的 IPv4 位址。
     - 服務帳戶使用者名稱 — 現有 Active Directory 中服務帳戶的使用者名稱。請勿包含網域前置字元或尾碼。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。
     - (選擇性) 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 中可管理您檔案系統的群組名稱。

       如果您正在使用 AWS Managed Microsoft AD，則必須指定群組，例如 AWS 委派的 FSx 系統管理員、 AWS 委派管理員或具有委派 OU 權限的自訂群組。

       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. 對於 SVM 根磁碟區安全性樣式，請根據存取資料的用戶端類型選擇 SVM 的安全性樣式。如果您主要使用 Linux 用戶端存取您的資料，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 磁碟區安全風格。
9. 選擇確認以建立儲存區虛擬機器。

您可以在 [檔案系統詳細資料] 頁面的 [儲存區虛擬機器] 窗格的 [狀態] 欄中監視更新進度。儲存區虛擬機器的狀態為 [已建立] 時，即可使用。

建立儲存區虛擬機器 (CLI)

- 若要為 ONTAP 儲存區虛擬機器 (SVM) 建立 FSx，請使用 create-storage-virtual-machineCLI 命令 (或等效的 CreateStorageVirtualMachineAPI 作業)，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 格式傳回其說明，如下列範例所示。

```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
```

```
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["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"
      }
    }
  }
}
```

更新儲存區虛擬機器

您可以使用 Amazon FSx 主控台和 Amazon FSx API 更新下列儲存虛擬機器 (SVM) 組態屬性： AWS CLI

- SVM 管理帳戶密碼。
- SVM 使用中目錄 (AD) 設定 — 您可以將 SVM 加入 AD，或修改已加入 AD 的 SVM 的 AD 組態。如需詳細資訊，請參閱 管理 SVM 作用中目錄組態。

若要更新 SVM 管理員帳戶認證 (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。
   - 選擇儲存區虛擬機器索引標籤。

   — 或者 —

   - 若要顯示目前的所有可用 SVM 的清單 AWS 區域，請展開 ONTAP 並選擇儲存虛擬機器。AWS 帳戶
3. 選擇您要更新的儲存區虛擬機器。
4. 選擇「動作」>「更新管理員密碼 [更新 SVM 管理認證] 視窗隨即出現。
5. 輸入vsadmin使用者的新密碼並加以確認。
6. 選擇「更新身份證明」以儲存新密碼。

若要更新 SVM 管理員帳戶認證 (CLI)

- 若要更新 ONTAP SVM 的 FSx 組態，請使用 update-storage-virtual-machineCLI 命令 (或同等的 UpdateStorageVirtualMachineAPI 作業)，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 格式傳回其說明，如下列範例所示。

```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
```

```
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["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"
      }
    }
  }
}
```

刪除儲存區虛擬機器 (SVM)

您只能使用 Amazon FSx 主控台、和 API 來刪除適用於 ONTAP SVM 的 AWS CLI FSx。刪除 SVM 之前，您必須先刪除附加至 SVM 的所有非根磁碟區。

Important

您無法使用 NetApp ONTAP CLI 或 API 刪除 SVM。

Note

刪除儲存區虛擬機器之前，請確定沒有應用程式正在存取 SVM 中的資料，而且您已刪除所有附加至 SVM 的非根磁碟區。

刪除儲存區虛擬機器 (主控台)

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 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]，然後選擇您要刪除 SVM 的 ONTAP 檔案系統。
   - 選擇儲存區虛擬機器索引標籤。

   — 或者 —

   - 若要顯示所有可用的 SVM 清單，請展開 ONTAP 並選擇儲存區虛擬機器。

   從清單中選取要刪除的 SVM。
3. 在磁碟區索引標籤中，檢視附加至 SVM 的磁碟區清單。如果有任何非根磁碟區連接至 SVM，您必須先刪除它們，然後才能刪除 SVM。如需更多資訊，請參閱刪除磁碟區。
4. 從動作功能表選擇刪除儲存區虛擬機器。
5. 在刪除確認對話方塊中，選擇刪除儲存區虛擬機器。

刪除儲存區虛擬機器 (CLI)

- 若要刪除 ONTAP 儲存區虛擬機器的 FSx，請使用 delete-storage-virtual-machineCLI 命令 (或等效的 DeleteStorageVirtualMachineAPI 作業)，如下列範例所示。

```
aws fsx delete-storage-virtual-machine --storage-virtual-machine-id svm-
abcdef0123456789d
```

檢視儲存區虛擬機器組態詳細

您可以使用 Amazon FSx 主控台、和 Amazon FSx API，查看檔案系統上目前存在的 ONTAP 儲存虛擬機器的 AWS CLI FSx。

若要檢視檔案系統上的儲存區虛擬機器：

- 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區虛擬機器，請選擇 [儲存區虛擬機器] 索引標籤，然後選擇您要檢視的儲存區虛擬機器。
- 使用 CLI 或 API — 使用 describe-storage-virtual-machinesCLI 命令或 DescribeStorageVirtualMachinesAPI 作業。

  系統回應是您帳戶中所有 SVM 的完整說明清單。 AWS 區域

管理安裝磁碟區的 FSx

ONTAP 檔案系統的 FSx 上的每個儲存區虛擬機器 (SVM) 都可以有一或多個磁碟區。磁碟區是用於檔案、目錄或 iSCSI 邏輯儲存裝置 (LUN) 的隔離資料容器。磁碟區是精簡佈建的，這表示它們只會消耗儲存在其中的資料的儲存容量。

您可以透過網路檔案系統 (NFS) 通訊協定、伺服器訊息區 (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，從 Linux、Windows 或 macOS 用戶端存取磁碟區，建立 iSCSI LUN (共用區塊儲存)。FSx for ONTAP 也支援同一磁碟區的多重通訊協定存取 (同時 NFS 和 SMB 存取)。

您可以使用 AWS Management Console、 AWS CLI、Amazon FSx API 或NetApp藍運算式建立磁碟區。您也可以使用 NetApp ONTAP CLI 或 REST API，使用檔案系統或 SVM 的管理端點來建立、更新和刪除磁碟區。

> **Note**
>
> 您可以為每個 HA 配對建立 500 個磁碟區，跨所有 HA 配對建立最多 1,000 個磁碟區。FlexGroup組成磁碟區計入此限制。依預設，每個彙總有八個構成磁碟區FlexGroup。

建立體積塊時，需要定義下列屬性：

- 音量樣式 — 音量樣式可以是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NetAppSnapMirror或SnapVault關係中的目的地。
- 磁碟區大小 — 這是磁碟區可儲存的最大資料量，無論儲存層為何。
- 結合路徑 — 這是 SVM 命名空間中裝載磁碟區的位置。
- 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) 可為一般用途檔案共用工作負載節省 65% 的典型儲存空間。
- 磁碟區安全性樣式 (Unix、NTFS 或混合) — 決定授權使用者時，磁碟區上的資料存取所使用的權限類型。
- 資料分層 — 分層原則會定義哪些資料儲存在符合成本效益的容量集區層中。
- 分層原則冷卻期間 — 定義資料被標記為冷並移至容量集區儲存的時機。
- 快照策略 — 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原則中進行選擇，也可以使用自訂原則。您已使用 ONTAP CLI 或 REST API 建立的原則。
- 將標籤複製到備份 — Amazon FSx 會使用此選項自動將磁碟區中的任何標籤複製到備份。您可以使用 AWS CLI 或 Amazon FSx API 來設定此選項。

主題

磁碟區樣式

FSx for ONTAP 提供兩種類型的磁碟區，您可以將其用於不同用途。您可以使用 Amazon FSx 主控台、和 Amazon FSx API 來 AWS CLI建立 FlexVol 或 FlexGroup 磁碟區。

- FlexVol對於具有一個高可用性 (HA) 配對的檔案系統，磁碟區可提供最簡單的體驗，而且是擴充檔案系統的預設磁碟區樣式。FlexVol磁碟區的最小大小為 20 MB，而最大大小為 314,572,800 兆位元組。

- FlexGroup磁碟區由多個組成FlexVol磁碟區組成，與具有多個 HA 配對之檔案系統的磁碟區相比，FlexVol磁碟區可提供更高的效能和儲存擴充性。 FlexGroup磁碟區是向外延展檔案系統的預設磁碟區樣式。FlexGroup磁碟區的最小大小為每個組成 100 GB (GiB)，而最大大小為 20 PB (PIB)。

您可以使用 ONTAP CLI 將具有FlexVol樣式的磁碟區轉換為FlexGroup樣式，後者會建立FlexGroup具有單一組成份的磁碟區。但是，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，以確保資料平均分佈在各個FlexGroup's組成部分之間。如需詳細資訊，請參閱FlexGroup成分。

> **Note**
>
> 如果您想要使用 ONTAP CLI 將磁碟區轉換為FlexVol磁碟區，請務必在轉換FlexGroup磁碟區之前刪除該FlexVol磁碟區的所有備份。 ONTAP不會在轉換過程中自動重新平衡資料，因此資料可能會在各個成分中失衡。FlexGroup

FlexGroup成分

體FlexGroup積是由成分組成的，這些成分是FlexVol卷。根據預設，ONTAP 的 FSx 會將八個成份股指派給每個 HA 對的一個FlexGroup磁碟區。

當您建立FlexGroup磁碟區時，磁碟區的大小會在其成分之間平均分配。例如，如果您建立一個含有八個成分的 800 GB FlexGroup 磁碟區，則每個成分的磁碟區大小為 100 GB。FlexGroup磁碟區的大小可以介於 100 GB 和 20 PIB 之間，但總大小取決於成分的大小。每個組成部分的最小大小為 100 GB，最大容量為 300 TiB。例如，具有八個成分的FlexGroup磁碟區的最小大小為 800 GB，最大大小為 20 PIB。

ONTAP 會在檔案層級將資料分配給所有成份股。您可以在FlexGroup磁碟區的每個組成部分中儲存多達 20 億個檔案。

當您更新FlexGroup磁碟區的大小時，新的大小會平均分佈在其現有組成部分之間。

您也可以使用 ONTAP CLI 或 REST API 為FlexGroup磁碟區新增更多成分。但是，我們建議您僅在需要額外的儲存容量且所有成分已達到其最大容量 (每個組成份 300 TiB) 的情況下才這樣做。添加成分可能會導致成分股的數據和 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%。當新數據寫入數FlexGroup量時，ONTAP 會優先將其分配給新成分，直到成分股平衡為止。如果您確實添加了新的成分股，我們建議您選擇偶數，而每個總數不超過八個。

> **Note**
>
> 如果您新增新的組成部分，您現有的快照會變成部分快照；因此，它們無法用來將FlexGroup磁碟區完全還原到先前的狀態。先前的快照無法提供FlexGroup磁碟區的完整 point-in-time 影像，因為新的組成部分尚未存在。但是，部分快照可用於還原個別檔案和目錄、建立新磁碟區或使用進行複製SnapMirror。

磁碟區類型

FSx 適用於 ONTAP 提供兩種類型的磁碟區，您可以使用 Amazon FSx 主控台和 Amazon FSx API 建立這些磁碟區。 AWS CLI

- 大多數情況下都會使用讀寫 (RW) 磁碟區。顧名思義，它們是可讀寫的。
- 資料保護 (DP) 磁碟區是您用來做為NetAppSnapMirror或SnapVault關係之目的地的唯讀磁碟區。當您要移轉或保護單一磁碟區的資料時，應該使用 DP 磁碟區。

FlexVolFlexGroup磁碟區可以是 RW 或 DP。

> **Note**
>
> 您無法在建立磁碟區之後更新磁碟區類型。

磁碟區安全風格

適用於 ONTAP 的 FSx 支援 3 種不同的磁碟區安全性樣式：Unix、NTFS 和混合。每個安全性樣式對資料權限的處理方式都有不同的影響。您必須瞭解不同的影響，以確保為您的目的選取適當的安全性型式。

請務必瞭解安全性樣式無法決定哪些用戶端類型可以存取資料，也不能存取資料。安全性樣式只會決定 ONTAP FSx 用來控制資料存取的權限類型，以及哪些用戶端類型可以修改這些權限。

您用來決定磁碟區安全性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，安全風格會自動設定為根磁碟區的安全性樣式。您可以使用 AWS CLI 或 API 修改磁碟區的安全性樣式。您可以在建立磁碟區之後修改此設定。如需詳細資訊，請參閱更新磁碟區。

當您在磁碟區上設定安全性樣式時，請考量環境的需求，以確保您選取最佳的安全性樣式，以避免管理權限發生問題。請記住，安全性樣式不會決定哪些用戶端類型可以存取資料。安全性樣式會決定用於允許資料存取的權限，以及可修改這些權限的用戶端類型。以下是可協助您決定為磁碟區選擇哪種安全性樣式的考量事項：

- Unix (Linux) — 如果檔案系統由 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會使用 Unix 使用者作為服務帳戶，請選擇此安全性樣式。只有 Linux 用戶端可以使用 Unix 安全性樣式修改權限，檔案和目錄上使用的權限類型為模式位元或 NFS v4.x ACL。
- NTFS — 如果檔案系統是由 Windows 系統管理員管理、大多數使用者是 SMB 用戶端，而存取資料的應用程式則使用 Windows 使用者做為服務帳戶，請選擇此安全性樣式。如果磁碟區需要任何 Windows 存取權，建議您使用 NTFS 安全性樣式。只有 Windows 用戶端可以使用 NTFS 安全性樣式修改權限，檔案和目錄上使用的權限類型為 NTFS ACL。
- 混合 — 這是進階設定。若要取得更多資訊，請參閱NetApp文件中心中的安全性型式及其效果主題。

建立磁碟區

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 為 NetApp ONTAP FlexVol 或FlexGroup磁碟區建立 FSx。

若要建立FlexVol磁碟區 (主控台)

> **Note**
>
> 磁碟區的安全性樣式會自動設定為根磁碟區的安全性樣式。

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 [磁碟區]。
3. 選擇建立磁碟區。
4. 針對檔案系統類型，請為 NetApp ONTAP 選擇 Amazon FSx。
5. 在「檔案系統詳細資訊」區段中，提供下列資訊：
   - 在 [檔案系統] 中，選擇要建立磁碟區的檔案系統。
   - 對於儲存區虛擬機器，請選擇要在其上建立磁碟區的儲存區虛擬機器 (SVM)。
6. 在「體積樣式」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。
- 在磁碟區大小中，輸入介於 20—314572800 範圍內的任何整數，以指定大小 (MB)。
- 對於磁碟區類型，請選擇讀寫 (RW) 來建立可讀取和可寫入的磁碟區，或選擇資料保護 (DP) 來建立唯讀且可用作或關係目的地的磁碟區。NetApp SnapMirror SnapVault如需詳細資訊，請參閱 磁碟區類型。
- 對於「結合路徑」，請在檔案系統中輸入要掛載磁碟區的位置。例如，名稱必須有前導正斜線/ vol3。
- 若要取得儲存效率，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 提供 ONTAP 儲存效率的 FSx。
- 對於磁碟區安全性樣式，請選擇磁碟區的 Unix (Linux)、NTFS 和混合。如需詳細資訊，請參閱磁碟區安全風格。
- 對於快照政策，請選擇磁碟區的快照政策。如需快照原則的詳細資訊，請參閱快照政策。

  如果您選擇 [自訂原則]，則必須在 [自訂原則] 欄位中指定原則的名稱。自訂原則必須已存在於 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原則。

8. 在「儲存體階層」區段中，提供下列資訊：
   - 對於容量集區分層原則，請選擇磁碟區的儲存池分層原則，可以是 [自動] (預設值)、[僅快照]、[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 [自動] 或 [僅限快照]，您可以設定分層原則冷卻期間，以定義尚未存取的資料標示為冷卻並移至容量集區儲存體之前的天數。您可以提供 2 到 183 天之間的值。預設設定為 31 天。
9. 在「進階」段落中，對於「SnapLock組態」，請選擇「啟用」和「停用」。如需設定SnapLock相容性磁碟區或SnapLock企業磁碟區的詳細資訊，請參閱建立SnapLock符合性磁碟區和建立SnapLock企業磁碟區。如需 SnapLock 的相關資訊，請參閱 保護您的資料 SnapLock。
10. 選擇 [確認] 以建立磁碟區。

您可以在 [檔案系統詳細資料] 頁面的 [磁碟區] 窗格的 [狀態] 欄中監視更新進度。當磁碟區狀態為「已建立」時，即可使用該磁碟區。

若要建立FlexGroup磁碟區 (主控台)

> **Note**
>
> 您只能使用 Amazon FSx 主控台為向外擴充檔案系統建立FlexGroup磁碟區。若要為您的向外延展檔案系統建立FlexVol磁碟區，請使用 Amazon FSx API 或 NetApp 管理工具。 AWS CLI

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 [磁碟區]。
3. 選擇建立磁碟區。
4. 針對檔案系統類型，請為 NetApp ONTAP 選擇 Amazon FSx。
5. 在「檔案系統詳細資訊」區段中，提供下列資訊：
   - 在 [檔案系統] 中，選擇要建立磁碟區的檔案系統。
   - 對於儲存區虛擬機器，請選擇要在其上建立磁碟區的儲存區虛擬機器 (SVM)。
6. 在「體積樣式」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。
   - 在磁碟區大小中，輸入 800 GB (GiB) —2,000 PB (PIB) 範圍內的任何整數。
   - 對於磁碟區類型，請選擇讀寫 (RW) 來建立可讀取和可寫入的磁碟區，或選擇資料保護 (DP) 來建立唯讀且可用作或關係目的地的磁碟區。NetApp SnapMirror SnapVault如需詳細資訊，請參閱 磁碟區類型。
   - 對於「結合路徑」，請在檔案系統中輸入要掛載磁碟區的位置。例如，名稱必須有前導正斜線/ `vol3`。
   - 若要取得儲存效率，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 提供 ONTAP 儲存效率的 FSx。
   - 對於磁碟區安全性樣式，請選擇磁碟區的 Unix (Linux)、NTFS 和混合。如需詳細資訊，請參閱磁碟區安全風格。

     > **Note**
     >
     > 磁碟區的安全性樣式會自動設定為根磁碟區的安全性樣式。

- 對於快照政策，請選擇磁碟區的快照政策。如需快照原則的詳細資訊，請參閱快照政策。

  如果您選擇 [自訂原則]，則必須在 [自訂原則] 欄位中指定原則的名稱。自訂原則必須已存在於 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原則。

8. 在「儲存體階層」區段中，提供下列資訊：

   - 對於容量集區分層原則，請選擇磁碟區的儲存池分層原則，可以是 [自動] (預設值)、[僅快照]、[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 [自動] 或 [僅限快照]，您可以設定分層原則冷卻期間，以定義尚未存取的資料標示為冷卻並移至容量集區儲存體之前的天數。您可以提供 2-183 天之間的值。預設設定為 31 天。

9. 在「進階」段落中，對於「SnapLock組態」，請選擇「啟用」和「停用」。如需設定SnapLock相容性磁碟區或SnapLock企業磁碟區的詳細資訊，請參閱建立SnapLock符合性磁碟區和建立SnapLock企業磁碟區。如需 SnapLock 的相關資訊，請參閱 保護您的資料 SnapLock。

10. 選擇 [確認] 以建立磁碟區。

您可以在 [檔案系統詳細資料] 頁面的 [磁碟區] 窗格的 [狀態] 欄中監視更新進度。當磁碟區狀態為「已建立」時，即可使用該磁碟區。

若要建立磁碟區 (CLI)

- 若要為 ONTAP 磁碟區建立 FSx，請使用建立磁碟區 CLI 命令 (或等效的 CreateVolumeAPI 作業)，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
```

成功建立磁碟區之後，Amazon FSx 會以 JSON 格式傳回其說明，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"


    }
}
```

您也可以透過將磁碟區備份還原到新磁碟區來建立新磁碟區。如需詳細資訊，請參閱 [將備份還原至新磁碟區](#)。

更新磁碟區

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 更新 NetApp ONTAP 磁碟區的 FSx 組態。您可以針對 ONTAP 磁碟區修改現有 FSx 的下列內容：

- 磁碟區名稱
- 路口路徑
- 磁碟區大小
- 儲存效率
- 容量集區分層原則

- 磁碟區安全風格
- 快照政策
- 分層政策冷卻期
- 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 管理安裝磁碟區的 FSx。

更新磁碟區組態 (主控台)

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 瀏覽至檔案系統，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

   隨即顯示磁碟區目前設定的「更新磁碟區」對話方塊。
6. 對於「結合路徑」，請輸入檔案系統內的現有位置以掛載磁碟區。名稱必須有前導正斜線，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FlexVol磁碟區，最大大小為 300 TiB。對於FlexGroup磁碟區，最大大小為 300 TiB 乘以您FlexGroup擁有的組成磁碟區總數，最多可達 20 個 PiB。
8. 若要取得儲存效率，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)，或選擇 [停用] 將其停用。
9. 對於容量集區分層原則，請為磁碟區選擇新的儲存池分層原則，可以是 [自動] (預設值)、[僅快照]、[全部] 或 [無]。如需容量集區分層原則的詳細資訊，請參閱磁碟區分層政策。
10. 對於磁碟區安全性樣式，請選擇 [Unix (Linux)]、[NTFS] 或 [混合]。磁碟區的安全性樣式會決定是否為 NTFS 或 UNIX ACL 提供多重通訊協定存取的偏好設定。多重通訊協定存取不需要混合模式，只建議進階使用者使用。
11. 對於快照政策，請選擇磁碟區的快照政策。如需快照原則的詳細資訊，請參閱快照政策。

    如果您選擇 [自訂原則]，則必須在 [自訂原則] 欄位中指定原則的名稱。自訂原則必須已存在於 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原則。
12. 對於分層策略冷卻期間，有效值為 2-183 天。磁碟區的分層原則冷卻期間定義了尚未存取的資料被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`策略。

13. 選擇 [更新] 以更新磁碟區。

更新磁碟區的組態 (CLI)

- 若要更新 ONTAP 磁碟區的 FSx 組態，請使用更新磁碟區 CLI 命令 (或等效的 UpdateVolumeAPI 作業)，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
```

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、和 Amazon FSx API 刪除 NetApp ONTAP 磁碟區的 FSx。 AWS CLI

> **Important**
>
> 如果磁碟區已啟用 Amazon FSx 備份，則只能使用 Amazon FSx 主控台、API 或 CLI 刪除磁碟區。

> **Important**
>
> 使用 Amazon FSx 主控台刪除磁碟區時，您可以選擇對磁碟區進行最終備份。您可以從備份建立新磁碟區。我們建議您選擇最終備份作為最佳實踐。如果您發現在一段時間後不需要它，則可以刪除此磁碟區和其他手動建立的磁碟區備份。當您使用 `delete-volume` CLI 命令刪除磁碟區時，Amazon FSx 預設會進行最終備份。

刪除磁碟區之前，請確定沒有應用程式存取您要刪除的磁碟區中的資料。

若要刪除磁碟區 (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 [檔案系統]，然後選擇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. 在 [動作] 中選擇 [刪除磁碟區]
6. 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] 以進行磁碟區的最終備份。顯示最終備份的名稱。
   - 如果您不想要磁碟區的最終備份，請選擇否。系統會要求您確認磁碟區一旦刪除，就無法再使用自動備份。
7. 在確認刪除欄位中輸入 delete 以確認磁碟區刪除。
8. 選擇刪除磁碟區。

若要刪除磁碟區 (CLI)

- 若要刪除 ONTAP 磁碟區的 FSx，請使用刪除磁碟區 CLI 命令 (或同等的 DeleteVolumeAPI 作業)，如下列範例所示。

```
aws fsx delete-volume --volume-id fsvol-1234567890abcde
```

檢視磁碟區

您可以使用 Amazon FSx 主控台、和 Amazon FSx API 和開發套件，查看檔案系統上目前存在的 AWS CLI ONTAP 磁碟區的 FSx。

若要檢視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] 索引標籤以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 — 使用描述磁碟區 CLI 命令或 API 作業。DescribeVolumes

建立一 iSCSI

此程序說明如何使用 ONTAP CLI 命令，在適用於 NetApp ONTAP 擴充檔案系統的 Amazon FSx 上建立 iSCSI LUN。 NetApp lun create如需詳細資訊，請參閱 lun create NetApp ONTAP 文件中心。

> **Note**
>
> 向外延展檔案系統不支援 iSCSI 通訊協定。

此程序假設您已經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。

1. 若要存取 NetApp ONTAP CLI，請執行下列命令，在適用於 NetApp ONTAP 檔案系統的 Amazon FSx 管理連接埠上建立安全殼層工作階段。取代*management_endpoint_ip*為檔案系統管理連接埠的 IP 位址。

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

   如需詳細資訊，請參閱 使用 ONTAP CLI 管理檔案系統。

2. 使用 lun create NetApp CLI 指令建立 LUN，並取代下列值：

   - ***svm_name***-提供 iSCSI 目標的儲存區虛擬機器 (SVM) 的名稱。主機會使用此值連線到 LUN。
   - ***vol_name***-主控 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 LUN 大小上限為 128 TB。

     > **Note**
     >
     > 我們建議您使用的磁碟區至少比 LUN 大小大 5%。此邊界會為磁碟區快照留下空間。

   - ***ostype***-主機的作業系統，`windows_2008`或`linux`。適用`windows_2008`於所有版本的 Windows；這可確保 LUN 具有適當的作業系統區塊偏移量，並將效能最佳化。

> **Note**
>
> 我們建議您在 LUN 上啟用空間分配。啟用空間分配後，ONTAP 可以在 LUN 容量不足時通知您的主機，並且可以在刪除 LUN 中的資料時回收空間。

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)
```

3. 確認 LUN 已建立、連線和對應。

```
> lun show
```

系統會以下列輸出回應：

```
Vserver   Path                            State   Mapped   Type         Size
--------- ------------------------------- ------- -------- ------------ --------
svm_name
          /vol/vol_name/lun_name          online  unmapped windows_2008 10GB
```

後續步驟

現在您已經建立了 iSCSI LUN，使用 iSCSI LUN 做為區塊儲存的程序的下一個步驟是將 LUN 對應至igroup。如需詳細資訊，請參閱 將 iSCSI 連接至用戶端 或 將 iSCSI LUN 掛載到視窗用戶端 。

管理中小企業股

若要管理 Amazon FSx 檔案系統上的 SMB 檔案共用，您可以使用 Microsoft 視窗共用資料夾圖形使用者介面。共用資料夾 GUI 提供一個集中位置，以管理儲存區虛擬機器 (SVM) 中的所有共用資料夾。下列程序詳細說明如何建立、更新和移除檔案共用。

> **Note**
>
> 您也可以使用 NetApp 系統管理員來管理 SMB 檔案共用。如需詳細資訊，請參閱 使用NetApp 系統管理員 BlueXP。

將共用資料夾連線到 Amazon FSx 檔案系統

1. 啟動您的 Amazon EC2 實例，並將其連接到您的 Amazon FSx 文件系統加入的 Microsoft 活動目錄。若要執行此操作，請從《AWS Directory Service 管理指南》中選擇下列其中一個程序：
   - 無縫加入執行個體
   - 手動聯結視窗執行個體
2. 以身為檔案系統管理員群組成員的使用者身分 Connect 至執行個體。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的連線到 Windows 執行個體。
3. 開啟 [開始] 功能表，並使用 [以系統管理員身分執行] 來執行 fsmgmt.msc。這麼做會開啟共用資料夾 GUI 工具。
4. 針對「動作」，選擇「Connect 到另一台電腦」
5. 例**netbios_name.corp.example.com**如，如果是其他電腦，請輸入儲存區虛擬機器 (SVM) 的 DNS 名稱。

   若要在 Amazon FSx 主控台上尋找您 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，直到找到 SMB DNS 名稱。您也可以在 DescribeStorageVirtualMachinesAPI 作業的回應中取得 DNS 名稱。
6. 選擇確定。然後，您 Amazon FSx 檔案系統的項目會顯示在共用資料夾工具的清單中。

現在共用資料夾已連線到 Amazon FSx 檔案系統，您可以透過下列動作在檔案系統上管理 Windows 檔案共用：

> **Note**
>
> 建議您在根磁碟區以外的磁碟區找到 SMB 共用。

- 建立新的檔案共用 — 在共用資料夾工具中，選擇左窗格中的 [共用] 以查看 Amazon FSx 檔案系統的使用中共用。磁碟區會顯示掛接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。

在建立新檔案共用之前，您必須先建立本端資料夾。你可以這樣做，如下所示：

- 使用共用資料夾工具：指定本機資料夾路徑時選擇「瀏覽」，然後選擇「建立新資料夾」以建立本機資料夾。
- 使用命令行：

```
New-Item -Type Directory -Path \\netbios_name.corp.example.com\C
$volume_path\MyNewFolder
```

- 修改檔案共用 — 在「共用資料夾」工具中，在右窗格中開啟您要修改之檔案共用的內容 (按一下滑鼠右鍵) 選單，然後選擇「內容」。修改屬性並選擇 「確定」。
- 移除檔案共用 — 在「共用資料夾」工具中，開啟右窗格中要移除之檔案共用的內容 (按一下滑鼠右鍵) 功能表，然後選擇「停止共用」。

> **Note**
>
> 只有當您使用 Amazon FSx 檔案系統的 DNS 名稱連線到 fsmgmt.msc 時，才能從 GUI 移除檔案共用。如果您使用檔案系統的 IP 位址或 DNS 別名連線，[停止共用] 選項將無法運作，且不會移除檔案共用。

檔案存取稽核

適用於 NetApp ONTAP 的 Amazon FSx 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

檔案存取稽核可讓您根據您定義的稽核策略，記錄使用者對個別檔案和目錄的存取。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遵循資料保護要求、及早識別潛在威脅，並降低資料外洩的風險。

跨檔案和目錄存取，Amazon FSx 支援記錄成功嘗試 (例如具有足夠權限的成功存取檔案的使用者)、嘗試失敗，或兩者都支援記錄。您也可以隨時關閉檔案存取稽核。

依預設，稽核事件記錄會以EVTX檔案格式儲存，讓您可以使用 Microsoft 事件檢視器來檢視這些記錄檔。

可稽核的 SMB 存取事件

下表列出 SMB 檔案和資料夾存取事件可以稽核。

事件識別碼 (EVT)	事件	描述	類別
560/4656	開啟物件/建立物件	對象訪問：對象（文件或目錄）打開	檔案存取
563/4659	開啟具有刪除意圖的物件	對象訪問：刪除意圖請求對象（文件或目錄）的句柄	檔案存取
564/4660	刪除物件	對象訪問：刪除對象（文件或目錄）。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	對象訪問：對象訪問嘗試（讀取，寫入，獲取屬性，設置屬性）。 Note 對於此事件，ONTAP 只會稽核物件上的第一個 SMB 讀取和第一個 SMB 寫	檔案存取

事件識別碼 (EVT)	事件	描述	類別
		入作業 (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作業時，建立過多的記錄項目。	
N/	硬鏈接	對象訪問：嘗試創建硬鏈接	檔案存取
N/A /N/A 安裝事件識別碼 9999	重命名物件	物件存取：已重新命名物件。這是一個 ONTAP 事件。Windows 目前不支援它做為單一事件。	檔案存取
N/A ONTAP 事件識別碼 9998	取消連結物件	物件存取：取消連結的物件。這是一個 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

可稽核下列 NFS 檔案和資料夾存取事件。

- READ
- OPEN
- CLOSE

- 讀取的
- WRITE
- 塞塔特爾
- 製作
- 連結
- 开放亚特
- 移除
- 獲得者
- 驗證
- N 驗證
- RENAME

設定檔案存取稽核的工作概觀

針對 ONTAP 設定 FSx 進行檔案存取稽核涉及下列高階工作：

1. 熟悉檔案存取稽核需求和考量事項。
2. 在特定 SVM 上建立稽核組態。
3. 在該 SVM 上啟用稽核。
4. 針對您的檔案和目錄設定稽核策略。
5. 檢視適用於 ONTAP 的 FSx 發出稽核事件記錄之後的稽核事件記錄。

作業詳細資訊在下列程序中提供。

針對檔案系統上您要啟用檔案存取稽核的任何其他 SVM 重複這些工作。

稽核要求

在 SVM 上設定並啟用下列列列列列列列列列列列列列列列列列列列列列列列列列列列列列列列列列列列列事項：

- NFS 稽核支援指定為類型的稽核存取控制項目 (ACE)u，當嘗試存取物件時，會產生稽核記錄項目。對於 NFS 稽核，模式位元和稽核 ACE 之間沒有對應。將 ACL 轉換為模式位元時，會略過稽核 ACE。將模式位元轉換為 ACL 時，不會產生稽核 ACE。

- 稽核取決於暫存磁碟區中的可用空間。(暫存磁碟區是 ONTAP 建立的專用磁碟區，用來儲存暫存檔案，這是個別節點上的中繼二進位檔案，其中稽核記錄會在轉換為 EVTX 或 XML 檔案格式之前儲存。) 您必須確定在包含稽核磁碟區的彙總中，有足夠的空間可供安裝磁碟區使用。
- 稽核取決於包含儲存已轉換稽核事件記錄檔之目錄的磁碟區中有可用空間。您必須確定用來儲存事件記錄的磁碟區中有足夠的空間。您可以在建立稽核配置時使用`-rotate-limit`參數來指定要保留在稽核目錄中的稽核記錄數目，這有助於確保磁碟區中有足夠的可用空間供稽核記錄檔使用。

在 SVM 上建立稽核組態

您必須先在儲存區虛擬機器 (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 上將其加以啟用。

在您使用命`vserver audit create`令建立稽核組態之前，請確定您已建立一個用作記錄目的地的目錄，而且該目錄沒有符號連結。您可以使用`-destination`參數指定目標目錄。

您可以建立稽核配置，根據記錄檔大小或排程輪替稽核記錄，如下所示：

- 若要根據記錄檔大小輪換稽核記錄，請使用以下指令：

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}] [-
rotate-limit integer] [-rotate-size {integer[KB|MB|GB|TB|PB]}]
```

下列範例會建立名為 SVM 的稽核組態，`svm1`以使用大小輪替來稽核檔案作業和 CIFS (SMB) 登入和登出事件 (預設值)。記錄檔格式為`EVTX` (預設值)，記錄會儲存在`/audit_log`目錄中，而且您一次只會有一個記錄檔 (大小最大為 200MB)。

```
vserver audit create -vserver svm1 -destination /audit_log -rotate-size 200MB
```

- 若要根據排程輪替稽核記錄，請使用以下指令：

```
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記錄輪替，則需要此`-rotate-schedule-minute`參數。

下列範例會針對svm2使用以時間為基礎的循環命名的 SVM 建立稽核組態。記錄檔格式為EVTX (預設值)，而且稽核記錄會在一週的所有日子每月 12:30 PM 進行輪換。

```
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的EVTX格式 (預設值) 還是以XML檔案格式建立稽核記錄。該EVTX格式允許您使用 Microsoft 事件查看器查看日誌文件。

根據預設，要稽核的事件類別包括檔案存取事件 (SMB 和 NFS)、CIFS (SMB) 登入和登出事件，以及授權原則變更事件。您可以透過參數更好地控制要記錄哪些事件，該-events參數具有下列格式：

```
-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可啟用檔案共用事件的稽核功能。

如需有關vserver audit create命令的詳細資訊，請參閱建立稽核配置。

在 SVM 上啟用稽核

完成設定稽核組態之後，您必須啟用 SVM 上的稽核功能。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，在名為的 SVM 上啟用下列命令svm1。

```
vserver audit enable -vserver svm1
```

您可隨時停用存取稽核。例如，使用下列命令關閉名為的 SVM 上的稽核svm4。

```
vserver audit disable -vserver svm4
```

當您停用稽核時，不會刪除 SVM 上的稽核設定，這表示您可以隨時在該 SVM 上重新啟用稽核。

設定檔案和資料夾稽核策略

您需要針對要稽核使用者存取嘗試進行稽核的檔案和資料夾設定稽核策略。您可以設定稽核策略來監控成功和失敗的存取嘗試。

您可以同時設定 SMB 和 NFS 稽核原則。SMB 和 NFS 稽核原則會根據磁碟區的安全性樣式，具有不同的組態需求和稽核功能。

NTFS 安全性樣式檔案和目錄的稽核策略

您可以使用視窗安全性索引標籤或 ONTAP CLI 來設定 NTFS 稽核原則。

若要設定 NTFS 稽核策略 (視窗安全性索引標籤)

您可以透過將項目新增至與 NTFS 安全性描述元相關聯的 NTFS SACL 來設定 NTFS 稽核策略。然後，安全性描述元會套用至 NTFS 檔案和目錄。這些工作會由視窗圖形用戶界面自動處理。安全性描述元可以包含用於套用檔案和資料夾存取權限的判別存取控制清單 (DACL)、檔案和資料夾稽核的 SACL，或同時包含 SACL 和 DACL。

1. 從 Windows 檔案總管的「工具」功能表中，選取「對應網路磁碟機」
2. 完成「對應網路磁碟機」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，其中包含您要稽核的資料以及共用的名稱。

    c. 選擇 Finish (完成)。

    您選取的磁碟機會掛載並準備好 Windows 檔案總管視窗，顯示共用中包含的檔案和資料夾。
3. 選取要為其啟用稽核存取的檔案或目錄。
4. 以滑鼠右鍵按一下檔案或目錄，然後選擇 [內容]。
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...	執行以下列操作
為新使用者或群組設定稽核	1. 選擇 Add (新增)。 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的名稱。 3. 選擇 OK (確定)。
從使用者或群組移除稽核	1. 在 [輸入要選取的物件名稱] 方塊中，選取您要移除的使用者或群組。 2. 選擇 Remove (移除)。 3. 選擇 OK (確定)。 4. 略過此程序的剩餘部分。
變更使用者或群組的稽核	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。 2. 選擇 編輯 。 3. 選擇 OK (確定)。

如果您要設定使用者或群組的稽核，或變更現有使用者或群組的稽核，則**##**的稽核項目] 方塊會開啟。

9. 在 [套用至] 方塊中，選取您要套用此稽核項目的方式。

   如果您要在單一檔案上設定稽核，則 [套用至] 方塊不會處於使用中狀態，因為它預設為 [僅此物件]。

10. 在「存取」方塊中，選取您要稽核的項目，以及是否要稽核成功事件、失敗事件或兩者。

    - 若要稽核成功的事件，請選擇成功方塊。
    - 若要稽核失敗事件，請選擇「失敗」方塊。

    選擇您需要監視的動作，以符合您的安全性需求。如需這些可稽核事件的詳細資訊，請參閱 Windows 文件。您可以稽核下列事件：

    - 完全控制
    - 遍歷文件夾/執行文件

- 列表文件夾/讀取數據
- 讀取屬性
- 讀取擴充屬性
- 建立檔案/寫入資料
- 建立資料夾/附加資料
- 寫入屬性
- 寫入擴充屬性
- 刪除子資料夾和檔案
- Delete
- 讀取許可
- 變更權限
- 取得所有權

11. 如果您不想將稽核設定傳播到原始容器的後續檔案和資料夾，請選擇 [將這些稽核項目套用至僅限此容器內的物件和/或容器] 方塊。
12. 選擇 Apply (套用)。
13. 完成新增、移除或編輯稽核項目之後，請選擇 [確定]。

    [物件的稽核項**#**] 方塊隨即關閉。
14. 在 [稽核] 方塊中，選擇此資料夾的繼承設定。請僅選擇提供符合安全性需求之稽核事件的最低層級。

    您可以選擇下列其中之一：

    - 選擇 [包含此物件父項中可繼承的稽核項目] 方塊。
    - 選擇 [以此物件的可繼承稽核項目取代所有子代上的所有現有可繼承稽核項目] 方塊。
    - 選擇這兩個方塊。
    - 兩個方塊都不選擇。

    如果您在單一檔案上設定 SACL，[稽核] 方塊中不會顯示 [使用此物件繼承的稽核項目取代所有子代上所有現有的可繼承稽核項目] 方塊。
15. 選擇 OK (確定)。

若要設定 NTFS 稽核原則

透過使用 ONTAP CLI，您可以設定 NTFS 稽核原則，而不需要使用 Windows 用戶端上的 SMB 共用連線至資料。

- 您可以使用 vserver 安全性檔案目錄命令系列來設定 NTFS 稽核策略。

例如，下列命令會將名為的安全性原則套用p1至名為的 SVMvs0。

```
vserver security file-directory apply -vserver vs0 -policy-name p1
```

UNIX 安全性樣式檔案和目錄的稽核原則

您可以將稽核 ACE (存取控制運算式) 新增至 NFS v4.x ACL (存取控制清單)，以設定 UNIX 安全性樣式檔案和目錄的稽核。這可讓您基於安全性目的監視特定 NFS 檔案和目錄存取事件。

> **Note**
>
> 對於 NFS v4.x，選擇性和系統 ACE 都儲存在相同的 ACL 中。因此，在將稽核 ACE 新增至現有 ACL 時，您必須小心，以避免覆寫和遺失現有 ACL。將稽核 ACE 新增至現有 ACL 的順序無關緊要。

若要配置 UNIX 稽核策略

1. 使用或等效指令擷取檔案或目錄的nfs4_getfacl現有 ACL。
2. 附加所需的稽核 ACE。
3. 使用或對等的指令，將更新的 ACL 套用至檔案nfs4_setfacl或目錄。

   此範例會使用此-a選項，將名為的檔案授予使用者 (名為testuser) 讀取權限file1。

   ```
   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記錄。

- EVTX檔案格式 — 您可以使用 Microsoft 事件檢視器將轉換後的EVTX稽核事件記錄檔開啟為已儲存的檔案。

  使用事件檢視器檢視事件記錄檔時，您可以使用兩個選項：

  - 一般檢視：會針對事件記錄顯示所有事件共用的資訊。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的資料。
  - 詳細視圖：友好的視圖和 XML 視圖可用。易記檢視和 XML 檢視會同時顯示所有事件通用的資訊，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 檔案格式的協力廠商應用程式上檢視和處理 XML 稽核事件記錄。如果您擁有 XML 結構描述和 XML 欄位定義的相關資訊，XML 檢視工具可用來檢視稽核記錄。

擴充固態硬碟儲存容量和佈建的 IOPS

當您需要為資料集的使用中部分提供額外儲存空間時，可以增加適用於 NetApp ONTAP 檔案系統之 Amazon FSx 的固態硬碟 (SSD) 儲存容量。您可以使用 Amazon FSx 主控台、Amazon FSx API 或 AWS Command Line Interface ()AWS CLI來執行此操作。

您也可以在增加主要 SSD 儲存容量或獨立動作時，針對檔案系統變更佈建的 SSD IOPS。如需擴充檔案系統主要 SSD 儲存容量和佈建 IOPS 數量的詳細資訊，請參閱更新檔案系統固態硬碟儲存和 IOPS。

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。您可以隨時修改向上擴充檔案系統的輸送量容量，但無法修改向外延展檔案系統的輸送量容量。請記住，您的檔案系統需要特定的組態才能達到最大的輸送量容量。例如，若要為向上擴充的檔案系統佈建 4 Gbps 的輸送量容量，您的檔案系統需要配置至少 5,120 GiB 的 SSD 儲存容量和 160,000 個固態硬碟 IOPS。如需詳細資訊，請參閱輸送量容量對效能的影響。

輸送量容量是決定主控檔案系統的檔案伺服器可以提供檔案資料的速度之一。較高的輸送量容量層級包含更高層級的網路、每秒磁碟讀取 I/O 作業 (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。

修改檔案系統的輸送量容量時，Amazon FSx 會切換為檔案系統提供動力的檔案伺服器。在此過程中，單一可用區和異地同步備份檔案系統都會遇到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) 和 iSCSI (網際網路小

型電腦系統介面) 用戶端來說是透明的，讓您的工作負載能夠繼續執行，而不會中斷或手動介入。檔案系統可使用新的輸送量容量後，我們會向您收取費用。

> **Note**
>
> 為了確保維護活動期間的資料完整性，FSx for ONTAP 會關閉所有隨機鎖定，並在維護開始之前，對託管檔案系統的基礎儲存磁碟區完成任何擱置的寫入作業。在排程的檔案系統維護期間，系統修改 (例如對輸送量容量的修改) 可能會延遲。系統維護可能會導致這些變更排入佇列狀態，直到處理完畢為止。如需詳細資訊，請參閱the section called “維護時段”。

主題

何時修改輸送量容量

Amazon FSx 與 Amazon 整合 CloudWatch，可協助您監控檔案系統持續的輸送量使用量等級。您可以透過檔案系統驅動的輸送量和 IOPS 效能，取決於特定工作負載的特性，以及檔案系統的輸送量容量。通常，您應該佈建足夠的輸送量容量來支援工作負載的讀取輸送量，以及工作負載寫入輸送量的兩倍。您可以使用 CloudWatch 指標來決定要變更哪些維度以提升效能。如需詳細資訊，請參閱the section called “如何將 FSx 用於 ONT CloudWatch AP 量度”。

> **Note**
>
> 您無法修改向外延展檔案系統的輸送量容量。

如何處理並行輸送量和儲存擴展要求

您可以在 SSD 儲存容量和佈建的 IOPS 更新工作流程開始或進行中之前，要求輸送量容量更新。Amazon FSx 處理這兩個請求的方式順序如下：

- 如果您同時提交 SSD/IOPS 更新和輸送量容量更新，則會接受這兩個要求。SSD/IOPS 更新會在輸送量容量更新之前排列優先順序。

- 如果您在 SSD/IOPS 更新正在進行時提交輸送量容量更新，則會接受輸送量容量更新要求，並在 SSD/IOPS 更新之後排入佇列。輸送量容量更新會在 SSD/IOPS 更新後 (有新值可用) 以及在最佳化步驟期間開始。這通常需要不到 10 分鐘。
- 如果您在輸送量容量更新進行時提交 SSD/IOPS 更新，則會接受 SSD/IOPS 儲存體更新要求，並在輸送量容量更新完成之後啟動 (新的輸送量容量可用)。這通常需要 20 分鐘。

如需 SSD 儲存和佈建 IOPS 更新的詳細資訊，請參閱管理儲存容量。

如何修改輸送量容量

您可以使用 Amazon FSx 主控台、AWS Command Line Interface (AWS CLI) 或 Amazon FSx API 修改檔案系統的輸送量容量。

修改檔案系統的輸送量容量 (主控台)

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 瀏覽至檔案系統，然後選擇您要增加輸送量容量的 ONTAP 檔案系統。
3. 對於動作，選擇更新輸送量容量。或者，在「摘要」面板中，選擇檔案系統的輸送量容量旁邊的「更新」。
4. 從清單中選擇「輸送量容量」的新值。

   > **Note**
   >
   > 您可以變更任何 ONTAP 檔案系統 FSx 的輸送量容量。不過，只有在 2021 年 12 月 9 日或之後建立的檔案系統，才能支援 128 MB/s 或 256 MB 的輸送量容量。

5. 選擇更新以起始輸送量容量更新。
6. 您可以在 [檔案系統詳細資料] 頁面的 [更新] 索引標籤上監視更新進度。

   您可以使用 Amazon FSx 主控台、和 API 來監控更新的進度。AWS CLI如需詳細資訊，請參閱監視輸送量容量變更。

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指令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`到要將檔案系統更新為的所需值。

您可以使用 Amazon FSx 主控台、和 API 來監控更新的進度。AWS CLI如需詳細資訊，請參閱監視輸送量容量變更。

監視輸送量容量變更

您可以使用 Amazon FSx 主控台、API 和. AWS CLI

監視主控台中的輸送量容量變更

在 [檔案系統詳細資訊] 視窗的 [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、儲存容量和儲存區最佳化。

目標值

將檔案系統的輸送量容量變更為所需的值。

狀態

更新的目前狀態。對於輸送量容量更新，可能的值如下：

- 擱置中 — Amazon FSx 已收到更新要求，但尚未開始處理。
- 進行中 — Amazon FSx 正在處理更新請求。
- 已完成 — 輸送量容量更新順利完成。
- 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-systemsCLI 命令和 DescribeFileSystemsAPI 動作來檢視和監視檔案系統輸送量容量修改要求。`AdministrativeActions`陣列會列出每個管理動作類型的 10 個最新更新動作。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 describe-file-systems CLI 命令的回應摘錄。檔案系統的輸送量容量為 128 MB/s，目標輸送量容量為每秒 256 MB。

```
.
.
.
    "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。然後檔案系統即可使用新的輸送量容量，並顯示在內ThroughputCapacity容中。這顯示在下面的 describe-file-systems CLI 命令的響應摘錄中。

```
.
.
.
    "ThroughputCapacity": 256,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "COMPLETED",
        "TargetFileSystemValues": {
          "OntapConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

如果輸送量容量修改失敗，狀態會變更為FAILED，且FailureDetails內容會提供失敗的相關資訊。

使用 Amazon FSx 維護時段將效能最佳化

FSx for ONTAP 是一項完全管理的服務，會定期對您的檔案系統執行維護和更新。此維護對大多數工作負載沒有任何影響。對於效能敏感的工作負載，在極少數情況下，您可能會注意到維護發生時對效能的短暫影響 (<60 秒)；Amazon FSx 可讓您使用維護時段控制何時發生此類潛在維護活動。

修補不常發生，通常每數週進行一次。對於向上擴充的檔案系統，修補通常只需要從維護時段開始 30 分鐘即可完成。對於向外延展檔案系統，修補需要從維護時段開始起最多 90 分鐘。在這幾分鐘內，您的檔案系統會自動容錯移轉並容錯回復。您可以在建立檔案系統期間選擇維護時段。如果您沒有時間偏好設定，則會指派 30 分鐘的開始時間。

FSx for ONTAP 可讓您根據需要調整維護時段，以符合您的工作負載和作業需求。您可以視需要頻繁地移動維護時段，前提是維護時段至少每 14 天發生一次。如果修補程式已發行，但未在 14 天內出現維護時段，則 FSx for ONTAP 將繼續對檔案系統進行維護，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 會關閉所有隨機鎖定，並在維護開始之前，對託管檔案系統的基礎儲存磁碟區完成任何擱置的寫入作業。

您可以使用 Amazon FSx 管理主控台 AWS CLI、 AWS API 或其中一個開 AWS 發套件來變更檔案系統的維護時段。

若要變更每週維護時段 (主控台)

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
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」維護視窗。
6. 輸入您要每週維護時段開始的新日期與時間。
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-systemCLI 指令變更每週維護時段，請參閱更新檔案系統 (CLI)。

標記您的 Amazon FSx 資源

為協助您管理您的檔案系統和其他 Amazon FSx 資源，您可將您自己的中繼資料，以標籤的形式指派給每個資源的每個資源。使用標籤，您可以用不同的方式將您的AWS資源分類，例如依用途、擁有者或環境。當您有許多相同類型的資源時，這種分類將會很有用，因為您可以依據先前指派的標籤，快速識別特定的資源。本主題說明標籤並示範如何建立它們。

主題

標籤基本概念

標籤是您指派給AWS資源的標籤。每個標籤都由您定義的兩個部分組成：

- 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。標籤值是可選的。

您可以使用標籤以不同的方式將您的AWS資源分類，例如依用途、擁有者或環境。例如，您可以為您帳戶的 Amazon FSx 檔案系統定義一組標籤，協助您追蹤各個執行個體的擁有者與堆疊層級。

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的管理您的資源。您可以根據您所新增的標籤來搜尋和篩選資源。如需有關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。

需要謹記的一些標記行為：

- 標籤對 Amazon FSx 來說不具有任何語意，並會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為空白字串，但您無法將標籤的值設為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開發套件，您可以執行下列動作：
  - 您可以使用 TagResource API 動作將標籤套用到現有資源。
  - 針對某些資源建立資源的動作，您可以在建立資源時指定資源的標籤。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。

    如果標籤無法在資源建立時套用，Amazon FSx 會轉返資源建立程序。此行為有助於確保資源不是具有標籤建立，就是不會建立，因此無論何時都不會有不具有標籤的資源。

    > **Note**
    >
    > 使用者在建立時為資源加上標籤的使用者需要特定的 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

您可以為您帳戶中現有的 Amazon FSx 資源新增標籤。若您使用 Amazon FSx 主控台，可以透過使用位於相關資源畫面上的標籤索引標籤來對資源套用標籤。建立資源時，您可以套用具有值的 Name 鍵，並且可以在建立新檔案系統時套用您選擇的標籤。但是，即使主控台根據 Name 金鑰整理資源，此金鑰對 Amazon FSx 服務來說不具有任何語意意意意意意意意意義。

若要對可在建立時為資源加上標籤的使用者和群組實作精密控制，您可以在 IAM 政策中將標籤式的資源層級許可套用到支援在建立時新增標籤的 Amazon FSx API 動作。在您的政策中使用此類許可，您可以獲得下列好處：

- 您的資源從建立時便已獲得適當保全。
- 由於標籤會立即套用到您的資源，控制使用資源的任何標籤式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。

若要控制哪些標籤金鑰和值會在您現有的資源上設定，您可以將資源層級許可套用到 IAM 政策中的TagResource和 UntagResource Amazon FSx API 動作。

如需在建立時為 Amazon FSx 資源加上標籤之 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。

如需有關在 IAM 政策中使用標籤來限制對 IAM 政策中 Amazon FSx 資源的使用，請參閱使用標籤來控制對 Amazon FSx 資源的存取。

如需為您的資源建立標籤以便計費的資訊，請參閱使用AWS Billing者指南中的使用成本分配標籤。

複製標籤到備份

在 Amazon FSx API 中建立或更新磁碟區時AWS CLI，或者可以啟用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，請參閱使用備份。如需有關啟用的詳細資訊CopyTagsToBackups，請參閱 若要建立磁碟區 (CLI) Amazon FSx 適用於 NetApp ONTAP 使用者指南的CreateVolume和UpdateVolume中的，或參閱 Amazon FSx 中的 NetApp ONTAP API 參考資料。更新磁碟區的組態 (CLI)

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。
- 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)。
- 允許的字元包括可用 UTF-8 表示的英文字母、數字和空格，還有以下特殊字元：+-(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。
- 此 aws: 字首已保留供 AWS 使用。如果標籤具有此字首的標籤金鑰，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。

您無法僅根據標籤來刪除資源，您必須指定資源識別符。例如，若要刪除您使用名為之標籤索引鍵標記的檔案系統DeleteMe，您必須將DeleteFileSystem動作與檔案系統資源識別元搭配使用，例如fs-1234567890abcdef0。

當您標記公AWS 帳戶有或共享資源時，您指派的標籤僅適用於您的標籤AWS 帳戶；其他標籤無其他標籤可以存取這些標籤。針對共享資源的標記型存取，每個標籤AWS 帳戶必須指派其自身的一組標籤，以控制對資源的存取權。

權限和標記

如需在建立時為 Amazon FSx 資源加上標籤之 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。

如需有關在 IAM 政策中使用標籤來限制對 IAM 政策中 Amazon FSx 資源的使用，請參閱使用標籤來控制對 Amazon FSx 資源的存取。

使用應用模組管理 ONTAP 資源的 FSx NetApp

除了、和 AWS API 和 SDK 之外 AWS Management Console AWS CLI，您還可以使用下列NetApp管理工具和應用程式來管理您的 ONTAP 資源 FSx：

主題

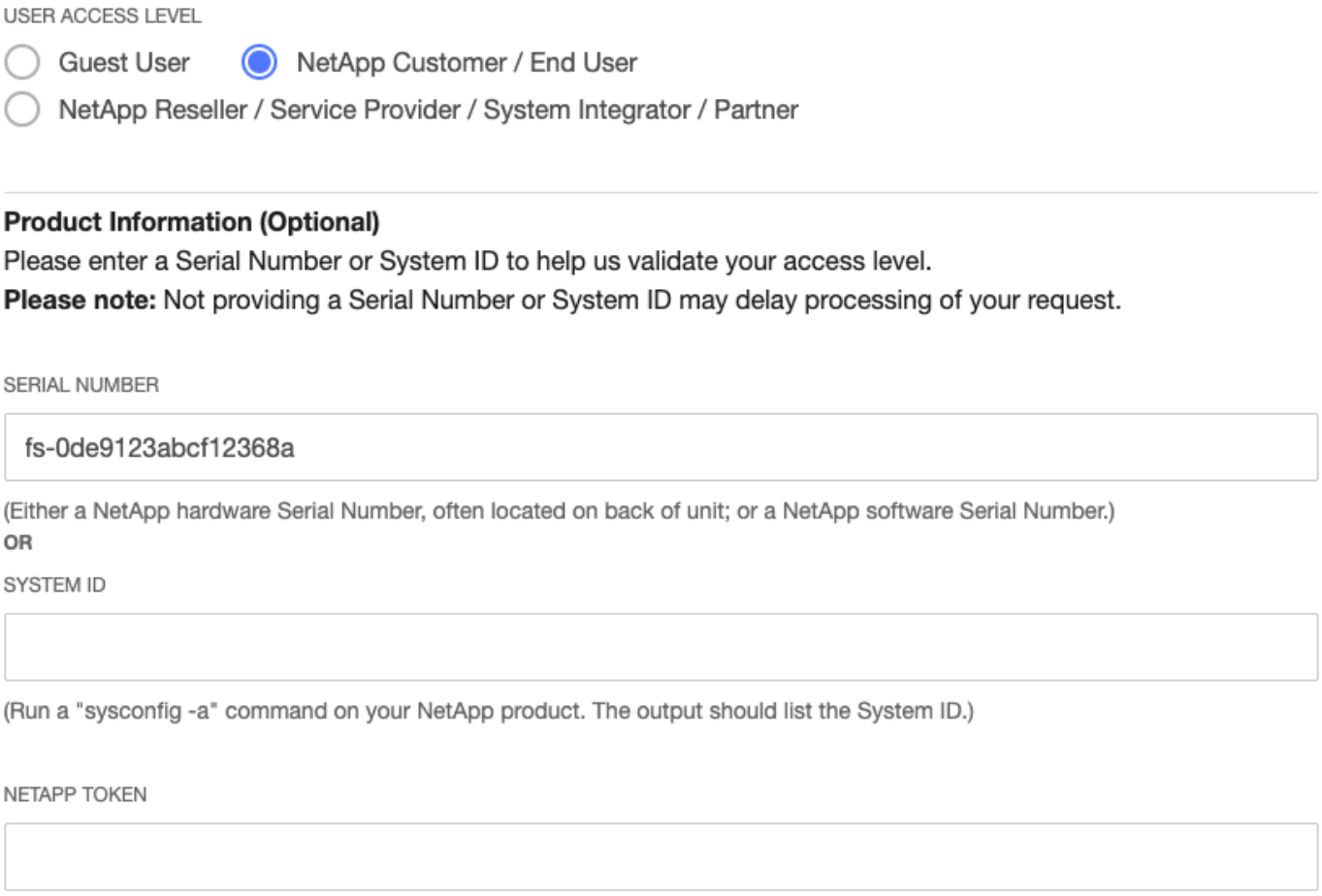
- 註冊一個NetApp帳戶
- 使用 NetApp BlueXP
- 使用 NetApp ONTAP CLI
- 使用 ONTAP REST API

> **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 SDK 中。

註冊一個NetApp帳戶

若要下載某些NetApp軟體，例如BlueXPSnapCenter、和ONTAP防毒連接器，您必須擁有一個NetApp帳戶。若要註冊NetApp帳戶，請執行以下步驟：

1. 轉到NetApp用戶註冊頁面並註冊一個新的NetApp用戶帳戶。
2. 填寫表格並提供您的資訊。請務必選取「NetApp客戶/一般使用者」存取層級。在序號欄位中，複製並貼上適用於 ONTAP 檔案系統 FSx 的檔案系統識別碼。請參閱下列範例：



註冊後會有什麼期望

擁有現有NetApp產品的客戶將在一個工作日內將其 NSS 帳戶分配到客戶級別訪問權限。新來的客戶除了NetApp將 NSS 帳戶提供給「客戶級別」存取權限外，還將使用標準商業慣例加入。提供檔案系統 ID 有助於加速此程序。您可以登入我的支援網站並瀏覽至歡迎頁面，以檢查您的 NSS 帳戶狀態。您帳戶的存取層級應為「客戶存取權」。

使用 NetApp BlueXP

NetApp BlueExp 是一個統一的控制平台，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。BlueExp 提供集中式使用者介面，用於管理、監控和自動化內部部署 AWS 和內部部署的

ONTAP。如需詳細資訊，請參閱 NetApp BlueExp 文件和適用於 ONTAP 的 Amazon FSX 的 NetApp BlueExp 文件。 NetApp

> **Note**
>
> NetApp BlueXP向外延展檔案系統不支援。

使用NetApp系統管理員 BlueXP

您可以直接使用系統管理員來管理適用於 NetApp ONTAP 檔案系統的 Amazon FSx。BlueXP BlueXP 可讓您使用您習慣使用的相同系統管理員介面，讓您從單一控制平台管理混合式多雲端基礎架構。您也可以使用 BlueExp 的其他功能。如需詳細資訊，請參閱 NetApp ONTAP 文件中的系統管理員與 BlueExp 整合主題。

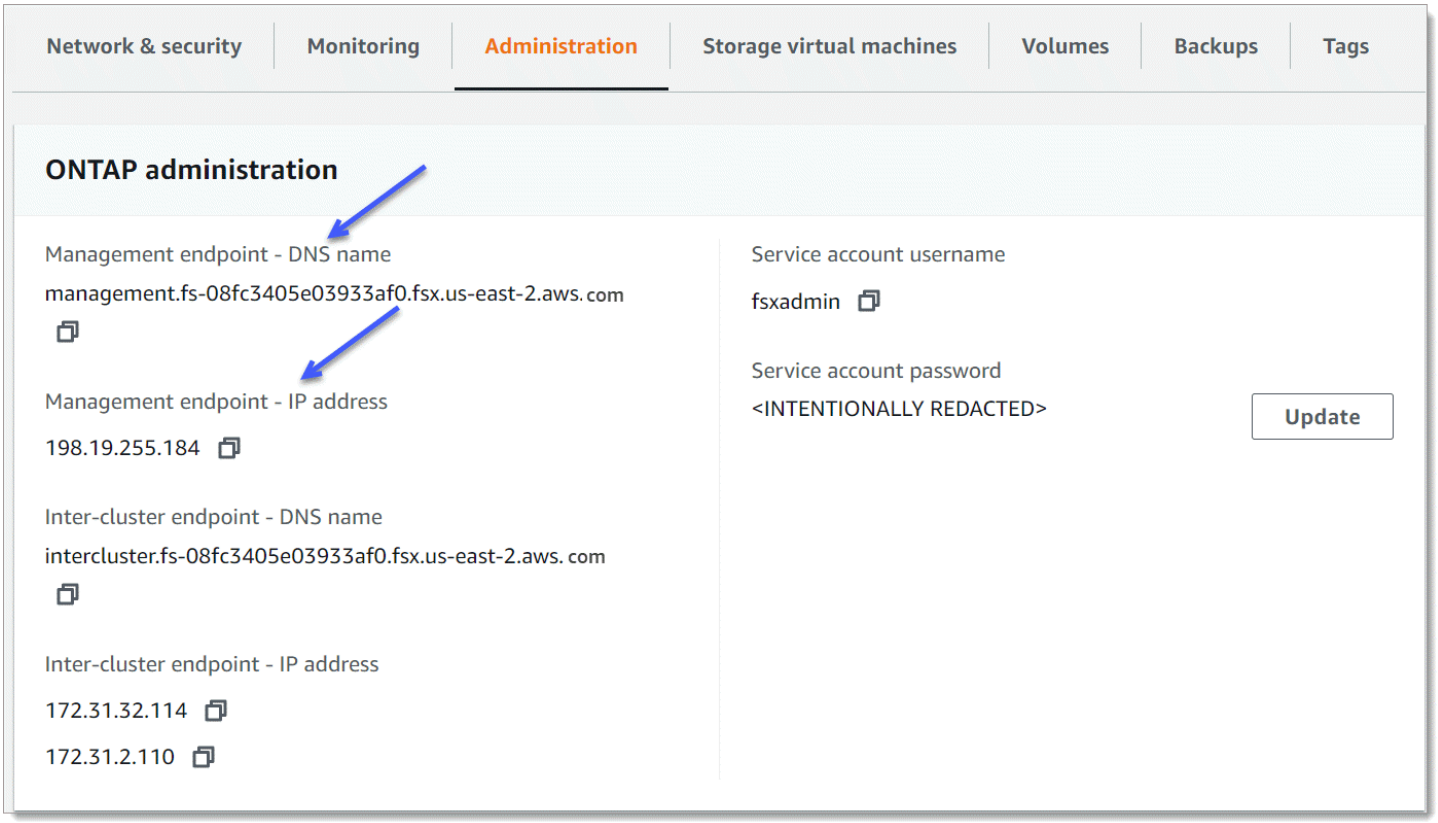
> **Note**
>
> NetApp 向外延展檔案系統不支援系統管理員。

使用 NetApp ONTAP CLI

您可以使用 CLI 管理適用於 NetApp ONTAP 資源的 Amazon FSx。NetApp ONTAP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 ONTAP CLI 管理檔案系統

您可以在 FSx for ONTAP 檔案系統上執行 ONTAP CLI 命令，類似於在叢集上執行這些命令。NetApp ONTAP您可以在檔案系統上存取 ONTAP CLI，方法是建立與檔案系統管理端點的安全殼層 (SSH) 連線，並`fsxadmin`使用使用者名稱和密碼登入。您可以選擇在使用自訂建立流程或使用建立檔案系統時設定密碼 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密碼以登入 ONTAP CLI。如需詳細資訊，請參閱 更新檔案系統。您可以在 Amazon FSx 主控台的 ONTAP 檔案系統詳細資訊頁面的 FSx 管理索引標籤中，找到檔案系統管理端點的 DNS 名稱和 IP 位址，如下圖所示。



若要透過 SSH 連線至檔案系統的管理端點，請使用使用`fsxadmin`者和密碼。您可以從與檔案系統位於相同 VPC 的用戶端以 SSH 方式存取檔案系統的管理端點 IP 位址或 DNS 名稱，如下列範例所示。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

帶有示例值的 SSH 命令：

```
ssh fsxadmin@198.51.100.0
```

使用管理端點 DNS 名稱的 SSH 命令：

```
ssh fsxadmin@file-system-management-endpoint-dns-name
```

使用範例 DNS 名稱的 SSH 命令：

```
$ ssh fsxadmin@management.fs-0abcdef123456789.fsx.us-east-2.aws.com
  Password: fsxadmin-password

This is your first recorded login.
```

```
FsxId0abcdef123456789::>
```

ONTAPCLI 命令的範圍可用於 **fsxadmin**

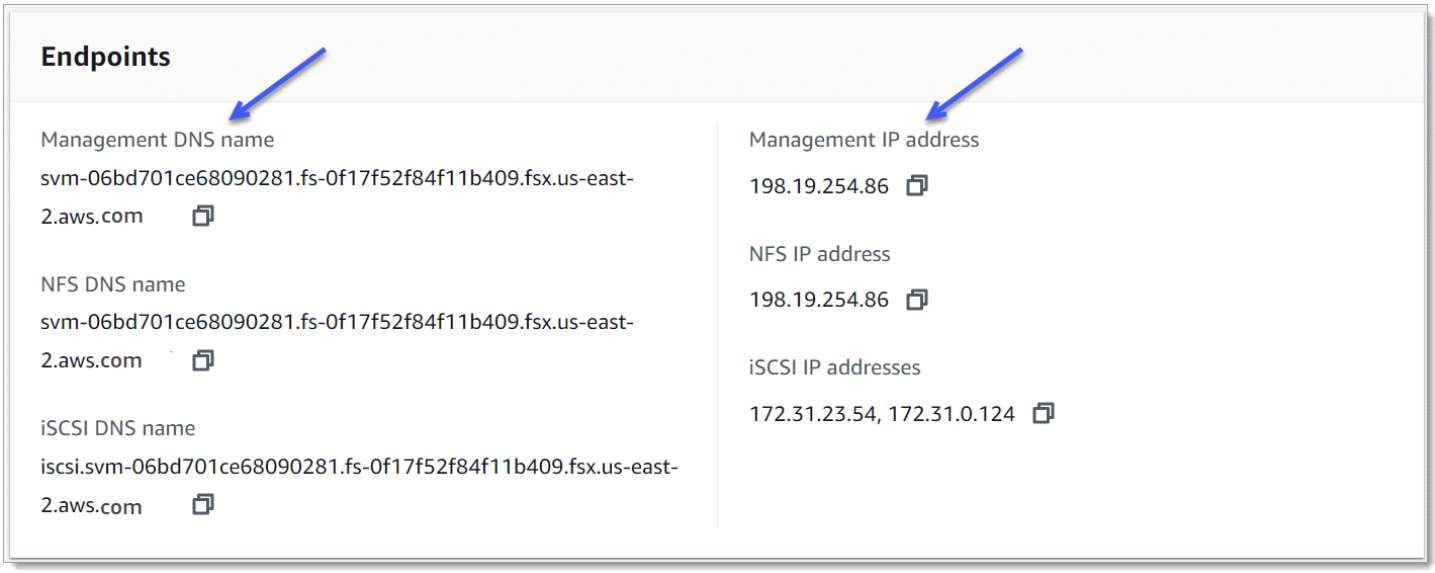
fsxadmin的管理檢視位於檔案系統層級，其中包括檔案系統中的所有 SVM 和磁碟區。
角fsxadmin色扮演ONTAP叢集管理員的角色。由於適用於 NetApp ONTAP 檔案系統的 Amazon FSx 是完全受管的，因此該fsxadmin角色可以執行可用 ONTAP CLI 命令的子集。

若要查看fsxadmin可執行的命令清單，請使用下列 security login role showONTAPCLI 命令：

```
FsxId0abc123def456::> security login role show -role fsxadmin -access !none
           Role          Command/                                    Access
Vserver    Name          Directory                          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
.
.
.
363 entries were displayed.
```

使用 CLI 管理 SVM ONTAP

您可以使用fsxadmin或使用vsadmin者名稱和密碼建立與 SVM 管理端點的安全殼層 (SSH) 連線，以存取 SVM 上的 ONTAP CLI。您可以在 Amazon FSx 主控台的儲存虛擬機器詳細資料頁面的端點面板中，找到 SVM 的管理端點 DNS 名稱和 IP 位址，如下圖所示。



若要透過 SSH 連線至 SVM 的管理端點，您可以使用vsadmin或使用fsxadmin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 更新儲存區虛擬機器。您可以使用管理端點 IP 位址或 DNS 名稱，從與檔案系統位於相同 VPC 中的用戶端以 SSH 方式存取 SVM。

```
ssh vsadmin@svm-management-endpoint-ip-address
```

具有範例值的指令：

```
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-0abcdef123456789.fsx.us-east-2.aws.com
```

```
Password: vsadmin-password

This is your first recorded login.
FsxId0abcdef123456789::>
```

適用於 NetApp ONTAP 的 Amazon FSx 支援 NetApp ONTAP CLI 命令。

如需 NetApp ONTAP CLI 命令的完整參考資料，請參閱 ONTAP 命令：手動頁面參考。

使用 ONTAP REST API

使用`fsxadmin`憑證使用 ONTAP REST API 存取 ONTAP 檔案系統的 FSx 時，請執行下列其中一個動作：

- 停用 TLS 驗證。

  或
- 信任 AWS 憑證授權單位 (CA) — 您可以在下列 URL 中找到每個區域中 CA 的憑證組合包：
  - https://fsx-aws-certificates.s3.amazonaws.com/bundle-適合公眾的 *`aws-region`*。 AWS 區域
  - https://fsx-aws-us-gov-certificates.s3.us-gov-west-1.amazonaws.com/bundle-適用於地區的 *`aws-region`*。 AWS GovCloud
  - https://fsx-aws-cn-certificates.s3.cn-north-1.amazonaws.com.cn/bundle-適用於中*`#### AWS`* 地區 AWS

如需 NetApp ONTAP REST API 命令的完整參考資料，請參閱 NetApp ONTAPREST API 線上參考資料。

適 NetApp 用於 ONTAP 的 Amazon FSx 中的安全性

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，這些架構是為了滿足對安全性最敏感的組織的需求而建置的。

安全是 AWS 與您之間共同承擔的責任。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：

- 雲端安全性 — AWS 負責保護中執行 AWS 服務的基礎架構 AWS 雲端。 AWS 還為您提供可以安全使用的服務。若要了解適用於 NetApp ONTAP 的 Amazon FSx 的合規計劃，請參閱合規計劃AWS 服務範圍內的服務範圍計劃)。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您了解如何在使用 Amazon FSx 時套用共同的責任模型。下列主題說明如何設定 Amazon FSx 以符合安全和合規目標。您也會學到如何使用其他可 AWS 協助您監控和保護 Amazon FSx 資源的服務。

主題

適 NetApp 用於 ONTAP 的 Amazon FSx 中的資料保護

AWS 共同責任模型適用於 NetApp ONTAP 的 Amazon FSx 中的資料保護。如此模型中所述， AWS 負責保護執行所有 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，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。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 資源進行通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 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。
- 如果透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用主控台、API 或 AWS 開發套件 AWS 服務 使用 Amazon FSx 或其他軟體時。 AWS CLI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。

適用於 ONTAP 的 FSx 中的資料加密

適用於 NetApp ONTAP 的 Amazon FSx 支援靜態資料加密和傳輸中的資料加密。建立 Amazon FSx 檔案系統時，系統會自動啟用靜態資料加密。Amazon FSx for NetApp ONTAP 支援透過 NFS 和 SMB 協定傳輸的 Kerberos 型加密，如果您要存取加入至作用中目錄的儲存虛擬機器 (SVM) 中的資料，或使用輕量型目錄存取通訊協定 (LDAP) 傳輸至網域的資料。

使用加密時

如果您的組織遵守需要加密靜態資料和中繼資料的公司或法規原則，您的資料會在靜態時自動加密。我們也建議您使用傳輸中的資料加密來掛接檔案系統，以啟用傳輸中資料的加密功能。

如需使用適用於 NetApp ONTAP 的 Amazon FSx 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

所有適用於 NetApp ONTAP 檔案系統的 Amazon FSx 都會使用 AWS Key Management Service ()AWS KMS管理的金鑰進行靜態加密。數據在寫入文件系統之前會自動加密，並在讀取時自動解密數據。Amazon FSx 會透明地處理這些程序，因此您不必修改應用程式。

Amazon FSx 使用業界標準的 AES-256 加密演算法來加密 Amazon FSx 資料和靜態中繼資料。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 金鑰管理基礎架構使用聯邦資訊處理標準 (FIPS) 140-2 核准的加密演算法。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 AWS KMS 金鑰管理整合。Amazon FSx 使用 KMS 金鑰來加密您的檔案系統。您可以選擇用來加密和解密檔案系統 (包括資料和中繼資料) 的 KMS 金鑰。您可以啟用、停用或撤銷此 KMS 金鑰的授權。此 KMS 金鑰可以是下列兩種類型之一：

- AWS-受管理的 KMS 金鑰 — 這是預設的 KMS 金鑰，可免費使用。
- 客戶管理的 KMS 金鑰 — 這是最靈活的 KMS 金鑰，因為您可以為多個使用者或服務設定其金鑰原則和授權。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，您可以啟用金鑰輪替。啟用金鑰輪換時， AWS KMS 每年會自動輪換金鑰一次。此外，透過客戶管理的 KMS 金鑰，您可以隨時選擇停用、重新啟用、刪除或撤銷 KMS 金鑰存取權的時間。如需詳細資訊，請參閱AWS Key Management Service 開發人員指南中的旋轉 AWS KMS keys和啟用和停用金鑰。

Amazon FSx 關鍵政策 AWS KMS

金鑰政策是控制對 KMS 金鑰之存取的主要方式。如需關鍵原則的詳細資訊，請參閱AWS Key Management Service 開發人員指南AWS KMS中的使用金鑰政策。下列清單說明 Amazon FSx 針對靜態檔案系統加密支援的所有 AWS KMS相關許可：

- 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。密文是先前已加密的純文本。此許可會納入預設的金鑰政策中。
- kms：ReEncrypt— (可選) 使用新的對服務器端的數據進行加密 AWS KMS key，而不會在客戶端暴露數據的純文本。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：GenerateDataKeyWithout純文字 — (必要) 傳回以 KMS 金鑰加密的資料加密金鑰。此權限包含在 kms: K GenerateData ey* 下的預設金鑰原則中。
- kms: CreateGrant — (必要) 將授權新增至金鑰，以指定誰可以使用金鑰，以及在何種情況下可以使用金鑰。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) 提供有關指定 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) 列出帳戶中的所有金鑰別名。當您使用主控台建立加密的檔案系統時，此權限會填入 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 ONTAP 檔案系統的 FSx 與連線用戶端之間傳輸時，可用來加密檔案資料的不同選項。它也提供指引，協助您選擇最適合您工作流程的加密方法。

在離開 AWS 安全 AWS 區域 設施之前，所有流經 AWS 全球網路的資料都會在實體層自動加密。可用區域之間的所有流量都會加密。其他加密層 (包括本節所列的加密層) 可提供額外的保護。有關如何為流動 AWS 區域、可用區域和執行個體的資料 AWS 提供保護的詳細資訊，請參閱 Amazon 彈性運算雲端 Linux 執行個體使用者指南中的傳輸中加密。

適用於 NetApp ONTAP 的 Amazon FSx 支援下列方法，針對 ONTAP 檔案系統和連線用戶端的 FSx 之間傳輸中的資料進行加密：

- 對所有支援的協定和在支援的 Amazon EC2 Linux 和 Windows 執行個體類型上執行的用戶端進行自動以硝基為基礎的加密。

- 透過 NFS 和 SMB 通訊協定進行 Kerberos 型加密。
- 透過 NFS、iSCSI 和中小企業通訊協定進行基於 IPSEC 的加密

所有支援的傳輸中資料加密方法都使用業界標準 AES-256 加密演算法，提供企業強度加密。

主題

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方法最適合您的工作流程。當您探索以下各節中詳細描述的支援選項時，請回到本節。

在選擇如何加密 FSx for ONTAP 檔案系統與連線用戶端之間傳輸中的資料時，有幾個因素需要考量。這些因素包括：

- 您 AWS 區域 的 ONTAP 文件系統的 FSx 正在運行。
- 用戶端執行所在的執行個體類型。
- 用戶端存取檔案系統的位置。
- 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 活動目錄。

AWS 區域

執 AWS 區域 行檔案系統會決定您是否可以使用 Amazon Nitro-based 加密。以下提供以硝基為基礎的加密： 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)
- 歐洲 (愛爾蘭)

此外，亞太區域 (雪梨) 的向外擴充檔案系統也提供以硝基為基礎的加密功能。 AWS 區域

客戶端實例類型

如果存取檔案系統的用戶端在任何受支援的 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硝基型加密的所有其他要求，則可以使用 Amazon Nit ro 加密。使用 Kerberos 或 IPsec 加密並沒有任何用戶端執行個體類型需求。

用戶端位置

用戶端存取資料相對於檔案系統位置的位置，會影響可使用的傳輸中加密方法。如果用戶端和檔案系統位於相同的 VPC 中，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 VPC 中，只要流量未經過虛擬網路裝置或服務 (例如傳輸閘道)，情況也是如此。如果用戶端不在相同或對等的 VPC 中，或者流量通過虛擬網路裝置或服務，則無法使用以硝基於硝基礎的加密選項。

網路效能

使用 Amazon 硝基加密技術不會影響網路效能。這是因為受支援的 Amazon EC2 執行個體利用基礎 Nitro 系統硬體的卸載功能，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，因此用戶端和伺服器必須使用計算資源來加密和解密傳輸中的流量。

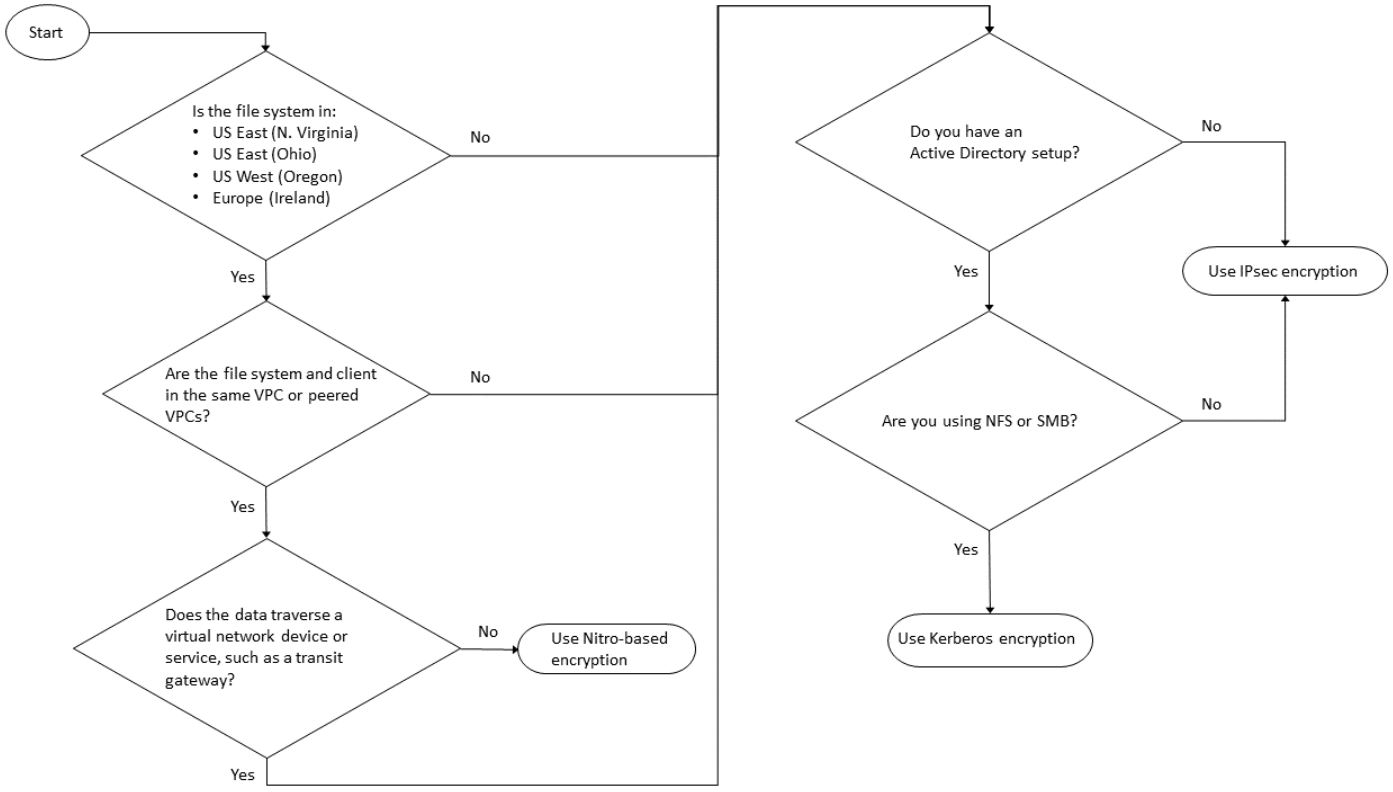
数据协议

您可以在所有支援的通訊協定 (NFS、SMB 和 iSCSI) 上使用 Amazon 硝基加密和 IPsec 加密。您可以將 Kerberos 加密與 NFS 和 SMB 通訊協定 (搭配使用中目錄) 搭配使用。

Active Directory

如果您使用的是Microsoft作用中目錄，您可以透過 NFS 和 SMB 通訊協定使用 Kerberos 加密。

使用下圖可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、中小型企業或 iSCSI 通訊協定。
- 您的工作流程不支援使用 Amazon 硝基加密。
- 您沒有使用Microsoft活動目錄域。

使用 AWS Nitro 系統對傳輸中的數據進行加密

透過以 Nitro 為基礎的加密，當存取檔案系統的用戶端在支援的 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。

使用 Amazon Nitro-based 加密不會影響網路效能。這是因為受支援的 Amazon EC2 執行個體利用基礎 Nitro 系統硬體的卸載功能，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的 VPC 中或與檔案系統的 VPC 對 AWS 區域 等的 VPC 中時，系統會自動啟用以 Nitro 為基礎的加密。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)，以便自動啟用以 Nitro 為基礎的加密。如需有關硝基加密的詳細資訊，請參閱 Amazon EC2 Linux 或 Windows 執行個體類型使用者指南中的傳輸中加密一節。

以硝基為基礎的傳輸中加密可用於 2022 年 11 月 28 日之後建立的檔案系統，如下所示： 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)
- 歐洲 (愛爾蘭)

此外，亞太區域 (雪梨) 的向外擴充檔案系統也提供以硝基為基礎的加密功能。 AWS 區域

如需有關可用於 ONTAP AWS 區域 的 FSx 的詳細資訊，請參閱 Amazon FSx 的 ONTAP 定價。NetApp

如需 ONTAP 檔案系統 FSx 的效能規格的相關資訊，請參閱。輸送量容量對效能的影響

使用 Kerberos 型加密技術加密傳輸中的資料

如果您使用的是Microsoft作用中目錄，您可以透過 NFS 和 SMB 通訊協定使用 Kerberos 型加密，針對已加入 Microsoft Active Directory 的 SVM 子磁碟區，加密傳輸中的資料。

使用 Kerberos 加密透過 NFS 傳輸的資料

NFSv3 和 NFSv4 通訊協定支援使用 Kerberos 進行傳輸中的資料加密。若要針對 NFS 通訊協定使用 Kerberos 在傳輸過程中啟用加密，請參閱「文件中心」中的使用 Kerberos 搭配 NFS 以獲得強大的安全性。NetApp ONTAP

使用 Kerberos 加密透過中小企業傳輸中的資料

對應至支援 SMB 通訊協定 3.0 或更新版本的運算執行個體上的檔案共用，支援透過 SMB 通訊協定傳輸中的資料加密。這包括所有Microsoft Windows版本從 Microsoft 視窗服務器 2012 及更高版本，以及 Microsoft 視窗 8 及更高版本。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。

適用於 ONTAP SMB 的 FSx 支援 128 位元和 256 位元加密，這是由用戶端工作階段要求決定的。如需不同加密層級的說明，請參閱NetApp ONTAP文件中心使用 CLI 管理 SMB 的 < 設定 SMB 伺服器最低驗證安全性層級 > 一節。

> **Note**
>
> 用戶端決定加密演算法。NTLM 和 Kerberos 驗證都可以使用 128 位元和 256 位元加密。該 FSx 的 ONTAP SMB 服務器接受所有標準的 Windows 客戶端請求，和細微的控制由 Microsoft 組策略或註冊表設置處理。

您可以使用 ONTAP CLI 來管理 FSx 上的 ONTAP SVM 和磁碟區的傳輸中加密設定。若要存取 NetApp ONTAP CLI，請在要在傳輸設定中進行加密的 SVM 上建立 SSH 工作階段，如中使用 CLI 管理 SVM ONTAP所述。

如需如何在 SVM 或磁碟區上啟用 SMB 加密的指示，請參閱對傳輸中的資料啟用 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，以確保資料在傳輸過程中持續安全且加密。IPsec 針對所有支援的 IP 流量 (NFS、iSCSI 和 SMB 通訊協定)，提供用戶端與 ONTAP 檔案系統之間傳輸中的資料 end-to-end 加密功能。使用 IPsec 加密，您可以在設定啟用 IPsec 的 ONTAP SVM 的 FSx 和存取資料的連線用戶端上執行的 IPsec 用戶端之間建立 IPsec 通道。

當從不支援 Nitro 加密的用戶端存取您的資料時，建議您使用 IPsec 來加密透過 NFS、SMB 和 iSCSI 通訊協定傳輸中的資料，以及如果您的用戶端和 SVM 未加入作用中目錄 (Kerberos 型加密所需)。當 iSCSI 用戶端不支援以硝基為基礎的加密時，IPsec 加密是唯一可用來加密 iSCSI 流量傳輸中資料的選項。

對於 IPsec 驗證，您可以使用預先共用金鑰 (PSK) 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第 2 版 (IKEv2)。針對 ONTAP 和用戶端的 FSx 設定 IPsec 加密的高階步驟如下：

1. 在您的檔案系統上啟用和設定 IPsec。
2. 在您的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 的相關資訊，請參閱文件中心的透過線路加密設定 IP 安全性 (IPsec)。NetApp ONTAP

如需如何使用憑證設定 IPsec 的相關資訊，請參閱使用憑證驗證來設定 IPsec。

對傳輸中的資料啟用 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上所需的 SMB 加密，也可以啟用 SVM 上所有共用的 SVM 加密功能。

> **Note**
>
> 在 SVM 或共用上啟用需要 SMB 加密時，不支援加密的 SMB 用戶端將無法連線至該 SVM 或共用。

要求對 SVM 上的內送 SMB 流量進行 SMB 加密

使用下列程序來要求使用 NetApp ONTAP CLI 在 SVM 上進行 SMB 加密。

1. 若要使用 SSH 連線至 SVM 管理端點，請使用您在建立 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 位址或 DNS 名稱，從與檔案系統位於相同 VPC 中的用戶端以 SSH 方式存取 SVM。

   ```
   ssh vsadmin@svm-management-endpoint-ip-address
   ```

   具有範例值的指令：

   ```
   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 ONTAPCLI 命令對 SVM 的內送 SMB 流量要求 SMB 加密。

```
vserver cifs security modify -vserver vserver_name -is-smb-encryption-required true
```

3. 若要停止對內送 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 `vserver cifs security show`NetApp ONTAPCLI 命令：

```
vserver cifs security show -vserver vs1 -fields is-smb-encryption-required

vserver  is-smb-encryption-required
-------- -------------------------
vs1      true
```

如需有關在 SVM 上管理 SMB 加密的詳細資訊，請參閱NetApp ONTAP文件中心在 SMB 伺服器上設定所需的 SMB 加密，以便透過 SMB 進行資料傳輸。

啟用磁碟區上的 SMB 加密

使用下列程序來使用 NetApp ONTAP CLI 在共用上啟用 SMB 加密。

1. 如中使用 CLI 管理 SVM ONTAP所述，建立與 SVM 管理端點的安全殼層 (SSH) 連線。
2. 使用下列 NetApp ONTAP CLI 命令建立新的 SMB 共用，並在存取此共用時需要 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 NetApp ONTAP CLI 命令線上手冊`vserver cifs share create`中的。

3. 若要在現有的 SMB 共用上要求 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 NetApp ONTAP CLI 命令線上手冊`vserver cifs share create`中的。

4. 若要關閉現有 SMB 共用上的 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 NetApp ONTAP CLI 命令線上手冊vserver cifs share properties remove中的。

5. 若要查看 SMB 共用上的目前is-smb-encryption-required設定，請使用下列 NetApp ONTAP CLI 命令：

```
vserver cifs share properties show -vserver vserver_name -share-name share_name -
fields share-properties
```

如果命令傳回的屬性之一是屬性，則該屬性會指定存取此共用時必須使用 SMB 加密。encrypt-data

如需詳細資訊，請參閱 NetApp ONTAP CLI 命令線上手冊vserver cifs share properties show中的。

使用 PSK 驗證設定 IPsec

如果您使用 PSK 進行驗證，則在 ONTAP 和用戶端的 FSx 上設定 IPsec 加密的步驟如下：

1. 在您的檔案系統上啟用和設定 IPsec。
2. 在您的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，請參閱文件中心的透過線路加密設定 IP 安全性 (IPSec)。NetApp ONTAP

使用憑證驗證來設定 IPsec

下列主題提供在 ONTAP 檔案系統的 FSx 和執行利伯斯旺 IPsec 的用戶端上，使用憑證驗證來設定 IPsec 加密的指示。此解決方案使 AWS Private Certificate Authority 用 AWS Certificate Manager 和建立私有憑證授權單位以及產生憑證。

針對 ONTAP 檔案系統和連線的用戶端，使用 FSx 上的憑證驗證來設定 IPsec 加密的高階步驟如下：

1. 擁有憑證授權單位來發行憑證。
2. 產生並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. 在您的檔案系統上安裝憑證並設定 IPsec。
5. 定義安全性原則資料庫 (SPD)。
6. 為多個用戶端存取設定 IPsec。

建立和安裝 CA 憑證

對於憑證驗證，您需要從 FSx for ONTAP 檔案系統上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。下列範例會用 AWS Private Certificate Authority 來設定私有憑證授權單位，並產生要安裝在檔案系統和用戶端上的憑證。您可以使用 AWS Private Certificate Authority，建立完全 AWS 託管的根憑證授權單位和從屬憑證授權單位 (CA) 階層，供組織內部使用。這個過程有五個步驟：

1. 使用建立私有憑證授權單位 (CA) AWS Private CA
2. 在私有 CA 上發行並安裝根憑證
3. 要求您的檔案系統和 AWS Certificate Manager 用戶端的私人憑證
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 使用指南》中的私人 CA 管理。

若要建立根私有 CA

1. 建立 CA 時，您必須在提供的檔案中指定 CA 組態。以下命令使用 Nano 文本編輯器創建文`ca_config.txt`件，該文件指定了以下信息：

   - 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《使用指南》中的〈建立 CA 的程序 AWS Private Certificate Authority〉。

4. 使用建立憑證授權單位 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 資源名稱 (ARN)。

```
{
   "CertificateAuthorityArn": "arn:aws:acm-pca:aws-region:111122223333:certificate-
authority/12345678-1234-1234-1234-123456789012"
}
```

建立並安裝私有根 CA 的憑證 (AWS CLI)

1. 使用 get-certificate-authority-csr AWS CLI 命令產生憑證簽署要求 (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` (以 base64 格式編碼的 PEM 檔案) 具有下列外觀。

```
-----BEGIN CERTIFICATE-----
 MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
 VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
 b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
 BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
 MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
 VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
 b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
 YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
 21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
 rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
 Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
 nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
 FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
 NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
 -----END CERTIFICATE-----
```

如需詳細資訊，請參閱 AWS Private Certificate Authority 使用指南中的安裝根 CA 憑證。

2. 使用此issue-certificate AWS CLI 命令在您的私有 CA 上發行並安裝根憑證。

```
$ 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 指令下載根憑證。

```
$ 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 指令在您的私有 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
```

產生並匯出檔案系統與用戶端憑證

1. 使用指request-certificate AWS CLI 令要求 AWS Certificate Manager 憑證以在您的檔案系統和用戶端上使用。

```
$ 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
```

如果要求成功，則會傳回已發行憑證的 ARN。

2. 為了安全起見，您必須在匯出私密金鑰時指派密碼片語。建立密碼片語並將其儲存在名為的檔案中 `passphrase.txt`

3. 使用指export-certificate AWS CLI 令匯出先前發行的私人憑證。匯出的檔案包含憑證、憑證鏈結以及與憑證中內嵌之公開金鑰相關聯的加密私密 2048 位元 RSA 金鑰。為了安全起見，您必須在匯出私密金鑰時指派密碼片語。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 回應中擷取私密金鑰和憑證。

```
$ cat exported_cert.json | jq -r .PrivateKey > prv.key

cat exported_cert.json | jq -r .Certificate > cert.pem
```

```
openssl rsa -in prv.key -passin pass:$passphrase -out decrypted.key
```

5. 使用下列openssl命令解密 JSON 回應中的私密金鑰。輸入指令後，系統會提示您輸入密碼。

```
$ openssl rsa -in prv.key -passin pass:$passphrase -out decrypted.key
```

在 Amazon Linux 2 客戶端上安裝和配置利布斯旺 IPsec

以下各節提供在執行 Amazon Linux 2 的 Amazon EC2 執行個體上安裝和設定利伯斯旺 IPSec 的說明。

若要安裝和設定利用軟體

1. 使用安全殼層 Connect 至您的 EC2 執行個體。有關如何執行此操作的特定指示，請參閱 Amazon 彈性運算雲端使用者指南中的 Linux 執行個體使用者指南中的使用安全殼層用戶端 Connect 到 Linux 執行個體。
2. 執行下列命令來安裝libreswan：

```
$ sudo yum install libreswan
```

3. (選擇性) 在稍後的步驟中驗證 IPsec 時，可能會在沒有這些設定的情況下標記這些內容。我們建議您先在沒有這些設定的情況下測試設定。如果您的連線發生問題，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Libreswan您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複雜密碼。

```
$ 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：

```
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
    leftrsasigkey=%cert
    leftid=%fromcert
    rightid=%fromcert
    rightrsasigkey=%cert
```

您將在檔案系統上設定 IPsec 之後，在用戶端上啟動 IPsec。

在您的檔案系統上設定 IPsec

本節提供在適用於 ONTAP 檔案系統的 FSx 上安裝憑證，以及設定 IPsec 的指示。

在您的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。您將需要知道憑證的複雜密碼。
2. 若要存取 NetApp ONTAP CLI，請執行下列命令，在適用於 NetApp ONTAP 檔案系統的 Amazon FSx 管理連接埠上建立安全殼層工作階段。取代*`management_endpoint_ip`*為檔案系統管理連接埠的 IP 位址。

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

   如需詳細資訊，請參閱 使用 ONTAP CLI 管理檔案系統。
3. cat在用戶端 (不在您的檔案系統上) 上使用來列出`rootCA.pem`、`cert.pem`和檔`decrypted.key`案的內容，以便您可以複製每個檔案的輸出，並在下列步驟提示時貼上檔案。

   ```
   $ > cat cert.pem
   ```

   複製憑證內容。
4. 除非已經安裝，否則您必須將相互驗證期間使用的所有 CA 憑證 (包括 OnTAP 端和用戶端 CA) 安裝至ONTAP憑證管理 (如 ONTAP 自我簽署 Root-CA 的情況)。

   使用 `security certificate install` NetApp CLI 命令，如下所示安裝用戶端憑證：

   ```
   FSxID123:: > security certificate install -vserver dr -type client -cert-name
    ipsec-client-cert
   ```

```
Please enter Certificate: Press <Enter> when done
```

貼上您先前複製的cert.pem檔案內容，然後按 Enter 鍵。

```
Please enter Private Key: Press <Enter> when done
```

粘貼到decrypted.key文件的內容中，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 SVM 使用的憑證。此憑證的發行者 CA 必須已安裝ONTAP並新增至 IPsec。

   使用下列指令來安裝根憑證。

```
FSxID123:: > security certificate install -vserver dr -type server-ca -cert-name
 ipsec-ca-cert
```

```
Please enter Certificate: Press <Enter> when done
```

粘貼到rootCA.pem文件的內容中，然後按 Enter 鍵。

6. 若要確保安裝的 CA 在驗證期間位於 IPsec CA 搜尋路徑內，請使用「安全性 IPsec CA-ONTAP 憑證新增」命令，將憑證管理 CA 新增至 IPsec 模組。

   輸入下列指令以新增根憑證。

```
FSxID123:: > security ipsec ca-certificate add -vserver dr -ca-certs ipsec-ca-cert
```

7. 輸入下列命令，在安全性原則資料庫 (SPD) 中建立必要的 IPsec 原則。

```
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要確認之檔案系統的 IPsec 原則。

```
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 ONTAP 檔案系統和用戶端的 FSx 上設定，您可以在用戶端上啟動 IPsec。

1. 使用 SSH Connect 到您的用戶端系統。
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. 在您的 FSx 上顯示 ONTAP 檔案系統的加密連線，以確認 IPsec 設定。

```
FSxID123:: > security ipsec show-ikesa -node FsxId123
```

```
FsxId08ac16c7ec2781a58::> security ipsec show-ikesa -node FsxId08ac16c7ec2781a58-01
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ---------------- -----------
dr          policy-name
                   198.19.254.13   172.31.77.6     551c55de57fe8976 ESTABLISHED
fsx         policy-name
                   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，針對每個用戶端使用單一 SPD 項目就足夠了。不過，當數百或甚至數千個用戶端需要利用 IPsec 時，我們建議您使用 IPsec 多重用戶端設定。

適用於 ONTAP 的 FSx 支援在啟用 IPsec 的情況下，將多個網路中的多個用戶端連線到單一 SVM IP 位址。您可以使用`subnet`組態或組態來完成此操作，這些`Allow all clients`設定將在下列程序中說明：

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 原則項目連線到單一 SVM IP 位址，您必須指定在子網路中的格式。`remote-ip-subnets`此外，您必須指定具有正確客戶端身份的`remote-identity`字段。

> **Important**
>
> 使用憑證驗證時，每個用戶端都可以使用自己的唯一憑證或共用憑證進行驗證。適用於 ONTAP IPsec 的 FSx 會根據其本機信任存放區上安裝的 CA 來檢查憑證的有效性。適用於 ONTAP 的 FSx 也支援憑證撤銷清單 (CRL) 檢查。

1. 若要存取 NetApp ONTAP CLI，請執行下列命令，在適用於 NetApp ONTAP 檔案系統的 Amazon FSx 管理連接埠上建立安全殼層工作階段。取代*management_endpoint_ip*為檔案系統管理連接埠的 IP 位址。

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

   如需詳細資訊，請參閱 使用 ONTAP CLI 管理檔案系統。

2. 如下所示使用 `security ipsec policy create` NetApp ONTAP CLI 指令，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 (不論其來源 IP 位址為何) 連線至啟用 SVM IPsec 的 IP 位址，請在指定欄位時使用`0.0.0.0/0`萬用字元。`remote-ip-subnets`

此外，您必須指定具有正確客戶端身份的`remote-identity`字段。對於憑證驗證，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 NetApp ONTAP CLI，請執行下列命令，在適用於 NetApp ONTAP 檔案系統的 Amazon FSx 管理連接埠上建立安全殼層工作階段。取代*management_endpoint_ip*為檔案系統管理連接埠的 IP 位址。

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

   如需詳細資訊，請參閱 使用 ONTAP CLI 管理檔案系統。

2. 如下所示使用 `security ipsec policy create` NetApp ONTAP CLI 指令，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
```

適用於 ONTAP 的 Amazon FSx 的身分識別和存取管理 NetApp

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。AWS 服務 IAM 管理員控制哪些人可以通過身份驗證 (登入) 和授權 (具有許可) 來使用 Amazon FSx 資源。IAM 是您可以使用的 AWS 服務 ，無需額外付費。

主題

物件

您使用 AWS Identity and Access Management (IAM) 的方式會有所不同，具體取決於您在 Amazon FSx 中執行的工作。

服務使用者 — 如果您使用 Amazon FSx 服務執行工作，則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 功能完成工作時，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 中的某個功能，請參閱針對 NetApp ONTAP 身分識別和存取的 Amazon FSx 進行疑難排。

服務管理員 — 如果您負責公司的 Amazon FSx 資源，您可能擁有 Amazon FSx 的完整存取權。判斷服務使用者應存取哪些 Amazon FSx 功能和資源是您的工作。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將 IAM 與 Amazon FSx 搭配使用，請參閱適用於 NetApp ONTAP 的 Amazon FSx 如何與 IAM 搭配使用。

IAM 管理員 — 如果您是 IAM 管理員，您可能想要了解如何撰寫政策以管理 Amazon FSx 存取權的詳細資訊。若要檢視可在 IAM 中使用的 Amazon FSx 身分型政策範例，請參閱。適用於 ONTAP 的 Amazon FSx 的身分識別原則範例 NetApp

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以 IAM 使用者身分或假設 IAM 角色進行驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM 身分中心) 使用者、貴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識別的範例。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 AWS 用同盟存取時，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 AWS 帳戶的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以加密方式簽署您的要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南中的簽署 AWS API 請求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。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 使用者指南中的在 AWS中使用多重要素驗證 (MFA)。

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，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 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

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時登入資料進行存取 AWS 服務 。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步到自己身分識別來源中的一組使用者和群組，以便在所有應用

程式 AWS 帳戶 和應用程式中使用。如需 IAM Identity Center 的相關資訊，請參閱 AWS IAM Identity Center 使用者指南中的什麼是 IAM Identity Center？。

IAM 使用者和群組

IAM 使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，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，但角色僅提供暫時憑證。如需進一步了解，請參閱 IAM 使用者指南中的建立 IAM 使用者 (而非角色) 的時機。

IAM 角色

IAM 角色是您 AWS 帳戶 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以切換角色，在中暫時擔任 IAM 角色。 AWS Management Console 您可以透過呼叫 AWS CLI 或 AWS API 作業或使用自訂 URL 來擔任角色。如需使用角色的方法更多相關資訊，請參閱 IAM 使用者指南中的使用 IAM 角色。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 – 若要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 (信任的委託人) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要了解跨帳戶存取權角色和資源型政策間的差異，請參閱 IAM 使用者指南中的 IAM 角色與資源類型政策的差異。

- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。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。
  - 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 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。如需更多資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但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 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。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 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需更多資訊，請參閱 IAM 使用者指南中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

若要了解是否要使用 IAM 角色或 IAM 使用者，請參閱 IAM 使用者指南中的建立 IAM 角色 (而非使用者) 的時機。

使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以 JSON 文件的形式儲存在中。如需 JSON 政策文件結構和內容的更多相關資訊，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哪些內容。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。具有該原則的使用者可以從 AWS Management Console AWS CLI、或 AWS API 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。若要了解如何建立身分類型政策，請參閱 IAM 使用者指南中的建立 IAM 政策。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。若要了解如何在受管政策及內嵌政策間選擇，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。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 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 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些委託人 (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 和 Amazon VPC 是支援 ACL 的服務範例。 AWS WAF若要進一步了解 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原則類型。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。如需許可範圍的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 實體許可範圍。

- 服務控制策略（SCP）— SCP 是 JSON 策略，用於指定中組織或組織單位（OU）的最大權限。AWS Organizations AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。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 限制成員帳戶中實體的權限，包括每個 AWS 帳戶根使用者帳戶。如需組織和 SCP 的更多相關資訊，請參閱 AWS Organizations 使用者指南中的 SCP 運作方式。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需更多資訊，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。要了解如何在涉及多個政策類型時 AWS 確定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

適用於 NetApp ONTAP 的 Amazon FSx 如何與 IAM 搭配使用

在您使用 IAM 管理 Amazon FSx 的存取權限之前，請先了解哪些 IAM 功能可用於 Amazon FSx。

您可以搭配 Amazon FSx 使用的 NetApp IAM 功能

IAM 功能	Amazon FSx 支持
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵	是
ACL	否

IAM 功能	Amazon FSx 支持
ABAC (政策中的標籤)	是
臨時憑證	是
轉送存取工作階段 (FAS)	是
服務角色	否
服務連結角色	是

若要深入瞭解 Amazon FSx 和其他 AWS 服務如何搭配大多數 IAM 功能搭配使用，請參閱 IAM 使用者指南中的搭配 IAM 使用的AWS 服務。

Amazon FSx 的基於身份識別的政策

支援身分型政策	是

身分型政策是可以連接到身分 (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。若要了解如何建立身分類型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

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 的基於身份的政策示例

若要檢視 Amazon FSx 身分識別型政策的範例，請參閱。適用於 ONTAP 的 Amazon FSx 的身分識別原則範例 NetApp

Amazon FSx 中以資源為基礎的政策

支援以資源基礎的政策	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哪些內容。也就是說，哪個主體在什麼条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。原則動作通常與關聯的 AWS API 作業具有相同的名稱。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 動作清單，請參閱服務授權參考資料中由 Amazon FSx 定義的動作。

Amazon FSx 中的政策動作會在動作前使用下列前置詞：

```
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 身分識別型政策的範例，請參閱。適用於 ONTAP 的 Amazon FSx 的身分識別原則範例 NetApp

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哪些內容。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 ARN 的清單，請參閱服務授權參考資料中的 Amazon FSx 定義的資源。若要了解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 身分識別型政策的範例，請參閱。適用於 ONTAP 的 Amazon FSx 的身分識別原則範例 NetApp

Amazon FSx 的政策條件金鑰

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哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，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條件金鑰。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

若要查看 Amazon FSx 條件金鑰清單，請參閱服務授權參考資料中的 Amazon FSx 的條件金鑰。若要了解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 身分識別型政策的範例，請參閱。適用於 ONTAP 的 Amazon FSx 的身分識別原則範例 NetApp

Amazon FSx 中的訪問控制列表（ACL）

支援 ACL	否

以屬性為基礎的存取控制 (ABAC) 搭配 Amazon FSx

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。在中 AWS，這些屬性稱為標籤。您可以將標籤附加到 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。

若要根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件金鑰，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》中的什麼是 ABAC?。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，請參閱標記您的 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。

使用臨時登入資料搭配 Amazon FSx

支援臨時憑證	是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配AWS 服務 使用，請參閱 IAM 使用者指南中的 IAM。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立暫時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱《IAM 使用者指南》中的切換至角色 (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。

Amazon FSx 的轉發存取工作階段

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，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 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

適用於 Amazon FSx 的服務連結角色

支援服務連結角色	是

服務連結角色是一種連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但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

適用於 ONTAP 的 Amazon FSx 的身分識別原則範例 NetApp

依預設，使用者和角色沒有建立或修改 Amazon FSx 資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。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。

若要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。

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 ARN 格式，請參閱服務授權參考中的 Amazon FSx 的動作、資源和條件金鑰。

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

以身分識別為基礎的政策可決定使用者是否可以在您的帳戶中建立、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 受管原則並邁向最低權限權限 — 若要開始將權限授與使用者和工作負載，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。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。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。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。您也可以使用條件來授與服務動作的存取權 (如透過特 AWS 服務定的方式使用) AWS CloudFormation。如需更多資訊，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，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。

- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫 API 作業時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 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

若要存取適用於 NetApp ONTAP 的 Amazon FSx 主控台，您必須擁有最少一組許可。這些許可必須允許您 AWS 帳戶列出和檢視有關. 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。

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。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。

為確保使用者和角色仍可使用 Amazon FSx 主控台，請同時將AmazonFSxConsoleReadOnlyAccess AWS 受管政策附加到實體。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AWS Amazon FSx 的受管政策中查看AmazonFSxConsoleReadOnlyAccess和其他 Amazon FSx 受管服務政策。

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。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

```
{
    "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": "*"
        }
    ]
}
```

針對 NetApp ONTAP 身分識別和存取的 Amazon FSx 進行疑難排

使用下列資訊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

- 我沒有授權在 Amazon FSx 中執行操作
- 我沒有授權執行 iam：PassRole
- 我想允許我以外的人訪 AWS 帳戶 問我的 Amazon FSx 資源

我沒有授權在 Amazon FSx 中執行操作

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 系統管理員。您的管理員提供您的簽署憑證。

我沒有授權執行 iam：PassRole

如果您收到未獲授權執行`iam:PassRole`動作的錯誤訊息，則必須更新您的政策以允許您將角色傳遞給 Amazon FSx。

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

當名為的 IAM 使用者`marymajor`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 系統管理員。您的管理員提供您的簽署憑證。

我想允許我以外的人訪 AWS 帳戶 問我的 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，請參閱適用於 NetApp ONTAP 的 Amazon FSx 如何與 IAM 搭配使用。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱《IAM 使用者指南》中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限。
- 若要了解如何向第三方提供對資源的存取權 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。
- 若要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)。
- 若要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 角色與資源型政策的差異。

使用標籤與 Amazon FSx

您可以使用標籤來控制對 Amazon FSx 資源的存取，以及實作以屬性為基礎的存取控制 (ABAC)。若要在建立期間將標籤套用至 Amazon FSx 資源，使用者必須擁有特定 AWS Identity and Access Management (IAM) 許可。

在建立期間授予標籤資源的許可

透過某些資源建立 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以屬性為基礎的存取控制 (ABAC)。如需詳細資訊，請參閱 ABAC 的用途為 AWS何？ 在 IAM 使用者指南中。

若要讓使用者在建立時標記資源，他們必須具有使用建立資源之動作的權限`fsx:CreateFileSystem`，例如`fsx:CreateStorageVirtualMachine`、或`fsx:CreateVolume`。如果在資源建立動作中指定了標籤，IAM 會對動作執行其他授權，以驗證使用者是否具有建立標籤的權限。`fsx:TagResource`因此，使用者必須同時具備使用 `fsx:TagResource` 動作的明確許可。

下列範例原則可讓使用者建立檔案系統和儲存區虛擬機器 (SVM)，並在特定 AWS 帳戶建立期間對其套用標籤。

```
{
  "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，下列原則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記套用至備份。

```
{
```

```
  "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，具有建立資源權限的使用者 (假設沒有標記條件)，如果要求中未指定標籤，則不需要使用`fsx:TagResource`動作的權限。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，請參閱標記您的 Amazon FSx 資源。如需使用標籤來控制 Amazon FSx 資源存取權的詳細資訊，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 資源和動作的存取權限，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。

如需如何使用標籤來控制 AWS 資源存取權的詳細資訊，請參閱 IAM 使用者指南中的使用標籤控制存取。如需有關在建立時標記 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 標記您的 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在 Amazon FSx 資源上執行哪些動作，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 範例原則 — 僅在使用特定標籤時建立檔案系統

這個原則允許使用者建立檔案系統，只有在使用特定的標籤索引鍵值組來標記檔案系統時，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 — 僅針對具有特定標籤的 NetApp ONTAP 磁碟區建立 Amazon FSx 的備份

此原則允許使用者僅針對以鍵值配對標記的 ONTAP 磁碟區建立 FSx 的備份。key=Department value=Finance備份是使用標籤創建的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 範例原則 — 使用特定標籤從備份建立具有特定標籤的磁碟區

此原則允許使用者建立Department=Finance僅從標記為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 範例原則 — 刪除具有特定標籤的檔案系統

此原則允許使用者僅刪除標記為的檔案系統Department=Finance。如果他們創建了最終備份，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 範例原則 — 刪除具有特定標記的磁碟區

此原則允許使用者僅刪除標記為的磁碟區Department=Finance。如果他們創建了最終備份，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"
                }
            }
        }
    ]
}
```

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。Amazon FSx 預先定義服務連結角色，並包含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輕鬆設定 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。這樣可以保護您的 Amazon FSx 資源，因為您無法意外移除存取資源的權限。

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。

適用於 Amazon FSx 的服務連結角色許可

Amazon FSx 使用名為的服務連結角色 AWSServiceRoleForAmazonFSx— 該角色會在您的帳戶中執行某些動作，例如為 VPC 中的檔案系統建立彈性網路界面，以及在中發佈檔案系統和磁碟區指標。CloudWatch

如需此政策的更新，請參閱 亞馬遜 SxService RolePolicy

許可詳細資訊

許可詳細資訊

AWSServiceRoleForAmazonFSx 角色權限由 AmazonF SxService RolePolicy AWS 管理策略定義。具 AWSServiceRoleForAmazonFSx 有以下權限：

> **Note**
>
> 所有 Amazon FSx 檔案系統類型都會使用 AWSServiceRoleForAmazonFSx 此功能；某些列出的許可不適用於適用於 ONTAP 的 FSx。

- ds— 允許 Amazon FSx 檢視、授權和取消授權目錄中的應用程式 AWS Directory Service 。
- ec2— 允許 Amazon FSx 執行以下操作：
  - 檢視、建立和取消與 Amazon FSx 檔案系統相關聯的網路界面的關聯。

  - 檢視與 Amazon FSx 檔案系統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 VPC、安全群組和子網路。
  - 為可與 VPC 搭配使用的所有安全群組提供增強的安全群組驗證。
  - 建立 AWS授權使用者在網路介面上執行特定作業的權限。
- `cloudwatch`— 允許 Amazon FSx 將指標資料點發佈到 AWS/FSx 命名空間 CloudWatch 下方。
- `route53`— 允許 Amazon FSx 將 Amazon VPC 與私有託管區域相關聯。
- `logs`— 允許 Amazon FSx 描述和寫入 CloudWatch 日誌串流。這樣使用者可以將 FSx 適用於 Windows 檔案伺服器檔案系統的檔案存取稽核記錄傳送至 CloudWatch 記錄資料流。
- `firehose`— 允許 Amazon FSx 描述和寫入 Amazon 數據 Firehose 交付流。這樣使用者就可以將 Amazon FSx 適用於 Windows 檔案伺服器檔案系統的檔案存取稽核日誌發佈到 Amazon 資料 Firehose 交付串流。

```
{
    "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"
                }
            }
        },
        {
            "Sid": "PutCloudWatchLogs",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
        },
        {
            "Sid": "ManageAuditLogs",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
        }
    ]
```

```
}
```

對此政策的任何更新將在中進行說明Amazon FSx 更新 AWS 受管政策。

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 IAM CLI 或 IAM API 中 AWS Management Console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 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。

支援 Amazon FSx 服務連結角色的區域

Amazon FSx 支援在提供服務的所有區域使用服務連結角色。如需詳細資訊，請參閱 AWS 區域與端點。

AWS Amazon FSx 的受管政策

受 AWS 管理的策略是由建立和管理的獨立策略 AWS。 AWS 受管理的策略旨在為許多常見使用案例提供權限，以便您可以開始將權限指派給使用者、群組和角色。

請記住， AWS 受管理的政策可能不會為您的特定使用案例授與最低權限權限，因為這些權限可供所有 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。

您無法變更受 AWS 管理策略中定義的權限。如果 AWS 更新 AWS 受管理原則中定義的權限，則此更新會影響附加原則的所有主體識別 (使用者、群組和角色)。 AWS 當新的啟動或新 AWS 服務 的 API 操作可用於現有服務時，最有可能更新 AWS 受管理策略。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

亞馬遜 SxService RolePolicy

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 管理策略：亞馬遜 SxDelete ServiceLinked RoleAccess

您不得將 `AmazonFSxDeleteServiceLinkedRoleAccess` 連接到 IAM 實體。此原則會連結至服務，且只能與該服務的服務連結角色搭配使用。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，這些許可允許 Amazon FSx 刪除其用於 Amazon S3 存取的服務連結角色，這些角色僅供 Amazon FSx 用於 Lustre。

許可詳細資訊

此政策包含中`iam`允許 Amazon FSx 檢視、刪除和檢視 Amazon S3 存取 FSx 服務連結角色的刪除狀態的許可。

若要檢視此政策的權限，請參閱《 AWS 受管策略參考指南》SxDeleteServiceLinkedRoleAccess中的AmazonF。

AWS 管理策略：亞馬遜訪SxFull問

您可以將亞馬遜 F 附加SxFullAccess 到您的 IAM 實體。Amazon FSx 也會將此政策附加到可讓 Amazon FSx 代表您執行動作的服務角色。

提供對 Amazon FSx 的完整存取權以及相關 AWS 服務的存取權。

許可詳細資訊

此政策包含以下許可。

- `fsx`— 允許主體完整存取權以執行除外的所有 Amazon FSx 動作。`BypassSnaplockEnterpriseRetention`
- `ds`— 允許主參與者檢視 AWS Directory Service 目錄的相關資訊。
- `ec2`
  - 允許主參與者在指定條件下建立標籤。
  - 為可與 VPC 搭配使用的所有安全群組提供增強的安全群組驗證。
- `iam`— 允許代表使用者建立 Amazon FSx 服務連結角色的原則。這是必要的，以便 Amazon FSx 可以代表使用者管理 AWS 資源。
- `logs`— 可讓主參與者建立記錄群組、記錄串流，以及將事件寫入記錄串流。這是必要的，以便使用者可以透過將稽核存取記錄傳送至記 CloudWatch 錄來監視 FSx 的 Windows 檔案伺服器檔案系統存取。
- `firehose`— 允許校長將記錄寫入 Amazon 資料 Firehose。這是必要的，以便使用者可以透過將稽核存取記錄傳送至 Firehose 來監控 FSx 的 Windows 檔案伺服器檔案系統存取。

若要檢視此政策的權限，請參閱《 AWS 受管策略參考指南》中的 AmazonF SxFull 存取。

AWS 管理策略：亞馬遜 SxConsole FullAccess

您可將 `AmazonFSxConsoleFullAccess` 政策連接到 IAM 身分。

此政策授予管理許可，允許完整存取 Amazon FSx 並 AWS 透過 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，但不包括。`BypassSnaplockEnterpriseRetention`
- `cloudwatch`— 允許主體在 Amazon FSx 管理主控台中檢視 CloudWatch 警示和指標。
- `ds`— 允許主參與者列出 AWS Directory Service 目錄的相關資訊。
- `ec2`
  - 允許主體在路由表上建立標籤、列出網路界面、路由表、安全群組、子網路以及與 Amazon FSx 檔案系統關聯的 VPC。
  - 允許主參與者針對可與 VPC 搭配使用的所有安全性群組提供增強的安全性群組驗證。
- `kms`— 允許主參與者列出 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所有物件 (最多 1000 個)。
- `iam`— 授予建立服務連結角色的權限，以允許 Amazon FSx 代表使用者執行動作。

若要檢視此政策的權限，請參閱《 AWS 受管理策略參考指南》SxConsoleFullAccess中的AmazonF。

AWS 管理策略：亞馬遜訪SxConsoleReadOnly問

您可將 `AmazonFSxConsoleReadOnlyAccess` 政策連接到 IAM 身分。

此政策授予 Amazon FSx 和相關 AWS 服務的唯讀許可，以便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 管理主控台中檢視有關 Amazon FSx 檔案系統的資訊，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 管理主控台中檢視與 Amazon FSx 檔案系統相關聯的網路界面、安全群組、子網路以及 VPC 擬私人雲端。
  - 為可與 VPC 搭配使用的所有安全群組提供增強的安全群組驗證。

- 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— 允許主體描述與提出請求的帳戶相關聯的 Amazon CloudWatch 日誌日誌群組。這是必要的，主體才能檢視 Windows 檔案伺服器檔案系統 FSx 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 資料 Firehose 交付串流。這是必要的，主體才能檢視 Windows 檔案伺服器檔案系統 FSx 的現有檔案存取稽核組態。

若要檢視此政策的權限，請參閱《 AWS 受管策略參考指南》中的 AmazonF SxConsole ReadOnly 存取。

AWS 管理策略：亞馬遜 SxRead OnlyAccess

您可將 AmazonFSxReadOnlyAccess 政策連接到 IAM 身分。

此政策包含以下許可。

- fsx— 允許主體在 Amazon FSx 管理主控台中檢視有關 Amazon FSx 檔案系統的資訊，包括所有標籤。
- ec2— 為可與 VPC 搭配使用的所有安全群組提供增強的安全群組驗證。

若要檢視此政策的權限，請參閱《 AWS 受管理策略參考指南》SxReadOnlyAccess中的 AmazonF。

Amazon FSx 更新 AWS 受管政策

檢視 Amazon FSx AWS 受管政策更新的詳細資訊，因為此服務開始追蹤這些變更。如需有關此頁面變更的自動警示，請訂閱 Amazon FSx 適用於 ONTAP 的 Amazon FSx 的文件歷史記錄 NetApp 頁面上的 RSS 摘要。

變更	描述	日期
亞馬遜 SxService RolePolicy- 更新到現有政策	Amazon FSx 新增了新權限，允ec2:GetSecurityGroupsForVpc 許主體對可搭配 VPC 使用的所有安全群組提供增強的安全群組驗證。	2024 年 1 月 9 日
亞馬遜 SxRead OnlyAccess- 更新到現有政策	Amazon FSx 新增了新權限，允ec2:GetSecurityGro	2024 年 1 月 9 日

變更	描述	日期
	upsForVpc 許主體對可搭配 VPC 使用的所有安全群組提供增強的安全群組驗證。	
亞馬遜SxConsoleReadOnly訪問-更新到現有策略	Amazon FSx 新增了新權限，允ec2:GetSecurityGroupsForVpc 許主體對可搭配 VPC 使用的所有安全群組提供增強的安全群組驗證。	2024 年 1 月 9 日
亞馬遜SxFull訪問-更新到現有策略	Amazon FSx 新增了新權限，允ec2:GetSecurityGroupsForVpc 許主體對可搭配 VPC 使用的所有安全群組提供增強的安全群組驗證。	2024 年 1 月 9 日
亞馬遜 SxConsole FullAccess-更新到現有政策	Amazon FSx 新增了新權限，允ec2:GetSecurityGroupsForVpc 許主體對可搭配 VPC 使用的所有安全群組提供增強的安全群組驗證。	2024 年 1 月 9 日
亞馬遜SxFull訪問-更新到現有策略	Amazon FSx 新增了新的權限，讓使用者能夠針對 OpenZFS 檔案系統的 FSx 執行跨區域和跨帳戶資料複寫。	2023 年 12 月 20 日
亞馬遜 SxConsole FullAccess-更新到現有政策	Amazon FSx 新增了新的權限，讓使用者能夠針對 OpenZFS 檔案系統的 FSx 執行跨區域和跨帳戶資料複寫。	2023 年 12 月 20 日
亞馬遜SxFull訪問-更新到現有策略	Amazon FSx 新增了新的權限，讓使用者能夠針對 OpenZFS 檔案系統的 FSx 執行隨選磁碟區複寫。	2023 年 11 月 26 日

變更	描述	日期
亞馬遜 SxConsole FullAccess-更新到現有政策	Amazon FSx 新增了新的權限，讓使用者能夠針對 OpenZFS 檔案系統的 FSx 執行隨選磁碟區複寫。	2023 年 11 月 26 日
亞馬遜SxFull訪問-更新到現有策略	Amazon FSx 新增了新的許可，讓使用者能夠檢視、啟用和停用針對 ONTAP 異地同步備份檔案系統 FSx 的共用 VPC 支援。	2023 年 11 月 14 日
亞馬遜 SxConsole FullAccess-更新到現有政策	Amazon FSx 新增了新的許可，讓使用者能夠檢視、啟用和停用針對 ONTAP 異地同步備份檔案系統 FSx 的共用 VPC 支援。	2023 年 11 月 14 日
亞馬遜SxFull訪問-更新到現有策略	Amazon FSx 增加了新的許可，以允許 Amazon FSx 管理適用於 OpenZFS 異地同步備份檔案系統的 FSx 網路組態。	2023 年 8 月 9 日
AWS 管理策略：AmazonFSxService RolePolicy-更新到現有策略	Amazon FSx 修改了現有的`cloudwatch:PutMetricData` 許可，以便 Amazon FSx 將 CloudWatch 指標發佈到命名空間。`AWS/FSx`	2023 年 7 月 24 日
亞馬遜SxFull訪問-更新到現有策略	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
亞馬遜 SxConsole FullAccess-更新到現有政策	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

變更	描述	日期
亞馬遜SxConsoleReadOnly訪問-更新到現有策略	Amazon FSx 新增了新的許可，讓使用者能夠在 Amazon FSx 主控台中檢視 Windows 檔案伺服器檔案系統 FSx 的增強效能指標和建議的動作。	2022 年 9 月 21 日
亞馬遜 SxConsole FullAccess-更新到現有政策	Amazon FSx 新增了新的許可，讓使用者能夠在 Amazon FSx 主控台中檢視 Windows 檔案伺服器檔案系統 FSx 的增強效能指標和建議的動作。	2022 年 9 月 21 日
亞馬遜 SxRead OnlyAccess-開始跟踪政策	此政策授予對所有 Amazon FSx 資源及其相關聯標籤的唯讀存取權。	2022 年 2 月 4 日
亞馬遜 SxDelete ServiceLinked RoleAccess-開始跟踪政策	此政策授予管理許可，這些許可允許 Amazon FSx 刪除其適用於 Amazon S3 存取的服務連結角色。	2022 年 1 月 7 日
亞馬遜 SxService RolePolicy-更新到現有政策	Amazon FSx 添加了新的許可，以允許 Amazon FSx 管理 NetApp ONTAP 文件系統的 Amazon FSx 的網絡配置。	2021 年 9 月 2 日
亞馬遜SxFull訪問-更新到現有策略	Amazon FSx 添加了新的許可，以允許 Amazon FSx 在 EC2 路由表上創建標籤以用於範圍關閉調用。	2021 年 9 月 2 日
亞馬遜 SxConsole FullAccess-更新到現有政策	Amazon FSx 添加了新的許可，以允許 Amazon FSx 為 NetApp ONTAP 異地同步備份文件系統創建 Amazon FSx。	2021 年 9 月 2 日

變更	描述	日期
亞馬遜 SxConsole FullAccess-更新到現有政策	Amazon FSx 添加了新的許可，以允許 Amazon FSx 在 EC2 路由表上創建標籤以用於範圍關閉調用。	2021 年 9 月 2 日
亞馬遜 SxService RolePolicy-更新到現有政策	Amazon FSx 添加了新的許可，以允許 Amazon FSx 描述和寫入日誌流 CloudWatch 日誌流。 這是必要的，以便使用者可以使用記錄檢視 Windows 檔案伺服器檔案系統 FSx 的檔案存取稽核記 CloudWatch 錄。	2021 年 6 月 8 日
亞馬遜 SxService RolePolicy-更新到現有政策	Amazon FSx 添加了新的許可，以允許 Amazon FSx 描述和寫入 Amazon 數據 Firehose 交付流。 這是必要的，以便使用者可以使用 Amazon 資料 Firehose 檢視 FSx 適用於 Windows 檔案伺服器檔案系統的檔案存取稽核日誌。	2021 年 6 月 8 日
亞馬遜SxFull訪問-更新到現有策略	Amazon FSx 新增了新許可，允許主體描述和建立 CloudWatch 日誌日誌群組、日誌串流，以及將事件寫入日誌串流。 這是必要的，主體才能使 CloudWatch 用記錄來檢視 Windows 檔案伺服器檔案系統 FSx 的檔案存取稽核記錄。	2021 年 6 月 8 日

變更	描述	日期
亞馬遜SxFull訪問-更新到現有策略	Amazon FSx 添加了新的許可，允許校長描述和寫入記錄到 Amazon 數據 Firehose。 這是必要的，以便使用者可以使用 Amazon 資料 Firehose 檢視 FSx 適用於 Windows 檔案伺服器檔案系統的檔案存取稽核日誌。	2021 年 6 月 8 日
亞馬遜 SxConsole FullAccess-更新到現有政策	Amazon FSx 新增了新許可，允許主體描述與提出請求的帳戶相關聯的 Amazon CloudWatch 日誌日誌群組。 這是必要的，這樣主體才能在設定 Windows 檔案伺服器檔案系統的 FSx 檔案存取稽核時，選擇現有的 CloudWatch 記錄檔記錄群組。	2021 年 6 月 8 日
亞馬遜 SxConsole FullAccess-更新到現有政策	Amazon FSx 新增了新的許可，允許校長描述與提出請求的帳戶相關聯的 Amazon 資料 Firehose 交付串流。 這是必要的，以便主體在為 Windows 檔案伺服器檔案系統設定檔案存取稽核時，可以選擇現有的 Firehose 傳遞串流。	2021 年 6 月 8 日

變更	描述	日期
亞馬遜SxConsoleReadOnly訪問-更新到現有策略	Amazon FSx 新增了新許可，允許主體描述與提出請求的帳戶相關聯的 Amazon CloudWatch 日誌日誌群組。 這是必要的，主體才能檢視 Windows 檔案伺服器檔案系統 FSx 的現有檔案存取稽核組態。	2021 年 6 月 8 日
亞馬遜SxConsoleReadOnly訪問-更新到現有策略	Amazon FSx 新增了新的許可，允許校長描述與提出請求的帳戶相關聯的 Amazon 資料 Firehose 交付串流。 這是必要的，主體才能檢視 Windows 檔案伺服器檔案系統 FSx 的現有檔案存取稽核組態。	2021 年 6 月 8 日
Amazon FSx 開始跟踪更改	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 進行檔案系統存取控制

您可以使用其中一個端點的 DNS 名稱或 IP 位址來存取適用於 NetApp ONTAP 檔案系統和 SVM 的 Amazon FSx，視其存取類型而定。DNS 名稱會對應至 VPC 中檔案系統或 SVM elastic network interface 的私有 IP 位址。只有相關 VPC 中的資源，或與相關 VPC AWS Direct Connect 或 VPN 連接的資源，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，請參閱什麼是 Amazon VPC？ 在 Amazon VPC 用戶指南中。

> **Warning**
>
> 您不得修改或刪除與檔案系統相關聯的 elastic network interface。修改或刪除網路介面可能會導致 VPC 與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 ONTAP 檔案系統 FSx 的虛擬防火牆，以控制傳入和傳出流量。輸入規則會控制檔案系統的傳入流量，輸出規則則會控制來自檔案系統的傳出流量。建立檔案系統時，您可以指定建立該檔案系統的 VPC，並套用該 VPC 的預設安全性群組。您可以將規則新增至每個安全性群組，以允許進出其關聯檔案系統和 SVM 的流量。您可隨時修改安全群組規則。新規則和修改過的規則會自動套用至與安全性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中的所有規則。

若要使用安全群組控制對 Amazon FSx 檔案系統的存取，請新增輸入和輸出規則。輸入規則可控制傳入流量，而輸出規則則會控制來自檔案系統的傳出流量。確保安全群組中有正確的網路流量規則，以將 Amazon FSx 檔案系統的檔案共用對應到受支援運算執行個體上的資料夾。

如需有關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。

建立 VPC 安全群組

若要為 Amazon FSx 建立安全群組

1. 在以下位置打開 Amazon EC2 控制台 https://console.aws.amazon.com/ec2。
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. 對於 VPC，請選擇與檔案系統關聯的 Amazon VPC，以在該 VPC 內建立安全群組。
6. 對於輸出規則，允許所有通訊埠上的所有流量。
7. 將下列規則新增至安全性群組的輸入連接埠。在來源欄位中，您應該選擇 [自訂]，然後輸入與需要存取您的 FSx for ONTAP 檔案系統的執行個體相關聯的安全群組或 IP 位址範圍，包括：

   - 透過 NFS、中小企業或 iSCSI 存取檔案系統中資料的 Linux、視窗及/或 macOS 用戶端。
   - 將對等至檔案系統的任何ONTAP 檔案系統/集 (例如，要使用 SnapMirror SnapVault、或)。FlexCache
   - 您將用來存取 ONTAP REST API、CLI 或 ZAPI 的任何用戶端 (例如，擷取/Grafana 執行個體、連接器或 BlueExp)。 NetApp NetApp

通訊協定	連接埠	角色
所有 ICMP	全部	偵測執行個體
SSH	22	透過 SSH 存取叢集管理 LIF 或節點管理 LIF 的 IP 位址
TCP	111	遠端程序呼叫 NFS
TCP	135	CIFS 的遠端程序呼叫
TCP	139	CIFS 的 NetBIOS 服務工作階段
TCP	161-162	簡易網路管理通訊協定 (SNMP)
TCP	443	對叢集管理 LIF 或 SVM 管理 LIF 的 IP 位址的 ONTAP REST API 存取
TCP	445	Microsoft 中小型企業通過 TCP 與 NetBIOS 框架
TCP	635	NFS 掛載
TCP	749	Kerberos
TCP	2049	NFS 伺服器精靈
TCP	3260	透過 iSCSI 資料 LIF 存取
TCP	4045	NFS 鎖定常駐程式
TCP	4046	NFS 的網路狀態監視器
TCP	10000	網路資料管理通訊協定 (NDMP) 與叢 NetApp SnapMirror 集間通訊
TCP	11104	NetApp SnapMirror 集群間通信的管理
TCP	11105	SnapMirror 使用叢集間 LIF 進行資料傳輸
UDP	111	遠端程序呼叫 NFS

通訊協定	連接埠	角色
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 伺服器精靈
UDP	4045	NFS 鎖定常駐程式
UDP	4046	NFS 的網路狀態監視器
UDP	4049	NFS 配額通訊協定

8. 將安全性群組新增至檔案系統的 elastic network interface。

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的網路，您可以移除與檔案系統 elastic network interface 相關聯的所有安全性群組，並將其取代為沒有入站/輸出規則的群組。

適用於 ONTAP 的 Amazon FSx 合規驗證 NetApp

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。

- 在 Amazon Web Services 上架構 HIPAA 安全性與合規性 — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 用程式。

> **Note**
>
> 並非所有人 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國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)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 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 controls reference。
- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您滿足特定合規性架構所要求的入侵偵測需求，如 PCI DSS 等各種合規性需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

適用於 NetApp ONTAP 的 Amazon FSx 和 VPC 端點介面 ()AWS PrivateLink

您可以將 Amazon FSx 設定為使用介面 VPC 人雲端端點，以改善 VPC 的安全狀態。介面 VPC 私人雲端端點採用這項技術 AWS PrivateLink，可讓您在沒有網際網路閘道、NAT 裝置、VPN 連線或 AWS Direct Connect 連線的情況下私有存取 Amazon FSx API。VPC 中的執行個體不需要公有 IP 地址即可與 Amazon FSx API 進行通訊。您的 VPC 和 Amazon FSx 之間的流量不會離開網路。 AWS

每個介面 VPC 端點都由子網路中的一或多個彈性網路介面表示。網路介面提供私有 IP 位址，可做為 Amazon FSx API 流量的進入點。

Amazon FSx 界面虛擬私人雲端端點的考量事

在為 Amazon FSx 設定介面虛擬私人雲端端點之前，請務必檢閱 Amazon VPC 使用者指南中的介面虛擬私人雲端端點屬性和限制。

您可以從 VPC 擬私人雲端呼叫任何 Amazon FSx API 作業。例如，您可以從 VPC 中呼叫 CreateFileSystem API，為 ONTAP 檔案系統建立 FSx。如需 Amazon FSx API 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 VPC 對等將其他 VPC 連線至具有介面 VPC 端點的 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 VPC 對等連線，或在另一個 VPC 中建立 VPC 對等連線。 AWS 帳戶 VPC 也可以有兩種不同 AWS 區域。

對等 VPC 之間的流量會保留在 AWS 網路上，且不會穿越公用網際網路。對等 VPC 之後，兩個 VPC 中的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體等資源都可以透過在其中一個 VPC 中建立的介面 VPC 端點存取 Amazon FSx API。

為 Amazon FSx API 創建一個接口 VPC 人雲端端點

您可以使用 Amazon 虛擬私人雲端主控台或 () 為 Amazon FSx API 建立 VPC 端點。 AWS Command Line Interface AWS CLI如需詳細資訊，請參閱 Amazon VPC 使用者指南中的建立介面虛擬私人雲端端點。

若要為 Amazon FSx 建立介面 VPC 人雲端端點，請使用下列其中一個方法：

- **com.amazonaws.*region*.fsx**— 為 Amazon FSx API 操作建立端點。
- **com.amazonaws.*region*.fsx-fips**— 為符合聯邦資訊處理標準 (FIPS) 140-2 的 Amazon FSx API 建立端點。

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。

例如， AWS 區域 在中國除外，如果您為端點啟用私有 DNS，則可以使用 VPC 端點的預設 DNS 名稱向 Amazon FSx 發出 API 請求。 AWS 區域`fsx.us-east-1.amazonaws.com`對於中國（北京）和中國（寧夏） AWS 區域，您可以分別使`fsx-api.cn-north-1.amazonaws.com.cn`用 and 向 VPC 端點發出 API 請求。`fsx-api.cn-northwest-1.amazonaws.com.cn`

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) 政策附加到 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。

適用於 ONTAP 的 Amazon FSx 的 NetApp 彈性

AWS 全球基礎架構是圍繞 AWS 區域 和可用區域建立的。 AWS 區域 提供多個實體分離和隔離的可用區域，這些區域與低延遲、高輸送量和高冗餘網路相連。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 全域基礎結構。

除了 AWS 全球基礎設施之外，Amazon FSx 還提供多種功能來協助支援您的資料彈性和備份需求。

備份和還原

Amazon FSx 會在適用於 NetApp ONTAP 檔案系統的 Amazon FSx 中建立並儲存磁碟區的自動備份。Amazon FSx 會在適用於 NetApp ONTAP 檔案系統的 Amazon FSx 備份視窗期間，建立磁碟區的自動備份。Amazon FSx 會根據您指定的備份保留期儲存磁碟區的自動備份。您也可以透過建立使用者啟動的備份來手動備份磁碟區。您可以隨時還原磁碟區備份，方法是使用指定為來源的備份來建立新磁碟區。

如需詳細資訊，請參閱 使用備份。

快照

Amazon FSx 為 NetApp ONTAP 磁碟區建立 Amazon FSx 的快照副本。快照複製提供保護，防止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。

可用區域

適用於 NetApp ONTAP 檔案系統的 Amazon FSx 旨在為資料提供持續可用性，即使在伺服器故障的情況下也是如此。每個檔案系統都由至少一個可用區域中的兩部檔案伺服器提供支援，每個檔案伺服器都有自己的儲存。Amazon FSx 會自動複寫您的資料以保護資料不受元件故障影響、持續監控硬體故障，並在發生故障時自動替換基礎設施元件。檔案系統會視需要自動容錯移轉和回復 (通常在 60 秒內)，而且用戶端會自動透過檔案系統進行容錯移轉和回復。

異地備份檔案系統

Amazon FSx for NetApp ONTAP 檔案系統在可用區域之間具有高可用性和耐用 AWS 性，旨在為資料提供持續可用性，即使在可用區域無法使用的情況下也是如此。

如需詳細資訊，請參閱 可用性與持久性。

單一可用區檔案系統

Amazon FSx for NetApp ONTAP 檔案系統在單一可用區域內具有高可用 AWS 性和耐用性，旨在在發生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 可用性與持久性。

適 NetApp 用於 ONTAP 的 Amazon FSx 基礎設施安全

作為一項受管服務，適用於 NetApp ONTAP 的 Amazon FSx 受到 AWS 全球網路安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎結構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的 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。

搭配 FS NetApp x 使用 ONTAP 網路掃描

您可以使用 NetApp ONTAP 的 Vscan 功能來執行支援的協力廠商防毒軟體。如需詳細資訊，請參閱下列各支援解決方案的資源。

- McAfee — 叢集資料 ONTAP 防毒解決方案指南： McAfee
- SentinelOne — Vscan 合作夥伴解決方案和SentinelOne 奇點雲端資料安全
- 賽門鐵克 — Vscan 合作夥伴解決方案和賽門鐵克防
- 趨勢科技 — 叢集資料 ONTAP 防毒解決方案指南：趨勢科技

適 NetApp 用於 ONTAP 的 Amazon FSx 中的角色和使用者

NetApp ONTAP包含強大且可擴充的角色型存取控制 (RBAC) 功能。 ONTAP角色會在使用 ONTAP CLI 和 REST API 時定義使用者權能和權限。每個角色都會定義不同層級的管理權能和權限。您可以將角色指派給使用者，以便在使用 ONTAP REST API 和 CLI 時控制他們對於 ONTAP 資源的 FSx 存取。對於 ONTAP 檔案系統使用者和儲存虛擬機器 (SVM) 使用者，FSx 有個別可用的ONTAP角色。

當您為 ONTAP 檔案系統建立 FSx 時，會在檔案系統層級和 SVM 層級建立預設ONTAP使用者。您可以建立其他檔案系統和 SVM 使用者，也可以建立其他 SVM 角色來滿足組織的需求。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與使用者

默認的ONTAP文件系統用戶是`fsxadmin`，它具有指定的`fsxadmin`角色。您可以將兩個預先定義的角色指定給檔案系統使用者，如下所示：

- **`fsxadmin`**具有此角色的管理員在系統中擁有不受限制的ONTAP權限。他們可以為 ONTAP 檔案系統設定 FSx 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檢視檔案系統層級的所有內容，但無法進行任何變更。

  此角色非常適合用於監視應用程式，例如，NetApp Harvest因為它對所有可用資源及其屬性具有唯讀存取權，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`角色指定給他們。您無法建立新角色或修改現有角色。如需詳細資訊，請參閱 建立檔案系統和 SVM 管理的新ONTAP使用者。

下表說明檔案系統管理員角色對 ONTAP CLI 和 REST API 命令和命令目錄具有的存取層級。

角色名稱	存取層級	至下列指令或指令目錄
`fsxadmin`	全部	適用於 ONTAP 的 FSx 中所有可用的指令目錄
`fsxadmin-readonly`	全部	`security login password` 僅用於管理自己的用戶帳戶本地密碼和密鑰信息
	無	`security`
	只讀	FSx 中可用於 ONTAP 的所有其他指令目錄

SVM 管理員角色和使用者

每個 SVM 都有個別的驗證網域，可由其自己的系統管理員獨立管理。對於檔案系統上的每個 SVM，預設使用者都是 vsadmin，依預設會指派`vsadmin`角色。除了`vsadmin`角色之外，還有其他預先定義的 SVM 角色可提供您可以指派給 SVM 使用者的關閉範圍權限。您也可以建立自訂角色，以提供符合組織需求的存取控制層級。

SVM 管理員的預先定義角色及其權能如下：

角色名稱	功能
`vsadmin`	• 管理您的使用者帳戶、本機密碼和金鑰資訊 • 管理磁碟區，磁碟區移動除外 • 管理配額、Q 樹狀結構、快照複本和檔案 • 管理 LUN • 執行 SnapLock 作業，授權刪除除外 • 設定通訊協定：NFS、中小型企業和 iSCSI • 設定服務：DNS、LDAP 和網路管理系統 • 監控作業

角色名稱	功能
	• 監控網絡連接和網絡接口 • 監控 SVM 的健全狀況
vsadmin-volume	• 管理您的使用者帳戶、本機密碼和金鑰資訊 • 管理磁碟區，包括磁碟區移動 • 管理配額、Q 樹狀結構、快照複本和檔案 • 管理 LUN • 設定通訊協定：NFS、中小型企業和 iSCSI • 設定服務：DNS、LDAP 和網路管理系統 • 監控網路介面 • 監控 SVM 的健全狀況
vsadmin-protocol	• 管理您的使用者帳戶、本機密碼和金鑰資訊 • 管理 LUN • 設定通訊協定：NFS、中小型企業和 iSCSI • 設定服務：DNS、LDAP 和網路管理系統 • 監控網路介面 • 監控 SVM 的健全狀況
vsadmin-backup	• 管理您的使用者帳戶、本機密碼和金鑰資訊 • 管理 NDMP 作業 • 使用復原的磁碟讀取/寫入 • 管理 SnapMirror 關係和快照副本 • 檢視磁碟區和網路資訊

角色名稱	功能
vsadmin-snaplock	• 管理您的使用者帳戶、本機密碼和金鑰資訊 • 管理磁碟區，磁碟區移動除外 • 管理配額、Q 樹狀結構、快照複本和檔案 • 執行 SnapLock 作業，包括授權刪除 • 設定通訊協定：NFS 和中小企業 • 設定服務：DNS、LDAP 和網路管理系統 • 監控作業 • 監控網絡連接和網絡接口
vsadmin-readonly	• 管理您的使用者帳戶、本機密碼和金鑰資訊 • 監控 SVM 的健全狀況 • 監控網路介面 • 檢視磁碟區和 LUN • 檢視服務和通訊協定

如需如何建立新 SVM 角色的詳細資訊，請參閱建立新的 SVM 角色。

使用活動目錄驗證用ONTAP戶

您可以驗證視窗作用中目錄網域使用者對 ONTAP 檔案系統和 SVM 之 FSx 的存取權。您必須先執行下列工作，才能存取您的檔案系統：

- 您需要設定 SVM 的使用中目錄網域控制站存取權。

  您用來設定為作用中目錄網域控制站存取的閘道或通道的 SVM 必須啟用 CIFS、加入作用中目錄，或兩者兼而有之。如果您未啟用 CIFS，而只將通道 SVM 加入作用中目錄，請確定 SVM 已加入您的作用中目錄。如需詳細資訊，請參閱 將 SVM 加入 Microsoft 活動目錄。
- 您必須啟用 Active Directory 網域使用者帳戶，才能存取檔案系統。

  對於存取 ONTAP CLI 或 REST API 的 Windows 網域使用者，您可以使用密碼驗證或安全殼層公開金鑰驗證。

如需說明如何使用來為檔案系統和 SVM 管理員設定 Active Directory 驗證的程序，請參閱設定ONTAP使用者的使用中目錄驗證。

建立檔案系統和 SVM 管理的新ONTAP使用者

每個ONTAP使用者都與 SVM 或檔案系統相關聯。具有該`fsxadmin`角色的檔案系統使用者可以使用`security login create`ONTAPCLI 命令建立新的 SVM 角色和使用者。

此指`security login create`令會建立管理公用程式的登入方法。登入方法是由使用者名稱、應用程式 (存取方法) 和驗證方法所組成。一個使用者名稱可以與多個應用程式相關聯。它可以選擇性地包含存取控制角色名稱。如果使用作用中目錄、LDAP 或 NIS 群組名稱，則登入方法會提供屬於指定群組的使用者存取權。如果使用者是安全性登入表格中佈建的多個群組的成員，則使用者將可存取授權給個別群組之命令的組合清單。

如需如何建立新ONTAP使用者的資訊，請參閱建立新的 ONTAP 使用者。

主題

- 建立新的 ONTAP 使用者
- 建立新的 SVM 角色
- 設定ONTAP使用者的使用中目錄驗證
- 設定公開金鑰驗證
- 更新檔案系統和 SVM 角色的密碼需求
- 更新fsxadmin帳號密碼失敗

建立新的 ONTAP 使用者

建立新的 SVM 或檔案系統使用者 (ONTAPCLI)

只有具有該`fsxadmin`角色的檔案系統使用者才能建立新的 SVM 和檔案系統使用者。

1. 若要存取 NetApp ONTAP CLI，請執行下列命令，在適用於 NetApp ONTAP 檔案系統的 Amazon FSx 管理連接埠上建立安全殼層工作階段。取代*`management_endpoint_ip`*為檔案系統管理連接埠的 IP 位址。

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

   如需詳細資訊，請參閱 使用 ONTAP CLI 管理檔案系統。

2. 使用 `security login create` ONTAP CLI 命令在您的 FSx (適用於 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`— 指定您要在其中建立新 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，請勿指定 SVM。
   - `-user-or-group-name`— 指定登入方法的使用者名稱或使用中目錄群組名稱。使用中的目錄群組名稱只能使用`domain`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, 安全碼, 和 SSH.
   - `-authentication-method`— 指定登入的驗證方法。可能的值包括以下：
     - 網域 — 用於作用中目錄驗證
     - 密碼 — 用於密碼認證
     - 公開金鑰 — 公開金鑰認證的使用者
   - `-role`— 指定登入方法的存取控制角色名稱。在檔案系統層級上，唯一可以指定的角色是`fsxadmin`。

   (選擇性) 您也可以搭配指令使用下列一或多個參數：

   - `[-comment]`— 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}]`— 指定第二因素驗證方法。您可以指定下列方法：
     - 密碼 — 用於密碼認證
     - 公開金鑰 — 用於公開金鑰驗證
     - NSswitch — 用於 NIS 或 LDAP 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
   ```

   下列指令會建立新的檔案系統使`new_fsxadmin`用者，並指派`fsxadmin-readonly`角色，並使用 SSH 與密碼登入。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，該使用者設定為使用 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. 下列指令會建立新的唯讀檔案系統使harvest2-user用者，以供 NetApp Harvest 應用程式用來收集效能和容量測量結果。如需詳細資訊，請參閱 使用收穫和 Grafana 監控 FSx 的 ONTAP 文件系統。

```
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 SVM 的所有登入資訊。

```
Fsx0123456::> security login show

Vserver: Fsx0123456
                                                                  Second
User/Group                Authentication                 Acct   Authentication
Name           Application Method        Role Name        Locked 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
                                                                  Second
User/Group                 Authentication                 Acct    Authentication
Name           Application Method        Role Name        Locked  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::>
```

建立新的 SVM 角色

您建立的每個 SVM 都有指派預先vsadmin定義角色的預設 SVM 管理員。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。此命令適用於具有該fsxadmin角色的檔案系統管理員。

若要建立新的 SVM 角色

1. 您可以使用以下`security login role create`ONTAP CLI命令建立新的 SVM 角色：

```
Fsx0123456::> security login role create -role vol_role -cmddirname volume
```

2. 在指令中指定下列必要參數：
   - `-role`— 角色的名稱。
   - `-cmddirname`— 角色可存取的指令或命令目錄。用雙引號括住命令子目錄名稱。例如 `"volume snapshot"`。輸入DEFAULT以指定所有指令目錄。
3. (選擇性) 您也可以將下列任何參數新增至指令：
   - `-vserver`— 與角色相關聯的 SVM 名稱。
   - `-access`— 角色的存取層級。對於命令目錄，這包括：
     - none— 拒絕存取指令目錄中的指令。這是自訂角色的預設值。

- `readonly`— 授予對命令目錄及其子目錄中 show 命令的存取權。
- `all`— 授予對命令目錄及其子目錄中所有命令的存取權。若要授與或拒絕內建命令的存取權，您必須指定命令目錄。

對於非內在命令（不以`create`、`modify`、或結尾的命令）：`deleteshow`

- none— 拒絕存取指令目錄中的指令。這是自訂角色的預設值。
- `readonly`— 不適用。不要使用。
- `all`— 授予對命令的存取權限。

- `-query`— 用來篩選存取層級的查詢物件，以命令的有效選項或指令目錄中的命令形式指定。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 伺服器建立名為「admin」的存取控制角色。該角色具有對「卷」命令的所有訪問權限，但只能在「aggr0」聚合中。

```
Fsx0123456::>security login role create -role admin -cmddirname volume -query "-
aggr aggr0" -access all -vserver vs1.example.com
```

設定ONTAP使用者的使用中目錄驗證

使用 ONTAP CLI 來設定ONTAP檔案系統和 SVM 使用者使用作用中目錄驗證的使用方式。

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指令。

若要為使用者設定作ONTAP用中目錄驗證 (ONTAPCLI)

具有該`fsxadmin`角色的檔案系統使用者可以使用此程序中的指令。

1. 若要存取 NetApp ONTAP CLI，請執行下列命令，在適用於 NetApp ONTAP 檔案系統的 Amazon FSx 管理連接埠上建立安全殼層工作階段。取代*`management_endpoint_ip`*為檔案系統管理連接埠的 IP 位址。

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

如需詳細資訊，請參閱 使用 ONTAP CLI 管理檔案系統。

2. 使用如下所示的`security login domain-tunnel create`命令來建立用於驗證 Windows 活動目錄使用者的網域通道。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. 使用此命security login create令建立將存取檔案系統的 Active Directory 網域使用者帳戶。

   在指令中指定下列必要參數：

   - -vserver— 使用 CIFS 設定的 SVM 名稱，並加入您的作用中目錄。它將用來作為驗證 Active Directory 網域使用者對檔案系統的通道。將會建立新角色或使用者。
   - -user-or-group-name— 登入方法的使用者名稱或使用中目錄群組名稱。使用中的目錄群組名稱只能使用domain驗證方法ontapi和ssh應用程式來指定。
   - -application— 登入方法的應用程式。可能的值包括 HTTP, 安全碼, 和 SSH.
   - -authentication-method— 用於登入的驗證方法。可能的值包括以下：
     - 域-用於活動目錄身份驗證
     - 密碼 — 用於密碼認證
     - 公開金鑰 — 用於公開金鑰認證
   - -role— 登入方法的存取控制角色名稱。在檔案系統層級上，唯一可以指定的角色是-role fsxadmin。

   下列範例會為filesystem1檔案系統建立 Active Directory 網域使用者帳戶CORP\Admin。

   ```
   FSxId012345::> security login create -vserver filesystem1 -username CORP\Admin -
   application ssh -authmethod domain -role fsxadmin
   ```

   下列範例會建立具有公開金鑰驗證的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".
   ```

   使用下列命令為使用CORP\Admin者建立公開金鑰：

   ```
   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 與活動目錄憑據登錄到文件系統

- 下列範例會示範如何在您選擇ssh-application類型時，使用 Active Directory 認證透過 SSH 連線至檔案系統。格式為"domain-name\user-name"，username也就是您在建立帳戶時提供的網域名稱和使用者名稱，並以反斜線分隔，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，請使用作用中目錄使用者的密碼。

設定公開金鑰驗證

若要啟用 SSH 公開金鑰驗證，您必須先產生安全殼層金鑰，並使用security login publickey create指令將其與管理員帳戶建立關聯。這可讓帳戶存取 SVM。該security login publickey create命令接受以下參數。

參數	描述
-vserver (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 公開金鑰驗證，請勿包含-versver。
-username	帳戶的使用者名稱。預設值是叢集管理員的預設名稱。admin
-index	公開金鑰的索引編號。如果金鑰是為帳戶建立的第一個金鑰，則預設值為 0。否則，預設值會比帳戶現有的最高索引編號多一個。
-publickey	開啟安全殼層公開金鑰。用雙引號括住索引鍵。
-role	指派給帳戶的存取控制角色。
-comment (選用)	公開金鑰的描述性文字。以雙引號括住文字。

下列範例會將公開金鑰與 SVM 的 SVM 管理員帳戶產生svmadmin關聯。svm01公鑰被分配索引號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工作。

更新檔案系統和 SVM 角色的密碼需求

您可以使用 security login role config modifyONTAPCLI 命令更新檔案系統或 SVM 角色的密碼需求。此命令僅適用於具有該fsxadmin角色的檔案系統管理員帳戶。修改密碼需求時，系統會發出警告，如果有任何具有該角色的現有使用者會受到變更的影響。

下列範例會針對在 fsx SVM 上具有vsadmin-readonly角色的使用者，將密碼需求下限修改為 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帳號密碼失敗

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需求，您可能會收到錯誤訊息。您可以使用 security login role config show ONTAP CLI 或 REST API 命令來檢視密碼需求。

檢視檔案系統或 SVM 角色的密碼需求

1. 若要存取 NetApp ONTAP CLI，請執行下列命令，在適用於 NetApp ONTAP 檔案系統的 Amazon FSx 管理連接埠上建立安全殼層工作階段。取代*management_endpoint_ip*為檔案系統管理連接埠的 IP 位址。

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

   如需詳細資訊，請參閱 使用 ONTAP CLI 管理檔案系統。

2. 此命`security login role config show`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
   ```

   對於`-fields`參數，請指定下列任一或所有項目：

   - `passwd-minlength`— 密碼的最小長度。
   - `passwd-min-special-chars`— 密碼中特殊字元的最小數目。
   - `passwd-min-lowercase-chars`— 密碼中小寫字元的最小數目。
   - `passwd-min-uppercase-chars`— 密碼中大寫字元的最小數目。
   - `passwd-min-digits`— 密碼中的最小位數。
   - `passwd-alphanum`— 包含或排除英數字元的相關資訊。
   - `passwd-expiry-time`— 密碼到期時間。
   - `passwd-expiry-warn-time`— 密碼到期警告時間。

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
       unlimited          0                         0                          0
                unlimited
```

遷移到 Amazon FSx 以進 NetApp 行 ONTAP

以下各節提供如何將現有的 NetApp ONTAP 檔案系統遷移到適 NetApp 用於 ONTAP 的 Amazon FSx 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，檔案中繼資料一律儲存在 SSD 層，而且所有新使用者資料都會先寫入 SSD 層。當資料寫入 SSD 層時，背景分層處理程序會開始將您的資料分層到容量集區儲存體，但分層程序並不是立即的，而且會消耗網路資源。您需要調整 SSD 層的大小，以考慮檔案中繼資料 (使用者資料大小的 3-7%)，作為使用者資料的緩衝區，然後才能將其分層到容量集區儲存體。建議您不要超過 SSD 層的 80% 使用率。
>
> 移轉資料時，請務必使用CloudWatch 檔案系統指標來監控 SSD 層，以確保其填入速度不會超過分層程序將資料移至容量集區儲存體的速度。

主題

使用移轉至 FSx 以進行啟動時使用 NetApp SnapMirror

您可以使用將 NetApp ONTAP 檔案系統遷移到 Amazon FSx 以進行 NetApp ONTAP。 NetApp SnapMirror

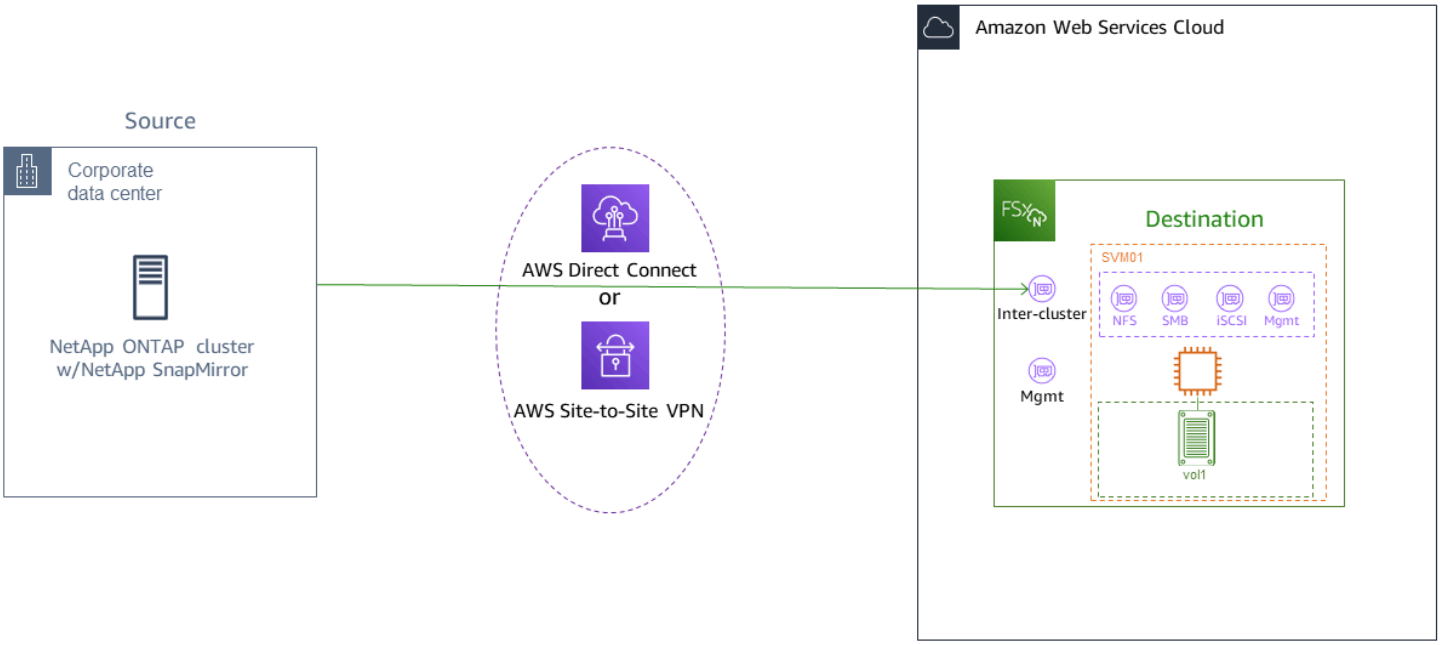
NetApp SnapMirror 在兩個 ONTAP 檔案系統之間採用區塊層級複製，將資料從指定的來源磁碟區複製到目的磁碟區。我們建議您使用 SnapMirror 將內部部署 NetApp ONTAP 檔案系統遷移至適用於 ONTAP 的 FSx。 NetApp SnapMirror即使對於具有以下功能的檔案系統，區塊層級複製也能快速且有效率：

- 複雜的目錄結構
- 超過 5 千萬個文件
- 非常小的檔案大小 (以 KB 為單位)

當您使用移轉 SnapMirror 至 FSx for ONTAP 時，刪除重複資料和壓縮的資料會保留在這些狀態，如此可減少傳輸時間並減少移轉所需的頻寬量。移轉至目標磁碟區時，來源 ONTAP 磁碟區上存在的快照會被保留。將您的內部部署 NetApp ONTAP 檔案系統遷移至適用於 ONTAP 的 FSx 包含下列高階工作：

1. 在 Amazon FSx 中創建目標磁碟區。
2. 收集來源和目的地邏輯介面 (LIF)。
3. 在來源檔案系統與目標檔案系統之間建立叢集對等。
4. 建立 SVM 對等關係。
5. 建立關 SnapMirror 係。
6. 維護更新的目的地叢集。
7. 切換到適用於 ONTAP 檔案系統的 FSx。

下圖說明本節所述的移轉案例。



主題

- 開始之前
- 建立目標磁碟區
- 記錄來源和目的地叢集間 LIF
- 在來源與目的地之間建立叢集對等
- 建立 SVM 對等關係

- 建立關 SnapMirror 係
- 將資料傳輸至您的 FSx 以供 ONTAP 檔案系統使用
- 切割到 Amazon FSx

開始之前

在開始使用下列各節中描述的程序之前，請確定您已符合下列先決條件：

- FSx for ONTAP 會將用戶端流量優先於背景工作，包括資料分層、儲存效率和備份。移轉資料時，我們建議您監控 SSD 層的容量，以確保其使用率不會超過 80%。您可以使用CloudWatch 檔案系統指標來監控 SSD 層的使用率。如需詳細資訊，請參閱 磁碟區指標。
- 如果您在移轉資料`All`時將目的磁碟區的資料分層政策設定為，則所有檔案中繼資料都會儲存在主要 SSD 儲存層。無論磁碟區的資料分層原則為何，檔案中繼資料一律會儲存在以 SSD 為基礎的主要層上。我們建議您假設主要層的比率為 1：10：容量集區層儲存容量。
- 來源和目的地檔案系統連接在相同的 VPC 中，或者位於使用 Amazon VPC 對等互連、Transit Gateway 或對等的網路中。AWS Direct Connect AWS VPN如需詳細資訊，請參閱從內部存取資料AWS和什麼是 VPC 對等互連？ 在 Amazon VPC 對等指南中。
- 適用於 ONTAP 檔案系統之 FSx 的 VPC 人雲端安全性群組具有輸入和輸出規則，可針對叢集間端點 (LIF) 在連接埠 443、10000、11104 和 11105 上允許 ICMP 以及 TCP。
- 建立 SnapMirror 資料保護關係之前，請先確認來源和目的地磁碟區執行相容的 NetApp ONTAP 版本。如需詳細資訊，請參閱 ONTAP 使用者文件中關 SnapMirror 係 NetApp的相容 ONTAP 版本。此處介紹的程序使用內部部署 NetApp ONTAP 檔案系統作為來源。
- 您的內部部署 (來源) NetApp ONTAP 檔案系統包含 SnapMirror 授權。
- 您已經使用 SVM 為 ONTAP 檔案系統建立了目標 FSx，但尚未建立目標磁碟區。如需詳細資訊，請參閱 為 ONTAP 檔案系統建立 FSx。

這些程序中的命令使用下列叢集、SVM 和磁碟區別名：

- *`FSx-Dest`*— 目的地 (FSx) 叢集的識別碼 (格式為 F SxIdabcdef 1234567890a)。
- *`OnPrem-Source`*— 來源叢集的 ID。
- *`DestSVM`*— 目的地 SVM 名稱。
- *`SourceSVM`*— 來源 SVM 名稱。
- 來源磁碟區和目標磁碟區名稱都是`vol1`。

> **Note**
>
> ONTAP 檔案系統的 FSx 在所有的 ONTAP CLI 指令中稱為叢集。

本節中的程序使用下列 NetApp ONTAP CLI 命令。

- 磁碟區建立指令
- 叢集指令
- 虛擬伺服器對等命令
- 快照鏡像指令

您將使用 NetApp ONTAP CLI 在您的 FSx 上建立和管理 ONTAP 檔案系統的 SnapMirror 組態。如需詳細資訊，請參閱 使用 NetApp ONTAP CLI。

建立目標磁碟區

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 來建立資料保護 (DP) 目的地磁碟區。如需使用 Amazon FSx 主控台建立目標磁碟區的相關資訊AWS CLI，請參閱建立磁碟區。

在下列程序中，您將使用 NetApp ONTAP CLI 在適用於 ONTAP 檔案系統的 FSx 上建立目標磁碟區。您將需要檔案系統管理連接埠的`fsxadmin`密碼和 IP 位址或 DNS 名稱。

1. 使用使用者`fsxadmin`和您在建立檔案系統時設定的密碼，與目的地檔案系統建立 SSH 工作階段。

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. 在目的地叢集上建立一個磁碟區，該磁碟區的儲存容量至少等於來源磁碟區的儲存容量。用`-type DP`來將其指定為 SnapMirror 關係的目的地。

   如果您打算使用資料分層，建議您將設定`-tiering-policy`為`all`。如此可確保您的資料會立即傳輸到容量集區儲存空間，並防止 SSD 層的容量不足。移轉後，您可以切換`-tiering-policy`至`auto`。

> **Note**
>
> 無論磁碟區的資料分層原則為何，檔案中繼資料一律會儲存在以 SSD 為基礎的主要層上。

```
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 LIF

SnapMirror 使用叢集間邏輯介面 (LIF)，每個介面都有唯一的 IP 位址，以促進來源和目的地叢集之間的資料傳輸。

1. 對於 ONTAP 檔案系統的目標 FSx，您可以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 位址。執行以下命令：

```
OnPrem-Source::> network interface show -role intercluster

Logical                         Network
Vserver     Interface  Status  Address/Mask
----------- ---------- ------- ------------
FSx-Dest
             inter_1    up/up  10.0.0.36/24
             inter_2    up/up  10.0.1.69/24
```

> **Note**
>
> 對於向外延展檔案系統，每個高可用性 (HA) 配對有兩個叢集間 IP 位址。儲存這些值以供稍後使用。

儲存inter_1和 inter_2 IP 位址。它們在FSx-Dest作為dest_inter_1和用於dest_inter_2OnPrem-Source和中參考source_inter_2。source_inter_1

在來源與目的地之間建立叢集對等

透過提供叢集間 IP 位址，在目的地叢集上建立叢集對等關係。您還需要建立複雜密碼，以便在來源叢集上建立叢集對等時輸入該密碼。

1. 使用下列命令在目的地叢集上設定對等互連。對於向外延展檔案系統，您需要提供每個叢集間 IP 位址。

```
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. 接下來，在來源叢集上建立叢集對等關係。您需要輸入上面創建的密碼才能進行身份驗證。對於向外延展檔案系統，您需要提供每個叢集間 IP 位址。

```
OnPrem-Source::> cluster peer create -address-family ipv4 -peer-
addrs dest_inter_1,dest_inter_2

Enter the passphrase:
Confirm the passphrase:
```

3. 在來源叢集上使用下列命令，確認對等互連是否成功。在輸出中，`Availability`應設定為`Available`。

```
OnPrem-Source::> cluster peer show

Peer Cluster Name  Availability   Authentication
-----------------  -------------- --------------
FSx-Dest           Available      ok
```

建立 SVM 對等關係

建立叢集對等互連後，下一個步驟就是對等 SVM。使用指令在目的地叢集 (FSX-dest) 上建立 SVM 對等關係。`vserver peer`下列指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 SVM 對等關係。

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver SourceSVM -peer-
cluster OnPrem-Source -applications snapmirror -local-name SourceLocalName

 Info: [Job 207] 'vserver peer create' job queued
```

2. 接受來源叢集上的對等關係：

```
OnPrem-Source::> vserver peer accept -vserver SourceSVM -peer-vserver DestSVM -
local-name DestLocalName

 Info: [Job 211] 'vserver peer accept' job queued
```

3. 使用下列命令驗證 SVM 對等狀態；Peer State應在回應peered中設定為。

```
OnPrem-Source::> vserver peer show

Peer    Peer     Peer   Peering  Remote
vserver Vserver  State  Cluster  Applications  Vserver
------- -------- ------ -------- ------------ ---------
svm01   destsvm1 peered FSx-Dest snapmirror    svm01
```

建立關 SnapMirror 係

現在您已對等來源和目的地 SVM，接下來的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 關係之後，目標磁碟區會是唯讀的，直到關係中斷為止。

- 使用命snapmirror create令在目的地叢集上建立 SnapMirror 關係。必須從目的地 SVM 使用該snapmirror create命令。

  您可以選擇性地使用-throttle來設定關係的最大頻寬 (以 KB/ 秒為單位)。 SnapMirror

```
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".
```

將資料傳輸至您的 FSx 以供 ONTAP 檔案系統使用

現在，您已經創建了 SnapMirror 關係，您可以將數據傳輸到目標文件系統。

1. 您可以在目的檔案系統上執行下列指令，將資料傳輸到目的檔案系統。

> **Note**
>
> 執行此命令後，會 SnapMirror 開始將資料快照從來源磁碟區傳輸到目的磁碟區。

```
FSx-Dest::> snapmirror initialize -destination-path DestSVM:vol1 -source-
path SourceLocalName:vol1
```

2. 如果您要移轉正在使用中的資料，則需要更新目的地叢集，使其與來源叢集保持同步。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. 您也可以在完成移轉之前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指令建立 SnapMirror 更新排程。

```
FSx-Dest::> snapmirror modify -destination-path DestSVM:vol1 -schedule hourly
```

切割到 Amazon FSx

若要準備切換至 ONTAP 檔案系統的 FSx，請執行下列動作：

- 中斷所有寫入來源叢集的用戶端。
- 執行最終 SnapMirror 傳輸，以確保切割時不會丟失數據。

- 打破關 SnapMirror 係。
- 將所有用戶端 Connect 至 ONTAP 檔案系統的 FSx。

1. 若要確保來源叢集中的所有資料都會傳輸至 ONTAP 檔案系統的 FSx，請執行最後的快照鏡像傳輸。

```
FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
```

2. 確認資料移轉已完成，方法是確認已`Mirror State`將資料移轉設定為`Snapmirrored`，且`Relationship Status`設定為`Idle`。您也應該確定`Last Transfer End Timestamp`日期如預期般，正如上次傳輸到目的地磁碟區的時間一樣。
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     Destination   Mirror        Relationship Last Transfer End
Path       Path          State         Status       Timestamp
---------- -----------   ----------    -------      ---------------
Svm01:vol1 svm02:DestVol Snapmirrored  Idle         09/02 09:02:21
```

4. 使用`snapmirror quiesce`指令停用任何 future 的 SnapMirror 傳輸。

```
FSx-Dest::> snapmirror quiesce -destination-path DestSVM:vol1
```

5. 確認`Relationship Status`已變更為使`Quiesced`用`snapmirror show`。

```
FSx-Dest::> snapmirror show

Source            Destination   Mirror        Relationship
Path              Path          State         Status
-----------       ------------  ------------- --------
sourcesvm1:vol1   svm01:DestVol Snapmirrored  Quiesced
```

6. 移轉期間，目的地磁碟區為唯讀。若要啟用讀取/寫入功能，您需要中斷 SnapMirror 關聯性，並切換至 ONTAP 檔案系統的 FSx。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 複製完成並中斷了 SnapMirror關係，您就可以掛載磁碟區以使資料可用。

```
FSx-Dest::> vol mount -vserver fsx -volume vol1 -junction-path /vol1
```

磁碟區現在可以使用來源磁碟區中的資料完全移轉至目的地磁碟區。用戶端也可以讀取和寫入磁碟區。如果您先前將此磁碟區`tiering-policy`的設定為`all`，您可以將其變更為`auto`或，`snapshot-only`且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存取此資料，請參閱存取 資料。

使用移轉至 FSx 以進行啟動時使用 AWS DataSync

我們建議您使用AWS DataSync在 ONTAP 檔案系統的 FSx 與非 OnTap 檔案系統之間傳輸資料，包括 FSx for Lustre、OpenZF 的 FSx、FSx for Windows File Server 專用的 FSx、亞馬遜 EFS、Amazon S3 和現場部署檔案管理員。如果您要在 FSx 適用於 ONTAP 和 NetApp ONTAP 之間傳輸檔案，我們建議您使用. NetApp SnapMirror AWS DataSync是一種資料傳輸服務，可透過網際網路或網際網路或儲存服務，簡化、自動化並加速資料在自我管理儲存系統與AWS儲存服務之間的移動和複製。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、時間戳記和存取權限。

您可 DataSync 以使用在 ONTAP 檔案系統的兩個 FSx 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 DataSync 與 FSx 搭配 ONTAP 檔案系統使用來執行其他工作。例如，您可以執行一次性資料移轉、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。

在中 DataSync，位置是 ONTAP 檔案系統 FSx 的端點。如需有關特定移轉案例的資訊，請參閱《AWS DataSync使用指南》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，檔案中繼資料一律儲存在 SSD 層，而且所有新使用者資料都會先寫入 SSD 層。當資料寫入 SSD 層時，背景分層處理程序會開始將您的資料分層到容量集區儲存體，但分層程序並不是立即的，而且會消耗網路資源。您需要調整 SSD 層的大小，以考慮檔案中繼資料 (使用者資料大小的 3-7%)，作為使用者資料的緩衝區，然後才能將其分層到容量集區儲存體。我們建議您不要超過 80% SSD 使用率。
>
> 移轉資料時，請務必使用CloudWatch 檔案系統指標來監控 SSD 層，以確保其填入速度不會超過分層程序將資料移至容量集區儲存體的速度。您也可以將 DataSync 傳輸限制為低於分層發

生的速率，以確保 SSD 層的使用率不會超過 80%。例如，對於輸送容量至少為 512 Mbps 的檔案系統，200 Mbps 的節流量通常會在資料傳輸和資料分層速率之間取得平衡。

必要條件

若要將資料移轉至 FSx 以進行 ONTAP 設定，您需要符合需求的伺服器和網路。 DataSync 若要深入瞭解，請參閱《AWS DataSync使用者指南》 DataSync中的「的需求」。

使用移轉檔案的基本步驟 DataSync

使用將文件從源傳輸到目的地 DataSync 涉及以下基本步驟：

- 在您的環境中下載並部署代理程式並啟用它 (如果在兩者之間進行轉移，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：

- 自我管理的儲存裝置與 AWS
- 建立適用於 ONTAP 的 Amazon FSx 位置 NetApp

監控 Amazon FSx 的 ONTAP NetApp

您可以使用下列服務和工具來監控 Amazon FSx 的 NetApp ONTAP 使用量和活動：

- 亞馬遜 CloudWatch — 您可以使用 Amazon 監控檔案系統 CloudWatch，該 Amazon 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，以便您存取歷史資訊並查看檔案系統的執行狀況。您也可以根據指定期間內的測量結果設定警示，並根據與您指定之臨界值相關的測量結果值執行一或多個動作。
- ONTAP EMS 事件 — 您可以使用 ONTAP 的事件管理系統 (EMS) 產生的事件來監控 FSx 的 ONTAP 檔案系統。EMS 事件是檔案系統中發生的通知，例如建立 iSCSI LUN 或磁碟區的自動調整大小。
- NetApp 雲端洞察 — 您可以使用 NetApp 雲端洞察服務監控 FSx 適用於 ONTAP 檔案系統的組態、容量和效能指標。您也可以根據測量結果條件建立警示。
- NetApp 收穫和 NetApp Grafana — 您可以使用「收穫」和「Grafana」來監視 FSx 的 ONTAP 文件 NetApp 系統。 NetApp NetApp 收穫會從適用於 ONTAP 檔案系統的 FSx 收集效能、容量和硬體度量來監控 ONTAP 檔案系統。Grafana 提供儀表板，可在其中顯示收集的「收穫」指標。
- AWS CloudTrail— 您可以用 AWS CloudTrail 來擷取 Amazon FSx 的所有 API 呼叫做為事件。這些事件提供 Amazon FSx 中使用者、角色或 AWS 服務所採取的動作記錄。

主題

使用 Amazon 監控 CloudWatch

您可以使用 Amazon 監控檔案系統 CloudWatch，該 Amazon 會收集適用於 NetApp ONTAP 的 Amazon FSx 的原始資料，並將其處理為可讀且接近即時的指標。這些統計資料會保留 15 個月，因此您可以存取歷史資訊以判斷檔案系統的執行方式。依預設，ONTAP 量度資料的 FSx 會 CloudWatch

在 1 分鐘期間自動傳送至。如需詳細資訊 CloudWatch，請參閱什麼是 Amazon CloudWatch？ 在 Amazon 用 CloudWatch 戶指南。

> **Note**
>
> 根據預設，ONTAP 的 FSx 會在 1 分鐘的時間傳送量度資料 CloudWatch 至 1 分鐘的時間，但以下以 5 分鐘間隔傳送的量度除外：
>
> - `FileServerDiskThroughputBalance`
> - `FileServerDiskIopsBalance`

CloudWatch ONTAP 的 FSx 量度分為四個類別，這些類別是由用來查詢每個量度的維度所定義。如需維度的詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的維度。

- 文件系統指標：F ile-system-level 性能和存儲容量指標。
- 詳細的檔案系統指標：每個ile-system-level 儲存層的 F 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) 的每個磁碟區儲存容量指標。

ONTAP 的 FSx 的所有 CloudWatch 測量結果都會發佈至中的`AWS/FSx`命名空間。 CloudWatch

主題

- 如何將 FSx 用於 ONT CloudWatch AP 量度
- 存取 CloudWatch 量度
- 檔案系統度量
- 向外延展檔案系統度量
- 磁碟區指標
- 效能警告與建議
- 創建 Amazon CloudWatch 警報來監控 Amazon FSx

如何將 FSx 用於 ONT CloudWatch AP 量度

Amazon FSx 所報告的 CloudWatch 指標可針對 ONTAP 檔案系統和磁碟區提供有關 FSx 的重要資訊。

主題

在 Amazon FSx 主控台中監控檔案系統指標

您可以使用 Amazon FSx 主控台檔案系統儀表板上的監控和效能面板，檢視下表所述的指標。如需詳細資訊，請參閱 存取 CloudWatch 量度。

監控與效能	我該如何...	图表	相關指標
Summary	... 判斷檔案系統上的可用儲存容量？	可用的主要儲存容量 (位元組)	StorageCapacity {SSD} - StorageUsed {SSD}
	... 確定我的文件系統的客戶端總吞吐量？	從屬端輸送量總計 (位元組/秒)	總和 (DataReadBytes +DataWriteBytes)/期間 (以秒為單位)
	... 確定我的文件系統的客戶端 IOPS 總數？	用戶端 IOPS 總計 (作業數/秒)	總和 (DataReadOperations DataWriteOperations +MetadataOperations)/期間 (以秒為單位)
	... 決定我的檔案系統讀取、寫入和中繼資料作業的平均延遲時間？	平均延遲 (MS/ 作業)	平均讀取延遲：DataReadOperationTime * 1000/DataReadOperations 平均寫入延遲：DataWriteOperationTime *

監控與效能	我該如何...	圖表	相關指標
			1000/DataWrite Operations 平均中繼資料延遲：MetadataOperationTime * 1000/MetadataOperations
	... 決定我的檔案系統上已使用和可用儲存容量的分佈情況？	儲存分佈	主要層級可用：StorageCapacity {SSD}-StorageUsed {SSD} 使用的主要層：StorageUsed {SSD} 使用的容量池：StorageUsed {StandardCapacityPool }
	... 決定儲存效率 (壓縮、重複資料刪除和壓縮) 所節省的成本？	節省儲存效率	StorageEfficiencySavings
儲存	... 決定有多少可用的主要儲存裝置？	可用的主要儲存容量 (位元組)	StorageCapacity {SSD} - StorageUsed {SSD}
	... 決定我的檔案系統使用的主要儲存空間百分比？	主要儲存容量使用率 (百分比)	StorageUsed {SSD} * 100/StorageCapacity {} SSD
檔案伺服器效能	... 確定我的文件系統是否正在接近其網絡吞吐量限制？	網路輸送量 — 使用率 (百分比)	NetworkThroughputUtilization

監控與效能	我該如何...	图表	相關指標
	... 確定我的文件系統是否正在接近其磁盤吞吐量限制？	磁碟輸送量 — 使用率 (百分比)	FileServerDiskThroughputUtilization
	... 判斷我的檔案系統是否已耗盡磁碟輸送量允許的突發積分？	磁碟輸送量 — 突發平衡 (百分比)	FileServerDiskThroughputBalance
	... 確定我的文件系統是否正在接近其文件服務器的 SSD IOPS 限制？	磁碟 IOPS — 使用率 (百分比)	FileServerDiskIopsUtilization
	... 確定我的文件系統是否已用盡其文件服務器的磁盤 SSD IOPS 允許的突發積分？	磁碟 IOPS — 突發平衡 (百分比)	FileServerDiskIopsBalance
	... 確定文件系統 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)	FileServerCacheHitRatio
磁碟效能	... 判斷我的檔案系統是否接近目前佈建的 SSD IOPS 容量？	磁碟 IOPS — 使用率 (SSD) (百分比)	DiskIopsUtilization

> **Note**
>
> 建議您將任何效能相關維度 (例如網路使用率、CPU 使用率和 SSD IOPS 使用率) 的平均輸送量容量使用率維度維持在 50% 以下。如此可確保您擁有足夠的備用輸送量容量，以應付工作負載中的意外峰值，以及任何背景儲存作業 (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 主控台的磁碟區儀表板上檢視監控面板，以查看其他效能指標。如需詳細資訊，請參閱 存取 CloudWatch 量度。

監控	我該如何...	图表	相關指標
	... 判斷我的磁碟區的可用儲存容量？	可用儲存容量	StorageCapacity
	... 判斷我的磁碟區的用戶端總輸送量？	從屬端輸送量總計 (位元組/秒)	總和 (DataReadBytes +DataWriteBytes)/期間 (以秒為單位)
	... 確定我的磁碟區用戶端 IOPS 總數？	用戶端 IOPS 總計 (作業數/秒)	總和 (DataReadOperations DataWriteOperations +MetadataOperations)/期間 (以秒為單位)
	... 決定有多少讀取和寫入作業來自或進入容量集區層？	容量集區 IOPS (作業/秒)	讀取操作：CapacityPoolReadOperations 寫操作：CapacityPoolWriteOperations
	... 決定磁碟區的讀取、寫入和中繼資料作業的平均延遲時間？	平均延遲 (MS/ 作業)	平均讀取延遲：DataReadOperationTime * 1000/DataReadOperations

監控	我該如何...	图表	相關指標
			平均寫入延遲：DataWrite OperationTime * 1000/DataWrite Operations 平均中繼資料延遲：MetadataOperationTime * 1000/MetadataOperations
	... 確定我的卷上可用的文件或 inode 的數量？	可用檔案 (節點)	FilesCapacity - FilesUsed
	... 決定我的磁碟區已使用和可用儲存容量的分佈情況？	儲存分佈	StorageCapacity - StorageUsed

存取 CloudWatch 量度

您可以透過下列方式查看 Amazon FSx 的 Amazon CloudWatch 指標：

- Amazon FSx 控制台
- Amazon CloudWatch 控制台
- 的 AWS Command Line Interface （ AWS CLI ）對於 CloudWatch
- 該 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/。
2. 在左側導覽窗格中，選擇 [檔案系統]，然後選擇您要檢視其度量的檔案系統。
3. 在「摘要」頁面上，從第二個面板選擇「監視與效能」，以檢視檔案系統測量結果的圖形。

[監視與效能] 面板上有四個索引標籤。

- 選擇「摘要」(預設標籤)，CloudWatch 以顯示「檔案系統」活動的任何使用中警告、警示及圖表。
- 選擇儲存體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和儲存體效能測量結果。
- 選擇CloudWatch 警示以檢視針對檔案系統設定之任何警示的圖形。

下列程序說明如何使用 Amazon FSx 主控台檢視磁碟區的 CloudWatch 指標

若要使用 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/。
2. 在左側導覽窗格中，選擇「磁碟區」，然後選擇您要檢視其量度的磁碟區。
3. 在 [摘要] 頁面上，從第二個面板中選擇 [監視] (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。

若要使用 Amazon CloudWatch 主控台檢視指標

1. 在檔案系統的 [摘要] 頁面上，從第二個面板選擇 [監視與效能]，以檢視檔案系統度量的圖形。
2. 從您要在 Amazon CloudWatch 主控台中檢視的圖形右上角的動作功能表中選擇「在指標中檢視」。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 主控台中的儀表板。

若要將指標新增至 Amazon CloudWatch 主控台

1. 在 Amazon FSx 主控台的監控和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「新增至管控面板」。這將打開 Amazon CloudWatch 控制台。
3. 從清單中選取現有的 CloudWatch 控制面板，或建立新的儀表板。如需詳細資訊，請參閱 Amazon 使用 CloudWatch 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度量 AWS CLI。

若要從存取度量 AWS CLI

- 使用 CloudWatch 清單公制 CLI 命令搭配參數。`--namespace "AWS/FSx"`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。

若要從 CloudWatch API 存取指標

- 呼叫「統GetMetric計資料 API」作業。如需詳細資訊，請參閱 Amazon CloudWatch API 參考資料。

檔案系統度量

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檔案系統指標。

- 檔案系統度量是採用單一維度的單一檔案系統的彙總效能和儲存度量`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) 中已使用的儲存容量。每個量度都包含`FileSystemId`、`StorageTier`、和`DataType`維度。

請注意以下有關 Amazon FSx 何時發佈這些指標的資料點以 CloudWatch：

- 對於使用率量度 (名稱以「使用率」結尾的任何量度，例如`NetworkThroughputUtilization`)，每個作用中檔案伺服器或彙總會在每個期間發出一個資料點。例如，Amazon FSx 會針對每個作用中檔案伺服器發出一分鐘的量度`FileServerDiskIopsUtilization`，每個彙總發出一分鐘量度。`DiskIopsUtilization`
- 對於所有其他量度，每個週期都會發出一個資料點，對應於所有作用中檔案伺服器 (`DataReadBytes`例如檔案伺服器量度) 或所有彙總 (例如`DiskReadBytes`儲存指標) 的量度總值。

主題

- 網路 I/O 指標
- 檔案伺服器度量
- 磁碟 I/O 測量結果
- 儲存容量指標
- 詳細的檔案系統指標

網路 I/O 指標

所有這些量度都採用一個維度`FileSystemId`。

指標	描述
NetworkThroughputUtilization	檔案系統的網路輸送量使用率百分比。 Average統計資料是指定期間內檔案系統的平均網路輸送量使用率。 Minimum統計資料是指定期間內檔案系統的最低網路輸送量使用率。 Maximum統計資料是指定期間內檔案系統的最高網路輸送量使用率。 單位：百分比 有效統計資料：Average、Minimum、和 Maximum
NetworkSentBytes	檔案系統傳送的位元組數 (網路 I/O)。 統Sum計資料是檔案系統在指定期間內傳送的位元組總數。 若要計算任何統計資料的傳送輸送量 (每秒位元組數)，請將統計值除以指定期間內的秒數。 單位：位元組 有效的統計資訊：Sum
NetworkReceivedBytes	檔案系統接收的位元組數 (網路 I/O)。 Sum統計資料是檔案系統在指定期間內接收到的位元組總數。 若要計算任何統計資料的接收輸送量 (每秒位元組)，請將統計值除以指定期間內的秒數。 單位：位元組 有效的統計資訊：Sum

指標	描述
DataReadBytes	從屬端讀取到檔案系統的位元組數 (網路 I/O)。 Sum統計值是指定期間內與讀取作業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統計值除以指定期間內的秒數。 單位：位元組 有效的統計資訊：Sum
DataWriteBytes	從屬端寫入檔案系統的位元組數 (網路 I/O)。 Sum統計資料是指定期間內與寫入作業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統計值除以指定期間內的秒數。 單位：位元組 有效的統計資訊：Sum
DataReadOperations	從用戶端讀取到檔案系統的讀取作業 (網路 I/O) 計數。 Sum統計值是指定期間內發生的 I/O 作業總數。若要計算一段期間內每秒的平均讀取作業，請將Sum統計值除以指定期間內的秒數。 單位：計數 有效的統計資訊：Sum

指標	描述
DataWriteOperations	從屬端寫入至檔案系統的寫入作業 (網路 I/O) 計數。 Sum統計值是指定期間內發生的 I/O 作業總數。若要計算一段期間內每秒的平均寫入作業，請將Sum統計值除以指定期間內的秒數。 單位：計數 有效的統計資訊：Sum
MetadataOperations	從屬端至檔案系統的中繼資料作業 (網路 I/O) 計數。 Sum統計值是指定期間內發生的 I/O 作業總數。若要計算一段期間內每秒的平均中繼資料作業，請將Sum統計值除以指定期間內的秒數。 單位：計數 有效的統計資訊：Sum
DataReadOperationTime	從用戶端存取檔案系統中資料的讀取作業 (網路 I/O)，在檔案系統內花費的總時間總和。 Sum統計值是指定期間內讀取作業所花費的總秒數。若要計算一段期間Sum的平均讀取延遲，請將Sum統計值除以同一期間內的DataReadOperations 指標。 單位：秒 有效的統計資訊：Sum

指標	描述
DataWriteOperationTime	在檔案系統內完成從屬端存取檔案系統中資料的寫入作業 (網路 I/O) 所花費的總時間總和。 Sum統計值是指定期間內寫入作業所花費的總秒數。若要計算一段期間Sum的平均寫入延遲，請將Sum統計值除以同一期間內的DataWrite Operations 度量。 單位：秒 有效的統計資訊：Sum
CapacityPoolReadBytes	從檔案系統的容量集區層讀取 (網路 I/O) 的位元組數目。 為確保資料完整性，ONTAP 會在執行寫入作業後，立即在容量集區上執行讀取作業。 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統計值除以指定期間內的秒數。 單位：位元組 有效的統計資訊：Sum

指標	描述
CapacityPoolReadOperations	來自檔案系統容量集區層的讀取作業 (網路 I/O) 數目。這會轉換為容量集區讀取要求。 為確保資料完整性，ONTAP 會在執行寫入作業後，立即在容量集區上執行讀取作業。 統Sum計資料是指定期間內檔案系統容量集區層的讀取作業總數。若要計算每秒的容量集區要求，請將Sum統計值除以指定期間內的秒數。 單位：計數 有效的統計資訊：Sum
CapacityPoolWriteBytes	寫入檔案系統容量集區層的位元組數 (網路 I/O)。 為確保資料完整性，ONTAP 會在執行寫入作業後，立即在容量集區上執行讀取作業。 Sum統計資料是指定期間內寫入檔案系統容量集區層的總位元組數。若要計算每秒的容量集區位元組，請將Sum統計值除以指定期間內的秒數。 單位：位元組 有效的統計資訊：Sum

指標	描述
CapacityPoolWriteOperations	從容量集區層對檔案系統的寫入作業 (網路 I/O) 數目。這轉換為寫入請求。 為確保資料完整性，ONTAP 會在執行寫入作業後，立即在容量集區上執行讀取作業。 統Sum計資料是指定期間內檔案系統容量集區層的寫入作業總數。若要計算每秒的容量集區要求，請將Sum統計值除以指定期間內的秒數。 單位：計數 有效的統計資訊：Sum

檔案伺服器度量

所有這些量度都採用一個維度FileSystemId。

指標	描述
CPUUtilization	檔案系統 CPU 資源的使用率百分比。 統Average計值是指定期間內檔案系統的平均 CPU 使用率。 統Minimum計資料是指定期間內檔案系統的最低 CPU 使用率。 統Maximum計資料是指定期間內檔案系統的最高 CPU 使用率。 單位：百分比 有效統計資料：Average、Minimum、和 Maximum

指標	描述
FileServerDiskThroughputUtilization	檔案伺服器與主要層之間的磁碟輸送量，佔佈建限制的百分比，由輸送量容量決定。 Average統計資料是指定期間內檔案伺服器磁碟輸送量的平均百分比使用率。 Minimum統計資料是指定期間內檔案伺服器磁碟輸送量使用率最低的百分比。 Maximum統計資料是指定期間內檔案伺服器磁碟輸送量的最高使用率。 單位：百分比 有效統計資料：AverageMinimum、和Maximum
FileServerDiskThroughputBalance	檔案伺服器與主要層之間磁碟輸送量的可用突發積分百分比。這對於佈建輸送容量為 512 Mbps 或更小的檔案系統有效。 Average統計值是指定期間內可用的平均成組分解餘額。 Minimum統計值是指定期間內可用的最小突發餘額。 Maximum統計值是指定期間內可用的最大突發餘額。 單位：百分比 有效統計資料：AverageMinimum、和Maximum

指標	描述
FileServerDiskIopsBalance	檔案伺服器與主要層之間磁碟 IOPS 的可用突發積分百分比。這對於佈建輸送容量為 512 Mbps 或更小的檔案系統有效。 Average統計值是指定期間內可用的平均成組分解餘額。 Minimum統計值是指定期間內可用的最小突發餘額。 Maximum統計值是指定期間內可用的最大突發餘額。 單位：百分比 有效統計資料：AverageMinimum、和 Maximum
FileServerDiskIopsUtilization	檔案伺服器之可用磁碟 IOPS 容量的 IOPS 使用率百分比。 統Average計值是指定期間內檔案系統的平均磁碟 IOPS 使用率。 Minimum統計資料是指定期間內檔案系統的最低磁碟 IOPS 使用率。 Maximum統計資料是指定期間內檔案系統的最大磁碟 IOPS 使用率。 單位：百分比 有效統計資料：AverageMinimum、和 Maximum

指標	描述
FileServerCacheHitRatio	檔案系統 RAM 和 NVMe 快取中資料所提供之所有讀取要求的百分比。較高的百分比表示檔案系統的讀取快取會提供更多讀取。 單位：百分比 統Average計值是指定期間內檔案系統的平均快取命中百分比。 Minimum統計資料是指定期間內檔案系統的最低快取命中百分比。 Maximum統計資料是指定期間內檔案系統的最高快取命中百分比。 有效統計資料：Average、Minimum、和 Maximum

磁碟 I/O 測量結果

所有這些量度都採用一個維度FileSystemId。

指標	描述
DiskReadBytes	從任何磁碟讀取到檔案系統主要層的位元組數 (磁碟 I/O)。 統Sum計資料是指定期間內從檔案系統讀取的位元組總數。 若要計算任何統計值的讀取磁碟輸送量 (每秒位元組數)，請將Sum統計值除以指定期間內的秒數。 單位：位元組 有效的統計資訊：Sum

指標	描述
DiskWriteBytes	任何磁碟寫入檔案系統主要層的位元組數 (磁碟 I/O)。 統Sum計資料是指定期間內從檔案系統寫入的總位元組數。 若要計算任何統計值的寫入磁碟輸送量 (每秒位元組數)，請將Sum統計值除以指定期間內的秒數。 單位：位元組 有效的統計資訊：Sum
DiskIopsUtilization	檔案伺服器與儲存磁碟區之間的磁碟 IOPS，佔主要分層佈建磁碟 IOPS 限制的百分比。 統Average計值是指定期間內檔案系統的平均磁碟 IOPS 使用率。 Minimum統計資料是指定期間內檔案系統的最低磁碟 IOPS 使用率。 Maximum統計資料是指定期間內檔案系統的最大磁碟 IOPS 使用率。 單位：百分比 有效統計資料：Average、Minimum、和 Maximum

指標	描述
DiskReadOperations	來自檔案系統主要層的讀取作業 (磁碟 I/O) 數目。 Sum統計資料是指定期間內主要層的讀取作業總數。 單位：計數 有效的統計資訊：Sum
DiskWriteOperations	檔案系統主要層的寫入作業 (磁碟 I/O) 數目。 Sum統計資料是指定期間內主要層的寫入作業總數。 單位：計數 有效的統計資訊：Sum

儲存容量指標

所有這些量度都採用一個維度FileSystemId。

指標	描述
StorageEfficiencySavings	儲存效率功能 (壓縮、重複資料刪除和壓縮) 所儲存的位元組。 Average統計值是指定期間內可節省的平均儲存效率。若要以一分鐘期間內儲存之所有資料的百分比來計算儲存效率節省的百StorageEfficiencySavings 分比，請StorageUsed 除以的總StorageEfficiencySavings 和與StorageUsed 檔案系統測量結果 (使用的Sum統計值)。

指標	描述
	Minimum統計資料是指定期間內節省的最低儲存效率。 Maximum統計資料是指定期間內可節省的最大儲存效率。 單位：位元組 有效統計資料：AverageMinimum、和Maximum
StorageUsed	在主要 (SSD) 層和容量集區層上儲存在檔案系統上的實體資料總量。此指標可節省儲存效率功能，例如資料壓縮和重複資料刪除。 單位：位元組 有效統計資料：AverageMinimum、和Maximum

指標	描述
LogicalDataStored	儲存在檔案系統上的邏輯資料總量，同時考慮 SSD 層和容量集區層。此測量結果包括快照的邏輯大小總計 FlexClones，但不包括透過壓縮、壓縮和重複資料刪除所節省的儲存效率。 若要計算以位元組為單位Average的StorageUsed 儲存效率節省，請在指定期間內取得的值，然後在相同Average的LogicalDataStored 週期中減去。 若要以邏輯資料總大小的百分比計算儲存效率節省的情況，請取Average出指定StorageUsed 時段內的指定期間，然後從相Average同期間減去。LogicalDataStored 然後除以LogicalDataStored 在同一時期Average的差異。 單位：位元組 有效統計資料：AverageMinimum、和Maximum

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。詳細的檔案系統度量都有維度FileSystemIdStorageTier、和DataType。

- StorageTier維度會指出量度所測量的儲存層，可能的值為SSD和StandardCapacityPool。
- DataType維度會指出量度所測量的資料類型，以及可能的值All。

指定量度和維度索引鍵值配對的每個唯一組合都會有一個資料列，其中包含該組合測量結果的說明。

指標	描述
StorageCapacityUtilization	每個檔案系統彙總的儲存容量使用率。每分鐘會針對每個檔案系統的彙總發出一個量度。 Average統計資料是指定期間內檔案系統效能層的平均儲存容量使用量。 Minimum統計資料是指定期間內檔案系統效能層的最低儲存容量使用量。 Maximum統計資料是指定期間內檔案系統效能層的最高儲存容量使用量。 單位：百分比 有效統計資料：AverageMinimum、和Maximum
StorageCapacity	主要 (SSD) 層的總儲存容量。 單位：位元組 有效的統計資訊：Maximum
StorageUsed	已使用的實體儲存容量 (位元組)，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 是SSD和StandardCapacityPool ，對應於此測量結果所測量的儲存層。此量度還需要具有值的DataType維度All。 AverageMinimum、和Maximum統計資料是指定期間內每層儲存體耗用量 (位元組)。 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同一期間內的任何資料，StorageTier 維度等於SSD。Maximum StorageCapacity

指標	描述
	若要計算主要 (SSD) 儲存層的可用儲存容量 (位元組)，請從相同期間減去任何這些統計資料，維度`StorageTier` 等於`SSD`。`Maximum StorageCapacity` 單位：位元組 有效統計資料：`Average`、`Minimum`、和 `Maximum`

向外延展檔案系統度量

下列是針對具有兩個或多個高可用性 (HA) 配對之 ONTAP 檔案系統的 FSx 提供的測量結果。針對指標，會針對每個 HA 配對和每個彙總 (針對儲存使用率指標) 發出資料點。

> **Note**
>
> 如果您的檔案系統具有多個 HA 配對，您也可以使用單 HA 配對檔案系統測量結果和磁碟區測量結果。

主題

- 網路 I/O 指標
- 檔案伺服器度量
- 磁碟 I/O 測量結果
- 詳細的檔案系統指標

網路 I/O 指標

所有這些量度都採用兩個維度，`FileSystemId`和`FileServer`。

- `FileSystemId`— 檔案系統的 AWS 資源 ID。
- `FileServer`— ONTAP 中檔案伺服器 (或節點) 的名稱 (例如，`FsxId01234567890abcdef-01`)。奇數的檔案伺服器是偏好的檔案伺服器 (也就是說，除非檔

案系統已容錯移轉至次要檔案伺服器，否則它們會提供流量服務)，而偶數的檔案伺服器則是次要檔案伺服器 (也就是說，它們僅在其合作夥伴無法使用時才提供流量)。因此，次要檔案伺服器的使用率通常比慣用的檔案伺服器少。

指標	描述
NetworkThroughputUtilization	網路輸送量使用率佔您檔案系統可用網路輸送量的百分比。此測量結果相當於您檔案系統之一 HA 配對之網路傳輸量容量的上限NetworkSentBytes 和NetworkReceivedBytes 百分比。此量度中會考慮所有流量，包括背景工作 (例如分層和備份)。 SnapMirror每分鐘會針對每個檔案系統的檔案伺服器發出一個量度。 Average統計值是指定期間內指定檔案伺服器的平均網路輸送量使用率。 Minimum統計值是指定期間內，指定檔案伺服器在一分鐘內最低的網路輸送量使用率。 Maximum統計值是指定期間內，指定檔案伺服器在一分鐘內的最高網路輸送量使用率。 單位：百分比 有效統計資料：AverageMinimum、和 Maximum
NetworkSentBytes	檔案系統傳送的位元組數 (網路 IO)。此量度中會考慮所有流量，包括背景工作 (例如分層和備份)。 SnapMirror每分鐘會針對每個檔案系統的檔案伺服器發出一個量度。 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。 Average統計資料是指定的檔案伺服器在指定期間內透過網路傳送的平均位元組數。

指標	描述
	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。 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多位元組數。 若要計算任何統計資料的傳送輸送量 (每秒位元組數)，請將統計值除以指定期間內的秒數。 單位：位元組 有效統計資料：SumAverage、Minimum、和 Maximum
NetworkReceivedBytes	檔案系統接收的位元組數 (網路 IO)。此量度中會考慮所有流量，包括背景工作 (例如分層和備份)。 SnapMirror每分鐘會針對每個檔案系統的檔案伺服器發出一個量度。 Sum統計資料是指定的檔案伺服器在指定期間內透過網路接收的位元組總數。 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。 Minimum統計資料是指定的檔案伺服器在指定期間內，每分鐘透過網路接收的位元組數目下限。 Maximum統計資料是指定的檔案伺服器在指定期間內，每分鐘透過網路接收的位元組數目上限。 若要計算任何統計資料的接收輸送量 (每秒位元組)，請將統計值除以期間中的秒數。 單位：位元組 有效統計資料：SumAverage、Minimum、和 Maximum

檔案伺服器度量

所有這些量度都採用兩個維度，FileSystemId和FileServer。

指標	描述
CPUUtilization	檔案系統 CPU 資源的使用率百分比。每分鐘會針對每個檔案系統的檔案伺服器發出一個量度。 統Average計值是指定期間內檔案系統的平均 CPU 使用率。 Minimum統計值是指定期間內指定檔案伺服器的最低 CPU 使用率。 Maximum統計值是指定期間內指定檔案伺服器的最高 CPU 使用率。 單位：百分比 有效統計資料：Average、Minimum、和 Maximum
FileServerDiskThroughputUtilization	檔案伺服器與彙總之間的磁碟輸送量，佔佈建限制的百分比，由輸送量容量決定。此量度中會考慮所有流量，包括背景工作 (例如分層和備份)。 SnapMirror此測量結果相當於檔案系統之一 HA 配對之檔案伺服器磁碟輸送量容量的總DiskReadBytes 和DiskWriteBytes 和百分比。每分鐘會針對每個檔案系統的檔案伺服器發出一個量度。 Average統計資料是指定期間內指定檔案伺服器的平均檔案伺服器磁碟輸送量使用率。 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。 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。

指標	描述
	單位：百分比 有效統計資料：AverageMinimum、和 Maximum
FileServerDiskIopsUtilization	檔案伺服器可用磁碟 IOPS 容量的 IOPS 使用率，佔其磁碟 IOPS 限制的百分比。這與磁碟 IOPS DiskIopsUtilization 的使用率超出檔案伺服器可處理的最大值，與佈建的磁碟 IOPS 不同。此量度中會考慮所有流量，包括背景工作 (例如分層和備份)。 SnapMirror每分鐘會針對每個檔案系統的檔案伺服器發出一個量度。 Average統計值是指定期間內指定檔案伺服器的平均磁碟 IOPS 使用率。 Minimum統計資料是指定期間內指定檔案伺服器中最低的磁碟 IOPS 使用率。 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。 單位：百分比 有效統計資料：AverageMinimum、和 Maximum

指標	描述
FileServerCacheHitRatio	每個 HA 配對 (例如 HA 配對中的作用中檔案伺服器)，由位於檔案系統 RAM 或 NVMe 快取中的資料所提供的所有讀取要求的百分比。較高的百分比表示快取讀取與總讀取的比例越高。將所有 I/O 納入考量，包括背景工作 (例如 SnapMirror，分層和備份)。每分鐘會針對每個檔案系統的檔案伺服器發出一個量度。 單位：百分比 Average統計資料是指定期間內，其中一個檔案系統 HA 配對的平均快取命中率。 Minimum統計資料是指定期間內，其中一個檔案系統 HA 配對的最低快取命中率。 Maximum統計資料是指定期間內，其中一個檔案系統 HA 配對的最高快取命中率。 有效統計資料：Average、Minimum、和 Maximum

磁碟 I/O 測量結果

所有這些量度都採用兩個維度，FileSystemId和Aggregate。

- FileSystemId— 檔案系統的 AWS 資源 ID。
- Aggregate— 檔案系統的效能層由稱為彙總的多個儲存集區組成。每個 HA 對都有一個彙總。例如，彙總對aggr1映至 HA 配對中的檔案伺服器 FsxId01234567890abcdef-01 (現用檔案伺服器) 和檔案伺服器 FsxId01234567890abcdef-02 (次要檔案伺服器)。

指標	描述
DiskReadBytes	從磁盤讀取的字節數（磁盤 IO）從此聚合中讀取。此量度中會考慮所有流量，包括背景工作

指標	描述
	(例如分層和備份)。 SnapMirror每分鐘會針對每個檔案系統的彙總發出一個量度。 Sum統計資料是指定期間內，從指定彙總每分鐘讀取的位元組總數。 Average統計值是指定期間內，從指定彙總每分鐘讀取的平均位元組數。 Minimum統計資料是指定期間內，從指定彙總每分鐘讀取的位元組數目下限。 Maximum統計資料是指定期間內，從指定彙總每分鐘讀取的位元組數目上限。 若要計算任何統計資料的讀取磁碟輸送量 (每秒位元組數)，請將統計值除以期間中的秒數。 單位：位元組 有效統計資料：SumAverage、Minimum、和 Maximum

指標	描述
DiskWriteBytes	從任何磁碟寫入此彙總的位元組數 (磁碟 IO)。此量度中會考慮所有流量，包括背景工作 (例如分層和備份)。 SnapMirror每分鐘會針對每個檔案系統的彙總發出一個量度。 Sum統計資料是指定期間內寫入給定彙總的位元組總數。 Average統計資料是指定期間內，每分鐘寫入指定彙總的平均位元組數。 Minimum統計資料是指定期間內，每分鐘寫入指定彙總的最低位元組數。 Maximum統計資料是指定期間內，每分鐘寫入指定彙總的最多位元組數。 若要計算任何統計值的寫入磁碟輸送量 (每秒位元組數)，請將統計值除以指定期間內的秒數。 單位：位元組 有效統計資料：SumAverage、Minimum、和 Maximum

指標	描述
DiskIopsUtilization	一個彙總的磁碟 IOPS 使用率，佔彙總磁碟 IOPS 限制的百分比 (亦即，檔案系統的 IOPS 總計除以您檔案系統的 HA 配對數目)。這與之不同之處FileServerDiskIops Utilization 在於，佈建磁碟 IOPS 對佈建 IOPS 限制的使用率，而不是檔案伺服器支援的最大磁碟 IOPS (亦即，由每個 HA 配對設定的輸送量容量決定)。此量度中會考慮所有流量，包括背景工作 (例如分層和備份)。 SnapMirror每分鐘會針對每個檔案系統的彙總發出一個量度。 Average統計值是指定期間內指定彙總的平均磁碟 IOPS 使用率。 Minimum統計值是指定期間內指定彙總的最低磁碟 IOPS 使用率。 Maximum統計資料 ii 指定期間內指定彙總的最高磁碟 IOPS 使用率。 單位：百分比 有效統計資料：AverageMinimum、和 Maximum

指標	描述
DiskReadOperations	此彙總的讀取作業 (磁碟 IO) 數目。此量度中會考慮所有流量，包括背景工作 (例如分層和備份)。 SnapMirror每分鐘會針對每個檔案系統的彙總發出一個量度。 Sum統計資料是指定彙總在指定期間內執行的讀取作業總數。 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作業數。 Minimum統計資料是指定彙總在指定期間內，每分鐘執行的讀取作業數目下限。 Maximum統計資料是指定彙總在指定期間內，每分鐘執行的最多讀取作業數目。 若要計算期間內的平均磁碟 IOPS，請使用Average統計值並將結果除以 60 (秒)。 單位：計數 有效統計資料：SumAverage、Minimum、和Maximum

指標	描述
DiskWriteOperations	此彙總的寫入作業 (磁碟 IO) 數目。此量度中會考慮所有流量，包括背景工作 (例如分層和備份)。 SnapMirror每分鐘會針對每個檔案系統的彙總發出一個量度。 Sum統計資料是指定彙總在指定期間內執行的寫入作業總數。 Average統計值是指定彙總在指定期間內，每分鐘執行的寫入作業平均數目。 若要計算期間內的平均磁碟 IOPS，請使用Average統計值並將結果除以 60 (秒)。 單位：計數 有效的統計數據：Sum和 Average

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。詳細的檔案系統量度具有FileSystemIdStorageTier、和DataType維度或FileSystemId、StorageTierDataType、和Aggregate維度。

- 未提供Aggregate維度時，量度會用於整個檔案系統。StorageUsed和指StorageCapacity標每分鐘都有一個資料點，對應於檔案系統的總使用儲存體 (每個儲存層) 和總儲存容量 (針對 SSD 層)。同時，StorageCapacityUtilization量度每分鐘會針對每個彙總發出一個量度。
- 提供Aggregate維度時，測量結果會針對每個彙總。

尺寸的含義如下：

- FileSystemId— 檔案系統的 AWS 資源 ID。
- Aggregate— 檔案系統的效能層由稱為彙總的多個儲存集區組成。每個 HA 對都有一個彙總。例如，彙總對aggr1映至 HA 配對中的檔案伺服器 FsxId01234567890abcdef-01 (現用檔案伺服器) 和檔案伺服器 FsxId01234567890abcdef-02 (次要檔案伺服器)。

- StorageTier— 指出量度所測量的儲存層，可能的值為SSD和StandardCapacityPool。
- DataType— 指出量度所測量的資料類型，以及可能的值All。

指定量度和維度索引鍵值配對的每個唯一組合都會有一個資料列，其中包含該組合測量結果的說明。

指標	描述
StorageCapacityUtilization	指定檔案系統彙總的儲存容量使用率。每分鐘會針對每個檔案系統的彙總發出一個量度。 Average統計值是指定期間內指定彙總的平均儲存容量使用量。 Minimum統計資料是指定期間內指定彙總的最小儲存容量使用量。 Maximum統計資料是指定期間內指定彙總的最大儲存容量使用量。 單位：百分比 有效統計資料：AverageMinimum、和Maximum
StorageCapacity	指定檔案系統彙總的儲存容量。每分鐘會針對每個檔案系統的彙總發出一個量度。 Average統計資料是指定期間內指定彙總的平均儲存容量。 Minimum統計資料是指定期間內指定彙總的最小儲存容量。 Maximum統計資料是指定期間內指定彙總的最大儲存容量。 單位：位元組

指標	描述
	有效統計資料：AverageMinimum、和 Maximum
StorageUsed	已使用的實體儲存容量 (位元組)，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 是SSD和StandardCapacityPool ，對應於此測量結果所測量的儲存層。每分鐘會針對每個檔案系統的彙總發出一個量度。 Average統計資料是指定期間內指定彙總在指定儲存層上使用的平均實體儲存容量。 Minimum統計資料是指定期間內指定彙總在指定儲存層上使用的實體儲存體容量下限。 Maximum統計資料是指定期間內指定彙總在指定儲存層上使用的實體儲存體容量上限。 單位：位元組 有效統計資料：AverageMinimum、和 Maximum

磁碟區指標

您的 Amazon FSx 適用於 NetApp ONTAP 檔案系統可以有一個或多個磁碟區來儲存您的資料。每個磁碟區都有一組量度，分類為「磁碟區」度量或「詳細的磁碟區」指標。

- 磁碟區指標是採用兩個維度的每個磁碟區效能和儲存指標，以FileSystemId及VolumeId。FileSystemId對映至磁碟區所屬的檔案系統。
- 詳細的磁碟區 per-storage-tier 指標是用來測量每層儲存體使用量的量StorageTier度 (可能值為SSD和StandardCapacityPool)，以及每個資料類型的DataType維度 (可能值為UserSnapshot、和Other)。這些量度具有FileSystemIdVolumeId、StorageTier、和DataType維度。

主題

網路 I/O 指標

所有這些量度都採用兩個維度，FileSystemId和VolumeId。

指標	描述
DataReadBytes	從屬端從磁碟區讀取的位元組數 (網路 I/O)。 Sum統計值是指定期間內與讀取作業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統計值除以指定期間內的秒數。 單位：位元組 有效的統計資訊：Sum
DataWriteBytes	從屬端寫入磁碟區的位元組數 (網路 I/O)。 Sum統計資料是指定期間內與寫入作業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統計值除以指定期間內的秒數。 單位：位元組 有效的統計資訊：Sum
DataReadOperations	從屬端在磁碟區上讀取作業 (網路 I/O) 的數目。 Sum統計值是指定期間內的讀取作業總數。若要計算一段期間內每秒的平均讀取作業，請將Sum統計值除以指定期間內的秒數。

指標	描述
	單位：計數 有效的統計資訊：Sum
DataWriteOperations	從屬端在磁碟區上執行的寫入作業 (網路 I/O) 數目。 Sum統計值是指定期間內的寫入作業總數。若要計算一段期間內每秒的平均寫入作業，請將Sum統計值除以指定期間內的秒數。 單位：計數 有效的統計資訊：Sum
MetadataOperations	從屬端至磁碟區之中繼資料活動的 I/O 作業 (網路 I/O) 數目。 Sum統計資料是指定期間內的中繼資料作業總數。若要計算一段期間內每秒的平均中繼資料作業，請將Sum統計值除以指定期間內的秒數。 單位：計數 有效的統計資訊：Sum
DataReadOperationTime	從用戶端存取磁碟區中資料的讀取作業 (網路 I/O) 在磁碟區內花費的總時間總和。 Sum統計值是指定期間內讀取作業所花費的總秒數。若要計算一段期間Sum的平均讀取延遲，請將Sum統計值除以同一期間內的DataReadOperations 指標。 單位：秒 有效的統計資訊：Sum

指標	描述
DataWriteOperationTime	磁碟區內用於完成從屬端存取磁碟區中資料的寫入作業 (網路 I/O) 所花費的總時間總和。 Sum統計值是指定期間內寫入作業所花費的總秒數。若要計算一段期間Sum的平均寫入延遲，請將Sum統計值除以同一期間內的DataWriteOperations 度量。 單位：秒 有效的統計資訊：Sum
MetadataOperationTime	從用戶端存取磁碟區中資料的中繼資料作業 (網路 I/O)，在磁碟區內花費的總時間總和。 Sum統計值是指定期間內讀取作業所花費的總秒數。若要計算一段期間Sum的平均延遲時間，請將Sum統計值除以相同期間的。MetadataOperations 單位：秒 有效的統計資訊：Sum
CapacityPoolReadBytes	從磁碟區的容量集區層讀取 (網路 I/O) 的位元組數目。 為確保資料完整性，ONTAP 會在執行寫入作業後，立即在容量集區上執行讀取作業。 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統計值除以指定期間內的秒數。 單位：位元組 有效的統計資訊：Sum

指標	描述
CapacityPoolReadOperations	磁碟區容量集區層的讀取作業 (網路 I/O) 數目。這會轉換為容量集區讀取要求。 為確保資料完整性，ONTAP 會在執行寫入作業後，立即在容量集區上執行讀取作業。 Sum統計資料是指定期間內，磁碟區容量集區層的讀取作業總數。若要計算每秒的容量集區要求，請將Sum統計值除以指定期間內的秒數。 單位：計數 有效的統計資訊：Sum
CapacityPoolWriteBytes	寫入磁碟區容量集區層的位元組數 (網路 I/O)。 為確保資料完整性，ONTAP 會在執行寫入作業後，立即在容量集區上執行讀取作業。 Sum統計資料是指定期間內寫入磁碟區容量集區層的位元組總數。若要計算每秒的容量集區位元組，請將Sum統計值除以指定期間內的秒數。 單位：位元組 有效的統計資訊：Sum

指標	描述
CapacityPoolWriteOperations	容量集區層對磁碟區的寫入作業 (網路 I/O) 數目。這轉換為寫入請求。 為確保資料完整性，ONTAP 會在執行寫入作業後，立即在容量集區上執行讀取作業。 Sum統計資料是指定期間內磁碟區容量集區層的寫入作業總數。若要計算每秒的容量集區要求，請將Sum統計值除以指定期間內的秒數。 單位：計數 有效的統計資訊：Sum

儲存容量指標

所有這些量度都採用兩個維度，FileSystemId和VolumeId。

指標	描述
StorageCapacity	磁碟區的大小 (以位元組為單位)。 單位：位元組 有效的統計資訊：Maximum
StorageUsed	磁碟區的已使用邏輯儲存容量。 單位：位元組 有效統計資料：AverageMinimum、和Maximum
StorageCapacityUtilization	磁碟區的儲存容量使用率。 單位：百分比 有效的統計資訊：Average

指標	描述
FilesUsed	磁碟區上使用的檔案 (檔案數目或 inode)。 單位：計數 有效統計資料：AverageMinimum、和Maximum
FilesCapacity	可在磁碟區上建立的 Inode 總數。 單位：計數 有效的統計資訊：Maximum

詳細的音量指標

詳細的磁碟區指標採用的維度比容量指標更多，因此能夠對資料進行更精細的測量。所有詳細的磁碟區量度都有維度FileSystemIdVolumeIdStorageTier、、和DataType。

- StorageTier維度會指出量度所測量的儲存層，可能的值為AllSSD、和StandardCapacityPool。
- DataType維度會指出量度所測量的資料類型，可能的值為AllUser、Snapshot、和Other。

下表定義所列維度的StorageUsed量度測量結果。

指標	描述
StorageUsed	使用的邏輯空間量，以位元組為單位。此量度會根據此量度使用的維度，測量不同類型的空間消耗量。當設定StorageTier 為SSD或StandardCapacityPool ，並設定DataType為時All，此量度會分別測量 SSD 和容量集區層之此磁碟區的邏輯空間使用量。將DataType維度設為、或UserSnapshot，並將設定StorageTier 為時 OtherAll，此測量結果會測量每個個別資料

指標	描述
	類型的邏輯空間使用狀況。資Snapshot料消耗包括快照保留，預設為磁碟區大小的 5%。 單位：位元組 有效統計資料：AverageMinimum、和Maximum
StorageCapacityUtilization	磁碟區已使用實體磁碟空間的百分比。 單位：百分比 有效的統計資訊：Maximum

效能警告與建議

每當其中一個 CloudWatch 量度接近或超過多個連續資料點的預定臨界值時，FSx for ONTAP 就會針對量度顯示警告。這些警告為您提供可行的建議，您可以使用這些建議來最佳化檔案系統的效能。

您可以在監視與效能儀表板的數個區域存取警告。所有使用中或最近的 Amazon FSx 效能警告，以及為處於 CloudWatch 警示狀態的檔案系統設定的任何警示，都會顯示在「摘要」區段的「監控與效能」面板中。警告也會顯示在顯示量度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 創建 Amazon CloudWatch 警報來監控 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，您可以使用這些建議來優化檔案系統的效能。這些建議描述了如何解決潛在的性能瓶頸. 如果您希望活動繼續進行，或者它會對檔案系統效能造成影響，則可以採取建議的動作。視觸發警告的測量結果而定，您可以增加檔案系統的傳輸量容量或儲存體容量來解決此問題，如下表所述。

儀表板區段	如果此量度有警告	執行此作業
儲存	主要儲存容量使用率	如果您的檔案系統尚未達到最大 SSD 儲存容量，請增加檔案系統的主要儲存容量。如需詳細資訊，請參閱 修改 SSD 儲存容量和佈建的 IOPS。

儀表板區段	如果此量度有警告	執行此作業
		如果您的檔案系統具有多個 HA 配對，而您的主要儲存容量使用率僅較高的檔案系統彙總子集 (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，讓您的主要儲存容量使用率更均勻地分散在檔案系統中。如需重新平衡工作負載的詳細資訊，請參閱監控 FSx 以取得 ONTAP 工作負載平衡。
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，請參閱如何修改輸送量容量。 如果您的檔案系統具有多個 HA 配對，而且只有一部分檔案伺服器的使用率很高，您也可以重新平衡工作負載，讓工作負載更均勻地利用每個檔案系統 HA 配對的效能能力。如需重新平衡工作負載的詳細資訊，請參閱監控 FSx 以取得 ONTAP 工作負載平衡。
	磁碟輸送量	
	磁碟 IOPS	
	CPU 使用率	
磁碟效能	磁碟 IOPS	如果您的檔案系統尚未達到檔案系統目前輸送量容量的最大 SSD IOPS，請增加 SSD IOPS。如需更新檔案系統佈建 IOPS 的詳細資訊，請參閱修改 SSD 儲存容量和佈建的 IOPS。 如果您的檔案系統具有多個 HA 配對，而您的磁碟 IOPS 使用率只有較高的檔案系統彙總子集 (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均勻地利用磁碟 IOPS。如需重新平衡工作負載的詳細資訊，請參閱監控 FSx 以取得 ONTAP 工作負載平衡。

如需檔案系統效能的詳細資訊，請參閱適用於 NetApp ONTAP 性能的 Amazon FSx。

創建 Amazon CloudWatch 警報來監控 Amazon FSx

您可以建立 CloudWatch 警示，在警示狀態變更時傳送 Amazon 簡單通知服務 (Amazon SNS) 訊息。警示會在您指定的期間監看單一指標。如有需要，警示會根據指定臨界值在數個期間內，根據指定臨界值的量度值執行一或多個動作。此動作是傳送到 Amazon SNS 主題或 Auto Scaling 政策的通知。

警示只會呼叫持續狀態變更的動作。 CloudWatch 警報不會只因為處於特定狀態而叫用動作；狀態必須已變更並維持指定數目的期間。您可以從 Amazon FSx 主控台或 Amazon 主控台建立警示。CloudWatch

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/。
2. 在左側導覽窗格中，選擇 [檔案系統]，然後選擇您要建立警示的檔案系統。
3. 在 [摘要] 頁面上，從第二個面板中選擇 [監視與效能]。
4. 選擇 [CloudWatch 鬧鐘] 索引標籤。
5. 選擇 [建立 CloudWatch 鬧鐘]。您會被重新引導至 CloudWatch 主控台。
6. 選擇選取指標。
7. 在「測量結果」段落中，選擇 FSx。
8. 選擇量度類別：
   - 檔案系統度量
   - 詳細的檔案系統度量
   - 體積指標
   - 詳細磁碟區指標
9. 選擇您要設定鬧鐘的量度，然後選擇 [選取量度]。
10. 在 [條件] 區段中，選擇您想要的鬧鐘條件，然後選擇 [下一步]。

> **Note**
>
> 在檔案系統維護期間，可能不會發佈量度。若要避免不必要且誤導性的警示情況變更，並設定警示以便對遺失的資料點有彈性，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。

11. 如果您想 CloudWatch 要在警示狀態啟動動作時傳送電子郵件或 Amazon SNS 通知給您，請為警示狀態觸發選擇警示狀態。

對於「傳送通知至下列 SNS 主題」，請選擇一個選項。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. 填入 [警示名稱] 和 [警示說明] 欄位，然後選擇 [下一步]。
13. 在 [預覽並建立] 頁面上，檢閱您即將建立的鬧鐘，然後選擇 [建立鬧鐘]。

使用 CloudWatch 主控台設定鬧鐘

1. 開啟主 CloudWatch 控台，網址為 https://console.aws.amazon.com/cloudwatch/。
2. 選擇 [建立警示] 以啟動 [建立警示精靈]。
3. 遵循使用 Amazon FSx 主控台設定警示中的程序，從步驟 6 開始。

若要使用設定鬧鐘 AWS CLI

- 呼叫放置量度警示 CLI 命令。如需詳細資訊，請參閱 AWS CLI 命令參考。

若要使用 CloudWatch API 設定警示

- 呼叫PutMetric警示 API 作業。如需詳細資訊，請參閱 Amazon CloudWatch API 參考資料。

監控 FSx 以取得 ONTAP 工作負載平衡

如果您的檔案系統具有多個 HA 配對，則其效能和輸送量會分散到每個 HA 配對中。FSx for ONTAP 會在檔案寫入檔案系統時自動平衡檔案，但在極少數情況下，您的工作負載資料或 I/O 可能會在 HA 配對之間失衡，進而影響工作負載的整體效能。您可以監控工作負載，以確保工作負載在每個檔案系統的 HA 配對 (及其相稱的檔案伺服器和彙總 — 組成主要儲存層的儲存池) 之間保持平衡。

主題

主要儲存使用率平衡

檔案系統的主要儲存容量會在儲存池中的每個 HA 配對之間平均分配，稱為彙總。每個 HA 對都有一個彙總。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 配對的檔案系統，建議您保持每個彙總的平均使用率高達 80%。

維持 80% 的使用率可確保有可用空間用於新的傳入資料，並為維護作業維護維護保持良好的額外負荷，這可以暫時在您的彙總上宣告可用空間。

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 (相當地增加每個彙總的儲存容量)，或者您可以使用 ONTAP CLI 中的磁碟區移動指令，在彙總之間移動磁碟區。

檔案伺服器與磁碟效能使用不平衡

檔案系統的整體效能能力 (例如網路輸送量、檔案伺服器到磁碟輸送量以及 IOPS，以及磁碟 IOPS) 會在檔案系統的 HA 配對中平均劃分。我們建議您將所有效能限制的平均使用率維持在 50% 以下 (最高尖峰使用率低於 80%)，這適用於所有 HA 配對的檔案系統檔案伺服器資源的整體使用率，以及依每個檔案伺服器為基礎。

如果您發現檔案伺服器效能使用率不平衡，而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 進一步診斷效能失衡的原因並加以修復。以下是可能的不平衡指標和進一步診斷的下一步步驟的表。

如果您的文件系統的...	Then...
檔案伺服器磁碟輸送量或檔案伺服器磁碟 IOPS 不平衡	您可能遇到 HA 配對子集 (包含存取大量資料的磁碟區子集) 上的 I/O 熱檢查，這可能會限制工作負載的整體效能，因為它對 HA 配對子集產生瓶頸。對於每個高度使用的檔案伺服器，請檢查使用率最高的磁碟區，以查看彙總中哪些磁碟區的活動最多。如需此程序的詳細資訊，請參閱重新平衡高度使用的磁碟區。

如果您的文件系統的...	Then...
網路輸送量不平衡，但檔案伺服器磁碟輸送量、檔案伺服器磁碟 IOPS 或磁碟 IOPS 並未失衡	您的數據均勻分佈在 HA 對之間，但您的客戶不是。對於比其他伺服器具有更多網路輸送量使用率的檔案伺服器，請檢查每部檔案伺服器的常用用戶端，然後從這些用戶端卸載任何磁碟區，然後使用不同 HA 配對上的不同端點重新掛載，以重新平衡這些用戶端。如需此程序的詳細資訊，請參閱重新平衡高流量用戶端。

將 CloudWatch 維度對應至 ONTAP CLI 和其餘 API 資源

您的向外延展檔案系統具有`FileServer`或`Aggregate`維 CloudWatch 度的 Amazon 指標。若要進一步診斷不平衡的情況，您需要將這些維度值對應至特定的檔案伺服器 (或節點)，並在 ONTAP CLI 或 REST API 中進行彙總。

- 對於檔案伺服器，每個檔案伺服器名稱都會對應到 ONTAP 中的檔案伺服器 (或節點) 名稱 (例如，`FsxId01234567890abcdef-01`)。奇數的檔案伺服器是偏好的檔案伺服器 (也就是說，除非檔案系統已容錯移轉至次要檔案伺服器，否則它們會提供流量服務)，而偶數的檔案伺服器則是次要檔案伺服器 (也就是說，它們僅在其合作夥伴無法使用時才提供流量)。因此，次要檔案伺服器的使用率通常會比慣用的檔案伺服器少。
- 對於彙總，每個彙總名稱都會對應至 ONTAP 中的彙總 (例如，`aggr1`)。每個 HA 配對都有一個彙總，表示彙總`aggr1`由檔案伺服器 `FsxId01234567890abcdef-01` (使用中檔案伺服器) 共用，而 HA 配對中的 `FsxId01234567890abcdef-02` (次要檔案伺服器) 共用彙總，彙總`aggr2`會由檔案伺服器`FsxId01234567890abcdef-03`共用`FsxId01234567890abcdef-04`，依此類推。

您可以使用 ONTAP CLI 檢視所有彙總與檔案伺服器之間的對應。

1. 若要使用 SSH 連線到檔案系統的 NetApp ONTAP CLI，請依照 Amazon FSx 適用於 NetApp ONTAP 使用者指南一使用 NetApp ONTAP CLI節中所述的步驟進行操作。

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. 使用存儲聚合 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.
```

重新平衡高流量用戶端

如果您遇到跨檔案伺服器的 I/O 不平衡 (特別是網路輸送量使用率)，可能是造成高 I/O 用戶端的原因。若要識別高流量的用戶端，請使用 ONTAP CLI。

1. 若要使用 SSH 連線到檔案系統的 NetApp ONTAP CLI，請依照 Amazon FSx 適用於 NetApp ONTAP 使用者指南一使用 NetApp ONTAP CLI節中所述的步驟進行操作。

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. 若要檢視流量最高的用戶端，請使用統計資料常用的用戶端顯示 ONTAP CLI 命令。您可以選擇性地指定-node參數，只檢視特定檔案伺服器的常用用戶端。如果您要診斷特定檔案伺服器的不平衡狀況，請使用-node參數，取代node_name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，提供輸出每個報表之前測量的間隔 (以秒為單位)。增加間隔 (例如，最大 300 秒) 可為每個磁碟區驅動的流量提供較長期的樣本。預設值為 5 (秒)。

   ```
   ::> statistics top client show -node FsxId01234567890abcdef-01 [-interval [5,300]]
   ```

   在輸出中，排名前的用戶端會依其 IP 位址和連接埠顯示。

   ```
                                                    *Total     Total
               Client   Vserver          Node           Ops     (Bps)
   ------------------- --------- ------------------------- ------ ---------
    172.17.236.53:938 svm01     FsxId01234567890abcdef-01   2143 140443648
   172.17.236.160:898 svm02     FsxId01234567890abcdef-01    812  53215232
   ```

3. 您可以將列出的高流量用戶端子集重新平衡至其他檔案伺服器。若要這麼做，請從用戶端卸載磁碟區，然後使用 SVM 的 NFS/SMB 端點的 DNS 名稱重新掛接磁碟區 — 這會傳回與隨機 HA 配對對應的隨機端點。

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裝載的 HA 配對。為了確保您正在將用戶端掛載到不同的端點，您可以改為指定與傳輸高流量之節點對應的端點 IP 位址不同的端點 IP 位址。您可以執行下列命令來執行此作業：

```
::> 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`命令的示例輸出，客戶端`172.17.236.53`正在驅動高流量`FsxId01234567890abcdef-01`。`network interface show`命令的輸出表示這是地址`172.31.15.89`。若要裝載到不同的端點，請選取任何其他位址 (在此範例中，唯一的其他位址是`172.31.8.112`對應的`FsxId01234567890abcdef-03`)。

重新平衡高度使用的磁碟區

如果您的磁碟區或彙總發生 I/O 不平衡，您可以重新平衡磁碟區，以便在磁碟區之間重新分配 I/O 流量。

> **Note**
>
> 如果您在整個彙總中遇到儲存使用率不平衡，除非高使用率加上 I/O 不平衡，否則通常不會對效能造成任何影響。雖然您可以在彙總之間移動磁碟區以平衡儲存使用率，但我們建議您只在發現效能影響時移動磁碟區，因為如果您不同時考慮將 I/O 導向到考慮移動的每個磁碟區，則移動磁碟區可能會對效能造成不利影響。

1. 若要使用 SSH 連線到檔案系統的 NetApp ONTAP CLI，請依照 Amazon FSx 適用於 NetApp ONTAP 使用者指南一使用 NetApp ONTAP CLI節中所述的步驟進行操作。

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. 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，並進行下列變更：

- 以*#####*取代彙總名稱 (例如，)。aggr1
- 您可以選擇性地新增-interval參數，提供輸出每個報表之前測量的間隔 (以秒為單位)。增加間隔 (例如，最大 300 秒) 可為每個磁碟區驅動的流量提供較長期的樣本。預設值為 5 (秒)。

```
::> statistics volume show -aggregate aggregate_name -sort-key total_ops [-interval
 [5,300]]
```

視您選擇的間隔而定，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，以及導向每個彙總的流量。

```
                          *Total Read Write Other      Read Write Latency
    Volume Vserver Aggregate    Ops  Ops   Ops   Ops     (Bps) (Bps)    (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
```

磁碟區統計資料會以每個組成部分為基礎顯示 (例如，vol1__0015是的第 15 個組成部分 FlexGroupvol1)。您可以從示例輸出中看到，的成分比成aggr1分股的利用率更高。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，以便更均勻地分佈流量。

3. 若要在彙總之間移動磁碟區，請使用磁碟區移動開始 ONTAP CLI 命令，取代下列值：

- 將 *svm_name* 取代為裝載您要移動之磁碟區之 SVM 的名稱。
- 將磁*####*取代為磁碟區構成的名稱 (例如，)。vol1__0001
- 將*####*取代為磁碟區的目標彙總名稱。

> **Important**
>
> 磁碟區移動會耗用來源和目標檔案伺服器的網路和磁碟資源。因此，任何進行中的磁碟區移動都可能會影響工作負載的效能。此外，磁碟區移動程序還有一個截止階段，會暫時暫停磁碟區的任何流量 I/O。

```
::> volume move start -vserver svm_name -volume volume_name -
destination 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.
```

若要檢查磁碟區移動作業的狀態，請使用 `volume move show` ONTAP CLI 指令。

```
::> 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: aggr2
                            Source Node: FsxId01234567890abcdef-01
                             Move State: healthy
```

此指令會將完成移動的估計時間顯示為其中一個資訊欄位。操作完成後，相同的命令將顯示該`Move Phase`字段已完成。

您應該確保每個聚合FlexGroup均勻分佈在聚合中，理想情況下，每個聚合使用推薦的 8 個成分。如果您將一個構成磁碟區移至另一個彙總以達到否則平衡FlexGroup，則應依次將另一個 (使用率較低) 的組成磁碟區移至來源彙總，以維持平衡。

監控 FSx 的安裝管理體系管理系統事件

您可以使用 NetApp ONTAP 的原生事件管理系統 (EMS) 來監控 FSx 中是否有 ONTAP 檔案系統事件。您可以使用 NetApp ONTAP CLI 檢視這些事件。

主題

- EMS 活動概要
- 檢視 EMS 事件
- EMS 事件轉寄至系統日誌伺服器

EMS 活動概要

EMS 事件會自動產生通知，在 ONTAP 檔案系統的 FSx 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，例如儲存區虛擬機器 (SVM) 驗證問題或完整磁碟區。

依預設，事件會記錄在事件管理系統記錄檔中。使用 EMS，您可以監控事件，例如使用者密碼變更、FlexGroup 接近完整容量的組成部分、手動上線或離線的邏輯單位編號 (LUN)，或是磁碟區自動調整大小。

如需更多關於 ONTAP EMS 事件的資訊，請參閱 ONTAP 管理系統文件中心的 NetApp ONTAP EMS 參考文件。若要顯示事件類別，請使用文件左側的導覽窗格。

> **Note**
>
> 在 ONTAP 檔案系統中，只有某些 ONTAP EMS 訊息可供 FSx 使用。若要檢視可用的 ONTAP EMS 訊息清單，請使用 NetApp ONTAP CLI 事件目錄顯示命令。

EMS 事件描述包含事件名稱、嚴重性、可能原因、記錄訊息和更正動作，可協助您決定如何回應。例如，自動調整磁碟區大小失敗時，就會發生 WAFL.VOL.AutoSize 事件。根據事件描述，更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 事件日誌顯示命令來顯示事件日誌的內容。如果您在檔案系統上具有該fsxadmin角色，則可以使用此指令。命令語法如下：

```
event log show [event_options]
```

最近的事件會先列出。依預設，此命令會顯示EMERGENCYALERT、和ERROR嚴重性層級事件，其中包含下列資訊：

- 時間 — 事件的時間。
- 節點 — 發生事件的節點。
- 嚴重性 — 事件的嚴重性層級。若要顯示NOTICEINFORMATIONAL、或DEBUG嚴重性層級事件，請使用選項-severity。
- 事件 — 事件名稱和訊息。

若要顯示有關事件的詳細資訊，請使用下表中列出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的事件資訊。
-instance	顯示有關所有欄位的詳細資訊。
-node *nodename*|local	顯示您指定之節點的事件清單。搭配使用此選項-seqnum可顯示詳細資訊。
-seqnum *sequence_number*	選取順序中符合此數字的事件。搭配使用-node可顯示詳細資訊。
-time *MM/DD/YYYY HH:MM:SS*	選取在此特定時間發生的事件。使用格式：毫米/日/年高：

事件選項	描述

	毫米：SS [+-高：毫米]。您可以在兩個 time 陳述式之間使用 `..` 運算子來指定時間範圍。
	
	`event log show -time "04/17/2023 05:55:00".."04/17/2023 06:10:00"`
	
	比較時間值與執行指令時的目前時間相關。下列範例顯示如何只顯示最後一分鐘內發生的事件：
	
	`event log show -time >1m`
	
	此選項的月份和日期欄位不會填補零。這些欄位可以是單一數字；例如，`4/1/2023 06:45:00`。

事件選項	描述
-severity *sev_level*	選取符合 *sev_level* 值的事件，該值必須為下列其中一項： • EMERGENCY — 中斷 • ALERT— 單點故障 • ERROR— 降解 • NOTICE— 資訊 • INFORMATIONAL — 資訊 • DEBUG— 調試信息 若要顯示所有事件，請依下列方式指定嚴重性： `event log show -severity <=DEBUG`

事件選項	描述
-ems-severity *ems_sev_level*	選取符合 *ems_sev_level* 值的事件，該值必須是下列其中一項： • NODE_FAULT — 偵測到資料損毀或節點無法提供用戶端服務。 • SVC_FAULT — 偵測到暫時性的服務中斷 (通常是暫時性軟體錯誤)。 • NODE_ERROR — 偵測到不是立即致命的硬體錯誤。 • SVC_ERROR — 偵測到不是立即致命的軟體錯誤。 • WARNING— 不表示錯誤的高優先順序訊息。 • NOTICE— 不表示錯誤的正常優先順序訊息。 • INFO— 不表示錯誤的低優先順序訊息。 • DEBUG— 偵錯訊息。 • VAR— 具有可變嚴重性的訊息，在執行時期選取。 若要顯示所有事件，請依下列方式指定嚴重性： `event log show -ems-severity <=DEBUG`
-source *text*	選取符合##值的事件。來源通常是軟體模組。

事件選項	描述
-message-name *message_name*	選取符合##名稱值的事件。郵件名稱具有描述性，因此依訊息名稱篩選輸出會顯示特定類型的訊息。
-event *text*	選取符合##值的事件。該字event段包含事件的全文，包括任何參數。
-kernel-generation-num *integer*	選取符合##值的事件。只有來自核心的事件才有核心產生編號。
-kernel-sequence-num *integer*	選取符合##值的事件。只有來自核心的事件才有核心序號。
-action *text*	選取符合##值的事件。此action欄位說明您必須採取哪些更正動作來補救這種情況(如果有的話)。
-description *text*	選取符合##值的事件。該description 字段描述了事件發生的原因以及它的含義。
-filter-name *filter_name*	選取符合#####值的事件。只有符合此值的現有篩選器所包含的事件才會顯示。
-fields *fieldname* ,...	指示命令輸出還包括指定的一個或多個字段。您可以使用-fields ?來選擇要指定的欄位。

若要檢視 EMS 事件

1. 若要使用 SSH 連線到檔案系統的 NetApp ONTAP CLI，請依照 Amazon FSx 適用於 NetApp ONTAP 使用者指南一使用 NetApp ONTAP CLI節中所述的步驟進行操作。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. 使用指event log show令顯示事件記錄檔的內容。

```
::> 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指令所傳回之 EMS 事件的相關資訊，請參閱 ONTAP 文件中心中的 NetApp ONTAP EMS 參考資料。

EMS 事件轉寄至系統日誌伺服器

您可以設定 EMS 事件，將通知轉寄給系統日誌伺服器。EMS 事件轉送可用於即時監控您的檔案系統，以判斷並隔離各種問題的根本原因。如果您的環境尚未包含用於事件通知的 Syslog 伺服器，則必須先建立一個伺服器。必須在檔案系統上設定 DNS，才能解析 Syslog 伺服器名稱。

設定 EMS 事件以將通知轉寄至系統日誌伺服器

1. 若要使用 SSH 連線到檔案系統的 NetApp ONTAP CLI，請依照 Amazon FSx 適用於 NetApp ONTAP 使用者指南一使用 NetApp ONTAP CLI節中所述的步驟進行操作。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. 使用事件通知目的地 create 命令來建立類型的事件通知目的地syslog，並指定下列屬性：

   - *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為：A-Z、a-z 或 0-9。
   - *syslog_name*— 系統日誌消息發送到的系統日誌服務器主機名或 IP 地址。

- *transport_protocol*— 用來傳送事件的通訊協定：
  - udp-unencrypted— 沒有安全性的用戶數據報協議。這是預設通訊協定。
  - tcp-unencrypted— 沒有安全性的傳輸控制協議。
  - tcp-encrypted— 具有傳輸層安全性（TLS）的傳輸控制協議。指定此選項時，ONTAP 的 FSx 會驗證目的地主機的憑證來驗證目的地主機的身分。
- *port_number*— 系統日誌消息被發送到的系統日誌服務器端口。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，則syslog-port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，預設連接埠會設定為514。

```
::> event notification destination create -name dest_name -syslog syslog_name -
syslog-transport transport_protocol -syslog-port port_number
```

3. 您可以使用事件通知 create 指令，針對事件篩選器所定義的一組事件建立新的通知通知通知，並指定下列屬性：
   - *node_name*— 事件篩選器的名稱。事件篩選器中包含的事件會轉寄至-destinations參數中指定的目的地。
   - *dest_name*— 將事件通知傳送至的現有通知目的地名稱。

```
::> event notification create -filter-name filter_name -destinations dest_name
```

4. 使用指event notification destination check令產生測試訊息，並確認您的設定是否正常運作。使用指令指定下列屬性：
   - *node_name*— 節點的名稱 (例如，FsxId07353f551e6b557b4-01)。
   - *dest_name*— 將事件通知傳送至的現有通知目的地名稱。

```
::> set diag
::*> event notification destination check -node node_name -destination-
name dest_name
```

使用雲端洞察進行監

NetApp 雲端洞察是一項 NetApp 服務，可用來監控 Amazon FSx 的 NetApp ONTAP 檔案系統以及其他 NetApp 儲存解決方案。透過 Cloud Insights，您可以監控一段時間內的組態、容量和效能指標，以了解工作負載的趨勢，並規劃 future 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建立警示。

> **Note**
>
> 向外延展檔案系統不支援雲端洞見。

雲端洞察提供：

- 廣泛的度量和記錄 — 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，瞭解您的工作負載趨勢。
- 使用者分析和勒索軟體防護 — 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 — 瞭解您的 SnapMirror 關係並設定複寫問題的警示。
- 容量規劃 — 瞭解內部部署工作負載的資源需求，以協助您將工作負載移轉至更有效率的 FSx 以進行 ONTAP 組態。您也可以使用這些見解來規劃何時需要更多的效能或容量來進行 ONTAP 部署的 FSx。

如需有關雲端洞見的詳細資訊，請參閱 NetApp 雲端中央上的NetApp 雲端洞察。

使用收穫和 Grafana 監控 FSx 的 ONTAP 文件系統

NetApp 收穫是一個開源工具，用於從 ONTAP 系統收集性能和容量指標，並與適用於 ONTAP 的 FSx 兼容。您可以將收穫與 Grafana 一起使用，以獲得開放原始碼監控解決方案。

開始使用豐收和 Grafana

以下部分詳細說明如何設定和設定 Harvest 和 Grafana，以測量 FSx 的 ONTAP 檔案系統效能和儲存容量使用率。

您可以使用收穫和 Grafana 監控您的 Amazon FSx 的 NetApp ONTAP 文件系統。 NetApp 收穫會從適用於 ONTAP 檔案系統的 FSx 收集效能、容量和硬體指標來監控 ONTAP 資料中心。Grafana 提供儀表板，可在其中顯示收集的「收穫」指標。

支援的收穫儀表

適用於 NetApp ONTAP 的 Amazon FSx 公開的指標組與現場部署 ONTAP 不同。 NetApp 因此，目前僅支援以下標記為的「 out-of-the-box 收穫」儀表板，以便與 FSx for ONTAP 搭配使用。`fsx`這些儀表板中的某些面板可能缺少不受支援的資訊。

- ONTAP：法規遵循
- ONTAP：資料保護快照
- ONTAP：安全性
- 開始：SVM
- 音量：音量

AWS CloudFormation 範本

若要開始使用，您可以部署 AWS CloudFormation 範本，以自動啟動執行豐收和 Grafana 的 Amazon EC2 執行個體。作為 AWS CloudFormation 範本的輸入，您可以為檔案系統指定`fsxadmin`使用者和 Amazon FSx 管理端點，這些端點將作為此部署的一部分新增。部署完成後，您可以登入 Grafana 儀表板來監控您的檔案系統。

此解決方案用 AWS CloudFormation 於自動化收穫和 Grafana 解決方案的部署。該模板創建一個 Amazon EC2 Linux 實例，並安裝收穫和 Grafana 軟件。若要使用此解決方案，請下載 FSX-收穫模板範 AWS CloudFormation 本。

> **Note**
>
> 實作此解決方案會產生相關 AWS 服務的費用。如需詳細資訊，請參閱這些服務的定價詳細資料頁面。

Amazon EC2 執行個體類型

設定範本時，您需要提供 Amazon EC2 執行個體類型。 NetApp執行個體大小的建議取決於您監視的檔案系統數量，以及您選擇收集的指標數量。使用預設組態時，針對您監視的每 10 個檔案系統，NetApp 建議：

- 中央處理器:2 核心
- 記憶體：1 GB

- 磁盤：500 MB（主要用於日誌文件）

以下是一些範例組態和您可能選擇的t3執行個體類型。

檔案系統	CPU	Disk	執行個體類型
10 歲以下	2 個核心	500 MB	t3.micro
10—40	4 個核心	千兆	t3.xlarge
40 歲以上	8 個核心	千兆	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。

執行個體埠規則

當您設定 Amazon EC2 執行個體時，請確定連接埠 3000 和 9090 已針對 Amazon EC2 收穫和 Grafana 執行個體所在的安全群組開放傳入流量。由於啟動的執行個體透過 HTTPS 連線到端點，因此需要解析端點，這需要連接埠 53 TCP/UDP 才能使用 DNS。此外，要到達端點，它需要端口 443 TCP 才能使用 HTTPS 和互聯網訪問。

部署程序

下列程序會設定並部署收成/Grafana 解決方案。部署大約需要五分鐘。在開始之前，您必須在您的 AWS 帳戶中的 Amazon 虛擬私有雲 (Amazon VPC) 中執行一個 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，請參閱為 ONTAP 檔案系統建立 FSx。

若要啟動收成/Grafana 解決方案堆疊

1. 下載 FSX-收穫模板模板 AWS CloudFormation 。如需有關建立 AWS CloudFormation 堆疊的詳細資訊，請參閱《使用指南》中的〈在 AWS CloudFormation 主控台上建立堆疊AWS CloudFormation〉。

   > **Note**
   >
   > 依預設，此範本會在美國東部 (維吉尼亞北部) AWS 區域啟動。您必須在提供 Amazon FSx 的 AWS 區域 位置啟動此解決方案。如需詳細資訊，請參閱.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加以修改。此解決方案使用下列預設值。

參數	預設	描述
InstanceType	`t3.micro`	Amazon EC2 實例類型。以下是實`t3`例類型。 • `t3.micro` • `t3.small` • `t3.medium` • `t3.large` • `t3.xlarge` • `t3.2xlarge` 如需此參數允許的 Amazon EC2 執行個體類型值的完整清單，請參閱 fsx-ontap-harvest-grafana .template。
KeyPair	無預設值	用來存取 Amazon EC2 執行個體的 key pair。
SecurityGroup	無預設值	收取/Grafana 執行個體的安全性群組識別碼。確保除了連接埠 53 和 443 以外的輸入連接埠 3000 和 9090，都是從您想要用來存取 Grafana 儀表板的用戶端開啟的。

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`。對必須連線到網際網`public`路的資源使用子網路，並為未連線至網際網路的資源使用私有子網路。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的子網路類型。
子網路	無預設值	針對 NetApp ONTAP 檔案系統的偏好子網路，指定與 Amazon FSx 相同的子網路。您可以在 Amazon FSx 主控台的 ONTAP 檔案系統詳細資訊頁面的「網路和安全」索引標籤中，找到檔案系統的偏好子網路 ID
LatestLinuxAmiId	`/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2`	在給定的 Amazon Linux 2 AMI 的最新版本 AWS 區域。
F SxEnd 點運算點	無預設值	檔案系統的管理端點 IP 位址。您可以在 Amazon FSx 主控台的 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 位址。
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提供的密碼。

3. 選擇下一步。

4. 在「選項」中選擇「下一步」
5. 對於「檢閱」，請檢閱並確認設定。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 AWS CloudFormation 主控台的 [狀態] 欄中檢視堆疊的狀態。您應該會在大約五分鐘內看到「建立 _ 完成」狀態。

登入 Grafana

部署完成後，使用瀏覽器登入 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，請參閱上的「 NetApp 收割」頁面 GitHub。

故障排除收穫和 Grafana

如果您遇到任何在 Harvest 和 Grafana 儀表板中提到的資料遺失，或是在使用 FSx 進行 ONTAP 設定 Harvest 和 Grafana 時遇到問題，請查看下列主題以取得潛在的解決方案。

主題

- SVM 和磁碟區儀表板為空白
- CloudFormation 堆棧在超時後回滾

SVM 和磁碟區儀表板為空白

如果 AWS CloudFormation 堆疊部署成功且可以聯絡 Grafana，但 SVM 和磁碟區儀表板為空白，請使用下列程序對環境進行疑難排解。您將需要 SSH 訪問 Amazon EC2 實例的收穫和 Grafana 部署在其上。

1. SSH 連接到您的收穫和 Grafana 客戶正在運行的 Amazon EC2 實例。

   ```
   [~]$ ssh ec2-user@ec2_ip_address
   ```

2. 使用以下命令打開harvest.yml文件並：

   - 驗證是否已針對 ONTAP 執行個體的 FSx 建立了一個項目。Cluster-2
   - 請確認使用者名稱和密碼的項目與您的認fsxadmin證相符。

```
[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密碼進行更新，如下所示：

```
[ec2-user@ip-ec2_ip_address ~]$ sudo vi /home/ec2-user/harvest_install/harvest/
harvest.yml
```

4. 請確定fsxadmin使用者認證以下列格式儲存在 Secrets Manager 中，以供 future 部署之用，並以您*fsxadmin_password*的密碼取代。

```
{"username" : "fsxadmin", "password" : "fsxadmin_password"}
```

CloudFormation 堆棧在超時後回滾

如果您無法成功部署 CloudFormation 堆疊，而且正在復原時發生錯誤，請使用下列程序來解決問題。您需要透過 SSH 存取 CloudFormation 堆疊部署的 EC2 執行個體。

1. 重新部署 CloudFormation 堆疊，確定已停用自動復原。
2. SSH 連接到您的收穫和 Grafana 客戶正在運行的 Amazon EC2 實例。

```
[~]$ ssh ec2-user@ec2_ip_address
```

3. 使用以下命令確認 docker 容器已成功啟動。

```
[ec2-user@ip-ec2_ip_address ~]$ sudo docker ps
```

在響應中，您應該看到五個容器，如下所示：

```
CONTAINER ID   IMAGE                    COMMAND                  CREATED
 STATUS                          PORTS                    NAMES
6b9b3f2085ef   rahulguptajss/harvest   "bin/poller --config…"   8 minutes ago
 Restarting (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 容器未運行，請按如下方式檢查/var/log/cloud-init-output.log文件中的故障。

```
[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/alertmanage
r", "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. 如果發生故障，請執行以下命令來部署收穫和 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. 通過運行sudo docker ps並連接到您的收穫和 Grafana 網址來驗證容器成功啟動。

使用 FSx 誌記錄用於 ONTAP API 調用AWS CloudTrail

亞馬遜 FSX 與AWS CloudTrail，是一種提供記錄使用者、角色或AWS服務在亞馬遜 FSX。 CloudTrail 捕獲亞馬遜 FSX 的所有亞馬遜 FSX API 調用 NetApp ONTAP 作為事件。已捕獲的呼叫包括從 Amazon FSx 主控台的呼叫，以及對 Amazon FSx API 操作的程式碼呼叫。

如果您建立追蹤，就可以啟用 CloudTrail 事件傳送至 Amazon S3 儲存儲體，包括 Amazon FSx 的事件。如果您不設定追蹤記錄，仍然可以透過 CloudTrail 主控台事件歷史記錄。使用 CloudTrail 所收集的資訊，可判斷向 Amazon FSx 提出了哪些請求。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

當您建立帳戶時，系統即會在 AWS 帳戶中啟用 CloudTrail。Amazon FSx 中發生 API 活動時，該活動會記錄在 CloudTrail 事件以及其他AWS中的服務事件事件歷史記錄。您可以檢視、搜尋和下載 AWS 帳戶的最新事件。如需詳細資訊，請參閱「」使用 CloudTrail 事件歷史記錄。

若要持續記錄AWS帳户（包括 Amazon FSx 事件），請建立線索。一個線索啟用 CloudTrail 將日誌檔案傳送至 Amazon S3 儲存儲體。根據預設，當您在主控台建立線索時，線索會套用到所有 AWS 區域。權杖會記錄來自 AWS 分割區中所有 AWS 區域的事件，然後將記錄檔案交付到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他AWS服務，以進一步分析和處理 CloudTrail 日誌。如需詳細資訊，請參閱《AWS CloudTrail 使用者指南》中的以下主題：

- 建立 AWS 帳戶 的追蹤

- AWS使用的服務整合 CloudTrail 日誌
- 設定 CloudTrail 的 Amazon SNS 通知
- 正在接收 CloudTrail 多個區域的日誌檔案和從多個帳戶接收 CloudTrail 記錄檔案

所有 Amazon FSxAPI 呼叫將由雲跟蹤記錄。例如，呼叫至`CreateFileSystem`和`TagResource`操作在 CloudTrail 日誌檔。

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

- 該請求是否透過根或 AWS Identity and Access Management (IAM) 使用者憑證來提出。
- 提出該要求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 該請求是否由另一項 AWS 服務提出。

如需詳細資訊，請參閱 。CloudTrail userIdentity 元素中的AWS CloudTrail使用者指南。

了解 Amazon FSx 日誌檔案項目

一個線索是一種配置，可讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存儲體。 CloudTrail 日誌檔案包含一個或多個日誌項目。同時事件表示來自任何來源的單一請求，並包含請求動作、動作的日期和時間、請求參數等資訊。 CloudTrail 日誌檔案並非依公有 API 呼叫追蹤記錄的堆疊排序，因此不會以任何特定順序出現。

以下範例顯示 CloudTrail 日誌項目，示範`TagResource`從主控台建立之檔案系統標籤時的操作。

```
{
    "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”
}
```

以下範例顯示 CloudTrail 日誌項目，示範UntagResource從主控台刪除之檔案系統標籤時的動作。

```
{
    "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"
}
```

配額

接下來，您可以在使用適用於 NetApp ONTAP 的 Amazon FSx 時瞭解配額的相關資訊。

主題

您可以提高的配額

以下是您可以增加的每 AWS 區域一個 NetApp AWS 帳戶 ONTAP 的 Amazon FSx 的配額。

資源	預設	描述
ONTAP 檔案系統	100	您可以在此帳戶中建立的 NetApp ONTAP 檔案系統的 Amazon FSx 數目上限。
ONTAPSSD 儲存容量	524,288	您可以在此帳戶中擁有的所有 Amazon FSx 適用於 NetApp ONTAP 檔案系統的固態硬碟儲存容量上限 (以 GiB 為單位)。
ONTAP輸送量容量	10,240	您可以在此帳戶中擁有的所有 Amazon FSx 適用於 NetApp ONTAP 檔案系統的最大輸送容量 (以 MBP 為單位)。
ONTAP固態硬碟 IOPS	1,000,000	您可以在此帳戶中擁有的所有 Amazon FSx 的 NetApp ONTAP 檔案系統的最大固態硬碟 IOPS 數量。
ONTAP每個檔案系統的備份	10,000	您可以在此帳戶中擁有的所有 Amazon FSx 適用於 NetApp

資源	預設	描述
		ONTAP 檔案系統的使用者啟動磁碟區備份數目上限。

請求提高配額

1. 開啟 AWS Support 頁面，若必要請登入，然後選擇 Create case (建立案例)。
2. 在 [建立案例] 中，選擇 [帳戶和帳單支援]。
3. 在案例詳細資料面板中，輸入下列項目：
   - 針對「類型」選擇「帳戶
   - 對於類別，選擇其他帳戶問題。
   - 對於主旨，請輸入**Amazon FSx for NetApp ONTAP service limit increase request**。
   - 提供您要求的詳細說明，包括：
     - 您要增加的 FSx 配額，以及您要增加的值 (如果知道的話)。
     - 為什麼你正在尋求增加配額的原因。
     - 您要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

下表列出一個中每個檔案系統之 Amazon FSx 的 NetApp ONTAP 資源配額。 AWS 區域

資源	每個檔案系統的限制
最低 SSD 儲存容量	每一對高可用性 (HA) 配對可用 1,024 GiB
最大 SSD 儲存容量	• 向外擴充：每個 HA 對 512 TiB，最高可達 1 個 PIB • 向上縮放：192 倍
最大固態硬碟 IOPS	向外擴充：

資源	每個檔案系統的限制
	• 每公頃對 20 萬 (最多 12 對) 向上擴展： • 160,000 個位置：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) • 在所有其他有提供 FSx 適用於 ONTAP 的 AWS 區域 情況下提供 80,000
最小輸送量容量	• 向外擴充：每個醫管局對 3,072 兆比特 • 向上擴充：128 兆倍
最大輸送量容量	向外擴充： • 1 兆比特 向上擴展： • 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) 的 4,096 MBps [2] • 在所有其他 AWS 區域 可用於 ONTAP 的 FSx 的情況下，具有 2,048 兆比特
磁碟區數目上限	• 向外擴充：1,000 • 向上擴充：500
快照數目上限	每筆磁碟區 3

資源	每個檔案系統的限制
最大備份數	第四卷 (每一卷)
SVM 的最大數量	向外擴充： • 5 向上擴展： • 6 (128 兆比特的輸送量容量) • 6 (256 兆比特的輸送量容量) • 14 (512 兆比特的輸送量容量) • 14 (1,024 兆比特的輸送量容量) • 24 (2,048 兆比特的輸送量容量) • 24 (4,096 兆比特的輸送量容量)
標籤的最大數量	50
自動備份的最長保留期	90 天
使用者啟動備份的最長保留期	沒有保留限制
每個檔案系統支援的最大路由數	50 [5]

Note

[1] 在具有 12 HA 對的向外延展檔案系統上 (每個 HA 配對 6,144 Mbps)。如需詳細資訊，請參閱高可用性 (HA) 配對。

[2] 若要佈建 4 Gbps 的輸送量容量，您的 ONTAP 擴充檔案系統的 FSx 需要在支援的情況下設定最大固態硬碟 IOPS (160,000) 和至少 5,120 GiB 的固態硬碟儲存容量。 AWS 區域如需 AWS 區域 支援 4,096 Mbps 輸送量容量的詳細資訊，請參閱。輸送量容量對效能的影響

[3] 您可以在任何時間點，每個磁碟區最多儲存 1,023 個快照。達到此限制後，您必須先刪除現有的快照，然後才能建立磁碟區的新快照。

[4] 您可以在任何時間點，每個磁碟區最多儲存 4,091 個備份。達到此限制後，您必須先刪除現有的備份，然後才能建立磁碟區的新備份。

[5] 您可以在任何時間點為每個檔案系統配置多達 50 個路由。達到此限制後，您必須先刪除現有路由，然後才能配置新路由。檔案系統的路由數量取決於其具有的 SVM 數量以及與其相關聯的路由表的數量。您可以使用下列方程式來決定檔案系統的現有路由數目：(檔案系統中 1+ SVM 數目) * (與檔案系統相關聯的路由表)。

針 NetApp 對 ONTAP 的 Amazon FSx 疑難排解

您可以使用下列各節來協助疑難排解 FSx for ONTAP 的問題。

主題

我的異地同步備份檔案系統處於狀態 MISCONFIGURED

檔案系統處於某個MISCONFIGURED狀態的可能原因有許多，每個原因都有自己的解析度，如下所示。

主題

VPC 擁有者帳戶已停用異地同步備份 VPC 共用

由於下列其中一個原因，由於共用 VPC 子網路 AWS 帳戶 中的參與者建立的異地同步備份檔案系統將進入MISCONFIGURED狀態：

- 共用 VPC 子網路的擁有者帳戶已停用 ONTAP 檔案系統 FSx 的異地同步備份 VPC 共用支援。
- 擁有者帳戶已取消共用 VPC 子網路。

如果擁有者帳戶已取消共用 VPC 子網路，您將在控制台中看到該檔案系統的下列訊息：

```
The vpc ID vpc-012345abcde does not exist
```

您必須連絡與您共用 VPC 子網路的擁有者帳戶以解決問題。如需詳細資訊在共用子網路中為 ONTAP 檔案系統建立 FSx，請參閱。

您無法在異地同步備份檔案系統上建立新的 SVM

對於共用 VPC AWS 帳戶 中的參與者建立的異地同步備份檔案系統，您將無法建立新的 SVM，原因如下：

- 共用 VPC 子網路的擁有者帳戶已停用 ONTAP 檔案系統 FSx 的異地同步備份 VPC 共用支援。
- 擁有者帳戶已取消共用 VPC 子網路。

您必須連絡與您共用 VPC 子網路的擁有者帳戶以解決問題。如需詳細資訊在共用子網路中為 ONTAP 檔案系統建立 FSx，請參閱。

您無法存取您的檔案系統

無法存取檔案系統的可能原因有很多，每個原因都有自己的解析度，如下所示。

主題

檔案系統的 elastic network interface 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介面。修改或刪除網路介面可能會導致虛擬私有雲 (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 網路界面。如需詳細資訊，請參閱 使用 Amazon VPC 進行檔案系統存取控制。

已刪除附加至檔案系統 elastic network interface 的彈性 IP 位址

Amazon FSx 不支援從公用網際網路存取檔案系統。Amazon FSx 會自動分離任何彈性 IP 位址，這是可從網際網路存取的公用 IP 位址，並連接至檔案系統的 elastic network interface。如需詳細資訊，請參閱 支援的用戶端。

檔案系統的 VPC 安全性群組缺少必要的輸入規則

檢閱中指定的輸入規則Amazon VPC 安全群組，並確定與檔案系統關聯的安全性群組具有對應的輸入規則。

運算執行個體的 VPC 安全性群組缺少必要的輸出規則

檢閱中指定的輸出規則Amazon VPC 安全群組，並確定與您的計算執行個體關聯的安全性群組具有對應的輸出規則。

運算執行個體的子網路不會使用與檔案系統相關聯的任何路由表

FSx for ONTAP 會在 VPC 路由表中建立用於存取檔案系統的端點。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 會使用您的 VPC 的主要路由表。您可以選擇性地指定一或多個路由表，供 Amazon FSx 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 到檔案系統的管理端點 (如檔案系統資源需詳細資訊，請參閱)，則您的用戶端可能不在與檔案系統之一路由表關聯的子網路中。若要存取檔案系統，請將檔案系統的其中一個路由表與用戶端的子網路建立關聯。如需更新檔案系統之 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 使用標籤式身份驗證來管理異地同步備份檔案系統的 VPC 路由表。這些路由表格以標籤`Key: AmazonFSx; Value: ManagedByAmazonFSx`。使用建立或更新 ONTAP 異地同步備份檔案系統的 FSx 時，建 AWS CloudFormation 議您手動新增標`Key: AmazonFSx; Value: ManagedByAmazonFSx`籤。

如果您無法連線到異地同步備份檔案系統，請檢查與檔案系統相關聯的 VPC 路由表是否有標記。`Key: AmazonFSx; Value: ManagedByAmazonFSx`如果不是，則 Amazon FSx 無法更新這些路由表，以便在發生容錯移轉事件時，將管理和資料連接埠的浮動 IP 位址路由到作用中的檔案伺服器。如需更新檔案系統之 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 中的客戶端通過 iSCSI 訪問文件系統

若要透過網際網路小型電腦系統介面 (iSCSI) 通訊協定從另一個 VPC 中的用戶端存取檔案系統，您可以設定 Amazon VPC 對等互連，或在與檔案系統關聯的 VPC 和用戶端所在的 VPC AWS Transit Gateway 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 對等連線。

擁有帳戶已取消共用 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，則擁有帳戶可能已取消共用 VPC 子網路。

如果擁有者帳戶已取消共用 VPC 子網路，您將在控制台中看到該檔案系統的下列訊息：

```
The vpc ID vpc-012345abcde does not exist
```

您將需要聯絡擁有的帳戶，以便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 從其他 VPC 擬私人雲端或內部部署的用戶端存取檔案系統

若要透過網路檔案系統 (NFS)、伺服器訊息區 (SMB) 或 NetApp ONTAP CLI 和 REST API 從其他 VPC 或內部部署的用戶端存取檔案系統，您必須使用與檔案系統關聯的 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 資料。

您無法將儲存虛擬機器 (SVM) 加入作用中目錄

如果您無法將 SVM 加入作用中目錄 (AD)，請先檢閱將 SVM 加入 Microsoft 活動目錄。下列各節會列出阻止 SVM 加入 Active Directory 的常見問題，包括針對每種情況產生的錯誤訊息。

主題

- SVM 的 NetBIOS 名稱與家用 NetBIOS 域的名稱相同。
- SVM 已加入另一個作用中目錄
- Amazon FSx 無法連接到您的活動目錄網域控制站，因為 SVM 的 NetBIOS 名稱已在使用中
- Amazon FSx 無法與您的活動目錄域控制器通信
- 由於未滿足的連接埠需求或服務帳戶許可，Amazon FSx 無法連線到您的作用中目錄
- Amazon FSx 無法連接到您的活動目錄網域控制站，因為服務帳戶登入資料無效

- Amazon FSx 無法連接到您的活動目錄網域控制站，因為服務帳戶登入資料不足
- Amazon FSx 無法與您的活動目錄 DNS 服務器或域控制器通信
- 由於活動目錄域名無效，Amazon FSx 無法與您的活動目錄進行通信。
- 服務帳戶無法存取 SVM Active Directory 組態中指定的系統管理員群組
- Amazon FSx 無法連線至使用中目錄網域控制站，因為指定的組織單位不存在或無法存取

SVM 的 NetBIOS 名稱與家用 NetBIOS 域的名稱相同。

將 SVM 加入您自我管理的作用中目錄失敗，並顯示下列錯誤訊息：

Amazon FSx 無法與您的活動目錄建立連接。這是因為您指定的伺服器名稱是主網域的 NetBIOS 名稱。若要修正這個問題，請為您的 SVM 選擇一個不同於主網域的 NetBIOS 名稱的 NetBIOS 名稱。然後重新嘗試將您的 SVM 加入您的活動目錄。

若要解決此問題，請按照中所述使用 AWS CLI 和 API 將 SVM 加入作用 AWS Management Console 中目錄的程序重新嘗試將 SVM 加入 AD。請確定您的 SVM 使用 NetBIOS 名稱，該名稱與作用中目錄主網域的 NetBIOS 名稱不同。

SVM 已加入另一個作用中目錄

將 SVM 加入作用中目錄失敗，並顯示下列錯誤訊息：

Amazon FSx 無法建立到您的活動目錄的連接。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 從作用中目錄取消加入此 SVM。然後重新嘗試將您的 SVM 加入不同的活動目錄。

若要解決此問題，請執行下列動作：

1. 使用 NetApp ONTAP CLI 從其目前的作用中目錄取消加入 SVM。如需詳細資訊，請參閱 使用 ONTAP CLI 從 SVM 取消加入作用中目錄 NetApp 。
2. 請按照中所述使用 AWS CLI 和 API 將 SVM 加入作用 AWS Management Console中目錄的步驟重新嘗試將 SVM 加入新 AD。

Amazon FSx 無法連接到您的活動目錄網域控制站，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 無法與您的活動目錄建立連接。這是因為您指定的 NetBIOS（計算機）名稱已在活動目錄中使用。若要修正這個問題，請為您的 SVM 選擇 NetBIOS 名稱不在您的作用中目錄中使用。，指定 NetBIOS (電腦) 然後再次嘗試將您的 SVM 加入您的使用中目錄。

若要解決此問題，請按照中所述使用 AWS CLI 和 API 將 SVM 加入作用 AWS Management Console 中目錄的程序重新嘗試將 SVM 加入 AD。請務必為您的 SVM 使用 NetBIOS 名稱，該名稱是唯一且尚未在作用中目錄中使用的。

Amazon FSx 無法與您的活動目錄域控制器通信

將 SVM 加入您的自我管理 AD 失敗，並顯示下列錯誤訊息：

Amazon FSx 無法與您的活動目錄進行通信。若要修正此問題，請確定 Amazon FSx 和網域控制站之間允許網路流量。然後重新嘗試將您的 SVM 加入您的活動目錄。

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 與 AD 之間的網路通訊。
2. 一旦 Amazon FSx 能夠與您的 AD 通訊，請按照中所述的程序進行，使用 AWS CLI 和 API 將 SVM 加入作用 AWS Management Console中目錄並重新嘗試將 SVM 加入您的 AD。

由於未滿足的連接埠需求或服務帳戶許可，Amazon FSx 無法連線到您的作用中目錄

將 SVM 加入您的自我管理 AD 失敗，並顯示下列錯誤訊息：

Amazon FSx 無法與您的活動目錄建立連接。這是因為不符合 Active Directory 的連接埠需求，或提供的服務帳戶沒有將儲存區虛擬機器加入至具有指定組織單位之網域的權限所致。若要修正此問題，請按照 Amazon FSx 使用者指南中的建議，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。

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網路需求，並確定所需連接埠上的通訊功能已啟用
2. 檢閱中所述的服務帳戶需求作用中目錄服務帳戶需求。確定服務帳戶具有使用指定的組織單位將 SVM 加入 AD 網域所需的委派權限。

3. 變更連接埠權限或服務帳戶後，請遵循中所述的程序，使用 AWS CLI 和 API 將 SVM 加入作用 AWS Management Console中目錄並重新嘗試將 SVM 加入 AD。

Amazon FSx 無法連接到您的活動目錄網域控制站，因為服務帳戶登入資料無效

將 SVM 加入您自我管理的作用中目錄失敗，並顯示下列錯誤訊息：

Amazon FSx 無法與您的作用中目錄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區虛擬機器的 Active Directory 組態。

若要解決此問題，請使用中所述的程序使用 AWS Management Console、 AWS CLI和 API 更新現有的 SVM 使用中目錄組態來更新 SVM 的服務帳戶認證。輸入服務帳戶使用者名稱時，請務必僅包含使用者名稱 (例如，`ServiceAcct`)，且不要包含任何網域前置詞 (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 (例如) 時，請勿使用辨別名稱 (`DNCN=ServiceAcct,OU=example,DC=corp,DC=com`)。

Amazon FSx 無法連接到您的活動目錄網域控制站，因為服務帳戶登入資料不足

將 SVM 加入您自我管理的作用中目錄失敗，並顯示下列錯誤訊息：

Amazon FSx 無法與您的活動目錄域控制器建立連接。這是因為尚未滿足 Active Directory 的連接埠需求，或者提供的服務帳戶沒有將儲存區虛擬機器加入具有指定組織單位之網域的權限。

若要解決這個問題，請確定您已將必要的權限委派給您提供的服務帳戶。服務帳戶必須能夠在您要加入檔案系統的網域中建立和刪除 OU 中的電腦物件。服務帳戶至少需要具有執行下列動作的權限：

- 重設密碼
- 限制帳戶讀取和寫入資料
- 已驗證寫入 DNS 主機名稱的能力
- 已驗證能夠寫入服務主體名稱
- 能夠創建和刪除計算機對象
- 經過驗證的讀取和寫入帳戶限制功能

如需有關使用正確權限建立服務帳戶的詳細資訊，請參閱作用中目錄服務帳戶需求和將許可委派給您的 Amazon FSx 服務帳戶。

Amazon FSx 無法與您的活動目錄 DNS 服務器或域控制器通信

將 SVM 加入您自我管理的作用中目錄失敗，並顯示下列錯誤訊息：

Amazon FSx 無法與您的活動目錄進行通信。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 伺服器和允許流量從儲存區虛擬機器流向網域控制站的網路組態來更新儲存區虛擬機器的 Active Directory 組態。

若要解決這個問題，請使用下列步驟：

1. 如果只能存取 Active Directory 中的某些網域控制站，例如由於地理限制或防火牆，您可以新增慣用的網域控制站。使用此選項時，Amazon FSx 會嘗試聯絡慣用的網域控制站。使用 vserver cifs domain preferred-dc add NetApp ONTAP CLI 命令新增慣用的網域控制站，如下所示：

   a. 若要存取 NetApp ONTAP CLI，請執行下列命令，在適用於 NetApp ONTAP 檔案系統的 Amazon FSx 管理連接埠上建立安全殼層工作階段。取代*management_endpoint_ip*為檔案系統管理連接埠的 IP 位址。

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

   如需詳細資訊，請參閱 使用 ONTAP CLI 管理檔案系統。

   b. 輸入以下命令，其中：

   - `-vserver vserver_name`指定儲存區虛擬機器 (SVM) 名稱。
   - `-domain domain_name`指定指定的網域控制站所屬網域的完整使用中目錄名稱 (FQDN)。
   - `-preferred-dc IP_address,…` 依喜好設定順序，指定慣用網域控制站的一或多個 IP 位址，以逗號分隔的清單。

   ```
   FsxId123456789::> vserver cifs domain preferred-dc add -vserver vserver_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 新增至偏好的網域控制站清單，SVM vs1 上的中小企業伺服器用來管理外部存取網域控制站。

```
FsxId123456789::> vserver cifs domain preferred-dc add -vserver vs1 -domain
 cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

2. 檢查您的網域控制站是否可以使用 DNS 解析。使用 vserver services access-check dns forward-lookup NetApp ONTAP CLI 指令，根據指定的 DNS 伺服器或虛擬伺服器的 DNS 組態上的查詢，傳回主機名稱的 IP 位址。

   a. 若要存取 NetApp ONTAP CLI，請執行下列命令，在適用於 NetApp ONTAP 檔案系統的 Amazon FSx 管理連接埠上建立安全殼層工作階段。取代*management_endpoint_ip*為檔案系統管理連接埠的 IP 位址。

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

   如需詳細資訊，請參閱 使用 ONTAP CLI 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. 輸入以下命令，其中：

   - `-vserver vserver_name`指定儲存區虛擬機器 (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 服務器上查找的 IP 地址的類型，默認為`all`。

   ```
   FsxId123456789::> vserver services access-check dns forward-lookup \
   -vserver vserver_name -node node_name \
   -domains domain_name -name-servers dns_server_ip_address \
   -hostname host_name
   ```

3. 檢閱將 SVM 加入 AD 時需要的資訊。
4. 將 SVM 加入 AD 時，請檢閱網路需求。
5. 請使用中所述的程序，使用 AD DNS 伺服器的正確 IP 位址網路組態需求來更新 SVM 的 AD 組態。

由於活動目錄域名無效，Amazon FSx 無法與您的活動目錄進行通信。

將 SVM 加入您自我管理的作用中目錄失敗，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，請使用符合組態需求的 FQDN 來更新儲存區虛擬機器的 Active Directory 組態。

若要解決這個問題，請使用下列步驟：

1. 檢閱內部部署 Active Directory 網域名稱需求，請將 SVM 加入作用中目錄時所需的資訊確定您嘗試加入的 AD 符合該需求。
2. 請使用中所述的程序，使用 AWS CLI 和 API 將 SVM 加入作用 AWS Management Console中目錄並重新嘗試將 SVM 加入 AD。請務必使用 AD 網域 FQDN 的正確格式。

服務帳戶無法存取 SVM Active Directory 組態中指定的系統管理員群組

將 SVM 加入您自我管理的作用中目錄失敗，並顯示下列錯誤訊息：

Amazon FSx 無法應用您的活動目錄配置。這是因為您提供的系統管理員群組不存在，或是您提供的服務帳戶無法存取。若要修正這個問題，請確定您的網路組態允許從 SVM 到 Active Directory 網域控制站和 DNS 伺服器的流量。然後更新您的 SVM 的作用中目錄組態，提供您 Active Directory 的 DNS 伺服器，並指定網域中提供的服務帳戶可存取的系統管理員群組。

要解決此問題，請依照下列步驟：

1. 檢閱提供網域群組以在 SVM 上執行管理動作的相關資訊。請確定您使用正確的 AD 網域管理員群組名稱。
2. 請使用中所述的程序，使用 AWS CLI 和 API 將 SVM 加入作用 AWS Management Console中目錄並重新嘗試將 SVM 加入 AD。

Amazon FSx 無法連線至使用中目錄網域控制站，因為指定的組織單位不存在或無法存取

將 SVM 加入您自我管理的作用中目錄失敗，並顯示下列錯誤訊息：

Amazon FSx 無法與您的活動目錄建立連接。這是因為您指定的組織單位不存在，或者無法存取所提供的服務帳戶。若要修正此問題，請更新儲存區虛擬機器的 Active Directory 組態，並指定服務帳戶具有加入權限的組織單位。

要解決此問題，請依照下列步驟：

1. 檢閱將 SVM 加入 AD 的必要條件。
2. 檢閱將 SVM 加入 AD 時所需要的資訊。
3. 使用此程序使用正確的組織單位重新嘗試將 SVM 加入 AD。

您無法刪除儲存區虛擬機器或磁碟區

ONTAP 檔案系統的每個 FSx 都可以包含一或多個儲存區虛擬機器 (SVM)，而且每個 SVM 可以包含一或多個磁碟區。刪除資源時，必須先確定已刪除其所有子系。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，則只能使用 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 可防止在特定情況下刪除 SVM 和磁碟區。如果您嘗試刪除 SVM 或磁碟區，但刪除請求不成功，Amazon FSx 會在 AWS 主控台、 AWS Command Line Interface (AWS CLI) 和 API 中提供資源未刪除的相關資訊。解決刪除失敗的原因之後，您可以重試刪除要求。

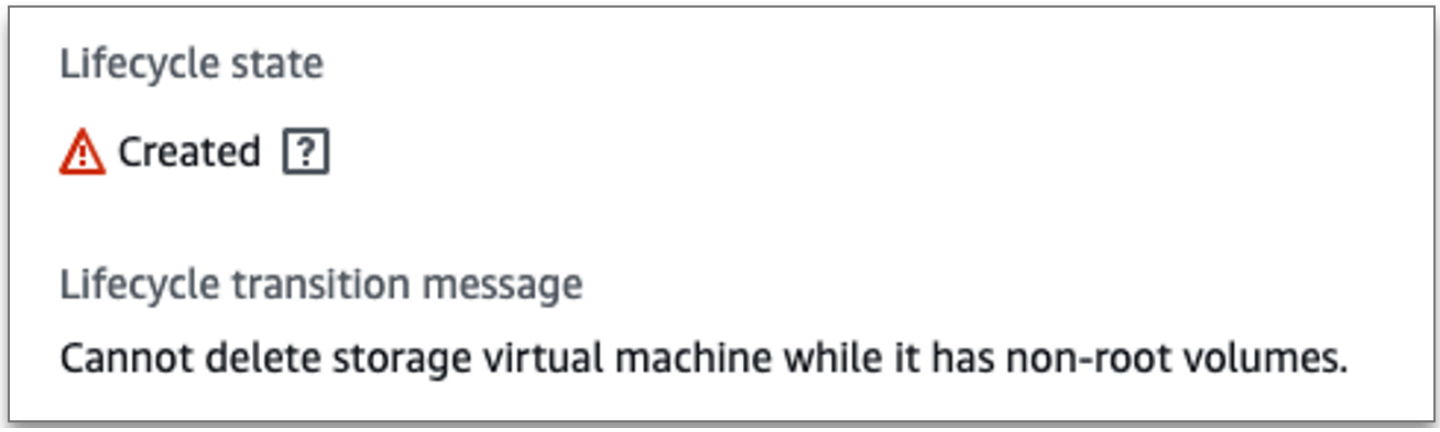
主題

- 識別失敗的刪除
- 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：已啟用 Kerberos 的 LIF
- SVM 刪除：其他原因
- 磁碟區刪除： FlexCache 關係

識別失敗的刪除

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 消失之前看到資源的`Lifecycle`狀態轉換`DELETING`為最多幾分鐘。

如果您嘗試刪除資源，且其`Lifecycle`狀態會從到`DELETING`再轉換回`CREATED`，此行為表示資源未成功刪除。在這種情況下，Amazon FSx 會在`CREATED`生命週期狀態旁的主控台中報告警示圖示。選擇警示圖示會顯示刪除失敗的原因，如下列範例所示。



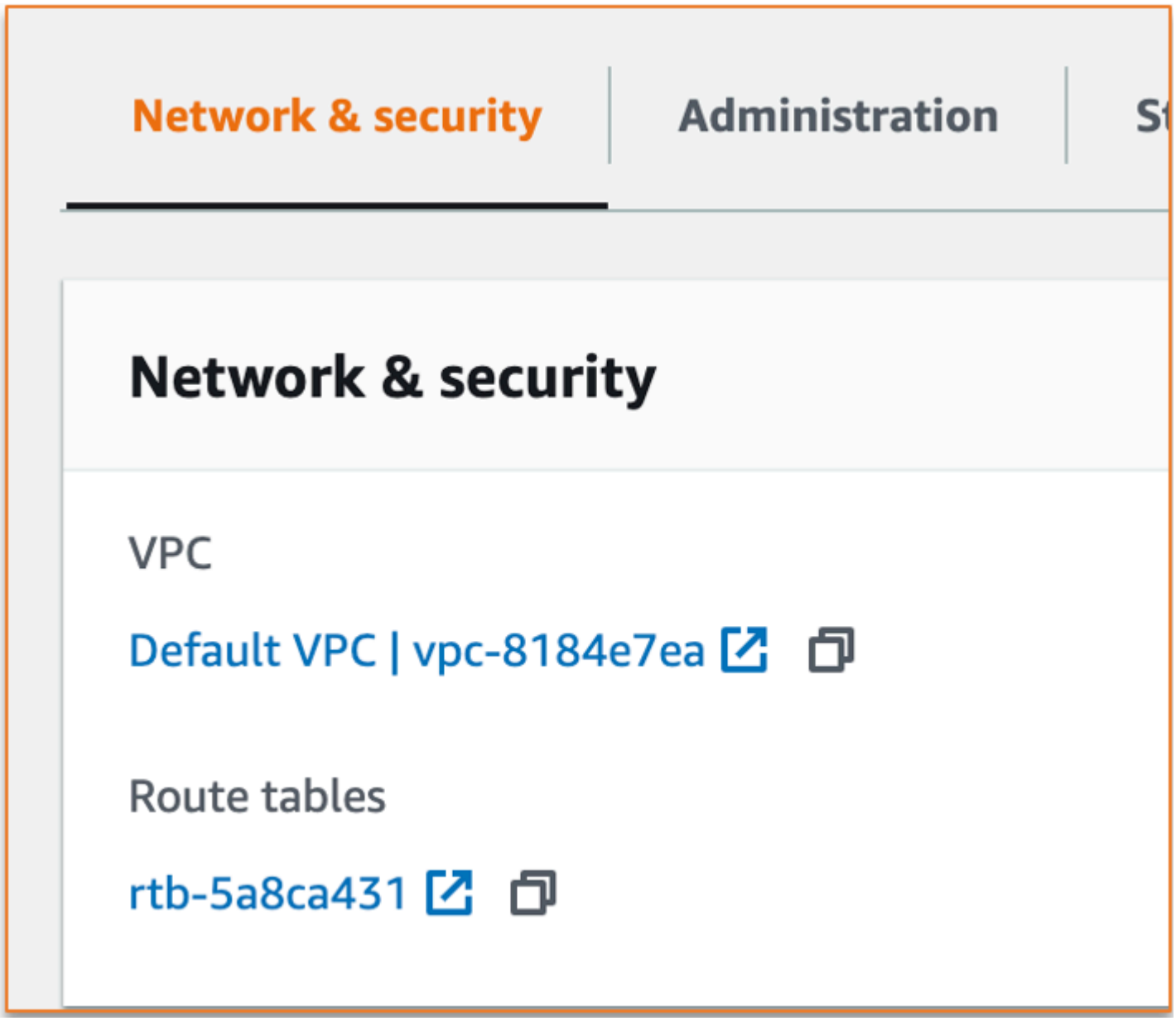
以下各節提供 Amazon FSx 防止 SVM 和磁碟區刪除的最常見原因，並提供如何解決這些問題的 step-by-step 指示。

SVM 刪除：無法存取路由表

ONTAP 檔案系統的每個 FSx 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移轉。依預設，這些路由表項目會建立在 VPC 的預設路由表中。您可以選擇性地指定一或多個非預設路由表格，其中可以建立 ONTAP 介面的 FSx。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，則可防止 Amazon FSx 刪除資源。如果發生這種情況，您會看到下列內容`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 AWS Support.
```

您可以在 Amazon FSx 主控台中找到檔案系統的「摘要」頁面，在「網路和安全」標籤下方找到檔案系統的路由表：



選擇路由表連結會帶您前往您的路由表。接下來，請確認與檔案系統相關聯的每個路由表都以此鍵值配對加上標籤：

```
Key: AmazonFSx
Value: ManagedByAmazonFSx
```

如果此標籤不存在，請重新建立它，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，則必須先刪除對等關係，然後才能刪除 SVM 或磁碟區。此要求可防止對等的 SVM 變得不健康。如果您的 SVM 因為對等關係而無法刪除，您會看到下列內容：`LifecycleTransitionReason`

Amazon FSx 無法刪除儲存虛擬機器，因為它是 SVM 對等或轉換對等關係的一部分。請刪除關係，然後再試一次。

您可以透過 ONTAP CLI 刪除 SVM 對等關係。若要存取 ONTAP CLI，請依照中的步驟執行使用 ONTAP CLI 管理檔案系統。使用 ONTAP CLI，請執行下列步驟。

1. 使用下列命令檢查 SVM 對等關係。*svm_name*以您的 SVM 的名稱取代。

   ```
   FsxId123456789::> vserver peer show -vserver svm_name
   ```

   如果此命令成功，您將看到類似以下內容的輸出：

   ```
               Peer        Peer                           Peering        Remote
   Vserver     Vserver     State        Peer Cluster      Applications   Vserver
   ----------- ----------- ------------ ----------------- -------------- ---------
   svm_name    test2       peered       FsxId02d81fef0d84734b6
                                                          snapmirror     fsxDest
   svm_name    test3       peered       FsxId02d81fef0d84734b6
                                                          snapmirror     fsxDest
   2 entries were displayed.
   ```

2. 使用下列命令刪除每個 SVM 對等關係。替換*svm_name*，並*remote_svm_name*與你的實際值。

```
FsxId123456789abcdef::> vserver peer delete -vserver svm_name -peer-
vserver remote_svm_name
```

如果這個命令成功，你會看到下面的輸出：

```
Info: 'vserver peer delete' command is successful.
```

SVM 或磁碟區刪除： SnapMirror

如果不先刪除對等關係，就無法刪除具有對等關係的 SVM 一樣 (請參閱SVM 刪除：對等關係)，您必須先刪除關係，就無法刪除具有 SnapMirror關係的 SnapMirror SVM。若要刪除 SnapMirror關係，請使用 ONTAP CLI 在關 SnapMirror 係的目的地的檔案系統上執行下列步驟。若要存取 ONTAP CLI，請依照中的步驟執行使用 ONTAP CLI 管理檔案系統。

> **Note**
>
> Amazon FSx 備份可用 SnapMirror 來建立 point-in-time檔案系統磁碟區的增量備份。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，會自動刪除此關係。

1. 使用下列指令列出您在目標檔案系統上的 SnapMirror 關係。*svm_name*以您的 SVM 的名稱取代。

   ```
   FsxId123456789abcdef::> snapmirror show -vserver svm_name
   ```

   如果此命令成功，您將看到類似以下內容的輸出：

   ```
   Source            Destination    Mirror  Relationship   Total             Last
   Path        Type  Path           State   Status         Progress  Healthy 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：已啟用 Kerberos 的 LIF

如果您嘗試刪除已啟用 Kerberos 的邏輯介面 (LIF) 的 SVM，您必須先停用該 LIF 上的 Kerberos，然後再刪除 SVM。

您可以透過 ONTAP CLI 停用 LIF 上的 Kerberos。若要存取 ONTAP CLI，請依照中的步驟執行使用 ONTAP 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. 檢查哪些介面已啟用 Kerberos。*svm_name*以您的 SVM 的名稱取代。

   ```
   FsxId123456789abcdef::> kerberos interface show -vserver svm_name
   ```

   如果此命令成功，您將看到類似以下內容的輸出：

   ```
   (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. 使用下列命令停用 Kerberos LIF。*svm_name*以您的 SVM 的名稱取代。您需要提供您用來將此 SVM 加入您的使用中目錄的使用中目錄使用者名稱和密碼。

```
FsxId123456789abcdef::> kerberos interface disable -vserver svm_name -lif
 nfs_smb_management_1
```

如果這個命令成功，你會看到下面的輸出。提供您用來將此 SVM 加入您的作用中目錄的使用中目錄使用者名稱和密碼。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. 使用下列命令確認已在 SVM 上停用 Kerberos。*svm_name*以您的 SVM 的名稱取代。

```
FsxId123456789abcdef::> kerberos interface show -vserver svm_name
```

如果此命令成功，您將看到類似以下內容的輸出：

```
(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 AWS CLI、API 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*以您的 SVM 的名稱取代。

> **Important**
>
> 以下命令可以在活動目錄上鏈接 SVM 的計算機對象。

```
FsxId123456789abcdef::> kerberos interface disable -vserver svm_name -lif
 nfs_smb_management_1 -force true
```

如果這個命令成功，你會看到類似下面的輸出。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

適用於 ONTAP SVM 的 FSx 會在您的活動目錄中建立一個電腦物件，當它們加入您的使用中目錄時。在某些情況下，您可能想要使用 ONTAP CLI 手動取消加入作用中目錄的 SVM。若要存取 ONTAP CLI，請依照中的步驟使用 ONTAP CLI 管理檔案系統，在檔案系統層級使用`fsxadmin`認證登入 ONTAP CLI。使用 ONTAP CLI，請執行下列步驟，從您的作用中目錄取消加入 SVM。

> **Important**
>
> 此程序可以將 SVM 的電腦物件串連到您的作用中目錄上。

1. 使用下列命令在 ONTAP CLI 中進入進階模式。

   ```
   FsxId123456789abcdef::> set adv
   ```

   運行此命令後，你會看到這個輸出。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. 使用以下命令刪除活動目錄的 DNS。*svm_name*以您的 SVM 的名稱取代。

```
FsxId123456789abcdef::> vserver services name-service dns dynamic-update record
 delete -vserver svm_name -lif nfs_smb_management_1
```

> **Note**
>
> 如果 DNS 記錄已被刪除，或者 DNS 伺服器無法連線，則此命令會失敗。如果發生這種情況，請繼續下一步。

3. 通過使用以下命令禁用 DNS。*svm_name*以您的 SVM 的名稱取代。

```
FsxId123456789abcdef::> vserver services name-service dns dynamic-update modify -
vserver svm_name -is-enabled false -use-secure false
```

如果這個命令成功，你會看到下面的輸出：

```
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. 從活動目錄中取消加入設備。*svm_name*以您的 SVM 的名稱取代。

```
FsxId123456789abcdef::> vserver cifs delete -vserver svm_name
```

運行此命令後，你會看到下面的輸出，其中*CORP.EXAMPLE.COM*被替換為您的域名。出現提示時，請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，否則您無法刪除作為 FlexCache 關係的原始磁碟區的磁碟區。若要判斷哪些磁碟區具有 FlexCache關聯性，您可以使用 ONTAP CLI。若要存取 ONTAP CLI，請依照中的步驟執行使用 ONTAP 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. 通過使用以下命令刪除任何緩存關係。替換*dest_svm_name*，並*dest_vol_name*與你的實際值。

```
FsxId123456789abcdef::> volume flexcache delete -vserver dest_svm_name -
volume dest_vol_name
```

3. 刪除快取關係後，請嘗試再次透過 AWS CLI、API 或主控台刪除 SVM。

自動每日備份因磁碟區容量不足而失敗

磁碟區的每日自動備份失敗，並顯示下列訊息：

```
Amazon FSx could not create a backup of your volume because the backup snapshot was
 deleted.
```

自動每日備份失敗，因為磁碟區上的可用儲存容量不足。若要減輕此情況，您必須釋放磁碟區上的儲存容量。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

您的磁碟區容量不足

如果磁碟區的空間不足，您可以使用此處顯示的程序來診斷並解決此情況。

主題

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消耗情況。此資訊可協助您決定如何回收或保留磁碟區儲存容量。如需詳細資訊，請參閱 監視磁碟區的儲存容量 (主控台)。

增加磁碟區的儲存容量

您可以使用 Amazon FSx 主控台和 Amazon FSx API 來增加磁碟區的儲存容量。 AWS CLI如需有關以增加容量更新磁碟區的詳細資訊，請參閱更新磁碟區。

或者，您也可以使用 `volume modify` NetApp ONTAP CLI 命令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

您可以使用磁碟區自動調整大小，讓磁碟區在達到已使用的空間臨界值時自動增加指定的大小。您可以使用 ONTAP CLI 指令針對 FlexVol 磁碟區類型執行此動作，這是 FSx 適用於 ONTAP 的預設磁碟區類型。`volume autosize` NetApp 如需詳細資訊，請參閱 啟用自動調整磁碟區。

檔案系統的主要儲存空間已滿

如果 FSx for ONTAP 檔案系統的主要儲存空間已滿，您就無法將任何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也一樣。您可以在 Amazon FSx 主控台檔案系統詳細資訊頁面的「監控和效能」索引標籤中檢視可用的主要儲存容量。如需更多資訊，請參閱 監控 SSD 儲存使用率

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 更新檔案系統固態硬碟儲存和 IOPS。

刪除快照

根據預設，磁碟區上的快照會使用預設快照原則啟用快照。快照儲存在磁碟區根.snapshot目錄的目錄中。您可以透過下列方式管理快照的磁碟區儲存容量：

- 手動刪除快照 — 手動刪除快照以回收儲存容量。
- 建立快照自動刪除原則 — 建立刪除快照比預設快照原則更積極的策略。
- 關閉自動快照 — 關閉自動快照以節省儲存容量。

如需刪除快照及管理快照原則以節省儲存容量的詳細資訊，請參閱刪除快照。

增加磁碟區的最大檔案容量

當可用的節點或檔案指標數量用盡時，ONTAP 磁碟區的 FSx 可能會耗盡檔案容量。根據預設，磁碟區大小每 32KiB 的磁碟區大小，磁碟區上的可用節點數目為 1。如需詳細資訊，請參閱 磁碟區檔案容量。

磁碟區中的 inode 數量會隨磁碟區的儲存容量而增加，最高可達 648 GiB 的臨界值。根據預設，儲存容量為 648 GiB 或以上的磁碟區都具有相同數量的索引節點數目，即 21,251,126。若要檢視磁碟區的最大檔案容量，請參閱檢視磁碟區的檔案容量。

如果您建立的磁碟區大於 648 GiB，並且想要有更多的 21,251,126 索引節點，則必須手動增加磁碟區上的檔案數目上限。如果磁碟區的儲存容量不足，您可以檢查其最大檔案容量。如果它接近其文件容量，則可以手動增加它。如需詳細資訊，請參閱 增加磁碟區上的檔案數目上限 (ONTAPCLI)。

排解網路問題

如果您遇到網路問題，可以使用此處顯示的程序來診斷問題。

您想捕獲數據包跟踪

數據包跟踪是驗證通過層到其目的地的數據包的路徑的過程。您可以使用下列 NetApp ONTAP CLI 指令來控制封包追蹤程序：

- network tcpdump start— 開始數據包跟踪
- network tcpdump show— 顯示當前運行的數據包跟踪
- network tcpdump stop— 停止正在運行的數據包跟踪

這些指令可供在您的檔案系統中具有該fsxadmin角色的使用者使用。

從檔案系統擷取封包追蹤

1. 若要使用 SSH 連線到檔案系統的 NetApp ONTAP CLI，請依照 Amazon FSx 適用於 NetApp ONTAP 使用者指南一使用 NetApp ONTAP CLI節中所述的步驟進行操作。

```
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. 識別檔案系統上要儲存封包追蹤的位置。磁碟區必須在線上，且必須以有效的結合路徑掛載在命名空間中。使用下列指令來檢查是否符合這些準則的磁碟區：

```
::*> 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. 使用最少必要的引數開始追蹤。取代以下項目：

   - 以節點的*#### node_name* (例如，)。FsxId01234567890abcdef-01
   - 將 *svm_name* 取代為儲存區虛擬機器的名稱 (例如，)。fsx
   - 以磁碟區的名*#######*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。在適用於 ONTAP 的 FSx 中，所有網路流量都使用此介面e0e。

使用封包追蹤時，請記住下列事項：

- *##############################/clus/ svm_name/junction-path-name*
- 選擇性地提供封包追蹤的檔案名稱。*############################ _ ### _ #### _hhmmss .trc*
- 如果指定了滾動軌跡，filter_name 會以指示旋轉序列中位置的數字加上尾碼。
- ONTAP CLI 也接受下列選用-pass-through引數：

```
-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>
```

- 如需有關篩選器運算式的資訊，請參閱 pcap-filter (7) 線上手冊。

5. 檢視進行中的追蹤：

```
::*> debug network tcpdump show
Node                    IPspace  Port     Filename
----------------------  -------- -------- --------
FsxId123456789abcdef-01  Default  e0e      /clus/fsx/test_vol1/
FsxId123456789abcdef-01_e0e_20230605_181451.trc
```

6. 停止跟踪：

```
::*> 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. 訪問數據包跟踪。

   您的封包追蹤會儲存在您使用指debug network tcpdump start令指定的磁碟區中，而且可透過 NFS 匯出或與該磁碟區對應的 SMB 共用來存取。

如需擷取封包追蹤的相關資訊，請參閱知識庫中的 ONTAP 9.10+ 中[如何使用 ONTAP 9.10+ 中的除錯網路 tcpdump]。 NetApp

適用於 ONTAP 的 Amazon FSx 的文件歷史記錄 NetApp

- API 版本：
- 最新文件更新：2024 年 4 月 30 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
為文件系統管理用戶添加了`fsxadmin-readonly`角色的 Support	此`fsxadmin-readonly`角色現在可供ONTAP檔案系統管理使用者使用，並可用於檔案系統監視應用程式，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
為 Windows 域管理用戶添加了 SSH 公鑰身份驗證的 Support	您現在可以對使用中目錄網域檔案系統和 SVM 使用者使用 SSH 公開金鑰驗證。如需詳細資訊，請參閱 https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/set-up-ad-auth.html。	2024 年 4 月 30 日
在向外延展檔案系統中新增 12 HA 配對的 Support 援	適用於 NetApp ONTAP 的 Amazon FSx 新增了對橫向擴充檔案系統中 12 個 HA 配對的支援。具有 12 HA 對的檔案系統，可在 12 個高可用性 (HA) 對中提供高達 72 Gbps 的輸送容量和 2,400,000 個固態硬碟 IOPS。如需詳細資訊，請參閱高可用性 (HA) 配對和	2024年3月4日

	Amazon FSx 以瞭解 NetApp ONT AP 效能。	
新 Support 雲端寫入模式的支援	適用於 NetApp ONTAP 的 Amazon FSx 增加了對磁碟區的雲寫入模式的支持。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
Support 加了備份 FlexGroup 磁碟區的支援 AWS Backup	您現在可以使 AWS Backup 用在 ONTAP 檔案系統的 FSx 上備份和還原 FlexGroup 磁碟區。如需詳細資訊，請參閱AWS Backup 搭配 Amazon FSx 使用。	2024年1月11日
Amazon FSx 更新了亞馬遜，亞馬遜，亞馬遜SxFullAccess，亞馬遜SxConsoleFullAccess和亞馬遜SxReadOnlyAccess管理政策 SxConsoleReadOnlyAccess SxServiceRolePolicy AWS	Amazon FSx 更新了亞馬遜，亞馬遜SxFullAccess，亞馬遜SxConsoleFullAccess，亞馬遜和亞馬遜 F SxReadOnlyAccess 政策以添加許可。SxConsoleReadOnlyAccess SxServiceRolePolicy `ec2:GetSecurityGroupsForVpc` 如需詳細資訊，請參閱 Amazon FSx 更新受 AWS 管政策。	2024 年 1 月 9 日
Amazon FSx 更新了亞馬遜 SxFullAccess 和亞馬遜管理政策 SxConsoleFullAccess AWS	Amazon FSx 更新了亞馬遜 SxFullAccess 和亞馬遜SxConsoleFullAccess 政策以添加操作。`ManageCrossAccountDataReplication` 如需詳細資訊，請參閱 Amazon FSx 更新受 AWS 管政策。	2023 年 12 月 20 日

已新 Support 向外延展量度的支援	適用於 ONTAP 的 FSx 現在可為具有多個 HA 配對的檔案系統提供 Amazon CloudWatch 指標。如需詳細資訊，請參閱向外延展檔案系統度量。	2023 年 11 月 26 日
已新 Support 向外延展檔案系統的支援	適用於 NetApp ONTAP 的 Amazon FSx 新增了對向外擴充檔案系統的支援，可在六個高可用性 (HA) 對中提供高達 36 Gbps 的輸送量容量和 120 萬個固態硬碟 IOPS。如需詳細資訊，請參閱高可用性 (HA) 配對和 Amazon FSx 以瞭解 NetApp ONT AP 效能。	2023 年 11 月 26 日
新 Support FlexGroup 磁碟區的支援	適用於 NetApp ONTAP 的 Amazon FSx 增加了對磁碟區的 FlexGroup 支持。如需詳細資訊，請參閱〈體積樣式〉。	2023 年 11 月 26 日
針對異地同步備份檔案系統新增共用 VPC 支援	參與者帳戶現在可以在已與他們共用的 VPC 中建立異地同步備份檔案系統。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為 ONTAP 檔案系統建立 FSx	2023 年 11 月 26 日
Amazon FSx 更新了亞馬遜 SxFullAccess 和亞馬遜管理政策 SxConsoleFullAccess AWS	Amazon FSx 更新了亞馬遜 SxFullAccess 和亞馬遜SxConsoleFullAccess 政策以添加許可。`fsx:CopySnapshotAndUpdateVolume` 如需詳細資訊，請參閱 Amazon FSx 更新受 AWS 管政策。	2023 年 11 月 26 日

Amazon FSx 更新了亞馬遜 SxFullAccess 和亞馬遜管理政策 SxConsoleFullAccess AWS	Amazon FSx 更新了亞馬遜 SxFullAccess 和亞馬遜 F SxConsoleFullAccess 政策以添加和許可。`fsx:DescribeSharedVPCConfiguration` `fsx:UpdateSharedVPCConfiguration` 如需詳細資訊，請參閱 Amazon FSx 更新受 AWS 管政策。	2023 年 11 月 14 日
已新 Support 建立額外 ONTAP 角色和使用者的支援	適用於 NetApp ONTAP 的 Amazon FSx 現在支援建立額外的 ONTAP 角色和使用者，以便在使用 ONTAP CLI 和 REST API 時定義使用者功能和權限。如需詳細資訊，請參閱適用於 NetApp ONTAP 的 Amazon FSx 中的角色和使用者。	2023 年 9 月 6 日
增加了對其他 CloudWatch 指標的 Support 和增強的監控儀表板	FSx for ONTAP 現在提供額外的效能指標和增強的監控儀表板，以改善檔案系統活動的可見度。如需詳細資訊，請參閱使用監視 CloudWatch。	2023 年 8 月 17 日
Amazon FSx 更新了亞馬遜託管政策 SxServiceRolePolicy AWS	Amazon FSx 更新了亞馬遜SxServiceRolePolicy 的`cloudwatch:PutMetricData` 許可。如需詳細資訊，請參閱 Amazon FSx 更新受 AWS 管政策。	2023 年 7 月 24 日

增加了直接使用 NetApp 系統管理器的 Support	您可以使用System Manager直接從管理適用於 ONTAP 檔案系統的 FSx。NetApp BlueXP 如需詳細資訊，請參閱搭配 BlueExp 使用 NetApp 系統管理員。	2023 年 7 月 13 日
增加了用於監控 EMS 事件的 Support	您可以使用 NetApp ONTAP 的原生來監視 FSx 中是否有 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，請參閱監視 FSx 的 ONTAP EMS 事件。	2023 年 7 月 13 日
增加了 Support SnapLock	適用於 ONTAP 的 FSx 現在支援SnapLock磁碟區。SnapLock可讓您將檔案轉換為「一次寫入多讀」(WORM)狀態，以保護檔案，防止在指定的保留期間內進行修改或刪除。適用於 ONTAP 的 FSx 支援符合性和企業保留模式。SnapLock如需詳細資訊，請參閱使用 SnapLock。	2023 年 7 月 13 日
為傳輸中的數據添加了 IPsec 加密的 Support	FSx for ONTAP 現在支援使用 IPsec 加密來加密檔案系統與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 驗證設定 IPSec 和使用憑證驗證設定 IPsec。	2023 年 7 月 13 日

最大磁碟區大小增加	適用於 ONTAP 的 FSx 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 更新了亞馬遜託管政策 SxFullAccess AWS	Amazon FSx 更新了 AmazonFSxFullAccess 政策，以移除`fsx:*`許可並新增特定動作。`fsx`如需詳細資訊，請參閱 AmazonF 政策SxFullAccess。	2023 年 7 月 13 日
Amazon FSx 更新了亞馬遜託管政策 SxConsoleFullAccess AWS	Amazon FSx 更新了 AmazonFSxConsoleFullAccess 政策，以移除`fsx:*`許可並新增特定動作。`fsx`如需詳細資訊，請參閱 AmazonF 政策SxConsoleFullAccess。	2023 年 7 月 13 日
已新 Support 將現有儲存虛擬機器加入作用中目錄的支援	您可以使用 AWS CLI 和 API 將現有儲存區虛擬機器加入作用中目錄。 AWS Management Console如需詳細資訊，請參閱將 SVM 加入作用中目錄。	2023 年 6 月 13 日
Support 新增單一可用區檔案系統的 NVMe 讀取快取	在 2022 年 11 月 28 日之後建立的單一可用區檔案系統現已支援 NVMe 讀取快取，而且在美國東部 (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) 至少有 2 Gbps 的輸送容量。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

Support 使用 VPC 內 IP 位址範圍建立異地同步備份檔案系統	您現在可以透過指定位於 VPC IP 位址範圍內的端點，為 ONTAP 檔案系統建立異地同步備份 FSX。如需詳細資訊，請參閱為 ONTAP 檔案系統建立 FSx。	2022 年 11 月 28 日
已新增 Support 更新異地同步備份檔案系統上的 VPC 路由表	您現在可以將新的 VPC 路由表關聯 (新增) 至 ONTAP 檔案系統的現有異地同步備份 FSX，或取消現有 VPC 路由表與 ONTAP 檔案系統的現有異地同步備份 FSX 的關聯 (移除)。如需詳細資訊，請參閱更新檔案系統。	2022 年 11 月 28 日
添加了對 AWS Nitro 系統傳輸中的數據進行加密的 Support	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) 受支援的 Amazon EC2 執行個體存取時，傳輸中的資料會自動加密。有關詳情，請參閱使用 AWS Nitro 系統加密傳輸中的資料。	2022 年 11 月 28 日
已新 Support 建立 DP 磁碟區的支援	您現在可以使用 Amazon FSx 主控台或 Amazon FSx API 來建立 DP (資料保護) 磁碟區。AWS CLI當您要移轉 NetApp SnapMirror 或保護單一磁碟區的資料時，可以使用 DP 磁碟區做為或 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

Support 將磁碟區標籤複製到備份	您現在可以在 AWS CLI 或 Amazon FSx API CopyTagsToBackups 中啟用，將標籤從磁碟區自動複製到備份。如需詳細資訊，請參閱將標籤複製到備份。	2022 年 11 月 28 日
新 Support 了選擇快照策略的支援	使用 Amazon FSx 主控台或 Amazon FSx API 建立或更新磁碟區時， AWS CLI您現在可以從三種內建快照政策中進行選擇。您也可以選取您在 ONTAP CLI 或 REST API 中建立的自訂快照原則。如需詳細資訊，請參閱快照政策。	2022 年 11 月 28 日
新 Support 額外檔案系統輸送量容量選項的支援	FSx for ONTAP 現在支援在 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) 區域以及歐洲 (愛爾蘭) 建立的檔案系統，提供 4,096 MBPS 的輸送容量。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 Support 額外固態硬碟 IOPS 的支援	FSx for ONTAP 現在支援 160,000 個 SSD IOPS，適用於 2022 年 11 月 28 日後建立的檔案系統，包括美國東部 (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，以及歐洲 (愛爾蘭)。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

已新增 Support 使用適用於 ONTAP 的 FSx 做為 VMware 雲端上的外部資料存放區 AWS	您可以使用適用於 ONTAP 的 FSx 做為 VMware 雲端上 AWS 軟體定義的資料中心 (SDDC) 的外部資料存放區。這項新增的支援可提供彈性，讓您可以獨立於針對 VMware Cloud AWS 工作負載的運算資源擴充或縮減儲存。如需詳細資訊，請參閱將 VMware 雲端搭配 FSx 搭配使用於 ONTAP。	2022 年 8 月 30 日
自動增加檔案系統的儲存容量	當使用的 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 現已與 AWS Backup	除了使用 AWS Backup 原生 Amazon FSx 備份之外，您現在還可以用來備份和還原 FSx 檔案系統。如需詳細資訊，請參閱AWS Backup 搭配 Amazon FSx 使用。	2022 年 5 月 18 日
新 Support 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 FSX，這些檔案系統的設計目的是在單一可用區域 (AZ) 內提供高可用性和耐久性。如需詳細資訊，請參閱選擇檔案系統部署。	2022 年 4 月 13 日

為 AWS PrivateLink 介面 VPC 端點新增 Support	您現在可以使用介面虛擬私人雲端端點從 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
已新增 Support 修改現有 ONTAP 檔案系統的輸送量容量	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 Support SSD 儲存容量和佈建 IOPS 擴充的支援	您現在可以隨著儲存和 IOPS 需求的演變，增加現有 FSx 適用於 ONTAP 檔案系統的固態硬碟儲存容量和佈建 IOPS。如需詳細資訊，請參閱管理儲存容量和佈建的 IOPS。	2022 年 1 月 25 日
為 Amazon CloudWatch 指標添加了 Support	您可以使用 Amazon 監控檔案系統 CloudWatch，該 Amazon 會從 FSx for ONTAP 的原始資料收集並處理成可讀且接近即時的指標。如需詳細資訊，請參閱使用 Amazon 進行監控 CloudWatch。	2022年1月19日
新 Support 額外檔案系統輸送量選項的支援	適用於 ONTAP 的 FSx 現在支援每秒 128 MB 和 256 MB 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

適用於 NetApp ONTAP 的 Amazon FSx 現已正式推出	FSx for ONTAP 是一項全受管服務，提供建置於 ONTAP 檔案系統之上 NetApp的高度可靠、可擴充、高效能及功能豐富的檔案儲存。它提供 NetApp 檔案系統熟悉的功能、效能、功能和 API，同時具備全代管 AWS 服務的敏捷性、可擴充性和簡易性。	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。