aws

Windows 使用者指南

Amazon FSx for Windows File Server

Amazon FSx for Windows File Server: Windows 使用者指南

Table of Contents

什麼是 FSx for Windows File Server？

Amazon FSx for Windows File Server 提供全受管 Microsoft Windows 檔案伺服器，這些伺服器由完全原生的 Windows 檔案系統支援。FSx for Windows File Server 具有功能、效能和相容性，可輕鬆將企業應用程式提升和轉移至 AWS 雲端。

Amazon FSX 支援一系列廣泛的企業 Windows 工作負載，具有在 Microsoft Windows Server 上建置的全受管檔案儲存。Amazon FSX 原生支援 Windows 檔案系統功能以及業界標準的伺服器訊息區塊 (SMB) 通訊協定，可透過網路存取檔案儲存。Amazon FSx 已針對 中的企業應用程式進行最佳化 AWS 雲端，具有原生 Windows 相容性、企業效能和功能，以及一致的低於毫秒延遲。

透過 Amazon FSx 上的檔案儲存，Windows 開發人員和管理員現今使用的程式碼、應用程式和工具可以維持不變。Windows 應用程式和工作負載非常適合 Amazon FSx，包括商業應用程式、主目錄、Web 服務、內容管理、資料分析、軟體建置設定和媒體處理工作負載。

作為全受管服務，FSx for Windows File Server 消除了設定和佈建檔案伺服器及儲存磁碟區的管理開銷。此外，Amazon FSx 會讓 Windows 軟體保持在最新狀態、偵測和解決硬體故障，以及執行備份。它還提供與其他 AWS 服務的豐富整合，例如 AWS IAM、AWS Directory Service for Microsoft Active Directory、Amazon WorkSpaces、 AWS Key Management Service和 AWS CloudTrail。

FSx for Windows File Server 資源：檔案系統、備份和檔案共用

Amazon FSx 中的主要資源是檔案系統和備份。檔案系統是您存放和存取檔案和資料夾的地方。檔案系統是由一或多個 Windows 檔案伺服器和儲存磁碟區所組成。建立檔案系統時，您可以指定儲存容量（以 GiB 為單位）、SSD IOPS 和輸送量容量 （以 MBps 為單位）。您可以在建立檔案系統之後，隨著需求變更而修改這些屬性。如需詳細資訊，請參閱管理儲存容量、管理 SSD IOPS及管理輸送量容量。

FSx for Windows File Server 備份是file-system-consistent、高耐用性和增量式備份。為了確保檔案系統一致性，Amazon FSx 會在 Microsoft Windows 中使用磁碟區陰影複製服務 (VSS)。在建立檔案系統時，預設會開啟自動每日備份，您也可以隨時進行額外的手動備份。如需詳細資訊，請參閱使用備份保護您的資料。

Windows 檔案共享是檔案系統中的特定資料夾 （及其子資料夾），可讓您使用 SMB 存取運算執行個體。您的檔案系統已隨附名為 的預設 Windows 檔案共享`\share`。您可以在 Windows 上使用共用資料夾圖形使用者介面 (GUI) 工具，視需要建立和管理任意數量的其他 Windows 檔案共用。如需詳細資訊，請參閱使用檔案共享存取資料。

您可以使用檔案系統的 DNS 名稱或您與檔案系統建立關聯的 DNS 別名來存取檔案共享。如需詳細資訊，請參閱管理 DNS 別名。

存取檔案共享

Amazon FSx 可透過使用 SMB 通訊協定（支援 2.0 至 3.1.1 版）的運算執行個體存取。您可以從 Windows Server 2008 和 Windows 7 開始的所有 Windows 版本存取共用，也可以從 Linux 的目前版本存取共用。您可以在 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體、WorkSpaces 執行個體、Amazon AppStream 2.0 執行個體和 VMware Cloud onVM 上映射 Amazon FSx 檔案共用。VMware AWS VMs

您可以使用 AWS Direct Connect 或 從內部部署運算執行個體存取檔案共享 Site-to-Site VPN。除了存取位於相同 VPC、 AWS 帳戶和 AWS 區域 檔案系統中的檔案共用之外，您也可以從位於不同 Amazon VPC、帳戶或 中的運算執行個體存取共用 AWS 區域。您可以使用 VPC 對等互連或傳輸閘道來執行此操作。如需詳細資訊，請參閱從 內存取資料 AWS 雲端。

安全性和資料保護

Amazon FSx 提供多層安全性和合規性，以協助確保您的資料受到保護。它會使用您在 () 中管理的金鑰自動加密靜態資料 AWS Key Management Service（適用於檔案系統和備份）AWS KMS。傳輸中的資料也會使用 SMB Kerberos 工作階段金鑰自動加密。它已經過評估，符合 ISO、PCI-DSS 和 SOC 認證，且符合 HIPAA 資格。

Amazon FSx 使用 Windows 存取控制清單 (ACLs) 在檔案和資料夾層級提供存取控制。它使用 Amazon Virtual Private Cloud (Amazon VPC) 安全群組在檔案系統層級提供存取控制。此外，它使用 AWS Identity and Access Management (IAM) 存取政策在 API 層級提供存取控制。存取檔案系統的使用者會使用 Microsoft Active Directory 進行身分驗證。Amazon FSx 與 整合 AWS CloudTrail ，可監控和記錄您的 API 呼叫，讓您看到使用者在 Amazon FSx 資源上採取的動作。

此外，它會每天自動對檔案系統進行高度耐用的備份來保護您的資料，並允許您隨時進行額外的備份。如需詳細資訊，請參閱Amazon FSx 的安全性。

可用性與持久性

FSx for Windows File Server 提供兩種可用性和耐用性層級的檔案系統。單一可用區檔案透過自動偵測和解決元件故障，確保單一可用區域 (AZ) 內的高可用性。此外，多可用區域檔案系統透過在區域內的個別可用區域中佈建和維護待命檔案伺服器，跨多個可用區域提供高可用性和容錯移轉支援 AWS 。若要進一步了解單一可用區和多可用區檔案系統部署，請參閱 可用性和耐久性：單一可用區和多可用區檔案系統。

管理檔案系統

您可以使用自訂遠端管理 PowerShell 命令或使用 Windows 原生 GUI 來管理 FSx for Windows File Server 檔案系統。若要進一步了解如何管理 Amazon FSx 檔案系統，請參閱 管理 FSx for Windows 檔案系統。

價格和效能彈性

FSx for Windows File Server 透過同時提供固態硬碟 (SSD) 和硬碟 (HDD) 儲存類型，為您提供價格和效能彈性。HDD 儲存體適用於各種工作負載，包括主目錄、使用者和部門共用，以及內容管理系統。SSD 儲存體專為最高效能和最易受延遲影響的工作負載而設計，包括資料庫、媒體處理工作負載和資料分析應用程式。

透過 FSx for Windows File Server，您可以獨立佈建檔案系統儲存、SSD IOPS 和輸送量，以實現適當的成本和效能組合。您可以修改檔案系統的儲存體、SSD IOPS 和輸送量容量，以滿足不斷變化的工作負載需求，因此您只需支付所需的費用。

Amazon FSx 定價

使用 Amazon FSx，無需預付硬體或軟體成本。您只需支付使用的資源，無需最低承諾、設定成本或額外費用。如需與服務相關的定價和費用資訊，請參閱 Amazon FSx for Windows File Server 定價。

前提

若要使用 Amazon FSx，您需要具有 Amazon EC2 執行個體、WorkSpaces 執行個體、WorkSpaces 應用程式執行個體或在 VMware Cloud 中對支援類型 AWS 環境執行的 VM AWS 的帳戶。

在本指南中，我們會做出下列假設：

- 如果您使用的是 Amazon EC2，我們假設您已熟悉 Amazon EC2。如需如何使用 Amazon EC2 的詳細資訊，請參閱 Amazon Elastic Compute Cloud 文件。
- 如果您使用的是 WorkSpaces，我們假設您熟悉 WorkSpaces。如需如何使用 WorkSpaces 的詳細資訊，請參閱 Amazon WorkSpaces 使用者指南。
- 如果您使用的是 VMware Cloud on AWS，我們假設您已熟悉它。如需詳細資訊，請參閱 VMware Cloud on AWS。
- 我們假設您熟悉 Microsoft Active Directory 概念。

先決條件

若要建立 Amazon FSx 檔案系統，您需要下列項目：

- 具有建立 Amazon FSx 檔案系統和 Amazon EC2 執行個體所需許可 AWS 的帳戶。如需詳細資訊，請參閱設定您的 AWS 帳戶。
- 根據您要與 Amazon FSx 檔案系統建立關聯的 Amazon VPC 服務，在虛擬私有雲端 (VPC) 中執行 Microsoft Windows Server 的 Amazon EC2 執行個體。 FSx 如需如何建立執行個體的詳細資訊，請參閱《Amazon EC2 使用者指南》中的 Amazon EC2 Windows 執行個體入門。Amazon EC2
- Amazon FSx 可與 Microsoft Active Directory 搭配使用，以執行使用者身分驗證和存取控制。您可以在建立時將 Amazon FSx 檔案系統加入 Microsoft Active Directory。如需詳細資訊，請參閱使用 Microsoft Active Directory。
- 本指南假設您尚未根據 Amazon VPC 服務變更 VPC 預設安全群組的規則。如果您有，則需要確保新增必要的規則，以允許從 Amazon EC2 執行個體到 Amazon FSx 檔案系統的網路流量。如需詳細資訊，請參閱Amazon FSx 的安全性。
- 安裝和設定 AWS Command Line Interface (AWS CLI)。支援的版本為 1.9.12 及更新版本。如需詳細資訊，請參閱《 使用者指南》中的安裝、更新和解除安裝 AWS CLI 。 AWS Command Line Interface

> **Note**
>
> 您可以檢查 AWS CLI 搭配 `aws --version`命令使用的 版本。

Amazon FSx for Windows File Server 論壇

如果您在使用 Amazon FSx 時遇到問題，請使用 論壇。

您是第一次使用 Amazon FSx 嗎？

如果您是第一次使用 Amazon FSx，我們建議您依序閱讀下列各節：

1. 如果您準備好建立第一個 Amazon FSx 檔案系統，請嘗試 Amazon FSx for Windows File Server 入門。
2. 如需有關效能的詳細資訊，請參閱FSx for Windows File Server 效能。
3. 如需 Amazon FSx 安全詳細資訊，請參閱 Amazon FSx 的安全性。

4. 如需 Amazon FSx API 的相關資訊，請參閱 Amazon FSx API 參考。

FSx for Windows File Server 的最佳實務

建議您在使用 Amazon FSx for Windows File Server 時遵循這些最佳實務。

主題

一般最佳實務

建立監控計畫

您可以使用檔案系統指標來監控儲存和效能用量、了解用量模式，並在用量接近檔案系統的儲存或效能限制時觸發通知。監控 Amazon FSx 檔案系統以及應用程式環境的其餘部分，可讓您快速偵錯可能影響效能的任何問題。

確保您的檔案系統有足夠的資源

資源不足可能會導致 I/O 請求的延遲和佇列增加，這可能會顯示為檔案系統完全或部分無法使用。如需監控效能和存取效能警告和建議的詳細資訊，請參閱 效能警告和建議。

安全最佳實務

我們建議您遵循這些最佳實務來管理檔案系統的安全性和存取控制。如需設定 Amazon FSx 以符合您的安全與合規目標的詳細資訊，請參閱 Amazon FSx 的安全性。

網路安全

請勿修改或刪除與您檔案系統相關聯的 ENI

您的 Amazon FSx 檔案系統是透過彈性網路界面 (ENI) 存取，該界面位於與您檔案系統相關聯的虛擬私有雲端 (VPC) 中。修改或刪除網路界面可能會導致 VPC 和檔案系統之間的連線永久中斷。

使用安全群組和網路 ACL

您可以使用安全群組和網路存取控制清單 (ACLs) 來限制對檔案系統的存取。對於 VPC 安全群組，預設安全群組已新增至主控台中的檔案系統。請確定您建立檔案系統之子網路的安全群組和網路 ACLs 允許連接埠上的流量。

Active Directory

當您建立 Amazon FSx 檔案系統時，您可以將其加入 Microsoft Active Directory 網域，以提供使用者身分驗證，以及共用、檔案和資料夾層級的存取控制授權。您的使用者可以使用其現有的 Active Directory 帳戶連線到檔案共用，並存取其中的檔案和資料夾。此外，您可以將現有的安全 ACL 組態遷移至 Amazon FSx，無需進行任何修改。Amazon FSx 為您提供兩種 Active Directory 選項：AWS 受管 Microsoft Active Directory 或自我管理 Microsoft Active Directory。

如果您使用的是 AWS 受管 Microsoft Active Directory，建議您保留 Active Directory 安全群組的預設設定。如果您修改這些設定，請確定您維護的網路組態符合網路需求。如需詳細資訊，請參閱網路先決條件。

如果您使用的是自我管理的 Microsoft Active Directory，您還有其他設定檔案系統的選項。將 Amazon FSx 與自我管理的 Microsoft Active Directory 搭配使用時，我們建議初始組態採用下列最佳實務：

- 將子網路指派給單一 Active Directory 網站：如果您的 Active Directory 環境有大量網域控制站，請使用 Active Directory 網站和服務，將 Amazon FSx 檔案系統所使用的子網路指派給具有最高可用性和可靠性的單一 Active Directory 網站。請確定DCs 上的 VPC 安全群組、VPC 網路 ACL、Windows 防火牆規則，以及您在 Active Directory 基礎設施中擁有的任何其他網路路由控制，允許在必要的連接埠上從 Amazon FSx 進行通訊。如果 Windows 無法使用指派的 Active Directory 網站，這可讓 Windows 還原至其他 DCs。如需詳細資訊，請參閱使用 Amazon VPC 的檔案系統存取控制。
- 使用單獨的組織單位 (OU)：為您的 Amazon FSx 檔案系統使用 OU，該檔案系統與您可能擁有的任何其他組織單位分開。
- 使用所需的最低權限設定您的服務帳戶：使用所需的最低權限設定或委派您提供給 Amazon FSx 的服務帳戶。如需詳細資訊，請參閱使用自我管理的 Microsoft Active Directory。
- 持續驗證您的 Active Directory 組態：在建立 Amazon FSx 檔案系統之前，針對您的 Active Directory 組態執行 Amazon FSx Active Directory 驗證工具，以驗證您的組態是否適用於 Amazon FSx，並探索工具可能公開的任何警告和錯誤。 FSx
- 使用 存放 Active Directory 登入 AWS Secrets Manager資料：您可以使用 AWS Secrets Manager 安全地存放和管理 Microsoft Active Directory 網域聯結服務帳戶登入資料。這種方法不需要在應用程式

程式碼或組態檔案中以純文字存放敏感登入資料，以強化您的安全狀態。如需詳細資訊，請參閱使用存放 Active Directory 登入資料 AWS Secrets Manager。

避免因 Active Directory 設定錯誤而失去可用性

搭配自我管理的 Microsoft Active Directory 使用 Amazon FSx 時，不僅在建立檔案系統期間擁有有效的 Active Directory 組態，而且對於持續的操作和可用性也很重要。在故障復原事件、例行維護事件和輸送量容量更新動作期間，Amazon FSx 會將檔案伺服器資源重新加入您的 Active Directory。如果 Active Directory 組態在事件期間無效，您的檔案系統會變更為設定錯誤的狀態，並且有無法使用的風險。以下是您可以避免失去可用性的一些方法：

- 使用 Amazon FSx 保持 Active Directory 組態更新：如果您進行變更，例如重設服務帳戶的密碼，請務必更新使用此服務帳戶的任何檔案系統的組態。
- 監控 Active Directory 設定錯誤：為自己設定設定錯誤狀態通知，以便您可以視需要重設檔案系統的 Active Directory 組態。如需使用 Lambda 型解決方案實現此目標的範例，請參閱使用 Amazon EventBridge 監控 Amazon FSx 檔案系統的運作狀態和 AWS Lambda 。
- 定期驗證您的 Active Directory 組態：如果您想要主動偵測 Active Directory 錯誤組態，我們建議您持續針對 Active Directory 組態執行 Active Directory 驗證工具。如果您在執行驗證工具時收到警告或錯誤，這表示您的檔案系統有設定錯誤的風險。
- 請勿移動或修改 FSx 建立的電腦物件：Amazon FSx 會使用您提供的服務帳戶和許可，在 Active Directory 中建立和管理電腦物件。移動或修改這些電腦物件可能會導致您的檔案系統設定錯誤。

Windows ACLs

透過 Amazon FSx，您可以使用標準 Windows 存取控制清單 (ACLs) 進行精細分級的共用、檔案和資料夾層級存取控制。Amazon FSx 檔案系統會自動驗證存取檔案系統資料以強制執行這些 Windows ACLs的使用者憑證。

- 請勿變更 SYSTEM 使用者的 NTFS ACL 許可：Amazon FSx 要求 SYSTEM 使用者擁有檔案系統內所有資料夾的完整控制 NTFS ACL 許可。變更 SYSTEM 使用者的 NTFS ACL 許可可能會導致您的檔案系統無法存取，且未來的檔案系統備份可能會變得無法使用。

設定和調整檔案系統的正確大小

選取部署類型

Amazon FSx 提供兩種部署選項：單一可用區和多可用區。對於大多數需要高可用性共用 Windows 檔案資料的生產工作負載，我們建議使用多可用區域檔案系統。如需詳細資訊，請參閱可用性和耐久性：單一可用區和多可用區檔案系統。

選取輸送量容量

為您的檔案系統設定足夠的輸送量容量，不僅符合工作負載的預期流量，還滿足支援您想要在檔案系統上啟用的功能所需的額外效能資源。例如，如果您正在執行重複資料刪除，您選取的輸送量容量必須提供足夠的記憶體，才能根據您擁有的儲存體執行重複資料刪除。如果您使用的是影子複本，請將輸送量容量增加到至少為工作負載預期驅動值的三倍的值，以避免 Windows Server 刪除您的影子複本。如需詳細資訊，請參閱輸送量容量對效能的影響。

增加儲存容量和輸送量容量

當檔案系統的可用儲存體不足，或預期您的儲存體需求增長大於目前的儲存體限制時，請增加檔案系統的儲存容量。我們建議您隨時在檔案系統上維持至少 20% 的可用儲存容量。我們也建議在增加儲存容量之前，將輸送量容量增加至少 20%，以抵消增加儲存期間的任何效能影響。您可以使用 FreeStorageCapacity CloudWatch 指標來監控可用的可用儲存量，並了解其趨勢。如需詳細資訊，請參閱管理儲存容量。

如果您的工作負載受限於目前的效能限制，您也應該增加檔案系統的輸送量容量。您可以使用 FSx 主控台上的監控和效能頁面，查看工作負載需求何時接近或超過效能限制，以判斷您的檔案系統是否針對工作負載佈建不足。

為了將儲存擴展持續時間降至最低，並避免降低寫入效能，建議您在增加儲存容量之前增加檔案系統的輸送量容量，然後在儲存容量增加完成後縮減輸送量容量。大多數工作負載在儲存擴展期間對效能的影響最小。不過，具有 HDD 儲存類型的檔案系統，以及涉及大量最終使用者、高階 I/O 或具有大量小型檔案的資料集的工作負載，可能會暫時降低效能。如需詳細資訊，請參閱儲存容量增加，且檔案系統效能。

修改閒置期間的輸送量容量

更新輸送量容量會中斷單一可用區檔案系統的可用性幾分鐘，並導致多可用區檔案系統的容錯移轉和容錯回復。對於多可用區域檔案系統，如果容錯移轉和容錯回復期間有持續的流量，則在此期間所做的任

何資料變更都需要在檔案伺服器之間同步。對於寫入密集型和 IOPS 密集型工作負載，資料同步程序最多可能需要數小時。雖然在此期間您的檔案系統將繼續可用，但我們建議您在檔案系統負載最少時，排定維護時段並在閒置期間執行輸送量容量更新，以減少資料同步的持續時間。如需進一步了解，請參閱管理輸送量容量。

Amazon FSx for Windows File Server 入門

接下來，您可以了解如何開始使用 FSx for Windows File Server。此入門練習包含下列步驟。

1. 註冊 AWS 帳戶 並在帳戶中建立管理使用者。
2. 使用 建立 AWS Managed Microsoft AD Active Directory Directory Service。您將將檔案系統和運算執行個體加入 Active Directory。
3. 建立執行 Microsoft Windows Server 的 Amazon Elastic Compute Cloud 運算執行個體。您將使用此執行個體來存取您的檔案系統。
4. 使用 Amazon FSx 主控台建立 Amazon FSx for Windows File Server 檔案系統。
5. 將檔案系統映射至 EC2 執行個體
6. 將資料寫入檔案系統。
7. 備份您的檔案系統。
8. 清除您建立的 資源。

主題

設定您的 AWS 帳戶

首次使用 Amazon FSx 之前，請先完成下列任務：

1. 註冊 AWS 帳戶

2. 建立具有管理存取權的使用者

註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

註冊 AWS 帳戶

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

   部分註冊程序需接收來電或簡訊，並在電話鍵盤輸入驗證碼。

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

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

建立具有管理存取權的使用者

註冊 後 AWS 帳戶，請保護您的 AWS 帳戶根使用者 AWS IAM Identity Center、啟用和建立管理使用者，如此您就不會將根使用者用於日常任務。

保護您的 AWS 帳戶根使用者

1. 選擇根使用者並輸入 AWS 帳戶 您的電子郵件地址，以帳戶擁有者AWS 管理主控台身分登入 。在下一頁中，輸入您的密碼。

   如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的以根使用者身分登入。
2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

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

建立具有管理存取權的使用者

1. 啟用 IAM Identity Center。

如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的啟用 AWS IAM Identity Center。

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

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

以具有管理存取權的使用者身分登入

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

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

指派存取權給其他使用者

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

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的建立許可集。

2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的新增群組。

步驟 1. 設定 Active Directory

使用 Amazon FSx，您可以針對 Windows 型工作負載操作全受管檔案儲存。同樣地， Directory Service 提供可在工作負載部署中使用的全受管目錄。如果您的現有企業 Active Directory 網域使用 EC2 執行個體在虛擬私有雲端 (VPC) AWS 中於 中執行，您可以啟用使用者型身分驗證和存取控制。您可以透過在 AWS Managed Microsoft Active Directory 和公司網域之間建立信任關係來執行此操作。對於 Amazon FSx 中的 Windows 身分驗證，您只需要單向樹系信任，其中 AWS 受管樹系信任公司網域樹系。

您的公司網域擔任信任網域的角色，而 Directory Service 受管網域則擔任信任網域的角色。已驗證的身分驗證請求只會以一個方向在網域之間傳輸，可讓公司網域中的帳戶針對受管網域中共用的資源進行身分驗證。在此情況下，Amazon FSx 只會與受管網域互動。受管網域接著會將身分驗證請求傳遞給您的公司網域。

> **Note**
>
> 您也可以將外部信任類型與 Amazon FSx 用於受信任網域。

您的 Active Directory 安全群組必須啟用來自 Amazon FSx 檔案系統安全群組的傳入存取。

建立適用於 Microsoft Active AWS Directory 的 Directory Services

- 如果您還沒有，請使用 Directory Service 來建立 AWS Managed Microsoft Active Directory 目錄。如需詳細資訊，請參閱《 AWS Directory Service 管理指南》中的建立您的 AWS 受管 Microsoft Active Directory。

  > **Important**
  >
  > 請記住您指派給管理員使用者的密碼；稍後在本入門練習中需要它。如果您忘記密碼，則需要對新 Directory Service 目錄和管理員使用者重複本練習中的步驟。

- 如果您有現有的 Active Directory，請在 AWS Managed Microsoft Active Directory 與現有的 Active Directory 之間建立信任關係。如需詳細資訊，請參閱《 管理指南》中的建立信任關係的時機。 AWS Directory Service

步驟 2：在 Amazon EC2 主控台中啟動 Windows 執行個體

您可以使用 啟動 Windows 執行個體 AWS 管理主控台 ，如下列程序所述。這是為了協助您快速啟動第一個執行個體，因此它不會涵蓋所有可能的選項。如需進階選項的詳細資訊，請參閱啟動執行個體。

啟動執行個體

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 請在主控台儀表板選擇 Launch Instance (啟動執行個體)。
3. Choose an Amazon Machine Image (AMI) (選擇 Amazon Machine Image (AMI)) 頁面會顯示基本的組態清單，稱為 Amazon Machine Image (AMI)，作用如同您執行個體的範本。選取適用於 Windows Server 2016 Base 或更新版本的 AMI。請注意，這些 AMI 會帶有 "Free tier eligible" (符合免費方案) 的標記。
4. 在 Choose an Instance Type (選擇執行個體類型) 頁面中，您可以選取您執行個體的硬體組態。選取 `t2.micro` 類型，其預設為選取。請注意，此執行個體類型符合免費方案資格。

5. 選擇 Review and Launch (檢閱和啟動)，讓精靈為您完成其他的組態設定。
6. 在檢閱執行個體啟動頁面的安全群組下，安全群組會顯示精靈已為您建立並選取。您可以使用此安全群組，也可以選擇您在設定時使用下列步驟建立的安全群組：

   a. 選擇 Edit security groups (編輯安全群組)。

   b. 在 Configure Security Group (設定安全群組) 頁面上，確定選取 Select an existing security group (選取現有的安全群組)。

   c. 從現有的安全群組清單中選取您的安全群組，然後選擇 Review and Launch (檢閱和啟動)。
7. 在 Review Instance Launch (檢閱執行個體啟動) 頁面，選擇 Launch (啟動)。
8. 當系統提示要求金鑰對時，請選取 Choose an existing key pair (選擇現有金鑰對)，然後選取您在設定時建立的金鑰對。

   或者，您也可以建立新的金鑰對。選取 Create a new key pair (建立新的金鑰對)，輸入金鑰對的名稱，然後選擇 Download Key Pair (下載金鑰對)。這是您儲存私有金鑰檔案的唯一機會，所以請務必下載它。將私有金鑰檔案存放在安全的地方。每次您連線至執行個體來啟動執行個體與對應的私有金鑰時，都需要提供您的金鑰對名稱。

   > ⚠ Warning
   >
   > 不要選取 Proceed without a key pair (不使用金鑰對而繼續) 選項。如果不使用金鑰對而啟動執行個體，就無法與它連線。

   準備就緒後，請選取 acknowledgment (確認) 核取方塊，然後選擇 Launch Instances (啟動執行個體)。
9. 會有確認頁面讓您知道您的執行個體正在啟動。選擇 View Instances (檢視執行個體) 關閉確認頁面並返回主控台。
10. 您可以在 Instances (執行個體) 畫面中檢視啟動狀態。啟動執行個體無須費時。當您啟動執行個體時，其初始狀態是 `pending`。在執行個體啟動後，其狀態會變更為 `running`，並得到公有的 DNS 名稱。（如果公有 DNS (IPv4) 或 (IPv6) 資料欄隱藏，請選擇頁面右上角的顯示/隱藏資料欄（齒輪形圖示），然後選取公有 DNS (IPv4) 或 (IPv6)。）
11. 執行個體可能需要幾分鐘的時間準備就緒讓您連線。確認您的執行個體是否已通過狀態檢查，您可以在 Status Checks (狀態檢查) 欄檢視此資訊。

> **Important**
>
> 請記下您啟動此執行個體時所建立之安全群組的 ID。當您建立 Amazon FSx 檔案系統時，將需要它。

現在您的執行個體已啟動，您可以連線至您的執行個體。

步驟 3：連接到您的執行個體

若要連線到 Windows 執行個體，您必須擷取初始系統管理員密碼，然後在使用遠端桌面連線到執行個體時指定此密碼。

系統管理員帳戶的名稱取決於作業系統的語言。例如，英文為管理員、法文為 Administrateur，葡萄牙文則為 Administrador。如需詳細資訊，請參閱 Microsoft TechNet Wiki 中的管理員帳戶在 Windows 中的當地語系化名稱。

如果您已將執行個體加入網域，您可以使用您在其中定義的網域登入資料來連線至執行個體 Directory Service。在遠端桌面登入畫面上，請勿使用本機電腦名稱和產生的密碼。請改用管理員的完整使用者名稱和此帳戶的密碼。例如，**`corp.example.com\Admin`**。

Windows Server 作業系統 (OS) 的授權允許兩個同時遠端連線用於管理目的。Windows Server 的授權包含在您的 Windows 執行個體價格中。如果您需要超過兩個同時的遠端連線，就必須購買 Remote Desktop Services (RDS) 授權。如果您嘗試第三個連線，就會出現錯誤。如需詳細資訊，請參閱設定連線允許的同時遠端連線數量。

使用 RDP 用戶端連線至您的 Windows 執行個體。

1. 在 Amazon EC2 主控台中，選取執行個體，然後選取 Connect (連線)。
2. 在連線至您的執行個體對話方塊中，選擇取得密碼 （ 啟動執行個體後需要幾分鐘的時間，才能使用密碼 ）。
3. 選擇 Browse (瀏覽) 並導覽至您在啟動執行個體時建立的私有金鑰檔案。選取檔案並選擇 Open (開啟)，將檔案的完整內容複製至 Contents (內容) 欄位。
4. 選擇 Decrypt Password (解密密碼)。主控台會在連線至您的執行個體對話方塊中顯示執行個體的預設管理員密碼，以實際密碼取代先前顯示的取得密碼連結。
5. 記錄預設的管理員密碼，或是複製到剪貼簿。您需要此密碼以連線至執行個體。
6. 選擇 Download Remote Desktop File (下載遠端桌面檔)。您的瀏覽器會提示您開啟或儲存 .rdp 檔案。兩個選項都可以。完成後，您可以選擇關閉以關閉連線至您的執行個體對話方塊。

- 如果您開啟了 .rdp 檔，將會看到 Remote Desktop Connection (遠端桌面連線) 對話方塊。
- 如果您儲存了 .rdp 檔案，請導覽至您的下載目錄，然後開啟 .rdp 檔案以顯示對話方塊。

7. 您可能會收到警告提示遠端連線的發佈者未知。您可以繼續連線至執行個體。
8. 提示出現時，使用作業系統的管理員帳戶以及您先前記錄或複製的密碼，登入執行個體。如果您的 Remote Desktop Connection (遠端桌面連線) 已設定管理員帳戶，您可能必須選擇 Use another account (使用其他帳戶) 選項，並手動輸入使用者名稱和密碼。

   > **Note**
   >
   > 有時候複製與貼上內容會損毀資料。如果您登入時遇到「密碼無效」錯誤，請嘗試手動輸入密碼。

9. 由於自我簽署憑證的性質，您可能會收到安全憑證無法驗證的警告。使用下列步驟驗證遠端電腦的身分，或者如果您信任此憑證，也可直接選擇 Yes (是) 或 Continue (繼續) 以繼續。

   a. 如果您是從 Windows PC 使用 Remote Desktop Connection (遠端桌面連線)，請選擇 View certificate (檢視憑證)。如果您是在 Mac 上使用 Microsoft Remote Desktop (Microsoft 遠端桌面)，請選擇 Show Certificate (顯示憑證)。

   b. 請選擇 Details (詳細資訊) 標籤，向下捲動至 Windows PC 上的 Thumbprint (拇指指紋) 項目，或是 Mac 上的 SHA1 Fingerprints (SHA1 指紋) 項目。這是遠端電腦安全憑證的唯一識別符。

   c. 在 Amazon EC2 主控台中選取執行個體，選取 Actions (動作)，然後選取 Get System Log (取得系統日誌)。

   d. 在系統日誌輸出尋找標示為 `RDPCERTIFICATE-THUMBPRINT` 的項目。如果此值符合憑證的拇指指紋或指紋，您就已驗證了遠端電腦的身分。

   e. 如果您是從 Windows PC 使用 Remote Desktop Connection (遠端桌面連線)，請返回憑證對話方塊並選擇 OK。如果您是在 Mac 上使用 Microsoft Remote Desktop (Microsoft 遠端桌面)，請返回驗證憑證並選擇繼續。

   f. [Windows] 選擇 Remote Desktop Connection (遠端桌面連線) 中的 Yes (是) 以連線到您的執行個體。

現在您已連線至執行個體，您可以將執行個體加入您的 Directory Service 目錄。

步驟 4：將執行個體加入您的 Directory Service 目錄

下列程序說明如何手動將現有的 Amazon EC2 Windows 執行個體加入您的 Directory Service 目錄。

將 Windows 執行個體加入 Directory Service 目錄

1. 使用任何遠端桌面協定用戶端連線到執行個體。
2. 開啟執行個體上的 TCP/IPv4 或 IPv6 屬性對話方塊。
   a. 開啟 Network Connections (網路連線)。

      > **Tip**
      >
      > 您可以在執行個體上，透過從命令提示執行下列命令，來直接開啟 Network Connections (網路連線)。
      >
      > ```
      > %SystemRoot%\system32\control.exe ncpa.cpl
      > ```

   b. 開啟任何已啟用網路連線的內容（按一下滑鼠右鍵）選單，然後選擇屬性。
   c. 在連線屬性對話方塊中，開啟（按兩下）網際網路通訊協定第 4 版或網際網路通訊協定第 6 版。
3. （選用）選取使用下列 DNS 伺服器地址，將偏好的 DNS 伺服器和備用 DNS 伺服器地址變更為 Directory Service所提供 DNS 伺服器的 IPv4 或 IPv6 地址，然後選擇確定。
4. 開啟執行個體的系統屬性對話方塊，選擇電腦名稱索引標籤，然後選擇變更。

   > **Tip**
   >
   > 您可以在執行個體上，透過從命令提示執行下列命令，來直接開啟 System Properties (系統內容對話方塊)。
   >
   > ```
   > %SystemRoot%\system32\control.exe sysdm.cpl
   > ```

5. 在成員方塊中，選擇網域，輸入 Directory Service 目錄的完整名稱，然後選擇確定。
6. 當系統提示您輸入網域管理員的名稱和密碼時，請輸入管理員帳戶的使用者名稱和密碼。

> **Note**
>
> 您可以輸入網域的完整名稱或 NetBios 名稱，後面接著反斜線 (\)，然後輸入使用者名稱，在此案例中為 Admin。例如，corp.example.com\Admin 或 corp\Admin。

7. 收到歡迎您加入網域的訊息之後，請重新啟動執行個體，讓變更生效。
8. 透過 RDP 重新連線至執行個體，並使用 Directory Service 目錄管理員使用者的使用者名稱和密碼登入執行個體。

現在您的執行個體已加入網域，您已準備好建立 Amazon FSx 檔案系統。

步驟 5. 建立您的檔案系統

建立檔案系統（主控台）

1. 開啟位於 https：//https://console.aws.amazon.com/fsx/ 的 Amazon FSx 主控台。
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 Select file system type (選取檔案系統類型) 頁面中，選擇 FSx for Windows File Server，然後選擇 Next (下一步)。Create file system (建立檔案系統) 頁面隨即顯示。
4. 對於建立方法，選擇標準建立。

檔案系統詳細資訊

1. 在 File system details (檔案系統詳細資訊) 區段中，輸入檔案系統的名稱。當您命名檔案系統時，更容易找到並管理您的檔案系統。您最多可以使用 256 個 Unicode 字母、空格和數字，加上特殊字元 + - = . _ : /
2. 針對部署類型，選擇異地同步備份或單一異地同步備份。

   - 選擇異地同步備份以部署可容忍可用區域無法使用的檔案系統。此選項支援 SSD 和 HDD 儲存。
   - 選擇單一可用區以部署部署在單一可用區域中的檔案系統。單一可用區 2 是最新一代的單一可用區域檔案系統，支援 SSD 和 HDD 儲存。

   如需詳細資訊，請參閱可用性和耐久性：單一可用區和多可用區檔案系統。
3. 對於儲存類型，您可以選擇 SSD 或 HDD。

FSx for Windows File Server 提供固態硬碟 (SSD) 和硬碟 (HDD) 儲存類型。SSD 儲存體專為最高效能和最延遲敏感的工作負載而設計，包括資料庫、媒體處理工作負載和資料分析應用程式。HDD 儲存體專為廣泛的工作負載而設計，包括主目錄、使用者和部門檔案共用，以及內容管理系統。如需詳細資訊，請參閱關於儲存體類型。

4. 對於佈建 SSD IOPS，您可以選擇自動或使用者佈建模式。

   如果您選擇自動模式，FSx for Windows File Server 會自動擴展您的 SSD IOPS，以維護每 GiB 儲存容量 3 個 SSD IOPS。如果您選擇使用者佈建模式，請輸入 96–400，000 範圍內的任何整數。擴展超過 80，000 個 SSD IOPS 適用於美國東部（維吉尼亞北部）、美國西部（奧勒岡）、美國東部（俄亥俄）、歐洲（愛爾蘭）、亞太區域（東京）和亞太區域（新加坡）。如需詳細資訊，請參閱管理 SSD IOPS。

5. 對於儲存容量，請以 GiB 為單位輸入檔案系統的儲存容量。如果您使用的是 SSD 儲存，請輸入 32–65，536 範圍內的任何整數。如果您使用的是 HDD 儲存，請輸入 2，000–65，536 範圍內的任何整數。您可以在建立檔案系統之後，隨時視需要增加儲存容量。如需詳細資訊，請參閱管理儲存容量。

6. 保留 Throughput capacity (輸送容量) 的預設設定。輸送量容量是託管檔案系統的檔案伺服器可以提供資料的持續速度。建議的輸送量容量設定取決於您選擇的儲存容量。如果您需要超過建議的輸送量容量，請選擇指定輸送量容量，然後選擇值。如需詳細資訊，請參閱FSx for Windows File Server 效能。

   > **Note**
   >
   > 如果您要啟用檔案存取稽核，您必須選擇 32 MBps 或更高的輸送量容量。如需詳細資訊，請參閱使用檔案存取稽核記錄最終使用者存取。

   您可以在建立檔案系統之後隨時視需要修改輸送量容量。如需詳細資訊，請參閱管理輸送量容量。

網路與安全

1. 在網路與安全區段中，選擇您要與檔案系統建立關聯的 Amazon VPC。針對此入門練習，請選擇您為 Directory Service 目錄和 Amazon EC2 執行個體選擇的相同 Amazon VPC。

2. 對於 VPC 安全群組，預設 Amazon VPC 的預設安全群組已新增至主控台中的檔案系統。如果您不是使用預設安全群組，請確定您選擇的安全群組與您的檔案系統 AWS 區域 位於相同的 中。為

了確保您可以將 EC2 執行個體與您的檔案系統連線，您需要將下列規則新增至您選擇的安全群組：

a. 新增下列傳入和傳出規則，以允許下列連接埠。

Rules	連接埠
UDP	53、88、123、389、464
TCP	53、88、135、389、445、464、636、3268、3269、5985、9389、49152-65535

將您要從中存取檔案系統之用戶端運算執行個體相關聯的 IP 地址或安全群組 IDs 新增 和 。

b. 新增傳出規則，以允許所有流量流向您要加入檔案系統的 Active Directory。若要執行此操作，請執行以下其中一項操作：

- 允許傳出流量到與 AWS Managed AD 目錄相關聯的安全群組 ID。
- 允許傳出流量傳送到與自我管理 Active Directory 網域控制站相關聯的 IP 地址。

> **Note**
>
> 在某些情況下，您可能已從預設設定修改 AWS Managed Microsoft AD 安全群組的規則。如果是這樣，請確定此安全群組具有必要的傳入規則，以允許來自 Amazon FSx 檔案系統的流量。如需所需傳入規則的詳細資訊，請參閱《 AWS Directory Service 管理指南》中的AWS Managed Microsoft AD 先決條件。

如需詳細資訊，請參閱使用 Amazon VPC 的檔案系統存取控制。

3. 多可用區域檔案系統具有主要和待命檔案伺服器，每個伺服器都在自己的可用區域和子網路中。如果您要建立多可用區檔案系統 （ 請參閱步驟 5)，請為主要檔案伺服器選擇偏好的子網路值，並為待命檔案伺服器選擇待命子網路值。

   如果您要建立單一可用區檔案系統，請選擇檔案系統的子網路。

4. 針對網路類型，選取 IPv4 （ 僅適用於 IPv4 支援 ） 或雙堆疊 （ 適用於 IPv4 和 IPv6 支援 ）。您可以隨時變更現有檔案系統的網路類型。如需詳細資訊，請參閱變更網路類型。

> **Note**
>
> 如果您想要建立使用雙堆疊模式的 FSx for Windows File Server 檔案系統，您必須先將 Amazon 提供的 IPv6 CIDR 區塊指派給 VPC 和子網路。如需詳細資訊，請參閱《Amazon Virtual Private Cloud 使用者指南》中的新增 VPC 的 IPv6 支援。

Windows 身分驗證

- 對於 Windows 身分驗證，您有下列選項：

  如果您想要將檔案系統加入由 管理的 Microsoft Active Directory 網域，請選擇 AWS Managed Microsoft Active Directory AWS，然後從清單中選擇您的 Directory Service 目錄。如需詳細資訊，請參閱使用 Microsoft Active Directory。

  如果您想要將檔案系統加入自我管理的 Microsoft Active Directory 網域，請選擇自我管理的 Microsoft Active Directory，並提供 Active Directory 的下列詳細資訊。如需更多資訊，請參閱使用自我管理的 Microsoft Active Directory。

  - Active Directory 的完整網域名稱。

    > **Important**
    >
    > 對於單一可用區 2 和所有多可用區檔案系統，Active Directory 網域名稱不能超過 47 個字元。此限制同時適用於 Directory Service 和自我管理的 Active Directory 網域名稱。Amazon FSx 需要直接連接內部流量到您的 DNS IP 地址。不支援透過網際網路閘道連線。反之，請使用 AWS Virtual Private Network VPC 對等 Direct Connect互連、 或 AWS Transit Gateway 關聯。

  - DNS 伺服器 IP 地址 — 網域 DNS 伺服器的 IPv4 或 IPv6 地址。

    > **Note**
    >
    > 您的 DNS 伺服器必須啟用 EDNS (DNS 的擴充機制）。如果停用 EDNS，您的檔案系統可能無法建立。

  - Amazon FSx 用來將檔案系統加入網域的 Active Directory 服務帳戶的登入資料。您可以提供下列其中一種方式：

    - 選項 1： AWS Secrets Manager 秘密 ARN - 包含 Active Directory 網域上服務帳戶的使用者名稱和密碼的秘密。如需詳細資訊，請參閱使用 存放 Active Directory 登入資料 AWS Secrets Manager。
    - 選項 2：純文字登入資料
        - 服務帳戶使用者名稱 – 現有 Microsoft Active Directory 中服務帳戶的使用者名稱。請勿包含網域字首或尾碼。例如，對於 `EXAMPLE\ADMIN`，僅使用 `ADMIN`。
        - 服務帳戶密碼 – 服務帳戶的密碼。
- （選用）組織單位 (OU) - 您要加入檔案系統之組織單位的辨別路徑名稱。
- （選用）委派檔案系統管理員群組 — Active Directory 中可管理檔案系統的群組名稱。預設群組為「網域管理員」。如需詳細資訊，請參閱Amazon FSx 服務帳戶。

加密、稽核和存取 (DNS 別名）

1. 針對加密，選擇用來加密靜態檔案系統上資料的 AWS KMS key 加密金鑰。您可以透過指定金鑰的 ARN AWS KMS，選擇由 管理的預設 aws/fsx （預設）、現有金鑰或客戶受管金鑰。如需詳細資訊，請參閱靜態資料加密。
2. 針對稽核 - 選用，預設會停用檔案存取稽核。如需啟用和設定檔案存取稽核的詳細資訊，請參閱使用檔案存取稽核記錄最終使用者存取。
3. 針對存取 - 選用，輸入您要與檔案系統建立關聯的任何 DNS 別名。每個別名名稱都必須格式化為完整網域名稱 (FQDN)。如需詳細資訊，請參閱管理 DNS 別名。

備份和維護

如需自動每日備份和本節中設定的詳細資訊，請參閱 使用備份保護您的資料。

1. 預設會啟用每日自動備份。如果您不希望 Amazon FSx 每天自動備份檔案系統，您可以停用此設定。
2. 如果啟用自動備份，它們會在稱為備份時段的期間內發生。您可以使用預設時段，或選擇最適合工作流程的自動備份時段開始時間。
3. 對於自動備份保留期間，您可以使用預設設定 30 天，或將 Amazon FSx 將保留檔案系統自動每日備份的值設定為 1 到 90 天。此設定不適用於使用者啟動的備份，或 採取的備份 AWS Backup。
4. 對於標籤 - 選用，輸入索引鍵和值以將標籤新增至檔案系統。標籤是區分大小寫的鍵值組，可協助您管理、篩選和搜尋檔案系統。如需詳細資訊，請參閱標記 Amazon FSx 資源。

選擇下一步。

檢閱您的組態並建立

1. 檢閱顯示在 Create file system (建立檔案系統) 頁面上的檔案系統組態。供您參考，您可以查看在建立檔案系統之後，可以和不可以修改哪些檔案系統設定。選擇 Create file system (建立檔案系統)。
2. Amazon FSx 建立檔案系統後，請從檔案系統儀表板的清單中選擇檔案系統 ID，以檢視詳細資訊。選擇連接，並在網路與安全索引標籤中記下檔案系統的 DNS 名稱。在下列程序中，您需要它才能將共享映射至 EC2 執行個體。

步驟 6. 將檔案共享映射至執行 Windows Server 的 EC2 執行個體

您現在可以將 Amazon FSx 檔案系統掛載到已加入 Directory Service 目錄的 Microsoft Windows Amazon EC2 執行個體。檔案共享的名稱與檔案系統的名稱不同。

使用 GUI 在 Amazon EC2 Windows 執行個體上映射檔案共享

1. 在 Windows 執行個體上掛載檔案共享之前，您必須先啟動 EC2 執行個體，並將其加入檔案系統已加入 AWS Directory Service for Microsoft Active Directory 的 。若要執行此動作，請從 AWS Directory Service 管理指南中選擇下列其中一個程序：
   - 無縫加入 Windows EC2 執行個體
   - 手動加入 Windows 執行個體
2. 連線到您的執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的連線至 Windows 執行個體。
3. 連線後，開啟 File Explorer。
4. 從導覽窗格中，開啟網路的內容 （ 按一下滑鼠右鍵 ） 選單，然後選擇映射網路磁碟機。
5. 為 Drive 選擇您選擇的磁碟機代號。
6. 您可以使用 Amazon FSx 指派的預設 DNS 名稱，或使用您選擇的 DNS 別名來映射檔案系統。此程序說明使用預設 DNS 名稱映射檔案共享。如果您想要使用 DNS 別名對應檔案共享，請參閱 使用 DNS 別名存取資料。

   針對資料夾，輸入檔案系統 DNS 名稱和共用名稱。預設的 Amazon FSx 共享稱為 `\share`。您可以在 Amazon FSx 主控台、https：//https://console.aws.amazon.com/fsx/、Windows File Server > Network & Security 區段，或 CreateFileSystem或 DescribeFileSystems API 命令的回應中找到 DNS 名稱。

   - 對於加入 AWS 受管 Microsoft Active Directory 的單一可用區檔案系統，DNS 名稱如下所示。

```
fs-0123456789abcdef0.ad-domain.com
```

- 對於加入自我管理 Active Directory 的單一可用區檔案系統，以及任何多可用區檔案系統，DNS 名稱如下所示。

```
amznfsxaa11bb22.ad-domain.com
```

例如，輸入 \\fs-0123456789abcdef0.*ad-domain*.com\share。

7. 選擇檔案共享是否應在登入時重新連線，然後選擇完成。

步驟 7. 將資料寫入檔案共享

現在您已將檔案共享映射至執行個體，您可以像 Windows 環境中的任何其他目錄一樣使用檔案共享。

將資料寫入檔案共享

1. 開啟記事本文字編輯器。
2. 在文字編輯器中撰寫一些內容。例如：*###World#*
3. 將檔案儲存至檔案共享的磁碟機代號。
4. 使用 File Explorer，導覽至檔案共享並尋找您剛儲存的文字檔案。

步驟 8. 備份您的檔案系統

現在您已有機會使用 Amazon FSx 檔案系統及其檔案共享，您可以備份它。根據預設，每日備份會在檔案系統的 30 分鐘備份時段期間自動建立。不過，您可以隨時建立使用者起始的備份。備份有與其相關聯的額外費用。如需備份定價的詳細資訊，請參閱 定價。

從主控台建立檔案系統的備份

1. 在 https://console.aws.amazon.com/fsx/：// 開啟 Amazon FSx 主控台。
2. 從主控台儀表板中，選擇您為此練習建立的檔案系統名稱。
3. 從檔案系統的概觀索引標籤中，選擇建立備份。
4. 在開啟的建立備份對話方塊中，提供備份的名稱。此名稱最多可包含 256 個 Unicode 字母，並包含空格、數字和下列特殊字元：+ - = . _ : /

5. 選擇 Create backup (建立備份)。
6. 若要檢視清單中的所有備份，以便您可以還原檔案系統或刪除備份，請選擇備份。

當您建立新的備份時，其狀態會在建立時設定為 CREATING。這可能需要幾分鐘的時間。當備份可供使用時，其狀態會變更為可用。

步驟 9. 清除資源

完成本練習後，您應該遵循這些步驟來清理資源並保護 AWS 您的帳戶。

清理資源

1. 在 Amazon EC2 主控台上，終止您的執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的終止您的執行個體。
2. 在 Amazon FSx 主控台上，刪除您的檔案系統。所有自動備份都會自動刪除。不過，您仍然需要刪除手動建立的備份。下列步驟概述此程序：
   a. 在 https://console.aws.amazon.com/fsx/：// 開啟 Amazon FSx 主控台。
   b. 從主控台儀表板中，選擇您為此練習建立的檔案系統名稱。
   c. 針對 Actions (動作)，選擇 Delete file system (刪除檔案系統)。
   d. 在開啟的刪除檔案系統對話方塊中，決定您是否要建立最終備份。如果您這麼做，請提供最終備份的名稱。也會刪除任何自動建立的備份。

      > **Important**
      > 您可以從備份建立新的檔案系統。建議您建立最終備份做為最佳實務。如果您發現在一段時間後不需要它，您可以刪除此備份和其他手動建立的備份。

   e. 在檔案系統 ID 方塊中，輸入您要刪除的檔案系統 ID。
   f. 選擇刪除檔案系統。
   g. 檔案系統現在正在刪除，且儀表板中的狀態會變更為刪除。刪除檔案系統後，它就不會再出現在儀表板中。
   h. 現在您可以刪除檔案系統的任何手動建立的備份。從左側導覽中，選擇備份。
   i. 從儀表板中，選擇與您刪除的檔案系統 ID 相同的任何備份，然後選擇刪除備份。
   j. 刪除備份對話方塊隨即開啟。勾選您所選備份 ID 的核取方塊，然後選擇刪除備份。

您的 Amazon FSx 檔案系統和相關的自動備份現已刪除。

3. 若要刪除您為此練習建立的 Directory Service 目錄，請參閱《 AWS Directory Service 管理指南》中的刪除您的目錄。

存取您的資料

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

主題

支援的用戶端

FSx for Windows File Server 支援伺服器訊息區塊 (SMB) 通訊協定 2.0 到 3.1.1 版，可讓您靈活地使用各種運算執行個體和作業系統連線到檔案系統。

下列 AWS 運算執行個體支援與 Amazon FSx 搭配使用：

- Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，包括 Microsoft Windows、Mac、Amazon Linux 和 Amazon Linux 2 執行個體。如需詳細資訊，請參閱映射檔案共享。
- Amazon Elastic Container Service (Amazon ECS) 容器。如需詳細資訊，請參閱《Amazon Elastic Container Service 開發人員指南》中的 FSx for Windows File Server 磁碟區。
- WorkSpaces 執行個體 – 若要進一步了解，請參閱 AWS 部落格文章使用 FSx for Windows File Server 搭配 Amazon WorkSpaces。
- Amazon AppStream 2.0 執行個體 – 若要進一步了解，請參閱使用 Amazon FSx 搭配 Amazon AppStream 2.0 的 AWS 部落格文章。
- 在 VMware Cloud on AWS environment 中執行VMs – 若要進一步了解，請參閱 AWS 部落格文章，在 VMware Cloud on AWS Environment 中存放檔案並與 FSx for Windows File Server 共用檔案。

下列作業系統支援與 Amazon FSx 搭配使用：

- Windows Server 2008、Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019 和 Windows Server 2022。
- Windows Vista、Windows 7、Windows 8、Windows 8.1、Windows 10（包括 WorkSpaces 的 Windows 7 和 Windows 10 桌面體驗）和 Windows 11。
- Linux，使用 `cifs-utils`工具。
- macOS

從 內存取資料 AWS 雲端

每個 Amazon FSx 檔案系統都與 Virtual Private Cloud (VPC) 相關聯。無論可用區域為何，您都可以從檔案系統的 VPC 中的任何位置存取 FSx for Windows File Server 檔案系統。您也可以從與檔案系統不同的 AWS 帳戶 VPCs 或 AWS 區域 存取檔案系統。除了以下各節所述存取 FSx for Windows File Server 資源的需求之外，您也需要確保已設定檔案系統的 VPC 安全群組，以便資料和管理流量可在檔案系統和用戶端之間流動。如需使用所需連接埠設定安全群組的詳細資訊，請參閱 使用 Amazon VPC 的檔案系統存取控制。

您可以從與檔案系統位於相同 VPC 的支援用戶端存取 FSx for Windows File Server 檔案系統。

下表說明 Amazon FSx 支援從每個支援環境中的用戶端存取的環境，取決於檔案系統建立的時間。

位於...的用戶端	存取 2019 年 2 月 22 日之前建立的檔案系統	存取 2020 年 12 月 17 日之前建立的檔案系統	存取 2020 年 12 月 17 日之後建立的檔案系統
建立檔案系統的子網路	✓	✓	✓
建立檔案系統所在 VPC 的主要 CIDR 區塊	✓	✓	✓
建立檔案系統的 VPC 次要 CIDRs 其他 CIDRs 或對等網路		在 RFC 1918 私有 IP 地址範圍內 IP 地址的用戶端： • 10.0.0.0/8	IP 地址超出下列 CIDR 區塊範圍的用戶端：198.19.0.0/16

位於...的用戶端	存取 2019 年 2 月 22 日之前建立的檔案系統	存取 2020 年 12 月 17 日之前建立的檔案系統	存取 2020 年 12 月 17 日之後建立的檔案系統
		• 172.16.0.0/12 • 192.168.0.0/16	

> **Note**
>
> 在某些情況下，您可能想要使用非私有 IP 地址範圍，從內部部署存取 2020 年 12 月 17 日之前建立的檔案系統。若要這樣做，請從檔案系統的備份建立新的檔案系統。如需詳細資訊，請參閱使用備份保護您的資料。

從不同的 VPC 存取資料 AWS 帳戶，或 AWS 區域

您可以從位於不同 VPC 中的支援用戶端 AWS 帳戶，或是使用 VPC 對等互連或傳輸閘道與檔案系統 AWS 區域 相關聯的用戶端，存取 FSx for Windows File Server 檔案系統。當您使用 VPC 對等互連或傳輸閘道來連接 VPCs 時，在一個 VPC 中的運算執行個體可以存取另一個 VPC 中的 Amazon FSx 檔案系統。即使 VPCs屬於不同的 AWS 帳戶，即使 VPCs位於不同的 中，此存取也是可能的 AWS 區域。

VPC 對等互連是兩個 VPCs之間的網路連線，您可以使用私有 IPv4 或 IP 第 6 版 (IPv6) 地址在它們之間路由流量。您可以使用 VPC 對等互連來連接相同 AWS 區域內或 AWS 區域之間的 VPCs。如需 VPC 互連的詳細資訊，請參閱《Amazon VPC 互連指南》中的什麼是 VPC 互連？。

傳輸閘道是網路傳輸中樞，您可以用於互相連接 VPC 和現場部署網路。如需使用 VPC 傳輸閘道的詳細資訊，請參閱 Amazon VPC 傳輸閘道中的傳輸閘道入門。

設定 VPC 對等互連或傳輸閘道連線後，您可以使用檔案系統 DNS 名稱來存取檔案系統。就像從相關聯 VPC 內的運算執行個體執行一樣。

從內部部署存取資料

FSx for Windows File Server 支援使用 AWS Direct Connect 或 Site-to-Site VPN ，從內部部署運算執行個體存取您的檔案系統。透過 的支援 AWS Direct Connect，FSx for Windows File Server 可讓您透過內部部署環境的專用網路連線存取檔案系統。透過 的支援 Site-to-Site VPN，FSx for Windows File Server 可讓您透過安全和私有通道，從內部部署裝置存取檔案系統。

將內部部署環境連線至與 Amazon FSx 檔案系統相關聯的 VPC 之後，您可以使用其 DNS 名稱或 DNS 別名來存取檔案系統。就像從 VPC 內的運算執行個體一樣。如需 Direct Connect的詳細資訊，請參閱《Direct Connect 使用者指南》。如需設定 Site-to-Site VPN 連線的詳細資訊，請參閱《Amazon VPC 使用者指南》中的 VPN 連線。

> **Note**
>
> 在某些情況下，您可能想要使用非私有 IP 地址範圍，從內部部署存取 2020 年 12 月 17 日之前建立的檔案系統。若要這樣做，請從檔案系統的備份建立新的檔案系統。如需詳細資訊，請參閱使用備份保護您的資料。

FSx for Windows File Server 也支援使用 Amazon FSx File Gateway，從內部部署運算執行個體提供低延遲、無縫存取雲端 FSx for Windows File Server 檔案共享。如需詳細資訊，請參閱《Amazon FSx 檔案閘道使用者指南》。

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

使用預設 DNS 名稱存取資料

FSx for Windows File Server 為每個檔案系統提供網域名稱系統 (DNS) 名稱。您可以使用此 DNS 名稱，將運算執行個體上的磁碟機代號映射至 Amazon FSx 檔案共享，以存取 FSx FSx for Windows File Server 檔案系統。如需進一步了解，請參閱 使用檔案共享存取資料。

> **Important**
>
> 如果您使用 Microsoft DNS 做為預設 DNS，Amazon FSx 只會註冊檔案系統的 DNS 記錄。如果您使用第三方 DNS，則必須手動設定 Amazon FSx 檔案系統的 DNS 項目。如需選擇要用於檔案系統的正確 IP 地址的詳細資訊，請參閱 取得用於手動 DNS 項目的正確檔案系統 IP 地址。

若要尋找 DNS 名稱：

- 在 Amazon FSx 主控台中，選擇檔案系統，然後選擇詳細資訊。在網路與安全區段中檢視 DNS 名稱。
- 或者，在 CreateFileSystem或 DescribeFileSystems API 命令的回應中檢視它。

對於加入 AWS Managed Microsoft Active Directory 的所有單一可用區檔案系統，DNS 名稱的格式如下： `fs-0123456789abcdef0.`*`ad-dns-domain-name`*

對於加入自我管理 Active Directory 的所有單一可用區檔案系統，以及任何多可用區檔案系統，DNS 名稱的格式如下： `amznfsxaa11bb22.`*`ad-domain`*`.com`

使用 Kerberos 身分驗證搭配 DNS 名稱

我們建議您在 Amazon FSx 傳輸中使用 Kerberos 型身分驗證和加密。Kerberos 為存取檔案系統的用戶端提供最安全的身分驗證。若要為 SMB 工作階段啟用傳輸中資料的 Kerberos 型身分驗證和加密，請使用 Amazon FSx 提供的檔案系統 DNS 名稱來存取您的檔案系統。

如果您的 AWS Managed Microsoft Active Directory 和內部部署 Active Directory 之間設定了外部信任，若要使用 Amazon FSx Remote PowerShell 搭配 Kerberos 身分驗證，您必須在用戶端上設定本機群組政策，以取得樹系搜尋順序。如需詳細資訊，請參閱 Microsoft 文件中的設定 Kerberos 樹系搜尋順序 (KFSO)。

支援分散式檔案系統 (DFS) 命名空間

FSx for Windows File Server 支援使用 Microsoft DFS 命名空間。使用 DFS 命名空間，將位於多個檔案系統上的檔案共用組織成一個通用資料夾結構（命名空間），供您用來存取整個檔案資料集。您可以使用 DFS 命名空間中的名稱，將 Amazon FSx 檔案系統的連結目標設定為檔案系統的 DNS 名稱，以存取該檔案系統。如需詳細資訊，請參閱使用 DFS 命名空間將多個 FSx for Windows File Server 檔案系統分組。

使用 DNS 別名存取資料

FSx for Windows File Server 為每個檔案系統提供 DNS 名稱，您可以用來存取檔案共享。您也可以註冊 FSx for Windows File Server 檔案系統的 DNS 別名，以使用預設 DNS 名稱以外的 DNS 名稱來存取檔案共享。

使用 DNS 別名，您可以將 Windows 檔案共用資料移至 FSx for Windows File Server，然後繼續使用現有的 DNS 名稱來存取 Amazon FSx 上的資料。DNS 別名也可讓您使用有意義的名稱，讓您更輕鬆

地管理工具和應用程式以連線至 Amazon FSx 檔案系統。您一次最多可將 50 個 DNS 別名與檔案系統建立關聯。如需將 DNS 別名與 FSx for Windows File Server 檔案系統建立關聯和取消關聯的詳細資訊，請參閱 管理 DNS 別名。

若要使用 DNS 別名設定對 FSx for Windows File Server 檔案系統的存取，您必須執行下列步驟：

1. 將 DNS 別名與您的檔案系統建立關聯.
2. 建立檔案系統的 DNS CNAME 記錄，以及與其相關聯的 DNS 別名。

如需搭配 FSx for Windows File Server 檔案系統使用 DNS 別名的詳細資訊，請參閱 管理 DNS 別名。

使用 Kerberos 身分驗證和加密搭配 DNS 別名

我們建議您在 Amazon FSx 傳輸中使用 Kerberos 型身分驗證和加密。Kerberos 為存取檔案系統的用戶端提供最安全的身分驗證。若要為使用 DNS 別名存取 Amazon FSx 的用戶端啟用 Kerberos 身分驗證，您必須新增對應至 Amazon FSx 檔案系統 Active Directory 電腦物件上 DNS 別名的服務主體名稱 (SPNs)。

若要在使用 DNS 別名存取檔案系統時設定 Kerberos 身分驗證和加密，請參閱 設定 Kerberos 的服務主體名稱 (SPNs)。

您可以選擇強制使用 DNS 別名存取檔案系統的用戶端使用 Kerberos 身分驗證和加密，方法是在 Active Directory 中設定下列群組政策物件 (GPOs)：

- 限制 NTLM：傳出 NTLM 流量至遠端伺服器 - 使用此政策設定，拒絕或稽核從電腦傳出 NTLM 流量至執行 Windows 作業系統的任何遠端伺服器。
- 限制 NTLM：為 NTLM 身分驗證新增遠端伺服器例外狀況 - 如果設定網路安全：限制 NTLM：將 NTLM 流量傳出至遠端伺服器政策設定，請使用此政策設定來建立允許用戶端裝置使用 NTLM 身分驗證的遠端伺服器例外狀況清單。

若要在使用 DNS 別名存取檔案系統時強制執行 Kerberos 身分驗證和加密，請參閱 使用群組政策物件 (GPOs) 強制執行 Kerberos 身分驗證。

如需將檔案系統設定為使用 DNS 別名的詳細資訊，請參閱下列程序：

- 將 DNS 別名與您的檔案系統建立關聯
- 設定 Kerberos 的服務主體名稱 (SPNs)
- 更新或建立 DNS CNAME 記錄

- 使用群組政策物件 (GPOs) 強制執行 Kerberos 身分驗證

將 DNS 別名與您的檔案系統建立關聯

您可以在建立新檔案系統時，以及使用 Amazon FSx 主控台、CLI 和 API 從備份建立新檔案系統時，將 DNS 別名與現有的 FSx for Windows File Server 檔案系統建立關聯。如果您要使用不同的網域名稱建立別名，請輸入完整名稱，包括父系網域，以建立別名的關聯。

此程序說明如何在使用 Amazon FSx 主控台建立新檔案系統時關聯 DNS 別名。如需將 DNS 別名與現有檔案系統建立關聯的相關資訊，以及使用 CLI 和 API 的詳細資訊，請參閱 管理 DNS 別名。

在建立新檔案系統時關聯 DNS 別名

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/：//。
2. 請遵循入門一節步驟 5. 建立您的檔案系統中所述建立新檔案系統的程序。
3. 在建立檔案系統精靈的存取 - 選用區段中，輸入您要與檔案系統建立關聯的 DNS 別名。

   指定 DNS 別名時，請使用下列準則：

   - 必須格式化為完整網域名稱 (FQDN)*hostname.domain*，例如 `accounting.example.com`。
   - 可包含英數字元和連字號 (-)。
   - 名稱開頭或結尾不能為連字號 (-)。
   - 可以從數字開頭。

   對於 DNS 別名名稱，Amazon FSx 會將字母字元儲存為小寫字母 (a-z)，不論儲存時指定為大寫、小寫字母或逸出碼中的對應字母。
4. 針對維護偏好設定，進行任何您想要的變更。
5. 在標籤 - 選用區段中，新增您需要的任何標籤，然後選擇下一步。
6. 檢閱顯示在 Create file system (建立檔案系統) 頁面上的檔案系統組態。選擇建立檔案系統以建立檔案系統。

設定 Kerberos 的服務主體名稱 (SPNs)

我們建議您在 Amazon FSx 傳輸中使用 Kerberos 型身分驗證和加密。Kerberos 為存取檔案系統的用戶端提供最安全的身分驗證。

若要為使用 DNS 別名存取 Amazon FSx 的用戶端啟用 Kerberos 身分驗證，您必須新增對應至 Amazon FSx 檔案系統 Active Directory 電腦物件上 DNS 別名的服務主體名稱 (SPNs)。SPN 一次只能與單一 Active Directory 電腦物件建立關聯。如果您為原始檔案系統 Active Directory 電腦物件設定的 DNS 名稱有現有的 SPNs，您必須先刪除它們。

Kerberos 身分驗證需要兩個 SPNs：

```
HOST/alias
HOST/alias.domain
```

如果別名為 `finance.domain.com`，則下列是兩個必要的 SPNs：

```
HOST/finance
HOST/finance.domain.com
```

> **Note**
>
> 您必須先刪除與 Active Directory 電腦物件上 DNS 別名對應的任何現有 HOST SPNs，才能為 Amazon FSx 檔案系統 Active Directory (AD) 電腦物件建立新的 HOST SPNs。如果 AD 中存在 DNS 別名SPNs，則嘗試設定 Amazon FSx 檔案系統的 SPN 將會失敗。

下列程序說明如何執行下列動作：

- 在原始檔案系統的 Active Directory 電腦物件上尋找任何現有的 DNS 別名 SPNs。
- 刪除找到的現有 SPNs，如果有的話。
- 為 Amazon FSx 檔案系統的 Active Directory 電腦物件建立新的 DNS 別名 SPNs。

安裝所需的 PowerShell Active Directory 模組

1. 登入已加入您 Amazon FSx 檔案系統之 Active Directory 的 Windows 執行個體。
2. 以管理員身分開啟 PowerShell。
3. 使用下列命令安裝 PowerShell Active Directory 模組。

   ```
   Install-WindowsFeature RSAT-AD-PowerShell
   ```

在原始檔案系統的 Active Directory 電腦物件上尋找和刪除現有的 DNS 別名 SPNs

如果您已針對已指派給 Active Directory 中電腦物件上另一個檔案系統的 DNS 別名設定 SPNs，您必須先移除這些 SPNs才能將 SPNs 新增至檔案系統的電腦物件。

1. 使用下列命令尋找任何現有的 SPNs。*alias_fqdn* 將 取代為您在步驟 1 中與檔案系統相關聯的 DNS 別名。

```
## Find SPNs for original file system's AD computer object
$ALIAS = "alias_fqdn"
SetSPN /Q ("HOST/" + $ALIAS)
SetSPN /Q ("HOST/" + $ALIAS.Split(".")[0])
```

2. 使用下列範例指令碼刪除上一個步驟中傳回的現有 HOST SPNs。

   - *alias_fqdn* 將 取代為您在步驟 1 中與檔案系統相關聯的完整 DNS 別名。
   - *file_system_DNS_name* 將 取代為原始檔案系統的 DNS 名稱。

```
## Delete SPNs for original file system's AD computer object
$Alias = "alias_fqdn"
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})

SetSPN /D ("HOST/" + ${Alias}) ${FSxAdComputer}.Name
SetSPN /D ("HOST/" + ${Alias}.Split(".")[0]) ${FSxAdComputer}.Name
```

3. 針對您在步驟 1 中與檔案系統相關聯的每個 DNS 別名重複上述步驟。

在 Amazon FSx 檔案系統的 Active Directory 電腦物件上設定 SPNs

1. 執行下列命令，為您的 Amazon FSx 檔案系統設定新的 SPNs。

   - *file_system_DNS_name* 將 取代為 Amazon FSx 指派給檔案系統的 DNS 名稱。

     若要在 Amazon FSx 主控台上尋找檔案系統的 DNS 名稱，請選擇檔案系統，然後選擇檔案系統詳細資訊頁面上的網路與安全窗格。

     您也可以在 DescribeFileSystems API 操作的回應中取得 DNS 名稱。

- *alias_fqdn* 將 取代為您在步驟 1 中與檔案系統相關聯的完整 DNS 別名。

```
## Set SPNs for FSx file system AD computer object
$FSxDnsName = "file_system_DNS_name"
$Alias = "alias_fqdn"
$FileSystemHost = (Resolve-DnsName $FSxDnsName | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity $FileSystemHost)

##Use the following command to set both the full FQDN and Alias SPNs
Set-AdComputer -Identity $FSxAdComputer -Add @{"msDS-AdditionalDnsHostname" =
 @($Alias, $Alias.Split(".")[0])}
```

> **Note**
>
> 如果原始檔案系統的電腦物件的 AD 中存在 DNS 別名的 SPN，則設定 Amazon FSx 檔案系統的 SPN 將會失敗。如需尋找和刪除現有 SPNs的資訊，請參閱 在原始檔案系統的 Active Directory 電腦物件上尋找和刪除現有的 DNS 別名 SPNs 。

2. 使用下列範例指令碼，確認已為 DNS 別名設定新的 SPNs。請確定回應包含兩個 HOST SPNs HOST/*alias*和 HOST/*alias_fqdn*，如本程序先前所述。

   file_system_DNS_name 將 取代為 Amazon FSx 指派給檔案系統的 DNS 名稱。若要在 Amazon FSx 主控台上尋找檔案系統的 DNS 名稱，請選擇檔案系統，然後選擇檔案系統詳細資訊頁面上的網路與安全窗格。

   您也可以在 DescribeFileSystems API 操作的回應中取得 DNS 名稱。

```
## Verify SPNs on FSx file system AD computer object
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})
SetSpn /L ${FSxAdComputer}.Name
```

3. 針對您在步驟 1 中與檔案系統相關聯的每個 DNS 別名重複上述步驟。

更新或建立 DNS CNAME 記錄

正確設定檔案系統的 SPNs 之後，您可以將解析至原始檔案系統的每個 DNS 記錄取代為解析為 Amazon FSx 檔案系統預設 DNS 名稱的 DNS 記錄，以切換到 Amazon FSx。

需要 `dnsserver`和 `activedirectory` Windows 模組才能執行本節中顯示的命令。

安裝所需的 PowerShell 模組

1. 以具有 DNS 管理許可的群組成員身分（中的AWS 委派網域名稱系統管理員 AWS Managed Microsoft AD，以及 網域管理員或您已在自我管理 Active Directory 中委派 DNS 管理許可的其他群組），登入已加入 Amazon FSx 檔案系統之相同 Active Directory 的 Windows 執行個體。

   如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的連線至 Windows 執行個體。
2. 以管理員身分開啟 PowerShell。
3. PowerShell DNS Server 模組需要執行此程序中的指示。使用以下命令進行安裝。

   ```
   Install-WindowsFeature RSAT-DNS-Server
   ```

更新或建立 Amazon FSx 檔案系統的自訂 DNS 名稱

1. 以具有 DNS 管理許可的群組成員身分（AWS 受管 Active Directory AWS 中的委派網域名稱系統管理員，以及在自我管理 Active Directory 中委派 DNS 管理許可的網域管理員或其他群組） 身分，連線至您的 Amazon EC2 執行個體。

   如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的連線至您的 Windows 執行個體。
2. 在命令提示字元中，執行下列指令碼。此指令碼會將任何現有的 DNS CNAME 記錄遷移到您的 Amazon FSx 檔案系統。如果找不到，它會為解析*alias_fqdn*為 Amazon FSx 檔案系統預設 DNS 名稱的 DNS 別名建立新的 DNS CNAME 記錄。

   執行指令碼：

   - *alias_fqdn* 將 取代為您與檔案系統相關聯的 DNS 別名。
   - *file_system_DNS_name* 將 取代為 Amazon FSx 已指派給檔案系統的 DNS 名稱。

   ```
   $Alias="alias_fqdn"
   $FSxDnsName="file_system_dns_name"
   $AliasHost=$Alias.Split('.')[0]
   ```

```
$ZoneName=((Get-WmiObject Win32_ComputerSystem).Domain)
$DnsServerComputerName = (Resolve-DnsName $ZoneName -Type NS | Where Type -eq 'A' |
 Select -ExpandProperty Name) | Select -First 1
Add-DnsServerResourceRecordCName -Name $AliasHost -ComputerName
 $DnsServerComputerName -HostNameAlias $FSxDnsName -ZoneName $ZoneName
```

3. 針對您在步驟 1 中與檔案系統相關聯的每個 DNS 別名，重複上述步驟。

您現在已為具有 DNS 別名的 Amazon FSx 檔案系統新增 DNS CNAME 值。您現在可以使用 DNS 別名來存取您的資料。

> **Note**
>
> 更新 DNS CNAME 記錄以指向先前指向另一個檔案系統的 Amazon FSx 檔案系統時，用戶端可能無法與檔案系統連接一小段時間。當用戶端 DNS 快取重新整理時，他們應該能夠使用 DNS 別名進行連線。如需詳細資訊，請參閱無法使用 DNS 別名存取檔案系統。

使用群組政策物件 (GPOs) 強制執行 Kerberos 身分驗證

您可以在 Active Directory 中設定下列群組政策物件 (GPOs)，以在存取檔案系統時強制執行 Kerberos 身分驗證：

- 限制 NTLM：傳出 NTLM 流量至遠端伺服器 - 使用此政策設定，拒絕或稽核從電腦傳出 NTLM 流量至執行 Windows 作業系統的任何遠端伺服器。
- 限制 NTLM：為 NTLM 身分驗證新增遠端伺服器例外狀況 - 如果已設定網路安全：限制 NTLM：將 NTLM 流量傳出至遠端伺服器政策設定，請使用此政策設定來建立允許用戶端裝置使用 NTLM 身分驗證的遠端伺服器例外狀況清單。

1. 登入已加入 Active Directory 的 Windows 執行個體，您的 Amazon FSx 檔案系統會以管理員身分加入其中。如果您要設定自我管理的 Active Directory，請直接將這些步驟套用至您的 Active Directory。
2. 選擇開始，選擇管理工具，然後選擇群組政策管理。
3. 選擇群組政策物件。
4. 如果您的群組政策物件不存在，請建立它。

5. 找出現有的網路安全：限制 NTLM：將 NTLM 流量傳出至遠端伺服器政策。（如果沒有現有政策，請建立新的政策。）在本機安全設定索引標籤中，開啟內容（按一下滑鼠右鍵）選單，然後選擇屬性。
6. 選擇全部拒絕。
7. 選擇套用以儲存安全設定。
8. 若要為用戶端設定特定遠端伺服器的 NTLM 連線例外狀況，請尋找網路安全：限制 NTLM：新增遠端伺服器例外狀況。

   開啟內容（按一下滑鼠右鍵）選單，然後在本機安全設定索引標籤中選擇屬性。
9. 輸入要新增至例外狀況清單的任何伺服器名稱。
10. 選擇套用以儲存安全設定。

使用檔案共享存取資料

Microsoft Windows 檔案共享是您檔案系統上的特定資料夾或目錄。它包含可能存在的任何子資料夾。用戶端會使用伺服器訊息區塊 (SMB) 通訊協定存取檔案系統上的檔案共享。您的 FSx for Windows File Server 檔案系統隨附名為 的預設 Windows 檔案共用`share`。您可以使用 Windows 共用資料夾圖形使用者介面 (GUI) 工具，視需要建立和管理任意數量的其他檔案共用。

Microsoft Windows 持續可用 (CA) 共享提供的主要優點是，即使叢集內的伺服器節點故障，維持共用檔案的不間斷存取。使用 CA 檔案共享可將伺服器應用程式在檔案系統維護時段期間，將資料檔案存放在這些檔案共享的中斷降至最低。

如需在 FSx for Windows File Server 檔案系統上建立和管理檔案共享的詳細資訊，包括 CA 共享，請參閱 建立、更新、移除檔案共用。

映射檔案共享

若要存取您的檔案共享，請使用 Windows Map Network Drive 功能，將運算執行個體上的磁碟機代號映射至 Amazon FSx 檔案共享。將檔案共享映射至運算執行個體上磁碟機的程序稱為在 Linux 中掛載檔案共享。此程序會根據運算執行個體的類型和作業系統而有所不同。映射檔案共享之後，您的應用程式和使用者可以存取檔案共享上的檔案和資料夾，就像它們是本機檔案和資料夾一樣。

如需映射和掛載檔案共用以存取檔案系統上資料的詳細資訊，請參閱下列程序：

- 映射 Amazon EC2 Windows 執行個體上的檔案共享.
- 在 Amazon EC2 Mac 執行個體上掛載檔案共享

- 在 Amazon EC2 Linux 執行個體上掛載檔案共享

映射 Amazon EC2 Windows 執行個體上的檔案共享

您可以使用 Windows File Explorer 或命令提示字元，在 EC2 Windows 執行個體上映射檔案共享以存取 FSx for Windows File Server 檔案系統。

在 Amazon EC2 Windows 執行個體上映射檔案共享 (File Explorer)

1. 啟動 EC2 Windows 執行個體，並將其連接至您加入 Amazon FSx 檔案系統的 Microsoft Active Directory。若要這樣做，請從 AWS Directory Service 管理指南中選擇下列其中一個程序：
   - 無縫加入 Windows EC2 執行個體
   - 手動加入 Windows 執行個體
2. 連接至 EC2 Windows 執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的連線至 Windows 執行個體。
3. 連線後，開啟檔案總管。
4. 在導覽窗格中，開啟網路的內容（按一下滑鼠右鍵）選單，然後選擇映射網路磁碟機。
5. 針對磁碟機，選擇磁碟機代號。
6. 針對資料夾，輸入檔案系統的 DNS 名稱或與檔案系統相關聯的 DNS 別名，以及共用名稱。

   > **Important**
   >
   > 使用 IP 地址而非 DNS 名稱可能會導致在多可用區檔案系統的容錯移轉程序期間無法使用。此外，多可用區和單一可用區檔案系統中的 Kerberos 型身分驗證需要 DNS 名稱或相關聯的 DNS 別名。

   您可以選擇 Windows File Server、Network & Security，在 Amazon FSx 主控台上尋找檔案系統的 DNS 名稱和任何相關聯的 DNS 別名。或者，您可以在 CreateFileSystem 或 DescribeFileSystems API 操作的回應中找到它們。如需使用 DNS 別名的詳細資訊，請參閱 管理 DNS 別名。

   - 對於加入 AWS Managed Microsoft Active Directory 的單一可用區檔案系統，DNS 名稱如下所示。

     ```
     fs-0123456789abcdef0.ad-domain.com
     ```

- 對於加入自我管理 Active Directory 的單一可用區檔案系統，以及任何多可用區檔案系統，DNS 名稱如下所示。

```
amznfsxaa11bb22.ad-domain.com
```

例如，若要使用單一可用區檔案系統的 DNS 名稱，請在資料夾中輸入下列內容。

```
\\fs-0123456789abcdef0.ad-domain.com\share
```

若要使用多可用區域檔案系統的 DNS 名稱，請在資料夾中輸入下列內容。

```
\\amznfsxaa11bb22.ad-domain.com\share
```

若要使用與檔案系統相關聯的 DNS 別名，請在資料夾中輸入下列內容。

```
\\fqdn-dns-alias\share
```

7. 選擇登入時重新連線的選項，指出檔案共享是否應在登入時重新連線，然後選擇完成。

在 Amazon EC2 Windows 執行個體上映射檔案共享（命令提示）

1. 啟動 EC2 Windows 執行個體，並將其連接至您加入 Amazon FSx 檔案系統的 Microsoft Active Directory。若要執行此作業，請從 AWS Directory Service 管理指南中選擇下列其中一個程序：
   - 無縫加入 Windows EC2 執行個體
   - 手動加入 Windows 執行個體
2. 以 AWS Managed Microsoft AD 目錄中的使用者身分連線至 EC2 Windows 執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的連線至 Windows 執行個體。
3. 連線之後，請開啟命令提示視窗。
4. 使用您選擇的磁碟機代號、檔案系統的 DNS 名稱和共用名稱來掛載檔案共用。您可以選擇 Windows File Server、Network & Security，以使用 Amazon FSx 主控台尋找 DNS 名稱。或者，您可以在 `CreateFileSystem`或 `DescribeFileSystems` API 操作的回應中找到它們。
   - 對於加入 AWS Managed Microsoft Active Directory 的單一可用區檔案系統，DNS 名稱如下所示。

```
fs-0123456789abcdef0.ad-domain.com
```

- 對於加入自我管理 Active Directory 的單一可用區檔案系統，以及任何多可用區檔案系統，DNS 名稱如下所示。

```
amznfsxaa11bb22.ad-domain.com
```

以下是掛載檔案共享的範例命令。

```
$ net use H: \\amzfsxaa11bb22.ad-domain.com\share /persistent:yes
```

您也可以使用任何支援的 PowerShell 命令來掛載檔案共享，而不是 `net use`命令。

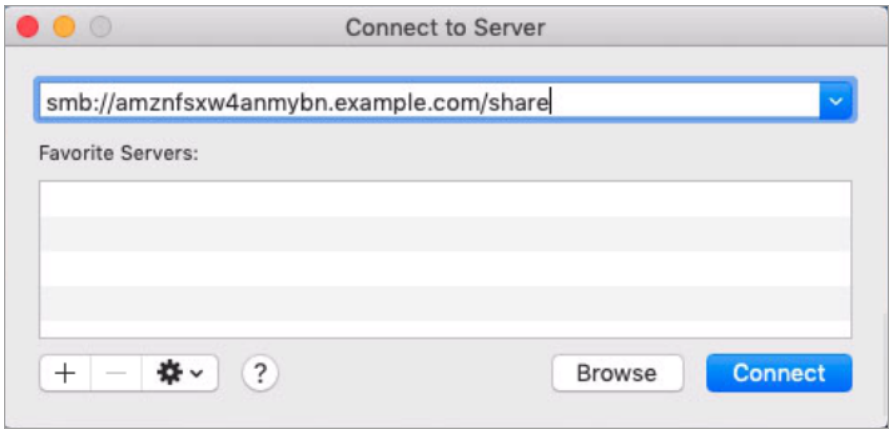
在 Amazon EC2 Mac 執行個體上掛載檔案共享

您可以在已加入 Active Directory 或未加入存取 FSx for Windows File Server 檔案系統的 Amazon EC2 Mac 執行個體上掛載檔案共享。如果執行個體未加入您的 Active Directory，請務必更新執行個體所在的 Amazon Virtual Private Cloud (Amazon VPC) 的 DHCP 選項集，以包含 Active Directory 網域的 DNS 名稱伺服器。然後重新啟動執行個體。

在 Amazon EC2 Mac 執行個體 (GUI) 上掛載檔案共享

1. 啟動 EC2 Mac 執行個體。若要這樣做，請從 Amazon EC2 使用者指南中選擇下列其中一個程序：
   - 使用主控台啟動 Mac 執行個體
   - 使用 啟動 Mac 執行個體 AWS CLI
2. 使用虛擬網路運算 (VNC) 連線至 EC2 Mac 執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的使用 VNC 連線至執行個體。
3. 在 EC2 Mac 執行個體上，連線至 Amazon FSx 檔案共享，如下所示：
   a. 開啟 Finder，選擇 Go，然後選擇連線至伺服器。
   b. 在連線至伺服器對話方塊中，輸入檔案系統的 DNS 名稱或與檔案系統相關聯的 DNS 別名，以及共用名稱。然後選擇 連線。

您可以選擇 Windows File Server、Network & Security，在 Amazon FSx 主控台上尋找檔案系統的 DNS 名稱和任何相關聯的 DNS 別名。或者，您可以在 CreateFileSystem 或 DescribeFileSystems API 操作的回應中找到它們。如需使用 DNS 別名的詳細資訊，請參閱管理 DNS 別名。



c. 在下一個畫面上，選擇連線以繼續。

d. 輸入 Amazon FSx 服務帳戶的 Microsoft Active Directory (AD) 登入資料，如下列範例所示。然後選擇 連線。

e. 如果連線成功，您可以在 Finder 視窗中的位置下看到 Amazon FSx 共用。

在 Amazon EC2 Mac 執行個體上掛載檔案共享 （命令列）

1. 啟動 EC2 Mac 執行個體。若要這樣做，請從 Amazon EC2 使用者指南中選擇下列其中一個程序：

   - 使用主控台啟動 Mac 執行個體

- 使用 啟動 Mac 執行個體 AWS CLI

2. 使用虛擬網路運算 (VNC) 連線至 EC2 Mac 執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的使用 VNC 連線至執行個體。
3. 使用以下命令掛載檔案共享。

```
mount_smbfs //file_system_dns_name/file_share mount_point
```

您可以選擇 Windows File Server、Network & Security，在 Amazon FSx 主控台上尋找 DNS 名稱。或者，您可以在 `CreateFileSystem`或 `DescribeFileSystems` API 操作的回應中找到它們。

- 對於加入 AWS Managed Microsoft Active Directory 的單一可用區檔案系統，DNS 名稱如下所示。

```
fs-0123456789abcdef0.ad-domain.com
```

- 對於加入自我管理 Active Directory 的單一可用區檔案系統，以及任何多可用區檔案系統，DNS 名稱如下所示。

```
amznfsxaa11bb22.ad-domain.com
```

此程序中使用的掛載命令會在指定點執行下列動作：

- *//file_system_dns_name/file_share* – 指定要掛載的檔案系統的 DNS 名稱和共用。
- *mount_point* – 您要掛載檔案系統之 EC2 執行個體上的目錄。

在 Amazon EC2 Linux 執行個體上掛載檔案共享

您可以在加入 Active Directory 或未加入存取 FSx for Windows File Server 檔案系統的 Amazon EC2 Linux 執行個體上掛載 FSx for Windows File Server 檔案共享。

> **Note**
>
> - 下列命令指定參數，例如 SMB 通訊協定、快取，以及讀取和寫入緩衝區大小，僅做為範例。Linux `cifs`命令的參數選擇以及使用的 Linux 核心版本，可能會影響用戶端和 Amazon

FSx 檔案系統之間的網路操作輸送量和延遲。如需詳細資訊，請參閱您正在使用的 Linux 環境`cifs`的文件。

- Linux 用戶端不支援自動 DNS 型容錯移轉。如需詳細資訊，請參閱Linux 用戶端的容錯移轉體驗。

在加入 Active Directory 的 Amazon EC2 Linux 執行個體上掛載檔案共享

1. 如果您尚未將執行中的 EC2 Linux 執行個體加入 Microsoft Active Directory，請參閱《 AWS Directory Service 管理指南》中的手動加入 Linux 執行個體，以取得執行此作業的指示。
2. 連線至 EC2 Linux 執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的連線至 Linux 執行個體。
3. 若要安裝此 `cifs-utils` 套件，請執行下列命令：此套件用於掛載網路檔案系統，例如 Linux 上的 Amazon FSx。

```
$ sudo yum install cifs-utils
```

4. 建立掛載點目錄 **`/mnt/fsx`**。這是您將掛載 Amazon FSx 檔案系統的位置。

```
$ sudo mkdir -p /mnt/fsx
```

5. 使用下列命令以 kerberos 驗證 。

```
$ kinit
```

6. 使用以下命令掛載檔案共享。

```
$ sudo mount -t cifs //file_system_dns_name/file_share mount_point --verbose -o
 vers=SMB_version,sec=krb5,cruid=ad_user,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=no
file-server-Ip
```

您可以選擇 Windows File Server、Network & Security，在 Amazon FSx 主控台上尋找 DNS 名稱。或者，您可以在 `CreateFileSystem`或 `DescribeFileSystems` API 操作的回應中找到它們。

- 對於加入 AWS Managed Microsoft Active Directory 的單一可用區檔案系統，DNS 名稱如下所示。

```
fs-0123456789abcdef0.ad-domain.com
```

- 對於加入自我管理 Active Directory 的單一可用區檔案系統，以及任何多可用區檔案系統，DNS 名稱如下所示。

```
amznfsxaa11bb22.ad-domain.com
```

CIFSMaxBufSize 將 取代為核心允許的最大值。執行下列命令以取得此值。

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

輸出顯示緩衝區大小上限為 130048。

7. 執行下列命令，僅傳回通用網際網路檔案系統 (CIFS) 類型的檔案系統，以確認檔案系統已掛載。

```
$ mount -l -t cifs
//fs-0123456789abcdef0/share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=krb5,cache=cache_mode,username=user1@CORP.NETWORK.COM,ui
```

此程序中使用的掛載命令會在指定點執行下列動作：

- *//file_system_dns_name/file_share* – 指定要掛載的檔案系統的 DNS 名稱和共用。
- *mount_point* – 您要掛載檔案系統之 EC2 執行個體上的目錄。
- `-t cifs vers=`*SMB_version* – 指定檔案系統的類型為 CIFS 和 SMB 通訊協定版本。Amazon FSx for Windows File Server 支援 SMB 2.0 到 3.1.1 版。
- `sec=krb5` – 指定使用 Kerberos 第 5 版進行身分驗證。
- `cache=`*cache_mode* – 設定快取模式。CIFS 快取的此選項可能會影響效能，您應該測試哪些設定最適合您的核心和工作負載 （ 並檢閱 Linux 文件 ）。none 建議使用 `strict`和 選項，因為 `loose`可能因通訊協定語意較鬆而導致資料不一致。
- `cruid=`*ad_user* – 將登入資料快取擁有者的 uid 設定為 AD 目錄管理員。
- */mnt/fsx* – 指定 EC2 執行個體上 Amazon FSx 檔案共享的掛載點。

- `rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize` – 將讀取和寫入緩衝區大小指定為 CIFS 通訊協定允許的最大值。*CIFSMaxBufSize* 將 取代為核心允許的最大值。執行下列命令`CIFSMaxBufSize`來判斷 。

  ```
  $ modinfo cifs | grep CIFSMaxBufSize
  parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
   16384 Range: 8192 to 130048 (uint)
  ```

  輸出顯示緩衝區大小上限為 130048。

- `ip=`*preferred-file-server-Ip* – 將目的地 IP 地址設定為檔案系統偏好檔案伺服器的 IP 地址。

  您可以擷取檔案系統偏好的檔案伺服器 IP 地址，如下所示：

  - 使用 Amazon FSx 主控台，在檔案系統詳細資訊頁面的網路與安全索引標籤上。
  - 在 CLI `describe-file-systems` 命令或同等 DescribeFileSystems API 命令的回應中。

在未加入 Active Directory 的 Amazon EC2 Linux 執行個體上掛載檔案共享

下列程序會將 Amazon FSx 檔案共享掛載到未加入 Active Directory (AD) 的 Amazon EC2 Linux 執行個體。對於未加入 AD 的 EC2 Linux 執行個體，您只能使用其私有 IP 地址掛載 FSx for Windows File Server 檔案共享。您可以使用 Amazon FSx 主控台，在偏好的檔案伺服器 IP 地址的網路與安全索引標籤上取得檔案系統的私有 IP 地址。

此範例使用 NTLM 身分驗證。若要執行此作業，您將檔案系統掛載為使用者，而該使用者是 FSx for Windows File Server 檔案系統加入的 Microsoft Active Directory 網域的成員。使用者帳戶的登入資料會在您在 EC2 執行個體 上建立的文字檔案中提供`creds.txt`。此檔案包含使用者的使用者名稱、密碼和網域。

```
$ cat creds.txt
username=user1
password=Password123
domain=EXAMPLE.COM
```

啟動和設定 Amazon Linux EC2 執行個體

1. 使用 Amazon EC2 主控台啟動 Amazon EC2 執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的啟動執行個體。

2. 連線至您的 Amazon Linux EC2 執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的連線至 Linux 執行個體。
3. 若要安裝此 `cifs-utils` 套件，請執行下列命令：此套件用於掛載網路檔案系統，例如 Linux 上的 Amazon FSx。

```
$ sudo yum install cifs-utils
```

4. 建立**/mnt/fsxx**您計劃掛載 Amazon FSx 檔案系統的掛載點。

```
$ sudo mkdir -p /mnt/fsx
```

5. 使用先前顯示的格式，在 /home/ec2-user目錄中建立creds.txt登入資料檔案。
6. 設定creds.txt檔案許可，以便只有您（擁有者）可以執行下列命令來讀取和寫入檔案。

```
$ chmod 700 creds.txt
```

掛載檔案系統

1. 您可以使用其私有 IP 地址掛載未加入 Active Directory 的檔案共用。您可以使用 Amazon FSx 主控台，在偏好的檔案伺服器 IP 地址的網路與安全索引標籤上，取得檔案系統的私有 IP 地址。
2. 使用以下命令掛載檔案系統：

```
$ sudo mount -t cifs //file-system-IP-address/file_share /mnt/fsx
 --verbose -o vers=SMB_version,sec=ntlmsspi,cred=/home/ec2-user/
creds.txt,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=none
```

CIFSMaxBufSize 將 取代為核心允許的最大值。執行下列命令以取得此值。

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

輸出顯示緩衝區大小上限為 130048。

3. 執行下列命令，僅傳回 CIFS 檔案系統，以確認檔案系統已掛載。

```
$ mount -l -t cifs
```

```
//file-system-IP-address/file_share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=ntlmsspi,cache=cache_mode,username=user1,domain=CORP.EXA
```

此程序中使用的掛載命令會在指定點執行下列動作：

- *//file-system-IP-address/file_share* – 指定您要掛載的檔案系統的 IP 地址和共用。
- `-t cifs vers=`*SMB_version* – 將檔案系統的類型指定為 CIFS 和 SMB 通訊協定版本。Amazon FSx for Windows File Server 支援 SMB 2.0 到 3.1.1 版。
- `sec=ntlmsspi` – 指定使用 NT LAN Manager 安全支援提供者界面 (NTLMSSPI) 進行身分驗證。
- `cache=`*cache_mode* – 設定快取模式。CIFS 快取的此選項可能會影響效能，您應該測試哪些設定最適合您的核心和工作負載（並檢閱 Linux 文件）。none 建議使用 `strict`和 選項，因為`loose`可能因通訊協定語意較鬆而造成資料不一致。
- `cred=/home/ec2-user/creds.txt` – 指定在何處取得使用者登入資料。
- */mnt/fsx* – 指定 EC2 執行個體上 Amazon FSx 檔案共享的掛載點。
- `rsize=`*CIFSMaxBufSize*`,wsize=`*CIFSMaxBufSize* – 將讀取和寫入緩衝區大小指定為 CIFS 通訊協定允許的最大值。*CIFSMaxBufSize* 將 取代為核心允許的最大值。執行下列命令`CIFSMaxBufSize`來判斷 。

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

在 Amazon EC2 Linux 執行個體上自動掛載檔案共享

您可以自動掛載 FSx for Windows File Server 檔案共享，以便在掛載的 Amazon EC2 Linux 執行個體重新啟動時存取 FSx for Windows File Server 檔案系統。若要這樣做，請將 項目新增至 EC2 執行個體上的 `/etc/fstab` 檔案。`/etc/fstab` 檔案包含檔案系統的資訊，在執行個體啟動期間執行`mount -a`的命令 會掛載`/etc/fstab`檔案中列出的檔案系統。

對於未加入 Active Directory 的 Amazon EC2 Linux 執行個體，您只能使用其私有 IP 地址掛載 FSx for Windows File Server 檔案共享。您可以使用 Amazon FSx 主控台，在偏好的檔案伺服器 IP 地址的網路與安全索引標籤上取得檔案系統的私有 IP 地址。

下列程序使用 Microsoft NTLM 身分驗證。您可以將檔案系統掛載為使用者，而該使用者是 FSx for Windows File Server 檔案系統加入的 Microsoft Active Directory 網域成員。您可以使用下列命令，從 `creds.txt` 檔案擷取使用者帳戶的登入資料。

```
$ cat creds.txt
username=user1
password=Password123
domain=EXAMPLE.COM
```

在未加入 Active Directory 的 Amazon Linux EC2 執行個體上自動掛載檔案共享

啟動和設定 Amazon Linux EC2 執行個體

1. 使用 Amazon EC2 主控台啟動 Amazon EC2 執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的啟動執行個體。
2. 連線到您的執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的連線至 Linux 執行個體。
3. 若要安裝此 `cifs-utils` 套件，請執行下列命令：此套件用於掛載網路檔案系統，例如 Linux 上的 Amazon FSx。

   ```
   $ sudo yum install cifs-utils
   ```

4. 建立 `/mnt/fsx` 目錄。這是您將掛載 Amazon FSx 檔案系統的位置。

   ```
   $ sudo mkdir /mnt/fsx
   ```

5. 在 `/home/ec2-user`目錄中建立`creds.txt`登入資料檔案。
6. 設定檔案許可，以便只有您（擁有者）可以執行下列命令來讀取檔案。

   ```
   $ sudo chmod 700 creds.txt
   ```

自動掛載檔案系統

1. 您可以使用其私有 IP 地址，自動掛載未加入 Active Directory 的檔案共享。您可以使用 Amazon FSx 主控台，在偏好的檔案伺服器 IP 地址的網路與安全索引標籤上取得檔案系統的私有 IP 地址。
2. 若要使用檔案共用的私有 IP 地址自動掛載檔案共用，請將以下幾行新增至`/etc/fstab`檔案。

```
//file-system-IP-address/file_share /mnt/fsx cifs
 vers=SMB_version,sec=ntlmsspi,cred=/home/ec2-user/
creds.txt,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=none 0 0
```

CIFSMaxBufSize 將 取代為核心允許的最大值。執行下列命令以取得此值。

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

輸出顯示緩衝區大小上限為 130048。

3. 使用 mount命令搭配 'fake' 選項以及 'all' 和 'verbose' 選項來測試fstab項目。

```
$ sudo mount -fav
home/ec2-user/fsx      : successfully mounted
```

4. 若要掛載檔案共享，請重新啟動 Amazon EC2 執行個體。
5. 當執行個體再次可用時，請執行下列命令來驗證檔案系統是否已掛載。

```
$ sudo mount -l -t cifs
//file-system-IP-address/file_share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=ntlmsspi,cache=cache_code,username=user1,domain=CORP.EXA
```

在此程序中新增至 /etc/fstab 檔案的行會在指定點執行下列動作：

- *//file-system-IP-address/file_share* – 指定您要掛載之 Amazon FSx 檔案系統的 IP 地址和共用。
- /mnt/fsx – 指定 EC2 執行個體上 Amazon FSx 檔案系統的掛載點。
- cifs vers=*SMB_version* – 將檔案系統的類型指定為 CIFS 和 SMB 通訊協定版本。Amazon FSx for Windows File Server 支援 SMB 2.0 到 3.1.1 版。
- sec=ntlmsspi – 指定使用 NT LAN Manager 安全支援提供者界面來促進 NTLM 挑戰-回應身分驗證。
- cache=*cache_mode* – 設定快取模式。CIFS 快取的此選項可能會影響效能，您應該測試哪些設定最適合您的核心和工作負載（並檢閱 Linux 文件）。none 建議使用 strict和 選項，因為 loose可能因通訊協定語意較鬆而造成資料不一致。
- cred=/home/ec2-user/creds.txt – 指定在何處取得使用者登入資料。

- `_netdev` – 告知作業系統檔案系統位於需要網路存取的裝置。使用此選項可防止執行個體掛載檔案系統，直到在用戶端上啟用網路服務為止。
- `0` – 指出如果檔案系統是非零值`dump`，應該由 備份。對於 Amazon FSx，此值應為 `0`。
- `0` – 指定在開機時`fsck`檢查檔案系統的順序。對於 Amazon FSx 檔案系統，此值應`0`指出`fsck`不應在啟動時執行。

建立、更新、移除檔案共用

本主題說明如何透過執行下列任務來管理檔案共享。

- 建立新的檔案共用
- 修改現有的檔案共用
- 移除現有的檔案共用

您可以使用 Windows 原生共用資料夾 GUI 和 Amazon FSx CLI 在 PowerShell 上進行遠端管理，以管理 FSx for Windows File Server 檔案系統上的檔案共用。使用共用資料夾 GUI (fsmgmt.msc) 時，您可能會在第一次開啟位於不同檔案系統之共用的內容選單時遇到延遲。為了避免這些延遲，請使用 PowerShell 來管理位於多個檔案系統上的檔案共用。

Microsoft Windows 會強制執行命名檔案和目錄的規則和限制。為了確保您可以成功建立和存取資料，您應該根據這些 Windows 指導方針命名檔案和目錄。如需詳細資訊，請參閱命名慣例。

> **Warning**
>
> Amazon FSx 要求 SYSTEM 使用者在您建立 SMB 檔案共用的每個資料夾上擁有完全控制 NTFS ACL 許可。請勿在您的資料夾上變更此使用者的 NTFS ACL 許可，因為這樣做會使您的檔案共用無法存取。

使用共用資料夾 GUI 管理檔案共用

若要管理 Amazon FSx 檔案系統上的檔案共用，您可以使用共用資料夾 GUI。共用資料夾 GUI 提供集中位置，用於管理 Windows 伺服器上的所有共用資料夾。下列程序說明如何管理您的檔案共用。

將共用資料夾連接至 FSx for Windows File Server 檔案系統

1. 啟動您的 Amazon EC2 執行個體，並將其連接至您的 Amazon FSx 檔案系統所加入的 Microsoft Active Directory。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 Windows EC2 執行個體
   - 手動加入 Windows 執行個體

2. 以檔案系統管理員群組成員身分的使用者身分連線至您的執行個體。在 AWS 受管 Microsoft Active Directory AWS 中，此群組稱為委派 FSx 管理員。在自我管理的 Microsoft Active Directory 中，此群組稱為網域管理員，或您在建立期間提供的管理員群組自訂名稱。如需詳細資訊，請參閱《Amazon Elastic Compute Cloud Windows 執行個體使用者指南》中的連線至您的 Windows 執行個體。
3. 開啟開始功能表，並使用以管理員身分執行 fsmgmt.msc。這樣做會開啟共用資料夾 GUI 工具。
4. 針對動作，選擇連線至另一部電腦。
5. 針對另一部電腦，輸入 Amazon FSx 檔案系統的網域名稱系統 (DNS) 名稱，例如 **amznfsxabcd0123.corp.example.com**。

   若要在 Amazon FSx 主控台上尋找檔案系統的 DNS 名稱，請選擇檔案系統、選擇檔案系統，然後檢查檔案系統詳細資訊頁面的網路與安全區段。您也可以在 DescribeFileSystems API 操作的回應中取得 DNS 名稱。
6. 選擇確定。然後，Amazon FSx 檔案系統的項目會出現在共用資料夾工具的清單中。

現在共用資料夾已連線至您的 Amazon FSx 檔案系統，您可以在檔案系統上管理 Windows 檔案共用。預設共用稱為 `\share`。您可以使用下列動作來執行此操作：

- 建立新的檔案共用 – 在共用資料夾工具中，選擇左側窗格中的共用，以查看 Amazon FSx 檔案系統的作用中共用。選擇新共用並完成建立共用資料夾精靈。

  您必須先建立本機資料夾，才能建立新的檔案共用。您可以執行以下操作：

  - 使用共用資料夾工具：指定本機資料夾路徑時，按一下「瀏覽」，然後按一下「建立新資料夾」來建立本機資料夾。
  - 使用命令列：

    ```
    New-Item -Type Directory -Path \\amznfsxabcd0123.corp.example.com\D$\share
    \MyNewShare
    ```

- 修改檔案共用 – 在共用資料夾工具中，開啟您要在右側窗格中修改之檔案共用的內容（按一下滑鼠右鍵）選單，然後選擇屬性。修改屬性，然後選擇確定。
- 移除檔案共用 – 在共用資料夾工具中，開啟您要在右側窗格中移除的檔案共用內容（按一下滑鼠右鍵）選單，然後選擇停止共用。

> **Note**
>
> 對於單一可用區 2 和多可用區檔案系統，只有在您使用 Amazon FSx 檔案系統的 DNS 名稱連線至 fsmgmt.msc 時，才能使用共用資料夾 GUI 工具移除檔案共用或修改檔案共用（包括更新許可、使用者限制和其他屬性）。如果您使用檔案系統的 IP 地址或 DNS 別名名稱進行連線，則共用資料夾 GUI 工具不支援這些動作。

> **Note**
>
> 如果您使用 fsmgmt.msc 共用資料夾 GUI 工具來存取位於多個 FSx for Windows File Server 檔案系統的共用，則在第一次開啟位於不同檔案系統之共用的檔案共用內容選單時，可能會遇到延遲。若要避免這些延遲，您可以使用 PowerShell 管理檔案共用，如下所述。

管理與 PowerShell 的檔案共用

您可以使用 PowerShell 的自訂 FSx for Windows File Server 遠端管理命令來管理檔案共用。這些命令可協助您自動管理檔案共用任務，例如：

- 將檔案共用從現有檔案伺服器遷移至 Amazon FSx
- 同步跨 的檔案共用 AWS 區域 以進行災難復原
- 以程式設計方式管理持續的檔案共用工作流程，例如團隊檔案共用佈建

若要了解如何在 PowerShell 上使用 Amazon FSx CLI 進行遠端管理，請參閱 使用 Amazon FSx CLI for PowerShell。

下表列出 Amazon FSx CLI 遠端管理 PowerShell 命令，您可以使用這些命令來管理 FSx for Windows File Server 檔案系統上的檔案共用。

共用管理命令	描述
New-FSxSmbShare	建立新的檔案共用。
Remove-FSxSmbShare	移除檔案共用。
Get-FSxSmbShare	擷取現有的檔案共用。
Set-FSxSmbShare	設定共享的屬性。
Get-FSxSmbShareAccess	擷取共用的存取控制清單 (ACL)。
Grant-FSxSmbShareAccess	將受信任者的允許存取控制項目 (ACE) 新增至共用的安全描述項。
Revoke-FSxSmbShareAccess	從共享的安全描述符中移除受信任者的所有允許 ACEs。
Block-FSxSmbShareAccess	將受託人的拒絕 ACE 新增至共享的安全描述項。
Unblock-FSxSmbShareAccess	從共享的安全描述符中移除受信任者的所有拒絕 ACEs。

每個命令的線上說明提供所有命令選項的參考。若要存取此說明，請使用 執行 命令-?，例如 `New-FSxSmbShare -?`。

將登入資料傳遞至 New-FSxSmbShare

您可以將登入資料傳遞至 New-FSxSmbShare，以便您可以循環執行登入資料，以建立數百或數千個共享，而不必每次重新輸入登入資料。

使用下列其中一個選項，準備在 FSx for Windows File Server 檔案伺服器上建立檔案共用所需的登入資料物件。

- 若要以互動方式產生登入資料物件，請使用下列命令。

```
$credential = Get-Credential
```

- 若要使用 AWS Secrets Manager 資源產生登入資料物件，請使用下列命令。

```
$credential = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
 $AdminSecret).SecretString
```

```
$FSxAdminUserCredential = (New-Object PSCredential($credential.UserName,(ConvertTo-
SecureString $credential.Password -AsPlainText -Force)))
```

建立持續可用的 (CA) 共享

您可以使用 Amazon FSx CLI for Remote Management on PowerShell 建立持續可用的 (CA) 共享。在 FSx for Windows File Server 多可用區域檔案系統上建立的 CA 共用具有高度耐用性和高可用性。Amazon FSx 單一可用區檔案系統建立在單一節點叢集上。因此，在單一可用區檔案系統上建立的 CA 共用非常耐用，但並非高度可用。使用 New-FSxSmbShare命令，並將 -ContinuouslyAvailable 選項設定為 $True，以指定共享是持續可用的共享。以下是建立 CA 共享的範例命令。

```
New-FSxSmbShare -Name "New CA Share" -Path "D:\share\new-share" -Description "CA share"
 -ContinuouslyAvailable $True
```

您可以使用 Set-FSxSmbShare命令修改現有檔案共享上的 -ContinuouslyAvailable選項。

判斷現有的檔案共用是否持續可用

使用下列命令來檢視現有檔案共享的持續可用屬性值。

```
Invoke-Command -ComputerName powershell_endpoint -ConfigurationName FSxRemoteAdmin -
scriptblock { get-fsxsmbshare -name share_name }
```

如果已啟用 CA，輸出將包含以下行：

```
[...]
ContinuouslyAvailable : True
[...]
```

如果未啟用 CA，輸出將包含以下行：

```
[...]
ContinuouslyAvailable : False
[...]
```

若要在現有檔案共享上啟用持續可用，請使用下列命令：

```
Invoke-Command -ComputerName powershell_endpoint -ConfigurationName FSxRemoteAdmin -
scriptblock { set-fsxsmbshare -name share_name -ContinuouslyAvailable $True}
```

New-FSxSmbShare 命令使用單向信任失敗

Amazon FSx 不支援在您擁有單向信任，且使用者所在的網域未設定為信任與 Amazon FSx 檔案系統相關聯的網域的情況下執行 New-FSxSmbShare PowerShell 命令。

您可以使用下列其中一個解決方案來解決這種情況：

- 執行 New-FSxSmbShare命令的使用者必須與 FSx 檔案系統位於相同的網域中。
- 您可以使用 fsmgmt.msc GUI 在檔案系統上建立共享。如需詳細資訊，請參閱使用共用資料夾 GUI 管理檔案共用。

可用性和耐久性：單一可用區和多可用區檔案系統

Amazon FSx for Windows File Server 提供兩種檔案系統部署類型：單一可用區和多可用區。下列各節提供的資訊可協助您為工作負載選擇正確的部署類型。如需服務可用性 SLA（服務層級協議）的相關資訊，請參閱 Amazon FSx 服務層級協議。

單一可用區域檔案系統由單一 Windows 檔案伺服器執行個體和單一可用區域 (AZ) 內的一組儲存磁碟區組成。使用單一可用區檔案系統時，資料會自動複寫，以防止在大多數情況下單一元件故障。Amazon FSx 會持續監控硬體故障，並透過取代故障的基礎設施元件，自動從故障事件中復原。單一可用區檔案系統通常會在故障復原事件期間，以及您為檔案系統設定的計劃維護時段期間，經歷大約 30 分鐘的停機時間。使用單一可用區檔案系統時，檔案系統故障在極少數情況下可能無法復原，例如由於多個元件故障，或由於單一檔案伺服器發生無法復原的故障，導致檔案系統處於不一致的狀態，在這種情況下，您可以從最新的備份復原檔案系統。

多可用區域檔案系統是由分散在兩個AZs（偏好的可用區域和待命可用區域）的 Windows 檔案伺服器的高可用性叢集組成，利用 Windows Server 容錯移轉叢集 (WSFC) 技術和兩個AZs上的一組儲存磁碟區。資料會同步複寫在每個個別 AZ 內和兩個 AZs 之間。相對於單一可用區部署，多可用區部署透過進一步複寫跨AZs的資料來提供增強的耐用性，並透過自動容錯移轉到待命可用區，在計劃的系統維護和計劃外服務中斷期間增強可用性。這可讓您繼續存取資料，並協助保護資料免於執行個體故障和可用區域中斷。

選擇單一可用區或多可用區檔案系統部署類型

考慮到多可用區域檔案系統提供的高可用性和耐久性模型，我們建議對大多數生產工作負載使用多可用區域檔案系統。單一可用區部署設計為符合成本效益的解決方案，適用於測試和開發工作負載、已建置複寫至應用程式層的特定生產工作負載，且不需要額外的儲存層級備援，以及需要輕鬆可用性和復原點目標 (RPO) 的生產工作負載。具有寬鬆可用性和 RPO 需求的工作負載，在計劃性檔案系統維護或未計劃的服務中斷時，可容忍暫時失去可用性長達 20 分鐘，在極少數情況下，會從最近的備份以來遺失資料更新。

我們也建議您檢閱檔案系統的可用性模型，並確保您的工作負載能夠適應您在檔案系統維護、輸送量容量變更和意外服務中斷等事件期間所選擇部署類型的預期復原行為。

依部署類型提供的功能支援

下表摘要說明 FSx for Windows File Server 檔案系統部署類型支援的功能：

部署類型	SSD 儲存體	HDD 儲存體	DFS 命名空間	DFS 複寫	自訂 DNS 名稱	CA 共享
單一可用區 1	✓		✓	✓	✓	
單一可用區 2	✓	✓	✓		✓	✓*
Multi-AZ	✓	✓	✓		✓	✓*

> **Note**
>
> * 雖然您可以在單一可用區域 2 檔案系統上建立持續可用的 (CA) 共用，但您應該在 SQL Server HA 部署的多可用區域檔案系統上使用 CA 共用。

程序失敗

如果發生以下任何情況，多可用區域檔案系統會自動從偏好的檔案伺服器容錯移轉至待命檔案伺服器：

- 發生可用區域中斷。
- 偏好的檔案伺服器無法使用。
- 偏好的檔案伺服器會進行計劃的維護。

當從一個檔案伺服器容錯移轉到另一個檔案伺服器時，新的作用中檔案伺服器會自動開始提供所有檔案系統讀取和寫入請求。當偏好子網路中的資源可用時，Amazon FSx 會自動失敗回偏好子網路中的偏好檔案伺服器。容錯移轉通常會在偵測作用中檔案伺服器上的失敗後不到 30 秒內完成，直到將待命檔案伺服器提升為作用中狀態為止。原始多可用區組態的容錯也會在不到 30 秒內完成，而且只有在慣用子網路中的檔案伺服器完全復原後才會發生。

在檔案系統容錯移轉和回復失敗的短暫期間內，I/O 可能會暫停，而 Amazon CloudWatch 指標可能會暫時無法使用。對於多可用區域檔案系統，容錯移轉和容錯回復期間發生的任何檔案讀取和寫入活動都需要在主要和次要檔案伺服器之間同步。對於具有 HDD 儲存的檔案系統，以及寫入密集和 IOPS 密集的工作負載，此程序最多可能需要數小時的時間。我們建議您在檔案系統負載較輕時測試容錯移轉對應用程式的影響。

Windows 用戶端的容錯移轉體驗

當從一個檔案伺服器容錯移轉到另一個檔案伺服器時，新的作用中檔案伺服器會自動開始為所有檔案系統讀取和寫入請求提供服務。在慣用子網路中的資源可用後，Amazon FSx 會自動失敗回慣用子網路中的慣用檔案伺服器。由於檔案系統的 DNS 名稱保持不變，因此容錯移轉對 Windows 應用程式而言是透明的，該應用程式無需手動介入即可恢復檔案系統操作。容錯移轉通常會在偵測作用中檔案伺服器上的失敗後不到 30 秒內完成，直到將待命檔案伺服器提升為作用中狀態為止。恢復原始多可用區組態也會在不到 30 秒內完成，而且只會在慣用子網路中的檔案伺服器完全復原後發生。

Linux 用戶端的容錯移轉體驗

Linux 用戶端不支援自動 DNS 型容錯移轉。因此，它們不會在容錯移轉期間自動連線到待命檔案伺服器。在多可用區域檔案系統無法傳回至偏好的子網路中的檔案伺服器之後，它們會自動恢復檔案系統操作。

在檔案系統上測試容錯移轉

您可以修改多可用區域檔案系統的輸送量容量，以測試容錯移轉。當您修改檔案系統的輸送量容量時，Amazon FSx 會移出檔案系統的檔案伺服器。多可用區域檔案系統會自動容錯移轉至次要伺服器，而 Amazon FSx 會先取代偏好的伺服器檔案伺服器。然後，檔案系統會自動故障回新的主要伺服器，Amazon FSx 會取代次要檔案伺服器。

您可以在 Amazon FSx 主控台、CLI 和 API 中監控輸送量容量更新請求的進度。一旦更新成功完成，您的檔案系統就無法容錯移轉至次要伺服器，也無法返回主要伺服器。如需修改檔案系統的輸送量容量和監控請求進度的詳細資訊，請參閱 管理輸送量容量。

單一可用區和多可用區檔案系統資源

單一可用區域和多可用區域檔案系統使用子網路和彈性網路介面的方式不同，如以下各節所述。

子網路

當您建立虛擬私有雲端 (VPC) 時，它會跨越 中的所有可用區域 (AZs) AWS 區域。可用區域是代表不同的位置，旨在隔離其他可用區域的故障。建立 VPC 之後，您可以在各個可用區域新增一或多個子網路。預設 VPC 在每個可用區域中都有子網路。子網是您的 VPC 中的 IP 地址範圍。子網必須位於單一可用區域。

FSx for Windows File Server 單一可用區檔案系統需要一個子網路，您在建立時指定該子網路。您選擇的子網路會定義檔案系統建立所在的可用區域。

多可用區域檔案系統需要兩個子網路，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 AWS 區域內的不同可用區域。

對於AWS 應用程式內，我們建議您在與偏好檔案伺服器相同的可用區域中啟動用戶端，以將延遲降至最低。

檔案系統彈性網路介面

彈性網路介面是 VPC 中的邏輯聯網元件，代表虛擬網路卡。當您建立 Amazon FSx 檔案系統時，Amazon FSx 會在與您檔案系統建立關聯的 VPC 中佈建一或多個彈性網路介面。彈性網路介面可讓用戶端與 檔案系統通訊並掛載。彈性網路介面被視為在 Amazon FSx 的服務範圍內，即使它屬於您帳戶的 VPC 的一部分。多可用區域檔案系統有兩個彈性網路介面，每個檔案伺服器各一個。單一可用區域檔案系統有一個彈性網路介面。

> **Warning**
>
> 請勿修改或刪除與檔案系統相關聯的彈性網路介面。修改或刪除網路介面可能會導致 VPC 和檔案系統之間的連線永久中斷。

下表摘要說明 FSx for Windows File Server Single-AZ 和 Multi-AZ 檔案系統的資源使用率：

檔案系統部署類型	子網路數量	彈性網路介面的數量	IP 地址數量
單一可用區 2	1	1	2
單一可用區 1	1	1	1
Multi-AZ	2	2	4

建立檔案系統後，其 IP 地址在刪除檔案系統之前不會變更。

> **Important**
>
> Amazon FSx 不支援從 存取檔案系統，或將檔案系統公開至公有網際網路。如果彈性 IP 地址，即可從網際網路連線的公有 IP 地址，連接至檔案系統的彈性網路介面，Amazon FSx 會自動將其分離。

使用 Microsoft Active Directory

當您建立 FSx for Windows File Server 檔案系統時，您可以將其加入 Active Directory 網域，以提供使用者身分驗證和檔案和資料夾層級存取控制。Amazon FSx 可與 Microsoft Active Directory 搭配使用，以與您現有的 Microsoft Windows 環境整合。Amazon FSx 透過 Active Directory 使用您的 FSx for Windows File Server 檔案系統提供兩個選項： 搭配 使用 Amazon FSx AWS Directory Service for Microsoft Active Directory和 使用自我管理的 Microsoft Active Directory。

Active Directory 是 Microsoft 目錄服務，用於儲存網路上物件的相關資訊，並讓管理員和使用者輕鬆尋找和使用此資訊。這些物件通常包含共用資源，例如檔案伺服器、網路使用者和電腦帳戶。

然後，您的使用者可以在 Active Directory 中使用其現有的使用者身分來驗證自己，並存取 FSx for Windows File Server 檔案系統。使用者也可以使用其現有的身分來控制對個別檔案和資料夾的存取。此外，您可以將現有的檔案和資料夾及其安全存取控制清單 (ACL) 組態遷移至 Amazon FSx，而不需進行任何修改。

> **Note**
>
> Amazon FSx 支援 Microsoft Azure Active Directory Domain Services，您可以加入 Microsoft Azure Active Directory。

為檔案系統建立聯結的 Active Directory 組態後，您只能更新下列屬性：

- 服務使用者登入資料
- DNS 伺服器 IP 地址

建立檔案系統後，您無法變更已加入 Microsoft AD 的下列屬性：

- DomainName
- OrganizationalUnitDistinguishedName
- FileSystemAdministratorsGroup

不過，您可以從備份建立新的檔案系統，並在新檔案系統的 Microsoft Active Directory 整合組態中變更這些屬性。如需詳細資訊，請參閱將備份還原至新的檔案系統。

> **Note**
>
> Amazon FSx 不支援 Active Directory Connector 和 Simple Active Directory。

如果您的 Active Directory 組態發生變更而中斷與檔案系統的連線，您的 FSx for Windows File Server 可能會設定錯誤。若要將檔案系統傳回可用狀態，請在 Amazon FSx 主控台中選取嘗試復原按鈕，或在 Amazon FSx API 或主控台中使用 `StartMisconfiguredStateRecovery`命令。如需詳細資訊，請參閱 檔案系統處於設定錯誤狀態。

主題

- 搭配 使用 Amazon FSx AWS Directory Service for Microsoft Active Directory
- 使用自我管理的 Microsoft Active Directory

搭配 使用 Amazon FSx AWS Directory Service for Microsoft Active Directory

AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) 在雲端提供全受管、高可用性的實際 Active Directory 目錄。您可以在工作負載部署中使用這些 Active Directory 目錄。

如果您的組織使用 AWS Managed Microsoft AD 來管理身分和裝置，我們建議您整合 Amazon FSx 檔案系統 AWS Managed Microsoft AD。如此一來，您就可以使用 Amazon FSx with AWS Managed Microsoft AD. 取得統包解決方案。 會 AWS 處理兩種服務的部署、操作、高可用性、可靠性、安全性和無縫整合，讓您專注於有效操作自己的工作負載。

若要搭配您的 AWS Managed Microsoft AD 設定使用 Amazon FSx，您可以使用 Amazon FSx 主控台。當您在主控台中建立新的 FSx for Windows File Server 檔案系統時，請選擇 Windows 驗證區段下的AWS 受管 Active Directory。您也可以選擇要使用的特定目錄。如需詳細資訊，請參閱步驟 5. 建立您的檔案系統。

您的組織可能會在自我管理的 Active Directory 網域（內部部署或雲端）上管理身分和裝置。若是如此，您可以將 Amazon FSx 檔案系統直接加入現有的自我管理 Active Directory 網域。如需詳細資訊，請參閱使用自我管理的 Microsoft Active Directory。

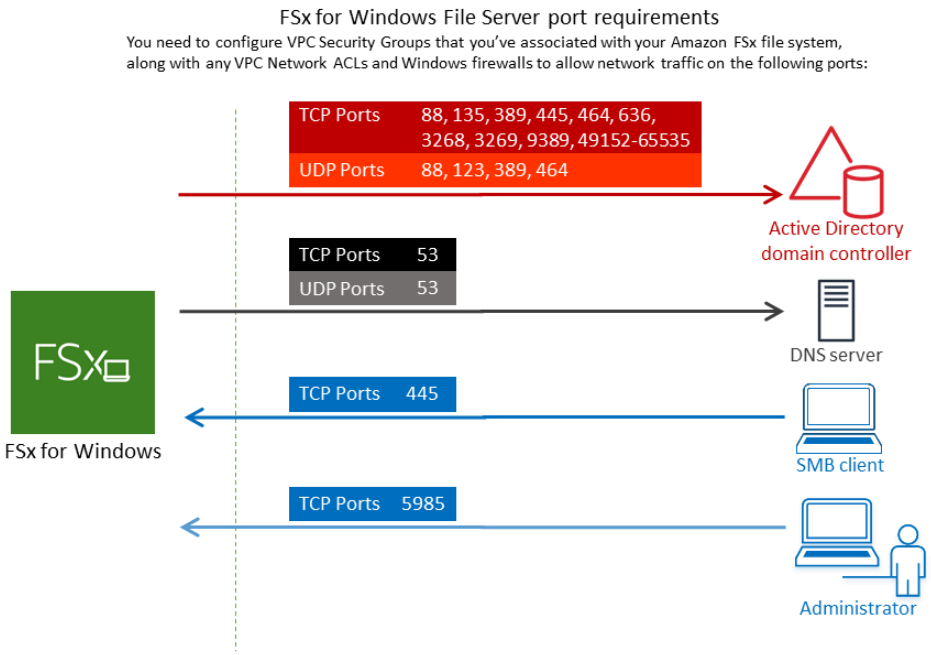
此外，您也可以設定您的系統，從資源樹系隔離模型中受益。在此模型中，您會將 資源隔離，包括您的 Amazon FSx 檔案系統，與使用者所在的樹系隔離成不同的 Active Directory 樹系。

> **Important**
>
> 對於單一可用區 2 和所有多可用區檔案系統，Active Directory 完整網域名稱 (FQDN) 不得超過 47 個字元。

網路先決條件

在建立加入 AWS Microsoft Managed Active Directory 網域的 FSx for Windows File Server 檔案系統之前，請確定您已建立並設定下列網路組態：

- 對於 VPC 安全群組，預設 Amazon VPC 的預設安全群組已新增至主控台中的檔案系統。請確定您建立 FSx 檔案系統之子網路的安全群組和 VPC 網路 ACLs 允許連接埠上的流量，並依照下圖所示的指示。



下表識別每個連接埠的角色。

通訊協定	連接埠	角色
TCP/UDP	53	網域名稱系統 (DNS)
TCP/UDP	88	Kerbe 身分驗證
TCP/UDP	464	變更/設定密碼
TCP/UDP	389	輕量型目錄存取通訊協定 (LDAP

通訊協定	連接埠	角色
UDP	123	網路時間通訊協定 (NTP)
TCP	135	分散式運算環境/端點映射器 (DCE/EPMAP)

通訊協定	連接埠	角色
TCP	445	目錄服務 SMB 檔案共用
TCP	636	透過 TLS/SSL 的輕量型目錄存取通訊協定 (LDAP
TCP	3268	Micros Globa Catalo

通訊協定	連接埠	角色
TCP	3269	透過 SSL 的 Micros Globa Catalo
TCP	5985	WinRI 2.0 (Micro t Windo 遠端管理）
TCP	9389	Micros AD DS Web Servic Powe l

通訊協定	連接埠	角色
TCP	49152 - 65535	適用於 RPC 的暫時性連接埠

> **Important**
>
> 單一可用區 2 和所有多可用區檔案系統部署需要允許 TCP 連接埠 9389 上的傳出流量。

> **Note**
>
> 如果您使用的是 VPC 網路 ACLs，您還必須允許來自 FSx 檔案系統的動態連接埠 (49152-65535) 上的傳出流量。

- 如果您要將 Amazon FSx 檔案系統連線到不同 VPC 或帳戶中的 AWS 受管 Microsoft Active Directory，請確保該 VPC 與您要建立檔案系統的 Amazon VPC 之間有連線。如需詳細資訊，請參閱在不同的 VPC 或帳戶中 AWS Managed Microsoft AD 使用 Amazon FSx 搭配。

> **Important**
>
> 雖然 Amazon VPC 安全群組要求連接埠僅以網路流量起始的方向開啟，但 VPC 網路 ACLs 要求連接埠雙向開啟。

使用 Amazon FSx 網路驗證工具來驗證與 Active Directory 網域控制站的連線。

使用資源樹系隔離模型

您可以將檔案系統加入 AWS Managed Microsoft AD 設定。然後，您可以在您建立的 AWS Managed Microsoft AD 網域與現有的自我管理 Active Directory 網域之間建立單向樹系信任關係。對於 Amazon FSx 中的 Windows 身分驗證，您只需單向樹系信任，其中 AWS 受管樹系信任公司網域樹系。

您的公司網域擔任信任網域的角色，而 Directory Service 受管網域則擔任信任網域的角色。驗證的身分驗證請求只會以一個方向在網域之間傳輸，允許您公司網域中的帳戶對受管網域中共用的資源進行身分驗證。在此情況下，Amazon FSx 只會與 AWS 受管網域互動。在 Kerberos 身分驗證案例中，來自公司用戶端的身分驗證請求會由公司網域進行驗證，然後其會參考 AWS Managed Microsoft AD，最終用戶端會向 FSx for Windows File Server 檔案系統出示其服務票證。如需信任的詳細資訊，請參閱 AWS 安全部落格中的文章 您要知道有關與 信任的所有相關資訊 AWS Managed Microsoft AD。

測試您的 Active Directory 組態

建立 Amazon FSx 檔案系統之前，建議您使用 Amazon FSx 網路驗證工具來驗證 Active Directory 網域控制站的連線。如需詳細資訊，請參閱驗證 Active Directory 網域控制站的連線。

下列相關資源可協助您 AWS Directory Service for Microsoft Active Directory 搭配 FSx for Windows File Server 使用：

- AWS Directory Service 管理指南中的內容 Directory Service
- 《AWS Directory Service 管理指南》中的建立 AWS Managed Active Directory
- 《AWS Directory Service 管理指南》中的建立信任關係的時機

在不同的 VPC 或帳戶中 AWS Managed Microsoft AD 使用 Amazon FSx 搭配

您可以使用 VPC 對等互連，將 FSx for Windows File Server 檔案系統加入同一帳戶中不同 VPC 中的 AWS Managed Microsoft AD 目錄。您也可以使用 AWS Managed Microsoft AD 目錄共用，將檔案系統加入不同 AWS 帳戶中的目錄。

> **Note**
>
> 您只能在與檔案系統 AWS 區域 相同的 AWS Managed Microsoft AD 內選取 。如果您想要使用跨區域 VPC 對等設定，您應該使用自我管理的 Microsoft Active Directory。如需詳細資訊，請參閱使用自我管理的 Microsoft Active Directory。

將檔案系統加入不同 VPC 中的 AWS Managed Microsoft AD 的工作流程包含下列步驟：

1. 設定您的聯網環境。
2. 共用您的目錄。
3. 將檔案系統加入共用目錄。

如需詳細資訊，請參閱《 Directory Service 管理指南》中的共用您的目錄。

若要設定您的聯網環境，您可以使用 AWS Transit Gateway 或 Amazon VPC 並建立 VPC 互連連線。此外，請確定兩個 VPCs 之間允許網路流量。

傳輸閘道是網路傳輸中樞，您可以用於互相連接 VPC 和現場部署網路。如需使用 VPC 傳輸閘道的詳細資訊，請參閱《Amazon VPC 傳輸閘道指南》中的傳輸閘道入門。

VPC 對等連接是在兩個 VPC 之間的網路連線。此連線可讓您使用私有網際網路通訊協定第 4 版 (IPv4) 或網際網路通訊協定第 6 版 (IPv6) 地址，在它們之間路由流量。您可以使用 VPC 對等互連來連接相同 AWS 區域 或兩者之間的 VPCs AWS 區域。如需 VPC 互連的詳細資訊，請參閱《Amazon VPC 互連指南》中的什麼是 VPC 互連？。

當您將檔案系統加入與檔案系統不同的 帳戶中的 AWS Managed Microsoft AD 目錄時，還有另一個先決條件。您也需要與其他 帳戶共用 Microsoft Active Directory。若要這樣做，您可以使用 AWS Managed Microsoft Active Directory 的目錄共用功能。若要進一步了解，請參閱《 AWS Directory Service 管理指南》中的共用您的目錄。

驗證 Active Directory 網域控制站的連線

建立加入 Active Directory 的 FSx for Windows File Server 檔案系統之前，請使用 Amazon FSx Active Directory 驗證工具來驗證與 Active Directory 網域的連線。無論您使用 FSx for Windows File Server 搭配 AWS Managed Microsoft Active Directory 或自我管理 Active Directory 組態，都可以使用此測試。網域控制站網路連線測試 (Test-FSxADControllerConnection) 不會對網域中的每個網域控制站執行完整的網路連線檢查套件。反之，請使用此測試對一組特定的網域控制站執行網路連線驗證。

驗證與 Active Directory 網域控制站的連線

1. 在相同子網路中啟動 Amazon EC2 Windows 執行個體，並使用您將用於 FSx for Windows File Server 檔案系統的相同 Amazon VPC 安全群組。對於異地同步備份部署類型，請將子網路用於偏好的作用中檔案伺服器。
2. 將 EC2 Windows 執行個體加入 Active Directory。如需詳細資訊，請參閱《 AWS Directory Service 管理指南》中的手動加入 Windows 執行個體。

3. 連線至 EC2 執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的連線至您的 Windows 執行個體。
4. 在 EC2 執行個體上開啟 Windows PowerShell 視窗（使用以管理員身分執行)。

   若要測試是否已安裝 Windows PowerShell 所需的 Active Directory 模組，請使用下列測試命令。

   ```
   PS C:\> Import-Module ActiveDirectory
   ```

   如果上述 傳回錯誤，請使用下列命令進行安裝。

   ```
   PS C:\> Install-WindowsFeature RSAT-AD-PowerShell
   ```
5. 使用下列命令下載網路驗證工具。

   ```
   PS C:\> Invoke-WebRequest "https://docs.aws.amazon.com/fsx/latest/WindowsGuide/
   samples/AmazonFSxADValidation.zip" -OutFile "AmazonFSxADValidation.zip"
   ```
6. 使用以下命令展開 zip 檔案。

   ```
   PS C:\> Expand-Archive -Path "AmazonFSxADValidation.zip"
   ```
7. 將 AmazonFSxADValidation 模組新增至目前的工作階段。

   ```
   PS C:\> Import-Module .\AmazonFSxADValidation
   ```
8. 設定 Active Directory 網域控制站 IP 地址的值，並使用下列命令執行連線測試：

   ```
   $ADControllerIp = '10.0.75.243'
   $Result = Test-FSxADControllerConnection -ADControllerIp $ADControllerIp
   ```
9. 下列範例示範擷取測試輸出，以及成功連線測試的結果。

   ```
   PS C:\AmazonFSxADValidation> $Result

   Name                           Value
   ----                           -----
   TcpDetails                     {@{Port=88; Result=Listening; Description=Kerberos
    authentication}, @{Port=135; Resul...
   ```

```
Server                          10.0.75.243
UdpDetails                      {@{Port=88; Result=Timed Out; Description=Kerberos
 authentication}, @{Port=123; Resul...
Success                         True


PS C:\AmazonFSxADValidation> $Result.TcpDetails

Port Result    Description
---- ------    -----------
  88 Listening Kerberos authentication
 135 Listening DCE / EPMAP (End Point Mapper)
 389 Listening Lightweight Directory Access Protocol (LDAP)
 445 Listening Directory Services SMB file sharing
 464 Listening Kerberos Change/Set password
 636 Listening Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
3268 Listening Microsoft Global Catalog
3269 Listening Microsoft Global Catalog over SSL
9389 Listening Microsoft AD DS Web Services, PowerShell
```

下列範例顯示執行測試並取得失敗的結果。

```
PS C:\AmazonFSxADValidation> $Result = Test-FSxADControllerConnection -
ADControllerIp $ADControllerIp
WARNING: TCP 9389 failed to connect. Required for Microsoft AD DS Web Services,
 PowerShell.
Verify security group and firewall settings on both client and directory
 controller.
WARNING: 1 ports failed to connect to 10.0.75.243. Check pre-requisites in
https://docs.aws.amazon.com/fsx/latest/WindowsGuide/self-managed-AD.html#self-
manage-prereqs

PS C:\AmazonFSxADValidation> $Result

Name                            Value
----                            -----
TcpDetails                      {@{Port=88; Result=Listening; Description=Kerberos
 authentication}, @{Port=135; Resul...
Server                          10.0.75.243
UdpDetails                      {@{Port=88; Result=Timed Out; Description=Kerberos
 authentication}, @{Port=123; Resul...
Success                         False
FailedTcpPorts                  {9389}
```

```
PS C:\AmazonFSxADValidation> $Result.FailedTcpPorts
9389
```

Windows socket error code mapping

https://msdn.microsoft.com/en-us/library/ms740668.aspx

> **Note**
>
> 除了上述程序之外，您也可以使用 AWSSupport-ValidateFSxWindowsADConfig Runbook 驗證自我管理的 Active Directory 組態。如需詳細資訊，請參閱 AWS Systems Manager Automation Runbook 參考 中的 AWSSupport-ValidateFSxWindowsADConfig。

使用自我管理的 Microsoft Active Directory

如果您的組織使用內部部署或雲端的自我管理 Active Directory 管理身分和裝置，您可以在建立時將 FSx for Windows File Server 檔案系統加入 Active Directory 網域。

當您將檔案系統加入自我管理的 Active Directory 時，您的 FSx for Windows File Server 檔案系統位於相同的 Active Directory 樹系 (Active Directory 組態中包含網域、使用者和電腦的最上層邏輯容器），以及與您的使用者和現有資源（包括現有的檔案伺服器）位於相同的 Active Directory 網域中。

> **Note**
>
> 您可以將 資源 - 包括 Amazon FSx 檔案系統 - 隔離到與使用者所在樹系不同的 Active Directory 樹系。若要這樣做，請將您的檔案系統加入 AWS Managed Microsoft Active Directory，並在您建立的 AWS Managed Microsoft Active Directory 與現有的自我管理 Active Directory 之間建立單向樹系信任關係。

- Active Directory 網域上服務帳戶的使用者名稱和密碼，讓 Amazon FSx 用來將檔案系統加入 Active Directory 網域。您可以將這些登入資料提供為純文字，或將其存放在 ， AWS Secrets Manager 並提供秘密 ARN（建議）。

- （選用）您要在其中加入檔案系統之網域中的組織單位 (OU)。
- （選用）您要委派授權對檔案系統執行管理動作的網域群組。例如，此網域群組可能會管理 Windows 檔案共用、管理檔案系統根資料夾上的存取控制清單 (ACLs)、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。

> **Note**
>
> 您提供的網域群組名稱在 Active Directory 中必須是唯一的。FSx for Windows File Server 不會在下列情況下建立網域群組：
>
> - 如果具有您指定名稱的群組已存在
> - 如果您未指定名稱，且 Active Directory 中已存在名為「網域管理員」的群組。

如需詳細資訊，請參閱將 Amazon FSx 檔案系統加入自我管理的 Microsoft Active Directory 網域。

主題

先決條件

將 FSx for Windows File Server 檔案系統加入自我管理的 Microsoft Active Directory 網域之前，請檢閱下列先決條件，以協助確保您可以將 Amazon FSx 檔案系統成功加入自我管理的 Active Directory。

內部部署組態

這些是您將加入 Amazon FSx 檔案系統的自我管理 Microsoft Active Directory 的先決條件，無論是內部部署或雲端型。

- Active Directory 網域控制站：
  - 必須具有 Windows Server 2008 R2 或更高版本的網域功能層級。
  - 必須可寫入。
  - 至少一個可連線網域控制站必須是樹系的全域目錄。
- DNS 伺服器必須能夠解析名稱，如下所示：
  - 在您加入檔案系統的網域中
  - 在樹系的根網域中
- DNS 伺服器和 Active Directory 網域控制站 IP 地址必須符合下列要求，這取決於建立 Amazon FSx 檔案系統的時間：

對於 2020 年 12 月 17 日之前建立的檔案系統	對於 2020 年 12 月 17 日之後建立的檔案系統
IP 地址必須位於 RFC 1918 私有 IP 地址範圍內： • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	IP 地址可以在任何範圍內，但以下除外： • 在 檔案系統所在的 中，與 Amazon Web Services 擁有 AWS 區域 的 IP 地址衝突的 IP 地址。如需依區域列出的 AWS 擁有 IP 地址清單，請參閱 AWS IP 地址範圍。 • CIDR 區塊範圍為 198.19.0.0/16 的 IP 地址

  如果您需要使用非私有 IP 地址範圍存取 2020 年 12 月 17 日之前建立的 FSx for Windows File Server 檔案系統，您可以透過還原檔案系統的備份來建立新的檔案系統。如需詳細資訊，請參閱將備份還原至新的檔案系統。
- 自我管理 Active Directory 的網域名稱必須符合下列要求：
  - 網域名稱不是單一標籤網域 (SLD) 格式。Amazon FSx 不支援 SLD 網域。
  - 對於單一可用區 2 和所有多可用區檔案系統，網域名稱不能超過 47 個字元。
- 您已定義的任何 Active Directory 網站必須符合下列先決條件：
  - VPC 中與您檔案系統相關聯的子網路必須在 Active Directory 網站中定義。
  - VPC 子網路和任何 Active Directory 站點子網路之間沒有任何衝突。

Amazon FSx 需要連線至您在 Active Directory 環境中定義的網域控制站或 Active Directory 網站。Amazon FSx 將忽略連接埠 389 上封鎖 TCP 和 UDP 的任何網域控制站。對於 Active Directory 中的其餘網域控制站，請確保它們符合 Amazon FSx 連線需求。此外，請確認您的服務帳戶的任何變更都會傳播到所有這些網域控制站。

> **Important**
>
> 建立檔案系統後，請勿移動 Amazon FSx 在 OU 中建立的電腦物件。這樣做會導致您的檔案系統設定錯誤。

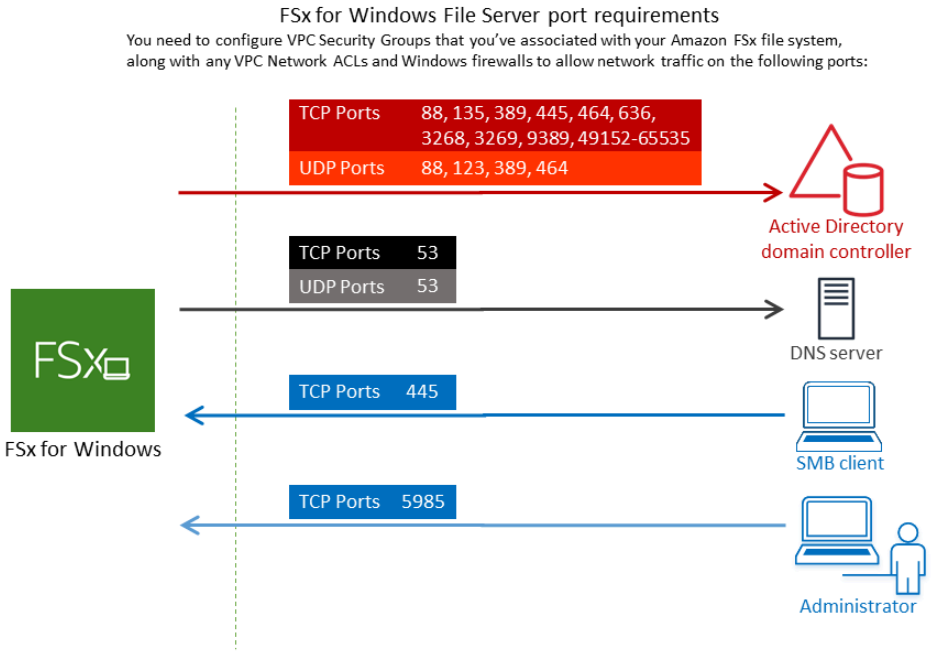
您可以使用 Amazon FSx Active Directory 驗證工具來驗證 Active Directory 組態，包括測試多個網域控制站的連線。若要限制需要連線的網域控制站數量，您也可以在內部部署網域控制站與 之間建立信任關係 AWS Managed Microsoft AD。如需詳細資訊，請參閱使用資源樹系隔離模型。

> **Important**
>
> 如果您使用 Microsoft DNS 做為預設 DNS 服務，Amazon FSx 只會註冊檔案系統的 DNS 記錄。如果您使用第三方 DNS，則需要在建立檔案系統之後手動設定 DNS 記錄項目。

網路組態

本節說明將檔案系統加入自我管理 Active Directory 的網路組態需求。強烈建議您在嘗試將檔案系統加入自我管理 Active Directory 之前，使用 Amazon FSx Active Directory 驗證工具來測試網路設定。

- 確保您的防火牆規則將允許 Active Directory 網域控制站與 Amazon FSx 之間的 ICMP 流量。
- 必須在您要建立檔案系統和自我管理 Active Directory 的 Amazon VPC 之間設定連線。您可以使用 Direct Connect、AWS Virtual Private Network、VPC 對等互連或 來設定此連線AWS Transit Gateway。
- 預設 Amazon VPC 的預設 VPC 安全群組必須使用 Amazon FSx 主控台新增至您的檔案系統。確定您建立檔案系統之子網路的安全群組和 VPC 網路 ACLs 允許連接埠和 上的流量，如下圖所示。



下表識別通訊協定、連接埠及其角色。

通訊協定	連接埠	Role
TCP/UDP	53	網域名稱系統 (DNS)
TCP/UDP	88	Kerberos 身分驗證
TCP/UDP	464	變更/設定密碼
TCP/UDP	389	輕量型目錄存取通訊協定 (LDAP)
UDP	123	網路時間通訊協定 (NTP)
TCP	135	分散式運算環境/端點映射器 (DCE/EPMAP)
TCP	445	目錄服務 SMB 檔案共用
TCP	636	透過 TLS/SSL 的輕量型目錄存取通訊協定 (LDAPS)
TCP	3268	Microsoft 全球目錄

通訊協定	連接埠	Role
TCP	3269	透過 SSL 的 Microsoft Global Catalog
TCP	5985	WinRM 2.0 (Microsoft Windows 遠端管理)
TCP	9389	Microsoft Active Directory DS Web Services、PowerShell **Important** 單一可用區 2 和多可用區檔案系統部署需要允許 TCP 連接埠 9389 上的傳出流量。
TCP	49152 - 65535	適用於 RPC 的暫時性連接埠

這些流量規則也需要在套用至每個 Active Directory 網域控制站、DNS 伺服器、FSx 用戶端和 FSx 管理員的防火牆上鏡像。

Note

如果您使用的是 VPC 網路 ACLs，您還必須允許來自檔案系統的動態連接埠 ((49152-65535) 上的傳出流量。

Important

雖然 Amazon VPC 安全群組要求僅在啟動網路流量的方向上開啟連接埠，但大多數 Windows 防火牆和 VPC 網路 ACLs 要求雙向開啟連接埠。

服務帳戶許可

您需要在自我管理的 Microsoft Active Directory 中擁有服務帳戶，具有將電腦物件加入自我管理 Active Directory 網域的委派許可。服務帳戶是自我管理 Active Directory 中已委派特定任務的使用者帳戶。

以下是必須委派給您要加入檔案系統之 OU 中 Amazon FSx 服務帳戶的一組最低許可。

- 如果在 Active Directory 使用者和電腦 MMC 中使用委派控制：
  - 重設密碼
  - 讀取和寫入帳戶限制
  - 驗證寫入 DNS 主機名稱
  - 驗證寫入服務主體名稱
- 如果在 Active Directory 使用者和電腦 MMC 中使用進階功能：
  - 修改許可
  - 建立電腦物件
  - 刪除電腦物件

如需詳細資訊，請參閱 Microsoft Windows Server 文件主題 錯誤：當被委派控制的非管理員使用者嘗試將電腦加入網域控制站時，存取遭拒。

如需設定所需許可的詳細資訊，請參閱 將許可委派給 Amazon FSx 服務帳戶或群組。

使用自我管理 Active Directory 時的最佳實務

主題

- 使用 存放 Active Directory 登入資料 AWS Secrets Manager

建議您在將 Amazon FSx for Windows File Server 檔案系統加入自我管理的 Microsoft Active Directory 時，遵循這些最佳實務。這些最佳實務可協助您維持檔案系統的持續、不間斷可用性。

使用 Amazon FSx 的個別服務帳戶

使用個別的服務帳戶來委派 Amazon FSx 所需的權限，以完整管理加入自我管理 Active Directory 的檔案系統。不建議為此目的使用網域管理員。

使用 Active Directory 群組

使用 Active Directory 群組來管理與 Amazon FSx 服務帳戶相關聯的 Active Directory 許可和組態。

隔離組織單位 (OU)

為了更輕鬆地尋找和管理 Amazon FSx 電腦物件，建議您將 FSx for Windows File Server 檔案系統所使用的組織單位 (OU) 與其他網域控制站問題分開。

將 Active Directory 組態up-to-date

您必須將檔案系統的 Active Directory 組態保持在up-to-date，才能進行任何變更。例如，如果您的自我管理 Active Directory 使用以時間為基礎的密碼重設政策，一旦重設密碼，請務必更新檔案系統上的服務帳戶密碼。如需詳細資訊，請參閱更新自我管理 Active Directory 組態。

變更 Amazon FSx 服務帳戶

如果您使用新的服務帳戶更新檔案系統，它必須具有加入 Active Directory 所需的許可和權限，並擁有與檔案系統相關聯之現有電腦物件的完整控制許可。如需詳細資訊，請參閱變更 Amazon FSx 服務帳戶。

將子網路指派給單一 Microsoft Active Directory 網站

如果您的 Active Directory 環境有大量的網域控制站，請使用 Active Directory 網站和服務，將 Amazon FSx 檔案系統使用的子網路指派給具有最高可用性和可靠性的單一 Active Directory 網站。請確定DCs 上的 VPC 安全群組、VPC 網路 ACL、Windows 防火牆規則，以及您在 Active Directory 基礎設施中擁有的任何其他網路路由控制，允許在必要的連接埠上從 Amazon FSx 進行通訊。如果 Windows 無法使用指派的 Active Directory 網站，這可讓 Windows 還原至其他網域控制站。如需詳細資訊，請參閱使用 Amazon VPC 的檔案系統存取控制。

使用安全群組規則來限制流量

使用安全群組規則在虛擬私有雲端 (VPC) 中實作最低權限原則。您可以使用 VPC 安全群組規則來限制檔案允許的傳入和傳出網路流量類型。例如，我們建議僅允許傳出流量到自我管理的 Active Directory 網域控制站，或您正在使用的子網路或安全群組內。如需詳細資訊，請參閱使用 Amazon VPC 的檔案系統存取控制。

請勿移動建立的 Amazon FSx 電腦物件

> **Important**
>
> 建立檔案系統後，請勿移動 Amazon FSx 在 OU 中建立的電腦物件。這樣做會導致您的檔案系統設定錯誤。

驗證您的 Active Directory 組態

在嘗試將 FSx for Windows File Server 檔案系統加入 Active Directory 之前，強烈建議您使用 Amazon FSx Active Directory 驗證工具來驗證 Active Directory 組態。

使用 存放 Active Directory 登入資料 AWS Secrets Manager

您可以使用 AWS Secrets Manager 安全地存放和管理 Microsoft Active Directory 網域聯結服務帳戶登入資料。這種方法不需要將敏感登入資料以純文字形式存放在應用程式程式碼或組態檔案中，以強化您的安全狀態。

您也可以設定 IAM 政策來管理對秘密的存取，並設定密碼的自動輪換政策。

在 AWS Secrets Manager （主控台）中存放 Active Directory 登入資料

步驟 1：建立 KMS 金鑰

建立 KMS 金鑰來加密和解密 Secrets Manager 中的 Active Directory 登入資料。

建立金鑰

> **Note**
>
> 對於加密金鑰，建立新的金鑰，請勿使用 AWS 預設 KMS 金鑰。請務必 AWS KMS key 在包含您要加入 Active Directory 之檔案系統的相同區域中建立 。

1. 在 https：//https://console.aws.amazon.com/kms 開啟 AWS KMS 主控台。
2. 選擇建立金鑰。
3. 對於金鑰類型，選擇對稱。
4. 對於金鑰用途，選擇加密和解密。
5. 對於進階選項，請執行下列動作：
   a. 對於金鑰材料來源，選擇 KMS。
   b. 針對區域性，選擇單一區域金鑰，然後選擇下一步。
6. 選擇下一步。
7. 對於別名，提供 KMS 金鑰的名稱。
8. (選用) 對於描述，提供 KMS 金鑰的描述。
9. （選用）針對標籤，提供 KMS 金鑰的標籤，然後選擇下一步。
10. （選用）對於金鑰管理員，請提供有權管理此金鑰的 IAM 使用者和角色。
11. 針對金鑰刪除，請保留選取允許金鑰管理員刪除此金鑰的方塊，然後選擇下一步。

12. （選用）對於金鑰使用者，請提供授權在密碼編譯操作中使用此金鑰的 IAM 使用者和角色。選擇下一步。
13. 針對金鑰政策，選擇編輯並在政策陳述式中包含以下內容，以允許 Amazon FSx 使用 KMS 金鑰，然後選擇下一步。請務必將 *us-west-2* 取代為部署 AWS 區域 檔案系統的 ，並將 *123456789012* 取代為您的 AWS 帳戶 ID。

```
{
    "Sid": "Allow FSx to use the KMS key",
    "Version": "2012-10-17",
    "Effect": "Allow",
    "Principal": {
        "Service": "fsx.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:DescribeKey"
    ],
    "Resource": "arn:aws:kms:us-west-2:123456789012:key:*",
    "Condition": {
        "StringEquals": {
            "kms:EncryptionContext:SecretARN": "arn:aws:secretsmanager:us-
west-2:123456789012:secret:*",
            "kms:ViaService": "secretsmanager.us-west-2.amazonaws.com",
            "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:fsx:us-west-2:123456789012:file-system/*"
        }
    }
}
```

14. 選擇完成。

> **Note**
>
> 您可以修改 `Resource`和 `aws:SourceArn` 欄位以鎖定特定秘密和檔案系統，藉此設定更精細的存取控制。

步驟 2：建立 AWS Secrets Manager 秘密

若要建立機密

1. 請開啟位於 https://console.aws.amazon.com/secretsmanager/ 的機密管理員控制台。
2. 選擇存放新的機密。
3. 針對機密類型，選擇其他類型的機密。
4. 對於金鑰/值對，請執行下列動作來新增您的兩個金鑰：
   a. 對於第一個金鑰，輸入 CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME。
   b. 對於第一個金鑰的值，僅輸入 AD 使用者的使用者名稱 (不含網域字首)。
   c. 對於第二個金鑰，輸入 CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD。
   d. 對於第二個金鑰的值，輸入您在網域上為 AD 使用者建立的密碼。
5. 對於加密金鑰，輸入您在上一個步驟中建立的 KMS 金鑰的 ARN，然後選擇下一步。
6. 對於秘密名稱，輸入可協助您稍後尋找密碼的描述性名稱。
7. (選用) 對於描述，輸入秘密名稱的描述。
8. 針對資源許可，選擇編輯。

   將下列政策新增至許可政策，以允許 Amazon FSx 使用秘密，然後選擇下一步。請務必將 *us-west-2* 取代為部署 AWS 區域 檔案系統的 ，並將 *123456789012* 取代為您的 AWS 帳戶 ID。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "fsx.amazonaws.com"
            },
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": "arn:aws:secretsmanager:us-west-2:123456789012:secret:*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
```

```
                    "aws:SourceArn": "arn:aws:fsx:us-west-2:123456789012:file-
system/*"
                }
            }
        }
    ]
}
```

> **Note**
>
> 您可以修改 `Resource`和 `aws:SourceArn` 欄位以鎖定特定秘密和檔案系統，藉此設定更精細的存取控制。

9. （選用）您可以設定 Secrets Manager 自動輪換您的登入資料。選擇下一步。
10. 選擇完成。

在 AWS Secrets Manager (CLI) 中存放 Active Directory 登入資料

步驟 1：建立 KMS 金鑰

建立 KMS 金鑰來加密和解密 Secrets Manager 中的 Active Directory 登入資料。

若要建立 KMS 金鑰，請使用 AWS CLI 命令 create-key。

在此命令中，設定 `--policy` 參數以指定定義 KMS 金鑰許可的金鑰政策。政策必須包含下列項目：

- Amazon FSx 的服務主體，即 `fsx.amazonaws.com`。
- 必要的 KMS 動作： `kms:Decrypt`和 `kms:DescribeKey`。
- 您 AWS 區域 和 帳戶的資源 ARN 模式。
- 限制金鑰用量的條件金鑰：
  - `kms:ViaService` 以確保請求來自 Secrets Manager。
  - `aws:SourceAccount` 限制為您的帳戶。
  - `aws:SourceArn` 限制為特定 Amazon FSx 檔案系統。

下列範例會使用允許 Amazon FSx 使用金鑰進行解密和金鑰描述操作的政策來建立對稱加密 KMS 金鑰。命令會自動擷取您的 AWS 帳戶 ID 和區域，然後使用這些值設定金鑰政策，以確保 Amazon FSx、Secrets Manager 和 KMS 金鑰之間的適當存取控制。請確定您的 AWS CLI 環境與將加入 Active Directory 的檔案系統位於相同的區域。

```
# Set region and get Account ID
REGION=${AWS_REGION:-$(aws configure get region)}
ACCOUNT_ID=$(aws sts get-caller-identity --query 'Account' --output text)

# Create Key
KMS_KEY_ARN=$(aws kms create-key --policy "{
  \"Version\": \"2012-10-17\",
  \"Statement\": [
    {
      \"Sid\": \"Enable IAM User Permissions\",
      \"Effect\": \"Allow\",
      \"Principal\": {
        \"AWS\": \"arn:aws:iam::$ACCOUNT_ID:root\"
      },
      \"Action\": \"kms:*\",
      \"Resource\": \"*\"
    },
    {
      \"Sid\": \"Allow FSx to use the KMS key\",
      \"Effect\": \"Allow\",
      \"Principal\": {
        \"Service\": \"fsx.amazonaws.com\"
      },
      \"Action\": [
        \"kms:Decrypt\",
        \"kms:DescribeKey\"
      ],
      \"Resource\": \"*\",
      \"Condition\": {
        \"StringEquals\": {
          \"kms:ViaService\": \"secretsmanager.$REGION.amazonaws.com\",
          \"aws:SourceAccount\": \"$ACCOUNT_ID\"
        },
        \"ArnLike\": {
          \"aws:SourceArn\": \"arn:aws:fsx:$REGION:$ACCOUNT_ID:file-system/*\"
        }
      }
    }
  ]
}" --query 'KeyMetadata.Arn' --output text)

echo "KMS Key ARN: $KMS_KEY_ARN"
```

> **Note**
>
> 您可以修改 `Resource`和 `aws:SourceArn` 欄位以鎖定特定秘密和檔案系統，藉此設定更精細的存取控制。

步驟 2：建立 AWS Secrets Manager 秘密

若要為 Amazon FSx 建立秘密以存取您的 Active Directory，請使用 AWS CLI 命令 create-secret 並設定下列參數：

- `--name`：秘密的識別符。
- `--description`：秘密用途的描述。
- `--kms-key-id`：您在步驟 1 中建立用於加密靜態秘密之 KMS 金鑰的 ARN。
- `--secret-string`：JSON 字串，其中包含以下格式的 AD 登入資料：
  - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME`：沒有網域字首的 AD 服務帳戶使用者名稱，例如 `svc-fsx`。請勿提供網域字首，例如 `CORP\svc-fsx`。
  - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD`：您的 AD 服務帳戶密碼。
- `--region`：建立 Amazon FSx 檔案系統的 AWS 區域 。如果`AWS_REGION`未設定 ，則預設為您設定的區域。

建立秘密後，使用 put-resource-policy 命令連接資源政策，並設定下列參數：

- `--secret-id`：要連接政策的秘密名稱或 ARN。下列範例使用 **`FSxSecret`**做為 `--secret-id`。
- `--region`：與您的秘密 AWS 區域 相同。
- `--resource-policy`：授予 Amazon FSx 存取秘密許可的 JSON 政策文件。政策必須包含下列項目：
  - Amazon FSx 的服務主體，即 **`fsx.amazonaws.com`**。
  - 必要的 Secrets Manager 動作： `secretsmanager:GetSecretValue`和 `secretsmanager:DescribeSecret`。
  - 您 AWS 區域 和 帳戶的資源 ARN 模式。
  - 限制存取的下列條件金鑰：
    - `aws:SourceAccount` 限制為您的帳戶。
    - `aws:SourceArn` 限制為特定 Amazon FSx 檔案系統。

下列範例會建立具有所需格式的秘密，並連接允許 Amazon FSx 使用秘密的資源政策。此範例會自動擷取您的 AWS 帳戶 ID 和區域，然後使用這些值設定資源政策，以確保 Amazon FSx 與秘密之間的適當存取控制。

請務必將 取代KMS_KEY_ARN為您在步驟 1、 和 中建立之金鑰的 ARNCUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME，CUSTOMER_MANAGED_ACTIVE_DIRECTORY 代為您的 Active Directory 服務帳戶憑證。此外，請確認您的 AWS CLI 環境已設定為與將加入 Active Directory 的檔案系統相同的區域。

```
# Set region and get account ID
REGION=${AWS_REGION:-$(aws configure get region)}
ACCOUNT_ID=$(aws sts get-caller-identity --query 'Account' --output text)

# Replace with your KMS key ARN from Step 1
KMS_KEY_ARN="arn:aws:kms:us-east-2:123456789012:key/1234542f-d114-555b-9ade-
fec3c9200d8e"

# Replace with your Active Directory credentials
AD_USERNAME="Your_Username"
AD_PASSWORD="Your_Password"

# Create the secret
SECRET_ARN=$(aws secretsmanager create-secret \
  --name "FSxSecret" \
  --description "Secret for FSx access" \
  --kms-key-id "$KMS_KEY_ARN" \
  --secret-string "{\"CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME\":\"$AD_USERNAME\",
\"CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD\":\"$AD_PASSWORD\"}" \
  --region "$REGION" \
  --query 'ARN' \
  --output text)

echo "Secret created with ARN: $SECRET_ARN"

# Attach the resource policy with proper formatting
aws secretsmanager put-resource-policy \
  --secret-id "FSxSecret" \
  --region "$REGION" \
  --resource-policy "{
    \"Version\": \"2012-10-17\",
    \"Statement\": [
      {
        \"Effect\": \"Allow\",
```

```
        \"Principal\": {
          \"Service\": \"fsx.amazonaws.com\"
        },
        \"Action\": [
          \"secretsmanager:GetSecretValue\",
          \"secretsmanager:DescribeSecret\"
        ],
        \"Resource\": \"$SECRET_ARN\",
        \"Condition\": {
          \"StringEquals\": {
            \"aws:SourceAccount\": \"$ACCOUNT_ID\"
          },
          \"ArnLike\": {
            \"aws:SourceArn\": \"arn:aws:fsx:$REGION:$ACCOUNT_ID:file-system/*\"
          }
        }
      }
    ]
  }"

echo "Resource policy attached successfully"
```

> **Note**
>
> 您可以修改 `Resource`和 `aws:SourceArn` 欄位以鎖定特定秘密和檔案系統，藉此設定更精細的存取控制。

Amazon FSx 服務帳戶

加入自我管理 Active Directory 的 Amazon FSx 檔案系統在其生命週期內都需要有效的服務帳戶。Amazon FSx 使用 服務帳戶來完整管理您的檔案系統，並執行需要將電腦物件取消加入和重新加入 Active Directory 網域的管理任務。這些任務包括取代失敗的檔案伺服器和修補 Microsoft Windows Server 軟體。若要讓 Amazon FSx 執行這些任務，Amazon FSx 服務帳戶至少必須擁有服務帳戶許可委派給該帳戶之 中所述的一組許可。

雖然網域管理員群組的成員有足夠的權限來執行這些任務，我們強烈建議您使用個別的服務帳戶，將所需的權限委派給 Amazon FSx。

如需如何使用 Active Directory 使用者和電腦 MMC 嵌入式中的委派控制或進階功能功能委派權限的詳細資訊，請參閱 將許可委派給 Amazon FSx 服務帳戶或群組。

如果您使用新的服務帳戶更新檔案系統，則新服務帳戶必須具有加入 Active Directory 所需的許可和權限，並擁有與檔案系統相關聯之現有電腦物件的完整控制許可。如需詳細資訊，請參閱變更 Amazon FSx 服務帳戶。

為了增強安全性，建議您將 Active Directory 服務帳戶登入資料存放在 中 AWS Secrets Manager 。這消除了以純文字存放敏感登入資料的需求，並符合安全最佳實務。如需詳細資訊，請參閱使用自我管理的 Microsoft Active Directory。

將許可委派給 Amazon FSx 服務帳戶或群組

Amazon FSx 服務帳戶或管理員群組必須具有將 FSx for Windows File Server 檔案系統加入自我管理 Active Directory 網域所需的權限。若要委派這些許可，您可以在 Active Directory User and Computers MMC Snap-in 中使用委派控制或進階功能，如下列程序所述。

使用委派控制指派許可

使用委派控制將許可指派給服務帳戶或群組

1. 以 Active Directory 網域的網域管理員身分登入您的系統。
2. 開啟 Active Directory 使用者和電腦 MMC 嵌入。
3. 在任務窗格中，展開網域節點。
4. 找到並開啟您要修改之 OU 的內容（按一下滑鼠右鍵）選單，然後選擇委派控制。
5. 在控制委派精靈頁面上，選擇下一步。
6. 選擇新增以新增 Amazon FSx 服務帳戶或群組的名稱，然後選擇下一步。
7. 在 Tasks to Delegate (要委派的任務) 頁面上，選擇 Create a custom task to delegate (建立要委派的自訂任務)，然後選擇 Next (下一步)。
8. 選擇僅資料夾中的下列物件，然後選擇電腦物件。
9. 選擇在此資料夾中建立選取的物件，以及在此資料夾中刪除選取的物件。然後選擇下一步。
10. 針對許可，選擇下列項目：
    - 重設密碼
    - 讀取和寫入帳戶限制
    - 驗證寫入 DNS 主機名稱
    - 驗證寫入服務主體名稱
11. 選擇 Next (下一步)，然後選擇 Finish (完成)。
12. 關閉 Active Directory 使用者和電腦 MMC 嵌入。

使用進階功能指派許可

1. 以 Active Directory 網域的網域管理員身分登入您的系統。
2. 開啟 Active Directory 使用者和電腦 MMC 嵌入。
3. 從選單列選取檢視，並確保已啟用進階功能（如果啟用此功能，旁邊會顯示核取記號）。
4. 在任務窗格中，展開網域節點。
5. 找到並開啟（按一下滑鼠右鍵）您要修改之 OU 的內容選單，然後選擇屬性。
6. 在 OU 屬性窗格中，選取安全性索引標籤。
7. 在安全索引標籤中，選取進階。然後選取新增。
8. 在許可項目頁面上，選擇選取委託人，然後輸入 Amazon FSx 服務帳戶或群組的名稱。對於套用至：，選擇此物件和所有子系電腦。請確定已選取下列項目：
   - 修改許可
   - 建立電腦物件
   - 刪除電腦物件
9. 選取套用，然後選取確定。
10. 關閉 Active Directory 使用者和電腦 MMC 嵌入。

驗證您的 Active Directory 組態

建立已加入 Active Directory 的 FSx for Windows File Server 檔案系統之前，建議您使用 Amazon FSx Active Directory 驗證工具來驗證 Active Directory 組態。請注意，需要傳出網際網路連線才能成功驗證 Active Directory 組態。

驗證您的 Active Directory 組態

1. 在相同子網路中啟動 Amazon EC2 Windows 執行個體，並使用您用於 FSx for Windows File Server 檔案系統的相同 Amazon VPC 安全群組。確保您的 EC2 執行個體具有必要的 `AmazonEC2ReadOnlyAccess` IAM 許可。您可以使用 IAM 政策模擬器來驗證 EC2 執行個體角色許可。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 政策模擬器測試 IAM 政策。
2. 將 EC2 Windows 執行個體加入 Active Directory。如需詳細資訊，請參閱《 AWS Directory Service 管理指南》中的手動加入 Windows 執行個體。
3. 連線至 EC2 執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的連線至 Windows 執行個體。
4. 在 EC2 執行個體上開啟 Windows PowerShell 視窗（使用以管理員身分執行)。

若要測試是否已安裝 Windows PowerShell 所需的 Active Directory 模組，請使用下列測試命令。

```
PS C:\> Import-Module ActiveDirectory
```

如果上述 傳回錯誤，請使用下列命令進行安裝。

```
PS C:\> Install-WindowsFeature RSAT-AD-PowerShell
```

5. 使用下列命令下載網路驗證工具。

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

6. 使用下列命令展開 zip 檔案。

```
PS C:\> Expand-Archive -Path "AmazonFSxADValidation.zip"
```

7. 將AmazonFSxADValidation模組新增至目前的工作階段。

```
PS C:\> Import-Module .\AmazonFSxADValidation
```

8. 將 替換為下列命令來設定必要的參數：

   - Active Directory 網域名稱 (*DOMAINNAME.COM*：//)
   - 使用下列其中一個選項準備服務帳戶密碼的$Credential物件。
     - 若要以互動方式產生登入資料物件，請使用下列命令。

       ```
       $Credential = Get-Credential
       ```

     - 若要使用 AWS Secrets Manager 資源產生登入資料物件，請使用下列命令。

       ```
       $Secret = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
        $AdminSecret).SecretString
       $Credential = (New-Object PSCredential($Secret.UserName,(ConvertTo-SecureString
        $Secret.Password -AsPlainText -Force)))
       ```

   - DNS 伺服器 IP 地址 (*IP_ADDRESS_1*、*IP_ADDRESS_2*)

- 子網路 ID（適用於您計劃建立 Amazon FSx 檔案系統的子網路）(*SUBNET_1*、*SUBNET_2*，例如 subnet-04431191671ac0d19)。

```
PS C:\>
$FSxADValidationArgs = @{
    # DNS root of ActiveDirectory domain
    DomainDNSRoot = 'DOMAINNAME.COM'

    # IP v4 addresses of DNS servers
    DnsIpAddresses = @('IP_ADDRESS_1', 'IP_ADDRESS_2')

    # Subnet IDs for Amazon FSx file server(s)
    SubnetIds = @('SUBNET_1', 'SUBNET_2')

    Credential = $Credential
}
```

9. （選用）在執行驗證工具之前，遵循隨附README.md檔案中的指示，設定組織單位、委派管理員群組、DomainControllersMaxCount 並啟用服務帳戶許可驗證。

> **Note**
>
> 如果作業系統不是英文，則Domain Admins群組會有不同的名稱。例如，群組在法文作業系統版本Administrateurs du domaine中命名。如果您未指定值，則會使用預設Domain Admins群組名稱，且檔案系統建立失敗。

10. 使用此命令執行驗證工具。

```
PS C:\> $Result = Test-FSxADConfiguration @FSxADValidationArgs
```

11. 以下是成功測試結果的範例。

```
Test 1 - Validate EC2 Subnets ...
...
Test 17 - Validate 'Delete Computer Objects' permission ...

Test computer object amznfsxtestd53f deleted!
...
```

```
SUCCESS - All tests passed! Please proceed to creating an Amazon FSx file system.
 For your convenience, SelfManagedActiveDirectoryConfiguration of result can be
 used directly in CreateFileSystemWindowsConfiguration for New-FSXFileSystem
PS C:\AmazonFSxADValidation> $Result.Failures.Count
0
PS C:\AmazonFSxADValidation> $Result.Warnings.Count
0
```

以下是發生錯誤的測試結果範例。

```
Test 1 - Validate EC2 Subnets ...
...
Test 7 - Validate that provided EC2 Subnets belong to a single AD Site ...

Name          DistinguishedName
     Site
----          -----------------
     ----
10.0.0.0/19   CN=10.0.0.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-
ad,DC=local   CN=SiteB,CN=Sites,CN=Configu...
10.0.128.0/19 CN=10.0.128.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-
ad,DC=local CN=Default-First-Site-Name,C...
10.0.64.0/19  CN=10.0.64.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-
ad,DC=local  CN=SiteB,CN=Sites,CN=Configu...



Best match for EC2 subnet subnet-092f4caca69e360e7 is AD site CN=Default-First-
Site-Name,CN=Sites,CN=Configuration,DC=te
st-ad,DC=local
Best match for EC2 subnet subnet-04431191671ac0d19 is AD site
 CN=SiteB,CN=Sites,CN=Configuration,DC=test-ad,DC=local
WARNING: EC2 subnets subnet-092f4caca69e360e7 subnet-04431191671ac0d19 matched to
 different AD sites! Make sure they
are in a single AD site.
...
9 of 16 tests skipped.
FAILURE - Tests failed. Please see error details below:

Name                          Value
----                          -----
SubnetsInSeparateAdSites      {subnet-04431191671ac0d19, subnet-092f4caca69e360e7}
```

```
Please address all errors and warnings above prior to re-running validation to
 confirm fix.
PS C:\AmazonFSxADValidation> $Result.Failures.Count
1
PS C:\AmazonFSxADValidation> $Result.Failures

Name                           Value
----                           -----
SubnetsInSeparateAdSites       {subnet-04431191671ac0d19, subnet-092f4caca69e360e7}


PS C:\AmazonFSxADValidation> $Result.Warnings.Count
0
```

如果您在執行驗證工具時收到警告或錯誤，請參閱驗證工具套件 (TROUBLESHOOTING.md) 和 中包含的故障診斷指南Amazon FSx 故障診斷。

將 Amazon FSx 檔案系統加入自我管理的 Microsoft Active Directory 網域

當您建立新的 FSx for Windows File Server 檔案系統時，您可以設定 Microsoft Active Directory 整合，使其加入您的自我管理 Microsoft Active Directory 網域。若要執行此作業，請提供 Microsoft Active Directory 的下列資訊：

- 您內部部署 Microsoft Active Directory 目錄的完整網域名稱 (FQDN)。

> **Note**
>
> Amazon FSx 目前不支援單一標籤網域 (SLD) 網域。

- 網域 DNS 伺服器的 IP 地址。
- Amazon FSx 用來將檔案系統加入網域的 Active Directory 服務帳戶的登入資料。您可以提供下列其中一種方式：
  - 選項 1： AWS Secrets Manager 秘密 ARN - 包含 Active Directory 網域上服務帳戶的使用者名稱和密碼的秘密。如需詳細資訊，請參閱使用 存放 Active Directory 登入資料 AWS Secrets Manager。
  - 選項 2：純文字登入資料

- 服務帳戶使用者名稱 – 您現有 Microsoft Active Directory 中服務帳戶的使用者名稱。請勿包含網域字首或尾碼。例如，對於 `EXAMPLE\ADMIN`，僅使用 `ADMIN`。
- 服務帳戶密碼 – 服務帳戶的密碼。

或者，您也可以指定以下內容：

- 網域中您希望 Amazon FSx 檔案系統加入的特定組織單位 (OU)。
- 網域群組的名稱，其成員會獲得 Amazon FSx 檔案系統的管理權限。您提供的網域群組名稱在 Active Directory 中必須是唯一的。

指定此資訊後，Amazon FSx 會使用您提供的服務帳戶，將新的檔案系統加入自我管理的 Active Directory 網域。

> **Important**
>
> 如果您加入檔案系統的 Active Directory 網域使用 Microsoft DNS 做為預設 DNS，Amazon FSx 只會註冊檔案系統的 DNS 記錄。如果您使用第三方 DNS，則在建立檔案系統之後，您將需要手動設定 Amazon FSx 檔案系統的 DNS 項目。如需選擇要用於檔案系統之正確 IP 地址的詳細資訊，請參閱 取得用於手動 DNS 項目的正確檔案系統 IP 地址。

開始之前

請確定您已完成 中先決條件詳述的 使用自我管理的 Microsoft Active Directory。

建立加入自我管理 Active Directory 的 FSx for Windows File Server 檔案系統 （主控台）

1. 在 https://console.aws.amazon.com/fsx/：// 開啟 Amazon FSx 主控台。
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. 選擇 FSx for Windows File Server，然後選擇下一步。Create file system (建立檔案系統) 頁面隨即顯示。
4. 為您的檔案系統提供名稱。您最多可以使用 256 個 Unicode 字母、空格和數字，加上特殊字元 + - = . _ : /
5. 對於儲存容量，請以 GiB 為單位輸入檔案系統的儲存容量。如果您使用的是 SSD 儲存體，請輸入 32–65，536 範圍內的任何整數。如果您使用的是 HDD 儲存，請輸入 2，000–65，536 範圍內的

任何整數。您可以在建立檔案系統之後，隨時視需要增加儲存容量。如需詳細資訊，請參閱管理儲存容量。

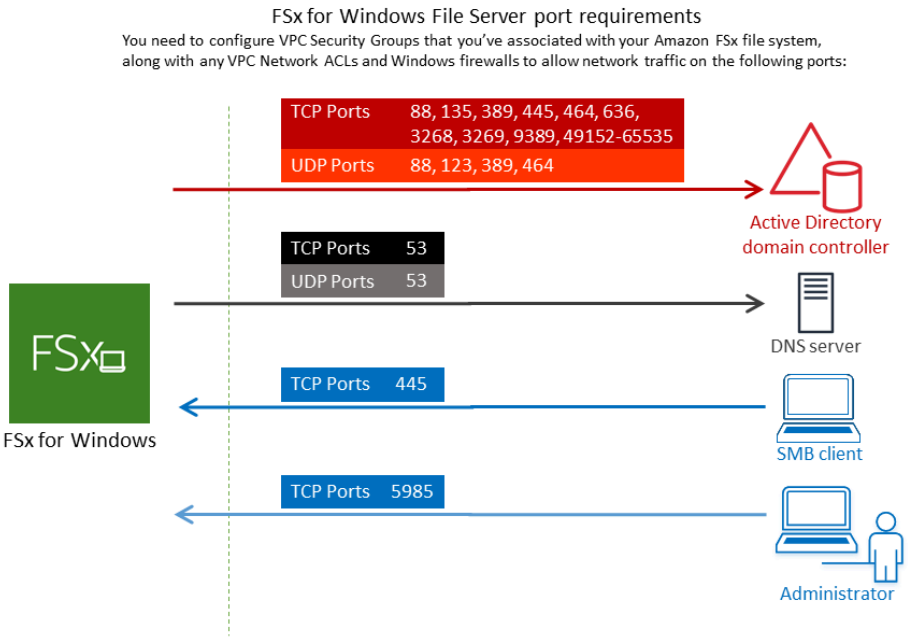
6. 保留 Throughput capacity (輸送容量) 的預設設定。輸送量容量是託管檔案系統的檔案伺服器可以提供資料的持續速度。建議的輸送量容量設定取決於您選擇的儲存容量。如果您需要超過建議的輸送量容量，請選擇指定輸送量容量，然後選擇值。如需詳細資訊，請參閱FSx for Windows File Server 效能。

   您可以在建立檔案系統之後隨時視需要修改輸送量容量。如需詳細資訊，請參閱管理輸送量容量。

7. 選擇您要與檔案系統建立關聯的 VPC。基於本入門練習的目的，請選擇與 Directory Service 目錄和 Amazon EC2 執行個體相同的 VPC。

8. 選擇可用區域和子網路的任何值。

9. 對於 VPC 安全群組，預設 Amazon VPC 的預設安全群組已新增至主控台中的檔案系統。請確定您建立 FSx 檔案系統之子網路的安全群組和 VPC 網路 ACLs（如下圖所示）允許連接埠上的流量。



下表識別每個連接埠的角色。

通訊協定	連接埠	Role
TCP/UDP	53	網域名稱系統 (DNS)
TCP/UDP	88	Kerbe 身分驗證
TCP/UDP	464	變更/設定密碼
TCP/UDP	389	輕量型目錄存取通訊協定 (LDAP

通訊協定	連接埠	Role
UDP	123	網路時間通訊協定 (NTP)
TCP	135	分散式運算環境/端點映射器 (DCE/EPMAP)
TCP	445	目錄服務 SMB 檔案共用

通訊協定	連接埠	Role
TCP	636	透過 TLS/SSL 的輕量型目錄存取通訊協定 (LDAP
TCP	3268	Micros Globa Catalo
TCP	3269	透過 SSL 的 Micros Globa Catalo

通訊協定	連接埠	Role
TCP	5985	WinRM 2.0 (Microsoft Windows 遠端管理)
TCP	9389	Microsoft Active Directory DS Web Service PowerShell
TCP	49152 - 65535	適用於 RPC 的暫時性連接埠

Important

單一可用區 2 和所有多可用區檔案系統部署需要允許 TCP 連接埠 9389 上的傳出流量。

> **Note**
>
> 如果您使用的是 VPC 網路 ACLs，您還必須允許來自 FSx 檔案系統的動態連接埠 ((49152-65535) 上的傳出流量。

- 允許所有流量流向與自我管理 Microsoft Active Directory 網域的 DNS 伺服器和網域控制站相關聯的 IP 地址的傳出規則。如需詳細資訊，請參閱 Microsoft 有關為 Active Directory 通訊設定防火牆的文件。
- 請確定這些流量規則也會在套用至每個 Active Directory 網域控制站、DNS 伺服器、FSx 用戶端和 FSx 管理員的防火牆上鏡像。

> **Note**
>
> 如果您已經定義 Active Directory 網站，則必須確保與 Amazon FSx 檔案系統相關聯的 VPC 中的子網路在 Active Directory 網站中定義，而且 VPC 中的子網路和其他站台中的子網路之間不存在衝突。您可以使用 Active Directory 網站和服務 MMC 嵌入來檢視和變更這些設定。

> **Important**
>
> 雖然 Amazon VPC 安全群組要求僅在啟動網路流量的方向上開啟連接埠，但大多數 Windows 防火牆和 VPC 網路 ACLs 要求雙向開啟連接埠。

10. 針對 Windows 身分驗證，選擇自我管理的 Microsoft Active Directory。
11. 輸入自我管理 Microsoft Active Directory 目錄的完整網域名稱的值。

> **Note**
>
> 網域名稱不得為單一標籤網域 (SLD) 格式。Amazon FSx 目前不支援 SLD 網域。

> **Important**
>
> 對於單一可用區 2 和所有多可用區檔案系統，Active Directory 網域名稱不能超過 47 個字元。

12. 輸入自我管理 Microsoft Active Directory 目錄的組織單位值。

> **Note**
>
> 請確定您提供的服務帳戶具有委派給您在此處指定之 OU 的許可，或如果您未指定預設 OU 的許可。

13. 為自我管理的 Microsoft Active Directory 目錄輸入至少一個且不超過兩個 DNS 伺服器 IP 地址的值。
14. 服務帳戶登入資料 – 選擇如何提供服務帳戶登入資料：

    - 選項 1： AWS Secrets Manager 秘密 ARN - 包含 Active Directory 網域上服務帳戶的使用者名稱和密碼的秘密。如需詳細資訊，請參閱使用 存放 Active Directory 登入資料 AWS Secrets Manager。
    - 選項 2：純文字登入資料
      - 服務帳戶使用者名稱 – 現有 Microsoft Active Directory 中服務帳戶的使用者名稱。請勿包含網域字首或尾碼。例如，對於 `EXAMPLE\ADMIN`，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。

    > **Important**
    >
    > 輸入服務帳戶使用者名稱時，請勿包含網域字首 (`corp.com\ServiceAcct`) 或網域尾碼 (`ServiceAcct@corp.com`)。
    > 輸入服務帳戶使用者名稱 () 時，請勿使用辨別名稱 (DN)`CN=ServiceAcct,OU=example,DC=corp,DC=com`。

15. 對於委派檔案系統管理員群組，指定`Domain Admins`群組或自訂委派檔案系統管理員群組 （如果您已建立）。您指定的 群組應有委派授權，可在您的檔案系統上執行管理任務。如果您未提供值，Amazon FSx 會使用內建`Domain Admins`群組。請注意，Amazon FSx 不支援在內建容器中

擁有 `Delegated file system administrators group`（您指定的`Domain Admins`群組或自訂群組）。

> **Important**
>
> 如果您未提供委派檔案系統管理員群組，根據預設，Amazon FSx 會嘗試在您的 Active Directory 網域中使用內建`Domain Admins`群組。如果此內建群組的名稱已變更，或者您使用不同的群組進行網域管理，則必須在此處提供該群組的名稱。

> **Important**
>
> 提供群組名稱參數時，請勿包含網域字首 (corp.com\FSxAdmins) 或網域尾碼 (FSxAdmins@corp.com)。
> 請勿對群組使用辨別名稱 (DN)。辨別名稱的範例為 CN=FSxAdmins，OU=example，DC=corp，DC=com。

建立加入自我管理 Active Directory 的 FSx for Windows File Server 檔案系統 (AWS CLI)

下列範例會建立 FSx for Windows File Server 檔案系統`SelfManagedActiveDirectoryConfiguration`，並在`us-east-2`可用區域中使用 。

```
aws fsx --region us-east-2 \
create-file-system \
--file-system-type WINDOWS \
--storage-capacity 300 \
--security-group-ids security-group-id \
--subnet-ids subnet-id\
--windows-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",FileSystemAdmini
 \
UserName="FSxService",Password="password", \
   DnsIps=["10.0.1.18"]}',ThroughputCapacity=8
```

> **Important**
>
> 建立檔案系統後，請勿移動 Amazon FSx 在 OU 中建立的電腦物件。這樣做會導致您的檔案系統設定錯誤。

取得用於手動 DNS 項目的正確檔案系統 IP 地址

如果您使用 Microsoft DNS 做為預設 DNS 服務，Amazon FSx 只會註冊檔案系統的 DNS 記錄。如果您使用第三方 DNS，則需要手動設定 Amazon FSx 檔案系統的 DNS 項目。本節說明如何取得正確的檔案系統 IP 地址，以便在您必須手動將檔案系統新增至 DNS 時使用。請注意，建立檔案系統後，在刪除檔案系統之前，其 IP 地址不會變更。

如何取得用於 DNS A 項目的檔案系統 IP 地址

1. 在 https://console.aws.amazon.com/fsx/：// 中，選擇要取得 IP 地址的檔案系統，以顯示檔案系統詳細資訊頁面。
2. 在網路與安全索引標籤中，執行下列其中一項：
   - 對於單一可用區 1 檔案系統：
     - 在子網路面板中，選擇網路界面下方顯示的彈性網路界面，以在 Amazon EC2 主控台中開啟網路界面頁面。
     - 要使用的單一可用區 1 檔案系統的 IP 地址會顯示在主要私有 IPv4 IP 欄中。
   - 對於單一可用區 2 或多可用區檔案系統：
     - 在偏好的子網路面板中，選擇網路界面下方顯示的彈性網路界面，以在 Amazon EC2 主控台中開啟網路界面頁面。
     - 要使用之偏好子網路的 IP 地址會顯示在次要私有 IPv4 IP 欄中。
     - 在 Amazon FSx 待命子網路面板中，選擇網路界面下方顯示的彈性網路界面，以在 Amazon EC2 主控台中開啟網路界面頁面。
     - 要使用的待命子網路 IP 地址會顯示在次要私有 IPv4 IP 欄中。

> **Note**
>
> 如果您需要為單一可用區 2 或多可用區檔案系統設定 Windows 遠端 PowerShell 端點的 DNS 項目，您應該使用主要私有 IPv4 地址做為偏好子網路的彈性網路界面。如需詳細資訊，請參閱使用 Amazon FSx CLI for PowerShell。

更新自我管理 Active Directory 組態

若要協助確保 Amazon FSx 檔案系統的持續、不間斷可用性，您必須在下列任何 Active Directory 屬性變更時更新檔案系統的 Active Directory 組態：

- DNS 伺服器 IP 地址
- 自我管理 Active Directory 的服務帳戶登入資料

當您更新 Amazon FSx 檔案系統的自我管理 Active Directory 組態時，在套用更新時，檔案系統的狀態會從可用切換到更新。確認狀態在套用更新後切換回可用 – 請注意，更新可能需要幾分鐘才能完成。如需詳細資訊，請參閱監控自我管理 Active Directory 更新。

如果更新的自我管理 Active Directory 組態發生問題，檔案系統狀態會切換到設定錯誤。此狀態會在主控台、API 和 CLI 的檔案系統描述旁顯示錯誤訊息和建議的修正動作。採取建議的修正動作後，請確認檔案系統的狀態最終變更為可用。

> **Important**
>
> 如果您使用新的服務帳戶更新檔案系統，請確保新的服務帳戶具有與檔案系統相關聯之現有電腦物件的完整控制許可。

如需自我管理 Active Directory 組態相關問題的疑難排解資訊，請參閱 檔案系統處於設定錯誤狀態。

您可以使用 AWS 管理主控台、Amazon FSx API 或 AWS CLI 來更新檔案系統自我管理 Active Directory 組態的服務帳戶憑證和 DNS 伺服器 IP 地址。您可以隨時使用 AWS 管理主控台、 CLI 和 API 追蹤自我管理 Active Directory 組態更新的進度。如需詳細資訊，請參閱監控自我管理 Active Directory 更新。

更新自我管理 Active Directory 組態（主控台）

1. 在 https://console.aws.amazon.com/fsx/：// 開啟 Amazon FSx 主控台。

2. 導覽至檔案系統，然後選擇您要更新自我管理 Active Directory 組態的 Windows 檔案系統。
3. 在網路與安全索引標籤中，選擇更新 DNS 伺服器 IP 地址或服務帳戶使用者名稱，視您要更新的 Active Directory 屬性而定。
4. 在出現的對話方塊中輸入新的 DNS 伺服器 IP 地址，或新的服務帳戶登入資料（使用者名稱和密碼）或秘密 ARN。您可以使用 AWS Secrets Manager 來存放您的登入資料。如需詳細資訊，請參閱使用 存放 Active Directory 登入資料 AWS Secrets Manager。
5. 選擇更新以啟動 Active Directory 組態更新。

   您可以使用 AWS 管理主控台 或 監控更新進度 AWS CLI。

更新自我管理 Active Directory 組態 (CLI)

- 若要更新 FSx for Windows File Server 檔案系統的自我管理 Active Directory 組態，請使用 AWS CLI 命令 update-file-system。設定下列參數：
  - `--file-system-id` 至您正在更新之檔案系統的 ID。
  - `UserName` 自我管理 Active Directory 服務帳戶的新使用者名稱。
  - `Password` 自我管理 Active Directory 服務帳戶的新密碼。
  - `DomainJoinServiceAccountSecret` 包含 Active Directory 網域上服務帳戶的使用者名稱和密碼的 AWS Secrets Manager 秘密

    > **Note**
    >
    > 您無法同時提供使用者名稱/密碼和網域聯結服務帳戶秘密，以連線至您的 Active Directory。僅提供一組登入資料。

  - `DnsIps` 自我管理 Active Directory DNS 伺服器的 IP 地址。

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 \
  --windows-configuration
 'SelfManagedActiveDirectoryConfiguration={UserName=username,Password=password,\
    DnsIps=[192.0.2.0,192.0.2.24]}'
```

如果更新動作成功，服務會傳回 HTTP 200 回應。回應中的`AdminstrativeActions`物件描述請求及其狀態。

變更 Amazon FSx 服務帳戶

如果您使用新的服務帳戶更新檔案系統，則新的服務帳戶必須具有加入 Active Directory 所需的許可和權限，並具有與檔案系統相關聯之現有電腦物件的完整控制許可。此外，請確定新的服務帳戶是已啟用群組政策設定網域控制器的信任帳戶的一部分：允許電腦帳戶在網域加入期間重複使用。

我們強烈建議使用 Active Directory 群組來管理與服務帳戶相關聯的 Active Directory 許可和組態。

變更 Amazon FSx 的服務帳戶時，請確定服務帳戶具有下列設定：

- 新的服務帳戶（或其成員的 Active Directory 群組）具有與檔案系統相關聯的現有電腦物件的完整控制許可。
- 新的和先前的服務帳戶（或其成員的 Active Directory 群組）是具有網域控制站的信任帳戶（或信任的 Active Directory 群組）的一部分：允許在 Active Directory 中所有網域控制站上啟用網域聯結群組政策設定期間重複使用電腦帳戶。

如果服務帳戶不符合這些要求，可能會發生下列情況：

- 對於單一可用區檔案系統，檔案系統可能會變成 MISCONFIGURED_UNAVAILABLE。
- 對於多可用區域檔案系統，檔案系統可能會變成 MISCONFIGURED，而 RemotePowerShell 端點名稱可能會變更。

設定網域控制站的群組政策

下列 Microsoft 建議程序說明如何使用網域控制站群組政策來設定允許清單政策。

設定網域控制站的允許清單政策

1. 在自我管理 Microsoft Active Directory 中的所有成員電腦和網域控制站上安裝 2023 年 9 月 12 日或更新版本的 Microsoft Windows 更新。
2. 在套用至自我管理 Active Directory 中所有網域控制站的新或現有群組政策中，設定下列設定。
    a. 導覽至電腦組態 > 政策>Windows 設定 > 安全性設定 > 本機政策 > 安全性選項。
    b. 按兩下網域控制器：允許在網域加入期間重複使用電腦帳戶。
    c. 選取定義此政策設定並 <編輯安全性...>。
    d. 使用物件挑選器，將信任的電腦帳戶建立者和擁有者的使用者或群組新增至允許許可。（最佳實務是強烈建議您使用 群組來取得許可。）請勿新增執行網域聯結的使用者帳戶。

> **Warning**
>
> 將政策的成員資格限制為信任的使用者和服務帳戶。請勿將已驗證的使用者、所有人或其他大型群組新增至此政策。反之，請將特定信任的使用者和服務帳戶新增至群組，並將這些群組新增至政策。

3. 等待群組政策重新整理間隔，或在所有網域控制站gpupdate /force上執行。
4. 確認 HKLM\System\CCS\Control\SAM – “ComputerAccountReuseAllowList” 登錄機碼已填入所需的 SDDL。請勿手動編輯登錄檔。
5. 嘗試加入已安裝 2023 年 9 月 12 日或更新版本更新的電腦。確保政策中列出的其中一個帳戶擁有該電腦帳戶。同時確保其登錄檔未啟用 NetJoinLegacyAccountReuse 金鑰 （ 設定為 1)。如果網域聯結失敗，請檢查 **`c:\windows\debug\netsetup.log`**。

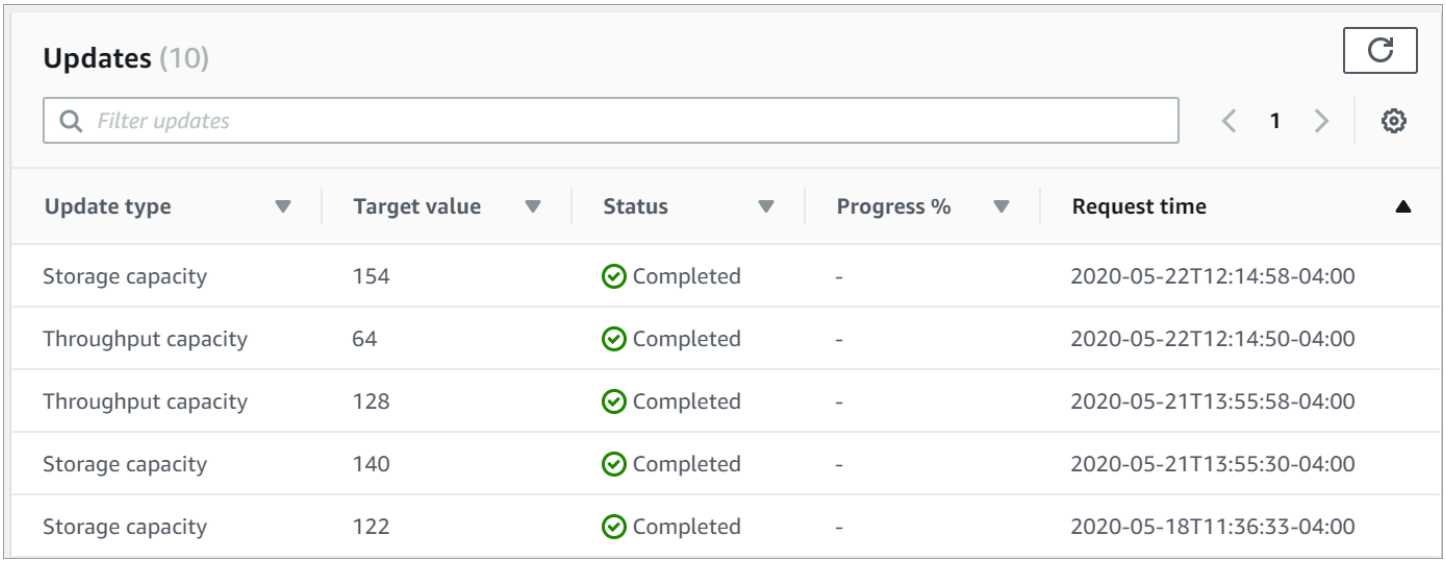
監控自我管理 Active Directory 更新

您可以使用 、 AWS 管理主控台 API 或 監控自我管理 Active Directory 組態更新的進度 AWS CLI，如下列程序所述。

當您更新檔案系統的自我管理 Active Directory 組態時，套用更新時，檔案系統的狀態會從可用切換到更新。更新完成後，狀態會切換回可用。Active Directory 組態更新可能需要幾分鐘的時間才能完成。

在主控台中監控更新

在檔案系統詳細資訊視窗中的更新索引標籤中，您可以檢視每個更新類型的 10 個最近更新。



對於自我管理 Active Directory 更新，您可以檢視下列資訊。

更新類型

支援的類型如下：

- DNS 伺服器 IP 地址
- 服務帳戶登入資料

目標值

要更新檔案系統屬性的所需值。對於服務帳戶登入資料更新，僅顯示使用者名稱，服務帳戶密碼絕不會包含在此欄位中。

狀態

更新的目前狀態。對於自我管理 Active Directory 更新，可能的值如下所示：

- 待定 – Amazon FSx 已收到更新請求，但尚未開始處理。
- 進行中 – Amazon FSx 正在處理更新請求。
- 已完成 – 檔案系統更新已成功完成。
- 失敗 – 檔案系統更新失敗。選擇問號 (?) 以查看失敗的詳細資訊。

進度 %

將檔案系統更新進度顯示為完成百分比。

請求時間

Amazon FSx 收到更新動作請求的時間。

使用 AWS CLI 和 API 監控更新

您可以使用 describe-file-systems AWS CLI 命令和 DescribeFileSystems API 動作，檢視和監控進行中的檔案系統更新請求。`AdministrativeActions` 陣列會列出每個管理動作類型的 10 個最近更新動作。

下列範例顯示 CLI describe-file-systems 命令回應的摘錄。輸出會顯示兩個自我管理 Active Directory 檔案系統更新。

```
{
    "OwnerId": "111122223333",
    .
```

```
            .
            .
            "StorageCapacity": 1000,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "RequestTime": 1581694766.757,
                    "Status": "PENDING",
                    "TargetFileSystemValues": {
                        "WindowsConfiguration": {
                            "SelfManagedActiveDirectoryConfiguration": {
                                "UserName": "serviceUser",
                            }
                        }
                    }
                },
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "RequestTime": 1619032957.759,
                    "Status": "FAILED",
                    "TargetFileSystemValues": {
                        "WindowsConfiguration": {
                            "SelfManagedActiveDirectoryConfiguration": {
                            "DnsIps": [
                                    "10.0.138.161"
                                ]
                            }
                        }
                    },
                    "FailureDetails": {
                        "Message": "Failure details message."
                    }
                }
            ],
        .
        .
        .
```

FSx for Windows File Server 效能

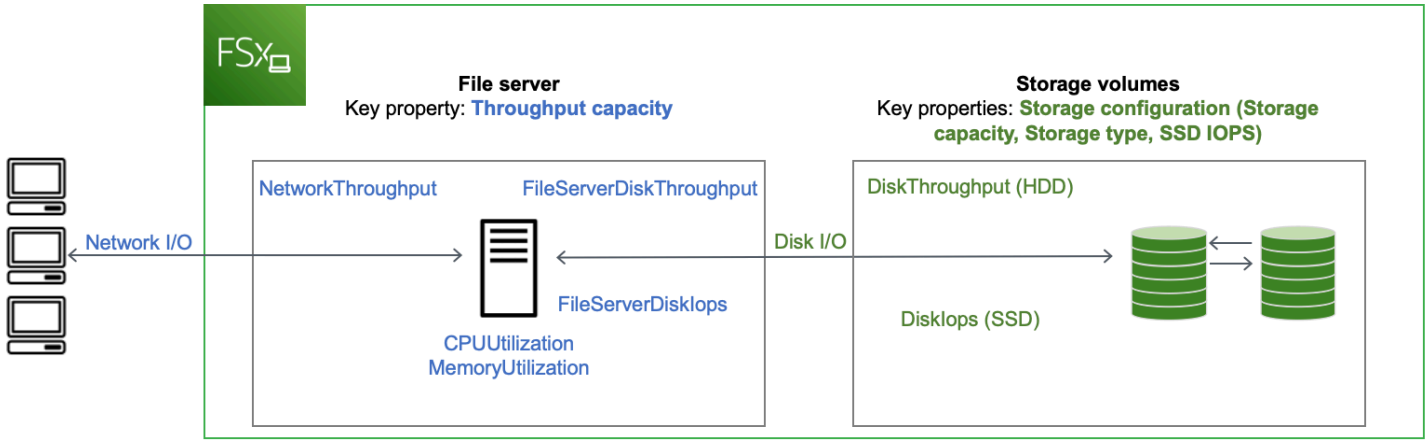
FSx for Windows File Server 提供檔案系統組態選項，以滿足各種效能需求。以下是 Amazon FSx 檔案系統效能的概觀，其中討論了可用的效能組態選項和有用的效能秘訣。

主題

檔案系統效能

每個 FSx for Windows File Server 檔案系統都包含一個 Windows 檔案伺服器，用戶端會與之通訊，以及一組連接到檔案伺服器的儲存磁碟區或磁碟。每個檔案伺服器都使用快速的記憶體內快取，來增強最常存取資料的效能。

下圖說明如何從 FSx for Windows File Server 檔案系統存取資料。



當用戶端存取儲存在記憶體內快取中的資料時，資料會直接做為網路 I/O 提供給請求用戶端。 檔案伺服器不需要從 讀取或寫入磁碟。此資料存取的效能取決於網路 I/O 限制和記憶體內快取的大小。

當用戶端存取不在快取中的資料時，檔案伺服器會從磁碟讀取或寫入磁碟做為磁碟 I/O。 然後，資料會從檔案伺服器以網路 I/O 的形式提供給用戶端。 此資料存取的效能取決於網路 I/O 限制和磁碟 I/O 限制。

網路 I/O 效能和檔案伺服器記憶體內快取取決於檔案系統的輸送量容量。磁碟 I/O 效能取決於輸送量容量和儲存組態的組合。檔案系統可達到的最大磁碟 I/O 效能，包含磁碟輸送量和磁碟 IOPS 層級，其較低者為：

- 檔案伺服器提供的磁碟 I/O 效能等級，根據您為檔案系統選取的輸送量容量而定。
- 儲存組態提供的磁碟 I/O 效能等級 （您為檔案系統選取的儲存容量、儲存類型和 SSD IOPS 等級）。

其他效能考量事項

檔案系統效能通常以其延遲、輸送量和每秒 I/O 操作 (IOPS) 來測量。

Latency (延遲)

FSx for Windows File Server 檔案伺服器採用快速記憶體內快取，以達成主動存取資料的一致毫秒內延遲。對於不在記憶體內快取中的資料，也就是說，對於需要在基礎儲存磁碟區上執行 I/O 提供的檔案操作，Amazon FSx 提供固態硬碟 (SSD) 儲存的低於毫秒的檔案操作延遲，以及硬碟 (HDD) 儲存的單一位數毫秒延遲。

輸送量和 IOPS

Amazon FSx 檔案系統在所有提供 Amazon FSx AWS 區域 的地區提供高達 2 GBps 和 80，000 IOPS，在美國東部 （維吉尼亞北部）、美國西部 （奧勒岡）、美國東部 （俄亥俄）、歐洲 （愛爾蘭）、亞太區域 （東京） 和亞太區域 （新加坡） 提供 12 GBps 的輸送量和 400，000 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輸送量容量、儲存容量和儲存類型，以及工作負載的性質，包括作用中工作集的大小。

單一用戶端效能

使用 Amazon FSx，您可以從存取檔案系統的單一用戶端，取得檔案系統的完整輸送量和 IOPS 層級。Amazon FSx 支援 SMB 多頻道。此功能可讓單一用戶端存取您的檔案系統，提供高達多個 GBps 的輸送量和數十萬個 IOPS。SMB 多頻道同時使用用戶端和伺服器之間的多個網路連線，以彙總網路頻寬以實現最大使用率。雖然 Windows 支援的 SMB 連線數有理論限制，但此限制以百萬為單位，而且實際上您可以擁有無限數量的 SMB 連線。

爆量效能

檔案型工作負載通常爆量，特徵是短暫、密集的高 I/O 期間，以及爆量之間的大量閒置時間。為了支援尖峰工作負載，除了檔案系統可以維持的基準速度之外，Amazon FSx 還為網路 I/O 和磁碟 I/O 操作提供一段時間內爆增至更高速度的功能。Amazon FSx 使用 I/O 額度機制，根據平均使用率來配置輸送量和 IOPS — 檔案系統會在輸送量和 IOPS 使用量低於其基準限制時累積額度，並在執行 I/O 操作時使用這些額度。

輸送量容量對效能的影響

輸送量容量決定下列類別的檔案系統效能：

- 網路 I/O – 檔案伺服器可以提供檔案資料給用戶端存取檔案資料的速度。
- 檔案伺服器 CPU 和記憶體 – 可用於提供檔案資料和執行背景活動的資源，例如重複資料刪除和陰影複製。
- 磁碟 I/O – 檔案伺服器可在檔案伺服器與儲存磁碟區之間支援 I/O 的速度。

下表提供有關每個佈建輸送量組態時可驅動之網路 I/O （輸送量和 IOPS) 和磁碟 I/O （輸送量和 IOPS) 的最大層級的詳細資訊，以及可用於快取和支援背景活動的記憶體數量，例如重複資料刪除和陰影複製。雖然當您使用 Amazon FSx API 或 CLI 時，您可以選擇每秒低於 32 MB (MBps) 的輸送量容量，但請記住，這些層級適用於測試和開發工作負載，而不是生產工作負載。

> **Note**
>
> 請注意，僅在下列區域支援 4，608 MBps 或更高的輸送量容量：美國東部 （維吉尼亞北部）、美國西部 （奧勒岡）、美國東部 （俄亥俄）、歐洲 （愛爾蘭）、亞太區域 （東京） 和亞太區域 （新加坡）。

網路 I/O 和記憶體

FSx 輸送量 (MBps)	網路輸送量 (MBps)		網路 IOPS	記憶體 (GB)
	基準	爆量 （每天幾分鐘）		

FSx 輸送量 (MBps)	網路輸送量 (MBps)		網路 IOPS	記憶體 (GB)
32	32	600	數千	4
64	64	600	數萬	8
128	150	1,250		8
256	300	1,250	數萬	16
512	600	1,250		32
1,024	1,500	–		72
2,048	3,125	–		144
4，608	9,375	–	數百萬	192
6,144	12,500	–		256
9,216	18,750	–		384
12,288	21,250	–		512

磁碟輸入/輸出

FSx 輸送量 (MBps)	磁碟輸送量 (MBps)		磁碟 IOPS	
	基準	爆量（每天 30 分鐘）	基準	爆量（每天 30 分鐘）
32	32	260	2K	12K
64	64	350	4K	16K
128	128	600	6K	20K
256	256	600	10K	20K

FSx 輸送量 (MBps)	磁碟輸送量 (MBps)		磁碟 IOPS	
512	512	–	20K	–
1,024	1,024	–	40K	–
2,048	2,048	–	80K	–
4，608	4,608	–	150K	–
6,144	6,144	–	200K	–
9,216	9,216[1]	–	300K[1]	–
12,288	12,288[1]	–	400K[1]	–

Note

[1]如果您的多可用區域檔案系統輸送量容量為 9，216 或 12，288 MBps，則僅限寫入流量的效能限制為 9，000 MBps 和 262，500 IOPS。否則，對於所有多可用區域檔案系統的讀取流量、所有單一可用區域檔案系統的讀取和寫入流量，以及所有其他輸送量容量層級，您的檔案系統將支援資料表中顯示的效能限制。

選擇適當的輸送量容量層級

當您使用 Amazon Web Services 管理主控台建立檔案系統時，Amazon FSx 會根據您設定的儲存容量，自動為您的檔案系統挑選建議的輸送量容量層級。雖然建議的輸送量容量應足以應付大多數工作負載，但您可以選擇覆寫建議，並設定特定數量的輸送量容量，以滿足工作負載的需求。例如，如果您的工作負載需要驅動 1 GBps 的流量到檔案系統，您應該選取至少 1，024 MBps 的輸送量容量。下表根據佈建的儲存容量量，提供檔案系統建議的最低輸送量容量層級。

SSD 儲存容量 (GiB)	HDD 儲存容量 (GiB)	最低建議輸送量 (MBps)
高達 640	高達 3，200	32
641—1，280	3201—6，400	64

SSD 儲存容量 (GiB)	HDD 儲存容量 (GiB)	最低建議輸送量 (MBps)
1281—2，560	6，401—12，800	128
2，561—5，120	12，801—25，600	256
5，121—10，240	25，601—51，200	512
10，241—20，480	>51，200	1,024
>20，480	NA	2,048

您也應該考慮計劃在檔案系統上啟用的功能，以決定要設定的輸送量層級。例如，啟用 Shadow Copies 可能需要您將輸送量容量提高到預期工作負載的三倍，以確保檔案伺服器可以使用可用的 I/O 效能容量來維護陰影複本。如果您啟用了重複資料刪除功能，您應該判斷與檔案系統輸送量容量相關聯的記憶體數量，並確保此記憶體數量足以滿足資料大小。

您可以在建立傳輸量之後，隨時調整容量。如需詳細資訊，請參閱管理輸送量容量。

您可以檢視 Amazon FSx 主控台的監控與效能 > 效能索引標籤，來監控工作負載對檔案伺服器效能資源的使用率，並取得要選取之輸送量容量的建議。建議您在生產前環境中進行測試，以確保您選取的組態符合工作負載的效能需求。對於多可用區域檔案系統，我們也建議測試檔案系統維護期間發生容錯移轉程序的影響、輸送量容量變更，以及意外的服務中斷對工作負載的影響，並確保您已佈建足夠的輸送量容量，以防止在這些事件期間造成效能影響。如需詳細資訊，請參閱存取檔案系統指標。

儲存體組態對效能的影響

檔案系統的儲存容量、儲存類型和 SSD IOPS 層級都會影響檔案系統的磁碟 I/O 效能。您可以設定這些資源，為您的工作負載提供所需的效能等級。

您可以隨時增加儲存容量和擴展 SSD IOPS。如需詳細資訊，請參閱 管理儲存容量 和 管理 SSD IOPS。您也可以將檔案系統從 HDD 儲存類型升級至 SSD 儲存類型。如需詳細資訊，請參閱管理檔案系統的儲存類型。

檔案系統提供下列預設層級的磁碟輸送量和 IOPS：

儲存體類型	磁碟輸送量 （每 TiB 儲存體的 MBps)	磁碟 IOPS （每個 TiB 的儲存體）
SSD	750	3，000[1]
HDD	12 個基準；80 次爆量 （每個檔案系統最多 1 GBps)	12 個基準；80 次爆量

> **Note**
>
> [1]對於具有 SSD 儲存類型的檔案系統，您可以佈建額外的 IOPS，每個 GiB 儲存體最大比率為 500 IOPS，每個檔案系統最大比率為 400，000 IOPS。

HDD 爆量效能

對於 HDD 儲存磁碟區，Amazon FSx 使用爆量儲存貯體模型來提供效能。磁碟區大小決定您磁碟區的基準輸送量，這是磁碟區累積輸送量額度的比率。磁碟區大小也決定您磁碟區的爆量輸送量，這是有輸送量可用時您能消耗的比率。磁碟區愈大，基準和爆量輸送量就愈高。您磁碟區擁有的額度愈多，它可在爆量層級驅動 I/O 的時間就愈長。

HDD 儲存磁碟區的可用輸送量以下列公式表示：

```
(Volume size) × (Credit accumulation rate per TiB) = Throughput
```

對於 1-TiB HDD 磁碟區，爆量輸送量限制為 80 MiBps，儲存貯體會以 12 MiBps 的額度填滿，並且可以保留高達 1 TiB 的額度。

HDD 儲存磁碟區可能會遇到顯著的效能變化，具體取決於工作負載。IOPS 或輸送量突然暴增可能會導致磁碟效能降低。此DiskThroughputBalance指標提供磁碟輸送量和磁碟 IOPS 使用率爆量額度餘額的相關資訊。例如，如果您的工作負載超過基準 HDD IOPS 限制 （每 TiB 儲存體 12 IOPS)，磁碟 IOPS 使用率 (HDD) 將超過 100%，並導致耗盡爆量額度餘額，您可以在 DiskThroughputBalance 指標中看到。為了讓您的工作負載繼續驅動高水準的 I/O，您可能需要執行下列其中一項操作：

- 降低工作負載的輸入/輸出需求，以補充爆量額度餘額。
- 增加檔案系統的儲存容量，以提供較高基準層級的磁碟 IOPS。

- 升級檔案系統以使用 SSD 儲存體，可提供更高基準層級的磁碟 IOPS，以更符合您工作負載的需求。

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。

設定 2 TiB 的 HDD 儲存容量和 32 MBps 的輸送量的檔案系統具有下列輸送量層級：

- 網路輸送量 – 32 MBps 基準和 600 MBps 爆量（請參閱輸送量資料表）
- 磁碟輸送量 – 基準 24 MBps 和高載 160 MBps，其值較低：
  - 檔案伺服器支援的 32 MBps 基準和 260 MBps 高載磁碟輸送量層級，以檔案系統的輸送量容量為基礎
  - 儲存磁碟區支援的 24 MBps 基準（每 TB 12 MBps * 2 TiB) 和 160 MBps 爆量（每 TiB 80 MBps * 2 TiB) 磁碟輸送量層級，以儲存類型和容量為基礎

因此，您存取檔案系統的工作負載將能夠針對在檔案伺服器記憶體內快取中主動存取的資料執行的檔案操作，驅動高達 32 MBps 的基準和 600 MBps 的爆量輸送量，以及針對因快取遺失而需要一路流向磁碟的檔案操作，則驅動高達 24 MBps 的基準和 160 MBps 的爆量輸送量。

使用 CloudWatch 指標測量效能

您可以使用 Amazon CloudWatch 來測量和監控檔案系統的輸送量和 IOPS。如需詳細資訊，請參閱使用 Amazon CloudWatch 監控。

對檔案系統效能問題進行故障診斷

FSx for Windows File Server 檔案系統的效能取決於幾個因素，包括您驅動到檔案系統的流量、如何佈建檔案系統，以及已啟用的功能所使用的資源，例如資料重複或影子副本。如需了解檔案系統效能的詳細資訊，請參閱FSx for Windows File Server 效能。

主題

- 如何判斷檔案系統的輸送量和 IOPS 限制？
- 網路 I/O 和磁碟 I/O 之間的差異是什麼？ 為什麼我的網路 I/O 與磁碟 I/O 不同？
- 為什麼我的 CPU 或記憶體用量很高，即使我的網路 I/O 很低？
- 什麼是爆量？ 我的檔案系統使用多少爆量？ 當爆量額度用完時會發生什麼情況？

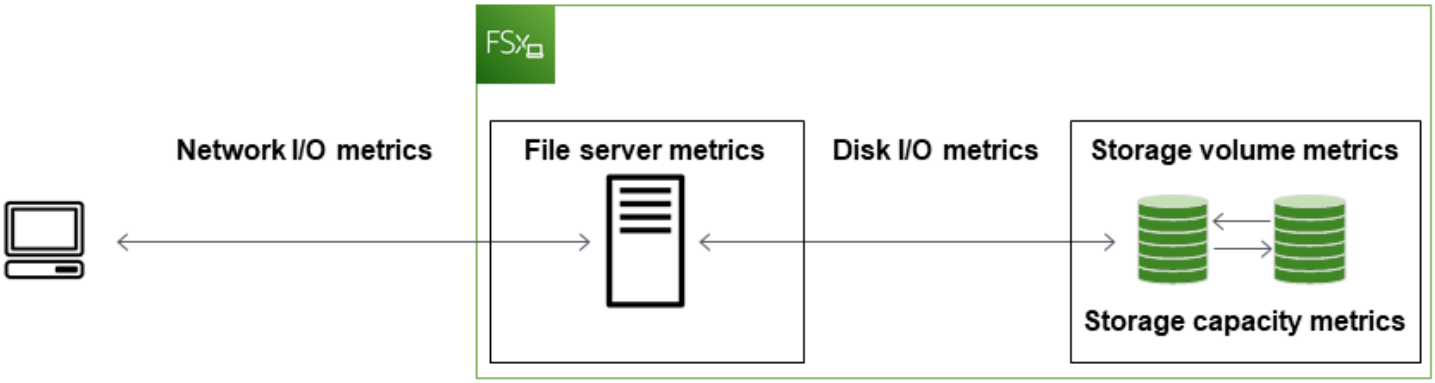
- 我在監控與效能頁面上看到警告 – 我是否需要變更檔案系統的組態？
- 我的指標暫時遺失，我應該擔心嗎？

如何判斷檔案系統的輸送量和 IOPS 限制？

若要檢視檔案系統的輸送量和 IOPS 限制，請參閱根據佈建輸送量容量量顯示效能層級的資料表。

網路 I/O 和磁碟 I/O 之間的差異是什麼？ 為什麼我的網路 I/O 與磁碟 I/O 不同？

Amazon FSx 檔案系統包含一或多個檔案伺服器，可透過網路將資料提供給存取檔案系統的用戶端。這是網路 I/O。 檔案伺服器具有快速的記憶體內快取，可增強最常存取資料的效能。檔案伺服器也會將流量驅動到託管檔案系統資料的儲存磁碟區。這是磁碟 I/O。 下圖說明 Amazon FSx 檔案系統的網路和磁碟 I/O。



如需詳細資訊，請參閱使用 Amazon CloudWatch 監控。

為什麼我的 CPU 或記憶體用量很高，即使我的網路 I/O 很低？

檔案伺服器 CPU 和記憶體用量不僅取決於您驅動的網路流量，還取決於您在檔案系統上啟用的功能。如何設定和排程這些功能可能會影響 CPU 和記憶體使用率。

進行中的重複資料刪除任務可能會耗用記憶體。您可以修改重複資料刪除任務的組態，以減少記憶體需求。例如，您可以限制最佳化以在特定檔案類型或資料夾上執行，或設定最佳化的最小檔案大小和期限。我們也建議您在檔案系統負載最少時，設定重複資料刪除任務在閒置期間執行。如需詳細資訊，請參閱使用重複資料刪除來降低儲存成本。

如果您已啟用以存取為基礎的列舉，當您的最終使用者檢視或列出檔案共用，或在儲存體擴展任務的最佳化階段期間，您可能會看到高 CPU 使用率。如需詳細資訊，請參閱 Microsoft Storage 文件中的在命名空間上啟用存取型列舉。

什麼是爆量？ 我的檔案系統使用多少爆量？ 當爆量額度用完時會發生什麼情況？

檔案型工作負載通常爆量，特徵是短暫、密集的高 I/O 時段，以及爆量之間的閒置時間。為了支援這些類型的工作負載，除了檔案系統可以維持的基準速度之外，Amazon FSx 還為網路 I/O 和磁碟 I/O 操作提供一段時間內爆增至更高速度的功能。

Amazon FSx 使用 I/O 額度機制根據平均使用率來配置輸送量和 IOPS — 檔案系統會在輸送量和 IOPS 使用量低於其基準限制時累積額度，並在需要時使用這些額度爆量超過基準限制（最高爆量限制）。如需檔案系統爆量限制和持續時間的詳細資訊，請參閱FSx for Windows File Server 效能。

我在監控與效能頁面上看到警告 – 我是否需要變更檔案系統的組態？

監控與效能頁面包含警告，指出最近的工作負載需求何時接近或超過您設定檔案系統的方式所決定的資源限制。這不一定表示您需要變更組態，但如果您不採取建議的動作，您的檔案系統可能未針對工作負載佈建不足。

如果造成警告的工作負載是非典型的，而且您預期它不會繼續，則不採取任何動作並密切監控您的使用率可能很安全。不過，如果造成警告的工作負載是典型的，而且您預期它會持續，甚至會增強，我們建議遵循建議的動作來提高檔案伺服器效能（透過增加輸送量容量）或提高儲存磁碟區效能（透過增加儲存容量，或從 HDD 切換到 SSD 儲存）。

> **Note**
>
> 某些檔案系統事件可能會消耗磁碟 I/O 效能資源，並可能觸發效能警告。例如：
>
> - 儲存容量擴展的最佳化階段可以產生增加的磁碟輸送量，如 中所述 儲存容量增加，且檔案系統效能
> - 對於多可用區域檔案系統，輸送量容量擴展、硬體替換或可用區域中斷等事件會導致自動容錯移轉和容錯回復事件。在此期間發生的任何資料變更都需要在主要和次要檔案伺服器之間同步，而 Windows Server 會執行可以取用磁碟 I/O 資源的資料同步任務。如需詳細資訊，請參閱管理輸送量容量。

我的指標暫時遺失，我應該擔心嗎？

在檔案系統維護、基礎設施元件替換以及可用區域無法使用時，單一可用區域檔案系統將無法使用。在此期間，指標將無法使用。

在異地同步備份部署中，Amazon FSx 會自動在不同的可用區域中佈建和維護待命檔案伺服器。如果有檔案系統維護或意外的服務中斷，Amazon FSx 會自動容錯移轉至次要檔案伺服器，讓您繼續存取資料，無需手動介入。在檔案系統容錯移轉和回復失敗的短暫期間內，指標可能會暫時無法使用。

管理 FSx for Windows 檔案系統

Amazon FSx 提供各種管理功能，可協助您輕鬆管理和擴展 Amazon FSx for Windows File Server 檔案系統，以滿足不斷變化的工作負載和使用者需求，以及您的組織法規和合規需求。以下是您可以使用 AWS CLI 和 API AWS 管理主控台、在 PowerShell 上進行遠端管理的 Amazon FSx CLI，以及原生 Microsoft Windows Server 圖形界面來管理的一些檔案系統組態清單。

- 儲存容量
- 儲存體類型
- SSD IOPS
- 輸送容量
- DNS 別名
- 重複資料刪除
- 陰影副本
- 儲存配額
- 檔案存取稽核
- 檔案共享

下列各節提供您可使用的檔案系統管理功能和設定的相關資訊。我們已納入指引，協助您判斷哪些選項最適合您的情況，以及適用的最佳實務。

主題

- 管理 FSx for Windows File Server 上的儲存
- 使用 DFS 命名空間
- 管理輸送量容量
- 管理網路類型
- 標記 Amazon FSx 資源
- 使用 更新檔案系統 AWS CLI

Amazon FSx 檔案系統狀態

您可以使用 Amazon FSx 主控台、 AWS CLI 命令 describe-file-systems 或 API 操作 DescribeFileSystems 來檢視 Amazon FSx 檔案系統的狀態。

檔案系統狀態	Description
AVAILABLE	檔案系統狀態良好，可存取和使用。
CREATING	Amazon FSx 正在建立新的檔案系統。
DELETING	Amazon FSx 正在刪除現有的檔案系統。
UPDATING	檔案系統正在進行客戶起始的更新。
MISCONFIGURED	由於 Active Directory 環境的變更，檔案系統處於受損狀態。您的檔案系統目前無法使用，或有失去可用性的風險，而且備份可能無法成功。如需還原可用性的資訊，請參閱 檔案系統處於設定錯誤狀態。
MISCONFIGURED_UNAVAILABLE	由於 Active Directory 環境中的變更，檔案系統目前無法使用。如需還原可用性的資訊，請參閱 檔案系統處於設定錯誤狀態。
失敗	• 建立新的檔案系統時，Amazon FSx 無法建立新的檔案系統。 • 檔案系統無法使用。 • 檔案系統失敗，Amazon FSx 無法復原它。

檔案系統狀態	Description
	• Amazon FSx 無法建立備份。

使用 Amazon FSx CLI for PowerShell

本章說明如何在 PowerShell 上存取 Amazon FSx CLI 進行遠端管理，以執行 FSx for Windows 檔案系統的檔案系統管理任務。您也可以使用 Microsoft Windows 原生圖形使用者介面 (GUI) 來執行一些管理任務。

PowerShell 上用於遠端管理的 Amazon FSx CLI 可為檔案系統管理員群組中的使用者啟用檔案系統管理。若要在 FSx for Windows File Server 檔案系統上啟動遠端 PowerShell 工作階段，您必須先符合下列先決條件：

- 能夠連線至與 FSx for Windows File Server 檔案系統具有網路連線能力的 Windows 運算執行個體。
- 以檔案系統管理員群組的成員身分登入 Windows 運算執行個體。如果您使用的是 AWS Managed Microsoft AD，即AWS 委派的 FSx 管理員群組。如果您使用的是自我管理的 Microsoft Active Directory，即您在建立檔案系統時為管理指定的網域管理員群組或自訂群組。如需詳細資訊，請參閱使用自我管理 Active Directory 時的最佳實務。
- 檔案系統的 VPC 安全群組傳入規則允許連接埠 5985 上的流量。

PowerShell 上用於遠端管理的 Amazon FSx CLI 使用以下安全功能：

- 使用 Kerberos 身分驗證來驗證使用者憑證。
- 連線用戶端和檔案系統之間的管理工作階段通訊會使用 Kerberos 加密。

您有兩個選項可在 Amazon FSx 檔案系統上執行遠端管理 CLI 命令：

- 您可以建立長時間執行的遠端 PowerShell 工作階段，並在工作階段內執行命令。
- 您可以使用 `Invoke-Command`執行單一命令或單一命令區塊，而無需建立長時間執行的遠端 PowerShell 工作階段。

如果您想要將變數設定為參數並將其傳遞至遠端管理命令，則需要使用 `Invoke-Command`。

> **Note**
>
> 對於多可用區域檔案系統，您只能在檔案系統使用其偏好的檔案伺服器時，使用 Amazon FSx CLI for Remote Management。如需詳細資訊，請參閱可用性和耐久性：單一可用區和多可用區檔案系統。

您需要使用檔案系統的 Windows Remote PowerShell 端點來存取遠端 PowerShell。遠端管理端點的格式為 `amznfsxctlyaa1k.`*`ActiveDirectory-DNS-name`*，例如 `amznfsxctlyaa1k.corp.example.com`。您可以使用 Network & Security 索引標籤 AWS 管理主控台 上檔案系統詳細資訊頁面中的 來尋找端點名稱。使用 AWS CLI `describe-file-systems`命令來檢視回應中傳回的 `RemoteAdministrationEndpoint` 屬性。

您可以使用 `Get-Command` cmdlet 擷取 PowerShell 中可用 cmdlet、函數和別名的相關資訊。如需詳細資訊，請參閱 Microsoft Get-Command 文件。

您也可以使用 `Invoke-Command` cmdlet，在檔案系統上使用下列語法，在 PowerShell 命令上執行 Amazon FSx CLI 進行遠端管理 CLI：

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName
 amznfsxctlyaa1k.corp.example.com -ConfigurationName FSxRemoteAdmin -scriptblock { fsx-
command}
```

如需如何在 FSx for Windows File Server 檔案系統上啟動長期遠端 PowerShell 工作階段的說明，請參閱 啟動 Amazon FSx 遠端 PowerShell 工作階段

啟動 Amazon FSx 遠端 PowerShell 工作階段

本主題提供在 FSx for Windows File Server 檔案伺服器上啟動長期遠端 PowerShell 工作階段的說明。

在檔案系統上啟動遠端 PowerShell 工作階段

1. 以建立檔案系統時所選擇的委派 FSx 管理員群組成員身分，連接至具有檔案系統網路連線能力的運算執行個體。
2. 在運算執行個體上開啟 Windows PowerShell 視窗。
3. 在 PowerShell 中，輸入下列命令，在您的 Amazon FSx 檔案系統上開啟長期遠端工作階段。*`Remote-PowerShell-Endpoint`* 將 取代為您要管理的檔案系統的 Windows Remote PowerShell 端點。使用 `FsxRemoteAdmin`做為工作階段組態名稱。

```
PS C:\Users\delegateadmin> enter-pssession -ComputerName Remote-PowerShell-Endpoint
 -ConfigurationName FsxRemoteAdmin
[fs-0123456789abcdef0]: PS>
```

如果您的執行個體不屬於 Amazon FSx Active Directory 網域，系統會提示您在快顯視窗中輸入使用者登入資料。輸入 FSx 管理員群組成員的使用者憑證。如果您的執行個體已加入網域，將不會要求您提供登入資料。

> **Important**
>
> 如果您使用自我管理的 Active Directory 組態，並在沒有適當 Active Directory 群組政策設定的情況下變更服務帳戶，Windows Remote PowerShell 端點可能會變更。如需詳細資訊，請參閱 變更 Amazon FSx 服務帳戶 以取得詳細資訊。

使用 Amazon FSx CLI 在 PowerShell 上進行遠端管理的一次性檔案系統設定任務

使用下列 Amazon FSx CLI for Remote Management on PowerShell 命令，依照我們的最佳實務快速實作檔案系統管理任務。

管理儲存體耗用量

使用下列命令來管理您的檔案系統儲存體使用量。

- 若要使用預設排程開啟重複資料刪除，請執行下列命令。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Enable-FsxDedup }
```

或者，使用下列命令，在建立檔案後立即取得檔案上的重複資料刪除操作，而不需要任何檔案最短存留期。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FSxDedupConfiguration -MinimumFileAgeDays 0 }
```

如需詳細資訊，請參閱使用重複資料刪除來降低儲存成本。

- 使用以下命令在「追蹤」模式中開啟使用者儲存配額，這僅用於報告目的，而非強制執行。

```
$QuotaLimit = Quota limit in bytes
$QuotaWarningLimit = Quota warning threshold in bytes
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Enable-FSxUserQuotas -Track -DefaultLimit
 $Using:QuotaLimit -DefaultWarningLimit $Using:QuotaWarningLimit }
```

如需詳細資訊，請參閱管理儲存配額。

開啟陰影副本，讓最終使用者能夠將檔案和資料夾復原至先前的版本

使用預設排程（工作日上午 7 點和中午 12 點）開啟陰影複本，如下所示。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxShadowStorage -Default }

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxShadowCopySchedule -Default -Confirm:$False}
```

如需詳細資訊，請參閱設定陰影複本以使用預設儲存體和排程。

強制執行傳輸中的加密

下列命令會對連線至檔案系統的用戶端強制執行加密。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxSmbServerConfiguration -EncryptData $True -
RejectUnencryptedAccess $True -Confirm:$False}
```

您可以關閉所有開啟的工作階段，並強制目前連線的用戶端使用加密重新連線。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Close-FSxSmbSession -Confirm:$False}
```

如需詳細資訊，請參閱管理傳輸中的加密及使用者工作階段和開啟的檔案。

對 PowerShell 上 Amazon FSx CLI 的存取進行故障診斷

有許多潛在原因導致 無法使用遠端 PowerShell 連線至您的檔案系統，每個系統都有自己的解析度，如下所示。

若要先確定您可以成功連線至 Windows Remote PowerShell 端點，您也可以執行基本連線測試。例如，您可以執行 `test-netconnection endpoint -port 5985`命令。

檔案系統的安全群組缺少允許遠端 PowerShell 連線所需的傳入規則

檔案系統的安全群組必須具有傳入規則，允許連接埠 5985 上的流量，才能建立遠端 PowerShell 工作階段。如需詳細資訊，請參閱Amazon VPC 安全群組。

您在 AWS 受管 Microsoft Active Directory 和內部部署 Active Directory 之間設定了外部信任

若要搭配 Kerberos 身分驗證使用 Amazon FSx Remote PowerShell，您需要在用戶端上設定本機群組政策以進行樹系搜尋順序。如需詳細資訊，請參閱 Microsoft 文件設定 Kerberos 樹系搜尋順序 (KFSO)。

嘗試啟動遠端 PowerShell 工作階段時發生語言當地語系化錯誤

您需要將下列項目`-SessionOption`新增至命令： `-SessionOption (New-PSSessionOption -uiCulture "en-US")`

以下是在檔案系統上啟動遠端 PowerShell 工作階段`-SessionOption`時使用 的兩個範例。

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName Windows Remote PowerShell
 Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {fsx-command} -SessionOption
 (New-PSSessionOption -uiCulture "en-US")
```

```
PS C:\Users\delegateadmin> Enter-Pssession -ComputerName Windows Remote PowerShell
 Endpoint -ConfigurationName FsxRemoteAdmin -SessionOption (New-PSSessionOption -
uiCulture "en-US")
```

檔案系統維護時段

Amazon FSx for Windows File Server 會針對其管理的 Microsoft Windows Server 軟體執行例行軟體修補。維護時段會指定一週中的某一天，以及此維護程序開始的時間。您可以在檔案系統建立期間指定

維護時段的開始期間。如果您未指定，則會指派 30 分鐘的預設維護啟動時段。維護時段的持續時間取決於多個因素，包括維護範圍，以及同步多可用區域檔案系統的主要和次要伺服器之間在維護期間發生的任何檔案讀取和寫入活動的程序。如需詳細資訊，請參閱程序失敗。

FSx for Windows File Server 可讓您調整維護時段的開始時間，以符合工作負載和操作需求。您可以視需要頻繁移動維護時段的開始時間，前提是至少每 14 天排定一次維護時段開始時間。如果修補程式已發行，而且您未在 14 天內排定維護時段，FSx for Windows File Server 會繼續維護檔案系統，以確保其安全性和可靠性。如需如何調整檔案系統維護時段開始時間的詳細資訊，請參閱 變更每週維護時段。

當修補正在進行時， 預期您的單一可用區檔案系統無法使用，通常不到 20 分鐘。多可用區域檔案系統仍然可用，並自動容錯移轉，並在偏好的 和待命檔案伺服器之間容錯。如需詳細資訊，請參閱程序失敗。由於異地同步備份檔案系統的修補涉及檔案伺服器之間的容錯移轉和容錯移轉，因此在此期間發生的任何檔案讀取和寫入活動都必須在偏好的 和待命檔案伺服器之間同步。為了縮短修補時間，我們建議您在檔案系統負載最少的閒置期間排定維護時段。

> **Note**
>
> 為了確保維護活動期間的資料完整性，Amazon FSx for Windows File Server 會在維護開始之前，對託管檔案系統的基礎儲存磁碟區完成任何待定的寫入操作。

變更每週維護時段

FSx for Windows File Server 可讓您在檔案系統的維護時段開始適應工作負載和操作需求時進行調整。您可以使用 AWS 管理主控台 AWS CLI和 Amazon FSx API，在每週維護時段開始時變更，如下列程序所述。

變更每週維護時段的開始時間（主控台）

1. 在 https://console.aws.amazon.com/fsx/：// 開啟 Amazon FSx 主控台。
2. 在左側導覽欄中選擇檔案系統。
3. 選擇您要變更其每週維護時段的檔案系統。隨即顯示檔案系統詳細資訊頁面。
4. 選擇管理以顯示檔案系統管理設定面板。
5. 選擇更新以顯示變更維護時段。
6. 輸入您希望每週維護時段開始的新日期和時間。
7. 選擇儲存，以儲存變更。新的維護開始時間會顯示在管理設定面板中。

若要使用 update-file-system CLI 命令變更每週維護時段的開始時間，請參閱 使用 更新檔案系統 AWS CLI。

管理 DNS 別名

除了 Amazon FSx 提供的預設網域名稱系統 (DNS) 名稱之外，您也可以將您選擇的 DNS 別名與檔案系統建立關聯。透過 DNS 別名，您可以將檔案系統儲存從內部部署遷移至 Amazon FSx 時，繼續使用現有的 DNS 名稱來存取 Amazon FSx 上存放的資料，而不需要更新任何工具或應用程式。

您可以使用 和 將 DNS 別名與新的和現有的 FSx for Windows File Server 檔案系統建立關聯，並在將備份還原至新的檔案系統時建立 AWS 管理主控台 關聯 AWS CLI。您一次最多可將 50 個 DNS 別名與檔案系統建立關聯。

> **Note**
>
> FSx for Windows File Server 檔案系統可在 2020 年 11 月 9 日東部時間下午 12：00 之後建立的 DNS 別名支援。若要在 2020 年 11 月 9 日東部時間中午 12：00 之前建立的檔案系統上使用 DNS 別名，請執行下列動作：
>
> 1. 備份現有的檔案系統。如需詳細資訊，請參閱使用使用者啟動的備份。
> 2. 將備份還原至新的檔案系統。如需詳細資訊，請參閱將備份還原至新的檔案系統。
>
> 一旦新的檔案系統可用，您就可以使用 DNS 別名，使用本節提供的資訊來存取該檔案系統。

> **Note**
>
> 此處顯示的資訊假設您完全在 Active Directory 中工作，而且不是使用外部 DNS 供應商。第三方 DNS 供應商可能會導致意外行為。
> 如果您加入檔案系統的 Active Directory 網域使用 Microsoft DNS 做為預設 DNS，Amazon FSx 只會註冊檔案系統的 DNS 記錄。如果您使用第三方 DNS，則需要在建立檔案系統之後手動設定 Amazon FSx 檔案系統的 DNS 項目。如需選擇要用於檔案系統之正確 IP 地址的詳細資訊，請參閱 取得用於手動 DNS 項目的正確檔案系統 IP 地址。

您可以在建立新檔案系統時，以及從備份建立新檔案系統時，將 DNS 別名與現有的 FSx for Windows File Server 檔案系統建立關聯。您一次最多可將 50 個 DNS 別名與檔案系統建立關聯。

除了將 DNS 別名與您的檔案系統建立關聯之外，若要讓用戶端使用 DNS 別名連線至檔案系統，您還必須執行下列動作：

- 設定 Kerberos 身分驗證和加密的服務主體名稱 (SPNs)。
- 為解析為 Amazon FSx 檔案系統預設 DNS 名稱的 DNS 別名設定 DNS CNAME 記錄。

如需詳細資訊，請參閱使用 DNS 別名存取資料。

FSx for Windows File Server 檔案系統的 DNS 別名名稱必須符合下列要求：

- 必須格式化為完整網域名稱 (FQDN)。
- 可包含英數字元和連字號 (-)。
- 名稱開頭或結尾不能為連字號 (-)。
- 可以從數字開頭。

對於 DNS 別名名稱，Amazon FSx 會將字母字元儲存為小寫字母 (a-z)，不論儲存時指定為大寫、小寫字母或逸出碼中的對應字母。

如果您嘗試將已與檔案系統建立關聯的別名建立關聯，則不會有任何影響。如果您嘗試取消別名與未與檔案系統建立關聯的檔案系統的關聯，Amazon FSx 會回應錯誤的請求錯誤。

> **Note**
>
> 當 Amazon FSx 在檔案系統上新增或移除別名時，連線的用戶端會暫時中斷連線，並自動重新連線至檔案系統。在中斷連線時，由對應non-Continuously-Available (非 CA) 共用的用戶端開啟的任何檔案都必須由用戶端重新開啟。

主題

DNS 別名狀態

DNS 別名可以有下列其中一個狀態值：

- 可用 – DNS 別名與 Amazon FSx 檔案系統相關聯。
- 建立 – Amazon FSx 正在建立 DNS 別名並將其與檔案系統建立關聯。
- 刪除 – Amazon FSx 正在取消 DNS 別名與檔案系統的關聯，並將其刪除。
- 無法建立 – Amazon FSx 無法將 DNS 別名與檔案系統建立關聯。
- 無法刪除 – Amazon FSx 無法取消 DNS 別名與檔案系統的關聯。

搭配 Kerberos 身分驗證使用 DNS 別名

我們建議您透過 Amazon FSx 使用傳輸中的 Kerberos 型身分驗證和加密。Kerberos 為存取檔案系統的用戶端提供最安全的身分驗證。若要為使用 DNS 別名存取 Amazon FSx 檔案系統的用戶端啟用 Kerberos 身分驗證，您必須設定對應至檔案系統 Active Directory 電腦物件上 DNS 別名的服務主體名稱 (SPNs)。

如果您已針對已指派給 Active Directory 中電腦物件上另一個檔案系統的 DNS 別名設定 SPNs，您必須先移除這些 SPNs才能將 SPNs 新增至檔案系統的電腦物件。如需詳細資訊，請參閱設定 Kerberos 的服務主體名稱 (SPNs)。

檢視檔案系統和備份的 DNS 別名

您可以使用 AWS CLI、 和 API 檢視目前與 FSx for Windows File Server 檔案系統和備份相關聯的 DNS AWS 管理主控台別名，如下列程序所述。

檢視與檔案系統相關聯的 DNS 別名

- 使用主控台 — 選擇檔案系統以檢視檔案系統詳細資訊頁面。選擇網路與安全索引標籤以檢視 DNS 別名。
- 使用 CLI 或 API — 使用 `describe-file-system-aliases` CLI 命令或 DescribeFileSystemAliases API 操作。

檢視與備份相關聯的 DNS 別名

- 使用主控台 — 在導覽窗格中，選擇備份，然後選擇您要檢視的備份。在摘要窗格中，檢視 DNS 別名欄位。

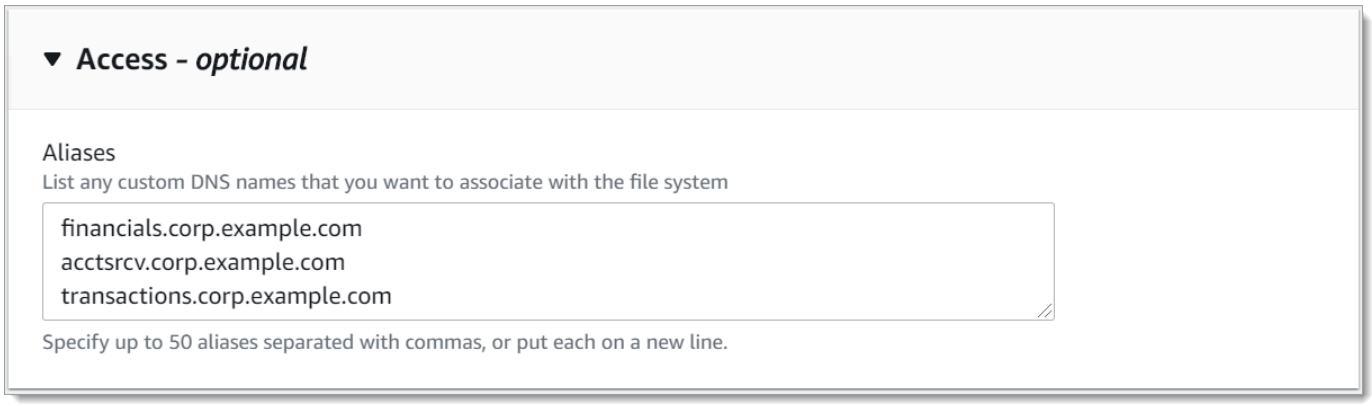
- 使用 CLI 或 API — 使用 `describe-backups` CLI 命令或 DescribeBackups API 操作。

將 DNS 別名與檔案系統建立關聯

您可以在從頭開始建立新的 FSx for Windows File Server 檔案系統，或使用 和 API 將備份還原至新的檔案系統時 AWS 管理主控台 AWS CLI，將 DNS 別名建立關聯，說明下列程序。

在建立新檔案系統時關聯 DNS 別名 （主控台）

1. 開啟位於 https：//https://console.aws.amazon.com/fsx/ 的 Amazon FSx 主控台。
2. 遵循 入門一節步驟 5. 建立您的檔案系統中所述建立新檔案系統的程序。
3. 在建立檔案系統精靈的存取 - 選用區段中，輸入您要與檔案系統建立關聯的 DNS 別名。



4. 當檔案系統可用時，您可以透過設定服務主體名稱 (SPNs) 以及更新或建立別名的 DNS CNAME 記錄，使用 DNS 別名來存取它。如需詳細資訊，請參閱使用 DNS 別名存取資料。

在建立新的 Amazon FSx 檔案系統 (CLI) 時關聯 DNS 別名

1. 建立新的檔案系統時，請使用別名屬性搭配 CreateFileSystem API 操作，將 DNS 別名與新的檔案系統建立關聯。

```
aws fsx create-file-system \
  --file-system-type WINDOWS \
  --storage-capacity 2000 \
  --storage-type SSD \
  --subnet-ids subnet-123456 \
  --windows-configuration Aliases=[financials.corp.example.com,accts-
rcv.corp.example.com]
```

2. 當檔案系統可用時，您可以透過設定服務主體名稱 (SPNs) 以及更新或建立別名的 DNS CNAME 記錄，使用 DNS 別名來存取它。如需詳細資訊，請參閱使用 DNS 別名存取資料。

在還原備份時新增或移除 DNS 別名 (CLI)

1. 從現有檔案系統的備份建立新的檔案系統時，您可以使用別名屬性搭配 CreateFileSystemFromBackup API 操作，如下所示：

   - 根據預設，與備份相關聯的任何別名都會與新的檔案系統相關聯。
   - 若要建立檔案系統而不保留備份中的任何別名，請使用 `Aliases` 屬性搭配空集。

     若要關聯其他 DNS 別名，請使用 `Aliases` 屬性，並同時包含與備份相關聯的原始別名和您要關聯的新別名。

   下列 CLI 命令會將兩個別名與 Amazon FSx 從備份建立的檔案系統建立關聯。

   ```
   aws fsx create-file-system-from-backup \
     --backup-id backup-0123456789abcdef0
     --storage-capacity 2000 \
     --storage-type HDD \
     --subnet-ids subnet-123456 \
     --windows-configuration Aliases=[transactions.corp.example.com,accts-
   rcv.corp.example.com]
   ```

2. 當檔案系統可用時，您可以透過設定服務主體名稱 (SPNs) 以及更新或建立別名的 DNS CNAME 記錄，使用 DNS 別名來存取它。如需詳細資訊，請參閱使用 DNS 別名存取資料。

管理現有檔案系統的 DNS 別名

您可以使用 和 在現有的 FSx for Windows File Server 檔案系統上新增 AWS 管理主控台 和移除別名 AWS CLI，如下列程序所述。

管理檔案系統 DNS 別名 （ 主控台 ）

1. 在 https://console.aws.amazon.com/fsx/：// 開啟 Amazon FSx 主控台。
2. 導覽至檔案系統，然後選擇您要管理 DNS 別名的 Windows 檔案系統。
3. 在網路與安全索引標籤上，選擇管理 DNS 別名以顯示管理 DNS 別名視窗。

   - 若要關聯 DNS 別名 – 在關聯新別名方塊中，輸入您要關聯的 DNS 別名。選擇關聯。

- 若要取消與 DNS 別名的關聯 – 在目前別名清單中，選擇要取消關聯的別名。選擇取消關聯。

您可以在目前別名清單中監控您管理的別名狀態。重新整理清單以更新狀態。別名與檔案系統建立關聯或取消關聯最多需要 2.5 分鐘。

4. 當別名可用時，您可以透過設定服務主體名稱 (SPNs) 以及更新或建立別名的 DNS CNAME 記錄，使用 DNS 別名存取您的檔案系統。如需詳細資訊，請參閱使用 DNS 別名存取資料。

將 DNS 別名與現有檔案系統 (CLI) 建立關聯

1. 使用 `associate-file-system-aliases` CLI 命令或 AssociateFileSystemAliases API 操作，將 DNS 別名與現有檔案系統建立關聯。

   下列 CLI 請求會將兩個別名與指定的檔案系統建立關聯。

   ```
   aws fsx associate-file-system-aliases \
     --file-system-id fs-0123456789abcdef0 \
     --aliases financials.corp.example.com transfers.corp.example.com
   ```

   回應會顯示 Amazon FSx 正在與檔案系統建立關聯的別名狀態。

   ```
   {
       "Aliases": [
           {
               "Name": "financials.corp.example.com",
               "Lifecycle": CREATING
           },
           {
               "Name": "transfers.corp.example.com",
               "Lifecycle": CREATING
           }
       ]
   }
   ```

2. 使用 `describe-file-system-aliases` CLI 命令 (DescribeFileSystemAliases 是同等的 API 操作） 來監控您正在關聯的別名狀態。

3. 當 的值`Lifecycle`為可用 （ 最多可能需要 2.5 分鐘的程序 ） 時，您可以使用 DNS 別名存取您的檔案系統，方法是設定服務主體名稱 (SPNs)，以及更新或建立別名的 DNS CNAME 記錄。如需詳細資訊，請參閱使用 DNS 別名存取資料。

取消 DNS 別名與檔案系統的關聯 (CLI)

- 使用 `disassociate-file-system-aliases` CLI 命令或 DisassociateFileSystemAliases API 操作，取消 DNS 別名與現有檔案系統的關聯。

  下列命令會取消一個別名與檔案系統的關聯。

  ```
  aws fsx disassociate-file-system-aliases \
    --file-system-id fs-0123456789abcdef0 \
    --aliases financials.corp.example.com
  ```

  回應會顯示 Amazon FSx 正在與檔案系統取消關聯的別名狀態。

  ```
  {
      "Aliases": [
          {
              "Name": "financials.corp.example.com",
              "Lifecycle": DELETING
          }
      ]
  }
  ```

  使用 `describe-file-system-aliases` CLI 命令 (DescribeFileSystemAliases 是同等的 API 操作）來監控別名的狀態。刪除別名最多需要 2.5 分鐘。

使用者工作階段和開啟的檔案

您可以使用共用資料夾工具，監控連線的使用者工作階段，並在 FSx for Windows File Server 檔案系統上開啟檔案。共用資料夾工具提供集中位置，可監控連線至檔案系統的人員，以及開啟哪些檔案以及由誰開啟。您可以使用此工具執行下列動作：

- 還原對鎖定檔案的存取。
- 中斷連接使用者工作階段，這會關閉該使用者開啟的所有檔案。

您可以使用 Windows 原生共用資料夾 GUI 工具和 Amazon FSx CLI 在 PowerShell 上進行遠端管理，以在 FSx for Windows File Server 檔案系統上管理使用者工作階段和開啟檔案。

使用 GUI 管理使用者和工作階段

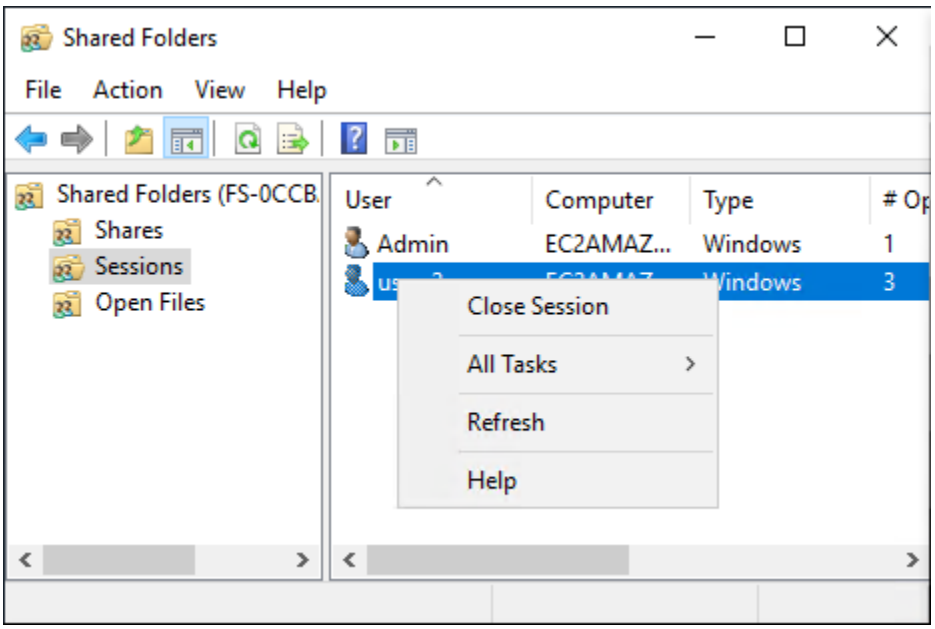
下列程序詳細說明如何使用 Microsoft Windows 共用資料夾工具，在 Amazon FSx 檔案系統上管理使用者工作階段和開啟檔案。

啟動共用資料夾工具

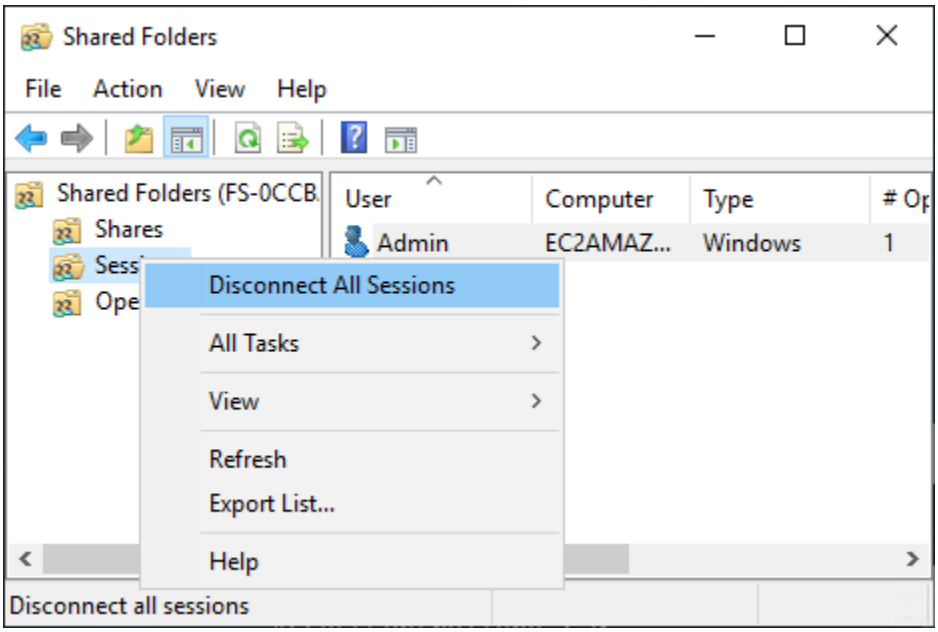
1. 啟動您的 Amazon EC2 執行個體，並將其連接至您的 Amazon FSx 檔案系統所加入的 Microsoft Active Directory。若要這樣做，請從 AWS Directory Service 管理指南中選擇下列其中一個程序：
   - 無縫加入 Windows EC2 執行個體
   - 手動加入 Windows 執行個體
2. 以檔案系統管理員群組成員的使用者身分連線至您的執行個體。在 AWS 受管 Microsoft Active Directory AWS 中，此群組稱為委派 FSx 管理員。在自我管理的 Microsoft Active Directory 中，此群組稱為網域管理員，或您在建立期間提供的管理員群組自訂名稱。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的連線至 Windows 執行個體。
3. 開啟開始功能表，並使用 執行 fsmgmt.mscRun As Administrator。這樣做會開啟共用資料夾 GUI 工具。
4. 針對動作，選擇連線至另一部電腦。
5. 針對另一部電腦，輸入 Amazon FSx 檔案系統的 DNS 名稱，例如 `fs-01234567890123456.ad-domain.com`。
6. 選擇確定。然後，Amazon FSx 檔案系統的項目會出現在共用資料夾工具的清單中。

管理使用者工作階段 (GUI)

在共用資料夾工具中，選擇工作階段以檢視連線至 FSx for Windows File Server 檔案系統的所有使用者工作階段。如果使用者或應用程式正在存取 Amazon FSx 檔案系統上的檔案共享，此增益集會顯示其工作階段。您可以開啟工作階段的內容 （ 按一下滑鼠右鍵 ） 功能表，然後選擇關閉工作階段，以中斷工作階段的連線。

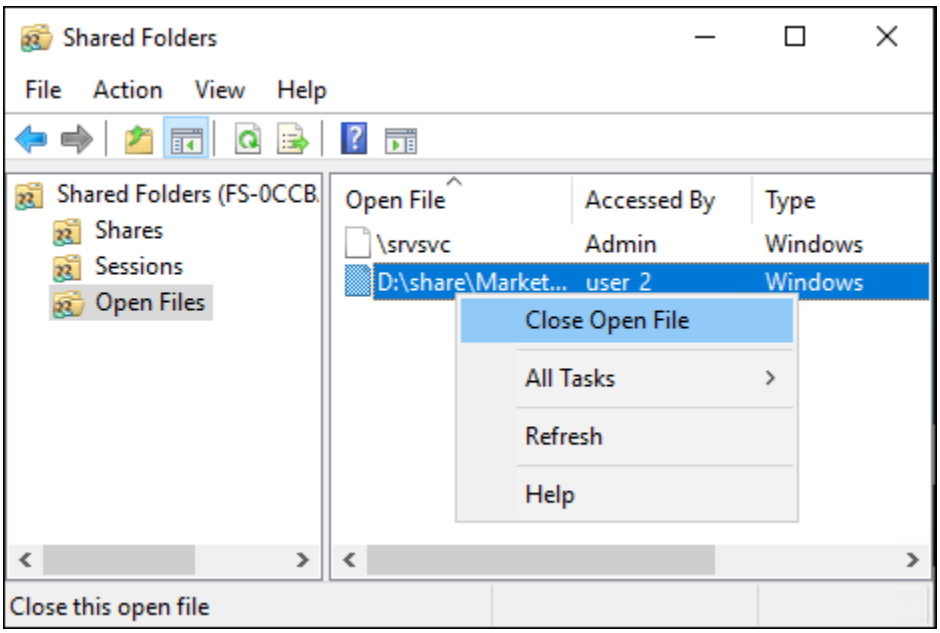


若要中斷連接所有開啟的工作階段，請開啟工作階段的內容（按一下滑鼠右鍵）選單，選擇中斷連接所有工作階段，然後確認您的動作。

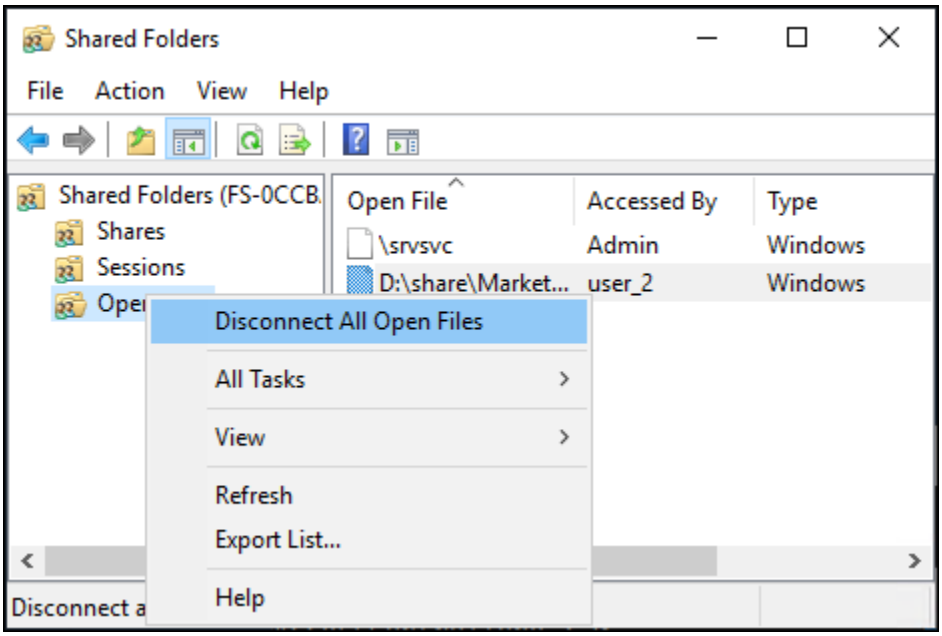


管理開啟的檔案 (GUI)

在共用資料夾工具中，選擇開啟檔案以檢視系統上目前開啟的所有檔案。檢視也會顯示哪些使用者開啟了檔案或資料夾。此資訊有助於追蹤其他使用者無法開啟特定檔案的原因。您可以關閉任何使用者開啟的任何檔案，只要開啟清單中檔案項目的內容（按一下滑鼠右鍵）選單，然後選擇關閉開啟檔案即可。



若要中斷連接檔案系統上所有開啟的檔案，開啟檔案的內容（按一下滑鼠右鍵）選單，然後選擇中斷所有開啟檔案的連線，然後確認您的動作。



使用 PowerShell 管理使用者工作階段和開啟檔案

您可以使用 Amazon FSx CLI 在 PowerShell 上進行遠端管理，在檔案系統上管理作用中的使用者工作階段和開啟檔案。若要了解如何使用此 CLI，請參閱 使用 Amazon FSx CLI for PowerShell。

以下是可用於使用者工作階段和開啟檔案管理的命令。

命令	Description
Get-FSxSmbSession	擷取目前在檔案系統和相關聯用戶端之間建立之伺服器訊息區塊 (SMB) 工作階段的相關資訊。
Close-FSxSmbSession	結束 SMB 工作階段。
Get-FSxSmbOpenFile	擷取連線至檔案系統之用戶端所開啟之檔案的相關資訊。
Close-FSxSmbOpenFile	關閉為 SMB 伺服器其中一個用戶端開啟的檔案。

每個命令的線上說明提供所有命令選項的參考。若要存取此說明，請使用 執行 命令-?，例如 Get-FSxSmbSession -?。

FSx for Windows File Server 上的檔案伺服器資源管理員

File Server Resource Manager (FSRM) 是一種 Windows Server 功能，可協助您管理和分類存放在 Amazon FSx for Windows File Server 檔案系統上的資料。FSRM 提供自動化政策強制執行和報告功能，可協助您控制儲存成本、維持資料管理政策的合規性，以及根據業務規則整理檔案。

使用 FSRM，您可以設定儲存限制，以防止使用者耗用過多儲存、自動識別和分類敏感資料、封鎖未經授權的檔案類型儲存到商業資料夾，以及產生有關儲存用量模式的詳細報告。這些功能可協助您維護有條不紊、有效率且合規的檔案系統，而無需為每個檔案或資料夾手動介入。

對於需要：

- 透過限制使用者和部門可以存放多少磁碟空間來控制儲存成本
- 識別敏感資料，例如個人身分識別資訊或財務記錄
- 強制執行有關特定資料夾中允許哪些檔案類型的政策
- 產生有關資料保留、檔案擁有權或儲存用量的合規報告
- 保持整個組織如何使用儲存體的可見性

關鍵功能

- 配額管理 - 設定資料夾的儲存限制，以控制使用者和應用程式可以使用的空間。您可以設定硬性配額，以防止使用者在傳送通知時超過允許超額的限制或軟性配額。配額可協助您管理儲存成本，並防止使用者或部門耗用不成比例的儲存量。

- 檔案篩選 - 控制使用者可以儲存到特定資料夾的檔案類型。您可以封鎖未經授權的檔案類型，例如可執行檔、媒體檔案或商業資料夾中的個人文件。檔案篩選可協助您強制執行資料管理政策、降低安全風險，並防止非業務檔案的儲存體浪費。
- 檔案分類 - 根據檔案的內容或位置，自動將中繼資料屬性指派給檔案。分類可協助您整理檔案、識別敏感資料、套用保留政策，並根據檔案特性產生報告。您可以依資料敏感性、部門、保留期或您定義的任何其他自訂屬性來分類檔案。
- 儲存報告 - 產生有關檔案系統用量的詳細報告，包括大型檔案、重複檔案、依擁有者的檔案、依類型列出的檔案和配額用量。儲存報告可協助您了解儲存體的使用方式、識別可封存或刪除的檔案，以及對儲存體管理做出明智的決策。

主題

File Server Resource Manager 入門

您可以在建立新的 Amazon FSx for Windows File Server 檔案系統時啟用 File Server Resource Manager (FSRM)，也可以更新現有的檔案系統以啟用 FSRM。

FSRM 僅在具有 SSD 儲存體且輸送量容量為 128 MB/s 或更高的 Amazon FSx for Windows File Server 檔案系統上受支援。您可以在建立檔案系統之後，隨時將儲存體類型更新為 SSD 並修改輸送量容量。如需詳細資訊，請參閱更新 FSx for Windows 檔案系統的儲存類型及管理輸送量容量。

在建立檔案系統時啟用 FSRM （主控台）

1. 在 https://console.aws.amazon.com/fsx/：// 開啟 Amazon FSx 主控台

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. 選擇 Amazon FSx for Windows File Server，然後選擇下一步。
4. 選取標準建立選項
5. 提供必要資訊
6. 開啟檔案伺服器資源管理員區塊，選擇已啟用。
7. 針對事件日誌目的地，選擇下列其中一個選項：
   - CloudWatch Logs - 選取 CloudWatch Logs 日誌群組以接收 FSRM 事件日誌。CloudWatch Logs 日誌群組的名稱必須以 `'/aws/fsx/'` 字首開頭。
   - Kinesis Data Firehose - 選取 Kinesis Data Firehose 交付串流以接收 FSRM 事件日誌
8. 完成其餘區段，然後選擇建立檔案系統。

在建立檔案系統時啟用 FSRM (CLI)

若要在建立 FSx for Windows File Server 檔案系統時啟用 FSRM，請使用 AWS CLI 命令 `create-file-system`。在 `--windows-configuration` 參數中包含下列 FSRM 組態：

- `FsrmServiceEnabled`：設定為 `true`
- `EventLogDestination` - 指定 FSRM 事件日誌目的地的 Amazon Resource Name (ARN)。可以是 CloudWatch Logs 日誌群組 ARN 或 Kinesis Data Firehose 交付串流 ARN。

```
aws fsx create-file-system \
        --file-system-type WINDOWS \
        --storage-capacity 300 \
        --storage-type SSD \
        --subnet-ids subnet-0123456789abcdef0 \
        --windows-configuration
 "ThroughputCapacity=128,WindowsFsrmConfiguration={FsrmServiceEnabled=true,EventLogDestination=
east-1:123456789012:log-group:/aws/fsx/fsrm}"
```

在現有檔案系統上修改 FSRM 組態（主控台）

1. 在 https://console.aws.amazon.com/fsx/：// 開啟 Amazon FSx 主控台。
2. 導覽至檔案系統，然後選擇您要修改的 Windows 檔案系統。
3. 選擇管理索引標籤。
4. 在檔案伺服器資源管理員區段中，選擇管理。

5. 進行必要的變更：

   - 若要變更事件日誌目的地，請選取不同的 CloudWatch Logs 日誌群組或 Kinesis Data Firehose 交付串流
   - 若要啟用 FSRM，請選擇已啟用
   - 若要停用 FSRM，請選擇已停用

   > **Important**
   >
   > 在此過程中，多可用區域檔案系統將遇到自動容錯移轉和容錯回復事件，而單一可用區域檔案系統將經歷短暫的無法使用。

6. 選擇儲存。

您可以在檔案系統詳細資訊頁面的更新索引標籤中監控更新進度。

修改現有檔案系統 (CLI) 上的 FSRM 組態

若要在現有的 FSx for Windows File Server 檔案系統上啟用和停用 FSRM，請使用 AWS CLI 命令 `update-file-system`。

啟用 FSRM

若要啟用 FSRM，請在 `--windows-configuration` 參數中包含下列 FSRM 組態：

- `FsrmServiceEnabled`：設定為 `true`
- `EventLogDestination` - 指定 FSRM 事件日誌目的地的 Amazon Resource Name (ARN)。可以是 CloudWatch Logs 日誌群組 ARN 或 Kinesis Data Firehose 交付串流 ARN。

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --windows-configuration
 FsrmConfiguration='{FsrmServiceEnabled=true,EventLogDestination=”arn:aws:logs:us-
east-1:123456789012:log-group:/aws/fsx/fsrm”}'
```

停用 FSRM

若要停用 FSRM：

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --windows-configuration FsrmConfiguration='{FsrmServiceEnabled=false}'
```

> **Important**
>
> 在此過程中，多可用區域檔案系統將遇到自動容錯移轉和容錯回復事件，而單一可用區域檔案系統將經歷短暫的無法使用。

FSx 遠端 PowerShell

若要設定和使用 FSRM 功能，您必須使用 Amazon FSx CLI 在 PowerShell 上進行遠端管理。如需相關資訊，請參閱啟動 Amazon FSx 遠端 PowerShell 工作階段。

配額管理

您可以使用 File Server Resource Manager (FSRM) 配額管理來控制使用者在 FSx for Windows File Server 檔案系統上使用的儲存空間量。配額透過限制可存放在特定資料夾中的資料量，以及在儲存用量接近或超過定義的閾值時產生通知，來協助您管理儲存容量。

配額管理的運作方式

配額管理提供兩種類型的配額，您可以套用至檔案系統上的資料夾：

硬性配額

防止使用者在達到配額限制後儲存檔案。當使用者嘗試儲存超過配額限制的檔案時，操作會失敗，且使用者會收到錯誤訊息。

軟配額

允許使用者在記錄違規時超過配額限制。軟配額適用於監控儲存體用量，而無須強制嚴格限制。

配額範本

配額範本提供可重複使用的組態，可定義配額設定，包括大小限制、配額類型（硬式或軟式）和閾值通知。建立配額範本之後，您可以將其套用至多個資料夾，而不必每次重新設定相同的設定。當您更新配額範本時，您可以選擇將變更套用至從該範本建立的所有配額。

使用配額範本有幾個優點：

- 一致性 - 確保類似的資料夾具有相同的配額組態
- 效率 - 快速將配額設定套用至多個資料夾
- 可維護性 - 透過修改範本來更新多個資料夾的配額設定

自動套用配額

自動套用配額會根據指定的範本自動建立子資料夾的配額。當您在父資料夾上建立自動套用配額時，FSRM 會自動為每個現有子資料夾和使用者未來建立的任何新子資料夾產生配額。此方法適用於您想要在多個使用者目錄或部門資料夾之間套用一致配額限制的情況。

閾值通知

閾值定義 FSRM 採取特定動作的用量層級。您可以為每個配額設定多個閾值，並將每個閾值設定為配額限制的百分比。當儲存體用量達到閾值百分比時，FSRM 可以執行下列動作：

事件記錄

將事件記錄到 Amazon CloudWatch 或 Amazon Kinesis Data Firehose 以進行監控和分析。您可以指定事件嚴重性等級（資訊、警告或錯誤），並提供自訂訊息內文。事件記錄有助於監控配額用量，並與現有的監控系統整合。

儲存報告

產生儲存用量報告，提供使用儲存空間之檔案和資料夾的詳細資訊。儲存報告可協助您識別哪些使用者或應用程式耗用最多的儲存體，並做出有關儲存體管理的明智決策。如需詳細資訊，請參閱儲存報告。

您可以為每個配額設定多個具有不同動作的閾值。例如，您可以使用 75% 用量的資訊事件和 90% 用量的警告事件來設定配額。

Quota Management 命令

您可以存取三個 FSx 遠端 PowerShell 命令系列來管理配額：

1. 配額命令 - 在特定資料夾上建立、擷取、修改、移除和更新配額。當您需要folder-by-folder管理配額時，請使用這些命令。
2. 配額範本命令 - 建立、擷取和修改定義可重複使用配額組態的配額範本。使用這些命令來建立標準配額政策，您可以將這些政策套用至多個資料夾。

3. Auto Quota 命令 - 建立、擷取、修改、移除和更新自動套用配額，以自動產生子資料夾的配額。當您需要跨多個子資料夾套用一致的配額限制，而無需手動建立個別配額時，請使用這些命令。

Quota Management FSx 遠端 PowerShell 命令的清單

> **Note**
>
> 此頁面中的所有範例都假設您已使用檔案系統的 Windows Remote PowerShell 端點定義 `$FSxWindowsRemotePowerShellEndpoint`變數。您可以在檔案系統的詳細資訊頁面上的 Amazon FSx 主控台中找到此端點，或使用 AWS CLI `describe-file-systems`命令。

配額命令

New-FSxFSRMQuota

在資料夾上建立新的配額。配額會限制使用者可以存放在資料夾中的資料量。您可以選擇性地設定配額，以便在使用者超過配額閾值時產生通知。

參數：

- `Folder (string)` - 必要。套用配額的資料夾路徑。
- `Size (string)` - 不使用範本時為必要：配額大小限制。
- `Template (string)` - 選用。要使用的現有配額範本名稱。當您指定範本時，您只能使用描述參數；所有其他設定都會繼承自範本。
- `Description (string)` - 選用。配額的描述。
- `SoftLimit (boolean)` - 選用。如果設為 true， 會建立軟配額，允許使用者在記錄違規時超過限制。
- `Disabled (boolean)` - 選用。如果設為 true， 會以停用狀態建立配額。
- `ThresholdConfigurations (array)` - 選用。閾值組態陣列，指定在不同用量層級要採取的動作。每個組態都有下列屬性：
  - `ThresholdPercentage (number)`：觸發動作的配額限制百分比。輸入介於 0 到 250 之間的值。
  - `Action (array)`：達到閾值時要採取的一或多個動作。每個動作都有下列屬性：
    - `ActionType`：要執行的動作類型。您可以指定下列值：
      1. `Event`：將事件記錄到檔案系統的事件日誌。當您指定事件時，也必須指定下列屬性：

- EventType：資訊、警告或錯誤
- MessageBody：使用事件記錄的訊息文字。

2. Report：產生儲存用量報告。

範例：

1。建立硬式 5GB 配額，而不使用配額範本。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMQuota -Folder "share\test" -Size 5GB
}
```

2. 使用閾值通知建立軟配額

```
$thresholds = [System.Collections.ArrayList]@()
$warning = @{
    ThresholdPercentage = 75
    Action = @(
        @{
            ActionType = "Event"
            EventType = "Warning"
            MessageBody = "Quota usage has reached 75%"
        }
    )
}

$thresholds.Add($warning)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList ($thresholds) -ScriptBlock {
        param($thresholds)
        New-FSxFSRMQuota -Folder "share/test" -Size 1GB -Description "Test quota" -
SoftLimit -ThresholdConfigurations $Using:thresholds
}
```

Get-FSxFSRMQuota

從檔案系統擷取一或多個配額。命令會傳回配額組態的詳細資訊，包括大小限制、閾值和目前用量。

參數：

- Folder (string) - 選用。要從中擷取配額的資料夾路徑。如果您未指定資料夾路徑，命令會傳回檔案系統上的所有配額。

範例：

1。取得檔案系統上所有現有的配額。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMQuota
}
```

Remove-FSxFSRMQuota

從檔案系統上指定的資料夾移除配額。

參數：

- Folder (string) - 必要。要從中移除配額的資料夾路徑。
- PassThru (boolean) - 選用。如果設定為 true， 會傳回移除的配額物件。

範例：

1。移除配額。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Remove-FSxFSRMQuota -Folder "share\test" -PassThru
}
```

Set-FSxFSRMQuota

修改現有配額的組態。

參數：

- Folder (string) - 必要。包含要修改配額的資料夾路徑。
- Description (string) - 選用。配額的新描述。
- Size (string) - 選用。配額的新大小限制。

- SoftLimit (boolean) - 選用。如果設為 true， 會將配額變更為軟性限制，讓使用者在記錄違規時超過限制。
- Disabled (boolean) - 選用。如果設為 true， 會停用配額。如果設定為 false，請啟用配額。
- ThresholdConfigurations (array) - 選用。新閾值組態的陣列。每個閾值組態都有下列屬性：
  - ThresholdPercentage (number)：觸發動作的配額限制百分比。輸入介於 0 到 250 之間的值。
  - Action (array)：達到閾值時要採取的一或多個動作。每個動作都有下列屬性：
    - ActionType：要執行的動作類型。您可以指定下列值：
      1. Event：將事件記錄到檔案系統的事件日誌。當您指定事件時，也必須指定下列屬性：
         - EventType：資訊、警告或錯誤
         - MessageBody：使用事件記錄的訊息文字。
      2. Report：產生儲存用量報告。
- PassThru (boolean) - 選用。如果設定為 true， 會傳回修改後的配額物件。

範例：

1。修改配額大小和描述。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMQuota  -Folder "share\department"  -Size 2GB  -Description "Updated
 quota for department share"
}
```

2. 停用配額

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMQuota -Folder "share\department" -Disabled: $true
}
```

Update-FSxFSRMQuota

掃描 資料夾以判斷實際使用的空間量，以重新計算配額的目前用量統計資料。

參數：

- Folder (string) - 必要。包含要更新的配額的資料夾路徑。
- PassThru (boolean) - 選用。如果設定為 true， 會傳回更新的配額物件。

範例：

1。重新計算指定配額的目前用量統計資料。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Update-FSxFSRMQuota -Folder "share\department" -PassThru
}
```

配額範本命令

New-FSxFSRMQuotaTemplate

建立新的配額範本，定義配額的可重複使用組態。

參數：

- Name (string) - 必要。配額範本的名稱。
- Size (string) - 必要。配額範本強制執行的大小限制。
- Description (string) - 選用。配額範本的說明。
- SoftLimit (boolean) - 選用。如果設為 true， 會為軟性配額建立範本，以報告用量，但不強制執行限制。
- ThresholdConfigurations (array) - 選用。閾值組態陣列，指定在不同用量層級採取的動作。每個組態都有下列屬性：
  - ThresholdPercentage (number)：觸發動作的配額限制百分比。輸入介於 0 到 250 之間的值。
  - Action (array)：達到閾值時要採取的一或多個動作。每個動作都有下列屬性：
    - ActionType：要執行的動作類型。您可以指定下列值：
      1. Event：將事件記錄到檔案系統的事件日誌。當您指定 Event 時，也必須指定下列屬性：
         - EventType：資訊、警告或錯誤
         - MessageBody：使用事件記錄的訊息文字。
      2. Report：產生儲存用量報告。

範例：

1。建立硬式 1 GB 限制範本。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMQuotaTemplate -Name "1GB Hard Limit" -Size 1GB -Description "Standard
 1GB hard limit template"
}
```

2. 建立 5 GB 軟性限制範本，警告閾值為 90% 用量

```
$threshold = @{
    ThresholdPercentage = 90
    Action = @(
        @{
            ActionType = "Event"
            EventType = "Warning"
            MessageBody = "Quota usage has reached 90% of the limit"
        }
    )
}

$thresholds = [System.Collections.ArrayList]@()
$thresholds.Add($threshold)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $thresholds -ScriptBlock {
    param($thresholds)

    New-FSxFSRMQuotaTemplate -Name "5GB Soft Limit" -Size 5GB -Description "5GB soft
 limit with 90% warning" -SoftLimit -ThresholdConfigurations $Using:thresholds
}
```

Get-FSxFSRMQuotaTemplate

從檔案系統擷取一或多個配額範本。

參數：

- Name （string）- 選用。要擷取的特定配額範本名稱。如果您未指定名稱，命令會傳回所有配額範本。

範例：

1。擷取檔案系統上的所有配額範本。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMQuotaTemplate
}
```

Set-FSxFSRMQuotaTemplate

修改配額範本的屬性。

參數：

- Name (string) - 必要。要修改的配額範本名稱。
- Description (string) - 選用。範本的新描述。
- Size (string) - 選用。範本的新大小限制。
- SoftLimit (boolean) - 選用。如果設為 true， 會變更範本以建立軟性配額來報告用量，但不強制執行限制。
- ThresholdConfigurations (array) - 選用。閾值組態陣列，指定在不同用量層級採取的動作。每個組態都有下列屬性：
  - ThresholdPercentage (number)：觸發動作的配額限制百分比。輸入介於 0 到 250 之間的值。
  - Action (array)：達到閾值時要採取的一或多個動作。每個動作都有下列屬性：
    - ActionType：要執行的動作類型。您可以指定下列值：
      1. Event：將事件記錄到檔案系統的事件日誌。當您指定 Event 時，也必須指定下列屬性：
         - EventType：資訊、警告或錯誤
         - MessageBody：使用事件記錄的訊息文字。
      2. Report：產生儲存用量報告。
- UpdateDerived (boolean) - 選用。如果設定為 true， 會更新從此範本建立的所有配額。
- UpdateDerivedMatching (boolean) - 選用。如果設為 true，則 只會更新從此範本建立且自建立以來尚未修改的配額。
- PassThru (boolean) - 選用。如果設定為 true， 會傳回修改後的範本物件。

範例：

1。修改配額範本的大小和描述。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMQuotaTemplate -Name "5GB Soft Limit" -Size 10GB -Description "Updated to
 10GB soft limit"
}
```

2. 修改配額範本，並更新從範本建立的所有配額。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMQuotaTemplate -Name "1GB Hard Limit" -Size 2GB -UpdateDerived
}
```

Reset-FSxFSRMQuota

重設配額以符合指定範本的設定。

Parameters

- `Folder (string)` - 必要。包含要重設配額的資料夾路徑。
- `Template (string)` - 必要。要套用的配額範本名稱。

範例

範例：重設配額以符合配額範本中定義的設定。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Reset-FSxFSRMQuota -Folder "share\department" -Template "1GB Hard Limit"
}
```

自動配額命令

New-FSxFSRMAutoQuota

`New-FSxFSRMAutoQuota` 命令會在指定的資料夾上建立自動套用配額。自動套用配額會根據每個現有子資料夾的指定範本，以及在指定資料夾中建立的任何新子資料夾，自動產生配額。

Parameters

- `Folder (string)` - 必要。建立自動套用配額的資料夾路徑。
- `Template (string)` - 選用。用於自動套用配額的現有配額範本名稱。
- `Disabled (boolean)` - 選用。如果設為 true，會在停用狀態下建立自動套用配額。

範例

1。建立自動套用配額，以自動將指定的範本套用至所有子資料夾。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMAutoQuota -Folder "share\department" -Template "250 MB Extended Limit"
}
```

Get-FSxFSRMAutoQuota

`Get-FSxFSRMAutoQuota` 命令會從檔案系統擷取一或多個自動套用配額。

Parameters

- `Folder (string)` - 選用。要從中擷取自動套用配額的資料夾路徑。您也可以`...`在路徑結尾使用來包含所有子資料夾。

如果您未指定資料夾路徑，命令會在檔案系統上傳回所有自動套用配額。

範例

1。擷取檔案系統上的所有自動套用配額。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMAutoQuota
}
```

Remove-FSxFSRMAutoQuota

`Remove-FSxFSRMAutoQuota` 命令會從指定的資料夾移除自動套用配額。當您移除自動套用配額時，命令也會從衍生自相關聯配額範本的子資料夾移除所有配額。

Parameters

- `Folder (string)` - 必要。要從中移除自動套用配額的資料夾路徑。
- `PassThru (boolean)` - 選用。如果設定為 true， 會傳回移除的自動套用配額物件。

範例

1。從特定資料夾移除自動套用配額。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Remove-FSxFSRMAutoQuota -Folder "share\department" -PassThru
}
```

Set-FSxFSRMAutoQuota

`Set-FSxFSRMAutoQuota` 命令會修改自動套用配額的組態設定。

Parameters

- `Folder (string)` - 必要。包含要修改之自動套用配額的資料夾路徑。
- `Template (string)` - 選用。要套用的配額範本名稱。
- `Disabled (boolean)` - 選用。如果設為 true， 會停用自動套用配額。如果設定為 false，則啟用自動套用配額。
- `UpdateDerived (boolean)` - 選用。如果設為 true， 會更新衍生自此自動套用配額的所有現有配額。
- `UpdateDerivedMatching (boolean)` - 選用。如果設為 true， 只會更新自建立以來尚未修改的衍生配額。
- `PassThru (boolean)` - 選用。如果設定為 true， 會傳回修改過的自動套用配額物件。

範例

1。變更自動套用配額所使用的配額範本。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMAutoQuota -Folder "share\department" -Template "100 MB Limit"
}
```

2. 停用自動套用配額，並更新衍生自該配額的所有配額。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMAutoQuota -Folder "share\department" -Disabled: $true -UpdateDerived
}
```

Update-FSxFSRMAutoQuota

`Update-FSxFSRMAutoQuota` 命令會重新計算自動套用配額的屬性，以及從中衍生的配額，方法是掃描 資料夾以判斷實際使用的空間量。

Parameters

- `Folder (string)` - 必要。包含要更新的自動套用配額的資料夾路徑。
- `PassThru (boolean)` - 選用。如果設定為 true， 會傳回更新的自動套用配額物件。

範例

1。重新計算用量統計資料，並傳回更新的自動套用配額物件。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Update-FSxFSRMAutoQuota -Folder "share\department" -PassThru
}
```

檔案群組

檔案群組會定義檔案名稱模式的邏輯集合，您必須在設定檔案畫面時使用，也可以選擇在產生儲存報告時使用。檔案群組包含模式（要比對的檔案）和排除模式（要從比對中排除的檔案），您可以由檔案群組名稱參考，而不是每次指定個別模式。

如何使用檔案群組

下列 FSRM 功能需要檔案群組：

- 檔案畫面 - 您必須指定一或多個檔案群組，以定義要封鎖或監控的檔案類型。
- 檔案畫面例外狀況 - 您必須指定一或多個檔案群組，以定義在父資料夾中封鎖檔案畫面時允許哪些檔案類型。
- 檔案畫面範本 - 您必須指定一或多個檔案群組，以定義範本將封鎖或監控的檔案類型。

下列 FSRM 功能可選用檔案群組：

- 儲存報告 - 您可以選擇性地依檔案群組篩選報告，以分析特定檔案類型的儲存用量。例如，您可以產生僅顯示音訊和影片檔案的報告。

檔案名稱模式

檔案群組使用萬用字元模式來比對檔案名稱。您可以同時指定包含模式（要比對的檔案）和排除模式（要從比對中排除的檔案）。

FSRM 支援下列萬用字元：

- 星號 (*) - 符合零個或多個字元
- 問號 (?) - 完全符合一個字元

例如，模式`*.doc*`符合 `report.doc`、 `report.docx`和 等檔案`document.doc`，而排除模式 `~$*`會排除 Microsoft Office 應用程式建立的暫存檔案。

預設檔案群組

當您在檔案系統上啟用 FSRM 時，系統會自動建立下列檔案群組：

音訊和視訊檔案

符合常見的音訊和視訊檔案格式，包括 `*.mp3`、 `*.wav`、`*.avi`、`*.mpeg`、 `*.mp4`和 `*.wmv`

備份檔案

符合備份檔案格式`*.backup`，包括 `*.bak`、 和 `*.old`

壓縮檔案

符合封存和壓縮檔案格式，包括 `*.zip`、 `*.rar`、`*.7z`、 `*.gz`和 `*.tar`

電子郵件檔案

符合電子郵件訊息和信箱格式`*.eml`，包括 `*.msg`、 和 `*.pst`

可執行檔

符合可執行檔和指令碼檔案格式，包括 `*.exe`、 `*.dll`、`*.com`、`*.bat`、 `*.cmd`和 `*.vbs`

映像檔案

符合常見的影像檔案格式，包括 `*.jpg`、 `*.jpeg`、`*.png`、`*.bmp`、 `*.gif`和 `*.tif`

Office 檔案

符合 Microsoft Office 文件格式，包括 *.doc、 *.docx、*.xls、*.ppt、 *.xlsx和 *.pptx

系統檔案

符合 Windows 系統檔案格式 *.dll，包括 *.sys、*.ocx、 和 *.drv

暫存檔案

符合暫時檔案格式*.tmp，包括 *.temp、 和 ~*

文字檔案

符合文字型檔案格式*.log，包括 *.txt、*.csv、 和 *.xml

網頁檔案

符合 Web 內容檔案格式，包括 *.html、 *.htm、*.asp、*.php、 *.aspx和 *.js

您可以在檔案畫面和儲存報告中立即使用這些預設檔案群組，也可以修改它們以符合您的特定需求。

檔案群組管理命令

FSRM 提供 PowerShell 命令來建立和管理檔案群組。使用這些命令來定義符合您組織檔案管理政策的自訂檔案群組。

> **Note**
>
> 此頁面中的所有範例皆假設您已使用檔案系統的 Windows Remote PowerShell 端點定義 $FSxWindowsRemotePowerShellEndpoint變數。您可以在檔案系統的詳細資訊頁面上的 AWS FSx 主控台中找到此端點，或使用 CLI AWS describe-file-systems命令。

New-FSxFSRMFileGroup

建立定義檔案名稱模式邏輯集合的檔案群組。這些模式可用於檔案畫面、檔案畫面例外狀況和儲存報告。

參數：

- Name (string) - 必要。檔案群組的名稱。
- Description (string) - 選用。檔案群組的描述。
- IncludePattern (array) - 選用。指定要包含之檔案的模式字串陣列。

- ExcludePattern (array) - 選用。指定要排除之檔案的模式字串陣列。

範例：

1. 建立文字檔案的檔案群組。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMFileGroup -Name "My Text Files" -IncludePattern "*.txt"
}
```

2. 使用包含和排除模式為原始碼建立檔案群組。

```
$includePatterns = @("*.cpp", "*.h", "*.cs", "*.py")
$excludePatterns = @("*.tmp", "*.bak")

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList @($includePatterns, $excludePatterns) -ScriptBlock {
    param($includePatterns, $excludePatterns)
    New-FSxFSRMFileGroup -Name "Source Code" -Description "Programming source files"
 -IncludePattern $includePatterns -ExcludePattern $excludePatterns
}
```

Get-FSxFSRMFileGroup

從檔案系統擷取一或多個檔案群組。檔案群組定義檔案篩選和報告中使用的檔案模式集合。

參數：

- Name (array) - 選用。要擷取的檔案群組名稱陣列。如果您未指定名稱，命令會傳回檔案系統上的所有檔案群組。

範例：

1. 擷取檔案系統上的所有檔案群組。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMFileGroup
}
```

Remove-FSxFSRMFileGroup

從您的檔案系統移除一或多個檔案群組。移除後，檔案群組無法在檔案畫面或檔案畫面例外狀況中使用。

參數：

- `Name (array)` - 必要。要移除的檔案群組名稱陣列。
- `PassThru (boolean)` - 選用。如果設定為 true， 會傳回移除的檔案群組物件。

範例：

1. 移除單一檔案群組。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Remove-FSxFSRMFileGroup -Name "My Text Files" -PassThru
}
```

Set-FSxFSRMFileGroup

修改現有檔案群組的屬性。

參數：

- `Name (array)` - 必要。要修改的檔案群組名稱陣列。
- `Description (string)` - 選用。檔案群組的新描述。
- `IncludePattern (array)` - 選用。新的模式字串陣列，指定要包含的檔案。
- `ExcludePattern (array)` - 選用。新的模式字串陣列，指定要排除的檔案。
- `PassThru (boolean)` - 選用。如果設定為 true， 會傳回修改過的檔案群組物件。

範例：

1. 更新檔案群組的描述和模式。

```
$includePatterns = @("*.docx", "*.pdf", "*.rtf")
$excludePatterns = @("~$*", "*.tmp")
```

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList @($includePatterns, $excludePatterns) -ScriptBlock {
    param($includePatterns, $excludePatterns)
    Set-FSxFSRMFileGroup -Name "Documents" -Description "Updated document types" -
IncludePattern $includePatterns -ExcludePattern $excludePatterns -PassThru
}
```

檔案篩選

檔案篩選控制使用者可以將哪些類型的檔案儲存至檔案系統上的資料夾。檔案篩選可協助您強制執行儲存政策、防止未經授權的檔案類型，以及維持組織需求的合規性。

> **Note**
>
> 檔案畫面使用檔案群組來定義要封鎖或監控的檔案類型。如需建立和管理檔案群組的詳細資訊，請參閱 檔案群組。

FSRM 支援兩種類型的檔案畫面：

1. 作用中檔案畫面 - 封鎖使用者儲存符合指定檔案群組的檔案，並在使用者嘗試儲存封鎖的檔案時產生通知。當您需要強制執行有關特定資料夾中允許哪些檔案類型的嚴格政策時，請使用作用中檔案畫面。
2. 被動檔案畫面 - 當使用者儲存符合指定檔案群組的檔案時監控和記錄，但不阻止儲存操作。當您想要追蹤檔案使用模式而不中斷使用者工作流程時，請使用被動檔案畫面。

檔案畫面範本

檔案畫面範本提供可重複使用的組態，可定義檔案篩選設定，包括要封鎖或監控的檔案群組，以及要產生的通知。建立檔案畫面範本後，您可以將其套用至多個資料夾，而不必每次重新設定相同的設定。當您更新檔案畫面範本時，您可以選擇將變更套用至從該範本建立的所有檔案畫面。

使用檔案畫面範本有幾個優點：

- 一致性 - 確保類似的資料夾具有相同的檔案篩選組態
- 效率 - 快速將檔案篩選設定套用至多個資料夾
- 可維護性 - 透過修改範本，跨多個資料夾更新檔案篩選設定

檔案畫面例外狀況

檔案畫面例外狀況會覆寫原本會套用至資料夾及其所有子資料夾的檔案篩選規則。當您建立檔案畫面例外狀況時，您可以指定要允許哪些檔案群組，無論父資料夾中是否有任何封鎖的檔案畫面。當您需要允許特定子資料夾中的特定檔案類型，同時在資料夾階層的更高層級維持更廣泛的限制時，檔案畫面例外狀況非常有用。

例如，您可以封鎖整個共用的可執行檔，但為管理員需要存放安裝檔案的特定子資料夾建立例外狀況。

檔案篩選通知

當使用者嘗試儲存由作用中檔案畫面封鎖的檔案時，FSRM 可以產生通知來提醒管理員或提供資訊給使用者。您可以設定下列類型的通知：

- 事件記錄 - 將事件記錄到 Amazon CloudWatch 或 Amazon Kinesis Data Firehose 以進行監控和分析。您可以指定事件的嚴重性等級（資訊、警告或錯誤），並提供自訂訊息內文。事件記錄有助於追蹤檔案畫面違規，並與現有的監控系統整合。
- 儲存報告 - 產生儲存用量報告，提供檔案篩選活動的詳細資訊。儲存報告可協助您識別檔案儲存嘗試中的模式，並對檔案篩選政策做出明智的決策。如需詳細資訊，請參閱儲存報告。

檔案篩選管理命令

您可以存取三個 FSx 遠端 PowerShell 命令系列來管理檔案畫面：

1. 檔案畫面命令 - 在特定資料夾上建立、擷取、修改、移除和重設個別檔案畫面。當您需要folder-by-folder管理檔案畫面時，請使用這些命令。
2. 檔案畫面範本命令 - 建立、擷取、修改和移除定義可重複使用檔案篩選組態的檔案畫面範本。使用這些命令來建立標準檔案篩選政策，您可以將這些政策套用至多個資料夾。
3. 檔案畫面例外狀況命令 - 建立、擷取、修改和移除覆寫父資料夾中檔案篩選規則的檔案畫面例外狀況。當您需要允許特定子資料夾中的特定檔案類型，同時維持更廣泛的限制時，請使用這些命令。

檔案篩選 FSx 遠端 PowerShell 命令的清單

> **Note**
>
> 此頁面中的所有範例都假設您已使用檔案系統的 Windows Remote PowerShell 端點定義 `$FSxWindowsRemotePowerShellEndpoint`變數。您可以在檔案系統的詳細資訊頁面上的 Amazon FSx 主控台中找到此端點，或使用 AWS CLI `describe-file-systems`命令。

檔案畫面命令

New-FSxFSRMFileScreen

建立檔案畫面，封鎖使用者將指定類型的檔案儲存至資料夾。

參數：

- `Folder (string)` - 必要。要套用檔案畫面的資料夾路徑。
- `Description (string)` - 選用。檔案畫面的說明。
- `IncludeGroup (array)` - 選用。指定要封鎖或監控哪些檔案的檔案群組名稱陣列。
- `Active (boolean)` - 選用。如果設定為 true， 會建立封鎖檔案的作用中檔案畫面。如果設定為 false， 會建立僅監控檔案的被動檔案畫面。預設為 true。
- `Template (string)` - 選用。要使用的現有檔案畫面範本名稱。
- `NotificationConfigurations (array)` - 選用。當使用者嘗試儲存封鎖的檔案時，通知的組態陣列。每個組態都有下列屬性：
  - `ActionType (string)`：要執行的動作類型。您可以指定下列值：
    1. `Event`：將事件記錄到檔案系統的事件日誌。當您指定 Event 時，也必須指定下列屬性：
       - `EventType (string)`：資訊、警告或錯誤
       - `MessageBody (string)`：使用事件記錄的訊息文字。
    2. `Report`：產生儲存用量報告。當您指定報告時，也必須指定：
       - `ReportType (string)`：報告的類型。您可以指定下列值：`DuplicateFiles`、`FilesByFileGroup`、`FilesByOwner`、`FilesByProperty`、`LargeF` 或 `QuotaUsage`。

範例：

1. 建立封鎖音訊檔案的基本作用中檔案畫面。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMFileScreen -Folder "share\department" -IncludeGroup "Audio and Video
 Files"
}
```

2. 建立封鎖影片檔案的檔案畫面，並在使用者嘗試儲存影片檔案時產生事件日誌項目。

```
$notifications = [System.Collections.ArrayList]@()
$eventNotification = @{
    ActionType = "Event"
    EventType = "Warning"
    MessageBody = "File screen violation detected"
}
$null = $notifications.Add($eventNotification)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $notifications -ScriptBlock {
    param($notifications)
    New-FSxFSRMFileScreen -Folder "share\projects" -IncludeGroup "Audio and Video
 Files" -NotificationConfigurations $Using:notifications
}
```

Get-FSxFSRMFileScreen

從檔案系統擷取一或多個檔案畫面。

參數：

- `Folder (string)` - 選用。要從中擷取檔案畫面的資料夾路徑。如果您未指定資料夾路徑，命令會傳回檔案系統上的所有檔案畫面。

範例：

1. 擷取檔案系統上的所有檔案畫面。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMFileScreen
```

```
}
```

Set-FSxFSRMFileScreen

修改現有檔案畫面的屬性。

參數：

- `Folder (string)` - 必要。包含要修改之檔案畫面的資料夾路徑。
- `Description (string)` - 選用。檔案畫面的新描述。
- `IncludeGroup (array)` - 選用。新的檔案群組名稱陣列，定義要封鎖或監控哪些檔案。
- `Active (boolean)` - 選用。如果設定為 true，會將檔案畫面設定為作用中模式（封鎖）。如果設定為 false，會將檔案畫面設定為被動模式（僅限監控）。預設為 true。
- `NotificationConfigurations (array)` - 選用。新的通知組態陣列。
- `PassThru (boolean)` - 選用。如果設定為 true，會傳回修改過的檔案畫面物件。

範例：

1. 修改檔案畫面的說明和檔案群組。

```
$includeGroups = @("Audio and Video Files")
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $includeGroups -ScriptBlock {
    param($includeGroups)
    Set-FSxFSRMFileScreen -Folder "share\projects" -Description "Updated screen" -
IncludeGroup $includeGroups
}
```

2. 將檔案畫面設定為作用中模式並新增通知。

```
$notifications = [System.Collections.ArrayList]@()
$eventNotification = @{
    ActionType = "Event"
    EventType = "Warning"
    MessageBody = "File screen violation detected"
}
$null = $notifications.Add($eventNotification)
```

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $notifications -ScriptBlock {
    param($notifications)
    Set-FSxFSRMFileScreen -Folder "share\projects" -Active: $true -
NotificationConfigurations $Using:notifications -PassThru
}
```

Remove-FSxFSRMFileScreen

從指定的資料夾移除檔案畫面。

參數：

- `Folder (string)` - 必要。要從中移除檔案畫面的資料夾路徑。
- `PassThru (boolean)` - 選用。如果設定為 true， 會傳回移除的檔案畫面物件。

範例：

1. 從特定資料夾移除檔案畫面。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Remove-FSxFSRMFileScreen -Folder "share\projects" -PassThru
}
```

Reset-FSxFSRMFileScreen

重設檔案畫面以符合指定範本的設定。

參數：

- `Folder (string)` - 必要。包含要重設之檔案畫面的資料夾路徑。
- `Template (string)` - 必要。要套用的現有檔案畫面範本名稱。

範例：

1. 重設檔案畫面以符合檔案畫面範本中定義的設定。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Reset-FSxFSRMFileScreen -Folder "share\department" -Template "Block Audio Files"
}
```

檔案畫面範本命令

Get-FSxFSRMFileScreenTemplate

`Get-FSxFSRMFileScreenTemplate` 命令會從檔案系統擷取一或多個檔案畫面範本。

Parameters

- `Name (array)` - 選用。要擷取的檔案畫面範本名稱陣列。如果您未指定名稱，命令會傳回檔案系統上的所有檔案畫面範本。

範例

1. 擷取所有檔案畫面範本。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMFileScreenTemplate
}
```

New-FSxFSRMFileScreenTemplate

`New-FSxFSRMFileScreenTemplate` 命令會建立檔案畫面範本，以定義檔案畫面的可重複使用組態。範本會指定要封鎖的檔案群組，以及在使用者嘗試儲存封鎖的檔案時要產生的通知。

Parameters

- `Name (string)` - 必要。檔案畫面範本的名稱。
- `Description (string)` - 選用。檔案畫面範本的說明。
- `IncludeGroup (array)` - 選用。指定要封鎖或監控哪些檔案的檔案群組名稱陣列。
- `Active (boolean)` - 選用。如果設定為 true， 會建立封鎖檔案的作用中檔案畫面範本。如果設定為 false， 會建立僅監控檔案的被動範本。預設為 true。

- NotificationConfigurations (array) - 選用。當使用者嘗試儲存封鎖的檔案時，通知的組態陣列。每個組態都有下列屬性：
  - ActionType (string)：要執行的動作類型。您可以指定下列值：
    1. Event：將事件記錄到檔案系統的事件日誌。當您指定事件時，也必須指定下列屬性：
       - EventType (string)：資訊、警告或錯誤
       - MessageBody (string)：使用事件記錄的訊息文字。
    2. Report：產生儲存用量報告。當您指定報告時，您還必須指定：
       - ReportType (string)：報告的類型。您可以指定下列值：DuplicateFiles、FilesByFileGroup、FilesByOwner、FilesByProperty、LargeF LeastRecentlyAccessed或 QuotaUsage

範例

1. 使用通知建立檔案畫面範本。

```
$notifications = [System.Collections.ArrayList]@()
$eventNotif = @{
    ActionType = "Event"
    EventType = "Warning"
    MessageBody = "Blocked file detected"
}
$null = $notifications.Add($eventNotif)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $notifications -ScriptBlock {
    param($notifications)
    New-FSxFSRMFileScreenTemplate -Name "Block Executables" -Description
 "Blocks executable files" -IncludeGroup "Executable Files" -Active: $true -
NotificationConfigurations $Using:notifications
}
```

Remove-FSxFSRMFileScreenTemplate

Remove-FSxFSRMFileScreenTemplate 命令會從檔案系統移除一或多個檔案畫面範本。當您移除範本時，從該範本建立的檔案畫面保持不變。

Parameters

- Name (array) - 必要。要移除的檔案畫面範本名稱陣列。

- PassThru (boolean) - 選用。如果設定為 true， 會傳回移除的檔案畫面範本物件。

範例

1. 移除單一檔案畫面範本。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Remove-FSxFSRMFileScreenTemplate -Name "Block Executables" -PassThru
}
```

Set-FSxFSRMFileScreenTemplate

Set-FSxFSRMFileScreenTemplate 命令會修改現有檔案畫面範本的屬性。選擇性地更新使用修改範本建立的檔案畫面。

Parameters

- Name (array) - 必要。要修改的檔案畫面範本名稱陣列。
- Description (string) - 選用。範本的新描述。
- IncludeGroup (array) - 選用。新的檔案群組名稱陣列，定義要封鎖或監控哪些檔案。
- Active (boolean) - 選用。如果設定為 true，請將範本設定為作用中模式 （封鎖）。如果設定為 false，請將範本設定為被動模式 （監控）。預設為 true。
- NotificationConfigurations (array) - 選用。新的通知組態陣列。
- UpdateDerived (boolean) - 選用。如果設為 true， 會更新從此範本建立的所有現有檔案畫面，無論這些檔案畫面進行任何修改。
- UpdateDerivedMatching (boolean) - 選用。如果設為 true，則 只會更新從此範本建立以來尚未修改的檔案畫面。
- PassThru (boolean) - 選用。如果設定為 true， 會傳回修改過的檔案畫面範本物件。

範例

1. 使用新的檔案群組更新檔案畫面範本。

```
$includeGroups = @("Audio and Video Files")
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $includeGroups -ScriptBlock {
```

```
    param($includeGroups)
    Set-FSxFSRMFileScreenTemplate -Name "Block Executables" -IncludeGroup
 $includeGroups
}
```

2. 將檔案畫面範本更新為作用中模式，並更新所有衍生的檔案畫面。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMFileScreenTemplate -Name "Block Executables" -Active: $true -
UpdateDerived
}
```

檔案畫面例外命令

New-FSxFSRMFileScreenException

New-FSxFSRMFileScreenException 命令會建立檔案畫面例外狀況，以覆寫任何原本會套用至資料夾及其所有子資料夾的檔案篩選規則。這允許在例外狀況資料夾中建立特定檔案類型，即使它們被父資料夾中的檔案畫面封鎖。

Parameters

- Folder (string) - 必要。套用檔案畫面例外狀況的資料夾路徑。例外狀況適用於此資料夾及其所有子資料夾。
- Description (string) - 選用。檔案畫面例外狀況的說明。
- IncludeGroup (array) - 選用。檔案群組名稱陣列，指定無論從父資料夾套用的任何封鎖檔案畫面，允許哪些檔案。

範例

1. 針對特定資料夾和檔案群組建立檔案畫面例外狀況。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMFileScreenException -Folder "share\department" -IncludeGroup "Text
 Files"
}
```

2. 使用多個檔案群組建立檔案畫面例外狀況。

```
$includeGroups = @("Audio and Video Files", "Documents")
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $includeGroups -ScriptBlock {
    param($includeGroups)
    New-FSxFSRMFileScreenException -Folder "share\projects" -Description "Allow media
 files in project folder" -IncludeGroup $includeGroups
    }
```

Get-FSxFSRMFileScreenException

`Get-FSxFSRMFileScreenException` 命令會從檔案系統擷取一或多個檔案畫面例外狀況。

Parameters

- `Folder (string)` - 選用。要從中擷取檔案畫面例外狀況的資料夾路徑。如果您未指定資料夾路徑，命令會傳回檔案系統上的所有檔案畫面例外狀況。

範例

1. 擷取檔案系統上的所有檔案畫面例外狀況。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMFileScreenException
}
```

2. 擷取特定資料夾的檔案畫面例外狀況。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMFileScreenException -Folder "share\department"
}
```

Remove-FSxFSRMFileScreenException

`Remove-FSxFSRMFileScreenException` 命令會從指定的資料夾移除檔案畫面例外狀況。移除後，資料夾及其子資料夾將受到先前被例外狀況覆寫之父資料夾的任何檔案篩選規則的約束。

Parameters

- `Folder (string)` - 必要。要從中移除檔案畫面例外狀況的資料夾路徑。

- PassThru (boolean) - 選用。如果設定為 true， 會傳回移除的檔案畫面例外狀況物件。

範例

1. 從特定資料夾移除檔案畫面例外狀況。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Remove-FSxFSRMFileScreenException -Folder "share\projects" -PassThru
}
```

Set-FSxFSRMFileScreenException

Set-FSxFSRMFileScreenException 命令會修改檔案畫面例外狀況的屬性。

Parameters

- Folder (string) - 必要。包含要修改的檔案畫面例外狀況的資料夾路徑。
- Description (string) - 選用。檔案畫面例外狀況的新描述。
- IncludeGroup (array) - 選用。新的檔案群組名稱陣列，定義無論從父資料夾套用的任何封鎖檔案畫面，要允許哪些檔案。
- PassThru (boolean) - 選用。如果設定為 true， 會傳回修改過的檔案畫面例外狀況物件。

範例

1. 更新檔案畫面例外狀況的允許檔案群組。

```
$includeGroups = @("Audio and Video Files")
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $includeGroups -ScriptBlock {
    param($includeGroups)
    Set-FSxFSRMFileScreenException -Folder "share\projects" -IncludeGroup
 $includeGroups -PassThru
}
```

檔案分類

檔案分類會根據檔案的內容、位置或其他屬性，自動將中繼資料屬性指派給檔案。分類可協助您組織檔案、強制執行資料管理政策，以及識別包含敏感資訊、屬於特定商業類別或需要保留期間的檔案，以符合合規要求。

檔案分類的運作方式

檔案分類使用三個步驟的程序：

1. 定義屬性 - 建立分類屬性定義，以指定您要指派給檔案的中繼資料類型，例如 "Data Sensitivity"或 "ContainsPII"。
2. 建立規則 - 設定分類規則，根據您指定的條件自動將屬性值指派給檔案，例如檔案內容模式或資料夾位置。例如，包含社會安全號碼等模式的檔案(XXX-XX-XXXX)可以自動分類為 ContainsPII=Yes。
3. 執行分類 - 執行分類程序以掃描檔案並套用規則。您可以視需要、排程或在背景持續執行分類。

分類完成後，您可以使用指派的屬性來產生儲存報告、套用 檔案管理任務，或搜尋具有特定特性的檔案。

分類屬性定義

分類屬性定義會指定可指派給檔案的中繼資料類型。每個屬性定義都有名稱、屬性類型，以及選用的允許值清單。例如，您可以建立名為 的屬性，"Data Sensitivity"其中包含 OrderedList 類型和可能的值：Public、Confidential、 Internal和 Restricted。

支援下列屬性類型：

- OrderedList - 排序清單，其中值具有特定序列 （例如，低、中、高）。當值的順序對於報告或政策決策很重要時，請使用此類型。
- MultiChoice - 允許從清單中選取多個值 （例如，檔案可能同時標記「財務」和「法律」類別）。
- SingleChoice - 僅允許從清單中選取一個值。
- String - 沒有預先定義選項的單一文字值。
- MultiString - 沒有預先定義選項的多個文字值。
- Integer - 數值。
- YesNo - 布林值 (true 或 false)。
- DateTime - 日期和時間值。

屬性定義可在多個分類規則中重複使用。建立屬性定義之後，您可以在需要為該屬性指派值的任何分類規則中參考它。

分類規則

分類規則會定義邏輯，以自動將屬性值指派給檔案。每個規則指定：

- 要設定的屬性
- 要指派給該屬性的值
- 套用規則的位置 （ 哪些資料夾 ）
- 如何識別應該接收屬性值的檔案。您可以使用兩種分類機制：

內容分類器

內容分類器會掃描特定文字模式或規則表達式的檔案內容。使用此機制根據檔案所包含的內容來識別檔案。內容分類器提供三種比對檔案內容的方式：

- `ContentString` - 搜尋不區分大小寫的文字字串。當您想要尋找特定的單字或片語，無論大小寫為何，都可以使用此選項。例如，搜尋「機密」將符合「機密」、「機密」和「機密」。
- `ContentStringCaseSensitive` - 搜尋區分大小寫的文字字串。當大寫對您的搜尋很重要時，請使用此選項。例如，搜尋 "SSN" 將符合 "SSN"，但不符合 "ssn" 或 "Ssn"。這適用於首字母縮寫詞、產品代碼或其他識別符，其中大小寫很重要。
- `ContentRegularExpression` - 使用規則表達式搜尋模式。當您需要比對複雜的模式或變數格式時，請使用此選項。例如，您可以使用規則表達式來偵測：
  - 格式為 123-45-6789 的社會安全號碼： `\b\d{3}-\d{2}-\d{4}\b`
  - 具有選用空格或破折號的信用卡號碼： `\b\d{4}[\s-]?\d{4}[\s-]?\d{4}[\s-]?\d{4}\b`
  - 電子郵件地址、電話號碼或其他結構化資料

您可以在單一規則中指定多個字串或模式，如果檔案的內容符合任何指定的值，則會分類檔案。

資料夾分類器

資料夾分類器會根據檔案的存放位置指派屬性值。使用此機制，依檔案在資料夾階層中的位置來分類檔案。例如：

- 設定法務文件資料夾中所有檔案的保留期間屬性
- 使用專案識別符標記特定專案資料夾中的所有檔案

此外，您可以使用 ReevaluateProperty 參數來控制分類在具有 屬性值的檔案上執行時會發生的情況。您可以選取下列組態：

- Never - 僅分類沒有此屬性值的檔案
- Overwrite - 當檔案變更時取代現有的值
- Aggregate - 結合新值與現有值 （適用於多值屬性）

管理屬性

管理屬性是套用至資料夾而非檔案的分類屬性。您可以使用管理屬性來整理和分類檔案系統階層中的資料夾。與透過分類規則自動指派的檔案屬性不同，您可以使用 Set-FSxFSRMMgmtProperty命令手動設定管理屬性。

若要分類資料夾，請使用 FolderUsage_MS 屬性。您可以指定下列值：

- User Files
- Group Share
- Application Files
- Backup and Archival

執行分類

您可以透過三種方式執行檔案分類：

1. 手動分類 - Start-FSxFSRMClassification用於立即執行分類。此方法適用於測試新規則或執行一次性分類任務。
2. 排程分類 - Set-FSxFSRMClassification用於設定自動分類的排程。您可以排定每週或每月在特定時間執行分類。排程分類適用於您想要定期、可預測的分類執行的大多數生產環境。
3. 持續分類 - Set-FSxFSRMClassification搭配 Continuous 參數使用，以啟用持續執行的背景分類。持續分類會在新檔案和修改後檔案建立或變更後立即自動分類。此方法提供up-to-date分類，但會耗用更多系統資源。

當您開始分類時，您可以指定 RunDuration來限制程序執行的時間長度。如果分類未在指定的時間內完成，它會在下一次排定的執行期間或當您再次手動啟動時停止並繼續。

分類完成後，您可以在 Windows File Explorer 中的檔案上按一下滑鼠右鍵，選取屬性，然後選擇分類索引標籤，以檢視指派給檔案的分類屬性。此索引標籤會顯示檔案的所有分類屬性及其值。

分類程序管理

您可以使用下列命令來監控和控制分類程序：

- Get-FSxFSRMClassification - 檢查分類的目前狀態 (Running、NotRunning、 Queued或 Unknown)
- Stop-FSxFSRMClassification - 停止執行中或已排入佇列的分類任務
- Wait-FSxFSRMClassification - 暫停指令碼執行，直到分類完成或逾時過期

使用這些命令來協調與其他任務的分類。例如，在產生取決於分類檔案屬性的儲存報告之前，您可以等待分類完成。

分類最佳實務

遵循這些最佳實務，以確保有效率且有效的檔案分類。

1. 效能考量

內容型分類需要大量資源，因為 FSRM 必須讀取和掃描檔案內容。

- 先測試小型資料集上的規則 - 將分類規則套用至整個檔案系統之前，請在代表性的檔案範例上對其進行測試，以驗證它們是否如預期運作，並估計分類需要多長時間。
- 限制內容掃描範圍 - 內容型分類需要大量資源，因為它需要讀取檔案內容。使用 Namespace 參數將規則限制在特定資料夾，而不是掃描整個檔案系統。
- 盡可能使用資料夾分類 - 資料夾分類器比內容分類器快得多，因為它不需要讀取檔案內容。當檔案可根據其位置進行分類時，請使用資料夾分類器而非內容分類器。
- 在離峰時間排程分類 - 在低系統活動期間執行排程分類，將對使用者效能的影響降至最低。避免在備份時段或其他維護任務期間執行分類。
- 設定適當的 RunDuration 限制 - 使用 RunDuration 參數防止分類執行太長並影響系統效能。如果分類未在時間限制內完成，則會在下一次排定的執行期間繼續。
- 監控分類效能 - Get-FSxFSRMClassification用來檢查分類狀態，並識別分類是否花費超過預期的時間。長時間執行的分類可能表示規則需要最佳化，或系統需要更多資源。

2. 規則設計

- 使用特定的規則表達式 - 使用 時ContentRegularExpression，請盡可能具體地寫入模式，以避免錯誤相符。在生產環境中部署規則表達式之前，請徹底測試規則表達式。

- 有效率地結合多個模式 - 將它們合併為具有多個 `ContentString`或 `ContentRegularExpression`值的單一規則，而不是為類似的模式建立單獨的規則。這可減少 FSRM 掃描每個檔案所需的次數。
- 排除不必要的資料夾 - 使用 中的 `ExcludeNamespace` 參數`Set-FSxFSRMClassification`來排除暫時目錄，以及其他不需要分類的位置。

3. 屬性管理

- 規劃您的屬性結構描述 - 在建立規則之前設計您的分類屬性。考慮報告、合規和檔案管理政策所需的屬性。
- 文件屬性定義 - 使用描述欄位來說明每個屬性的含義及其使用方式。這有助於其他管理員了解您的分類結構描述。

4. 持續維護

- 定期檢閱分類結果 - 產生儲存報告，以驗證分類是否如預期運作，以及檔案是否收到正確的屬性值。
- 視需要更新規則 - 隨著組織的資料管理需求變更，請更新分類規則以反映新的政策或合規需求。
- 清除未使用的屬性 - 移除不再需要的屬性定義和規則，以維持分類組態的可管理性。

分類管理命令

您可以存取四個 FSx 遠端 PowerShell 命令系列來管理檔案分類：

1. 屬性定義命令 - 建立和管理分類屬性定義，以指定您可以指派給檔案的中繼資料類型。
2. 分類規則命令 - 建立和管理根據檔案內容或位置指派屬性值的自動分類規則。
3. 管理屬性命令 - 在資料夾而非檔案上設定和擷取分類屬性。
4. 分類程序命令 - 啟動、停止、監控和設定分類程序。

檔案分類 FSx 遠端 PowerShell 命令的清單

> **Note**
>
> 此頁面中的所有範例皆假設您已使用檔案系統的 Windows Remote PowerShell 端點定義 `$FSxWindowsRemotePowerShellEndpoint`變數。您可以在檔案系統的詳細資訊頁面上的 Amazon FSx 主控台中找到此端點，或使用 AWS CLI `describe-file-systems`命令。

屬性定義命令

New-FSxFSRMClassificationPropertyDefinition

New-FSxFSRMClassificationPropertyDefinition：建立可用於分類檔案的分類屬性定義。屬性定義定義可透過分類規則指派給檔案的屬性。

參數：

- Name (string) - 必要。屬性定義的名稱。
- DisplayName (string) - 選用。屬性定義的顯示名稱。
- Description (string) - 選用。屬性定義的描述。
- Type (string) - 必要。分類屬性的類型。您可以指定下列值：
  - OrderedList：可能值的排序清單
  - MultiChoice：從可能的值中選擇多個選項
  - SingleChoice：可能值的單一選擇
  - String：單一文字字串
  - MultiString：多個文字字串
  - Integer：數值
  - YesNo：布林值
  - DateTime：日期和時間值
- PossibleValueConfigurations (array) - 選用。OrderedList、MultiChoice 或 SingleChoice 屬性類型的組態陣列。每個組態都有下列屬性：
  - Name (string)：值的名稱 (必要)
  - Description (string)： 值的描述 (選用)
- Parameters (array) - 選用。用於其他組態的"name=value"格式字串陣列。

範例：

1。建立 PII 資料的屬性清單。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationPropertyDefinition -Name "ContainsPII" -Type OrderedList -
PossibleValueConfigurations @(
            @{ Name = "Yes" },
```

```
            @{ Name = "No" })
}
```

2. 建立資料敏感度的排序清單屬性。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationPropertyDefinition -Name "DataSensitivity" -Type
 OrderedList -PossibleValueConfigurations @(
            @{ Name = "Public" },
            @{ Name = "Internal" },
            @{ Name = "Confidential" },
            @{ Name = "Restricted" }
        )
}
```

Get-FSxFSRMClassificationPropertyDefinition

`Get-FSxFSRMClassificationPropertyDefinition`：從您的檔案系統擷取一或多個分類屬性定義。

參數：

- `Name (array)` - 選用。要擷取的屬性定義名稱陣列。如果您未指定名稱，命令會傳回檔案系統上的所有屬性定義。

範例：

1。擷取檔案系統上的所有分類屬性定義。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMClassificationPropertyDefinition
}
```

Set-FSxFSRMClassificationPropertyDefinition

修改現有分類屬性定義的屬性。

Parameters

- `Name (array)` - 必要。要修改的屬性名稱陣列。

- DisplayName (string) - 選用。屬性定義的新顯示名稱。
- Description (string) - 選用。屬性定義的新描述。
- PossibleValueConfigurations (array) - 選用。OrderedList、MultiChoice 或 SingleChoice 屬性的新組態陣列。每個組態都有下列屬性：
  - Name (string)：值的名稱（必要）
  - Description (string)：值的描述（選用）
- Parameters (array) - 選用。"name=value" 格式的新字串陣列。
- PassThru (boolean) - 選用。如果設定為 true，會傳回修改過的屬性定義物件。

範例：

1. 使用現有屬性定義的描述更新可能的值。

```
$values = [System.Collections.ArrayList]@()
$null = $values.Add(@{
    Name = "High"
    Description = "High Risk Content"
})
$null = $values.Add(@{
    Name = "Medium"
    Description = "Medium Risk Content"
})

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $values -ScriptBlock {
    param($values)
    Set-FSxFSRMClassificationPropertyDefinition -Name "RiskLevel" -
PossibleValueConfigurations $Using:values -PassThru
}
```

Remove-FSxFSRMClassificationPropertyDefinition

從檔案系統移除一或多個分類屬性定義。只能移除本機定義的屬性定義。

Parameters

- Name (array) - 必要。要移除的屬性名稱陣列。
- PassThru (boolean) - 選用。如果設定為 true，會傳回移除的屬性定義物件。

範例：

1. 移除單一屬性定義。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Remove-FSxFSRMClassificationPropertyDefinition -Name "RiskLevel" -PassThru
}
```

分類規則命令

New-FSxFSRMClassificationRule

建立自動分類規則，根據指定的條件將屬性值指派給檔案。每個規則都會為單一屬性設定值。

Parameters

- Name (string) - 必要。分類規則的名稱。
- Description (string) - 選用。分類規則的描述。
- Property (string) - 必要。要設定的分類屬性名稱。必須是現有的屬性定義名稱。
- PropertyValue (string) - 選用。要指派給 屬性的值。必須對指定的分類機制有效。
- Namespace (array) - 必要。套用規則的路徑或資料夾類型陣列。
- Disabled (boolean) - 選用。如果設定為 true， 會以停用狀態建立規則。
- ReevaluateProperty (string) - 選用。指定何時重新評估檔案。您可以指定下列值：
  - Never：僅評估沒有現有屬性值的檔案
  - Overwrite：當檔案變更並覆寫現有值時重新評估
  - Aggregate：當檔案變更並與現有值結合時，重新評估
- Flags (array) - 選用。指定規則的特殊行為。您可以指定下列值：
  - ClearAutomaticallyClassifiedProperty
  - ClearManuallyClassifiedProperty
  - Deprecated
- ContentRegularExpression (array) - 選用。符合檔案內容的規則表達式陣列。
- ContentString (array) - 選用。在檔案內容中搜尋的不區分大小寫字串陣列。
- ClassificationMechanism (string) - 必要。用於分類檔案的機制。您可以指定下列值：

  - `Content Classifier`：掃描特定字串或規則表達式模式的檔案內容。當您指定內容分類器時，您可以使用 ContentString、ContentStringCaseSensitive 或 ContentRegularExpression 參數來定義要搜尋的內容。
  - `Folder Classifier`：根據檔案的資料夾位置分類檔案
- `Parameters (array)` - 選用。用於其他組態的"name=value"字串陣列。

範例：

1. 使用常規表達式偵測社會安全號碼。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationRule -Name "Detect_SSN" -Property "ContainsPII" -
PropertyValue "Yes" -Namespace "share" -ClassificationMechanism "Content Classifier" -
ContentRegularExpression "\b\d{3}-\d{2}-\d{4}\b"
}
```

2. 使用一般運算式偵測信用卡號碼。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationRule -Name "Detect_CreditCard" -Property "ContainsPII" -
PropertyValue "Yes" -Namespace "share" -ClassificationMechanism "Content Classifier" -
ContentRegularExpression "\b\d{4}[\s-]?\d{4}[\s-]?\d{4}[\s-]?\d{4}\b"
}
```

3. 在具有 7 年保留期屬性的資料夾下分類每個檔案。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationRule -Name "Contracts_Records_7Year" -Property
 "RetentionPeriod" -PropertyValue "7 years" -Namespace "share/Legal Documents" -
ClassificationMechanism "Folder Classifier"
}
```

Get-FSxFSRMClassificationRule

從檔案系統擷取一或多個分類規則。

Parameters

- Name (array) - 選用。要擷取的分類規則名稱陣列。如果您未指定名稱，命令會傳回檔案系統上的所有規則。

範例：

1. 擷取檔案系統上的所有分類規則。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMClassificationRule
}
```

Set-FSxFSRMClassificationRule

修改現有分類規則的屬性。

Parameters

- Name (array) - 必要。要修改的分類規則名稱陣列。
- Description (string) - 選用。規則的新描述。
- Property (string) - 選用。要設定的分類屬性名稱。
- PropertyValue (string) - 選用。要指派給 屬性的新值。
- Namespace (array) - 選用。套用規則的新路徑或資料夾類型陣列。
- Disabled (boolean) - 選用。如果設為 true， 會停用規則。如果設定為 false，則 會啟用規則。
- ReevaluateProperty (string) - 選用。變更何時重新評估檔案。您可以指定下列值：
  - Never：僅評估沒有現有屬性值的檔案
  - Overwrite：當檔案變更並覆寫現有值時重新評估
  - Aggregate：重新評估檔案何時變更並與現有值結合
- Flags (array) - 選用。規則的新特殊行為。您可以指定下列值：
  - ClearAutomaticallyClassifiedProperty
  - ClearManuallyClassifiedProperty
  - Deprecated
- ContentRegularExpression (array) - 選用。新的規則表達式陣列。
- ContentString (array) - 選用。不區分大小寫的新搜尋字串陣列。

- ContentStringCaseSensitive (array) - 選用。區分大小寫的新搜尋字串陣列。
- ClassificationMechanism (string) - 選用。要使用的新分類機制。您可以指定下列值：
  - Content Classifier：掃描特定字串或規則表達式模式的檔案內容。當您指定內容分類器時，您可以使用 ContentString、ContentStringCaseSensitive 或 ContentRegularExpression 參數來定義要搜尋的內容。
  - Folder Classifier：根據檔案的資料夾位置分類檔案
- Parameters (array) - 選用。新的"name=value"組態字串陣列。
- PassThru (boolean) - 選用。如果設定為 true，會傳回修改過的規則物件。

範例：

1. 更新現有分類規則的規則屬性和命名空間。

```
$namespaces = @("share\finance", "share\accounting")

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $namespaces -ScriptBlock {
    param($namespaces)
    Set-FSxFSRMClassificationRule -Name "Detect_CreditCard" -Description "Updated PII
 detection" -Namespace $Using:namespaces -ReevaluateProperty "Overwrite"
}
```

Remove-FSxFSRMClassificationRule

從您的檔案系統移除一或多個分類規則。

Parameters

- Name (array) - 必要。要移除的分類規則名稱陣列。
- PassThru (boolean) - 選用。如果設定為 true，會傳回移除的規則物件。

範例：

1. 移除單一分類規則。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Remove-FSxFSRMClassificationRule -Name "Find Confidential Files" -PassThru
```

```
}
```

管理屬性命令

Get-FSxFSRMMgmtProperty

從指定的資料夾擷取管理屬性。管理屬性是套用至資料夾而非檔案的分類屬性。

Parameters

- Namespace (string) - 選用。資料夾的路徑。
- Name (string) - 選用。要擷取的管理屬性名稱。如果您未指定名稱，命令會擷取所有管理屬性。
- Recurse (boolean) - 選用。如果設定為 true， 會擷取命名空間內所有資料夾的管理屬性。需要命名空間參數。
- Effective (boolean) - 選用。如果設定為 true， 會擷取具有指定名稱之最近資料夾的管理屬性。搜尋包含指定的命名空間及其父階層。需要 Name 參數。

範例：

1. 擷取檔案系統上的所有管理屬性。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMMgmtProperty
}
```

2. 擷取特定資料夾的管理屬性。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMMgmtProperty -Namespace "share\department"
}
```

Remove-FSxFSRMMgmtProperty

從指定的資料夾移除管理屬性。

Parameters

- Namespace (string) - 選用。資料夾的路徑。

- Name (string) - 必要。要移除的管理屬性名稱。
- Recurse (boolean) - 選用。如果設定為 true，會移除命名空間內所有資料夾的管理屬性。需要命名空間參數。

範例：

1. 移除管理屬性的所有執行個體。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Remove-FSxFSRMMgmtProperty -Name "FolderUsage_MS"
}
```

2. 從特定資料夾移除管理屬性。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Remove-FSxFSRMMgmtProperty -Name "FolderUsage_MS" -Namespace "share\department"
}
```

Set-FSxFSRMMgmtProperty

變更指定命名空間的管理屬性值。管理屬性是套用至資料夾的分類屬性，且未設定安全旗標。

Parameters

- Namespace (string) - 選用。資料夾路徑。
- Name (string) - 必要。要修改的管理屬性名稱。必須是套用至資料夾的現有分類屬性。
- Value (string) - 必要。要指派給管理屬性的新值。

範例：

1. 設定資料夾用量屬性。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMMgmtProperty -Namespace "share\department" -Name "FolderUsage_MS" -Value
 "User Files"
```

```
}
```

分類程序命令

Get-FSxFSRMClassification

擷取執行中檔案分類程序的狀態。狀態可以是下列其中一個值：

- Unknown：無法判斷分類狀態
- NotRunning：目前沒有正在執行的分類
- Queued：分類已排入佇列以啟動
- Running：分類目前正在進行中

Parameters

無

範例：

1. 擷取目前的分類狀態。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMClassification
}
```

Start-FSxFSRMClassification

啟動檔案分類程序，將分類規則套用至檔案並產生分類報告。

Parameters

- Queue (boolean) - 選用。如果設定為 true， 會將分類任務新增至佇列，以便在接下來的 5 分鐘內執行。在此期間排入佇列的任何任務都會一起執行。如果設定為 false 或未指定，分類會立即開始。
- RunDuration (number) - 選用。指定分類程序在取消之前應執行多少小時。有效值：-1 到 2147483。特殊值：
  - -1：執行 直到取消

- 0：執行 以完成
- 如果未指定， 會執行 直到完成。

範例：

1. 開始分類，沒有時間限制。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Start-FSxFSRMClassification -RunDuration 0
}
```

Stop-FSxFSRMClassification

停止檔案系統上任何執行中或已排入佇列的分類任務。

Parameters

無

範例：

1. 停止執行中的分類。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Stop-FSxFSRMClassification
}
```

Wait-FSxFSRMClassification

等待檔案分類程序完成。當您需要執行取決於分類完成的動作時，例如根據分類檔案產生報告時，請使用此命令。

Parameters

- Timeout （number）- 選用。指定分類完成的等待時間，以秒為單位。如果逾時在分類完成之前過期，則命令會傳回 ，但分類會在背景中繼續執行。有效值：-1 到 2147483。特殊值：
  - -1：無限期等待分類完成 （ 預設 ）
  - 0：檢查目前狀態並立即傳回，無需等待

範例：

1. 無限期等待分類完成。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Wait-FSxFSRMClassification
}
```

Set-FSxFSRMClassification

修改檔案分類的組態設定。

Parameters

- ExcludeNamespace (array) - 選用。要從分類中排除的其他資料夾陣列。
- ScheduleConfigurations (hashtable) - 選用。包含具有下列屬性的排程組態的雜湊：
  - Time (datetime)：指定何時執行任務的 DateTime 物件（必要）
  - RunDuration (number)：執行任務的時數（選用）
  - Weekly (array)：工作日陣列（選用）
  - Monthly (array)：月份的陣列，最後一天使用 -1（選用）
- Continuous (boolean) - 選用。如果設定為 true，會啟用連續背景分類。
- PassThru (boolean) - 選用。如果設定為 true，會傳回修改過的分類組態物件。

範例：

1. 啟用持續分類。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMClassification -Continuous $true
}
```

2. 設定每週排程來執行分類。

```
$schedule = @{
    Time = ("12:00am")
    Weekly = @('Monday', 'Wednesday', 'Friday')
}
```

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $schedule -ScriptBlock {
    param($schedule)
    Set-FSxFSRMClassification -ScheduleConfigurations $schedule
}
```

3. 設定具有自訂排除的每月排程。

```
$schedule = @{
    Time = ("12:00am")
    Monthly = @(1, 15, -1) # 1st, 15th, and last day
    RunDuration = 4
}
$excludeNamespaces = @("share\folder /s")

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList @($schedule, $excludeNamespaces) -ScriptBlock {
    param($schedule, $excludeNamespaces)
    Set-FSxFSRMClassification -ScheduleConfigurations $schedule -ExcludeNamespace
 $excludeNamespaces
}
```

儲存報告

儲存報告提供檔案系統用量的詳細分析，協助您了解儲存的使用方式、識別可封存或刪除的檔案，以及監控檔案管理政策的合規性。您可以產生多種類型的報告，以分析檔案所有權、檔案類型、重複檔案、大型檔案、檔案篩選和配額用量。

報告類型

您可以建立下列報告類型：

- `DuplicateFiles`

  根據檔案大小和雜湊比較，識別具有相同內容的檔案。使用此報告來尋找耗用不必要的儲存空間的備援檔案。報告會將重複的檔案分組在一起，並顯示可透過移除重複項目來復原的總空間。

- `FilesByFileGroup`

  依檔案群組成員資格將檔案分組，並顯示每個檔案群組的儲存使用量。使用此報告來了解哪些類型的檔案（文件、媒體、可執行檔等）會耗用最多的儲存空間。

- FilesByOwner

  依擁有者分組檔案，並顯示每個使用者或群組使用的儲存空間。使用此報告來識別耗用最多儲存空間的使用者，並適當地配置儲存成本或配額。

- FilesByProperty

  依屬性值分類檔案，並顯示每個屬性值的檔案計數和儲存體耗用。使用此報告根據檔案的分類進行分析，例如資料敏感程度、部門或保留期。此報告需要使用 分類檔案分類規則。

- FileScreenAuditFiles

  列出使用者嘗試儲存作用中檔案畫面封鎖之檔案的檔案篩選違規。使用此報告來監控檔案篩選政策的合規性，並識別經常嘗試儲存未經授權檔案類型的使用者。

- FoldersByProperty

  依管理屬性值將資料夾分組，並顯示每個屬性值的儲存耗用量。使用此報告依資料夾用途分析儲存體用量，例如使用者檔案、群組共用或應用程式檔案。

- LargeFiles

  列出超過指定大小閾值的檔案。使用此報告來識別耗用大量儲存空間的檔案，這些檔案可能是封存、壓縮或刪除的候選項目。

- LeastRecentlyAccessed

  列出指定天數內未存取的檔案。使用此報告來識別可以封存或移至低成本儲存層的非作用中檔案。

- MostRecentlyAccessed

  列出在指定天數內存取的檔案。

- QuotaUsage

  顯示已設定配額之資料夾的配額用量統計資料。使用此報告來監控配額合規性，並識別接近配額限制的資料夾。

報告格式

您可以產生多種格式的報告，以符合不同的使用案例：

- DHTML - 動態 HTML 格式，具有排序和篩選等互動式功能。
- HTML - 適合封存或傳送電子郵件的靜態 HTML 格式。
- XML - 用於程式設計處理的結構化資料格式。

- CSV - 用於匯入試算表應用程式的逗號分隔值格式。
- Text - 用於簡單檢視或處理的純文字格式。

您可以為單一報告指定多種格式。

互動式和排程報告

您可以建立兩種類型的儲存報告：

1. 互動式報告 - 建立時立即執行，且僅執行一次。使用互動式報告進行臨機操作分析或故障診斷。互動式報告沒有排程，無法在建立後修改。若要執行另一個互動式報告，您必須使用不同的名稱建立新的報告。
2. 排程報告 - 根據設定的排程自動執行。使用排程報告進行定期監控和合規報告。您可以排定報告在特定時間每週或每月執行。排程的報告可以修改以變更其組態，您也可以使用 Start-FSxFSRMStorageReport命令隨需執行，而無需等待排程時間。

執行報告

建立排程報告之後，您可以透過多種方式執行報告：

- 自動執行 - 排程報告會在設定的排程時間自動執行。
- 手動執行 - Start-FSxFSRMStorageReport用於隨需執行排程報告，而無需等待排程時間。

您可以使用 監控報告執行，Get-FSxFSRMStorageReport以檢查狀態。

存取儲存報告

FSRM 產生儲存報告後，報告檔案會儲存到檔案系統的預設位置。若要存取這些報告，您需要映射檔案系統的管理 D$ 共用。

存取儲存報告

1. 使用下列路徑格式對應管理 D$ 共用：

   ```
   \\file-system-dns-name\D$
   ```

   例如：

```
\\amznfsxaa11bb22.corp.example.com\D$
```

2. 導覽至 StorageReports 資料夾。此資料夾包含依報告類型和執行日期整理的子資料夾。

> **Note**
>
> 存取管理 D$ 共享需要管理員登入資料。

儲存報告最佳實務

遵循這些最佳實務，以確保高效且有效的儲存報告：

效能考量

儲存報告產生需要大量資源，因為 FSRM 必須掃描大量檔案。

- 限制報告範圍 - 使用 `Namespace` 參數將報告限制在特定資料夾，而不是掃描整個檔案系統。掃描大型目錄結構需要大量資源，可能需要數小時才能完成。
- 在離峰時間排程報告 - 在低系統活動期間執行排程報告，將對效能的影響降至最低。避免在備份時段或其他維護任務期間執行報告。
- 設定合理的閾值 - 使用閾值參數將報告輸出限制為可操作的資料。例如，`LargeFileMinimum`將 設定為識別值得調查的檔案的值，而不是每個超過 1MB 的檔案。
- 使用 RunDuration 限制 - 設定 `RunDuration` 參數以防止報告執行太長並影響系統效能。如果報告未在時間限制內完成，則會在下一次排定的執行期間繼續。
- 監控報告效能 - Get-FSxFSRMStorageReport用來檢查報告完成所需的時間。如果報告持續需要太長的時間，請考慮縮小範圍或減少執行頻率。

報告設計

- 使用描述性名稱 - 提供報告清晰的描述性名稱，指出它們分析的內容和執行時間，例如「每週大型檔案 - 財務共享」或「每月重複檔案 - 所有共享」。
- 合併相關分析 - 為相同命名空間產生多個報告類型時，請使用多個`ReportType`值建立單一報告，而非個別的報告。這更有效率，因為 FSRM 只需要掃描目錄結構一次。
- 依檔案模式篩選 - 使用檔案模式參數來專注於特定檔案類型的報告。例如，分析大型檔案時，您可以建立影片檔案、資料庫檔案和封存檔案的個別報告，以進一步了解儲存體耗用模式。

- 利用分類屬性 - 使用`FilesByProperty`報告根據檔案的分類來分析檔案。這可提供更有意義的洞見。

報告管理

- 定期檢閱報告 - 排定時間檢閱報告結果，並對問題清單採取動作。報告只有在您使用它們來做出儲存管理決策時才有價值。
- 封存舊報告 - 報告檔案會隨著時間累積並耗用儲存空間。為報告檔案建立保留政策，並刪除或封存不再需要的舊報告。
- 排程前測試報告 - 建立互動式報告以測試報告組態，並在建立排程版本之前驗證它們產生預期結果。

儲存報告管理命令

您可以存取兩個 FSx 遠端 PowerShell 命令系列來管理儲存報告：

1. 報告定義命令 - 建立、擷取、修改和移除儲存報告組態，以指定要分析哪些資料、何時執行報告，以及要產生的格式。
2. 報告執行命令 - 開始、停止、監控和等待產生儲存報告。使用這些命令可隨需執行報告或管理長時間執行的報告任務。

Storage Report FSx 遠端 PowerShell 命令的清單

> **Note**
>
> 此頁面中的所有範例都假設您已使用檔案系統的 Windows Remote PowerShell 端點定義`$FSxWindowsRemotePowerShellEndpoint`變數。您可以在檔案系統的詳細資訊頁面上的 Amazon FSx 主控台中找到此端點，或使用 AWS CLI `describe-file-systems`命令。

報告定義命令

New-FSxFSRMStorageReport

New-FSxFSRMStorageReport：建立儲存報告，分析指定的目錄以產生一或多個報告類型。

參數：

- `Name (string)` - 必要。儲存報告的名稱。

- Namespace (array) - 必要。要分析的路徑或資料夾類型的陣列。您可以指定多種格式的路徑：
  - 資料夾路徑
  - 資料夾分類。例如，【FolderUsage_MS="User Files"】
- ReportType (array) - 必要。要產生的報告類型陣列。您可以指定下列值：
  - DuplicateFiles：根據檔案大小和內容識別重複的檔案
  - FilesByFileGroup：依檔案群組成員資格將檔案分組
  - FilesByOwner：依擁有者分組檔案
  - FilesByProperty：依分類屬性將檔案分組
  - FileScreenAuditFiles：列出檔案篩選違規
  - FoldersByProperty：依管理屬性分組資料夾
  - LargeFiles：列出超過指定大小閾值的檔案
  - LeastRecentlyAccessed：列出最近未存取的檔案
  - MostRecentlyAccessed：列出最近存取的檔案
  - QuotaUsage：顯示配額用量統計資料
- ReportFormat (array) - 選用。輸出格式的陣列。您可以指定下列值：
  - DHTML：動態 HTML 格式
  - HTML：靜態 HTML 格式
  - XML：XML 格式
  - CSV：逗號分隔值格式
  - Text：純文字格式
- Interactive (boolean) - 選用。如果設定為 true，會產生互動式報告。互動式報告無法在建立後修改。
- ScheduleConfigurations (hashtable) - 除非報告為互動式，否則為必要。包含具有下列屬性之排程組態的雜湊：
  - Time (datetime)：指定何時執行任務的 DateTime 物件（必要）
  - RunDuration (number)：執行任務的時數（選用）
  - Weekly (array)：工作日陣列（選用）
  - Monthly (array)：月份的陣列，-1用於最後一天（選用）

報告特定參數：

- FileScreenAuditDaysSince (number) - 選用。針對 FileScreenAuditFiles 報告，指定要包含稽核事件的天數。
- FileScreenAuditUser (array) - 選用。針對 FileScreenAuditFiles 報告，指定要包含在報告中的使用者帳戶陣列。只有這些使用者的檔案篩選違規才會包含在內。
- FileGroupIncluded (array) - 選用。針對 FilesByFileGroup 報告，指定要包含的檔案群組。
- FileOwnerFilePattern (string) - 選用。針對 FilesByOwner 報告，指定要篩選結果的檔案模式。
- PropertyName (string) - 選用。針對 FilesByProperty 報告，指定分組依據的分類屬性。
- FolderPropertyName (string) - 選用。對於 FoldersByProperty 報告，指定要分組的資料夾屬性。
- PropertyFilePattern (string) - 選用。針對 FilesByProperty 和 FoldersByProperty，指定要篩選結果的檔案模式。
- LargeFileMinimum (number) - 選用。對於 LargeFiles 報告，指定以位元組為單位的最小檔案大小。
- LargeFilePattern (string) - 選用。對於 LargeFiles 報告，指定要篩選結果的檔案模式。
- LeastAccessedMinimum (number) - 選用。針對 LeastRecentlyAccessed 報告，指定自上次存取以來的天數下限。
- LeastAccessedFilePattern (string) - 選用。針對 LeastRecentlyAccessed 報告，指定要篩選結果的檔案模式。
- MostAccessedMaximum (number) - 選用。針對 MostRecentlyAccessed 報告，指定自上次存取以來的天數上限。
- MostAccessedFilePattern (string) - 選用。對於 MostRecentlyAccessed 報告，指定要篩選結果的檔案模式。
- QuotaMinimumUsage (number) - 選用。對於 QuotaUsage 報告，指定要包含的最低配額用量百分比。

範例：

1. 建立每月大型檔案報告。

```
$schedule = @{
    Time = ("3:00 AM")
    Monthly = @(1) # Run on first day
```

```
}

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $schedule -ScriptBlock {
    param($schedule)
    New-FSxFSRMStorageReport -Name "Monthly Large Files" -Namespace "share
\data" -ReportType "LargeFiles" -LargeFileMinimum 100MB -ReportFormat "HTML" -
ScheduleConfigurations $schedule
}
```

2. 建立具有多個命名空間和格式的每週重複檔案報告。

```
$schedule = @{
    Time = ("12:00 AM")
    Weekly = @('Sunday')
    RunDuration = 4
}

$namespaces = @("share\docs", "[FolderUsage_MS=User Files]")
$reportFormats = @("HTML", "CSV")
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList @($schedule, $namespaces, $reportFormats) -ScriptBlock {
    param($schedule, $namespaces, $reportFormats)
    New-FSxFSRMStorageReport -Name "Weekly Duplicates" -Namespace $namespaces -
ReportType "DuplicateFiles" -ReportFormat $reportFormats -ScheduleConfigurations
 $schedule
}
```

3. 建立立即執行的互動式報告。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMStorageReport -Name "Find large files" -Namespace "share" -Interactive
 $true -ReportType "QuotaUsage"
}
```

Get-FSxFSRMStorageReport

Get-FSxFSRMStorageReport：從您的檔案系統擷取一或多個儲存報告。傳回報告組態和狀態的詳細資訊。

參數：

- Name (array) - 選用。要擷取的報告名稱陣列。如果您未指定名稱，命令會傳回檔案系統上的所有儲存報告。

範例：

1. 擷取檔案系統上的所有儲存報告。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMStorageReport
}
```

Remove-FSxFSRMStorageReport

Remove-FSxFSRMStorageReport：從您的檔案系統移除一或多個儲存報告。您無法移除目前正在執行的報告。

參數：

- Name (array) - 必要。要移除的報告名稱陣列。
- PassThru (boolean) - 選用。如果設定為 true， 會傳回移除的報告物件。

範例：

1. 移除單一儲存報告。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Remove-FSxFSRMStorageReport -Name "Monthly Report" -PassThru
}
```

Set-FSxFSRMStorageReport

Parameters

- Name (array) - 必要。要修改的報告名稱陣列。
- Namespace (array) - 選用。要分析的路徑或資料夾類型陣列。您可以指定多種格式的路徑：
  - 資料夾路徑
  - 資料夾分類。例如，【FolderUsage_MS="User Files"】

- ReportType (array) - 選用。要產生的報告類型陣列。您可以指定下列值：
  - DuplicateFiles：根據檔案大小和內容識別重複的檔案
  - FilesByFileGroup：依檔案群組成員資格將檔案分組
  - FilesByOwner：依擁有者分組檔案
  - FilesByProperty：依分類屬性將檔案分組
  - FileScreenAuditFiles：列出檔案篩選違規
  - FoldersByProperty：依管理屬性分組資料夾
  - LargeFiles：列出超過指定大小閾值的檔案
  - LeastRecentlyAccessed：列出最近未存取的檔案
  - MostRecentlyAccessed：列出最近存取的檔案
  - QuotaUsage：顯示配額用量統計資料
- ReportFormat (array) - 選用。輸出格式的陣列。您可以指定下列值：
  - DHTML：動態 HTML 格式
  - HTML：靜態 HTML 格式
  - XML：XML 格式
  - CSV：逗號分隔值格式
  - Text：純文字格式
- ScheduleConfigurations (hashtable) - 除非報告為互動式，否則為必要。包含具有下列屬性的排程組態的雜湊：
  - Time (datetime)：指定何時執行任務的 DateTime 物件（必要）
  - RunDuration (number)：執行任務的時數（選用）
  - Weekly (array)：工作日陣列（選用）
  - Monthly (array)：月份的陣列，-1用於最後一天（選用）
- PassThru (boolean) - 選用。如果設定為 true， 會傳回修改的報告物件。

報告特定參數

- FileScreenAuditDaysSince (number) - 選用。針對 FileScreenAuditFiles 報告，指定要包含稽核事件的天數。
- FileScreenAuditUser (array) - 選用。針對 FileScreenAuditFiles 報告，指定要包含在報告中的使用者帳戶陣列。只有這些使用者的檔案篩選違規才會包含在內。

- `FileGroupIncluded (array)` - 選用。針對 FilesByFileGroup 報告，指定要包含的檔案群組。
- `FileOwnerFilePattern (string)` - 選用。針對 FilesByOwner 報告，指定要篩選結果的檔案模式。
- `PropertyName (string)` - 選用。針對 FilesByProperty 報告，指定分組依據的分類屬性。
- `FolderPropertyName (string)` - 選用。對於 FoldersByProperty 報告，指定要分組的資料夾屬性。
- `PropertyFilePattern (string)` - 選用。針對 FilesByProperty 和 FoldersByProperty，指定要篩選結果的檔案模式。
- `LargeFileMinimum (number)` - 選用。對於 LargeFiles 報告，指定以位元組為單位的最小檔案大小。
- `LargeFilePattern (string)` - 選用。對於 LargeFiles 報告，指定要篩選結果的檔案模式。
- `LeastAccessedMinimum (number)` - 選用。針對 LeastRecentlyAccessed 報告，指定自上次存取以來的天數下限。
- `LeastAccessedFilePattern (string)` - 選用。針對 LeastRecentlyAccessed 報告，指定要篩選結果的檔案模式。
- `MostAccessedMaximum (number)` - 選用。針對 MostRecentlyAccessed 報告，指定自上次存取以來的天數上限。
- `MostAccessedFilePattern (string)` - 選用。針對 MostRecentlyAccessed 報告，指定要篩選結果的檔案模式。
- `QuotaMinimumUsage (number)` - 選用。對於 QuotaUsage 報告，指定要包含的最低配額用量百分比。

範例：

1. 更新現有報告的排程和格式。

```
$schedule = @{
    Time = ("3:00 AM")
    Monthly = @(1)
}
$reportFormats = @("HTML", "CSV")

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList @($schedule, $reportFormats) -ScriptBlock {
    param($schedule, $reportFormats)
```

```
    Set-FSxFSRMStorageReport -Name "Monthly Report" -ScheduleConfigurations $schedule -
ReportFormat $reportFormats -PassThru
}
```

報告執行命令

Start-FSxFSRMStorageReport

Parameters

- Name (array) - 必要。要啟動的報告名稱陣列。
- Queue (boolean) - 選用。如果設定為 true， 會將報告新增至佇列，以便在接下來的 5 分鐘內執行。在此期間排入佇列的任何報告都會一起執行。如果設定為 false 或未指定，則報告會立即開始。
- RunDuration (number) - 選用。指定報告在取消之前應執行多少小時。有效值：-1 到 2147483。特殊值：
  - 0：執行 以完成
  - -1：執行 直到取消

  如果未指定， 會執行 直到完成。

範例

1. 立即啟動儲存報告。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Start-FSxFSRMStorageReport -Name "Monthly Report"
}
```

2. 使用持續時間限制將儲存報告排入佇列。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Start-FSxFSRMStorageReport -Name "Quarterly Report" -Queue: $true -RunDuration 4
}
```

Stop-FSxFSRMStorageReport

Parameters

- Name (array) - 必要。要停止的報告名稱陣列。

範例：

1. 停止單一儲存報告。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Stop-FSxFSRMStorageReport -Name "Monthly Report"
}
```

Wait-FSxFSRMStorageReport

Parameters

- Name (array) - 必要。要等待的報告名稱陣列。
- Timeout (number) - 選用。指定報告完成的等待時間，以秒為單位。如果逾時在報告完成之前過期，則命令會傳回 ，但報告產生會在背景中繼續執行。有效值：-1 到 2147483。特殊值：
  - -1：無限期等待直到報告完成（預設）
  - 0：檢查目前狀態並立即傳回，無需等待

範例：

1. 無限期等待儲存報告完成。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Wait-FSxFSRMStorageReport -Name "Monthly Report"
}
```

檔案管理任務

Amazon FSx for Windows File Server 不支援 FSRM 檔案管理任務。不過，您可以從具有檔案系統網路存取權的用戶端機器使用原生 PowerShell 命令，來達成常見的使用案例，例如資料封存和保留政策。

例如，您可以在用戶端電腦上使用 PowerShell 指令碼來：

- 根據存留期或上次存取時間移動或封存檔案
- 刪除超過保留期的分類檔案
- 根據分類屬性將檔案複製到封存儲存體

您可以使用 `Get-FsrmClassification`命令存取檔案屬性，並根據值採取動作。

若要從用戶端 PowerShell 指令碼存取 FSRM 分類屬性或其他 FSRM 中繼資料，用戶端機器也必須安裝 FSRM。

FSRM 設定

FSRM 設定提供全系統的組態，可讓您自訂行為並簡化功能管理。使用這些設定來控制 FSRM 如何在您的檔案系統中運作，並設定預設值，以簡化建立和設定儲存報告和檔案篩選等功能。

設定類別

FSRM 設定分為三個類別：

檔案畫面稽核

當使用者嘗試儲存作用中檔案畫面封鎖的檔案時，檔案畫面稽核記錄。此資訊對於監控檔案篩選政策的合規性，以及識別經常嘗試儲存未經授權檔案類型的使用者至關重要。

- `ReportFileScreenAuditEnable` - 此設定會控制 FSRM 是否完全記錄檔案篩選違規。如果停用，FSRM 不會記錄檔案畫面違規，而且`FileScreenAuditFiles`報告不會顯示任何資料。您必須啟用此設定才能使用檔案畫面稽核報告。
- `ReportFileScreenAuditDaysSince` - 此設定提供檔案畫面稽核報告的預設時間範圍。當您建立`FileScreenAuditFiles`報告而未指定要往前看多遠時，FSRM 會使用此值。設定適當的預設值（例如 30 天）可確保報告專注於最近的違規，而不會包含過多的歷史資料。
- `ReportFileScreenAuditUser` - 此設定提供要包含在檔案畫面稽核報告中的預設使用者清單。當您在不指定要包含哪些使用者的情況下建立`FileScreenAuditFiles`報告時，FSRM 會使用此清單。如果為空，則報告預設會包含所有使用者。您可以使用此設定來專注於特定使用者群組或部門的報告。

預設報告篩選條件

預設報告篩選條件設定提供建立儲存報告時所使用的值，而無需指定特定參數。這些預設值可簡化報告建立，並確保類似報告之間的一致性。

每個報告類型都有相關聯的預設設定：

- 大型檔案報告 - ReportLargeFileMinimum設定預設的最小檔案大小，並ReportLargeFilePattern設定預設的檔案模式篩選條件。
- 最少存取的檔案報告 - ReportLeastAccessedMinimum設定自上次存取以來的預設天數，並ReportLeastAccessedFilePattern設定預設的檔案模式篩選條件。
- 最常存取的檔案報告 - ReportMostAccessedMaximum設定自上次存取以來的預設天數上限，並ReportMostAccessedFilePattern設定預設的檔案模式篩選條件。
- 依擁有者報告的檔案 - ReportFileOwnerFilePattern設定預設檔案模式篩選條件，並ReportFileOwnerUser設定要包含的使用者預設清單。
- 依屬性分類的檔案報告 - ReportPropertyName設定要分析的預設分類屬性，並ReportPropertyFilePattern設定預設檔案模式篩選條件。
- 依檔案群組報告的檔案 - ReportFileGroupIncluded設定要包含的檔案群組預設清單。
- 配額用量報告 - ReportQuotaMinimumUsage設定預設的最小配額用量百分比。

建立報告時，您可以透過在報告組態中明確指定 參數來覆寫任何這些預設值。全域預設值只有在您未指定值時才適用。

報告限制

報告限制設定控制要包含在儲存報告中的項目數量上限。這些限制有兩個用途：

1. 效能管理 - 限制報告中的項目數量可防止報告產生或耗用過多系統資源的時間過長。分析數百萬個檔案的大型報告可能需要數小時才能完成並影響系統效能。
2. 報告可用性 - 有數千個項目的報告很難檢閱和分析。報告限制可確保報告專注於最相關的資料。

您可以設定對報告限制的精細控制：

- 整體限制 - ReportLimitMaxFile 限制任何報告中的檔案總數，無論類型為何。
- Per-report-type限制 - 如 ReportLimitMaxFileGroup、 ReportLimitMaxOwner和 等設定會ReportLimitMaxPropertyValue限制要包含在特定報告類型中的群組、擁有者或屬性值數量。

- 每個群組限制 - 如 `ReportLimitMaxFilesPerFileGroup`、`ReportLimitMaxFilesPerOwner`和 等設定會 `ReportLimitMaxFilesPerPropertyValue`限制報告中每個群組內要顯示的檔案數量。

當報告達到限制時，FSRM 會包含消耗最多儲存空間或與報告類型最相關的項目，並在報告中指出已達到限制。

FSRM 設定命令

您可以存取命令來擷取和修改全域設定。使用這些命令來設定整個系統的 FSRM 行為。

FSRM 設定 FSx 遠端 PowerShell 命令的清單

> **Note**
>
> 此頁面中的所有範例皆假設您已使用檔案系統的 Windows Remote PowerShell 端點定義 `$FSxWindowsRemotePowerShellEndpoint`變數。您可以在檔案系統的詳細資訊頁面上的 Amazon FSx 主控台中找到此端點，或使用 AWS CLI `describe-file-systems`命令。

Get-FSxFSRMSetting

`Get-FSxFSRMSetting`：擷取檔案系統上目前的檔案伺服器資源管理員設定。僅傳回可使用 Set-FSxFSRMSetting 修改的設定。

參數：

無

範例：

1. 擷取所有目前的 FSRM 設定。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
Get-FSxFSRMSetting
}
```

Set-FSxFSRMSetting

Set-FSxFSRMSetting：修改檔案系統上的全域檔案伺服器資源管理員設定。這些設定提供儲存報告和控制 FSRM 行為的預設值。

參數：

檔案畫面稽核設定：

- ReportFileScreenAuditEnable (boolean) - 選用。控制檔案篩選稽核事件是否包含在 FSRM 報告中。
- ReportFileScreenAuditDaysSince (number) - 選用。產生 FileScreenAuditFiles 報告時，查詢檔案篩選違規的預設天數。
- ReportFileScreenAuditUser (array) - 選用。要包含在 FileScreenAuditFiles 報告中的預設使用者帳戶清單陣列。

預設報告篩選條件設定：

- ReportFileGroupIncluded (array) - 選用。根據預設，要包含在報告中的檔案群組名稱陣列。
- ReportFileOwnerFilePattern (string) - 選用。依擁有者報告的檔案預設檔案模式。支援萬用字元 (* 和 ?)。
- ReportFileOwnerUser (array) - 選用。依擁有者報告之檔案的 Domain\User 格式使用者陣列。
- ReportLargeFileMinimum (number) - 選用。大型檔案報告的預設最小檔案大小，以位元組為單位。
- ReportLargeFilePattern (string) - 選用。大型檔案報告的預設檔案模式。支援萬用字元 (* 和 ?)。
- ReportLeastAccessedFilePattern (string) - 選用。最低存取檔案報告的預設檔案模式。支援萬用字元 (* 和 ?)。
- ReportLeastAccessedMinimum (number) - 選用。上次存取最少存取檔案報告後的預設最短天數。
- ReportMostAccessedFilePattern (string) - 選用。最常存取的檔案報告的預設檔案模式。支援萬用字元 (* 和 ?)。
- ReportMostAccessedMaximum (number) - 選用。自上次存取大多數存取檔案報告以來的預設天數上限。

- ReportPropertyFilePattern (string) - 選用。屬性報告的預設檔案模式。支援萬用字元 (* 和 ?)。
- ReportPropertyName (string) - 選用。屬性報告的預設屬性名稱。
- ReportQuotaMinimumUsage (number) - 選用。配額用量報告的預設最低配額用量百分比。

報告限制設定：

- ReportLimitMaxDuplicateGroup (number) - 選用。要在重複檔案報告中包含的重複檔案群組數目上限。
- ReportLimitMaxFile (number) - 選用。要包含在儲存報告中的檔案數目上限。
- ReportLimitMaxFileGroup (number) - 選用。要包含在報告中的檔案群組數量上限。
- ReportLimitMaxFileScreenEvent (number) - 選用。檔案畫面稽核報告中要包含的檔案畫面事件數目上限。
- ReportLimitMaxFilesPerDuplicateGroup (number) - 選用。重複檔案報告中每個重複群組的檔案數量上限。
- ReportLimitMaxFilesPerFileGroup (number) - 選用。檔案群組報告中每個檔案群組的檔案數量上限。
- ReportLimitMaxFilesPerOwner (number) - 選用。根據擁有者報告，每個擁有者在檔案中的檔案數量上限。
- ReportLimitMaxFilesPerPropertyValue (number) - 選用。依屬性報告區分，檔案中每個屬性值的檔案數量上限。
- ReportLimitMaxOwner (number) - 選用。依擁有者報告包含在檔案中的擁有者數量上限。
- ReportLimitMaxPropertyValue (number) - 選用。依屬性報告包含在檔案中的屬性值數目上限。
- ReportLimitMaxQuota (number) - 選用。配額用量報告中要包含的配額數量上限。

其他設定：

- PassThru (boolean) - 選用。如果設定為 true， 會傳回修改的設定物件。

範例：

1. 使用 30 天歷史記錄設定預設檔案畫面稽核。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMSetting -ReportFileScreenAuditDaysSince 30 -PassThru
}
```

2. 設定預設大型檔案報告設定。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMSetting -ReportLargeFileMinimum 100MB -ReportLargeFilePattern "*.iso"
 -PassThru
}
```

事件日誌

當您在檔案系統上啟用 FSRM 時， AWS FSx for Windows File Server 會產生檔案管理活動的事件日誌，並將其傳送至您設定的目的地 (AWS CloudWatch Logs 或 AWS Kinesis Data Firehose)。這些日誌可協助您監控 FSRM 操作、疑難排解問題，以及維護檔案管理活動的稽核線索。

FSRM 日誌的內容

當您在檔案系統上啟用 FSRM 時， AWS FSx for Windows File Server 會記錄事件並將其傳送至您設定的目的地。將記錄下列事件：

- 檔案篩選違規 - 當使用者嘗試儲存由具有事件通知動作的檔案畫面監控的檔案時
- 配額閾值通知 - 當配額用量達到具有事件通知動作的已設定閾值時
- FSRM 服務事件 – 確認通知設定、服務錯誤和操作失敗

存取 FSRM 日誌

您存取 FSRM 日誌的位置取決於您在啟用 FSRM 時設定的目的地：

CloudWatch Logs

透過導覽至您指定的日誌群組，在 CloudWatch Logs 主控台中檢視日誌。您可以使用 CloudWatch Logs Insights 搜尋、篩選和分析日誌，並設定 CloudWatch 警示來通知您特定事件。

Kinesis Data Firehose

日誌會傳送到 Kinesis Data Firehose 交付串流中設定的目的地，例如 Amazon S3、 AWS Redshift 或 AWS OpenSearch Service。您可以使用與您的交付串流整合的工具和服務來處理和分析日誌。

常用案例

本主題提供常見 File Server Resource Manager 任務的step-by-step範例。這些範例示範如何使用和實作 FSRM 功能來解決典型的檔案管理挑戰。

> **Note**
>
> 此頁面中的所有範例都假設您已使用檔案系統的 Windows Remote PowerShell 端點定義 `$FSxWindowsRemotePowerShellEndpoint`變數。您可以在檔案系統的詳細資訊頁面上的 Amazon FSx 主控台中找到此端點，或使用 AWS CLI `describe-file-systems`命令。

在資料夾上設定硬性配額

此範例示範如何建立硬配額，以防止使用者在「部門」資料夾中儲存超過 10 GB。

若要設定資料夾的配額：

1. 建立 10 GB 限制的硬性配額：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMQuota -Folder "share\department" -Size 10GB -Description "10 GB hard
 limit for department folder"
}
```

2. （選用）修改配額以新增 85% 用量的閾值通知：

```
$thresholds = [System.Collections.ArrayList]@()
$threshold = @{
    ThresholdPercentage = 85
    Action = @(
        @{
            ActionType = "Event"
            EventType = "Warning"
```

```
            MessageBody = "Department folder has reached 85% of quota limit"
        }
    )
}

$null = $thresholds.Add($threshold)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList ($thresholds) -ScriptBlock {
    param($thresholds)
    Set-FSxFSRMQuota -Folder "share\department" -ThresholdConfigurations
 $Using:thresholds
}
```

3. 確認已建立配額：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMQuota -Folder "share\department"
}
```

使用檔案群組限制特定檔案類型

此範例示範如何使用預設「Audio and Video Files」檔案群組，封鎖使用者將音訊和影片檔案儲存至商業文件資料夾。

若要使用檔案群組來限制檔案類型：

1. 建立可封鎖音訊和影片檔案的作用中檔案畫面：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
New-FSxFSRMFileScreen -Folder "share\business-documents" -IncludeGroup "Audio and
 Video Files" -Description "Block media files in business documents folder"
}
```

2. （選用）更新檔案畫面，以在使用者嘗試儲存封鎖的檔案時新增通知：

```
$notifications = [System.Collections.ArrayList]@()

$eventNotification = @{
    ActionType = "Event"
```

```
    EventType = "Warning"
    MessageBody = "User attempted to save blocked media file"
}
$null = $notifications.Add($eventNotification)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $notifications -ScriptBlock {
    param($notifications)
    Set-FSxFSRMFileScreen -Folder "share\business-documents" -
NotificationConfigurations $Using:notifications
}
```

3. 確認已建立檔案畫面：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMFileScreen -Folder "share\business-documents"
}
```

識別和分類 PII 資料

此範例說明如何自動識別包含社會安全號碼的檔案，並將其分類為包含個人身分識別資訊 (PII)。

若要識別和分類 PII 資料：

1. 建立 PII 的分類屬性：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationPropertyDefinition -Name "ContainsPII" -Type
 OrderedList -PossibleValueConfigurations @(
        @{ Name = "Yes" },
        @{ Name = "No" })
}
```

2. 建立分類規則以偵測社會安全號碼：

> **Note**
>
> 下列規則表達式會搜尋模式為 XXX-XX-XXXX 的文字檔案。對於生產用途，請考慮使用更複雜的模式或結合多種偵測方法。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationRule -Name "Detect_SSN" -Property "ContainsPII"
 -PropertyValue "Yes" -Namespace "share" -ClassificationMechanism "Content
 Classifier" -ContentRegularExpression "\b\d{3}-\d{2}-\d{4}\b"
}
```

3. 執行分類：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Start-FSxFSRMClassification
}
```

4. （選用）設定持續分類以自動分類新檔案：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMClassification -Continuous $true
}
```

5. 檢查狀態 (1 表示已完成）：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMClassification
}
```

6. 分類完成後，您可以在 Windows File Explorer 中的檔案上按一下滑鼠右鍵，選取屬性，然後選擇分類索引標籤，以檢視指派給檔案的分類屬性。此索引標籤會顯示檔案的所有分類屬性及其值。

建立檔案的保留政策

此範例顯示如何根據檔案的資料夾位置，依保留期間分類檔案，然後您可以搭配用戶端 PowerShell 指令碼來封存或刪除檔案。

若要建立檔案的保留政策：

1. 建立保留期間的分類屬性：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationPropertyDefinition -Name "RetentionPeriod" -Type
 String -Description "File retention period"
}
```

2. 建立不同保留期的分類規則：

   - 資料夾法務文件下法律文件的 7 年保留期：

   ```
   Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -
   ConfigurationName FSxRemoteAdmin -ScriptBlock {
       New-FSxFSRMClassificationRule -Name "Legal_7Year" -Property
    "RetentionPeriod" -PropertyValue "7 years" -Namespace "share/Legal Documents" -
   ClassificationMechanism "Folder Classifier"
   }
   ```

   - 資料夾 Finance 下財務記錄的 3 年保留期：

   ```
   Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -
   ConfigurationName FSxRemoteAdmin -ScriptBlock {
       New-FSxFSRMClassificationRule -Name "Finance_3Year" -Property
    "RetentionPeriod" -PropertyValue "3 years" -Namespace "share/Finance" -
   ClassificationMechanism "Folder Classifier"
   }
   ```

   您也可以依檔案內容分類並搜尋字串，例如「保留期七年」。若要達成此目的，請使用 `ClassificationMechanism "Content Classifier"`和 `ContentString "Retention seven years"`。

3. 執行分類以套用保留屬性：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Start-FSxFSRMClassification
}
```

4. （選用）設定持續分類以自動分類新檔案：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
```

```
    Set-FSxFSRMClassification -Continuous $true
}
```

5. 檢查狀態 (1 表示已完成）：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMClassification
}
```

6. 分類完成後，您可以在 Windows File Explorer 中的檔案上按一下滑鼠右鍵，選取屬性，然後選擇分類索引標籤，以檢視指派給檔案的分類屬性。此索引標籤會顯示檔案的所有分類屬性及其值。
7. 將檔案分類為保留期間後，您可以使用用戶端 PowerShell 指令碼，根據檔案的`RetentionPeriod`屬性和存留期來封存或刪除檔案。例如，您可以掃描檔案系統，並將檔案的存留期與其保留期分類進行比較。如需詳細資訊，請參閱檔案管理任務。

設定常見的儲存報告

本節說明如何建立兩個常用的儲存報告：大型檔案報告和依擁有者報告的檔案。

大型檔案報告

此範例會建立每月報告，以識別大於 200 MB 的檔案。

若要建立大型檔案報告：

1. 建立排程的大型檔案報告：

```
$schedule = @{
    Time = "2:00 AM"
    Monthly = @(1) # Run on the 1st of each month
}

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $schedule -ScriptBlock {
    param($schedule)
    New-FSxFSRMStorageReport -Name "Monthly Large Files Report" -Namespace "share"
 -ReportType "LargeFiles" -LargeFileMinimum 200MB -ReportFormat "HTML","CSV" -
ScheduleConfigurations $schedule
}
```

2. （選用）立即執行報告以測試：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Start-FSxFSRMStorageReport -Name "Monthly Large Files Report"
}
```

依擁有者報告的檔案

此範例會建立每週報告，顯示使用者使用的儲存體。

若要依擁有者報告建立檔案：

1. 依擁有者報告建立排程檔案：

```
$schedule = @{
    Time = "3:00 AM"
    Weekly = @('Sunday')
}

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $schedule -ScriptBlock {
    param($schedule)
    New-FSxFSRMStorageReport -Name "Weekly Files by Owner Report" -
Namespace "share" -ReportType "FilesByOwner" -ReportFormat "HTML","CSV" -
ScheduleConfigurations $schedule
}
```

2. （選用）立即執行報告以測試：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Start-FSxFSRMStorageReport -Name "Weekly Files by Owner Report"
}
```

透過映射管理 D$ 共用來存取產生的報告。如需詳細資訊，請造訪 存取儲存報告。

管理 FSx for Windows File Server 上的儲存

檔案系統的儲存組態包含佈建儲存容量的數量、儲存類型，以及如果儲存類型是固態硬碟 (SSD)，則為 SSD IOPS 的數量。您可以在建立檔案系統時和建立檔案系統之後，設定這些資源以及檔案系統的輸送

量容量，以達成工作負載所需的效能。了解如何使用 管理檔案系統的儲存和儲存相關效能 AWS 管理主控台 AWS CLI，以及透過探索下列主題在 PowerShell 上進行遠端管理的 Amazon FSx CLI。

主題

將儲存體成本最佳化

您可以使用 FSx for Windows 中提供的儲存組態選項來最佳化儲存成本。

儲存類型選項 - FSx for Windows File Server 提供兩種儲存類型：硬碟 (HDD) 和固態硬碟 (SSD)，可讓您最佳化成本/效能，以符合工作負載需求。HDD 儲存體專為廣泛的工作負載而設計，包括主目錄、使用者和部門共享，以及內容管理系統。SSD 儲存體專為最高效能和最延遲敏感的工作負載而設計，包括資料庫、媒體處理工作負載和資料分析應用程式。如需儲存類型和檔案系統效能的詳細資訊，請參閱FSx for Windows File Server 效能。

重複資料刪除 - 大型資料集通常具有備援資料，這會增加資料儲存成本。例如，使用者檔案共享可以有多個由多個使用者存放的相同檔案副本。軟體開發共享可以包含許多從建置到建置保持不變的二進位檔。您可以開啟檔案系統的重複資料刪除功能，以降低資料儲存成本。開啟時，重複資料刪除會自動減

少或消除冗餘資料，方法是只儲存資料集的重複部分一次。如需重複資料刪除的詳細資訊，以及如何為 Amazon FSx 檔案系統輕鬆開啟重複資料刪除功能，請參閱 使用重複資料刪除來降低儲存成本。

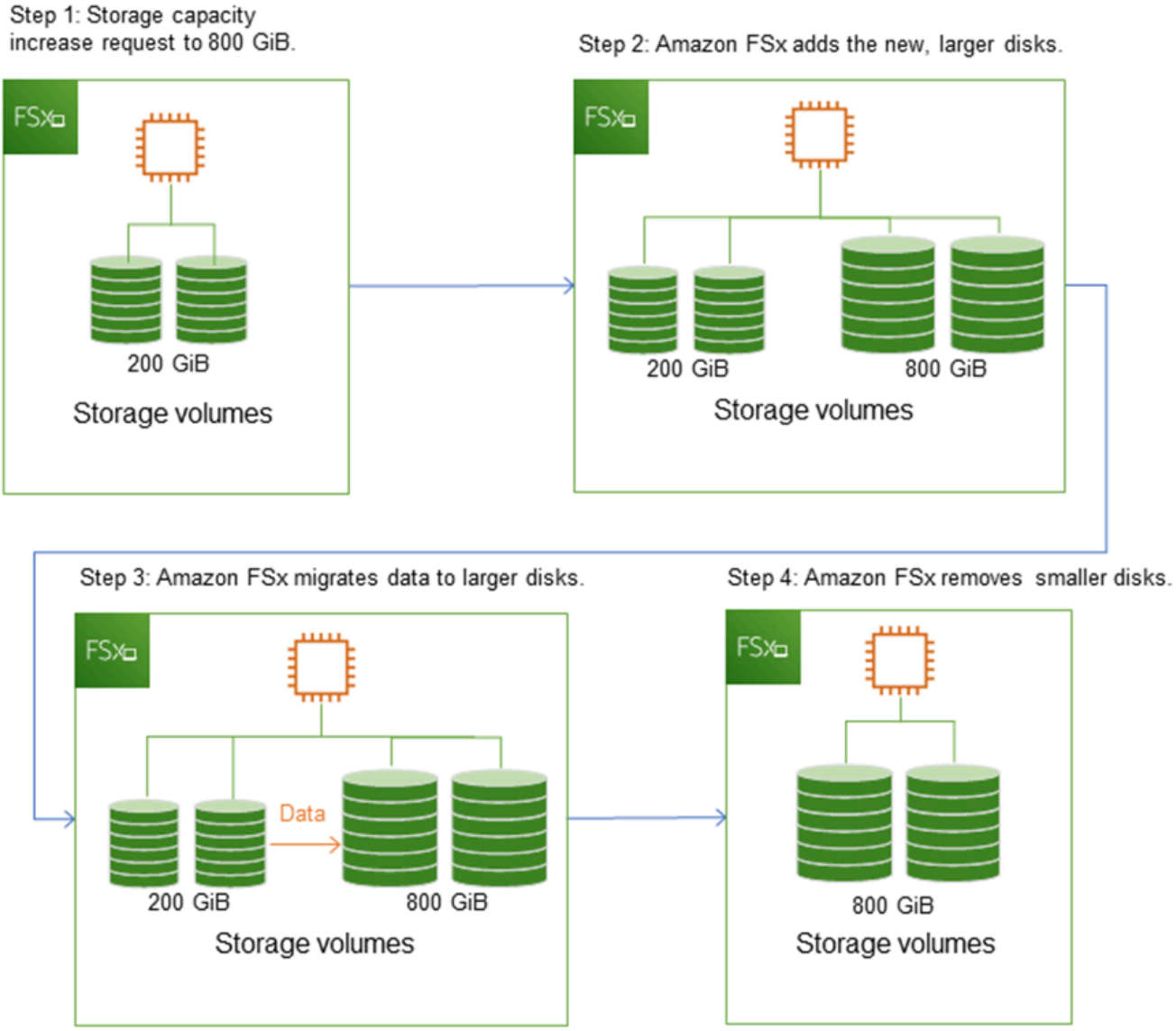
管理儲存容量

您可以隨著儲存需求變更，增加 FSx for Windows 檔案系統的儲存容量。您可以使用 Amazon FSx 主控台、Amazon FSx API 或 AWS Command Line Interface () 來執行此操作AWS CLI。規劃增加儲存容量時需要考慮的因素包括了解何時需要增加儲存容量、了解 Amazon FSx 如何處理儲存容量增加，以及追蹤儲存增加請求的進度。您只能增加檔案系統的儲存容量；您無法減少儲存容量。

> **Note**
>
> 您無法增加 2019 年 6 月 23 日之前建立之檔案系統的儲存容量，也無法從屬於 2019 年 6 月 23 日之前建立之檔案系統的備份還原檔案系統。

當您增加 Amazon FSx 檔案系統的儲存容量時，Amazon FSx 會在幕後為您的檔案系統新增一組新的、較大的磁碟。然後，Amazon FSx 會在背景執行儲存最佳化程序，以透明方式將資料從舊磁碟遷移到新磁碟。儲存最佳化可能需要數小時到數天的時間，取決於儲存類型和其他因素，對工作負載效能的影響微乎其微。在此最佳化期間，備份用量會暫時提高，因為新舊儲存磁碟區都包含在檔案系統層級備份中。包含兩組儲存磁碟區，以確保 Amazon FSx 即使在儲存擴展活動期間也能成功從備份中取得和還原。備份用量會在舊儲存磁碟區不再包含在備份歷史記錄中之後，還原至其先前的基準層級。當新的儲存容量可用時，您只需支付新的儲存容量費用。

下圖顯示 Amazon FSx 在增加檔案系統的儲存容量時所使用的四個主要步驟。



您可以使用 Amazon FSx 主控台、CLI 或 API，隨時追蹤儲存最佳化、SSD 儲存容量增加或 SSD IOPS 更新的進度。如需詳細資訊，請參閱監控儲存容量增加。

增加檔案系統的儲存容量須知

以下是在增加儲存容量時需要考慮的一些重要事項：

- 僅限增加 – 您只能增加檔案系統的儲存容量；您無法減少儲存容量。

- 最小增加 – 每個增加的儲存容量必須至少為檔案系統目前儲存容量的 10%，最高允許值為 65，536 GiB。
- 最低輸送量容量 – 若要增加儲存容量，檔案系統必須至少有 16 MBps 的輸送量容量。這是因為儲存最佳化步驟是輸送量密集的程序。
- 增加之間的時間 – 直到請求最後一次增加後 6 小時，或直到儲存最佳化程序完成，以時間較長者為準，您才能進一步增加檔案系統的儲存容量。儲存最佳化可能需要幾小時到幾天的時間才能完成。為了將完成儲存最佳化所需的時間降至最低，建議您在增加儲存容量之前，先增加檔案系統的輸送量容量（儲存擴展完成後，可以縮減輸送量容量），並在檔案系統上流量最少時增加儲存容量。

> **Note**
>
> 某些檔案系統事件可能會耗用磁碟 I/O 效能資源 例如：
> 儲存容量擴展的最佳化階段可能會增加磁碟輸送量，並可能導致效能警告。如需詳細資訊，請參閱效能警告和建議。

知道何時增加儲存容量

當檔案系統的可用儲存容量不足時，請提高其儲存容量。使用 `FreeStorageCapacity` CloudWatch 指標來監控檔案系統上可用的可用儲存量。您可以在此指標上建立 Amazon CloudWatch 警示，並在低於特定閾值時收到通知。如需詳細資訊，請參閱使用 Amazon CloudWatch 監控。

我們建議您隨時在檔案系統上維持至少 20% 的可用儲存容量。使用您的所有儲存容量可能會對效能產生負面影響，並可能導致資料不一致。

當可用儲存容量低於您指定的定義閾值時，您可以自動增加檔案系統的儲存容量。使用 AWS開發的自訂 CloudFormation 範本來部署實作自動化解決方案所需的所有元件。如需詳細資訊，請參閱動態增加儲存容量。

儲存容量增加，且檔案系統效能

大多數工作負載在新的儲存容量可用後，在 Amazon FSx 於背景執行儲存最佳化程序時，會受到最小的效能影響。不過，具有 HDD 儲存類型的檔案系統，以及涉及大量最終使用者、高階 I/O 或具有大量小型檔案的資料集的工作負載，可能會暫時降低效能。在這些情況下，我們建議您先增加檔案系統的輸送量容量，然後再增加儲存容量。對於這些類型的工作負載，我們也建議您在檔案系統負載最少時，在閒置期間變更輸送量容量。這可讓您繼續提供相同水準的輸送量，以滿足應用程式的效能需求。如需詳細資訊，請參閱管理輸送量容量。

管理檔案系統的儲存類型

您可以使用 AWS 管理主控台 和 將檔案系統儲存類型從 HDD 變更為 SSD AWS CLI。當您將儲存類型變更為 SSD 時，請記住，在請求最後一次更新後 6 小時或儲存最佳化程序完成之前，您無法再次更新檔案系統組態，以時間較長者為準。儲存最佳化可能需要幾個小時到幾天的時間才能完成。為了將這段時間降至最低，我們建議您在檔案系統流量最少時更新您的儲存類型。如需詳細資訊，請參閱更新 FSx for Windows 檔案系統的儲存類型。

您無法將檔案系統儲存類型從 SSD 變更為 HDD。如果您想要將檔案系統的儲存類型從 SSD 變更為 HDD，則需要將檔案系統的備份還原至您設定使用 HDD 儲存的新檔案系統。如需詳細資訊，請參閱將備份還原至新的檔案系統。

關於儲存體類型

您可以設定 FSx for Windows File Server 檔案系統，以使用固態硬碟 (SSD) 或磁性硬碟 (HDD) 儲存類型。

SSD 儲存體適用於具有高效能需求和延遲敏感度的大多數生產工作負載。這些工作負載的範例包括資料庫、資料分析、媒體處理和商業應用程式。我們也建議 SSD 用於涉及大量最終使用者、高階 I/O 或具有大量小型檔案之資料集的使用案例。最後，如果您打算啟用陰影複本，建議您使用 SSD 儲存體。您可以使用 SSD 儲存體為檔案系統設定和擴展 SSD IOPS，但不能為 HDD 儲存體設定和擴展 SSD IOPS。

HDD 儲存體專為廣泛的工作負載而設計，包括主目錄、使用者和部門檔案共用，以及內容管理系統。與 SSD 儲存體相比，HDD 儲存體的成本較低，但每單位儲存體的延遲和磁碟輸送量和磁碟 IOPS 水準較高。它可能適合具有低輸入/輸出需求的一般用途使用者共用和主目錄、不常擷取資料的大型內容管理系統 (CMS)，或具有少量大型檔案的資料集。

如需詳細資訊，請參閱儲存組態與效能。

管理 SSD IOPS

對於使用 SSD 儲存體設定的檔案系統，SSD IOPS 的數量會決定檔案系統必須讀取資料並將資料寫入磁碟時可用的磁碟 I/O 數量，而不是快取中的資料。您可以選取和擴展 SSD IOPS 的數量，而不受儲存容量影響。您可以佈建的最大 SSD IOPS 取決於您為檔案系統選取的儲存容量和輸送量容量。如果您嘗試將 SSD IOPS 增加到超過輸送量容量支援的限制，您可能需要增加輸送量容量，以取得該層級的 SSD IOPS。如需詳細資訊，請參閱 FSx for Windows File Server 效能 和 管理輸送量容量。

以下是有關更新檔案系統佈建 SSD IOPS 的一些重要事項：

- 選擇 IOPS 模式 – 有兩種 IOPS 模式可供選擇：

  - 自動 – 選擇此模式，Amazon FSx 會自動擴展您的 SSD IOPS，以維持每 GiB 儲存容量 3 個 SSD IOPS，每個檔案系統最多 400，000 個 SSD IOPS。
  - 使用者佈建 – 選擇此模式，以便您可以指定 96–400，000 範圍內的 SSD IOPS 數量。為可使用 Amazon FSx 的所有 指定每 GiB AWS 區域 儲存容量 3–50 IOPS 之間的數字，或在美國東部（維吉尼亞北部）、美國西部（奧勒岡）、美國東部（俄亥俄）、歐洲（愛爾蘭）、亞太區域（東京）和亞太區域（新加坡）每 GiB 儲存容量 3–500 IOPS 之間的數字。當您選擇使用者提供的模式，且您指定的 SSD IOPS 數量不是每 GiB 至少 3 IOPS 時，請求會失敗。對於更高層級的佈建 SSD IOPS，您需要為每個檔案系統平均 IOPS 超過每 GiB 3 IOPS。
- 儲存容量更新 – 如果您增加檔案系統的儲存容量，且依預設所需的 SSD IOPS 數量大於目前使用者佈建的 SSD IOPS 層級，Amazon FSx 會自動將您的檔案系統切換為自動模式，且您的檔案系統每 GiB 儲存容量至少會有 3 個 SSD IOPS。
- 輸送量容量更新 – 如果您增加輸送量容量，且新輸送量支援的最大 SSD IOPS 高於使用者佈建的 SSD IOPS 層級，Amazon FSx 會自動將您的檔案系統切換為自動模式。
- SSD IOPS 的頻率增加 – 在請求最後一次增加後 6 小時或儲存最佳化程序完成之前，您無法進一步增加 SSD IOPS、增加輸送量容量或更新檔案系統上的儲存類型，以時間較長者為準。儲存最佳化可能需要幾小時到幾天的時間才能完成。為了將完成儲存最佳化所需的時間降至最低，我們建議在檔案系統流量最少時擴展 SSD IOPS。

> **Note**
>
> 請注意，僅在以下項目中支援 4，608 MBps 或更高的輸送量容量： AWS 區域美國東部（維吉尼亞北部）、美國西部（奧勒岡）、美國東部（俄亥俄）、歐洲（愛爾蘭）、亞太區域（東京）和亞太區域（新加坡）。

如需如何更新 FSx for Windows File Server 檔案系統佈建 SSD IOPS 數量的詳細資訊，請參閱 更新檔案系統的 SSD IOPS。

使用重複資料刪除來降低儲存成本

重複資料刪除通常簡稱為 Dedup，有助於儲存管理員降低與重複資料相關聯的成本。透過 FSx for Windows File Server，您可以使用 Microsoft Data Deduplication 來識別和消除備援資料。大型資料集通常具有備援資料，這會增加資料儲存成本。例如：

- 使用者檔案共享可能有許多相同或類似檔案的副本。
- 軟體開發共享可以有許多從建置到建置保持不變的二進位檔。

您可以為檔案系統啟用重複資料刪除功能，以降低資料儲存成本。重複資料刪除透過僅儲存資料集的重複部分一次來減少或消除冗餘資料。當您啟用重複資料刪除時，預設會啟用資料壓縮，在重複資料刪除之後壓縮資料，以節省更多成本。重複資料刪除可最佳化冗餘，而不會犧牲資料真實性或完整性。重複資料刪除作為背景程序執行，持續並自動掃描和最佳化您的檔案系統，且對使用者和連線的用戶端而言是透明的。

透過重複資料刪除，您可以實現的儲存節省取決於資料集的性質，包括檔案之間存在多少重複。一般用途檔案共用的典型節省平均 50–60%。在共享中，使用者文件節省 30–50% 到軟體開發資料集節省 70–80%。您可以使用如下所述的`Measure-FSxDedupFileMetadata`遠端 PowerShell 命令來測量潛在的重複資料刪除節省。

您也可以自訂重複資料刪除，以符合您的特定儲存需求。例如，您可以將重複資料刪除設定為僅在特定檔案類型上執行，也可以建立自訂任務排程。由於重複資料刪除任務可能會耗用檔案伺服器資源，建議您使用 監控重複資料刪除任務的狀態`Get-FSxDedupStatus`。

如需有關在檔案系統上設定重複資料刪除的資訊，請參閱 管理重複資料刪除。

如需解決重複資料刪除相關問題的資訊，請參閱

使用下列資訊，以協助疑難排解設定和使用重複資料刪除時的一些常見問題。

主題

重複資料刪除無法運作

若要查看重複資料刪除的目前狀態，請執行 `Get-FSxDedupStatus` PowerShell 命令以檢視最新重複資料刪除任務的完成狀態。如果一或多個任務失敗，則檔案系統上可能無法看到可用的儲存容量增加。

重複資料刪除任務失敗的最常見原因是記憶體不足。

- Microsoft 建議最好擁有每 1 TB 邏輯資料的 1 GB 記憶體 （或每 1 TB 邏輯資料至少 350 MB)。使用 Amazon FSx 效能表來判斷與檔案系統輸送量容量相關聯的記憶體，並確保記憶體資源足以容納您的資料大小。如果不是，您需要將檔案系統的輸送量容量提高到符合每 1 TB 邏輯資料記憶體需求 1 GB 的層級。
- 重複資料刪除任務設定為 Windows 建議的預設值 25% 記憶體配置，這表示對於具有 32 GB 記憶體的檔案系統，8 GB 將可用於重複資料刪除。記憶體配置是可設定的 （使用 Set-

FSxDedupSchedule命令搭配 參數 -Memory)。請注意，使用較高的記憶體配置進行刪除可能會影響檔案系統效能。

- 您可以修改重複資料刪除任務的組態，以減少所需的記憶體量。例如，您可以限制最佳化以在特定檔案類型或資料夾上執行，或設定最佳化的最小檔案大小和期限。當您的檔案系統負載最少時，我們也建議設定重複資料刪除任務在閒置期間執行。

如果重複資料刪除任務的時間不足而無法完成，您也可能看到錯誤。您可能需要變更任務的最長持續時間，如中所述修改重複資料刪除排程。

如果重複資料刪除任務長時間失敗，且在此期間檔案系統上的資料有所變更，則後續重複資料刪除任務可能需要更多資源才能第一次成功完成。

重複資料刪除值意外設定為 0

SavedSpace 和 的值意外OptimizedFilesSavingsRate為 0，表示您在其中設定了重複資料刪除的檔案系統。

當您增加檔案系統的儲存容量時，這可能會在儲存最佳化過程中發生。當您增加檔案系統的儲存容量時，Amazon FSx 會在儲存最佳化程序期間取消現有的重複資料刪除任務，將資料從舊磁碟遷移到新的大型磁碟。儲存最佳化任務完成後，Amazon FSx 會在檔案系統上繼續重複資料刪除。如需增加儲存容量和儲存最佳化的詳細資訊，請參閱管理儲存容量。

刪除檔案後，檔案系統不會釋放空間

重複資料刪除的預期行為是，如果已刪除的資料是 dedup 節省了空間，則在垃圾收集任務執行之前，檔案系統上不會實際釋放空間。

您可能會發現有用的做法是設定排程，以便在刪除大量檔案後立即執行垃圾收集任務。垃圾收集任務完成後，您可以將垃圾收集排程設回其原始設定。這可確保您可以立即從刪除中快速查看空間。

使用下列程序，將垃圾收集任務設定為在 5 分鐘內執行。

1. 若要確認已啟用重複資料刪除功能，請使用 Get-FSxDedupStatus命令。如需 命令及其預期輸出的詳細資訊，請參閱 檢視已儲存空間的數量。
2. 使用下列設定排程，從現在開始 5 分鐘執行垃圾收集任務。

```
$FiveMinutesFromNowUTC = ((get-date).AddMinutes(5)).ToUniversalTime()
$DayOfWeek = $FiveMinutesFromNowUTC.DayOfWeek
$Time = $FiveMinutesFromNowUTC.ToString("HH:mm")
```

```
Invoke-Command -ComputerName ${RPS_ENDPOINT} -ConfigurationName FSxRemoteAdmin -
ScriptBlock {

    Set-FSxDedupSchedule -Name "WeeklyGarbageCollection" -Days $Using:DayOfWeek -
Start $Using:Time -DurationHours 9
}
```

3. 垃圾收集任務執行且空間已釋出後，請將排程設回其原始設定。

。

如需重複資料刪除的詳細資訊，請參閱 Microsoft 了解重複資料刪除文件。

> **Warning**
>
> 不建議執行具有重複資料刪除的特定 Robocopy 命令，因為這些命令可能會影響區塊存放區的資料完整性。如需詳細資訊，請參閱 Microsoft Data Deduplication 互通性文件。

使用重複資料刪除時的最佳實務

以下是使用重複資料刪除的一些最佳實務：

- 排程在檔案系統閒置時執行重複資料刪除任務：預設排程包含每週任務，每週`GarbageCollection`任務的 UTC 為星期六 2：45。如果您的檔案系統上有大量資料流失，可能需要數小時才能完成。如果此時間不適合您的工作負載，請將此任務安排在預期檔案系統流量低時執行。
- 設定足夠的輸送量容量以完成重複資料刪除：較高的輸送量可提供更高層級的記憶體。Microsoft 建議每 1 TB 邏輯資料有 1 GB 的記憶體來執行重複資料刪除。使用 Amazon FSx 效能表來判斷與您檔案系統輸送量容量相關聯的記憶體，並確保記憶體資源足以滿足資料大小。
- 自訂重複資料刪除設定，以滿足您的特定儲存需求並降低效能需求：您可以限制最佳化以在特定檔案類型或資料夾上執行，或設定最佳化的最小檔案大小和使用期限。如需進一步了解，請參閱 使用重複資料刪除來降低儲存成本。

管理儲存配額

您可以在檔案系統上設定使用者儲存配額，以限制使用者可以使用的資料儲存量。設定配額後，您可以追蹤配額狀態以監控用量，並查看使用者何時超過配額。

您也可以透過阻止達到配額的使用者寫入儲存空間來強制執行配額。當您強制執行配額時，超出配額的使用者會收到「磁碟空間不足」錯誤訊息。

您可以為配額設定設定這些閾值：

- 警告 - 用於追蹤使用者或群組是否接近配額限制，僅與追蹤相關。
- 限制 – 使用者或群組的儲存配額限制。

您可以設定預設配額，這些配額會套用到存取檔案系統和配額的新使用者，這些配額會套用到特定使用者或群組。您也可以檢視報告，了解每個使用者或群組耗用多少儲存空間，以及他們是否超過配額。

使用者層級的儲存體使用量會根據檔案擁有權進行追蹤。儲存體耗用是使用邏輯檔案大小計算，而不是檔案佔用的實際實體儲存空間。資料寫入檔案時，會追蹤使用者儲存配額。

更新多個使用者的配額時，需要為每個使用者執行一次更新命令，或將使用者組織為群組，並更新該群組的配額。

您可以使用 Amazon FSx CLI 在 PowerShell 上進行遠端管理，在檔案系統上管理使用者儲存配額。若要了解如何使用此 CLI，請參閱使用 Amazon FSx CLI for PowerShell。

以下是可用於管理使用者儲存配額的命令。

使用者儲存配額命令	描述
Enable-FSxUserQuotas	開始追蹤或強制執行使用者儲存配額，或兩者。
Disable-FSxUserQuotas	停止追蹤和強制執行使用者儲存配額。
Get-FSxUserQuotaSettings	擷取檔案系統的目前使用者儲存配額設定。
Get-FSxUserQuotaEntries	擷取檔案系統上個別使用者和群組的目前使用者儲存配額項目。
Set-FSxUserQuotas	設定個別使用者或群組的使用者儲存配額。配額值以位元組為單位指定。

每個命令的線上說明提供所有命令選項的參考。若要存取此說明，請使用 執行 命令-?，例如 Enable-FSxUserQuotas -?。

增加檔案系統儲存容量

您可以隨著儲存需求變更，增加 FSx for Windows File Server 檔案系統的儲存容量。使用 Amazon FSx 主控台 AWS CLI、 或 Amazon FSx API 來增加檔案系統的儲存容量，如下列程序所述。如需詳細資訊，請參閱管理儲存容量。

增加檔案系統的儲存容量 （主控台）

1. 在 https://console.aws.amazon.com/fsx/：// 開啟 Amazon FSx 主控台。
2. 導覽至檔案系統，然後選擇您要增加儲存容量的 Windows 檔案系統。
3. 針對動作，選擇更新儲存體。或者，在摘要面板中，選擇檔案系統的儲存容量旁的更新。

   更新儲存容量視窗隨即出現。
4. 針對輸入類型，選擇百分比以輸入新儲存容量做為與目前值的百分比變更，或選擇絕對以 GiB 輸入新值。
5. 輸入所需的儲存容量。

   > **Note**
   >
   > 所需的容量值必須至少大於目前值的 10%，最大值上限為 65，536 GiB。

6. 選擇更新以啟動儲存容量更新。
7. 您可以在檔案系統詳細資訊頁面的更新索引標籤中監控更新進度。

增加檔案系統的儲存容量 (CLI)

若要增加 FSx for Windows File Server 檔案系統的儲存容量，請使用 AWS CLI 命令 update-file-system。設定下列參數：

- `--file-system-id` 至您正在更新之檔案系統的 ID。
- `--storage-capacity` 的值至少比目前值大 10%。

您可以使用 AWS CLI 命令 describe-file-systems 來監控更新進度。在輸出`administrative-actions`中尋找 。

如需詳細資訊，請參閱 AdministrativeAction。

監控儲存容量增加

增加檔案系統的儲存容量後，您可以使用 Amazon FSx 主控台、API 或 監控儲存容量增加的進度 AWS CLI ，如下列程序所述。

在主控台中監控增加

在檔案系統詳細資訊視窗中的更新索引標籤中，您可以檢視每個更新類型的 10 個最新更新。

如需儲存容量更新，您可以檢視下列資訊。

更新類型

可能的值是儲存容量。

目標值

更新檔案系統的儲存容量所需的值。

狀態

更新的目前狀態。對於儲存容量更新，可能的值如下所示：

- 待處理 – Amazon FSx 已收到更新請求，但尚未開始處理。
- 進行中 – Amazon FSx 正在處理更新請求。
- 更新最佳化 – Amazon FSx 已增加檔案系統的儲存容量。儲存最佳化程序現在正在將檔案系統資料移至新的大型磁碟。
- 已完成 – 儲存容量增加已成功完成。
- 失敗 – 儲存容量增加失敗。選擇問號 (?) 以查看儲存更新失敗原因的詳細資訊。

進度 %

儲存最佳化程序的進度顯示為完成百分比。

請求時間

Amazon FSx 收到更新動作請求的時間。

監控會隨著 AWS CLI 和 API 而增加

您可以使用 describe-file-systems AWS CLI 命令和 DescribeFileSystems API 動作來檢視和監控檔案系統儲存容量增加請求。`AdministrativeActions` 陣列會列出每個管理動作類型的 10 個最近更新動作。當您增加檔案系統的儲存容量時，`AdministrativeActions`會產生兩個：`FILE_SYSTEM_UPDATE`和 `STORAGE_OPTIMIZATION`動作。

下列範例顯示 CLI describe-file-systems 命令回應的摘錄。檔案系統的儲存容量為 300 GB，而且有待定的管理動作，可將儲存容量增加到 1000 GB。

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 300,
            "AdministrativeActions": [
                {
                     "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                     "RequestTime": 1581694764.757,
                     "Status": "PENDING",
                     "TargetFileSystemValues": {
                         "StorageCapacity": 1000
                     }
                },
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
                    "Status": "PENDING",
                }
            ]
```

Amazon FSx 會先處理FILE_SYSTEM_UPDATE動作，將新的大型儲存磁碟新增至檔案系統。當新的儲存可供檔案系統使用時，FILE_SYSTEM_UPDATE狀態會變更為 UPDATED_OPTIMIZING。儲存容量會顯示新的較大值，Amazon FSx 會開始處理STORAGE_OPTIMIZATION管理動作。這會顯示在 CLI describe-file-systems 命令回應的下列摘錄中。

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

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
```

```
            .
            "StorageCapacity": 1000,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "RequestTime": 1581694764.757,
                    "Status": "UPDATED_OPTIMIZING",
                    "TargetFileSystemValues": {
                        "StorageCapacity": 1000
                }
                },
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
                    "Status": "IN_PROGRESS",
                    "ProgressPercent": 50,
                }
            ]
```

如果儲存容量增加失敗，FILE_SYSTEM_UPDATE動作的狀態會變更為 FAILED。FailureDetails 屬性提供有關失敗的資訊，如下列範例所示。

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 300,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "FailureDetails": {
                        "Message": "string"
                    },
                    "RequestTime": 1581694764.757,
                    "Status": "FAILED",
                    "TargetFileSystemValues":
                        "StorageCapacity": 1000
                }
            ]
```

如需故障診斷失敗動作的相關資訊，請參閱 儲存或輸送量容量更新失敗。

動態增加 FSx for Windows File Server 檔案系統的儲存容量

除了隨著儲存的資料量增加，手動增加 FSx for Windows File Server 檔案系統的儲存容量外，您也可以使用 CloudFormation 範本自動增加儲存。本節中介紹的解決方案會在可用儲存容量低於您指定的定義閾值時，動態增加檔案系統的儲存容量。

此 AWS CloudFormation 範本會自動部署定義可用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 函數。

解決方案採用下列參數：

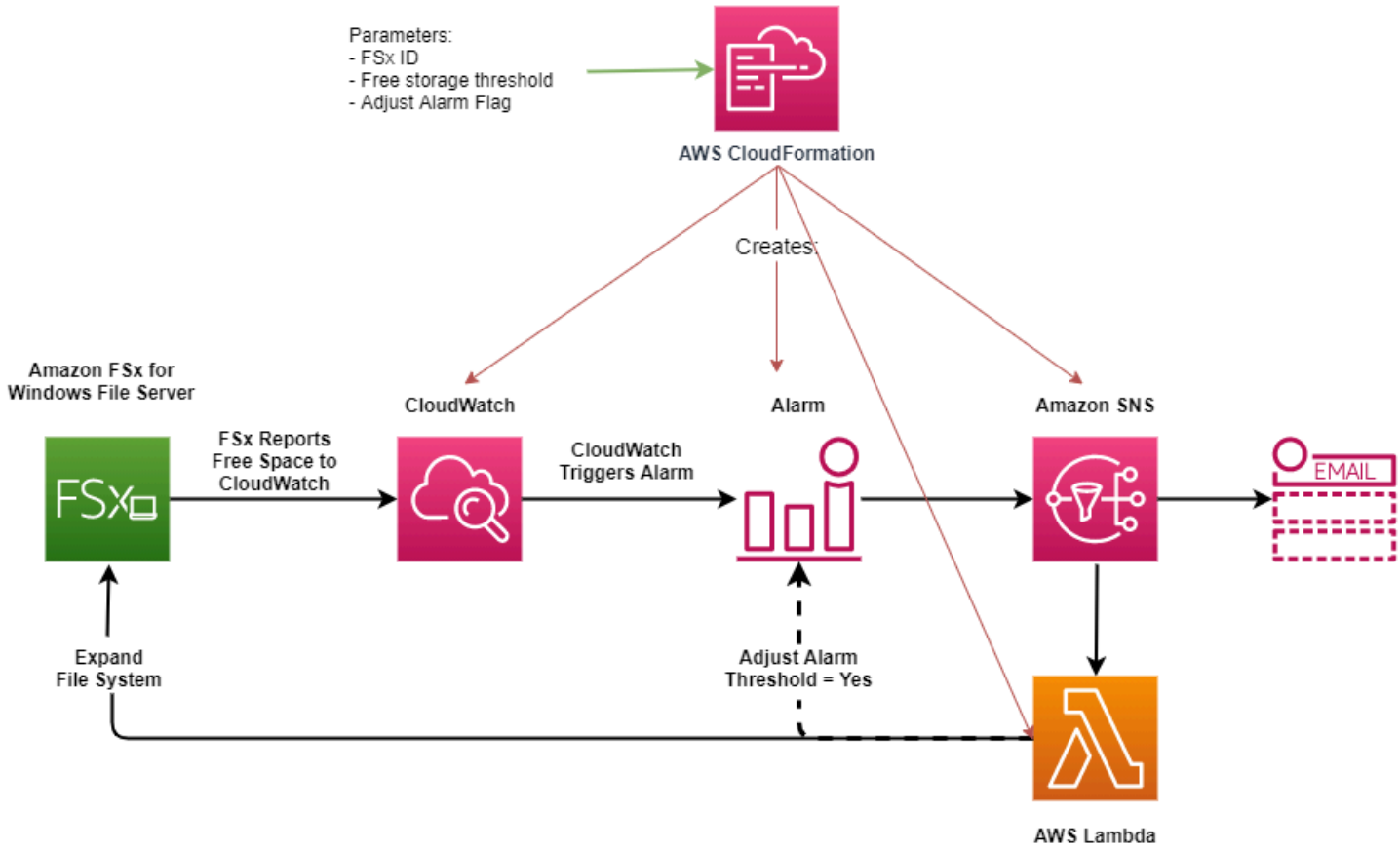
- 檔案系統 ID
- 可用儲存容量閾值 （ 數值 ）
- 度量單位 （ 百分比 【預設】 或 GiB)
- 增加儲存容量的百分比 (%)
- SNS 訂閱的電子郵件地址
- 調整警示閾值 （ 是/否 ）

主題

- 架構概觀
- CloudFormation 範本
- 使用 自動部署 CloudFormation

架構概觀

部署此解決方案會在 AWS 雲端中建置下列資源。



此圖說明了下列步驟：

1. CloudFormation 範本會部署 CloudWatch 警示、 AWS Lambda 函數、Amazon Simple Notification Service (Amazon SNS) 佇列，以及所有必要 AWS Identity and Access Management (IAM) 角色。IAM 角色提供 Lambda 函數呼叫 Amazon FSx API 操作的許可。
2. 當檔案系統的可用儲存容量低於指定的閾值時，CloudWatch 會觸發警示，並將訊息傳送至 Amazon SNS 佇列。
3. 解決方案接著會觸發訂閱此 Amazon SNS 主題的 Lambda 函數。
4. Lambda 函數會根據指定的百分比增加值計算新的檔案系統儲存容量，並設定新的檔案系統儲存容量。
5. Lambda 函數可以選擇性地調整可用儲存容量閾值，使其等於檔案系統新儲存容量的指定百分比。
6. 原始 CloudWatch 警示狀態和 Lambda 函數操作的結果會傳送至 Amazon SNS 佇列。

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

CloudFormation 範本

此解決方案使用 CloudFormation 自動部署元件，這些元件用於自動增加 FSx for Windows File Server 檔案系統的儲存容量。若要使用此解決方案，請下載 IncreaseFSxSize CloudFormation 範本。

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

FileSystemId

無預設值。您要自動增加儲存容量的檔案系統 ID。

LowFreeDataStorageCapacityThreshold

無預設值。指定初始可用儲存容量閾值，以觸發警示並自動增加以 GiB 指定的檔案系統的儲存容量，或以檔案系統目前儲存容量的百分比 (%) 表示。當以百分比表示時，CloudFormation 範本會重新計算為 GiB，以符合 CloudWatch 警示設定。

LowFreeDataStorageCapacityThresholdUnit

預設為 %。以 `LowFreeDataStorageCapacityThreshold` GiB 或目前儲存容量的百分比來指定 的單位。

AlarmModificationNotification

預設為是。如果設定為是，初始 `LowFreeDataStorageCapacityThreshold`會按比例增加為後續警示閾值`PercentIncrease`的 值。

例如，當 `PercentIncrease` 設為 20 且 AlarmModificationNotification 設為 Yes 時，GiB 中指定的可用空間閾值 (`LowFreeDataStorageCapacityThreshold`) 會針對後續儲存容量增加事件增加 20%。

EmailAddress

無預設值。指定用於 SNS 訂閱的電子郵件地址，並接收儲存容量閾值提醒。

PercentIncrease

無預設值。指定增加儲存容量的數量，以目前儲存容量的百分比表示。

使用 自動部署 CloudFormation

下列程序會設定和部署 CloudFormation 堆疊，以自動增加 FSx for Windows File Server 檔案系統的儲存容量。部署大約需要 5 分鐘。

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

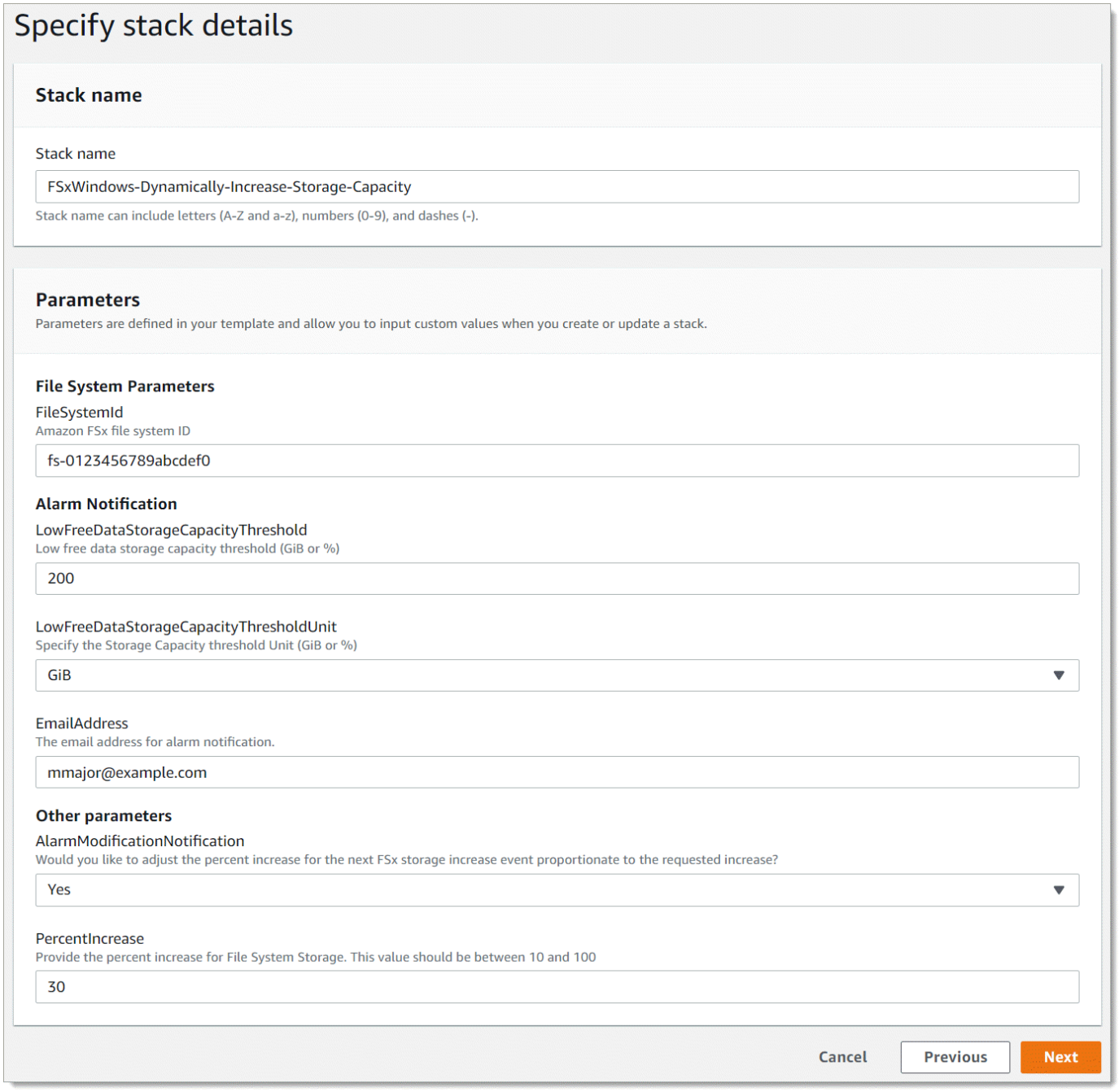
開始之前，您必須在 AWS 帳戶中的 Amazon Virtual Private Cloud (Amazon VPC) 中執行 Amazon FSx 檔案系統的 ID。如需建立 Amazon FSx 資源的詳細資訊，請參閱Amazon FSx for Windows File Server 入門。

啟動自動儲存容量增加解決方案堆疊

1. 下載 IncreaseFSxSize CloudFormation 範本。如需建立 CloudFormation 堆疊的詳細資訊，請參閱AWS CloudFormation 《 使用者指南》中的在 AWS CloudFormation 主控台上建立堆疊。

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

2. 在指定堆疊詳細資訊中，輸入自動儲存容量增加解決方案的值。



3. 輸入堆疊名稱。
4. 對於 參數，請檢閱範本的參數，並根據檔案系統的需求修改它們。然後選擇下一步。
5. 輸入自訂解決方案所需的任何選項設定，然後選擇下一步。
6. 針對檢閱，檢閱並確認解決方案設定。您必須選取確認範本建立 IAM 資源的核取方塊。
7. 選擇建立以部署堆疊。

您可以在狀態欄的 CloudFormation 主控台中檢視堆疊的狀態。您應該會在大約 5 分鐘內看到 CREATE_COMPLETE 狀態。

更新堆疊

建立堆疊之後，您可以使用相同的範本並針對參數提供新的值來更新堆疊。如需詳細資訊，請參閱AWS CloudFormation 《 使用者指南》中的直接更新堆疊。

更新 FSx for Windows 檔案系統的儲存類型

您可以變更使用 HDD 儲存來使用 SSD 儲存的檔案系統的儲存類型。您可以使用 Amazon FSx 主控台 AWS CLI、 或 Amazon FSx API 來變更檔案系統的儲存類型，如下列程序所示。如需詳細資訊，請參閱管理檔案系統的儲存類型。

更新檔案系統的儲存類型 （ 主控台 ）

1. 在 https://console.aws.amazon.com/fsx/ ：// 開啟 Amazon FSx 主控台。
2. 導覽至檔案系統，然後選擇您要更新儲存類型的 Windows 檔案系統。
3. 在動作下，選擇更新儲存體類型。或者，在摘要面板中，選取 HDD 旁的更新按鈕。更新儲存類型視窗隨即出現。
4. 針對所需的儲存體類型，選擇 SSD。選擇更新以啟動儲存類型更新。

   您可以使用 主控台和 CLI 監控儲存類型更新的進度。

更新檔案系統的儲存類型 (CLI)

若要更新 FSx for Windows File Server 檔案系統的儲存類型，請使用 AWS CLI 命令 update-file-system。設定下列參數：

- `--file-system-id` 至您要更新之檔案系統的 ID。
- `--storage-type` 至 SSD。您無法從 SSD 儲存體類型切換到 HDD 儲存體類型。

您可以使用 AWS CLI 命令 describe-file-systems 來監控更新進度。在輸出`administrative-actions`中尋找 。

如需詳細資訊，請參閱 AdministrativeAction。

監控儲存類型更新

將檔案系統的儲存類型從 HDD 更新為 SSD 儲存之後，您可以使用 Amazon FSx 主控台 AWS CLI、或 API 監控儲存類型更新的進度，如下列程序所述。

在 主控台中監控檔案系統更新

在檔案系統詳細資訊視窗中的更新索引標籤上，您可以檢視每個更新類型的 10 個最新更新。

如需儲存類型更新，您可以檢視下列資訊。

更新類型

可能的值是儲存類型。

目標值

SSD

狀態

更新的目前狀態。對於儲存類型更新，可能的值如下所示：

- 待處理 – Amazon FSx 收到更新請求，但尚未開始處理。
- 進行中 – Amazon FSx 正在處理更新請求。
- 更新最佳化 – SSD 儲存效能可用於寫入操作。更新會進入更新最佳化狀態，通常持續數小時，在此期間，讀取操作在 HDD 和 SSD 之間會有效能層級。更新動作完成後，新的 SSD 效能可供讀取和寫入使用。
- 已完成 – 儲存類型更新已成功完成。
- 失敗 – 儲存類型更新失敗。選擇問號 (?) 以查看詳細資訊。

進度 %

依完成的百分比顯示儲存最佳化程序的進度。

請求時間

Amazon FSx 收到更新動作請求的時間。

使用 AWS CLI 和 API 監控更新

您可以使用 describe-file-systems AWS CLI 命令和 DescribeFileSystems API 動作來檢視和監控檔案系統儲存類型更新請求。`AdministrativeActions` 陣列會列出每個管理動作類型的 10 個

最近更新動作。當您增加檔案系統的 SSD IOPS 時，AdministrativeActions會產生兩個：FILE_SYSTEM_UPDATE和 STORAGE_TYPE_OPTIMIZATION動作。

更新檔案系統的 SSD IOPS

對於使用 SSD 儲存體設定的檔案系統，佈建的 SSD IOPS 層級會決定檔案系統必須讀取資料並將資料寫入磁碟時可用的磁碟 I/O 數量，而不是讀取或寫入快取中的資料。您可以使用 Amazon FSx 主控台、 AWS CLI或 Amazon FSx API 更新檔案系統的 SSD IOPS，如下列程序所述。如需管理 SSD IOPS 的詳細資訊，請參閱 管理 SSD IOPS。

更新檔案系統的 SSD IOPS （主控台）

1. 在 https://console.aws.amazon.com/fsx/：// 開啟 Amazon FSx 主控台。
2. 導覽至檔案系統，然後選擇您要更新 SSD IOPS 的 Windows 檔案系統。
3. 在動作下，選擇更新 SSD IOPS。或者，在摘要面板中，選取佈建 SSD IOPS 旁的更新按鈕。更新 IOPS 佈建視窗隨即開啟。
4. 針對 模式，選擇自動或使用者佈建。如果您選擇自動，Amazon FSx 會自動為您的檔案系統每 GiB 儲存容量佈建 3 個 SSD IOPS。如果您選擇使用者佈建，請輸入 96–400，000 範圍內的任何整數。
5. 選擇更新以啟動佈建的 SSD IOPS 更新。
6. 您可以在檔案系統詳細資訊頁面的更新索引標籤上監控更新進度。

更新檔案系統的 SSD IOPS (CLI)

若要更新 FSx for Windows File Server 檔案系統的 SSD IOPS，請使用 `--windows-configuration DiskIopsConfiguration` 屬性。此屬性有兩個參數 `Iops`和 `Mode`：

- 如果您想要指定 SSD IOPS 的數量，請使用 `Iops=`*`number_of_IOPS`*，在支援 AWS 的區域和 中上限為 400，000`Mode=USER_PROVISIONED`。
- 如果您希望 Amazon FSx 自動增加 SSD IOPS，請使用 `Mode=AUTOMATIC`，請勿使用 `Iops` 參數。Amazon FSx 會在檔案系統上自動維護每 GiB 儲存容量 3 個 SSD IOPS，支援 AWS 區域中最多 400，000 個。

您可以使用 describe-file-systems AWS CLI 命令來監控更新進度。在輸出`administrative-actions`中尋找 。

如需詳細資訊，請參閱 AdministrativeAction。

監控佈建的 SSD IOPS 更新

更新檔案系統的佈建 SSD IOPS 數量後，您可以使用 Amazon FSx 主控台 AWS CLI、 和 API 監控 SSD IOPS 更新的進度，如下列程序所述。

在主控台中監控更新

在檔案系統詳細資訊視窗中的更新索引標籤中，您可以檢視每個更新類型的 10 個最近更新。

對於佈建的 SSD IOPS 更新，您可以檢視以下資訊。

更新類型

可能的值為 IOPS 模式和 SSD IOPS。

目標值

更新檔案系統 IOPS 模式和 SSD IOPS 的目標值。

狀態

更新的目前狀態。對於 SSD IOPS 更新，可能的值如下所示：

- 待處理 – Amazon FSx 已收到更新請求，但尚未開始處理。
- 進行中 – Amazon FSx 正在處理更新請求。
- 更新最佳化 – 新的 IOPS 層級可用於工作負載的寫入操作。您的更新會進入更新最佳化狀態，此狀態通常持續數小時，在此期間，工作負載的讀取操作在上一個層級和新層級之間具有 IOPS 效能。更新動作完成後，新的 IOPS 層級即可用於讀取和寫入。
- 已完成 – SSD IOPS 更新已成功完成。
- 失敗 – SSD IOPS 更新失敗。選擇問號 (?) 以查看儲存更新失敗原因的詳細資訊。

進度 %

儲存最佳化程序的進度顯示為完成百分比。

請求時間

Amazon FSx 收到更新動作請求的時間。

使用 AWS CLI 和 API 監控更新

您可以使用 describe-file-systems AWS CLI 命令和 DescribeFileSystems API 動作來檢視和監控檔案系統 SSD IOPS 更新請求。`AdministrativeActions` 陣列會列出每個管理動作類型的 10

個最近更新動作。當您增加檔案系統的 SSD IOPS 時，AdministrativeActions會產生兩個：FILE_SYSTEM_UPDATE和 IOPS_OPTIMIZATION動作。

管理重複資料刪除

您可以使用 Amazon FSx CLI 在 PowerShell 上進行遠端管理，來管理檔案系統的重複資料刪除設定。如需在 PowerShell 上使用 Amazon FSx CLI 遠端管理的詳細資訊，請參閱 使用 Amazon FSx CLI for PowerShell。

以下是可用於重複資料刪除的命令。

重複資料刪除命令	描述
Enable-FSxDedup	在檔案共用上啟用重複資料刪除。當您啟用重複資料刪除時，預設會啟用重複資料刪除之後的資料壓縮。
Disable-FSxDedup	停用檔案共用上的重複資料刪除功能。
Get-FSxDedupConfiguration	擷取重複資料刪除組態資訊，包括最佳化的最小檔案大小和使用期、壓縮設定，以及排除的檔案類型和資料夾。
Set-FSxDedupConfiguration	變更重複資料刪除組態設定，包括最佳化的最小檔案大小和期限、壓縮設定，以及排除的檔案類型和資料夾。
Get-FSxDedupStatus	擷取重複資料刪除狀態，並包含唯讀屬性，描述檔案系統最佳化節省和檔案系統狀態、時間，以及檔案系統上最後重複資料刪除任務的完成狀態。
Get-FSxDedupMetadata	擷取重複資料刪除最佳化中繼資料。
Update-FSxDedupStatus	計算和擷取更新的重複資料刪除節省資訊。
Measure-FSxDedupFileMetadata	如果您刪除一組資料夾，請測量和擷取您可以在檔案系統上回收的潛在儲存空間。檔案通常具有跨其他資料夾共用的區塊，而重複資料刪除引擎會計算哪些區塊是唯一的，並將被刪除。
Get-FSxDedupSchedule	擷取目前定義的重複資料刪除排程。
New-FSxDedupSchedule	建立和自訂重複資料刪除排程。

重複資料刪除命令	描述
Set-FSxDedupSchedule	變更現有重複資料刪除排程的組態設定。
Remove-FSxDedupSchedule	刪除重複資料刪除排程。
Get-FSxDedupJob	取得所有目前執行中或佇列重複資料刪除任務的狀態和資訊。
Stop-FSxDedupJob	取消一或多個指定的重複資料刪除任務。

每個命令的線上說明提供所有命令選項的參考。若要存取此說明，請使用 執行 命令-?，例如 Enable-FSxDedup -?。

啟用重複資料刪除

您可以使用 `Enable-FSxDedup`命令在 Amazon FSx for Windows File Server 檔案共享上啟用重複資料刪除，如下所示。

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {Enable-FsxDedup }
```

當您啟用重複資料刪除時，會建立預設排程和組態。您可以使用以下命令建立、修改和移除排程和組態。

您可以使用 `Disable-FSxDedup`命令來完全停用檔案系統上的重複資料刪除功能。

建立重複資料刪除排程

雖然預設排程在大多數情況下都運作良好，但您可以使用 `New-FsxDedupSchedule`命令建立新的重複資料刪除排程，如下所示。重複資料刪除排程使用 UTC 時間。

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {
New-FSxDedupSchedule -Name "CustomOptimization" -Type Optimization -Days Mon,Wed,Sat -
Start 08:00 -DurationHours 7
}
```

此命令會建立名為 `CustomOptimization` 的排程，在星期一、星期三和星期六的天執行，從每天上午 8：00 (UTC) 開始任務，最長持續時間為 7 小時，之後如果任務仍在執行，則會停止。

請注意，建立新的自訂重複資料刪除任務排程不會覆寫或移除現有的預設排程。建立自訂重複資料刪除任務之前，如果您不需要，建議您停用預設任務。

您可以使用 Set-FsxDedupSchedule命令來停用預設重複資料刪除排程，如下所示。

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com
 -ConfigurationName FSxRemoteAdmin -ScriptBlock {Set-FSxDedupSchedule -Name
 “BackgroundOptimization” -Enabled $false}
```

您可以使用 Remove-FSxDedupSchedule -Name "ScheduleName"命令移除重複資料刪除排程。請注意，預設的重複BackgroundOptimization資料刪除排程無法修改或移除，因此需要改為停用。

修改重複資料刪除排程

您可以使用 Set-FsxDedupSchedule命令來修改現有的重複資料刪除排程，如下所示。

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {
Set-FSxDedupSchedule -Name "CustomOptimization" -Type Optimization -Days
 Mon,Tues,Wed,Sat -Start 09:00 -DurationHours 9
}
```

此命令會修改現有的CustomOptimization排程，以在星期一至星期三和星期六的天數執行，從每天上午 9：00 (UTC) 開始任務，最長持續時間為 9 小時，之後任務仍會在仍在執行時停止。

若要在最佳化設定之前修改最低檔案使用期，請使用 Set-FSxDedupConfiguration命令。

檢視已儲存空間的數量

若要檢視您從執行重複資料刪除中節省的磁碟空間量，請使用 Get-FSxDedupStatus命令，如下所示。

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FsxRemoteAdmin -ScriptBlock {
Get-FSxDedupStatus } | select
 OptimizedFilesCount,OptimizedFilesSize,SavedSpace,OptimizedFilesSavingsRate

OptimizedFilesCount OptimizedFilesSize SavedSpace OptimizedFilesSavingsRate
------------------- ------------------ ---------- -------------------------
              12587           31163594   25944826                        83
```

> **Note**
>
> 下列參數的命令回應中顯示的值不可靠，您不應該使用這些值：Capacity、FreeSpace、UsedSpace、UnoptimizedSize 和 SavingsRate。

對重複資料刪除進行故障診斷

使用下列資訊，以協助疑難排解設定和使用重複資料刪除時的一些常見問題。

主題

- 重複資料刪除無法運作
- 重複資料刪除值意外設定為 0
- 刪除檔案後，檔案系統不會釋放空間

重複資料刪除無法運作

若要查看重複資料刪除的目前狀態，請執行 `Get-FSxDedupStatus` PowerShell 命令以檢視最新重複資料刪除任務的完成狀態。如果一或多個任務失敗，則檔案系統上可能無法看到可用的儲存容量增加。

重複資料刪除任務失敗的最常見原因是記憶體不足。

- Microsoft 建議最好擁有每 1 TB 邏輯資料的 1 GB 記憶體（或每 1 TB 邏輯資料至少 350 MB)。使用 Amazon FSx 效能表來判斷與檔案系統輸送量容量相關聯的記憶體，並確保記憶體資源足以容納您的資料大小。如果不是，您需要將檔案系統的輸送量容量提高到符合每 1 TB 邏輯資料記憶體需求 1 GB 的層級。
- 重複資料刪除任務設定為 Windows 建議的預設值 25% 記憶體配置，這表示對於具有 32 GB 記憶體的檔案系統，8 GB 將可用於重複資料刪除。記憶體配置是可設定的（使用 `Set-FSxDedupSchedule`命令搭配 參數 `-Memory`)。請注意，使用較高的記憶體配置進行刪除可能會影響檔案系統效能。
- 您可以修改重複資料刪除任務的組態，以減少所需的記憶體量。例如，您可以限制最佳化以在特定檔案類型或資料夾上執行，或設定最佳化的最小檔案大小和期限。當您的檔案系統負載最少時，我們也建議設定重複資料刪除任務在閒置期間執行。

如果重複資料刪除任務的時間不足而無法完成，您也可能看到錯誤。您可能需要變更任務的最長持續時間，如中所述修改重複資料刪除排程。

如果重複資料刪除任務長時間失敗，且在此期間檔案系統上的資料有所變更，則後續重複資料刪除任務可能需要更多資源才能第一次成功完成。

重複資料刪除值意外設定為 0

`SavedSpace` 和 的值意外`OptimizedFilesSavingsRate`為 0，表示您在其中設定了重複資料刪除的檔案系統。

當您增加檔案系統的儲存容量時，這可能會在儲存最佳化過程中發生。當您增加檔案系統的儲存容量時，Amazon FSx 會在儲存最佳化程序期間取消現有的重複資料刪除任務，將資料從舊磁碟遷移到新的大型磁碟。儲存最佳化任務完成後，Amazon FSx 會在檔案系統上繼續重複資料刪除。如需增加儲存容量和儲存最佳化的詳細資訊，請參閱管理儲存容量。

刪除檔案後，檔案系統不會釋放空間

重複資料刪除的預期行為是，如果已刪除的資料是 dedup 節省了空間，則在垃圾收集任務執行之前，檔案系統上不會實際釋放空間。

您可能會發現有用的做法是設定排程，以便在刪除大量檔案後立即執行垃圾收集任務。垃圾收集任務完成後，您可以將垃圾收集排程設回其原始設定。這可確保您可以立即從刪除中快速查看空間。

使用下列程序，將垃圾收集任務設定為在 5 分鐘內執行。

1. 若要確認已啟用重複資料刪除功能，請使用 `Get-FSxDedupStatus`命令。如需 命令及其預期輸出的詳細資訊，請參閱 檢視已儲存空間的數量。
2. 使用下列設定排程，從現在開始 5 分鐘執行垃圾收集任務。

```
$FiveMinutesFromNowUTC = ((get-date).AddMinutes(5)).ToUniversalTime()
$DayOfWeek = $FiveMinutesFromNowUTC.DayOfWeek
$Time = $FiveMinutesFromNowUTC.ToString("HH:mm")

Invoke-Command -ComputerName ${RPS_ENDPOINT} -ConfigurationName FSxRemoteAdmin -
ScriptBlock {
    Set-FSxDedupSchedule -Name "WeeklyGarbageCollection" -Days $Using:DayOfWeek -
Start $Using:Time -DurationHours 9
}
```

3. 垃圾收集任務執行且空間已釋出後，請將排程設回其原始設定。

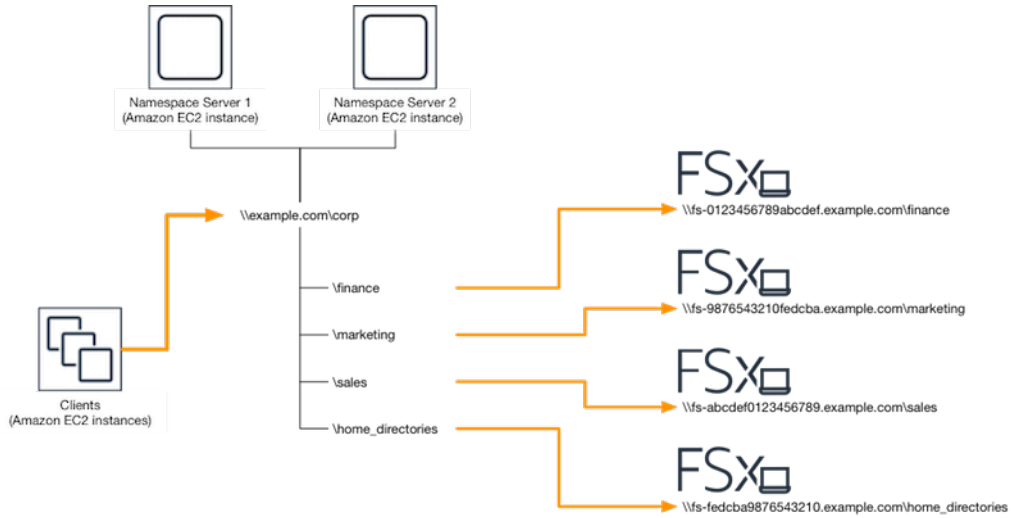
使用 DFS 命名空間

DFS 命名空間是一種 Windows Server 角色服務，可用來將位於不同伺服器上的共用資料夾分組為一或多個邏輯結構命名空間。這讓使用者可以虛擬檢視共用資料夾，其中單一路徑會導向位於多個檔案系統上的檔案，如下圖所示。除了組織和統一跨多個檔案系統對檔案共用的存取之外，

使用 DFS 命名空間將多個 FSx for Windows File Server 檔案系統分組

您可以使用 Microsoft 的分散式檔案系統 (DFS) 命名空間，將多個 FSx for Windows File Server 檔案系統上的檔案共用分組為一個通用資料夾結構或命名空間。使用 DFS 命名空間，您可以將檔案儲存擴展到超過大型檔案資料集的單一檔案系統 (64 TiB) 最大儲存容量，最多可達數百 PB。本節說明如何在多個 FSx for Windows File Server 檔案系統上設定 DFS 命名空間。

DFS 命名空間是一種 Windows Server 角色服務，可用來將位於不同伺服器上的共用資料夾分組為一或多個邏輯結構命名空間。這讓使用者可以虛擬檢視共用資料夾，其中單一路徑會導向位於多個檔案系統上的檔案，如下圖所示。除了組織和統一跨多個檔案系統對檔案共用的存取之外，



如需使用 DFS 命名空間分組 Windows 檔案系統的 step-by-step程序，請參閱 在單一命名空間下將多個檔案系統分組。 FSx

使用碎片改善效能

Amazon FSx for Windows File Server 支援使用 Microsoft 分散式檔案系統 (DFS)。透過使用 DFS 命名空間，您可以將檔案資料分散到多個 Amazon FSx 檔案系統，以擴展效能（讀取和寫入）來提供 I/O 密集型工作負載。同時，您仍然可以在應用程式的一般命名空間下呈現統一的檢視。此解決方案涉及將您的檔案資料分割為較小的資料集或碎片，並將其儲存在不同的檔案系統中。從多個執行個體存取資料的應用程式可以平行讀取和寫入這些碎片，以達到高水準的效能。

您可以使用 中提供的解決方案使用 DFS 命名空間來遮蔽資料，以實現橫向擴展效能，在多個 FSx for Windows File Server 檔案系統中統一分配資料的讀取/寫入存取權。

在單一命名空間下將多個檔案系統分組

在此程序中，您將在兩個命名空間伺服器上建立單一網域型命名空間 (`example.com\corp`)，以合併存放在多個 FSx for Windows 檔案系統 （ 財務、行銷、銷售、Home_directories) 上的檔案共用。您也將在命名空間下設定四個檔案共用，每個檔案共用都會透明地將使用者重新導向至託管於個別 FSx for Windows 檔案系統上的共用。這可讓您的使用者使用通用命名空間存取檔案共用，而不必為託管檔案共用的每個檔案系統指定 DNS 名稱。

> **Note**
>
> Amazon FSx 無法新增至 DFS 共用路徑的根目錄。

將多個檔案系統分組到通用的 DFS 命名空間

1. 如果您尚未讓 DFS 命名空間伺服器執行，您可以使用 setup-DFSN-servers.template CloudFormation 範本啟動一對高可用性的 DFS 命名空間伺服器。如需建立 CloudFormation 堆疊的詳細資訊，請參閱AWS CloudFormation 《 使用者指南》中的在 AWS CloudFormation 主控台上建立堆疊。
2. 以AWS 委派管理員群組中的使用者身分，連線至上一個步驟中啟動的其中一個 DFS 命名空間伺服器。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的連線至您的 Windows 執行個體。
3. 開啟 以存取 DFS 管理主控台。開啟開始功能表並執行 dfsmgmt.msc。這會開啟 DFS Management GUI 工具。
4. 選擇動作，然後選擇新命名空間，輸入您為伺服器啟動的第一個 DFS 命名空間伺服器的電腦名稱，然後選擇下一步。
5. 針對名稱，輸入您要建立的命名空間 （ 例如 corp)。
6. 選擇編輯設定，並根據您的需求設定適當的許可。選擇 Next (下一步)。
7. 保留預設的網域型命名空間選項，保留啟用 Windows Server 2008 模式選項，然後選擇下一步。

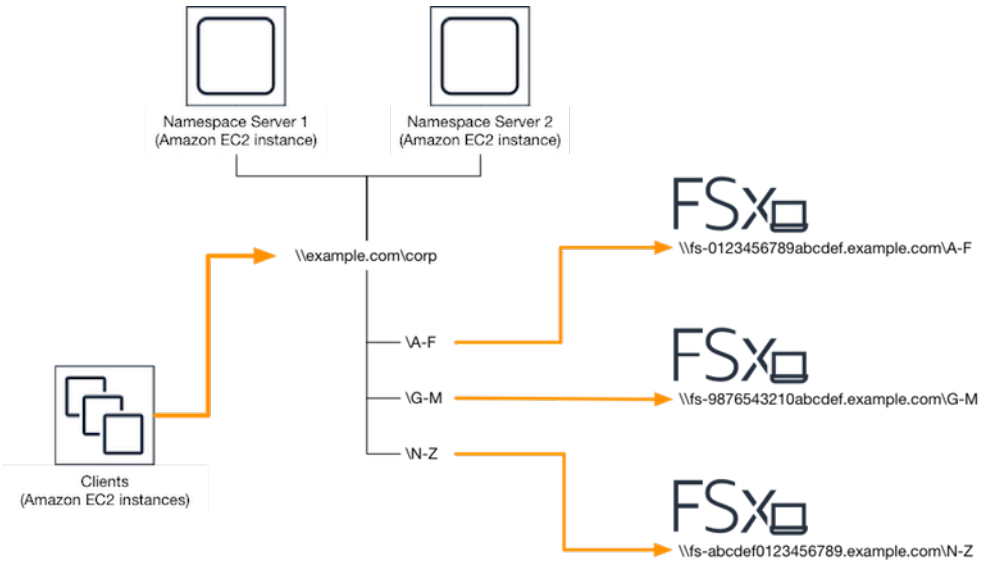
   > **Note**
   >
   > Windows Server 2008 模式是命名空間的最新可用選項。

8. 檢閱命名空間設定，然後選擇建立。

9. 在導覽列的命名空間下選取新建立的命名空間時，選擇動作，然後選擇新增命名空間伺服器。
10. 輸入您為命名空間伺服器啟動的第二個 DFS 命名空間伺服器的電腦名稱。
11. 選擇編輯設定，根據您的需求設定適當的許可，然後選擇確定。
12. 開啟您剛建立之命名空間的內容（按一下滑鼠右鍵）選單，選擇新資料夾，輸入資料夾的名稱（例如，finance針對名稱，然後選擇確定。
13. 輸入您希望 DFS 命名空間資料夾以 UNC 格式指向檔案共用的 DNS 名稱（例如，\\fs-0123456789abcdef0.example.com\finance)，以讓路徑指向資料夾目標，然後選擇確定。
14. 如果共用不存在：
    a. 選擇是來建立它。
    b. 從建立共用對話方塊中，選擇瀏覽。
    c. 選擇現有資料夾，或在 D$ 下建立新資料夾，然後選擇確定。
    d. 設定適當的共用許可，然後選擇確定。
15. 從新資料夾對話方塊中，選擇確定。新資料夾將在命名空間下建立。
16. 針對要在相同命名空間下共用的其他資料夾，重複最後四個步驟。

使用 DFS 命名空間來遮蔽資料，以實現橫向擴展效能

下列程序會引導您在 Amazon FSx 上建立 DFS 解決方案，以取得橫向擴展效能。在此範例中，存放在 *corp* 命名空間中的資料會依字母順序碎片。資料檔案「A-F」、「G-M」和「N-Z」都存放在不同的檔案共享中。根據資料類型、I/O 大小和 I/O 存取模式，您應該決定如何在多個檔案共享之間最好地分割資料。選擇分片慣例，將 I/O 平均分佈到您計劃使用的所有檔案共用。請記住，每個命名空間最多支援 50，000 個檔案共用，以及總計數百 PB 的儲存容量。



設定橫向擴展效能的 DFS 命名空間

1. 如果您尚未讓 DFS 命名空間伺服器執行，您可以使用 setup-DFSN-servers.template CloudFormation 範本啟動一對高可用性的 DFS 命名空間伺服器。如需建立 CloudFormation 堆疊的詳細資訊，請參閱AWS CloudFormation 《 使用者指南》中的在 AWS CloudFormation 主控台上建立堆疊。
2. 以AWS 委派管理員群組中的使用者身分，連線至上一個步驟中啟動的其中一個 DFS 命名空間伺服器。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的連線至 Windows 執行個體。
3. 存取 DFS 管理主控台。開啟開始功能表並執行 dfsmgmt.msc。這會開啟 DFS Management GUI 工具。
4. 選擇動作，然後選擇新命名空間，輸入您為伺服器啟動的第一個 DFS 命名空間伺服器的電腦名稱，然後選擇下一步。
5. 針對名稱，輸入您要建立的命名空間 （ 例如 corp)。
6. 選擇編輯設定，並根據您的需求設定適當的許可。選擇 Next (下一步)。
7. 保留選取預設的網域型命名空間選項，保留選取啟用 Windows Server 2008 模式選項，然後選擇下一步。

   > **Note**
   >
   > Windows Server 2008 模式是命名空間的最新可用選項。

8. 檢閱命名空間設定，然後選擇建立。
9. 在導覽列的命名空間下選取新建立的命名空間時，選擇動作，然後選擇新增命名空間伺服器。

10. 輸入您為命名空間伺服器啟動的第二個 DFS 命名空間伺服器的電腦名稱。
11. 選擇編輯設定，根據您的需求設定適當的許可，然後選擇確定。
12. 開啟您剛建立之命名空間的內容（按一下滑鼠右鍵）選單，選擇新資料夾，輸入第一個碎片的資料夾名稱（例如A-F，名稱），然後選擇新增。
13. 輸入託管此碎片之檔案共用的 DNS 名稱，格式為 UNC 格式（例如 \\fs-0123456789abcdef0.example.com\A-F），讓路徑指向資料夾目標，然後選擇確定。
14. 如果共用不存在：
    a. 選擇是來建立它。
    b. 從建立共用對話方塊中，選擇瀏覽。
    c. 選擇現有資料夾，或在 D$ 下建立新資料夾，然後選擇確定。
    d. 設定適當的共用許可，然後選擇確定。
15. 現在新增了碎片的資料夾目標，請選擇確定。
16. 針對您要新增至相同命名空間的其他碎片，重複最後四個步驟。

管理輸送量容量

您可以增加和減少檔案系統的輸送量容量，以協助隨時管理其效能。輸送量容量是其中一個維度，可決定託管 FSx for Windows File Server 檔案系統的檔案伺服器可以提供資料的速度。更高的輸送量容量也會在檔案伺服器上提供更高的每秒 I/O 操作 (IOPS) 層級和大量的快取記憶體。如需詳細資訊，請參閱FSx for Windows File Server 效能。

主題

輸送量擴展的運作方式

當您修改檔案系統的輸送量容量時，Amazon FSx 會將檔案系統的檔案伺服器切換為在幕後具有更多或更少輸送量的檔案伺服器。對於多可用區檔案系統，切換到新的檔案伺服器會在 Amazon FSx 將偏好的檔案伺服器和次要檔案伺服器切換時觸發自動容錯移轉和容錯回復。在傳輸量容量擴展期間切換檔案

伺服器時，單一可用區檔案系統將無法使用幾分鐘。新的輸送量容量一旦可供檔案系統使用，就會向您收取費用。

> **Note**
>
> 在後端的維護操作期間，系統修改（包括輸送量容量修改）可能會延遲。維護操作可能會導致系統修改排入佇列，進而進行處理。

對於多可用區檔案系統，輸送量容量擴展會導致自動容錯移轉和容錯回復，而 Amazon FSx 則會關閉偏好的和次要檔案伺服器。在傳輸量容量擴展以及檔案系統維護和意外服務中斷期間，檔案系統的任何持續流量將由剩餘的檔案伺服器提供。當取代的檔案伺服器恢復上線時，FSx for Windows 會執行重新同步任務，以確保資料同步回新取代的檔案伺服器。

FSx for Windows 旨在將此重新同步活動對應用程式和使用者的影響降至最低。不過，重新同步程序涉及同步大型區塊中的資料。這表示即使僅更新一小部分，大量資料區塊仍可能需要同步處理。因此，重新同步的數量不僅取決於資料流失的數量，還取決於檔案系統上資料流失的性質。如果您的工作負載具有大量寫入和 IOPS，則資料同步程序可能需要更長的時間，並需要額外的效能資源。

在此期間，您的檔案系統將繼續可用，但為了減少資料同步的持續時間，我們建議您在檔案系統負載最少時，修改閒置期間的輸送量容量。我們也建議您確保檔案系統有足夠的輸送量容量，除了工作負載之外，也能執行同步任務，以減少資料同步的持續時間。最後，我們建議您在檔案系統負載較輕時測試容錯移轉的影響。

知道何時修改輸送量容量

Amazon FSx 與 Amazon CloudWatch 整合，可讓您監控檔案系統的持續輸送量用量層級。您可以透過檔案系統驅動的效能（輸送量和 IOPS) 取決於特定工作負載的特性，以及檔案系統的輸送量容量、儲存容量和儲存類型。您可以使用 CloudWatch 指標來決定要變更哪些維度來改善效能。如需詳細資訊，請參閱使用 Amazon CloudWatch 監控。

FSx for Windows File Server 會根據 Amazon FSx 主控台的檔案系統詳細資訊頁面中的監控與效能儀表板中檔案系統的 CloudWatch 指標值，提供效能提醒。這包括輸送量容量，以及可從輸送量容量增加中受益的其他檔案系統指標。如需詳細資訊，請參閱效能警告和建議。

為您的檔案系統設定足夠的輸送量容量，不僅符合工作負載的預期流量，還滿足支援您在檔案系統上啟用的功能所需的額外效能資源。例如，如果您正在執行重複資料刪除，則您選取的輸送量容量必須提供足夠的記憶體，以根據您所擁有的儲存來執行重複資料刪除。如果您使用的是影子複本，請將輸送量容量增加到至少為工作負載預期驅動值的三倍，以避免 Windows Server 刪除影子複本。如需詳細資訊，請參閱輸送量容量對效能的影響。

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 來增加或減少檔案系統的輸送量容量，如下列程序所述。

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/：//www.。
2. 導覽至檔案系統，然後選擇您要增加輸送量容量的 Windows 檔案系統。
3. 針對動作，選擇更新輸送量。

   或者，在摘要面板中，選擇檔案系統輸送量容量旁的更新。

   更新輸送量容量視窗隨即出現。
4. 從清單中選擇輸送量容量的新值。
5. 選擇更新以啟動輸送量容量更新。

   > **Note**
   >
   > 更新輸送量擴展時，多可用區域檔案系統會容錯移轉並故障恢復，並且完全可用。單一可用區檔案系統在更新期間發生非常短暫的無法使用。
6. 您可以在檔案系統詳細資訊頁面的更新索引標籤中監控更新進度。

   您可以使用 Amazon FSx 主控台、 AWS CLI和 API 來監控更新進度。如需詳細資訊，請參閱監控輸送量容量更新。

修改檔案系統的輸送量容量 (CLI)

若要增加或減少檔案系統的輸送量容量，請使用 AWS CLI 命令 update-file-system。設定下列參數：

- `--file-system-id` 至您要更新之檔案系統的 ID。
- `ThroughputCapacity` 至所需值；有效值為 8、16、32、64、128、256、512、1024、2048、4608、6144、9216、12288 MBps。

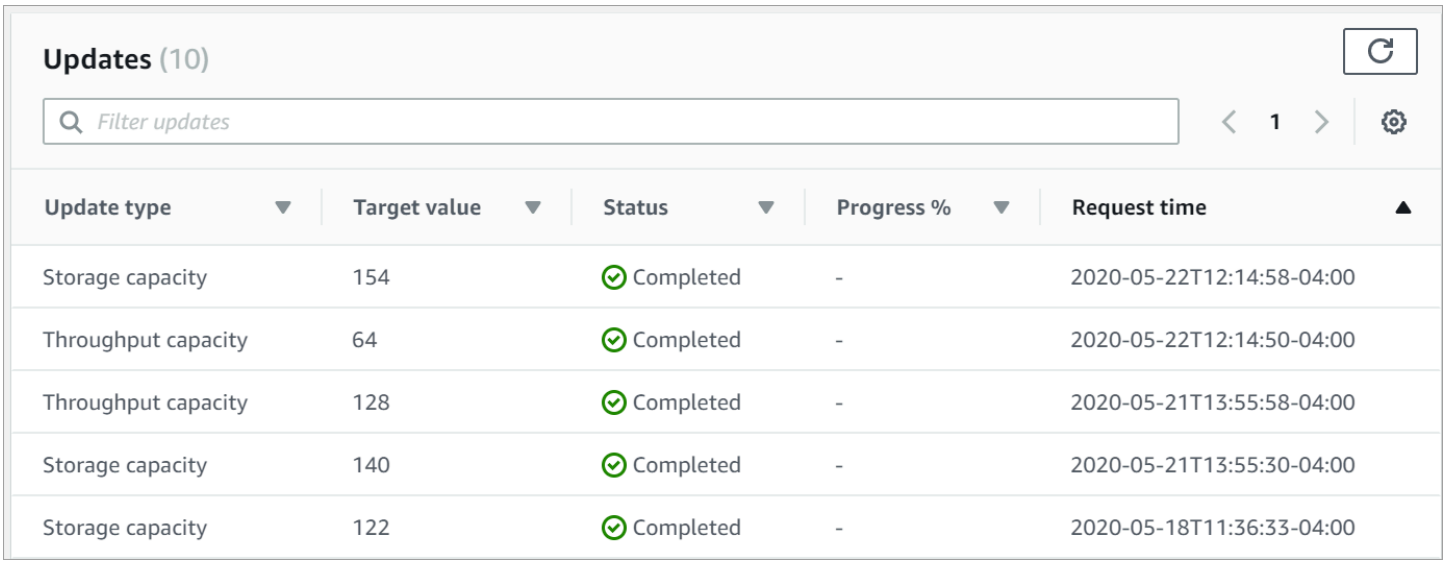
您可以使用 Amazon FSx 主控台、 AWS CLI和 API 來監控更新進度。如需詳細資訊，請參閱監控輸送量容量更新。

監控輸送量容量更新

您可以使用 Amazon FSx 主控台、API 和 監控輸送量容量修改的進度 AWS CLI。

在主控台中監控輸送量容量變更

在檔案系統詳細資訊視窗中的更新索引標籤中，您可以檢視每個更新動作類型的 10 個最近更新動作。



對於輸送量容量更新動作，您可以檢視下列資訊。

更新類型

可能的值是輸送量容量。

目標值

變更檔案系統輸送量容量所需的值。

狀態

更新的目前狀態。對於輸送量容量更新，可能的值如下：

- 待定 – Amazon FSx 已收到更新請求，但尚未開始處理。
- 進行中 – Amazon FSx 正在處理更新請求。
- 更新最佳化 – Amazon FSx 已更新檔案系統的網路 I/O、CPU 和記憶體資源。新的磁碟 I/O 效能等級可用於寫入操作。您的讀取操作將看到上一個層級與新層級之間的磁碟 I/O 效能，直到您的檔案系統不再處於此狀態為止。
- 已完成 – 輸送量容量更新已成功完成。

- 失敗 – 輸送量容量更新失敗。選擇問號 (?) 以查看輸送量更新失敗原因的詳細資訊。

請求時間

Amazon FSx 收到更新請求的時間。

使用 AWS CLI 和 API 監控變更

您可以使用 describe-file-systems CLI 命令和 DescribeFileSystems API 動作來檢視和監控檔案系統輸送量修改請求。AdministrativeActions 陣列會列出每個管理動作類型的 10 個最近更新動作。當您修改檔案系統的輸送量容量時，會產生FILE_SYSTEM_UPDATE管理動作。

下列範例顯示 CLI describe-file-systems 命令的回應摘錄。檔案系統的輸送量容量為 8 MBps，目標輸送量容量為 256 MBps。

```
.
.
.
    "ThroughputCapacity": 8,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "WindowsConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

當 Amazon FSx 成功完成處理動作時，狀態會變更為 COMPLETED。然後，新的輸送量容量可供檔案系統使用，並在 ThroughputCapacity 屬性中顯示 。這會顯示在 CLI describe-file-systems 命令的下列回應摘錄中。

```
.
.
.
    "ThroughputCapacity": 256,
"AdministrativeActions": [
```

```
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "COMPLETED",
        "TargetFileSystemValues": {
          "WindowsConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

如果輸送量容量修改失敗，狀態會變更為 FAILED，而 FailureDetails 屬性會提供失敗的相關資訊。如需故障診斷失敗動作的相關資訊，請參閱 儲存或輸送量容量更新失敗。

管理網路類型

建立 FSx for Windows 檔案系統時，您必須指定網路類型，其必須是下列其中一個選項：

- IPv4 允許您的檔案系統僅使用網際網路通訊協定第 4 版 (IPv4) 進行通訊。
- Dual-stack 可讓您的檔案系統同時使用網際網路通訊協定第 6 版 (IPv6) 和 IPv4 進行通訊。

您可以隨時使用 Amazon FSx 管理主控台、 AWS CLI AWS API 或其中一個 AWS SDKs 變更現有 FSx for Windows 檔案系統的網路類型。例如，如果您的子網路同時支援 IPv4 和 IPv6 定址，您可以將現有的檔案系統從IPv4-only 更新為雙堆疊模式，您也可以將雙堆疊檔案系統更新為IPv4-only。

使用雙堆疊模式

如果您需要從 IPv6 用戶端原生存取和管理 Amazon FSx 檔案系統，您應該使用雙堆疊模式。透過將 Amazon FSx 檔案系統設定為使用雙堆疊定址，您可以從 IPv6 用戶端以及 IPv4 用戶端、相同 Amazon VPC、另一個 AWS 帳戶 VPC 或內部部署網路存取檔案資料。例如，在將 Amazon FSx 檔案系統設定為使用雙堆疊的情況下，您可以讓現有的 IPv4 用戶端和新的 IPv6 用戶端存取存放在檔案系統中的檔案資料。

根據預設，Amazon FSx 和 Amazon VPC 會使用 IPv4 定址通訊協定。因此，作為使用 IPv6 的先決條件，您必須先將 Amazon 提供的 IPv6 無類別網域間範圍 (CIDR) 區塊指派給 VPC 和子網路，才能搭配 Amazon FSx 檔案系統使用 IPv6。如需為 VPC 啟用 IPv6 的資訊，請參閱《Amazon Virtual Private Cloud 使用者指南》中的為您的 VPC 新增 IPv6 支援。

變更網路類型

您可以使用 Amazon FSx 主控台、 AWS Command Line Interface (AWS CLI) 或 Amazon FSx API 修改檔案系統的網路類型。

變更檔案系統的網路類型 （主控台）

1. 在 https://console.aws.amazon.com/fsx/：// 開啟 Amazon FSx 主控台。
2. 導覽至檔案系統，然後選擇您要變更其網路類型的 FSx for Windows 檔案系統。
3. 針對動作，選擇更新網路類型。或者，在網路與安全面板中，選擇檔案系統網路類型旁的管理。

   更新網路類型視窗隨即出現。
4. 針對所需的網路類型，選擇 IPv4 或雙堆疊。
   - 如果您選擇 `IPv4`，則不需要進一步的組態。
   - 如果您選擇 `Dual-stack`，請指定檔案系統端點將使用的 IPv6 地址範圍：
     - 來自 VPC 的未配置 IPv6 地址範圍 – Amazon FSx 會從其中一個 VPC 的 IPv6 CIDR 範圍中選擇可用的 /118 IP 地址範圍，以用作檔案系統的端點 IPv6 地址範圍。
5. 選擇更新。

修改檔案系統的網路類型 (CLI)

- 若要修改檔案系統的網路類型，請使用 update-file-system CLI 命令 （或同等的 UpdateFileSystem API 操作），如下列範例所示。

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --network-type DUAL
```

標記 Amazon FSx 資源

為了協助您管理檔案系統和其他 FSx for Windows File Server 資源，您可以標籤形式將自己的中繼資料指派給每個資源。標籤可讓您以不同的方式分類 AWS 資源，例如，依用途、擁有者或環境。當您有許多相同類型的資源時，這將會很有用，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。每個標籤皆包含由您定義的一個金鑰與一個選用值。

標籤可讓您以不同的方式分類 AWS 資源，例如，依用途、擁有者或環境。例如，您可以為帳戶的 FSx for Windows File Server 檔案系統定義一組標籤，協助您追蹤每個執行個體的擁有者和堆疊層級。

我們建議您為每種資源類型建立符合您需求的標籤金鑰。使用一致的標籤金鑰組可讓您更輕鬆管理您的資源。您可以根據您新增的標籤搜尋和篩選資源。如需如何實作有效資源標記策略的詳細資訊，請參閱 AWS 白皮書標記最佳實務。

標籤對 Amazon FSx 沒有任何語意意義，並嚴格解譯為字元字串。此外，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 FSx for Windows File Server API、CLI AWS 或 AWS SDK，您可以使用 `TagResource` API 動作將標籤套用至現有資源。此外，有些資源建立動作可讓您在建立資源時指定資源的標籤。若標籤無法在資源建立時套用，我們會轉返資源建立程序。這可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。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。如需有關讓使用者在建立時為資源加上標籤的詳細資訊，請參閱 在建立期間授予標籤資源的許可。

標記您的 資源

您可以標記 帳戶中存在的 FSx for Windows File Server 資源。如果您使用的是 Amazon FSx 主控台，您可以使用相關資源畫面上的標籤索引標籤，將標籤套用至資源。建立資源時，您可以套用名稱索引鍵與值，並在建立新的檔案系統時套用您選擇的標籤。主控台可能會根據名稱標籤組織資源，但此標籤對 FSx for Windows File Server 服務沒有任何語意意義。

您可以將 IAM 政策中的標籤型資源層級許可套用至支援建立時標記的 FSx for Windows File Server API 動作，以對建立時可標記資源的使用者和群組實作精細控制。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，因此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。

您也可以將資源層級許可套用至 IAM 政策中的 `TagResource`和 `UntagResource` FSx for Windows File Server API 動作，以控制在現有資源上設定的標籤索引鍵和值。

如需為您的資源建立標籤以便計費的詳細資訊，請參閱 AWS Billing 使用者指南中的 Using cost allocation tags (使用成本分配標籤)。

標籤限制

以下基本限制適用於標籤：

- 每一資源最多標籤數 – 50
- 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。
- 索引鍵長度上限 - 128 個 UTF-8 Unicode 字元
- 值的長度上限 - 256 個 UTF-8 Unicode 字元
- FSx for Windows File Server 標籤允許的字元為：以 UTF-8 表示的字母、數字和空格，以及下列字元：+ - = . _ : / @。
- 標籤金鑰與值皆區分大小寫。
- 字`aws:`首會保留供 AWS 使用。如果標籤具有此字首的標籤金鑰，則您無法編輯或刪除標籤的金鑰或值。具 `aws:` 字首的標籤，不算在受資源限制的標籤計數內。

您無法僅根據資源的標籤刪除資源；您必須指定資源識別符。例如，若要刪除您以名為 的標籤金鑰標記的檔案系統`DeleteMe`，您必須使用 `DeleteFileSystem`動作搭配檔案系統資源識別符，例如 fs-1234567890abcdef0。

當您標記公有或共用資源時，您指派的標籤僅供您的 使用 AWS 帳戶，其他 AWS 帳戶 無法存取這些標籤。對於共用資源的標籤型存取控制，每個 AWS 帳戶 都必須指派自己的一組標籤來控制對資源的存取。

標記資源所需的許可

如需在建立時標記 Amazon FSx 資源所需許可的詳細資訊，請參閱 在建立期間授予標籤資源的許可。如需使用標籤來限制存取 IAM 政策中的 Amazon FSx 資源的詳細資訊，請參閱 使用標籤來控制對 Amazon FSx 資源的存取。

使用 更新檔案系統 AWS CLI

您可以使用本演練中的程序來更新三個元素。您可以更新檔案系統的所有其他元素，您可以從 主控台執行此操作。這些程序假設您已在本機電腦上 AWS CLI 安裝並設定 。如需詳細資訊，請參閱AWS Command Line Interface 《 使用者指南》中的安裝和設定。

- AutomaticBackupRetentionDays – 您希望保留檔案系統自動備份的天數。
- DailyAutomaticBackupStartTime – 您希望每日自動備份時段開始的一天中國際標準時間 (UTC) 的時間。從此指定時間開始，視窗為 30 分鐘。此時段無法與每週維護備份時段重疊。
- WeeklyMaintenanceStartTime – 您希望維護時段開始的一週時間。第 1 天是星期一，第 2 天是星期二，以此類推。從此指定時間開始，視窗為 30 分鐘。此時段無法與每日自動備份時段重疊。

下列程序概述如何使用 更新檔案系統 AWS CLI。

更新您的檔案系統自動備份保留多久

1. 在電腦上開啟命令提示字元或終端機。
2. 執行下列命令，以檔案系統的 ID 取代檔案系統 ID，以及您要保留自動備份的天數。

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration AutomaticBackupRetentionDays=30
```

更新檔案系統的每日備份時段

1. 在電腦上開啟命令提示字元或終端機。
2. 執行下列命令，以檔案系統的 ID 取代檔案系統 ID，並以您想要開始視窗的時間取代時間。

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration DailyAutomaticBackupStartTime=01:00
```

更新檔案系統的每週維護時段

1. 在電腦上開啟命令提示字元或終端機。
2. 執行下列命令，將檔案系統 ID 取代為檔案系統的 ID，並將日期和時間取代為您要開始視窗的時間。

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration WeeklyMaintenanceStartTime=1:01:30
```

使用備份、陰影複製和排程複寫來保護您的資料

除了自動複寫檔案系統的資料以確保高耐用性之外，Amazon FSx 還提供下列選項，以進一步保護存放在檔案系統上的資料：

- 原生 Amazon FSx 備份支援 Amazon FSx 內的備份保留和合規需求。
- AWS Backup Amazon FSx 檔案系統的備份是雲端和內部部署中跨 AWS 服務集中且自動化備份解決方案的一部分。
- Windows 影子複本可讓您的使用者輕鬆復原檔案變更，並透過將檔案還原至先前的版本來比較檔案版本。
- AWS DataSync 排程將您的 Amazon FSx 檔案系統複寫到第二個檔案系統可提供資料保護和復原。

主題

使用備份保護您的資料

您可以透過定期備份檔案系統來保護 FSx for Windows File Server 檔案系統上的資料。Amazon FSx 為您提供多種備份檔案系統的選項。您可以使用自動每日備份來每天備份。您可以隨時對檔案系統進行使用者起始的備份。您也可以使用 AWS Backup 做為 AWS 資源集中備份解決方案的一部分。這些備份解決方案可協助您滿足資料保留、業務和合規需求。

我們建議您使用 檔案系統預設啟用的自動每日備份，以及使用 跨 AWS Backup 的集中式備份解決方案 AWS 服務。 AWS Backup 可讓您設定具有不同頻率 （ 例如，每天、每天或每週多次） 和保留期的其他備份計劃。

使用 Amazon FSx，備份具有file-system-consistent、高耐用性和增量性。每個備份都包含建立新檔案系統所需的所有資訊，有效還原檔案系統的point-in-time快照。為了確保檔案系統一致性，Amazon FSx 會在 Microsoft Windows 中使用磁碟區陰影複製服務 (VSS)。為了確保高耐用性，Amazon FSx 會將備份存放在 Amazon Simple Storage Service (Amazon S3) 中。

Amazon FSx 備份是增量備份，無論是使用自動每日備份還是使用者起始的備份功能產生。這表示只會儲存您最近一次備份後變更的檔案系統上的資料。這可最大限度地減少建立備份所需的時間，並透過不複製資料來節省儲存成本。

在備份程序的某些時間點，儲存 I/O 可能會短暫暫停，通常是幾秒鐘。由於 VSS 服務需要在恢復 I/O 之前排清對磁碟的任何快取寫入，因此如果您的工作負載具有每秒大量寫入操作 ()，暫停的持續時間可能會更長DataWriteOperations。大多數最終使用者和應用程式會將此 I/O 暫停視為短暫的 I/O 暫停。根據您的設定方式，您的應用程式可能對逾時設定有不同的敏感度。

為您的檔案系統建立定期備份是最佳實務，可補充 Amazon FSx for Windows File Server 為您的檔案系統執行的複寫。Amazon FSx 備份有助於支援備份保留和合規需求。使用 Amazon FSx 備份非常簡單，無論是建立備份、複製備份、從備份還原檔案系統，還是刪除備份。請注意，若要檢視單一檔案系統備份的用量，您需要啟用該特定備份的標籤，並啟用標籤型帳單報告。

主題

使用自動每日備份

根據預設，Amazon FSx 會對您的檔案系統進行自動每日備份。這些自動每日備份會在您建立檔案系統時建立的每日備份時段期間進行。當您選擇每日備份時段時，我們建議您為使用 檔案系統的應用程式選擇正常操作時間以外的方便時間。我們也建議您在維護時段之外選擇備份時段，因為如果有進行中的檔案系統維護，則可能不會進行自動備份。

自動每日備份會保留一段時間，稱為保留期。當您在 Amazon FSx 主控台中建立檔案系統時，預設的每日自動備份保留期為 30 天。Amazon FSx API 和 CLI 的預設保留期間不同。您可以將保留期間設定為 0-90 天。將保留期間設定為 0 （零） 天會關閉自動每日備份。刪除檔案系統時，會自動刪除每日備份。

> **Note**
>
> 將保留期間設定為 0 天表示您的檔案系統永遠不會自動備份。強烈建議您針對具有任何層級重要功能的檔案系統，使用自動每日備份。

您可以使用 AWS CLI 或其中一個 AWS SDKs 來變更檔案系統的備份時段和備份保留期。使用 `UpdateFileSystem` API 操作或 `update-file-system` CLI 命令。如需詳細資訊，請參閱使用 更新檔案系統 AWS CLI。

> **Important**
>
> 縮短自動每日備份的保留期間會導致在新的保留時段之外永久刪除備份。在繼續之前，請確定您不再需要這些較舊的備份。

使用使用者啟動的備份

使用 Amazon FSx，您可以隨時手動備份檔案系統。您可以使用 Amazon FSx 主控台、API 或 AWS Command Line Interface () 來執行此操作AWS CLI。您使用者啟動的 Amazon FSx 檔案系統備份永遠不會過期，而且只要您想要保留它們，這些備份就可以使用。即使您刪除已備份的檔案系統，也會保留使用者啟動的備份。您只能使用 Amazon FSx 主控台、API 或 CLI 刪除使用者啟動的備份。Amazon FSx 永遠不會自動刪除它們。如需詳細資訊，請參閱刪除備份。

如果在修改檔案系統時啟動備份 （ 例如在更新輸送量容量期間或在檔案系統維護期間），備份請求會排入佇列，並在活動完成時繼續。

若要了解如何取得檔案系統的使用者起始備份，請參閱 建立使用者啟動的備份。

AWS Backup 搭配 Amazon FSx 使用

AWS Backup 透過備份 Amazon FSx 檔案系統，以簡單且經濟實惠的方式保護您的資料。 AWS Backup 是一種統一的備份服務，旨在簡化建立、 複製、 還原、 和刪除備份、 同時提供改善的報告和稽核。 AWS Backup 可讓您更輕鬆地為法務、 法規、 和專業合規。 AWS Backup 也讓 保護您的 AWS 儲存磁碟區、 資料庫、 和 檔案系統更簡單，提供您可以執行下列動作的中心位置：

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

- 跨 AWS 區域和跨 AWS 帳戶複製備份。
- 監控所有最近的備份、複製和還原活動。

AWS Backup 使用 Amazon FSx 的內建備份功能。從 AWS Backup 主控台取得的備份具有與透過 Amazon FSx 主控台取得的備份相同的檔案系統一致性和效能層級，以及相同的還原選項。從 取得的備份 AWS Backup 是相對於您採取的任何其他 Amazon FSx 備份遞增的，無論是使用者啟動或自動。

如果您使用 AWS Backup 來管理這些備份，您可以獲得其他功能，例如無限的保留選項，以及每小時建立排程備份的能力。此外，即使刪除來源檔案系統， 仍會 AWS Backup 保留您的不可變備份。這可防止意外或惡意刪除的情形發生。

執行的備份 AWS Backup 會被視為使用者啟動的備份，並計入 Amazon FSx 的使用者啟動備份配額。您可以在 Amazon FSx 主控台、CLI 和 API AWS Backup 中查看和還原 採取的備份。不過，您無法刪除 於 Amazon FSx 主控台、CLI 或 API AWS Backup 中取得的備份。如需如何使用 AWS Backup 備份 Amazon FSx 檔案系統的詳細資訊，請參閱《 AWS Backup 開發人員指南》中的使用 Amazon FSx 檔案系統。

複製備份

您可以使用 Amazon FSx 將相同 AWS 帳戶中的備份手動複製到另一個 AWS 區域 （跨區域複本）或相同 AWS 區域 （區域內複本）。您只能在相同的 AWS 分割區內進行跨區域複製。您可以使用 Amazon FSx 主控台 AWS CLI或 API 建立使用者啟動的備份複本。當您建立使用者起始的備份複本時，其類型為 `USER_INITIATED`。

您也可以使用 AWS Backup 跨 AWS 區域和跨 AWS 帳戶複製備份。 AWS Backup 是一種全受管備份管理服務，可提供政策型備份計劃的中央介面。透過其跨帳戶管理，您可以自動使用備份政策，將備份計劃套用至組織內的帳戶。

跨區域備份複本對於跨區域災難復原特別重要。您可以取得備份並將其複製到另一個 AWS 區域，以便在主要 AWS 區域中發生災難時，您可以從備份還原，並快速復原其他區域中的可用性 AWS 。您也可以使用備份複本，將檔案資料集複製到另一個 AWS 區域或相同 AWS 區域內。您可以使用 Amazon FSx 主控台或 Amazon FSx API AWS CLI，在相同 AWS 帳戶 （跨區域或區域） 內建立備份複本。您也可以使用 AWS Backup執行隨需或政策型備份複本。

跨帳戶備份複本對於滿足法規合規要求，將備份複製到隔離帳戶非常有用。它們也提供額外的資料保護層，以協助防止意外或惡意刪除備份、遺失登入資料或洩露 AWS KMS 金鑰。跨帳戶備份支援廣發（將備份從多個主要帳戶複製到一個隔離備份複本帳戶） 和廣發 （將備份從一個主要帳戶複製到多個隔離備份複本帳戶）。

您可以使用 AWS Backup 搭配 AWS Organizations 支援，建立跨帳戶備份複本。跨帳戶複本的帳戶界限由 AWS Organizations 政策定義。如需使用 AWS Backup 建立跨帳戶備份複本的詳細資訊，請參閱《 AWS Backup 開發人員指南》中的跨 建立備份複本 AWS 帳戶。

備份複製限制

以下是您複製備份時的一些限制：

- 僅在任兩個商業 AWS 區域之間、中國 （北京） 和中國 （寧夏） 區域之間，以及 AWS GovCloud （美國東部） 和 AWS GovCloud （美國西部） 區域之間支援跨區域備份複本，但不適用於這些區域集。
- 選擇加入區域不支援跨區域備份複本。
- 您可以在任何區域內建立區域內備份複本 AWS 。
- 來源備份的狀態必須為 ，AVAILABLE才能進行複製。
- 如果來源備份正在複製，則無法刪除該備份。當目的地備份可供使用，以及允許您刪除來源備份時，可能會有短暫的延遲。如果您重試刪除來源備份，您應該記住此延遲。
- 每個帳戶最多可以有五個備份複製請求正在進行到單一目的地 AWS 區域。

跨區域備份複本的許可

您可以使用 IAM 政策陳述式來授予執行備份複製操作的許可。若要與來源 AWS 區域通訊以請求跨區域備份複本，申請者 (IAM 角色或 IAM 使用者） 必須能夠存取來源備份和來源 AWS 區域。

您可以使用 政策來授予備份複製操作之 CopyBackup動作的許可。您可以在政策的 Action 欄位中指定動作，並在政策的 Resource欄位中指定資源值，如下列範例所示。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "fsx:CopyBackup",
            "Resource": "arn:aws:fsx:*:111111111111:backup/*"
        }
    ]
}
```

如需 IAM 政策的詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的政策和許可。

完整複本和增量複本

當您將備份從來源備份複製到不同的目的地 AWS 區域或目的地 AWS 帳戶時，第一個複本是完整備份複本，即使您使用相同的 KMS 金鑰來加密備份的來源和目的地複本。

在第一次備份複本之後，所有後續備份都會遞增至相同 AWS 帳戶中的相同目的地區域，前提是您尚未刪除該區域中先前複製的所有備份，且已使用相同的 AWS KMS 金鑰。如果不符合任一條件，則複製操作會產生完整（非增量）備份複本。

若要了解如何複製檔案系統的備份，請參閱 複製相同帳戶中的備份。

將備份還原至新的檔案系統

您可以使用可用的備份來建立新的檔案系統，有效地還原另一個檔案系統的point-in-time快照。您可以使用 主控台 AWS CLI或其中一個 AWS SDKs來還原備份。將備份還原至新檔案系統所需的時間，會與建立新檔案系統所需的時間相同。從備份還原的資料會延遲載入檔案系統，在此期間您將遇到稍高的延遲。

為了確保使用者可以繼續存取還原的檔案系統，請確定與還原檔案系統關聯的 Active Directory 網域與原始檔案系統相同，或受原始檔案系統的 Active Directory 網域信任。如需 Active Directory 的詳細資訊，請參閱 使用 Microsoft Active Directory。

若要了解如何將備份還原至新的 FSx for Windows 檔案系統，請參閱 將備份還原至新的檔案系統。

> **Note**
>
> 您只能將檔案系統備份還原至與原始部署類型和儲存容量相同的新檔案系統。您可以在新檔案系統的儲存容量可用後增加儲存容量。如需詳細資訊，請參閱管理儲存容量。

將備份還原至新的檔案系統時，您可以變更下列任何檔案系統設定：

- 儲存體類型
- 輸送容量
- VPC
- 可用區域
- 子網路
- VPC security groups (VPC 安全群組)

- Active Directory 組態
- AWS KMS 加密金鑰
- 每日自動備份開始時間
- 每週維護時段

建立使用者啟動的備份

除了自動每日檔案系統備份之外，您可以隨時使用 Amazon FSx 主控台建立使用者啟動的檔案系統備份，如下列程序所述。

建立使用者啟動的檔案系統備份

1. 在 https://console.aws.amazon.com/fsx/：// 開啟 Amazon FSx 主控台。
2. 從主控台儀表板中，選擇您要備份的檔案系統名稱。
3. 在動作中，選擇建立備份。
4. 在開啟的建立備份對話方塊中，提供備份的名稱。備份名稱最多可包含 256 個 Unicode 字元，包括字母、空格、數字和特殊字元 。+ - = _ : /
5. 選擇 Create backup (建立備份)。

您現在已建立檔案系統備份。您可以在左側導覽中選擇備份，在 Amazon FSx 主控台中找到所有備份的資料表。您的新使用者起始備份具有 類型USER_INITIATED，其狀態為 ，CREATING直到變成為止AVAILABLE。如需詳細資訊，請參閱使用使用者啟動的備份。

刪除備份

您可以使用 Amazon FSx 主控台、CLI 或 API 刪除檔案系統的任何使用者啟動和自動每日備份，如下列程序所述。若要刪除 AWS Backup具有 Backup 類型的 所採取的AWS 備份，您必須使用 AWS Backup 主控台、CLI 或 API。刪除備份是永久且無法復原的動作。也會刪除已刪除備份中的任何資料。除非您確定未來不需要該備份，否則請勿刪除備份。

刪除備份原則 (主控台)

1. 在 https://console.aws.amazon.com/fsx/：// 開啟 Amazon FSx 主控台。
2. 從主控台儀表板中，從左側導覽中選擇備份。
3. 從備份資料表中選擇要刪除的備份，然後選擇刪除備份。
4. 在開啟的刪除備份對話方塊中，確認備份的 ID 可識別您要刪除的備份。

5. 確認已針對您要刪除的備份勾選核取方塊。
6. 選擇刪除備份。

您的備份和所有包含的資料現在都會永久且無法復原地刪除。

備份的大小

備份大小是使用檔案系統中使用過的儲存體來決定，而不是總佈建儲存容量。備份的大小取決於使用過的儲存容量，以及檔案系統上的資料流失量。視您的資料在檔案系統的儲存磁碟區中分佈的方式及其變更頻率而定，您的總備份用量可能大於或小於您使用的儲存容量。當您刪除備份時，只會移除該備份特有的資料。

為了提供file-system-consistent、耐用且增量的備份，Amazon FSx 會在區塊層級備份資料。檔案系統的儲存磁碟區上的資料可能會跨多個區塊儲存，具體取決於寫入或覆寫的模式。因此，備份用量的總大小可能不符合檔案系統上檔案和目錄的確切大小。您可以在 AWS Billing Dashboard 或 中找到整體備份用量和成本 AWS Cost Management Console。

使用標籤來整理 AWS 帳單，以反映您自己的成本結構。若要這樣做，請註冊 以取得包含標籤索引鍵值的 AWS 帳戶 帳單。接著，若要查看合併資源的成本，請根據具有相同標籤鍵值的資源來整理您的帳單資訊。例如，您可以使用特定應用程式名稱來標記數個資源，然後整理帳單資訊以查看該應用程式跨數項服務的總成本。如需詳細資訊，請參閱《AWS Billing 》使用者指南中的使用成本分配標籤。

> **Note**
>
> 當您增加儲存容量時，將資料從舊組儲存磁碟遷移到新、較大組儲存磁碟的程序可能會導致備份用量暫時增加，直到刪除與舊組儲存磁碟相關聯的備份為止。如果在增加儲存容量之前只部分使用檔案系統的儲存體，則需要遷移到新磁碟的資料大小可能大於原始儲存磁碟上存在的資料大小。這可能會導致備份用量增加到新的儲存容量層級。您應該考慮增加儲存容量對備份規劃的影響。

複製相同帳戶中的備份

您可以使用 AWS 管理主控台 和 AWS CLI ，使用下列程序，將相同 AWS 帳戶中的備份手動複製到另一個 AWS 區域 （跨區域副本） 或相同 AWS 區域 （區域副本）。

使用主控台在相同帳戶 （跨區域或區域） 內複製備份

1. 開啟位於 https：//https://console.aws.amazon.com/fsx/ 的 Amazon FSx 主控台。

2. 在導覽窗格中，選擇備份。
3. 在備份表格中，選擇您要複製的備份，然後選擇複製備份。
4. 在 Settings (設定) 區段中，執行下列動作：
   - 在目的地區域清單中，選擇要複製備份的目標 AWS 區域。目的地可以位於另一個 AWS 區域（跨區域複製）或相同 AWS 區域內（區域複製）。
   - （選用）選取複製標籤，將標籤從來源備份複製到目的地備份。如果您在步驟 6 選取複製標籤並新增標籤，則會合併所有標籤。
5. 針對加密，選擇 AWS KMS 加密金鑰以加密複製的備份。
6. 對於標籤 - 選用，輸入索引鍵和值來為複製的備份新增標籤。如果您在此處新增標籤，並在步驟 4 也選取複製標籤，則會合併所有標籤。
7. 選擇複製備份。

您的備份會在相同的 AWS 帳戶中複製到選取的 AWS 區域。

使用 CLI 在相同帳戶（跨區域或區域）內複製備份

- 使用 `copy-backup` CLI 命令或 CopyBackup API 操作來複製同一 AWS 帳戶內的備份，無論是跨 AWS 區域或在 AWS 區域內。

  下列命令`backup-0abc123456789cba7`會從 `us-east-1`區域複製 ID 為 的備份。

  ```
  aws fsx copy-backup \
    --source-backup-id backup-0abc123456789cba7 \
    --source-region us-east-1
  ```

  回應會顯示所複製備份的描述。

  您可以在 Amazon FSx 主控台上檢視備份，或使用 `describe-backups` CLI 命令或 DescribeBackups API 操作以程式設計方式檢視備份。

將備份還原至新的檔案系統

您可以使用 AWS 管理主控台、 CLI 和 API 還原檔案系統備份，以建立新的檔案系統，如下列程序所述。

從備份還原檔案系統

1. 開啟位於 https：//https://console.aws.amazon.com/fsx/ 的 Amazon FSx 主控台。
2. 從主控台儀表板中，從左側導覽中選擇備份。
3. 從備份資料表中選擇您要還原的備份，然後選擇還原備份。

   這樣做會開啟檔案系統建立精靈。此精靈與標準檔案系統建立精靈相同，但已設定部署類型和儲存容量，且無法變更。不過，您可以變更輸送量容量、相關聯的 VPC 和其他設定，以及儲存類型。儲存類型預設為 SSD，但您可以在下列條件下將其變更為 HDD：

   - 檔案系統部署類型為異地同步備份或單一異地同步備份 2。
   - 儲存容量至少為 2，000 GiB。
4. 完成精靈，就像您在建立新檔案系統時一樣。
5. 選擇 Review and create (檢閱和建立)。
6. 檢閱您為 Amazon FSx 檔案系統選擇的設定，然後選擇建立檔案系統。

   Amazon FSx 正在建立新的檔案系統，一旦其狀態變更為 `AVAILABLE`，您就可以正常使用檔案系統。

使用陰影複本保護您的資料

Microsoft Windows 影子複本是 Windows 檔案系統在某個時間點的快照。啟用陰影複製後，使用者可以快速復原存放在網路上的已刪除或變更的檔案，並比較檔案版本。儲存管理員可以輕鬆排程使用 Windows PowerShell 命令定期拍攝的陰影副本。

影子副本會與您的檔案系統資料一起存放，並僅針對變更的檔案部分使用檔案系統儲存容量。所有存放在檔案系統中的陰影副本都會包含在檔案系統備份中。

> **Note**
>
> 預設不會在 FSx for Windows File Server 上啟用陰影複本。若要使用陰影複製來保護檔案系統上的資料，您必須在檔案系統上啟用陰影複製並設定陰影複製排程。如需詳細資訊，請參閱設定陰影複本以使用預設儲存體和排程。

> **Warning**
>
> 陰影副本無法取代備份。如果您啟用陰影複製，請確定您繼續執行定期備份。

主題

使用陰影複本時的最佳實務

您可以為檔案系統啟用陰影副本，以允許最終使用者從 Windows File Explorer 中較早的快照檢視和還原個別檔案或資料夾。Amazon FSx 使用 Microsoft Windows Server 提供的陰影複製功能。將下列最佳實務用於陰影複製：

- 確保您的檔案系統具有足夠的效能資源：Microsoft Windows copy-on-write方法來記錄自上次影子複製點以來的變更，且此copy-on-write活動最多可針對每個檔案寫入操作產生三個 I/O 操作。
- 使用 SSD 儲存並提高輸送量容量：由於 Windows 需要高層級的 I/O 效能來維護陰影複製，因此我們建議您使用 SSD 儲存，並將輸送量容量提高到您預期工作負載的三倍。這有助於確保您的檔案系統有足夠的資源，以避免刪除不需要的影子副本等問題。
- 僅維護您需要的影子複本數量：如果您有大量影子複本，例如，超過 64 個最新的影子複本，或在單一檔案系統上佔用大量儲存空間 (TB 級） 的影子複本，容錯移轉和容錯回復等程序可能需要一

些額外的時間。這是因為 FSx for Windows 需要對陰影複製儲存體執行一致性檢查。由於 FSx for Windows 在維護影子複本時需要執行copy-on-write也可能會遇到較高的 I/O 操作延遲。若要將影子複本的可用性和效能影響降至最低，請手動刪除未使用的影子複本，或設定指令碼自動刪除檔案系統上的舊影子複本。

> **Note**
>
> 在異地同步備份檔案系統的容錯移轉事件期間，FSx for Windows 會執行一致性檢查，在新的作用中檔案伺服器上線之前，需要掃描檔案系統上的陰影複製儲存體。一致性檢查的持續時間與檔案系統上陰影複製的數量以及使用的儲存體有關。為了防止延遲容錯移轉和容錯回復事件，建議您在檔案系統上維持少於 64 個影子複本，並依照下列步驟定期監控和刪除最舊的影子複本。

設定陰影複本

您可以使用 Amazon FSx 定義的 Windows PowerShell 命令，在檔案系統上啟用和排程定期陰影複製。以下是在 FSx for Windows File Server 檔案系統上設定陰影副本時的三個主要設定：

- 設定陰影複製可在檔案系統上使用的最大儲存量
- （選用）設定可在檔案系統上存放的影子複本數量上限。預設值為 20。
- （選用）設定排程，定義擷取影子副本的時間和間隔，例如每日、每週和每月

您隨時可以為每個檔案系統儲存最多 500 個陰影複本；不過，我們建議隨時維持少於 64 個陰影複本，以確保可用性和效能。當您達到此限制時，您拍攝的下一個陰影複製會取代最舊的陰影複製。同樣地，達到陰影複製儲存量上限時，會刪除一或多個最舊的陰影複製，以為下一個陰影複製提供足夠的儲存空間。

如需有關如何使用預設 Amazon FSx 設定快速啟用和排程定期影子複本的資訊，請參閱 設定陰影複本以使用預設儲存體和排程。

配置陰影複製儲存體的考量事項

影子複製是自上次影子複製以來所進行檔案變更的區塊層級複製。不會複製整個檔案，只會複製變更。因此，舊版檔案通常不會佔用與目前檔案相同的儲存空間。用於變更的磁碟區空間可能根據您的工作負載而有所不同。修改檔案時，陰影副本使用的儲存空間取決於您的工作負載。當您決定要為影子複本配置多少儲存空間時，您應該考慮工作負載的檔案系統使用模式。

當您啟用影子複本時，您可以指定影子複本在檔案系統上可以使用的最大儲存量。預設限制為檔案系統的 10%。如果您的使用者經常新增或修改檔案，我們建議您提高限制。設定過小的限制可能會導致最舊的影子副本比使用者預期更頻繁地刪除。

您可以將陰影複製儲存體設定為未繫結 (`Set-FsxShadowStorage -Maxsize "UNBOUNDED"`)。不過，不受限制的組態可能會導致大量影子複本消耗您的檔案系統儲存體。這可能會導致您的工作負載沒有足夠的儲存容量。如果您設定無限制的儲存，請務必在達到陰影複製限制時擴展儲存容量。如需將影子複製儲存體設定為特定大小或無限制的詳細資訊，請參閱 設定陰影複製儲存體的最大數量。

啟用影子複本之後，您可以監控影子複本耗用的儲存空間量。如需詳細資訊，請參閱檢視陰影複製儲存。

設定陰影複製數量上限時的考量

當您啟用影子複本時，您可以指定存放在檔案系統上的影子複本數目上限。預設限制為 20，為了將陰影複製的可用性和效能影響降至最低，Microsoft 建議將陰影複製的數量上限設定為小於 64。由於 Windows 需要高層級的 I/O 效能來維護影子複本，因此我們建議您使用 SSD 儲存體，並將輸送量容量提高到您預期工作負載的三倍。這有助於確保您的檔案系統有足夠的資源，以避免刪除不需要的影子副本等問題。

您可以將陰影複製的數量上限設定為 500。不過，如果您有大量陰影複製或陰影複製在單一檔案系統上佔用大量儲存空間 (TB 級），容錯移轉和容錯回復等程序可能會比預期更久。這是因為 Windows 需要在陰影複製儲存體上執行一致性檢查。由於 Windows 需要執行copy-on-write活動，同時維護影子複本，因此您可能會遇到較高的 I/O 操作延遲。

陰影副本的檔案系統建議

以下是使用陰影複本的檔案系統建議。

- 請務必為檔案系統上的工作負載需求佈建足夠的效能容量。Amazon FSx 提供由 Microsoft Windows Server 提供的陰影複製功能。根據設計，Microsoft Windows copy-on-write方法來記錄自最新影子複製點以來的變更，此copy-on-write活動最多可針對每個檔案寫入操作產生三個 I/O 操作。如果 Windows 無法跟上每秒輸入 I/O 操作的速率，可能會導致所有影子複本遭到刪除，因為它無法再透過copy-on-write來維護影子複本。因此，請務必為檔案系統上的工作負載需求佈建足夠的 I/O 效能容量（包括決定檔案伺服器 I/O 效能的輸送量容量維度，以及決定儲存 I/O 效能的儲存類型和容量）。
- 我們通常建議您在啟用影子複本時，使用以 SSD 儲存體設定的檔案系統，而不是 HDD 儲存體，因為 Windows 會使用較高的 I/O 效能來維護影子複本，並且假設 HDD 儲存體為 I/O 操作提供較低的效能容量。

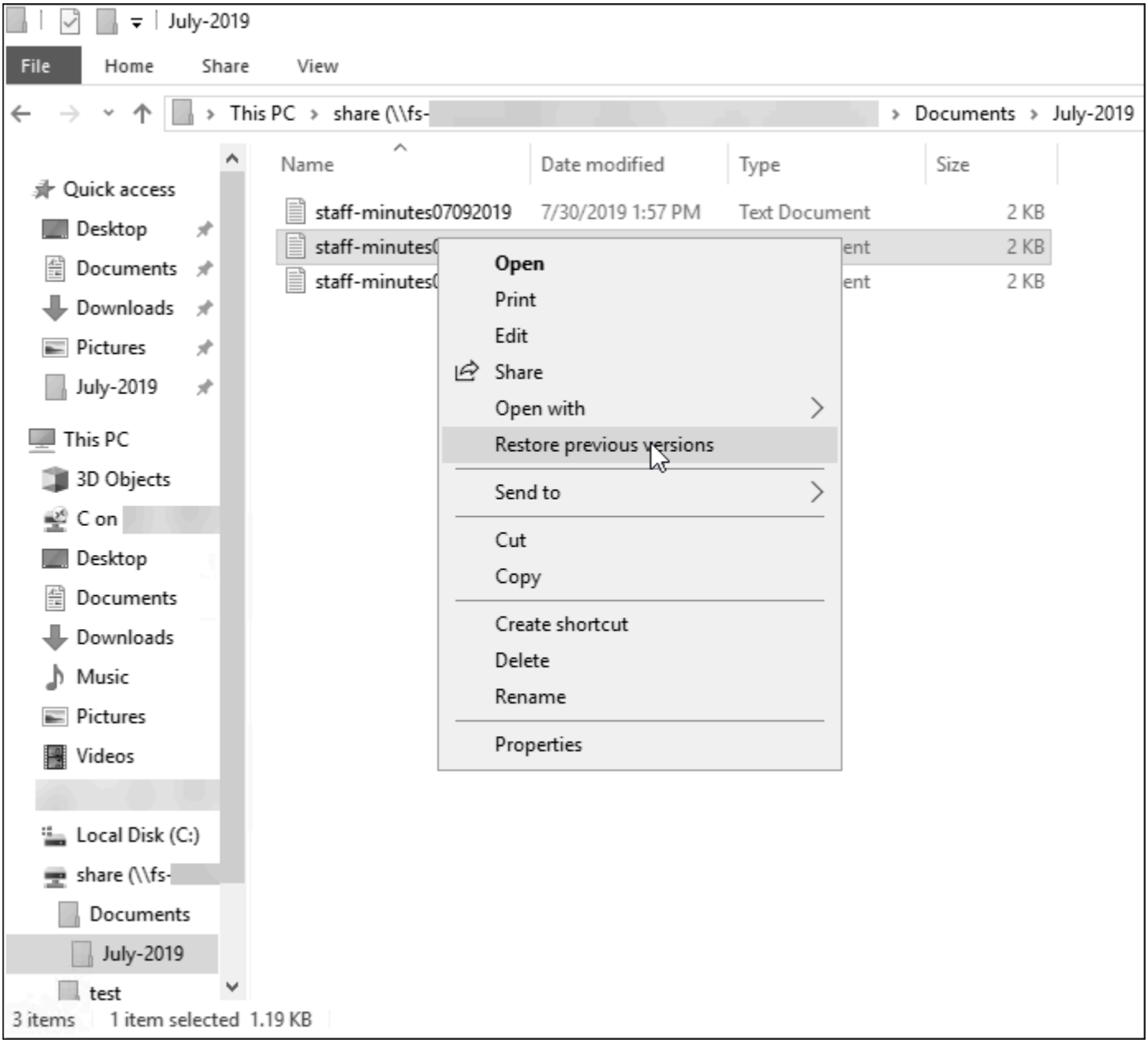
- 除了設定的陰影複製儲存量上限 () 之外，您的檔案系統應至少具有 320 MB 的可用空間MaxSpace。例如，如果您配置 5 GB MaxSpace給影子副本，您的檔案系統除了 5 GB 之外，應一律至少擁有 320 MB 的可用空間MaxSpace。

> **Warning**
>
> 設定陰影複製排程時，請確定您在遷移資料或排定執行重複資料刪除任務時，未排程陰影複製。當您預期檔案系統閒置時，您應該排程陰影副本。如需設定自訂陰影複製排程的資訊，請參閱 建立自訂陰影複製排程。

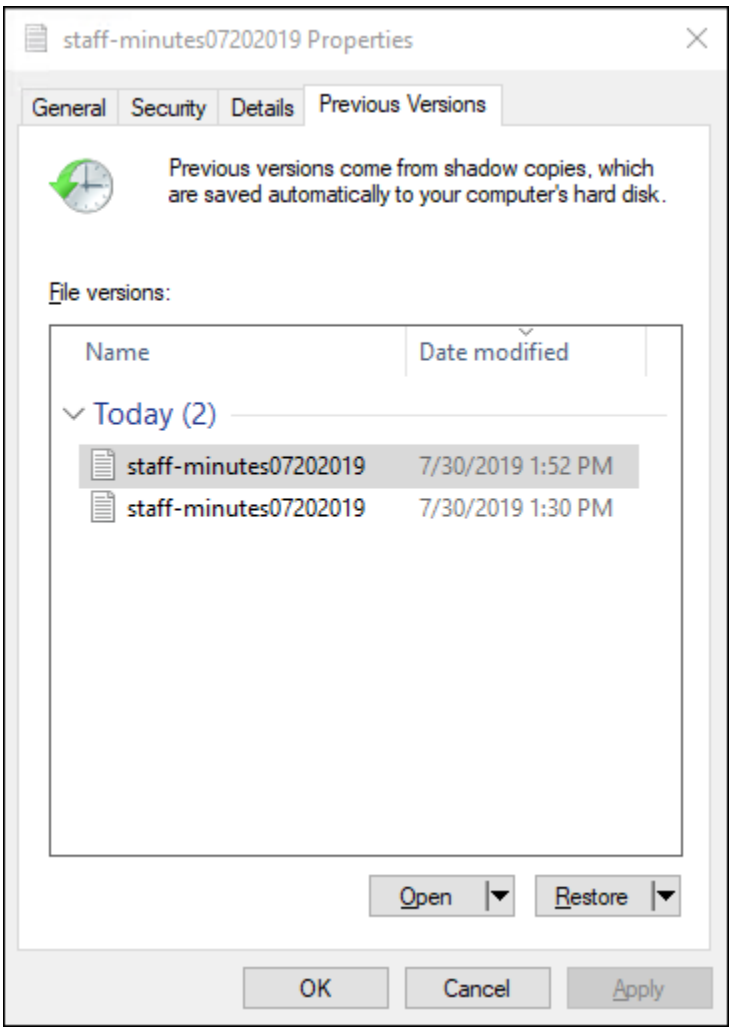
還原個別檔案和資料夾

在 Amazon FSx 檔案系統上設定陰影副本後，您的使用者可以快速還原個別檔案或資料夾的先前版本，並復原已刪除的檔案。

使用者使用熟悉的 Windows File Explorer 介面將檔案還原至舊版。若要還原檔案，您可以選擇要還原的檔案，然後從內容選單中選擇還原先前的版本 （按一下滑鼠右鍵）。



然後，使用者可以從先前版本清單中檢視和還原先前版本。



設定陰影複本以使用預設儲存體和排程

您可以使用預設的陰影複製儲存設定和排程，在檔案系統上快速設定陰影複製。預設陰影複製儲存設定可讓陰影複製最多使用檔案系統儲存容量的 10%。如果您增加檔案系統的儲存容量，目前配置的陰影複製儲存量不會同樣增加。

預設排程會在 UTC 的每週一、週二、週三、週四和週五上午 7：00 和下午 12：00 自動擷取影子複本。

設定陰影複製儲存的預設層級

1. 連線至與您的檔案系統具有網路連線能力的 Windows 運算執行個體。
2. 以檔案系統管理員群組的成員身分登入 Windows 運算執行個體。在 中 AWS Managed Microsoft AD，該群組是AWS 委派的 FSx 管理員。在自我管理的 Microsoft AD 中，該群組是網域管理員，

或您在建立檔案系統時為管理指定的自訂群組。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的連線至 Windows 執行個體。

3. 使用下列命令設定預設的陰影儲存量。*FSxFileSystem-Remote-PowerShell-Endpoint* 將取代為您要管理之檔案系統的 Windows Remote PowerShell 端點。您可以在 Amazon FSx 主控台、檔案系統詳細資訊畫面的網路與安全區段，或 DescribeFileSystem API 操作的回應中找到 Windows Remote PowerShell 端點。

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName FSxFileSystem-Remote-PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {Set-FsxShadowStorage -Default}
```

回傳的結果如下所示。

```
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- ------------------
             0         0 10737418240                 20
```

設定預設陰影複製排程

1. 連線至與您的檔案系統具有網路連線能力的 Windows 運算執行個體。
2. 以檔案系統管理員群組的成員身分登入 Windows 運算執行個體。在 中 AWS Managed Microsoft AD，該群組是AWS 委派的 FSx 管理員。在自我管理的 Microsoft AD 中，該群組是網域管理員或您在建立檔案系統時為管理指定的自訂群組。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的連線至 Windows 執行個體。
3. 使用下列命令設定預設陰影複製排程。

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName FSxFileSystem-Remote-PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {Set-FsxShadowCopySchedule -Default}
```

回應會顯示現在設定的預設排程。

```
FSx Shadow Copy Schedule

Start Time                Days of week                            WeeksInterval
----------                ------------                            -------------
```

```
2019-07-16T07:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday          1
2019-07-16T12:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday          1
```

若要了解其他選項並建立自訂陰影複製排程，請參閱 建立自訂陰影複製排程。

設定陰影複製儲存體的最大數量

您可以使用Set-FsxShadowStorage自訂 PowerShell 命令，定義陰影複製可在檔案系統上使用的最大儲存量。您可以使用 -Maxsize或 -Default 參數，指定陰影複製可成長到的大小上限。使用 Default 會將最大 設定為檔案系統儲存容量的 10%。您無法在相同的命令中指定 -Maxsize和 -Default 參數。

使用 -Maxsize，您可以定義陰影複製儲存，如下所示：

- 以位元組為單位： Set-FsxShadowStorage -Maxsize 2500000000
- 以 KB、MB、GB 或其他單位為單位： Set-FsxShadowStorage -Maxsize (2500MB) 或 Set-FsxShadowStorage -Maxsize (2.5GB)
- 以整體儲存體的百分比表示： Set-FsxShadowStorage -Maxsize "20%"
- 無限制： Set-FsxShadowStorage -Maxsize "UNBOUNDED"

使用 -Default 設定影子儲存體，以使用高達 10% 的檔案系統：Set-FsxShadowStorage -Default。若要進一步了解如何使用預設選項，請參閱 設定陰影複本以使用預設儲存體和排程。

在 FSx for Windows File Server 檔案系統上設定陰影複製儲存量

1. 以檔案系統管理員群組的成員身分，連線至具有檔案系統網路連線能力的運算執行個體。在 中 AWS Managed Microsoft AD，該群組是AWS 委派的 FSx 管理員。在自我管理的 Microsoft AD 中，該群組是網域管理員或您在建立檔案系統時為管理指定的自訂群組。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的連線至 Windows 執行個體。
2. 在運算執行個體上開啟 Windows PowerShell 視窗。
3. 使用下列命令在您的 Amazon FSx 檔案系統上開啟遠端 PowerShell 工作階段。*FSxFileSystem-Remote-PowerShell-Endpoint* 將 取代為您要管理之檔案系統的 Windows Remote PowerShell 端點。您可以在 Amazon FSx 主控台、檔案系統詳細資訊畫面的網路與安全區段，或 DescribeFileSystem API 操作的回應中找到 Windows Remote PowerShell 端點。

```
PS C:\Users\delegateadmin> enter-pssession -computername FSxFileSystem-Remote-
PowerShell-Endpoint -configurationname fsxremoteadmin
```

4. 使用以下命令，確認尚未在檔案系統上設定陰影複製儲存。

```
[fs-1234567890abcef12]: PS>Get-FsxShadowStorage
No Fsx Shadow Storage Configured
```

5. 使用 -Default選項，將陰影儲存量設定為 磁碟區的 10%，並將陰影貼圖數目上限設定為 20。

```
[fs-1234567890abcef12]: PS>Set-FsxShadowStorage -Default
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- ------------------
             0         0 32530536858                 20
```

您可以使用 Set-FSxShadowStorage命令搭配 -MaxShadowCopyNumber 參數，並指定 1-500 的值，來限制檔案系統上允許的陰影複製數上限。根據 Microsoft 對作用中工作負載的建議，預設會將影子複本數目上限設為 20。

檢視陰影複製儲存

您可以在檔案系統的遠端 PowerShell 工作階段中使用 Get-FsxShadowStorage命令，來檢視檔案系統上影子複本目前使用的儲存量。如需在檔案系統上啟動遠端 PowerShell 工作階段的說明，請參閱 使用 Amazon FSx CLI for PowerShell。

```
[fs-1234567890abcef12]: PS>PS>Get-fsxshadowstorage
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- ------------------
             0         0 10737418240                 20
```

輸出會顯示陰影儲存組態，如下所示：

- AllocatedSpace – 檔案系統上目前配置給陰影複本的儲存量，以位元組為單位。一開始，此值為 0。
- UsedSpace – 影子複本目前使用的儲存量，以位元組為單位。一開始，此值為 0。

- MaxSpace – 影子儲存可以成長的最大儲存量，以位元組為單位。這是您使用 Set-FsxShadowStorage命令為陰影複製儲存設定的值。
- MaxShadowCopyNumber – 檔案系統可擁有的影子複本數目上限，從 1 到 500。

當UsedSpace數量達到設定的陰影複製儲存量上限 (MaxSpace) 或陰影複製數量達到設定的陰影複製數量上限 (MaxShadowCopyNumber) 時，您拍攝的下一個陰影複製會取代最舊的陰影複製。如果您不想遺失最舊的影子複本，請監控影子複本儲存體，以確保您有足夠的儲存空間存放新的影子複本。如果您需要更多空間，您可以刪除現有的影子複本，或增加影子複本儲存體的最大數量。

> **Note**
>
> 當陰影複製自動或手動建立時，它們會使用您設定為儲存限制的陰影複製儲存量。陰影複製會隨時間增加大小，並利用 CloudWatch FreeStorageCapacity 指標顯示的可用儲存空間，達到設定的陰影複製儲存量上限 (MaxSpace)。

建立自訂陰影複製排程

陰影複製排程會使用 Microsoft Windows 中的排程任務觸發來指定何時自動取得陰影複製。陰影複製排程可以有多個觸發條件，為您提供許多排程彈性。一次只能存在一個陰影複製排程。您必須先設定陰影複製儲存量，才能建立陰影複製排程。

當您在檔案系統上執行 Set-FsxShadowCopySchedule命令時，會覆寫任何現有的影子複製排程。如果您的用戶端電腦位於 UTC 時區，您也可以使用 Windows 時區和 -TimezoneId選項來指定觸發的時區。如需 Windows 時區的清單，請參閱 Microsoft 的預設時區文件，或在 Windows 命令提示字元中執行下列動作：tzutil /l。若要進一步了解 Windows 任務觸發程序，請參閱 Microsoft Windows 開發人員中心文件中的任務觸發程序。

您也可以使用 -Default選項快速設定預設陰影複製排程。如需詳細資訊，請參閱 設定陰影複本以使用預設儲存體和排程。

建立自訂陰影複製排程

1. 建立一組 Windows 排程任務觸發，以定義在陰影複製排程中擷取陰影複本的時間。在本機電腦上的 PowerShell 中使用 new-scheduledTaskTrigger命令來設定多個觸發。

   下列範例會建立自訂陰影複製排程，其會在 UTC 每週一至週五的上午 6：00 和下午 6：00 擷取陰影複製。根據預設，除非您在建立的 Windows 排程任務觸發中指定時區，否則時間會以 UTC 為單位。

```
PS C:\Users\delegateadmin> $trigger1 = new-scheduledTaskTrigger -weekly -DaysOfWeek
 Monday,Tuesday,Wednesday,Thursday,Friday -at 06:00
PS C:\Users\delegateadmin> $trigger2 = new-scheduledTaskTrigger -weekly -DaysOfWeek
 Monday,Tuesday,Wednesday,Thursday,Friday -at 18:00
```

2. 使用 invoke-command執行 scriptblock命令。這樣做會編寫指令碼，以您剛建立new-scheduledTaskTrigger的值設定陰影複製排程。*FSxFileSystem-Remote-PowerShell-Endpoint* 將 取代為您要管理的檔案系統的 Windows Remote PowerShell 端點。您可以在 Amazon FSx 主控台、檔案系統詳細資訊畫面的網路與安全區段，或 DescribeFileSystem API 操作的回應中找到 Windows Remote PowerShell 端點。

```
PS C:\Users\delegateadmin> invoke-command -ComputerName FSxFileSystem-Remote-
PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {
```

3. 在>>提示中輸入以下行，以使用 set-fsxshadowcopyschedule命令設定陰影複製排程。

```
>> set-fsxshadowcopyschedule -scheduledtasktriggers $Using:trigger1,$Using:trigger2
 -Confirm:$false }
```

回應會顯示您在檔案系統上設定的陰影複製排程。

```
FSx Shadow Copy Schedule


Start Time:     : 2019-07-16T06:00:00+00:00
Days of Week    : Monday,Tuesday,Wednesday,Thursday,Friday
WeeksInterval   : 1
PSComputerName : fs-0123456789abcdef1
RunspaceId      : 12345678-90ab-cdef-1234-567890abcde1

Start Time:     : 2019-07-16T18:00:00+00:00
Days of Week    : Monday,Tuesday,Wednesday,Thursday,Friday
WeeksInterval   : 1
PSComputerName : fs-0123456789abcdef1
RunspaceId      : 12345678-90ab-cdef-1234-567890abcdef
```

檢視陰影複製排程

若要檢視檔案系統上現有的影子複製排程，請在檔案系統的遠端 PowerShell 工作階段中輸入下列命令。如需在檔案系統上啟動遠端 PowerShell 工作階段的說明，請參閱 使用 Amazon FSx CLI for PowerShell。

```
[fs-0123456789abcdef1]PS> Get-FsxShadowCopySchedule
FSx Shadow Copy Schedule

Start Time                Days of week                              WeeksInterval
----------                ------------                              -------------
2019-07-16T07:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
2019-07-16T12:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
```

建立陰影複製

若要手動建立陰影副本，請在檔案系統的遠端 PowerShell 工作階段中輸入下列命令。如需在檔案系統上啟動遠端 PowerShell 工作階段的說明，請參閱 使用 Amazon FSx CLI for PowerShell。

```
[fs-0123456789abcdef1]PS>New-FsxShadowCopy

Shadow Copy {ABCDEF12-3456-7890-ABCD-EF1234567890} taken successfully
```

檢視現有的影子複本

若要檢視檔案系統上現有的影子複本集，請在檔案系統的遠端 PowerShell 工作階段中輸入下列命令。如需在檔案系統上啟動遠端 PowerShell 工作階段的說明，請參閱 使用 Amazon FSx CLI for PowerShell。

```
[fs-0123456789abcdef1]PS>Get-FsxShadowCopies
FSx Shadow Copies: 2 total

Shadow Copy ID                        Creation Time
--------------                        -----------------
{ABCDEF12-3456-7890-ABCD-EF1234567890} 6/17/2019 7:11:09 AM
{FEDCBA21-6543-0987-0987-EF3214567892} 6/19/2019 11:24:19 AM
```

刪除陰影複本

您可以在檔案系統的遠端 PowerShell 工作階段中使用 Remove-FsxShadowCopies命令，刪除檔案系統上的一或多個現有影子複本。如需在檔案系統上啟動遠端 PowerShell 工作階段的說明，請參閱 使用 Amazon FSx CLI for PowerShell。

使用下列其中一個必要選項，指定要刪除的影子複本：

- -Oldest 刪除最舊的陰影複製
- -All 刪除所有現有的影子複本
- -ShadowCopyId 會依 ID 刪除特定影子複本。

您只能搭配 命令使用一個選項。如果您未指定要刪除的陰影複製、指定多個陰影複製 IDs，或指定無效的陰影複製 ID，就會發生錯誤。

若要刪除檔案系統上最舊的影子副本，請在檔案系統的遠端 PowerShell 工作階段中輸入下列命令。

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopies -Oldest
Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FSxShadowCopies" on target "Removing oldest shadow
 copy".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y": Y
Shadow Copy {ABCDEF12-3456-7890-ABCD-EF1234567890} deleted
```

若要刪除檔案系統上的特定影子副本，請在檔案系統的遠端 PowerShell 工作階段中輸入下列命令。

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopies -ShadowCopyId "{ABCDEF12-3456-7890-
ABCD-EF1234567890}"
Are you sure you want to perform this action?
Performing the operation "Remove-FSxShadowCopies" on target "Removing shadow copy
 {ABCDEF12-3456-7890-ABCD-EF1234567890}".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y":>Y
Shadow Copy \\AMZNFSXABCDE123\root\cimv2:Wind32_ShadowCopy.ID{ABCDEF12-3456-7890-ABCD-
EF1234567890}".ID deleted.
```

若要刪除檔案系統上最舊影子複本的特定數量，請將 -MaxShadowCopyNumber 參數更新為您想要保留的影子複本數量。不過，此變更只會在拍攝下一個陰影複製快照之後生效，此時系統會自動刪除多餘的陰影複製。在檔案系統的遠端 PowerShell 工作階段中使用以下命令。

```
[fs-1234567890abcef12]: PS>Get-fsxshadowstorage
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace MaxSpace    MaxShadowCopyNumber
-------------- --------- ----------- -------------------
     556679168  21659648 10737418240                  50

[fs-1234567890abcef12]: PS>Set-FsxShadowStorage  -MaxShadowCopyNumber 5
Validation
You have 50 shadow copies. Older versions of shadow copies will be deleted, keeping 5
 latest shadow copies on your file system.
Do you want to continue?
[Y] Yes  [N] No  [?] Help (default is "N"): y
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- -------------------
     556679168  21659648 10737418240                   5
```

刪除陰影複製排程

若要刪除檔案系統上現有的影子複製排程，請在檔案系統的遠端 PowerShell 工作階段中輸入下列命令。如需在檔案系統上啟動遠端 PowerShell 工作階段的說明，請參閱 使用 Amazon FSx CLI for PowerShell。

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopySchedule

Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FsxShadowCopySchedule" on target "Removing FSx Shadow
 Copy Schedule".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y"): Y
[fs-0123456789abcdef1]PS>
```

刪除陰影複製儲存、排程和所有陰影複製

您可以刪除陰影複製組態，包括所有現有的陰影複製和陰影複製排程。同時，您可以在檔案系統上釋放陰影複製儲存體。

若要這樣做，請在檔案系統的遠端 PowerShell 工作階段中輸入 Remove-FsxShadowStorage命令。如需在檔案系統上啟動遠端 PowerShell 工作階段的說明，請參閱 使用 Amazon FSx CLI for PowerShell。

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowStorage

Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FsxShadowStorage" on target "Removing all Shadow
 Copies, Shadow Copy Schedule, and Shadow Storage".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y": Y
FSx Shadow Storage Configuration
Removing Shadow Copy Schedule
Removing Shadow Copies
All shadow copies removed.
Removing Shadow Storage
Shadow Storage removed successfully.
```

對陰影複本進行故障診斷

當影子複本遺失或無法存取時，有許多潛在原因，如下節所述。

主題

- 缺少最舊的陰影副本
- 缺少我的所有影子複本
- 無法在最近還原或更新的檔案系統上建立 Amazon FSx 備份或存取陰影複本

缺少最舊的陰影副本

在下列其中一種情況下，最舊的陰影複本會被刪除：

- 如果您有 500 個陰影複本，則下一個陰影複本會取代最舊的陰影複本，無論陰影複本剩餘的配置儲存空間為何。
- 如果達到設定的陰影複製儲存量上限，下一個陰影複製會取代一或多個最舊的陰影複製，即使您的陰影複製少於 500 個。

這兩個結果都是預期的行為。如果您為影子複本配置的儲存空間不足，請考慮增加您配置的儲存空間。

缺少我的所有影子複本

檔案系統沒有足夠的 I/O 效能容量 （例如，因為您使用 HDD 儲存體，因為 HDD 儲存體的爆量容量不足，或輸送量容量不足） 可能會導致 Windows Server 刪除所有影子複本，因為它無法以可用的 I/O 效能容量維護影子複本。請考慮下列建議，以協助預防此問題：

- 如果您使用 HDD 儲存，請使用 Amazon FSx 主控台或 Amazon FSx API 切換到使用 SSD 儲存。如需詳細資訊，請參閱管理檔案系統的儲存類型。
- 將檔案系統的輸送量容量增加到您預期工作負載的三倍。
- 除了設定的陰影複製儲存數量上限之外，請確定您的檔案系統至少有 320 MB 的可用空間。
- 當您預期檔案系統閒置時，排程陰影複製。

如需詳細資訊，請參閱陰影副本的檔案系統建議。

無法在最近還原或更新的檔案系統上建立 Amazon FSx 備份或存取陰影複本

這是預期的行為。Amazon FSx 會在最近還原的檔案系統上重建陰影複製狀態，不允許在重建進行時存取陰影複製或備份。

使用 排程複寫 AWS DataSync

您可以使用 AWS DataSync 將 FSx for Windows File Server 檔案系統定期複寫到第二個檔案系統。此功能適用於區域內和跨區域部署。若要進一步了解，請參閱本指南使用 將現有檔案遷移至 FSx for Windows File Server AWS DataSync中的 和AWS DataSync 《 使用者指南》中的AWS 儲存服務之間的資料傳輸。

將 FSx for Windows File Server 與 Microsoft SQL Server 搭配使用

高可用性 (HA) Microsoft SQL Server 通常部署在 Windows Server 容錯移轉叢集 (WSFC) 中的多個資料庫節點，每個節點都可以存取共用檔案儲存。您可以使用 FSx for Windows File Server 做為高可用性 (HA) Microsoft SQL Server 部署的共用儲存體，方法有兩種：做為作用中資料檔案的儲存體，以及做為 SMB 檔案共用見證。

> **Note**
>
> 目前，Amazon FSx 不支援 Microsoft SQL Server IFI （即時檔案初始化） 功能。

SQL Server 建議使用 SSD 儲存體。SSD 儲存體專為最高效能和最延遲敏感的工作負載而設計，包括資料庫。

如需使用 Amazon FSx 降低 SQL Server 高可用性部署的複雜性和成本的詳細資訊，請參閱 AWS Storage 部落格上的下列文章：

- 使用 Amazon FSx for Windows File Server 簡化 Microsoft SQL Server 高可用性部署
- 在 上最佳化高可用性 SQL Server 部署的成本 AWS
- 使用 AWS 啟動精靈和 Amazon FSx 簡化 SQL Server Always On 部署

使用 Amazon FSx for Active SQL Server 資料檔案

Microsoft SQL Server 可以使用 SMB 檔案共用部署，做為作用中資料檔案的儲存選項。Amazon FSx 經過最佳化，透過支援持續可用的 (CA) 檔案共用，為 SQL Server 資料庫提供共用儲存。這些檔案共用是專為 SQL Server 這類需要不間斷存取共用檔案資料的應用程式所設計。雖然您可以在單一可用區 2 檔案系統上建立 CA 共享，但您必須在所有 SQL Server 部署的多可用區檔案系統上使用 CA 共享，無論是否有 HA。

建立持續可用共享

您可以使用 Amazon FSx CLI for Remote Management on PowerShell 來建立 CA 共享。若要指定共享是持續可用的共享，請使用 `New-FSxSmbShare`，並將 `-ContinuouslyAvailable`選項設定為 `$True`。如需詳細資訊，請參閱建立持續可用的 (CA) 共享。

設定 SMB 逾時設定

如 中所述程序失敗，多可用區容錯移轉和容錯回復可能會導致 I/O 暫停，通常在 30 秒內完成。根據設定方式，您的 SQL Server 應用程式可能對逾時設定有不同的敏感度。

您可以調整 SMB 用戶端組態工作階段逾時，以確保您的應用程式對多可用區檔案系統容錯移轉具有彈性。您可以在容錯移轉期間透過更新檔案系統的輸送量容量來測試應用程式的行為，這會啟動自動容錯移轉和容錯回復。

使用 Amazon FSx 做為 SMB 檔案共用見證

Windows Server 容錯移轉叢集部署通常會部署 SMB 檔案共用見證，以維持叢集資源的人數。見證檔案共享只需要少量的儲存量來提供規定人數資訊。Amazon FSx 檔案系統可以用作 Windows Server 容錯移轉叢集部署的 SMB 檔案共用見證。

將現有的檔案儲存遷移至 Amazon FSx

Amazon FSx for Windows File Server 具有功能、效能和相容性，可協助您輕鬆將企業應用程式提升和轉移至 Amazon Web Services Cloud。將內部部署 Microsoft Windows File Server 儲存體遷移至 FSx for Windows File Server 的程序有下列四個主要步驟：

1. 將您的檔案遷移至 FSx for Windows File Server。如需詳細資訊，請參閱將現有的檔案儲存遷移至 FSx for Windows File Server。
2. 將您的檔案共用組態遷移至 FSx for Windows File Server。如需詳細資訊，請參閱將內部部署檔案共用組態遷移至 Amazon FSx。
3. 將現有的 DNS 名稱關聯為 Amazon FSx 檔案系統的 DNS 別名。如需詳細資訊，請參閱將 DNS 別名與 Amazon FSx 建立關聯。
4. 切換至 FSx for Windows File Server。如需詳細資訊，請參閱將操作切換至 Amazon FSx for Windows File Server。

您可以在以下各節中找到程序中每個步驟的詳細資訊。

主題

- 將現有的檔案儲存遷移至 FSx for Windows File Server
- 將內部部署檔案共用組態遷移至 Amazon FSx
- 將內部部署 DNS 組態遷移至 FSx for Windows File Server
- 將操作切換至 Amazon FSx for Windows File Server

將現有的檔案儲存遷移至 FSx for Windows File Server

若要將現有檔案遷移至 FSx for Windows File Server 檔案系統，建議您使用 線上資料傳輸服務 AWS DataSync，該服務旨在簡化、自動化和加速在 AWS 儲存服務之間複製大量資料。DataSync 透過網際網路或 複製資料 Direct Connect。作為全受管服務，DataSync 無需修改應用程式、開發指令碼或管理基礎設施。如需詳細資訊，請參閱使用 將現有檔案遷移至 FSx for Windows File Server AWS DataSync。

做為替代解決方案，您可以使用強式檔案複製或 Robocopy，這是 Microsoft Windows 的命令列目錄和檔案複寫命令集。如需如何使用 Robocopy 將檔案儲存遷移至 FSx for Windows File Server 的詳細程序，請參閱 使用 Robocopy 將現有檔案遷移至 FSx for Windows File Server。

將現有檔案儲存遷移至 FSx for Windows File Server 的最佳實務

若要盡快將大量資料遷移至 FSx for Windows File Server，請使用使用固態硬碟 (SSD) 儲存體設定的 Amazon FSx 檔案系統。遷移完成後，如果您的應用程式的最佳解決方案，您可以使用硬碟 (HDD) 儲存將資料移至 Amazon FSx 檔案系統。

若要使用 SSD 儲存體將資料從 Amazon FSx 檔案系統移動到 HDD 儲存體，您可以執行下列步驟。（請注意，HDD 檔案系統的儲存容量至少為 2TB，您無法在從備份還原時變更儲存容量。）

1. 備份您的 SSD 檔案系統。如需詳細資訊，請參閱建立使用者啟動的備份。
2. 使用 HDD 儲存將備份還原至檔案系統。如需詳細資訊，請參閱將備份還原至新的檔案系統。

使用 將現有檔案遷移至 FSx for Windows File Server AWS DataSync

建議您使用 AWS DataSync 在 FSx for Windows File Server 檔案系統之間傳輸資料。DataSync 是一種資料傳輸服務，可簡化、自動化和加速透過網際網路或 ，在內部部署儲存系統與其他 AWS 儲存服務之間移動和複寫資料 Direct Connect。DataSync 可以傳輸檔案系統資料和中繼資料，例如擁有權、時間戳記和存取許可。

DataSync 支援複製 NTFS 存取控制清單 ACLs)，也支援複製檔案稽核控制資訊，也稱為 NTFS 系統存取控制清單 (SACLs)，供管理員用來控制使用者嘗試存取檔案的稽核記錄。

您可以使用 DataSync 在兩個 FSx for Windows File Server 檔案系統之間傳輸檔案，也可以將資料移至不同 AWS 區域 或 AWS 帳戶中的檔案系統。您可以使用 DataSync 搭配 FSx for Windows File Server 檔案系統進行其他任務。例如，您可以執行一次性資料遷移、定期擷取分散式工作負載的資料，以及排程複寫以進行資料保護和復原。

在 中 AWS DataSync，FSx for Windows File Server 的位置是 FSx for Windows File Server 的端點。您可以在 FSx for Windows File Server 的位置與其他檔案系統的位置之間傳輸檔案。如需詳細資訊，請參閱AWS DataSync 《 使用者指南》中的使用位置。

DataSync 會使用伺服器訊息區塊 (SMB) 通訊協定存取您的 FSx for Windows File Server。它使用您在 AWS DataSync 主控台或 中設定的使用者名稱和密碼進行身分驗證 AWS CLI。

先決條件

若要將資料遷移至 Amazon FSx for Windows File Server 設定，您需要符合 DataSync 需求的伺服器和網路。若要進一步了解，請參閱AWS DataSync 《 使用者指南》中的 DataSync 需求。

如果您要執行大型資料遷移，或涉及許多小型檔案的遷移，我們建議您使用具有 SSD 儲存類型的 Amazon FSx 檔案系統。這是因為 DataSync 任務涉及掃描檔案中繼資料，這會耗盡 HDD 檔案系統的磁碟 IOPS 限制，導致長時間執行遷移和檔案系統效能影響。如需詳細資訊，請參閱 將現有檔案儲存遷移至 FSx for Windows File Server 的最佳實務。

如果您的資料集大部分是由小型檔案組成，且檔案計數以百萬為單位，或者您有比單一 DataSync 任務能耗更多的可用網路頻寬，您也可以使用向外擴展架構加速資料傳輸。如需詳細資訊，請參閱：如何使用 AWS DataSync 橫向擴展架構加速資料傳輸。

您可以使用 FSx 效能指標監控檔案系統的磁碟 I/O 使用率。

使用 DataSync 遷移檔案的基本步驟

若要使用 DataSync 將檔案從來源位置傳輸到目的地位置，請執行下列基本步驟：

- 在您的環境下載並部署代理程式，並啟用該代理程式。
- 建立和設定來源與目的地位置。
- 建立並設定任務。
- 執行任務以將檔案從來源傳輸至目的地。

若要了解如何將檔案從現有的現場部署檔案系統傳輸到 FSx for Windows File Server，請參閱AWS DataSync 《 使用者指南》中的自我管理儲存與 之間的資料傳輸 AWS、建立 SMB 位置，以及為 Amazon FSx for Windows File Server 建立位置。

若要了解如何將檔案從現有的雲端檔案系統傳輸到 FSx for Windows File Server，請參閱AWS DataSync 《 使用者指南》中的將代理程式部署為 Amazon EC2 執行個體。

在兩個 Amazon FSx 檔案系統之間遷移

您可以使用 DataSync 在兩個 Amazon FSx 檔案系統之間遷移資料。如果您需要將工作負載從現有檔案系統移至具有不同組態的新檔案系統，例如從單一可用區移至多可用區組態，這可能會有所幫助。您也可以使用 DataSync 在兩個檔案系統之間分割工作負載。

以下是遷移程序的範例概觀：

1. 建立來源和目的地檔案系統的 DataSync 位置。請注意，來源和目的地必須屬於相同的 Active Directory (AD) 網域，或其網域之間具有 AD 信任關係。
2. 建立並設定 DataSync 任務，將資料從來源傳輸到目的地。您可以一次性執行個體執行任務，或將任務設定為按照您設定的排程自動執行。

3. 任務成功完成後，目的地檔案系統中的資料就是來源的確切複本。請注意，您將需要暫停來源檔案系統上的任何寫入活動或檔案更新，以完成任務。然後，您可以切換到目的地檔案系統，並刪除來源檔案系統。

從生產檔案系統遷移之前，您可以在從最近備份還原的檔案系統上測試遷移程序。這可讓您預估資料傳輸程序需要多長時間，並事先對 DataSync 錯誤進行故障診斷。

若要將切換時間降至最低，您可以事先執行 DataSync 任務，將大部分資料從來源檔案系統移至目的地檔案系統。停止來源檔案系統的流量後，您可以執行一次最終任務傳輸，以同步自停止流量以來新更新的任何資料，然後切換到目的地檔案系統。

您可以將 DataSync 任務設定為僅在特定目錄中執行，或包含或排除特定路徑。如果您平行執行多個任務，或者您想要遷移一部分的資料，這很有用。

您可以在目的地檔案系統上建立與來源檔案系統 DNS 名稱相同的 DNS 別名。這可讓最終使用者和應用程式繼續使用來源檔案系統的 DNS 名稱來存取檔案資料。如需如何設定 DNS 別名的詳細資訊，請參閱：使用 DNS 別名存取資料。

執行這類遷移時，我們建議下列事項：

- 排程您的遷移，以避免任何檔案系統備份、每週維護時段和Data Deduplication任務。具體而言，如果任務與您規劃的遷移重疊，建議您停用該Data Deduplication GarbageCollection任務。
- 為您的來源和目的地檔案系統使用 SSD 儲存類型。您可以從備份還原，在 HDD 和 SSD 儲存類型之間切換。如需詳細資訊，請參閱：將現有的檔案儲存遷移至 FSx for Windows File Server。
- 針對您需要傳輸的資料量，設定具有足夠輸送量的來源和目的地檔案系統。在 DataSync 任務程序期間，監控來源和目的地檔案系統的效能使用率。如需詳細資訊，請參閱 使用 Amazon CloudWatch 監控。
- 設定 DataSync 監控，以協助您了解進行中任務的進度。您也可以將 DataSync 日誌傳送至 Amazon CloudWatch Logs 群組，以便在遇到任何錯誤時協助您偵錯任務。

使用 Robocopy 將現有檔案遷移至 FSx for Windows File Server

Amazon FSx for Windows File Server 以 Microsoft Windows Server 為基礎，可讓您將現有的資料集完全遷移至 Amazon FSx 檔案系統。您可以遷移每個檔案的資料。您也可以遷移所有相關檔案中繼資料，包括屬性、時間戳記、存取控制清單 (ACLs)、擁有者資訊和稽核資訊。Amazon FSx 支援此整體遷移，可讓您將依賴這些檔案資料集的 Windows 工作負載和應用程式移至 Amazon Web Services Cloud。

使用下列主題做為複製現有檔案資料程序的指南。當您執行此複製時，您會保留內部部署資料中心或 Amazon EC2 上自我管理檔案伺服器的所有檔案中繼資料。

使用 Robocopy 遷移檔案的先決條件

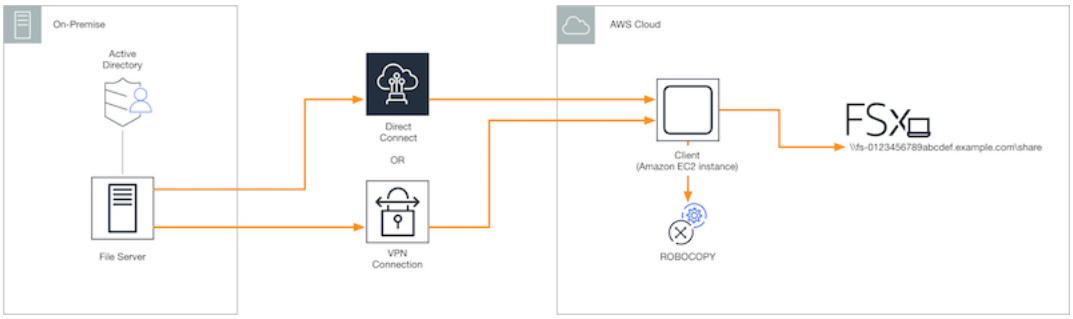
開始之前，請務必執行下列動作：

- 在現場部署 Active Directory 和您要建立 Amazon FSx 檔案系統的 VPC 之間建立網路連線（使用 Direct Connect 或 VPN)。
- 在 Active Directory 上建立服務帳戶，並具有將電腦加入網域的委派許可。如需詳細資訊，請參閱 AWS Directory Service 管理指南中的將權限委派給您的服務帳戶。
- 建立 Amazon FSx 檔案系統，加入您的自我管理（內部部署）Microsoft AD 目錄。
- 請注意檔案共用（內部部署或 中`\\Source\Share`) 的位置（例如 AWS)，其中包含您要轉移到 Amazon FSx 的現有檔案。
- 請注意 Amazon FSx 檔案系統上檔案共用的位置（例如 `\\Target\Share`)，您要透過現有檔案傳輸。

下表摘要說明三個遷移使用者存取模型的來源和目的地檔案系統可存取性需求。

遷移使用者存取模型	來源檔案系統可存取性需求	目的地 FSx 檔案伺服器可存取性要求
直接讀取/寫入許可模型	使用者至少需要對要遷移的檔案和資料夾具有讀取許可 (NTFS ACLs)。	使用者至少需要對要遷移的檔案和資料夾擁有寫入許可 (NTFS ACLs)。
備份/還原權限模型以覆寫存取許可	使用者必須是內部部署 Active Directory 備份運算子群組的成員，並使用 /b 旗標搭配 RoboCopy。	使用者必須是 Amazon FSx 檔案系統管理員群組* 的成員，並搭配 RoboCopy 使用 /b 旗標。
網域管理員（完整）權限模型，以覆寫存取許可	使用者必須是現場部署 Active Directory 網域管理員群組的成員。	使用者必須是 Amazon FSx 檔案系統管理員群組* 的成員，並搭配 RoboCopy 使用 /b 旗標

> **Note**
>
> * 對於加入 AWS Managed Microsoft AD 的檔案系統，Amazon FSx 檔案系統管理員群組是AWS 委派的 FSx 管理員。在自我管理的 Microsoft AD 中，Amazon FSx 檔案系統管理員群組是網域管理員，或您在建立檔案系統時為管理指定的自訂群組。



使用 Robocopy 遷移檔案

您可以使用下列程序，將現有檔案從現場部署檔案系統遷移至 FSx for Windows File Server 檔案系統。

使用 Robocopy 將現有檔案遷移至 Amazon FSx

1. 在與 Amazon FSx 檔案系統相同的 Amazon VPC 中啟動 Windows Server 2016 Amazon EC2 執行個體。 FSx
2. 連線到您的 Amazon EC2 執行個體。如需詳細資訊，請參閱《Amazon EC2 Windows 執行個體使用者指南》中的連線至您的 Windows 執行個體。
3. 開啟命令提示字元，並將現有檔案伺服器上的來源檔案共用（內部部署或內部 AWS) 映射至磁碟機代號（例如 *Y*：），如下所示。為此，您會為內部部署 Active Directory 網域管理員群組的成員提供登入資料。

```
C:\>net use Y: \\fileserver1.mydata.com\localdata /user:mydata.com\Administrator
Enter the password for 'fileserver1.mydata.com': _

Drive Y: is now connected to \\fileserver1.mydata.com\localdata.

The command completed successfully.
```

4. 將 Amazon FSx 檔案系統上的目標檔案共用映射至 Amazon EC2 執行個體上的不同磁碟機代號（例如 *Z*：），如下所示。為此，您會為使用者帳戶提供登入資料，該帳戶是現場部署 Active

Directory 網域管理員群組和 Amazon FSx 檔案系統管理員群組的成員。對於加入 AWS Managed Microsoft AD 的檔案系統，該群組為 **AWS Delegated FSx Administrators**。在自我管理的 Microsoft AD **Domain Admins**中，該群組是您建立檔案系統時為管理指定的自訂群組。

如需詳細資訊，請參閱 中的來源和目的地檔案系統存取需求資料表使用 Robocopy 遷移檔案的先決條件。

```
C:\>net use Z: \\amznfsxabcdef1.mydata.com\share /user:mydata.com\Administrator
Enter the password for 'amznfsxabcdef1.mydata.com': _

Drive Z: is now connected to \\amznfsxabcdef1.mydata.com\share.

The command completed successfully.
```

5. 從內容功能表中選擇以管理員身分執行。以管理員身分開啟命令提示字元或 Windows PowerShell，並執行下列 Robocopy 命令，將檔案從來源共用複製到目標共用。

   ROBOCOPY 命令是一種靈活的檔案傳輸公用程式，具有多個選項來控制資料傳輸程序。由於此ROBOCOPY命令程序，來自來源共用的所有檔案和目錄都會複製到 Amazon FSx 目標共用。複本會保留檔案和資料夾 NTFS ACLs、屬性、時間戳記、擁有者資訊和稽核資訊。

   ```
   robocopy Y:\ Z:\ /copy:DATSOU /secfix /e /b /MT:8
   ```

   上述命令範例使用下列元素和選項：

   - Y – 指位於內部部署 Active Directory 樹系 mydata.com 中的來源共用。
   - Z – 是指 Amazon FSx 上的目標共享 \\amznfsxabcdef1.mydata.com\share。
   - /copy – 指定要複製的下列檔案屬性：
     - D – 資料
     - A – 屬性
     - T – 時間戳記
     - S – NTFS ACLs
     - O – 擁有者資訊
     - U – 稽核資訊。
   - /secfix – 修正所有檔案上的檔案安全性，甚至是略過的檔案安全性。
   - /e – 複製子目錄，包括空的子目錄。

- /b – 使用 Windows 中的備份和還原權限來複製檔案，即使其 NTFS ACLs拒絕目前使用者的許可。
- /MT：8 – 指定要用於執行多執行緒複本的執行緒數量。

> **Note**
>
> 如果您要透過緩慢或不可靠的連線複製大型檔案，您可以使用 /zb選項來啟用可重新啟動模式，robocopy並取代 /b選項。使用可重新啟動模式時，如果大型檔案的傳輸中斷，則後續的 Robocopy 操作可以在傳輸過程中提取，而不必從頭重新複製整個檔案。啟用可重新啟動模式可以降低資料傳輸速度。

將內部部署檔案共用組態遷移至 Amazon FSx

您可以使用下列程序，將現有的檔案共用組態遷移至 Amazon FSx。在此程序中，來源檔案伺服器是您要遷移至 Amazon FSx 的檔案共用組態的檔案伺服器。

> **Note**
>
> 首先將檔案遷移至 Amazon FSx，然後再遷移檔案共用組態。如需詳細資訊，請參閱[將現有的檔案儲存遷移至 FSx for Windows File Server]。

將現有檔案共用遷移至 FSx for Windows File Server

1. 在來源檔案伺服器上，從內容功能表中選擇以管理員身分執行。以管理員身分開啟 Windows PowerShell。
2. 在 PowerShell 中`SmbShares.xml`執行下列命令，將來源檔案伺服器的檔案共用匯出至名為 的檔案。在此範例中，將 F： 取代為您匯出檔案共用之檔案伺服器上的磁碟機代號。

   ```
   $shareFolder = Get-SmbShare -Special $false | ? { $_.Path -like “F:\*” }
   $shareFolder | Export-Clixml -Path F:\SmbShares.xml
   ```

3. 編輯 `SmbShares.xml` 檔案，將 F： （磁碟機代號） 的所有參考取代為 D：\share，因為 Amazon FSx 檔案系統位於 D：\share。
4. 將現有的檔案共用組態匯入 FSx for Windows File Server。在可存取目的地 Amazon FSx 檔案系統和來源檔案伺服器的用戶端上，複製儲存的檔案共用組態。然後使用下列命令將其匯入變數。

```
$shares = Import-Clixml -Path F:\SmbShares.xml
```

5. 使用下列其中一個選項，準備在 FSx for Windows File Server 檔案伺服器上建立檔案共用所需的登入資料物件。

   若要以互動方式產生登入資料物件，請使用下列命令。

   ```
   $credential = Get-Credential
   ```

   若要使用 AWS Secrets Manager 資源產生登入資料物件，請使用下列命令。

   ```
   $credential = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
    $AdminSecret).SecretString
   $FSxAdminUserCredential = (New-Object PSCredential($credential.UserName,(ConvertTo-
   SecureString $credential.Password -AsPlainText -Force)))
   ```

6. 使用下列指令碼將檔案共用組態遷移至 Amazon FSx 檔案伺服器。

   ```
   $FSxAcceptedParameters = ("ContinuouslyAvailable", "Description",
    "ConcurrentUserLimit", "CATimeout", "FolderEnumerationMode", "CachingMode",
    "FullAccess", "ChangeAccess", "ReadAccess", "NoAccess", "SecurityDescriptor",
    "Path", "Name", "EncryptData")
   ForEach ($item in $shares) {
       $param = @{};
       Foreach ($property in $item.psObject.properties) {
           if ($property.Name -In $FSxAcceptedParameters) {
               $param[$property.Name] = $property.Value
           }
       }
       Invoke-Command -ConfigurationName FSxRemoteAdmin -ComputerName
    amznfsxxxxxxxxx.corp.com -ErrorVariable errmsg -ScriptBlock { New-FSxSmbShare -
   Credential $Using:credential @Using:param }
   }
   ```

將內部部署 DNS 組態遷移至 FSx for Windows File Server

FSx for Windows File Server 為每個檔案系統提供預設網域名稱系統 (DNS) 名稱，您可以用來存取檔案系統上的資料。您也可以使用您選擇的任何 DNS 名稱來存取檔案系統，方法是將備用 DNS 名稱設定為 Amazon FSx 檔案系統的 DNS 別名。

透過 DNS 別名，您可以將檔案系統儲存從內部部署遷移到 Amazon FSx 時，繼續使用現有的 DNS 名稱來存取 Amazon FSx 上存放的資料。這有助於消除在遷移至 Amazon FSx 時，更新任何使用您的 DNS 名稱之工具或應用程式的需求。您可以在建立新檔案系統時，以及從備份建立新檔案系統時，將 DNS 別名與現有的 FSx for Windows File Server 檔案系統建立關聯。您一次最多可將 50 個 DNS 別名與檔案系統建立關聯。如需詳細資訊，請參閱管理 DNS 別名。

DNS 別名名稱必須符合下列要求：

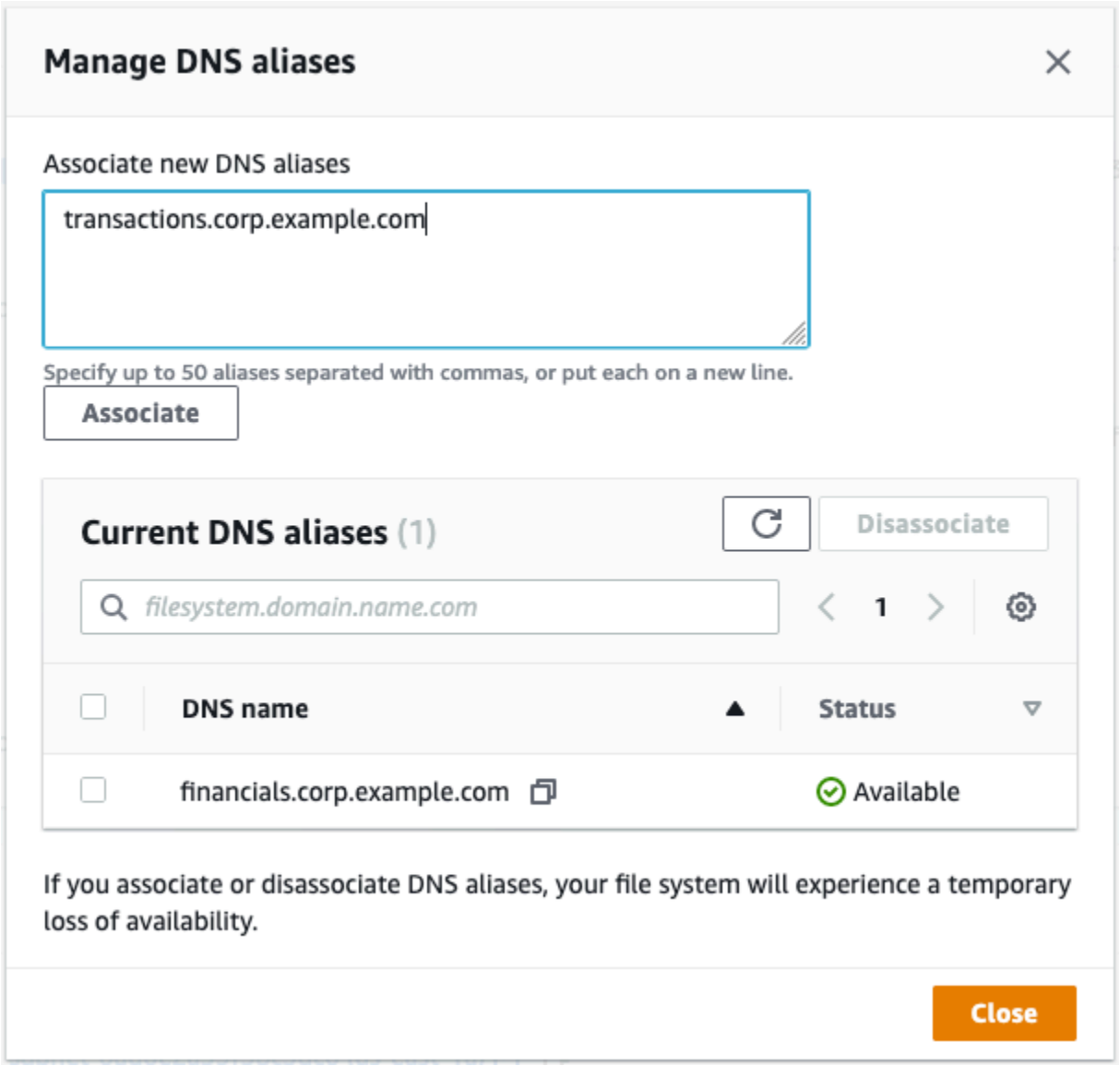
- 必須格式化為完整網域名稱 (FQDN)，例如 `accounting.example.com`。
- 可包含英數字元和連字號 (-)。
- 名稱開頭或結尾不能為連字號 (-)。
- 可以從數字開頭。

對於 DNS 別名名稱，Amazon FSx 會將字母字元儲存為小寫字母 (a-z)，不論儲存時指定為大寫、小寫字母或逸出碼中的對應字母。

下列程序說明如何使用 Amazon FSx 主控台、CLI 和 API 將 DNS 別名與現有的 FSx for Windows File Server 檔案系統建立關聯。如需在建立新檔案系統時關聯 DNS 別名的詳細資訊，包括來自備份的新檔案系統，請參閱 將 DNS 別名與檔案系統建立關聯。

將 DNS 別名與現有檔案系統建立關聯 （主控台）

1. 在 https://console.aws.amazon.com/fsx/：// 開啟 Amazon FSx 主控台。
2. 導覽至檔案系統，然後選擇您要與 DNS 別名建立關聯的 Windows 檔案系統。
3. 在網路與安全索引標籤上，選擇管理 DNS 別名以開啟管理 DNS 別名對話方塊。



4. 在關聯新別名方塊中，輸入您要關聯的 DNS 別名。
5. 選擇關聯，將別名新增至檔案系統。

   您可以監控您在目前別名清單中剛關聯的別名狀態。當狀態讀取為可用時，別名會與檔案系統相關聯（最多可能需要 2.5 分鐘的程序）。

將 DNS 別名與現有檔案系統 (CLI) 建立關聯

- 使用 `associate-file-system-aliases` CLI 命令或 AssociateFileSystemAliases API 操作，將 DNS 別名與現有檔案系統建立關聯。

  下列 CLI 請求會將兩個別名與指定的檔案系統建立關聯。

```
aws fsx associate-file-system-aliases \
    --file-system-id fs-0123456789abcdef0 \
    --aliases financials.corp.example.com transfers.corp.example.com
```

回應會顯示 Amazon FSx 正在與檔案系統建立關聯的別名狀態。

```
{
      "Aliases": [
          {
              "Name": "financials.corp.example.com",
              "Lifecycle": CREATING
          },
          {
              "Name": "transfers.corp.example.com",
              "Lifecycle": CREATING
          }
      ]
  }
```

若要監控您正在關聯的別名狀態，請使用 `describe-file-system-aliases` CLI 命令 (DescribeFileSystemAliases 是同等的 API 操作）。當 `Lifecycle` 別名的值為可用時，您可以使用它來存取檔案系統 （最多可能需要 2.5 分鐘的程序）。

將操作切換至 Amazon FSx for Windows File Server

在您遷移內部部署檔案儲存、檔案共用組態和 DNS 組態之後，下一步是將操作縮減至 FSx for Windows File Server 檔案系統。若要切換到 FSx for Windows File Server 檔案系統，請執行下列步驟：

- 準備切開。
  - 暫時中斷 SMB 用戶端與原始檔案系統的連線。
  - 執行最終檔案和檔案共享組態同步。
- 為您的 Amazon FSx 檔案系統設定服務主體名稱 (SPNs)。
- 更新 DNS CNAME 記錄以指向您的 Amazon FSx 檔案系統。

以下各節提供執行每個步驟的程序。

主題

準備切換到 Amazon FSx

若要準備切換到您的 Amazon FSx 檔案系統，您必須執行下列動作：

- 中斷所有寫入原始檔案系統的用戶端的連線。
- 使用 AWS DataSync 或 Robocopy 執行最終檔案同步。如需詳細資訊，請參閱將現有的檔案儲存遷移至 FSx for Windows File Server。
- 執行最終檔案共享組態同步。如需詳細資訊，請參閱將內部部署檔案共用組態遷移至 Amazon FSx。

設定 SPNs以進行 Kerberos 身分驗證

我們建議您使用 Kerberos 型身分驗證和加密與 Amazon FSx 傳輸。Kerberos 為存取檔案系統的用戶端提供最安全的身分驗證。若要為使用 DNS 別名存取 Amazon FSx 的用戶端啟用 Kerberos 身分驗證，您必須新增對應至 Amazon FSx 檔案系統 Active Directory 電腦物件上 DNS 別名的服務主體名稱 (SPNs)。

Kerberos 身分驗證需要兩個 SPNs。

```
HOST/alias
HOST/alias.domain
```

例如，如果別名為 `finance.domain.com`，則兩個必要的 SPNs 如下所示。

```
HOST/finance
HOST/finance.domain.com
```

SPN 一次只能與單一 Active Directory 電腦物件建立關聯。如果為原始檔案系統的 Active Directory 電腦物件設定的 DNS 名稱有現有的 SPNs，您必須先刪除它們，才能為 Amazon FSx 檔案系統建立 SPNs。

下列程序說明如何尋找任何現有的 SPNs、刪除它們，以及為 Amazon FSx 檔案系統 Active Directory 電腦物件建立新的 SPNs。

安裝所需的 PowerShell Active Directory 模組

1. 登入已加入您 Amazon FSx 檔案系統所加入之 Active Directory 的 Windows 執行個體。
2. 以管理員身分開啟 PowerShell。
3. 使用以下命令安裝 PowerShell Active Directory 模組。

```
Install-WindowsFeature RSAT-AD-PowerShell
```

在原始檔案系統的 Active Directory 電腦物件上尋找和刪除現有的 DNS 別名 SPNs

1. 使用以下命令尋找任何現有的 SPNs。*alias_fqdn* 將 取代為您在 中與檔案系統相關聯的 DNS 別名將內部部署 DNS 組態遷移至 FSx for Windows File Server。

```
## Find SPNs for original file system's AD computer object
$ALIAS = "alias_fqdn"
SetSPN /Q ("HOST/" + $ALIAS)
SetSPN /Q ("HOST/" + $ALIAS.Split(".")[0])
```

2. 使用下列範例指令碼刪除上一個步驟中傳回的現有 HOST SPNs。

   - *alias_fqdn* 將 取代為您在 中與檔案系統相關聯的完整 DNS 別名將內部部署 DNS 組態遷移至 FSx for Windows File Server。
   - *file_system_DNS_name* 將 取代為原始檔案系統的 DNS 名稱 。

```
## Delete SPNs for original file system's AD computer object
$Alias = "alias_fqdn"
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})

SetSPN /D ("HOST/" + ${Alias}) ${FSxAdComputer}.Name
SetSPN /D ("HOST/" + ${Alias}.Split(".")[0]) ${FSxAdComputer}.Name
```

3. 針對您在 中與檔案系統相關聯的每個 DNS 別名重複這些步驟將內部部署 DNS 組態遷移至 FSx for Windows File Server。

在 Amazon FSx 檔案系統的 Active Directory 電腦物件上設定 SPNs

1. 執行下列命令，為您的 Amazon FSx 檔案系統設定新的 SPNs。

   - *file_system_DNS_name* 將 取代為 Amazon FSx 指派給檔案系統的 DNS 名稱。

     若要在 Amazon FSx 主控台上尋找檔案系統的 DNS 名稱，請選擇檔案系統，然後選擇您的檔案系統。選擇檔案系統詳細資訊頁面的網路與安全窗格。您也可以在 DescribeFileSystems API 操作的回應中取得 DNS 名稱。

   - *alias_fqdn* 將 取代為您在 中與檔案系統相關聯的完整 DNS 別名將內部部署 DNS 組態遷移至 FSx for Windows File Server。

```
## Set SPNs for FSx file system AD computer object
$FSxDnsName = "file_system_DNS_name"
$Alias = "alias_fqdn"
$FileSystemHost = (Resolve-DnsName $FSxDnsName | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity $FileSystemHost)

Set-AdComputer -Identity $FSxAdComputer -Add @{"msDS-
AdditionalDnsHostname"="$Alias"}
SetSpn /S ("HOST/" + $Alias.Split('.')[0]) $FSxAdComputer.Name
SetSpn /S ("HOST/" + $Alias) $FSxAdComputer.Name
```

> **Note**
>
> 如果原始檔案系統的電腦物件的 AD 中存在 DNS 別名的 SPN，則設定 Amazon FSx 檔案系統的 SPN 將會失敗。如需尋找和刪除現有 SPNs的資訊，請參閱 在原始檔案系統的 Active Directory 電腦物件上尋找和刪除現有的 DNS 別名 SPNs 。

2. 使用下列範例指令碼，確認已為 DNS 別名設定新的 SPNs。確保回應包含兩個 HOST SPNs HOST/*alias*和 HOST/*alias_fqdn*。

   file_system_DNS_name 將 取代為 Amazon FSx 指派給檔案系統的 DNS 名稱。若要在 Amazon FSx 主控台上尋找檔案系統的 DNS 名稱，請選擇檔案系統，然後選擇檔案系統詳細資訊頁面上的網路與安全窗格。

   您也可以在 DescribeFileSystems API 操作的回應中取得 DNS 名稱。

```
## Verify SPNs on FSx file system AD computer object
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})
SetSpn /L ${FSxAdComputer}.Name
```

3. 針對您在 中與檔案系統相關聯的每個 DNS 別名重複上述步驟將內部部署 DNS 組態遷移至 FSx for Windows File Server。

> **Note**
>
> 您可以在 Active Directory 中設定下列群組政策物件 (GPOs)，透過使用 DNS 別名連線至檔案系統的用戶端，強制執行傳輸中的 Kerberos 身分驗證和加密：
>
> - 限制 NTLM：將 NTLM 流量傳出至遠端伺服器
> - 限制 NTLM：為 NTLM 身分驗證新增遠端伺服器例外狀況
>
> 如需詳細資訊，請參閱使用群組政策物件 (GPOs) 強制執行 Kerberos 身分驗證演練 5：使用 DNS 別名存取您的檔案系統。

更新 Amazon FSx 檔案系統的 DNS CNAME 記錄

為檔案系統正確設定 SPNs 後，您可以將解析至原始檔案系統的每個 DNS 記錄取代為解析為 Amazon FSx 檔案系統預設 DNS 名稱的 DNS 記錄，以切換到 Amazon FSx。

安裝所需的 PowerShell cmdlet

1. 登入已加入 Active Directory 的 Windows 執行個體，您的 Amazon FSx 檔案系統會以使用者身分加入，該使用者是具有 DNS 管理許可的群組成員（AWS Managed Microsoft Active Directory AWS 中的委派網域名稱系統管理員，以及網域管理員，或您已在自我管理 Active Directory 中委派 DNS 管理許可的其他群組）

   如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的連線至 Windows 執行個體。
2. 以管理員身分開啟 PowerShell。
3. PowerShell DNS 伺服器模組需要執行此程序中的指示。使用以下命令安裝它。

```
Install-WindowsFeature RSAT-DNS-Server
```

更新現有的 DNS CNAME 記錄

1. 下列指令碼會將 的任何現有 DNS CNAME 記錄更新*alias_fqdn*為 Amazon FSx 檔案系統的電腦物件。如果找不到，它會為*alias_fqdn*解析為 Amazon FSx 檔案系統預設 DNS 名稱的 DNS 別名建立新的 DNS CNAME 記錄。

   執行指令碼：

   - *alias_fqdn* 將 取代為您與檔案系統相關聯的 DNS 別名。
   - *file_system_DNS_name* 將 取代為 Amazon FSx 已指派給檔案系統的預設 DNS 名稱。

   ```
   $Alias="alias_fqdn"
   $FSxDnsName="file_system_dns_name"
   $AliasHost=$Alias.Split('.')[0]
   $ZoneName=((Get-WmiObject Win32_ComputerSystem).Domain)
   $DnsServerComputerName = (Resolve-DnsName $ZoneName -Type NS | Where Type -eq 'A' |
    Select -ExpandProperty Name)[0]

   Add-DnsServerResourceRecordCName -Name $AliasHost -ComputerName
    $DnsServerComputerName -HostNameAlias $FSxDnsName -ZoneName $ZoneName
   ```

2. 針對您在 中與檔案系統相關聯的每個 DNS 別名，重複上述步驟將內部部署 DNS 組態遷移至 FSx for Windows File Server。

監控 FSx for Windows File Server 檔案系統

監控是維護 FSx for Windows File Server 和 AWS 解決方案可靠性、可用性和效能的重要部分。您應該從 AWS 解決方案的所有部分收集監控資料，以便在發生故障時更輕鬆地偵錯。不過，在開始監控 FSx for Windows File Server 之前，您應該建立監控計畫，其中包含下列問題的答案：

- 監控目標是什麼？
- 要監控哪些資源？
- 監控這些資源的頻率為何？
- 要使用哪些監控工具？
- 誰將執行監控任務？
- 發生問題時應該通知誰？

如需在 FSx for Windows File Server 中記錄和監控的詳細資訊，請參閱下列主題。

主題

自動和手動監控

AWS 提供各種工具，您可以用來監控 FSx for Windows File Server。您可以設定其中一些工具為您執行監控，而某些工具需要手動介入。建議您盡可能自動化監控任務。

自動化監控工具

您可以使用下列自動化監控工具來監看 FSx for Windows File Server，並在發生錯誤時回報：

- Amazon CloudWatch 警示：監看指定時段內的單一指標，並根據與多個時段內給定之閾值相對的指標值來執行一或多個動作。此動作是傳送到 Amazon Simple Notification Service (Amazon SNS) 主題或 Amazon EC2 Auto Scaling 政策的通知。CloudWatch 警示不會只因處於特定狀態就叫用動作，狀態必須已變更並已維持一段指定的時間。如需詳細資訊，請參閱使用 Amazon CloudWatch 監控。

- Amazon CloudWatch Logs：監控、存放及存取來自 AWS CloudTrail 或其他來源的日誌檔案。如需詳細資訊，請參閱《Amazon CloudWatch Logs 使用者指南》中的什麼是 Amazon CloudWatch Logs？。
- AWS CloudTrail 日誌監控 – 在帳戶之間共用日誌檔案、透過將日誌檔案傳送到 CloudTrail CloudWatch Logs 來即時監控 CloudTrail 日誌檔案、在 Java 中寫入日誌處理應用程式，以及驗證您的日誌檔案在 CloudTrail 交付後並未變更。如需詳細資訊，請參閱《AWS CloudTrail 使用者指南》中的使用 CloudTrail 日誌檔案。

手動監控工具

監控 FSx for Windows File Server 的另一個重要部分是手動監控 Amazon CloudWatch 警示未涵蓋的項目。FSx for Windows File Server、CloudWatch 和其他 AWS 主控台儀表板提供 AWS 環境狀態的 at-a-glance。

Amazon FSx 監控與效能儀表板會顯示：

- 目前警告和 CloudWatch 警示
- 檔案系統活動的摘要
- 檔案系統儲存容量和使用率
- 檔案伺服器和儲存磁碟區效能
- CloudWatch 警示

Amazon CloudWatch 儀表板會顯示：

- 目前警示與狀態
- 警示與資源的圖表
- 服務運作狀態

此外，您可以使用 CloudWatch 執行下列動作：

- 建立自訂儀表板以監控您使用的服務。
- 用於疑難排解問題以及探索驅勢的圖形指標資料。
- 搜尋和瀏覽您的所有 AWS 資源指標。
- 建立與編輯要通知發生問題的警示。

如需 Amazon FSx 監控與效能儀表板的詳細資訊，請參閱 使用檔案系統指標。

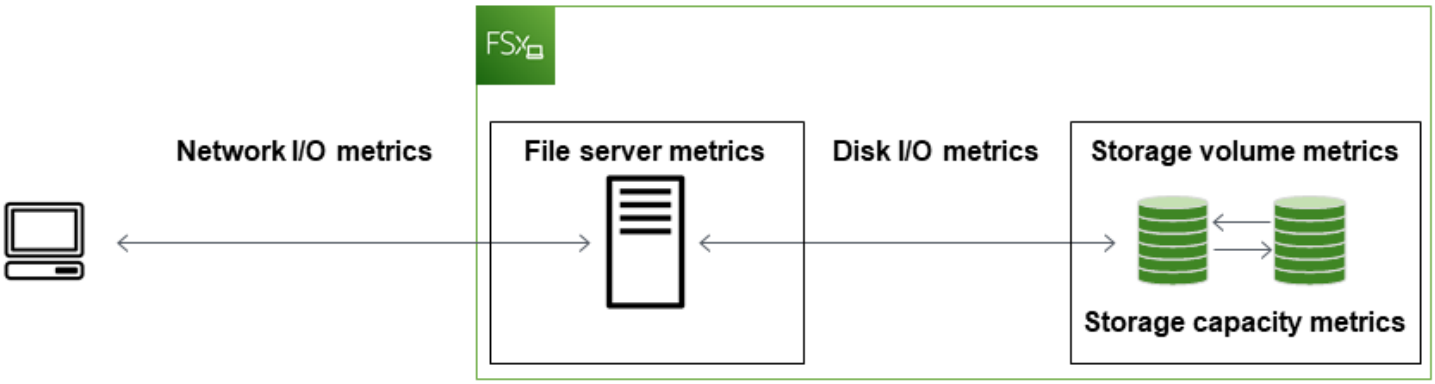
使用 Amazon CloudWatch 監控

Amazon CloudWatch 會從 FSx for Windows File Server 檔案系統收集原始資料，並將其處理為可讀且幾近即時的指標。這些統計資料會保留 15 個月，讓您存取歷史資訊，以協助深入了解工作流程或檔案系統的運作方式。

FSx for Windows File Server 會在下列網域中發佈 CloudWatch 指標：

- 網路 I/O 指標會測量存取檔案系統和檔案伺服器的用戶端之間的活動。
- 檔案伺服器指標會測量網路輸送量使用率、檔案伺服器 CPU 和記憶體，以及檔案伺服器磁碟輸送量和 IOPS 使用率。
- 磁碟 I/O 指標會測量檔案伺服器與儲存磁碟區之間的活動。
- 儲存磁碟區指標會測量 HDD 儲存磁碟區的磁碟輸送量使用率，以及 SSD 儲存磁碟區的 IOPS 使用率。
- 儲存容量指標會測量儲存用量，包括因重複資料刪除而節省的儲存成本。

下圖說明 FSx for Windows File Server 檔案系統、其元件和指標網域。



根據預設，Amazon FSx for Windows File Server 會以 1 分鐘的期間將指標資料傳送至 CloudWatch，但下列例外狀況會以 5 分鐘的間隔發出：

- `FileServerDiskThroughputBalance`
- `FileServerDiskIopsBalance`

如需 CloudWatch 的詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的什麼是 Amazon CloudWatch？。

在檔案系統維護或基礎設施元件取代期間，針對單一可用區檔案系統，以及主要和次要檔案伺服器之間的容錯移轉和容錯回復期間，可能無法發佈指標。

某些 Amazon FSx CloudWatch 指標會報告為原始位元組。位元組不會捨入到單位的十進位或二進位倍數。

主題

CloudWatch 指標和維度

FSx for Windows File Server 會將下列指標發佈到 Amazon CloudWatch 中所有檔案系統的AWS/FSx命名空間：

- DataReadBytes
- DataWriteBytes
- DataReadOperations
- DataWriteOperations
- MetadataOperations
- FreeStorageCapacity

FSx for Windows File Server 會將以下各節中所述的指標發佈到 Amazon CloudWatch 中AWS/FSx命名空間，適用於輸送量容量至少為 32 MBps 的檔案系統。

網路 I/O 指標

AWS/FSx 命名空間包含下列網路 I/O 指標。

指標	描述
DataReadBytes	用戶端存取檔案系統的讀取操作位元組數。

指標	描述
	單位：位元組 有效的統計資訊：Sum
DataWriteBytes	用戶端存取檔案系統的寫入操作位元組數。 單位：位元組 有效的統計資訊：Sum
DataReadOperations	用戶端存取檔案系統的讀取操作數目。 單位：計數 有效的統計資訊：Sum
DataWriteOperations	用戶端存取檔案系統的寫入操作數目。 單位：計數 有效的統計資訊：Sum
MetadataOperations	用戶端存取檔案系統的中繼資料操作數目。 單位：計數 有效的統計資訊：Sum
ClientConnections	用戶端與檔案伺服器之間的作用中連線數目。 單位：計數

檔案伺服器指標

AWS/FSx 命名空間包含下列檔案伺服器指標。

指標	描述
NetworkThroughputUtilization	用戶端存取檔案系統的網路輸送量，以佈建限制的百分比表示。 單位：百分比
CPUUtilization	檔案伺服器的 CPU 資源使用率百分比。 單位：百分比
MemoryUtilization	檔案伺服器的記憶體資源使用率百分比。 單位：百分比
FileServerDiskThroughputUtilization	檔案伺服器與其儲存磁碟區之間的磁碟輸送量，以輸送量容量決定的佈建限制百分比表示。 單位：百分比
FileServerDiskThroughputBalance	檔案伺服器與其儲存磁碟區之間磁碟輸送量的可用爆量額度百分比。適用於佈建輸送量容量為 256 MBps 或以下的檔案系統。 單位：百分比
FileServerDiskIopsUtilization	檔案伺服器和儲存磁碟區之間的磁碟 IOPS，以輸送量容量決定的佈建限制百分比表示。 單位：百分比
FileServerDiskIopsBalance	檔案伺服器及其儲存磁碟區之間磁碟 IOPS 的可用爆量額度百分比。適用於佈建輸送量容量為 256 MBps 或以下的檔案系統。 單位：百分比

磁碟 I/O 指標

AWS/FSx 命名空間包含下列磁碟 I/O 指標。

指標	描述
DiskReadBytes	存取儲存磁碟區的讀取操作的位元組數。 單位：位元組 有效的統計資訊：總和
DiskWriteBytes	存取儲存磁碟區的寫入操作位元組數。 單位：位元組 有效的統計資訊：總和
DiskReadOperations	存取儲存磁碟區之檔案伺服器的讀取操作數目。 單位：計數 有效的統計資訊：Sum
DiskWriteOperations	存取儲存磁碟區之檔案伺服器的寫入操作數目。 單位：計數 有效的統計資訊：Sum

FSx for Windows 儲存磁碟區指標

AWS/FSx 命名空間包含下列儲存磁碟區指標。

指標	描述
DiskThroughputUtilization	（僅限 HDD) 檔案伺服器與其儲存磁碟區之間的磁碟輸送量，以儲存磁碟區決定的佈建限制百分比表示。 單位：百分比
DiskThroughputBalance	（僅限 HDD) 磁碟輸送量的可用爆量額度百分比，以及儲存磁碟區的磁碟 IOPS。

指標	描述
	單位：百分比
DiskIopsUtilization	（僅限 SSD) 檔案伺服器和儲存磁碟區之間的磁碟 IOPS，以儲存磁碟區決定的佈建 IOPS 限制百分比表示。 單位：百分比

儲存容量指標

AWS/FSx 命名空間包含下列儲存容量指標。

指標	描述
FreeStorageCapacity	可用儲存容量的數量。 單位：位元組 有效的統計資訊：Average、Minimum
StorageCapacityUtilization	使用實體儲存容量佔總儲存容量的百分比。 單位：百分比
DeduplicationSavedStorage	如果已啟用重複資料刪除，則由重複資料刪除儲存的儲存空間量。 單位：位元組

FSx for Windows File Server 指標的命名空間和維度

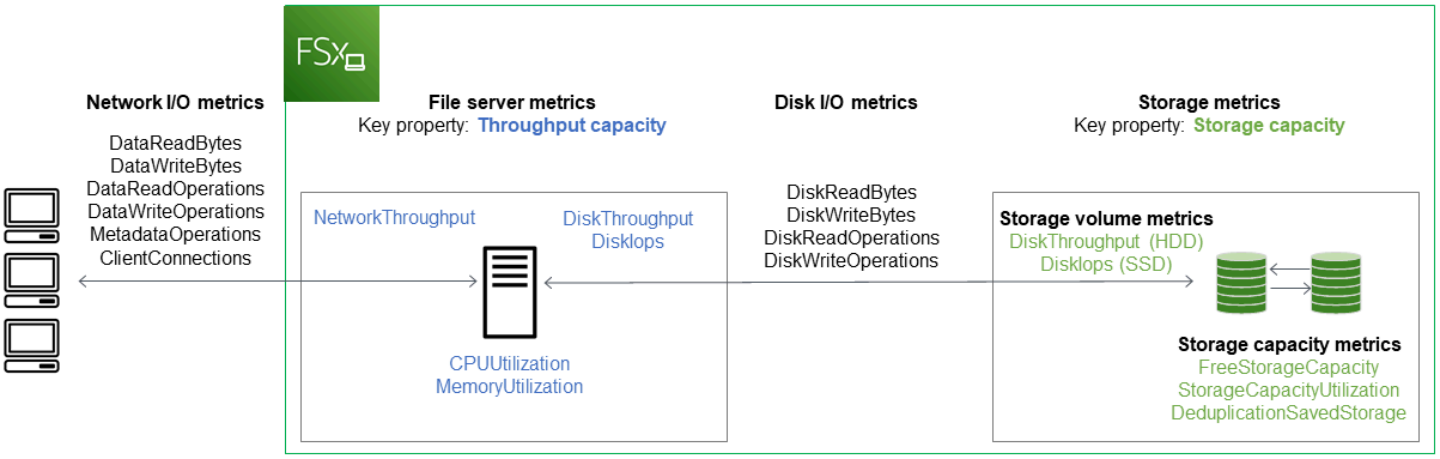
FSx for Windows File Server 指標使用 FSx 命名空間，並提供單一維度 的指標FileSystemId。您可以使用 describe-file-systems AWS CLI 命令或 DescribeFileSystems API 命令來尋找檔案系統的 ID。檔案系統 ID 採用 *fs-0123456789abcdef0* 的形式。

使用檔案系統指標

每個 Amazon FSx 檔案系統有兩個主要架構元件：

- 將資料提供給存取檔案系統之用戶端的檔案伺服器。
- 在您的檔案系統中託管資料的儲存磁碟區。

FSx for Windows File Server 會在 CloudWatch 中報告指標，以追蹤檔案系統檔案伺服器和儲存磁碟區的效能和資源使用率。下圖說明 Amazon FSx 檔案系統及其架構元件，以及可用於監控的效能和資源 CloudWatch 指標。一組指標顯示的金鑰屬性是決定這些指標容量的檔案系統屬性。調整該屬性會修改該組指標的檔案系統效能。



使用 Amazon FSx 主控台中的監控與效能面板，檢視下表所述的 FSx for Windows File Server CloudWatch 指標。

監控與效能面板	如何...	圖表	相關指標
Summary	...決定檔案系統的總 IOPS？	總 IOPS	SUM(DataReadOperations + DataWriteOperations + MetadataOperations)/期間（以秒為單位）
	...決定檔案系統的總輸送量？	總輸送量	SUM(DataReadBytes + DataWriteBytes)/期間（以秒為單位）
	...決定檔案系統上可用的儲存容量？	可用的儲存容量	FreeStorageCapacity

監控與效能面板	如何...	圖表	相關指標
儲存	...決定用戶端和檔案伺服器之間建立的連線數目？	用戶端連線	ClientConnections
	...以檔案系統的總儲存容量百分比來決定使用過的實體磁碟空間數量？	儲存容量使用率	StorageCapacityUtilization
	...決定重複資料刪除所儲存的實體磁碟空間量？	從重複資料刪除儲存的儲存體	DeduplicationSavedStorage
效能 - 檔案伺服器	...以檔案系統佈建輸送量的百分比來決定存取檔案系統的用戶端的網路輸送量？	網路輸送量使用率	NetworkThroughputUtilization [1]
	...以輸送量容量決定的佈建限制百分比來決定檔案伺服器及其儲存磁碟區之間的磁碟輸送量？	磁碟輸送量使用率	FileServerDiskThroughputUtilization [1]
	...決定檔案伺服器及其儲存磁碟區之間磁碟輸送量的可用爆量額度百分比？	磁碟輸送量爆量平衡	FileServerDiskThroughputBalance
	...以輸送量容量決定的佈建限制百分比來決定檔案伺服器和儲存磁碟區之間的磁碟 IOPS 數量？	磁碟 IOPS 使用率	FileServerDiskIopsUtilization
	...決定檔案伺服器和儲存磁碟區之間磁碟 IOPS 的可用爆量額度百分比？	磁碟 IOPS 爆量餘額	FileServerDiskIopsBalance
	...決定檔案伺服器的 CPU 使用率百分比？	CPU 使用率	CPUUtilization
	...決定檔案伺服器的記憶體使用率百分比？	記憶體使用率	MemoryUtilization

監控與效能面板	如何...	圖表	相關指標
效能 – 儲存磁碟區	...以 HDD Storage Capacity 決定的佈建限制百分比來決定存取儲存磁碟區之操作的輸送量？	磁碟輸送量使用率 (HDD)	`DiskThroughputUtilization`
	...決定存取 HDD 儲存磁碟區之操作的可用輸送量和 IOPS 爆量額度百分比？	磁碟輸送量高載平衡 (HDD)	`DiskThroughputBalance` [2]
	...以 HDD Storage Capacity 決定的佈建限制百分比來決定存取儲存磁碟區的操作 IOPS？	磁碟 IOPS 使用率 (HDD)	SUM(`DiskReadOperations` + `DiskWriteOperations`) / `Period`（以秒為單位）/ (12 * 以 TiB 為單位的佈建 HDD 儲存容量)
	...以 SSD Storage Capacity 決定的佈建限制百分比來決定存取儲存磁碟區的操作 IOPS？	磁碟 IOPS 使用率 (SSD)	`DiskIopsUtilization`

Note

[1]我們建議您將平均輸送量容量使用率維持在 50% 以下，以確保您有足夠的備用輸送量容量，可因應工作負載中意外尖峰，以及任何背景 Windows 儲存操作（例如儲存同步、重複資料刪除或陰影複製）。

[2]HDD 儲存磁碟區可能會遇到顯著的效能變化，具體取決於工作負載。IOPS 或輸送量突然峰值可能會導致磁碟效能降低。如需詳細資訊，請參閱HDD 爆量效能。

效能警告和建議

FSx for Windows 會針對輸送量容量至少為 32 MBpss 的檔案系統，提供效能警告。每當其中一個指標接近或超過多個連續資料點的預定閾值時，Amazon FSx 就會顯示一組 CloudWatch 指標的警告。這些警告為您提供可行的建議，您可以用來最佳化檔案系統的效能。

您可以在監控與效能儀表板的數個區域中存取警告。所有作用中或最近的 Amazon FSx 效能警告，以及針對處於 ALARM 狀態的檔案系統所設定的任何 CloudWatch 警示，都會出現在摘要區段的監控與效能面板中。警告也會顯示在顯示指標圖形的儀表板區段中。

您可以為任何 Amazon FSx 指標建立 CloudWatch 警示。如需詳細資訊，請參閱建立 CloudWatch 警示。

使用效能警告來改善檔案系統效能

Amazon FSx 提供可行的建議，您可以用來最佳化檔案系統的效能。這些建議說明如何解決潛在的效能瓶頸。如果您預期活動會繼續，或對檔案系統的效能造成影響，您可以採取建議的動作。根據哪個指標已觸發警告，您可以透過增加檔案系統的輸送量容量或儲存容量來解決它，如下表所述。

如果有此指標的警告	執行此作業
網路輸送量 – 使用率	增加輸送量容量
檔案伺服器 > 磁碟 IOPS – 使用率	
檔案伺服器 > 磁碟輸送量 – 使用率	
檔案伺服器 > 磁碟 IOPS - 爆量餘額	
檔案伺服器 > 磁碟輸送量 – 爆量平衡	
儲存容量使用率	增加儲存容量
儲存磁碟區 > 磁碟輸送量 – 使用率 (HDD)	增加儲存容量或切換至 SDD 儲存類型
儲存磁碟區 > 磁碟輸送量 – 爆量平衡 (HDD)	
儲存磁碟區 > 磁碟 IOPS – 使用率 (SSD)	增加 SSD IOPS

> **Note**
>
> 某些檔案系統事件可能會耗用磁碟 I/O 效能資源，並可能觸發效能警告。例如：
>
> - 儲存容量擴展的最佳化階段可產生增加的磁碟輸送量，如 中所述 儲存容量增加，且檔案系統效能
> - 對於多可用區檔案系統，輸送量容量擴展、硬體取代或可用區域中斷等事件會導致自動容錯移轉和容錯回復事件。在此期間發生的任何資料變更都需要在主要和次要檔案伺服器之間同步，而 Windows Server 會執行可以取用磁碟 I/O 資源的資料同步任務。如需詳細資訊，請參閱管理輸送量容量。

如需檔案系統效能的詳細資訊，請參閱 FSx for Windows File Server 效能。

存取檔案系統指標

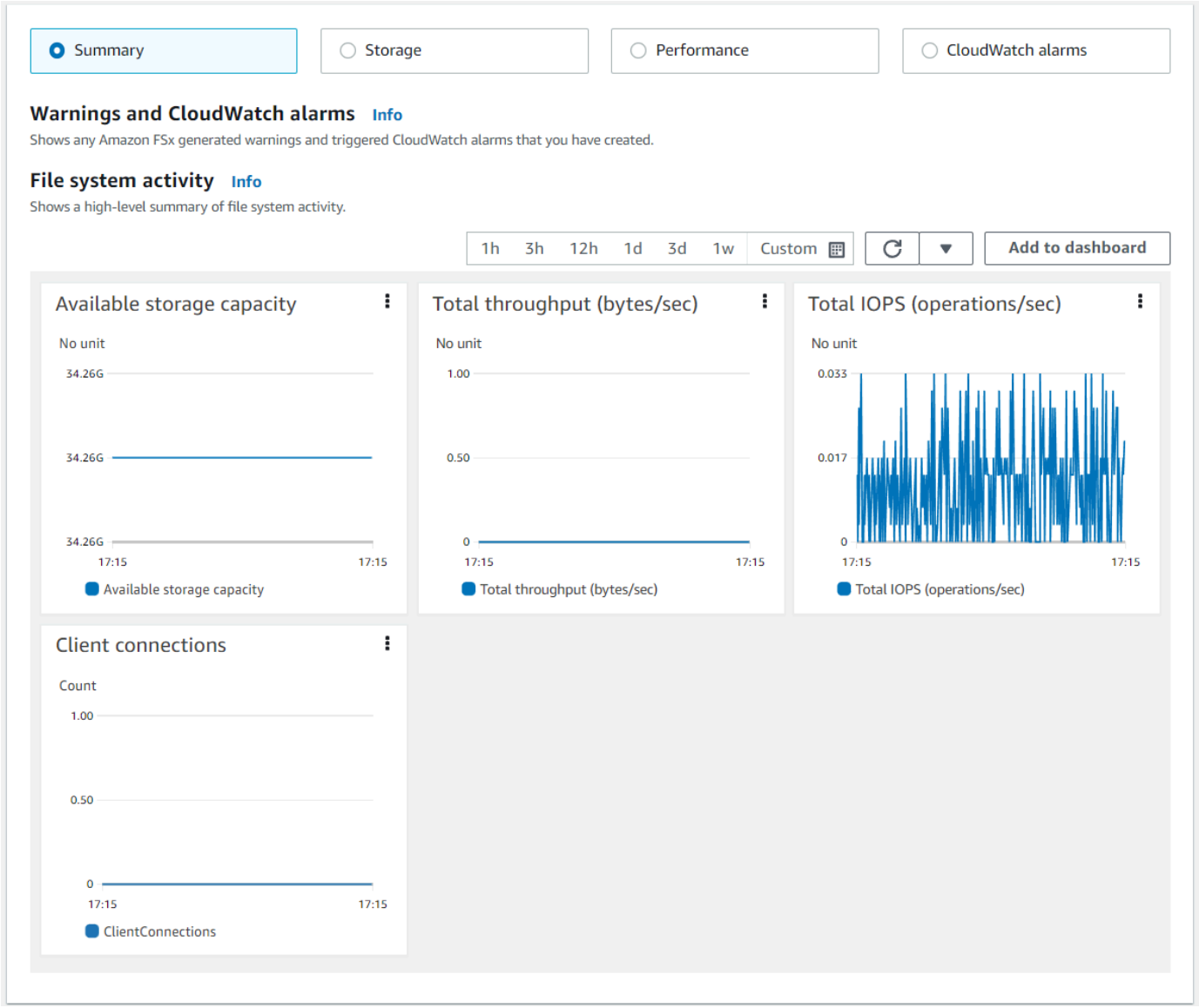
您可以透過下列方式查看 CloudWatch 的 Amazon FSx 指標。

- Amazon FSx 主控台
- CloudWatch 主控台
- CloudWatch CLI
- CloudWatch API

下列程序說明如何使用這些各種工具來存取檔案系統的指標。

使用 Amazon FSx 主控台檢視檔案系統指標

1. 在 Amazon FSx 主控台開啟 https：//https://console.aws.amazon.com/fsx/。
2. 若要顯示檔案系統詳細資訊頁面，請在導覽窗格中選擇檔案系統。
3. 選擇您要檢視其指標的檔案系統。
4. 若要檢視檔案系統指標的圖表，請在第二個面板上選擇監控和效能。

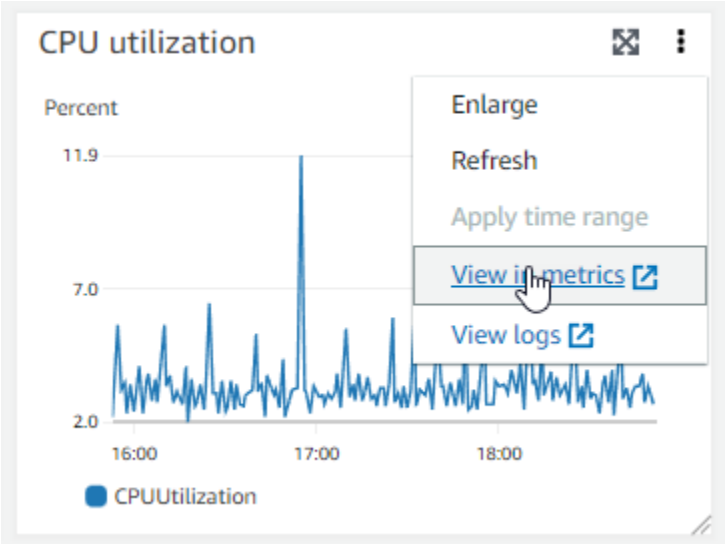


- 預設會顯示摘要指標，顯示任何作用中的警告和 CloudWatch 警示，以及檔案系統活動指標。
- 選擇儲存以檢視儲存容量和使用率指標。
- 選擇效能以檢視檔案伺服器和儲存效能指標
- 選擇 CloudWatch 警示以檢視針對檔案系統設定的任何警示圖形。

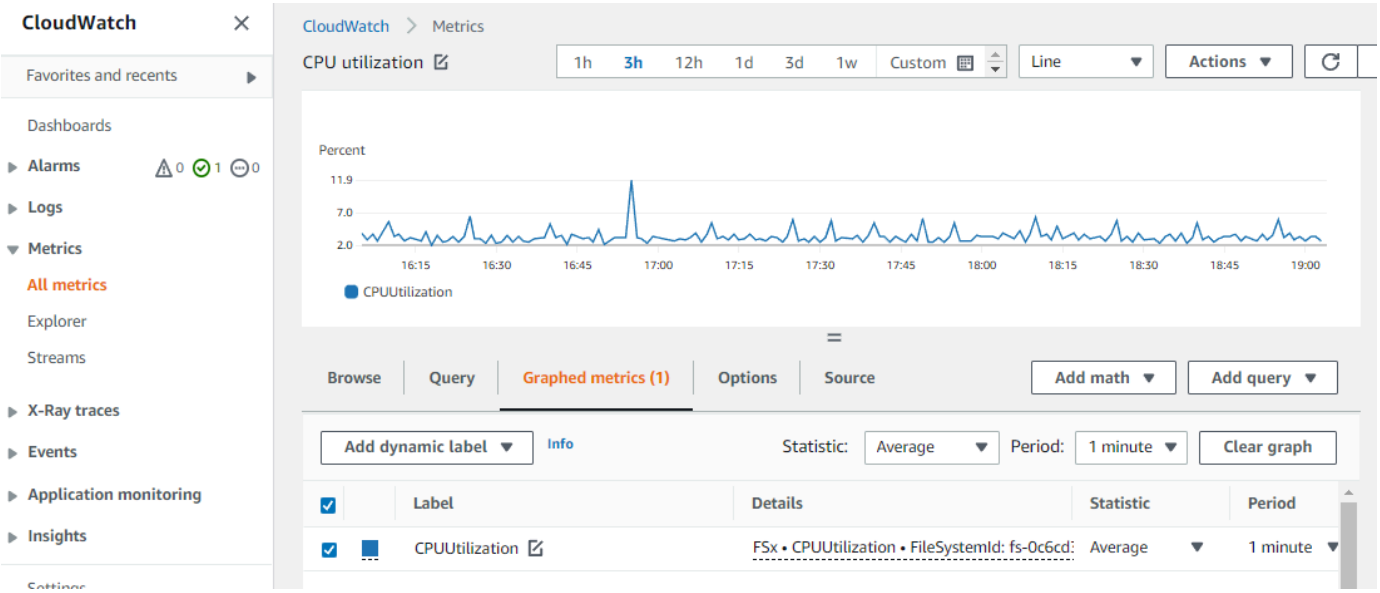
如需詳細資訊，請參閱使用檔案系統指標

若要在 CloudWatch 主控台中檢視指標

1. 若要在 Amazon CloudWatch 主控台的指標頁面中檢視檔案系統指標，請導覽至 Amazon FSx 主控台的監控與效能面板中的指標。
2. 從指標圖表右上角的動作選單中選擇在指標中檢視，如下圖所示。



這會在 CloudWatch 主控台中開啟指標頁面，顯示指標圖表，如下圖所示。



將指標新增至 CloudWatch 儀表板

1. 若要將一組 FSx for Windows 檔案系統指標新增至 CloudWatch 主控台中的儀表板，請在 Amazon FSx 主控台的監控與效能面板中選擇一組指標 (摘要、儲存或效能)。

2. 選擇面板右上角的新增至儀表板，這會開啟 CloudWatch 主控台。
3. 從清單中選擇現有的 CloudWatch 儀表板，或建立新的儀表板。如需詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的使用 Amazon CloudWatch 儀表板。

從 存取指標 AWS CLI

- 使用具有 `--namespace "AWS/FSx"` 命名空間的 `list-metrics` 命令。如需詳細資訊，請參閱《AWS CLI 命令參考》https://docs.aws.amazon.com/cli/latest/reference/。

```
$ aws cloudwatch list-metrics --namespace "AWS/FSx"
aws cloudwatch list-metrics --namespace "AWS/FSx"
{
    "Metrics": [
        {
            "Namespace": "AWS/FSx",
            "MetricName": "DataWriteOperationTime",
            "Dimensions": [
                {
                    "Name": "FileSystemId",
                    "Value": "fs-09a106ebc3a0bb087"
                }
            ]
        },
        {
            "Namespace": "AWS/FSx",
            "MetricName": "CapacityPoolWriteBytes",
            "Dimensions": [
                {
                    "Name": "VolumeId",
                    "Value": "fsvol-0cb2281509f5db3c2"
                },
                {
                    "Name": "FileSystemId",
                    "Value": "fs-09a106ebc3a0bb087"
                }
            ]
        },
        {
            "Namespace": "AWS/FSx",
            "MetricName": "DiskReadBytes",
            "Dimensions": [
                {
```

```
                    "Name": "FileSystemId",
                    "Value": "fs-09a106ebc3a0bb087"
                }
            ]
        },
        {
            "Namespace": "AWS/FSx",
            "MetricName": "CompressionRatio",
            "Dimensions": [
                {
                    "Name": "FileSystemId",
                    "Value": "fs-0f84c9a176a4d7c92"
                }
            ]
        },
.
.
.
}
```

使用 CloudWatch API

使用 CloudWatch API 存取指標

- 呼叫 `GetMetricStatistics`。如需詳細資訊，請參閱 Amazon CloudWatch API 參考。

建立 CloudWatch 警示

您可以建立 CloudWatch 警報，在警示變更狀態時傳送 Amazon SNS 訊息。警示會監看指定時段內的單一指標，並根據與多個時段內指定閾值相對的指標值來執行一或多個動作。此動作是傳送到 Amazon SNS 主題或 Auto Scaling 政策的通知。

警示僅會針對持續狀態變更調用動作。CloudWatch 警示不會只因為處於特定狀態而叫用動作；狀態必須已變更並維持在指定的期間數。您可以從 Amazon FSx 主控台或 CloudWatch 主控台建立警示。

下列程序說明如何使用主控台、 AWS CLI和 API 為 Amazon FSx 建立警示。

設定 CloudWatch 警示（主控台）

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/：//https：//https：//https：//https：///

2. 從導覽窗格中，選擇檔案系統，然後選擇您要為其建立警示的檔案系統。
3. 選擇動作功能表，然後選擇檢視詳細資訊。
4. 在摘要頁面上，選擇監控和效能。
5. 選擇 CloudWatch 警示。
6. 選擇建立 CloudWatch 警示。系統會將您重新導向至 CloudWatch 主控台。
7. 選擇選取指標，然後選擇下一步。
8. 在指標區段中，選擇 FSX。
9. 選擇檔案系統指標，選擇您要設定警示的指標，然後選擇選取指標。
10. 在條件區段中，選擇您想要警示的條件，然後選擇下一步。

> **Note**
>
> 在單一可用區檔案系統的檔案系統維護期間，或容錯移轉和容錯移轉期間，可能無法發佈指標，或從多可用區檔案系統的主要或次要伺服器進行容錯移轉和容錯回復。若要防止不必要的和誤導性的警示條件變更，以及設定警示，使其對遺失的資料點具有彈性，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。Amazon CloudWatch

11. 如果您希望 CloudWatch 在警示狀態觸發動作時傳送電子郵件或 SNS 通知給您，請為每當此警示狀態為 時選擇警示狀態。

    若要選取 SNS 主題，請選擇現有的 SNS 主題。如果您選取建立主題，即可為新電子郵件訂閱清單設定名稱和電子郵件地址。此清單會儲存並顯示在欄位中供未來警示使用。選擇下一步。

> **Note**
>
> 如果您使用建立主題來建立新的 Amazon SNS 主題，電子郵件地址必須先經過驗證才會接收通知。電子郵件只有在警示進入警示狀態時才會傳送。如果此警示狀態在驗證電子郵件地址之前發生變更，就不會收到通知。

12. 填寫指標的名稱、描述和每當值，然後選擇下一步。
13. 在預覽和建立頁面上，檢閱您要建立的警示，然後選擇建立警示。

使用 CloudWatch 主控台設定警示

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 選擇建立警示以啟動建立警示精靈。
3. 選擇 FSx 指標，然後捲動 Amazon FSx 指標，以尋找您要對其發出警示的指標。若要在此對話方塊中僅顯示 Amazon FSx 指標，請搜尋檔案系統的檔案系統 ID。選取要建立警示的指標，然後選擇下一步。
4. 填入指標的 Name (名稱)、Description (說明) 和 Whenever (每當) 值。
5. 如果您希望 CloudWatch 在達到警示狀態時傳送電子郵件給您，請在 Whenever this alarm: (每當此警示：) 中選擇 State is ALARM (狀態為警示)。在 Send notification to: (傳送通知至：) 中，選擇現有 SNS 主題。如果您選取建立主題，即可為新電子郵件訂閱清單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。

   > **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。

6. 此時，警示預覽區域可讓您預覽即將建立的警示。選擇建立警示 。

設定 CloudWatch 警示 (CLI)

- 呼叫 `put-metric-alarm`。如需更多詳細資訊，請參閱 AWS CLI 命令參考。

設定警示 (API)

- 呼叫 `PutMetricAlarm`。如需詳細資訊，請參閱 Amazon CloudWatch API 參考。

使用 記錄 Amazon FSx for Windows File Server API 呼叫 AWS CloudTrail

Amazon FSx for Windows File Server 已與 服務整合 AWS CloudTrail，該服務提供 Amazon FSx AWS 中使用者、角色或服務所採取動作的記錄。CloudTrail 會將 Amazon FSx 的所有 API 呼叫擷取為事件。擷取的呼叫包括從 Amazon FSx 主控台呼叫，以及對 Amazon FSx API 操作的程式碼呼叫。

如果您建立線索，您可以啟用 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 Amazon FSx 的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。使用 CloudTrail 收集的資訊，您可以判斷對 Amazon FSx 提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，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

建立帳戶 AWS 帳戶 時，您的 上會啟用 CloudTrail。當 Amazon FSx 中發生活動時，該活動會記錄於 CloudTrail 事件中，以及事件歷史記錄中的其他服務 AWS 事件。您可以在 中檢視、搜尋和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱「使用 CloudTrail 事件歷史記錄檢視事件」。

若要持續記錄 中的事件 AWS 帳戶，包括 Amazon FSx 的事件，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。追蹤會記錄 AWS 分割區中所有 區域的事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析 CloudTrail 日誌中收集的事件資料並對其採取行動。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 接收多個區域的 CloudTrail 日誌檔案和接收多個帳戶的 CloudTrail 日誌檔案

所有 Amazon FSx 動作都會由 CloudTrail 記錄，並記錄在 Amazon FSx API 參考中。例如，對 `CreateFileSystem`、`CreateBackup` 和 `TagResource` 動作發出的呼叫會在 CloudTrail 記錄檔案中產生專案。

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

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

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

了解 Amazon FSx 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

下列範例顯示的 CloudTrail 日誌項目，示範從主控台建立之檔案系統標籤時的 `TagResource` 操作。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": “111122223333”,
        "arn": "arn:aws:sts::111122223333:root”,
        "accountId": “111122223333”,
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE”,
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T22:36:07Z"
            }
        }
    },
    "eventTime": "2018-11-14T22:36:07Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": “192.0.2.0”,
    "userAgent": “console.amazonaws.com”,
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789”
    },
    "responseElements": null,
    "requestID": “aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51”,
    "eventID": “bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p”,
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": “111122223333”
}
```

下列範例顯示的 CloudTrail 日誌項目，示範從主控台刪除之檔案系統標籤時的 UntagResource 動作。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": "111122223333",
        "arn": "arn:aws:sts::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T23:40:54Z"
            }
        }
    },
    "eventTime": "2018-11-14T23:40:54Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "UntagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789"
    },
    "responseElements": null,
    "requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
    "eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": "111122223333"
}
```

Amazon FSx 的安全性

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

安全性是 AWS 與您之間的共同責任。共同責任模型 將此描述為雲端的安全和雲端內的安全：

- 雲端的安全性 – AWS 負責保護在 Amazon Web Services Cloud 中執行 AWS 服務的基礎設施。AWS 也為您提供可安全使用的服務。在 AWS 合規計畫中，第三方稽核員會定期測試並驗證我們的安全功效。若要了解適用於 Amazon FSx for Windows File Server 的合規計劃，請參閱AWS 合規計劃範圍內的服務。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您了解如何在使用 Amazon FSx for Windows File Server 時套用共同責任模型。下列主題說明如何設定 Amazon FSx for Windows File Server 以符合您的安全與合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 Amazon FSx for Windows File Server 資源。

主題

- Amazon FSx for Windows File Server 中的資料保護
- 使用 Windows ACLs的檔案層級和資料夾層級存取控制
- 使用 Amazon VPC 的檔案系統存取控制
- 使用檔案存取稽核記錄最終使用者存取
- Amazon FSx for Windows File Server 的身分和存取管理
- Amazon FSx for Windows File Server 的合規驗證
- Amazon FSx for Windows File Server 和介面 VPC 端點

Amazon FSx for Windows File Server 中的資料保護

AWS 共同的責任模型適用於 Amazon FSx for Windows File Server 中的資料保護。如此模型所述，AWS 負責保護執行所有 的 全球基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

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

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 CloudTrail 追蹤。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 FSx for Windows File Server 或使用主控台、API AWS CLI或 AWS SDKs的其他 AWS 服務 時。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

FSx for Windows File Server 中的資料加密

Amazon FSx for Windows File Server 支援靜態資料加密和傳輸中資料的加密。建立 Amazon FSx 檔案系統時，會自動啟用靜態資料加密。在支援 SMB 通訊協定 3.0 或更新版本的運算執行個體上映射的檔案共用支援傳輸中的資料加密。當您存取檔案系統時，Amazon FSx 會使用 SMB 加密自動加密傳輸中的資料，而不需要修改應用程式。

使用加密時

如果您的組織需要遵守公司或法規政策，該政策要求對靜態資料和中繼資料進行加密，我們建議您使用傳輸中的資料加密建立掛載檔案系統的加密檔案系統。

如果您的組織受限於需要加密靜態資料和中繼資料的公司或法規政策，您的資料會自動靜態加密。我們也建議您使用傳輸中資料的加密來掛載檔案系統，以啟用傳輸中資料的加密。

靜態資料加密

所有 Amazon FSx 檔案系統都會使用 AWS Key Management Service () 管理的金鑰進行靜態加密 AWS KMS。資料會在寫入檔案系統之前自動加密，並在讀取時自動解密。這些程序由 Amazon FSx 透明處理，因此您不需要修改應用程式。

Amazon FSx 使用業界標準的 AES-256 加密演算法來加密 Amazon FSx 靜態資料和中繼資料。如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的密碼編譯基礎。

> **Note**
>
> AWS 金鑰管理基礎設施使用聯邦資訊處理標準 (FIPS) 140-2 核准的密碼編譯演算法。基礎設施符合國家標準技術研究所 (NIST) 800-57 的建議。

Amazon FSx 如何使用 AWS KMS

Amazon FSx 與 整合 AWS KMS 以進行金鑰管理。Amazon FSx 使用 AWS KMS key 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的 KMS 金鑰 （資料和中繼資料）。您可以啟用、停用或撤銷此 KMS 金鑰的授予。此 KMS 金鑰可以是下列兩種類型之一：

- AWS 受管金鑰 – 這是預設 KMS 金鑰，可免費使用。
- 客戶受管金鑰：這是使用起來最靈活的 KMS 金鑰，因為您可以設定它的金鑰政策和授予多個使用者或服務。如需建立客戶受管金鑰的詳細資訊，請參閱 AWS Key Management Service 《開發人員指南》中的建立金鑰。

如果您使用客戶受管金鑰做為檔案資料加密和解密的 KMS 金鑰，您可以啟用金鑰輪換。啟用金鑰輪換時， AWS KMS 每年會自動輪換金鑰一次。此外，使用客戶受管金鑰，您可以選擇何時停用、重新啟用、刪除或撤銷對 KMS 金鑰的存取權。如需詳細資訊，請參閱《開發人員指南》中的輪換 AWS KMS keys。 AWS Key Management Service

的 Amazon FSx 金鑰政策 AWS KMS

金鑰政策是控制對 KMS 金鑰之存取的主要方式。如需金鑰政策的詳細資訊，請參閱《 開發人員指南》中的在 中使用金鑰政策 AWS KMS。 AWS Key Management Service 下列清單說明 Amazon FSx 支援用於靜態檔案系統加密的所有相關 AWS KMS許可：

- kms:Encrypt：(選用) 將純文字加密為加密文字。此許可會納入預設的金鑰政策中。

- kms:Decrypt：(必要) 對密文進行解密。加密文字為之前已加密的純文字。此許可會納入預設的金鑰政策中。
- kms:ReEncrypt –（選用）使用新的 KMS 金鑰加密伺服器端的資料，而不會公開用戶端資料的純文字。資料會先解密，然後重新加密。此許可會納入預設的金鑰政策中。
- kms:GenerateDataKeyWithoutPlaintext –（必要）傳回以 KMS 金鑰加密的資料加密金鑰。此許可會納入 kms:GenerateDataKey* 下預設的金鑰政策中。
- kms:CreateGrant：(必要) 將授予新增至金鑰，以指定誰可以使用金鑰和使用條件。授予是金鑰政策的備用許可機制。如需授予的詳細資訊，請參閱《 AWS Key Management Service 開發人員指南》中的使用授予。此許可會納入預設的金鑰政策中。
- kms:DescribeKey –（必要）提供指定 KMS 金鑰的詳細資訊。此許可會納入預設的金鑰政策中。
- kms:ListAliases：(選用) 列出帳戶中所有金鑰別名。當您使用 主控台建立加密的檔案系統時，此許可會填入 KMS 金鑰清單。我們建議您使用此許可，以提供最佳使用者體驗。此許可會納入預設的金鑰政策中。

加密傳輸中的資料

在支援 SMB 通訊協定 3.0 或更新版本的運算執行個體上映射的檔案共用支援傳輸中的資料加密。這包括從 Windows Server 2012 和 Windows 8 開始的所有 Windows 版本，以及具有 Samba 用戶端 4.2 版或更新版本的所有 Linux 用戶端。當您存取檔案系統時，Amazon FSx for Windows File Server 會使用 SMB 加密自動加密傳輸中的資料，而不需要修改應用程式。

SMB 加密使用 AES-128-GCM 或 AES-128-CCM （如果用戶端支援 SMB 3.1.1，則會選擇 GCM 變體）做為其加密演算法，並使用 SMB Kerberos 工作階段金鑰提供簽署資料完整性。使用 AES-128-GCM 可提升效能，例如，透過加密 SMB 連線複製大型檔案時，效能提升高達 2 倍。

若要符合一律加密data-in-transit合規要求，您可以將檔案系統存取限制為僅允許支援 SMB 加密的用戶端存取。您也可以啟用或停用每個檔案共享或整個檔案系統的傳輸中加密。這可讓您在相同的檔案系統上混合加密和未加密的檔案共用。

管理傳輸中的加密

您可以使用一組自訂 PowerShell 命令來控制 FSx for Windows File Server 檔案系統和用戶端之間傳輸中的資料的加密。您可以將檔案系統存取限制為僅支援 SMB 加密的用戶端，以便一律加密data-in-transit。啟用data-in-transit加密強制執行時，從不支援 SMB 3.0 加密的用戶端存取檔案系統的使用者將無法存取已開啟加密的檔案共用。

您也可以控制檔案共用層級上的data-in-transit加密，而非檔案伺服器層級。如果您想要針對具有敏感資料的某些檔案共享強制執行傳輸中加密，並允許所有使用者存取其他檔案共享，您可以使用檔案共享層級加密控制，在同一檔案系統上混合加密和未加密的檔案共享。全伺服器加密的優先順序高於共用層級加密。如果啟用全域加密，則您無法選擇性地停用特定共用的加密。

您可以使用 Amazon FSx CLI 在 PowerShell 上進行遠端管理，在檔案系統上管理傳輸中加密。若要了解如何使用此 CLI，請參閱 使用 Amazon FSx CLI for PowerShell。

以下是您可以用來管理檔案系統上使用者傳輸中加密的命令。

傳輸中加密命令	描述
Get-FSxSmbServerConfiguration	擷取伺服器訊息區塊 (SMB) 伺服器組態。在系統回應中，您可以根據 `EncryptData` 和 `RejectUnencryptedAccess` 屬性的值，判斷檔案系統的傳輸中加密設定。
Set-FSxSmbServerConfiguration	此命令有兩個選項可在檔案系統上全域設定傳輸中加密： • `-EncryptData $True\|$False` – 將此參數設為 `True`以開啟傳輸中資料加密。將此參數設為 `False`以關閉傳輸中資料加密。 • `-RejectUnencryptedAccess $True\|$False` – 將此參數設定為 `True`，以不允許不支援加密的用戶端存取檔案系統。將此參數設定為 `False`，以允許不支援加密的用戶端存取檔案系統。
Set-FSxSmbShare -name ***name*** -EncryptData $True	將此參數設為 `True`以開啟共享的傳輸中資料加密。將此參數設為 `False` 以關閉共享的傳輸中資料加密。

每個命令的線上說明提供所有命令選項的參考。若要存取此說明，請使用 執行 命令-?，例如 Get-FSxSmbServerConfiguration -?。

使用 Windows ACLs的檔案層級和資料夾層級存取控制

Amazon FSx for Windows File Server 透過 Microsoft Active Directory 透過伺服器訊息區塊 (SMB) 通訊協定支援身分型身分驗證。Active Directory 是 Microsoft 目錄服務，可儲存網路上物件的相關資訊，並讓管理員和使用者輕鬆尋找和使用此資訊。這些物件通常包含共用資源，例如檔案伺服器，以及網路

使用者和電腦帳戶。若要進一步了解 Amazon FSx 中的 Active Directory 支援，請參閱 使用 Microsoft Active Directory。

加入網域的運算執行個體可以使用 Active Directory 憑證存取 Amazon FSx 檔案共享。您可以使用標準 Windows 存取控制清單 (ACLs) 進行精細定義的檔案層級和資料夾層級存取控制。Amazon FSx 檔案系統會自動驗證存取檔案系統資料的使用者憑證，以強制執行這些 Windows ACLs。

每個 Amazon FSx 檔案系統都隨附名為 的預設 Windows 檔案共用`share`。此共用資料夾ACLs 設定為允許網域使用者的讀取/寫入存取。它們還允許對 Active Directory 中的委派管理員群組進行完全控制，該群組被委派在您的檔案系統上執行管理動作。如果您要整合檔案系統與 AWS Managed Microsoft AD，則此群組是 AWS 委派的 FSx 管理員。如果您要將檔案系統與自我管理的 Microsoft AD 設定整合，則此群組可以是網域管理員。或者，它可以是您在建立檔案系統時指定的自訂委派管理員群組。若要變更 ACLs，您可以將共用對應為委派管理員群組的成員。

> **Warning**
>
> Amazon FSx 要求 SYSTEM 使用者對檔案系統中的所有資料夾具有完全控制 NTFS ACL 許可。請勿在您的資料夾上變更此使用者的 NTFS ACL 許可。這樣做會使您的檔案共享無法存取，並防止檔案系統備份可供使用。

相關連結

- 《 AWS Directory Service 管理指南》中的什麼是 AWS Directory Service？。
- 《 AWS 管理指南》中的建立 Managed Microsoft AD 目錄。 AWS Directory Service
- 《 AWS Directory Service 管理指南》中的建立信任關係的時機。
- 步驟 1. 設定 Active Directory.

使用 Amazon VPC 的檔案系統存取控制

您可以透過彈性網路界面存取 Amazon FSx 檔案系統。此網路介面根據您與檔案系統建立關聯的 Amazon Virtual Private Cloud (Amazon VPC) 服務，位於虛擬私有雲端 (VPC) 中。您可以透過網域名稱服務 (DNS) 名稱連線至 Amazon FSx 檔案系統。DNS 名稱會映射至 VPC 中檔案系統彈性網路界面的私有 IP 地址。只有關聯 VPC 內的資源、透過 Direct Connect 或 VPN 與關聯 VPC 連線的資源，或對等 VPCs內的資源，才能存取檔案系統的網路界面。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的什麼是 Amazon VPC？。

> **Warning**
>
> 您不得修改或刪除與檔案系統相關聯的彈性網路界面 ()。修改或刪除網路界面可能會導致 VPC 和檔案系統之間的連線永久中斷。

FSx for Windows File Server 支援 VPC 共用，可讓您檢視、建立、修改和刪除另一個 AWS 帳戶所擁有之 VPC 中共用子網路中的資源。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 使用共享 VPC。

Amazon VPC 安全群組

若要進一步控制透過 VPC 內檔案系統彈性網路界面的網路流量，請使用安全群組來限制對檔案系統的存取。安全群組是一種具狀態防火牆，可控制進出其相關聯網路介面的流量。在此情況下，相關聯的資源是您檔案系統的網路介面 ()。

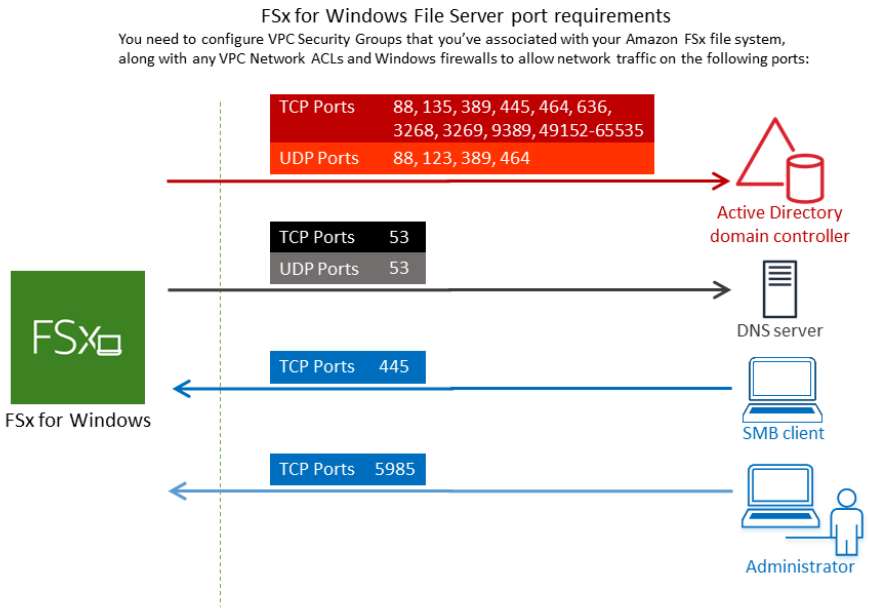
若要使用安全群組來控制對 Amazon FSx 檔案系統的存取，請新增傳入和傳出規則。傳入規則控制傳入流量，傳出規則控制來自檔案系統的傳出流量。請確定您的安全群組中有正確的網路流量規則，將 Amazon FSx 檔案系統的檔案共用映射至支援的運算執行個體上的資料夾。

如需安全群組規則的詳細資訊，請參閱《Amazon EC2 使用者指南》中的安全群組規則。 Amazon EC2

建立 Amazon FSx 的安全群組

1. 開啟位於 https：//https://console.aws.amazon.com/ec2 的 Amazon EC2 主控台。
2. 在導覽窗格中，選擇 Security Groups (安全群組)。
3. 選擇 Create Security Group (建立安全群組)。
4. 指定安全群組的名稱和描述。
5. 針對 VPC，選擇與檔案系統相關聯的 Amazon VPC，在該 VPC 內建立安全群組。
6. 新增下列規則，以允許下列連接埠上的傳出網路流量：

   a. 對於 VPC 安全群組，預設 Amazon VPC 的預設安全群組已新增至主控台中的檔案系統。請確定您建立 FSx 檔案系統之子網路的安全群組和 VPC 網路 ACLs （如下圖所示） 允許連接埠上的流量。



下表識別每個連接埠的角色。

通訊協定	連接埠	Role
TCP/UDP	53	網域名稱系統 (DNS)
TCP/UDP	88	Kerberos 身分驗證
TCP/UDP	464	變更/設定密碼
TCP/UDP	389	輕量型目錄存取通訊協定 (LDAP)
UDP	123	網路時間通訊協定 (NTP)
TCP	135	分散式運算環境/端點映射器 (DCE/EPMAP)
TCP	445	目錄服務 SMB 檔案共用
TCP	636	透過 TLS/SSL 的輕量型目錄存取通訊協定 (LDAPS)
TCP	3268	Microsoft Global Catalog

通訊協定	連接埠	Role
TCP	3269	透過 SSL 的 Microsoft Global Catalog
TCP	5985	WinRM 2.0 (Microsoft Windows 遠端管理)
TCP	9389	Microsoft AD DS Web Services、PowerShell
TCP	49152 - 65535	適用於 RPC 的暫時性連接埠

> **Important**
>
> 單一可用區 2 和所有多可用區檔案系統部署需要允許 TCP 連接埠 9389 上的傳出流量。

b. 請確定這些流量規則也會鏡像至套用至每個 AD 網域控制站、DNS 伺服器、FSx 用戶端和 FSx 管理員的防火牆。

> **Important**
>
> 雖然 Amazon VPC 安全群組要求僅在啟動網路流量的方向上開啟連接埠，但大多數 Windows 防火牆和 VPC 網路 ACLs 要求雙向開啟連接埠。

> **Note**
>
> 如果您已定義 Active Directory 網站，您必須確定與 Amazon FSx 檔案系統相關聯的 VPC 中的子網路是在 Active Directory 網站中定義，而且 VPC 中的子網路和其他站台中的子網路之間不存在衝突。您可以使用 Active Directory 網站和服務 MMC 嵌入來檢視和變更這些設定。

> **Note**
>
> 在某些情況下，您可能已從預設設定修改安全 AWS Managed Microsoft AD 群組的規則。如果是這樣，請確定此安全群組具有必要的傳入規則，以允許來自 Amazon FSx 檔案系統

的流量。如需所需傳入規則的詳細資訊，請參閱《 AWS Directory Service 管理指南》中的AWS Managed Microsoft AD 先決條件。

現在您已建立安全群組 (Amazon FSx 檔案系統的彈性網路界面）。

將安全群組與您的 Amazon FSx 檔案系統建立關聯

1. 開啟位於 https：//https://console.aws.amazon.com/fsx/ 的 Amazon FSx 主控台。
2. 在儀表板上，選擇您的檔案系統以檢視其詳細資訊。
3. 選擇網路與安全索引標籤，然後選擇檔案系統的網路界面（例如 ENI-01234567890123456)。對於單一可用區檔案系統，您會看到單一網路界面。對於多可用區域檔案系統，您會在偏好的子網路中看到一個網路界面，並在待命子網路中看到一個。
4. 針對每個網路界面，選擇網路界面，然後在動作中選擇變更安全群組。
5. 在變更安全群組對話方塊中，選擇要使用的安全群組，然後選擇儲存。

不允許存取檔案系統

若要暫時禁止從所有用戶端存取檔案系統，您可以移除與檔案系統彈性網路界面相關聯的所有安全群組，並將其取代為沒有傳入/傳出規則的群組。

Amazon VPC 網路 ACLs

保護 VPC 內檔案系統存取權的另一個選項是建立網路存取控制清單（網路 ACLs)。網路 ACLs 與安全群組不同，但具有類似的功能，可為 VPC 中的資源新增額外的安全層。如需網路 ACLs 的詳細資訊，請參閱《Amazon VPC 使用者指南》中的網路 ACLs。

使用檔案存取稽核記錄最終使用者存取

Amazon FSx for Windows File Server 支援稽核最終使用者對檔案、資料夾和檔案共享的存取權。您可以選擇將檔案系統的稽核事件日誌傳送至提供一組豐富功能的 AWS 其他服務。這包括啟用查詢、處理、儲存和封存日誌、發出通知和觸發動作，以進一步提升您的安全和合規目標。

如需使用檔案存取稽核來深入了解存取模式並實作最終使用者活動的安全性通知的詳細資訊，請參閱檔案儲存存取模式洞察和實作最終使用者活動的安全性通知。

> **Note**
>
> 只有輸送量容量為 32 MBps 或更高的 FSx for Windows 檔案系統才支援檔案存取稽核。您可以修改現有檔案系統的輸送量容量。如需詳細資訊，請參閱管理輸送量容量。

檔案存取稽核可讓您根據您定義的稽核控制項，記錄個別檔案、資料夾和檔案共用的最終使用者存取。稽核控制項也稱為 NTFS 系統存取控制清單 SACLs)。如果您已在現有檔案資料上設定稽核控制項，您可以透過建立新的 Amazon FSx for Windows File Server 檔案系統並遷移資料來利用檔案存取稽核。

Amazon FSx 支援下列檔案、資料夾和檔案共享存取的 Windows 稽核事件：

- 對於檔案存取，它支援：全部、周遊資料夾/執行檔案、列出資料夾/讀取資料、讀取屬性、建立檔案/寫入資料、建立資料夾/附加資料、寫入屬性、刪除子資料夾和檔案、刪除、讀取許可、變更許可和取得所有權。
- 對於檔案共享存取，它支援：連線至檔案共享。

在檔案、資料夾和檔案共享存取中，Amazon FSx 支援記錄成功的嘗試（例如具有足夠許可的使用者成功存取檔案或檔案共享）、失敗的嘗試或兩者。

您可以設定是否只對檔案和資料夾、僅對檔案共用或兩者進行存取稽核。您也可以設定應記錄的存取類型（僅成功嘗試、僅失敗嘗試，或兩者）。您也可以隨時關閉檔案存取稽核。

> **Note**
>
> 檔案存取稽核只會記錄啟用後的最終使用者存取資料。也就是說，檔案存取稽核不會產生在啟用檔案存取稽核之前所發生之最終使用者檔案、資料夾和檔案共用存取活動的稽核事件日誌。

支援的存取稽核事件速率上限為每秒 5，000 個事件。存取稽核事件不是針對每個檔案讀取和寫入操作產生，而是針對每個檔案中繼資料操作產生一次，例如當使用者建立、開啟或刪除檔案時。

主題

- 稽核事件日誌目的地
- 遷移您的稽核控制項
- 檢視事件日誌
- 設定檔案和資料夾稽核控制項

- 管理檔案存取稽核

稽核事件日誌目的地

啟用檔案存取稽核時，您必須設定 Amazon FSx 傳送稽核事件日誌 AWS 的服務。您可以將稽核事件日誌傳送至 Amazon CloudWatch Logs 日誌群組中的 Amazon CloudWatch Logs 日誌串流或 Amazon Data Firehose 交付串流。您可以在建立 Amazon FSx for Windows File Server 檔案系統時，或更新現有檔案系統之後的任何時間，選擇稽核事件日誌目的地。如需詳細資訊，請參閱管理檔案存取稽核。

以下是一些建議，可協助您決定要選擇哪些稽核事件日誌目的地：

- 如果您想要在 Amazon CloudWatch 主控台中存放、檢視和搜尋稽核事件日誌、使用 CloudWatch Logs Insights 在日誌上執行查詢，以及觸發 CloudWatch 警示或 Lambda 函數，請選擇 CloudWatch Logs。
- 如果您想要持續將事件串流到 Amazon S3 中的儲存體、Amazon Redshift 中的資料庫、Amazon OpenSearch Service 或 Splunk 或 Datadog 等 AWS 合作夥伴解決方案以進行進一步分析，請選擇 Amazon Data Firehose。

根據預設，Amazon FSx 會在您的帳戶中建立並使用預設 CloudWatch Logs 日誌群組做為稽核事件日誌目的地。如果您想要使用自訂 CloudWatch Logs 日誌群組，或使用 Firehose 做為稽核事件日誌目的地，以下是稽核事件日誌目的地的名稱和位置需求：

- CloudWatch Logs 日誌群組的名稱必須以 `/aws/fsx/`字首開頭。如果您在主控台上建立或更新檔案系統時沒有現有的 CloudWatch Logs 日誌群組，Amazon FSx 可以在 CloudWatch Logs `/aws/fsx/windows`日誌群組中建立和使用預設日誌串流。如果您不想使用預設日誌群組，組態 UI 可讓您在主控台上建立或更新檔案系統時建立 CloudWatch Logs 日誌群組。
- Firehose 交付串流的名稱必須以 `aws-fsx-`字首開頭。如果您沒有現有的 Firehose 交付串流，您可以在 主控台建立或更新檔案系統時建立一個。
- Firehose 交付串流必須設定為使用 `Direct PUT`做為其來源。您無法使用現有的 Kinesis 資料串流做為交付串流的資料來源。
- 目的地 (CloudWatch Logs 日誌群組或 Firehose 交付串流） 必須與 Amazon FSx 檔案系統 AWS 區域 AWS 帳戶 位於相同的 AWS 分割區中。

您可以隨時變更稽核事件日誌目的地 （ 例如，從 CloudWatch Logs 變更為 Firehose)。當您這樣做時，新的稽核事件日誌只會傳送至新的目的地。

盡最大努力稽核事件日誌交付

一般而言，稽核事件日誌記錄會在幾分鐘內交付至目的地，但有時可能需要更長的時間。在極少數情況下，可能會遺漏稽核事件日誌記錄。如果您的使用案例需要特定的語意（例如，確保不會遺漏任何稽核事件），我們建議您在設計工作流程時考慮遺漏的事件。您可以掃描檔案系統上的檔案和資料夾結構，以稽核遺漏的事件。

遷移您的稽核控制項

如果您已在現有檔案資料上設定稽核控制 SACLs)，您可以建立 Amazon FSx 檔案系統，並將資料遷移至新的檔案系統。建議使用 AWS DataSync 將資料和相關聯的 SACLs 傳輸到您的 Amazon FSx 檔案系統。做為替代解決方案，您可以使用 Robocopy（強大的檔案複製）。如需詳細資訊，請參閱將現有的檔案儲存遷移至 Amazon FSx。

檢視事件日誌

您可以在 Amazon FSx 開始發出稽核事件日誌之後檢視它們。檢視日誌的位置和方式取決於稽核事件日誌目的地：

- 您可以前往 CloudWatch 主控台並選擇稽核事件日誌要傳送到的日誌群組和日誌串流，以檢視 CloudWatch Logs 日誌。如需詳細資訊，請參閱《Amazon CloudWatch Logs 使用者指南》中的檢視傳送至 CloudWatch Logs 的日誌資料。 Amazon CloudWatch

  您可以使用 CloudWatch Logs Insights 以互動方式搜尋和分析日誌資料。如需詳細資訊，請參閱《Amazon CloudWatch Logs 使用者指南》中的使用 CloudWatch Logs Insights 分析日誌資料。 Amazon CloudWatch

  您也可以將稽核事件日誌匯出至 Amazon S3。如需詳細資訊，請參閱《Amazon CloudWatch Logs 使用者指南》中的將日誌資料匯出至 Amazon S3。 Amazon CloudWatch
- 您無法在 Firehose 上檢視稽核事件日誌。不過，您可以設定 Firehose 將日誌轉送到您可以從中讀取的目的地。目的地包括 Amazon S3、Amazon Redshift、Amazon OpenSearch Service 和 Splunk 和 Datadog 等合作夥伴解決方案，如需詳細資訊，請參閱《Amazon Data Firehose 開發人員指南》中的選擇目的地。

稽核事件欄位

本節說明稽核事件日誌中的資訊，以及稽核事件的範例。

以下是 Windows 稽核事件中 salient 欄位的描述。

- EventID 是指 Microsoft 定義的 Windows 事件日誌事件 ID。如需檔案系統事件和檔案共用事件的資訊，請參閱 Microsoft 文件。
- SubjectUserName 是指執行存取的使用者。
- ObjectName 是指存取的目標檔案、資料夾或檔案共享。
- ShareName 適用於為檔案共享存取而產生的事件。例如， `EventID 5140` 會在存取網路共用物件時產生。
- IpAddress 是指啟動檔案共享事件的用戶端。
- 關鍵字可用時，請參閱檔案存取是否成功或失敗。對於成功存取，值為 `0x8020000000000000`。對於失敗的存取，值為 `0x8010000000000000`。
- TimeCreated SystemTime 是指事件在系統中產生並以 <YYYY-MM-DDThh：mm：ss.s>Z 格式顯示的時間。
- 電腦是指檔案系統的 DNS 名稱 Windows Remote PowerShell 端點，可用於識別檔案系統。
- AccessMask 可用時，是指所執行的檔案存取類型 （例如 ReadData、WriteData)。
- AccessList 是指請求或授予物件的存取權。如需詳細資訊，請參閱下表和 Microsoft 文件 （例如 Event 4556)。

存取類型	存取遮罩	Value
讀取資料或清單目錄	0x1	%%4416
寫入資料或新增檔案	0x2	%%4417
附加資料或新增子目錄	0x4	%%4418
讀取延伸屬性	0x8	%%4419
寫入延伸屬性	0x10	%%4420
執行/周遊	0x20	%%4421
刪除子項	0x40	%%4422
讀取屬性	0x80	%%4423
寫入屬性	0x100	%%4424

存取類型	存取遮罩	Value
刪除	0x10000	%%1537
讀取 ACL	0x20000	%%1538
寫入 ACL	0x40000	%%1539
寫入擁有者	0x80000	%%1540
同步	0x100000	%%1541
存取安全 ACL	0x1000000	%%1542

以下是一些具有範例的關鍵事件。請注意，XML 已格式化以供讀取。

刪除物件時，會記錄事件 ID 4660。

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4660</EventID><Version>0</Version><Level>0</Level>
<Task>12800</Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-05-18T04:51:56.916563800Z'/>
<EventRecordID>315452</EventRecordID><Correlation/>
<Execution ProcessID='4' ThreadID='5636'/><Channel>Security</Channel>
<Computer>amznfsxgyzohmw8.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x50932f71</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='HandleId'>0x12e0</Data><Data Name='ProcessId'>0x4</Data><Data
 Name='ProcessName'></Data>
<Data Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data></EventData></
Event>
```

事件 ID 4659 會記錄在刪除檔案的請求上。

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
```

```
<EventID>4659</EventID><Version>0</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-0603T19:18:09.951551200Z'/>
<EventRecordID>308888</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='5540'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device\HarddiskVolume8\shar
\event.txt</Data>
<Data Name='HandleId'>0x0</Data><Data
 Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data>
<Data Name='AccessList'>%%1537
    %%4423
    </Data><Data Name='AccessMask'>0x10080</Data><Data Name='PrivilegeList'>-</Data>
<Data Name='ProcessId'>0x4</Data></EventData></Event>
```

在物件上執行特定操作時，會記錄事件 ID 4663。下列範例顯示從 檔案讀取資料，可從 解譯AccessList %%4416。

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4663< /EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:10:13.887145400Z'/>
<EventRecordID>308831</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='6916'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData>< Data
 Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113< /Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\event.txt</Data>
<Data Name='HandleId'>0x101c</Data><Data Name='AccessList'>%%4416
    </Data>
```

```
<Data Name='AccessMask'>0x1</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data><Data Name='ResourceAttributes'>S:AI</Data>
</EventData></Event>
```

下列範例顯示來自 檔案的寫入/附加資料，可從 解譯AccessList %%4417。

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4663</EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:12:16.813827100Z'/>
<EventRecordID>308838</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='5828'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\event.txt</Data>
<Data Name='HandleId'>0xa38</Data><Data Name='AccessList'>%%4417
    </Data><Data Name='AccessMask'>0x2</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data><Data Name='ResourceAttributes'>S:AI</Data></
EventData></Event>
```

事件 ID 4656 表示已請求物件的特定存取。在下列範例中，讀取請求已啟動至 ObjectName "permtest"，且嘗試失敗，如 的關鍵字值所示0x8010000000000000。

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4656</EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8010000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:22:55.113783500Z'/>
<EventRecordID>308919</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='4924'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
```

```
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\permtest</Data>
<Data Name='HandleId'>0x0</Data><Data
 Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data>
<Data Name='AccessList'>%%1541
    %%4416
    %%4423
    </Data><Data Name='AccessReason'>%%1541: %%1805
    %%4416: %%1805
    %%4423: %%1811 D:(A;OICI;0x1301bf;;;AU)
    </Data><Data Name='AccessMask'>0x100081</Data><Data Name='PrivilegeList'>-</Data>
<Data Name='RestrictedSidCount'>0</Data><Data Name='ProcessId'>0x4</Data><Data
 Name='ProcessName'></Data>
<Data Name='ResourceAttributes'>-</Data></EventData></Event>
```

變更物件的許可時，會記錄事件 ID 4670。下列範例顯示使用者 "admin" 修改 ObjectName "permtest" 的許可，將許可新增至 SID "S-1-5-21-658495921-4185342820-3824891517-1113"。如需如何解譯許可的詳細資訊，請參閱 Microsoft 文件。

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4670</EventID><Version>0</Version><Level>0</Level>
<Task>13570</Task><Opcode>0</Opcode><Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime='2021-06-03T19:39:47.537129500Z'/><EventRecordID>308992</
EventRecordID>
<Correlation/><Execution ProcessID='4' ThreadID='2776'/><Channel>Security</Channel>
<Computer>amznfsxgyzohmw8.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\permtest</Data>
<Data Name='HandleId'>0xcc8</Data>
<Data Name='OldSd'>D:PAI(A;OICI;FA;;;SY)
(A;OICI;FA;;;S-1-5-21-658495921-4185342820-3824891517-2622)</Data>
<Data Name='NewSd'>D:PARAI(A;OICI;FA;;;S-1-5-21-658495921-4185342820-3824891517-1113)
(A;OICI;FA;;;SY)(A;OICI;FA;;;
S-1-5-21-658495921-4185342820-3824891517-2622)</Data><Data Name='ProcessId'>0x4</Data>
```

```
<Data Name='ProcessName'></Data></EventData></Event>
```

每次存取檔案共享時都會記錄事件 ID 5140。

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>5140</EventID><Version>1</Version><Level>0</Level><Task>12808</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:32:07.535208200Z'/>
<EventRecordID>308947</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='3120'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-2620</
Data>
<Data Name='SubjectUserName'>EC2AMAZ-1GP4HMN$</Data><Data
 Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2d4ca529</Data><Data Name='ObjectType'>File</Data><Data
 Name='IpAddress'>172.45.6.789</Data>
<Data Name='IpPort'>49730</Data><Data Name='ShareName'>\\AMZNFSXCYDKLDZZ\share</Data>
<Data Name='ShareLocalPath'>\??\D:\share</Data><Data Name='AccessMask'>0x1</Data><Data
 Name='AccessList'>%%4416
    </Data></EventData></Event>
```

在檔案共享層級拒絕存取時，會記錄事件 ID 5145。下列範例顯示對 ShareName "demoshare01" 的存取遭拒。

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>5145</EventID><Version>0</Version><Level>0</Level>
<Task>12811</Task><Opcode>0</Opcode><Keywords>0x8010000000000000</Keywords>
<TimeCreated SystemTime='2021-05-19T22:30:40.485188700Z'/><EventRecordID>282939</
EventRecordID>
<Correlation/><Execution ProcessID='4' ThreadID='344'/><Channel>Security</Channel>
<Computer>amznfsxtmn9autz.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-
1113</Data><Data Name='SubjectUserName'>Admin</Data><Data
 Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x95b3fb7</Data><Data Name='ObjectType'>File</Data>
<Data Name='IpAddress'>172.31.7.112</Data><Data Name='IpPort'>59979</Data>
```

```
<Data Name='ShareName'>\\AMZNFSXDPNTE0DC\demoshare01</Data><Data Name='ShareLocalPath'>
\??\D:\demoshare01</Data>
<Data Name='RelativeTargetName'>Desktop.ini</Data><Data Name='AccessMask'>0x120089</
Data>
<Data Name='AccessList'>%%1538 %%1541 %%4416 %%4419 %%4423 </Data><Data
 Name='AccessReason'>%%1538:
%%1804 %%1541: %%1805 %%4416: %%1805 %%4419: %%1805 %%4423: %%1805 </Data></
EventData></Event>
```

如果您使用 CloudWatch Logs Insights 搜尋日誌資料，您可以在事件欄位上執行查詢，如下列範例所示：

- 若要查詢特定事件 ID：

```
fields @message
   | filter @message like /4660/
```

- 若要查詢符合特定檔案名稱的所有事件：

```
fields @message
   | filter @message like /event.txt/
```

如需 CloudWatch Logs Insights 查詢語言的詳細資訊，請參閱《Amazon CloudWatch Logs 使用者指南》中的使用 CloudWatch Logs Insights 分析日誌資料。 Amazon CloudWatch

設定檔案和資料夾稽核控制項

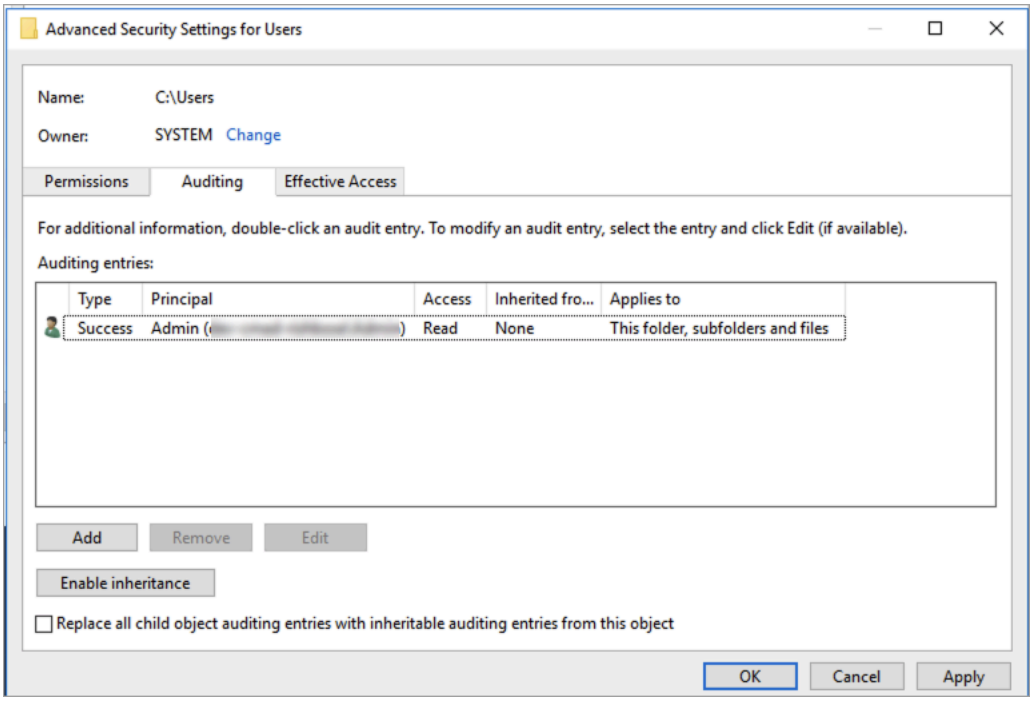
您需要對要針對使用者存取嘗試進行稽核的檔案和資料夾設定稽核控制。稽核控制項也稱為 NTFS 系統存取控制清單 SACLs)。

您可以使用 Windows 原生 GUI 界面或使用 Windows PowerShell 命令以程式設計方式設定稽核控制項。如果啟用繼承，您通常只需要在要記錄存取權的頂層資料夾上設定稽核控制項。

使用 Windows GUI 設定稽核存取權

若要使用 GUI 在檔案和資料夾上設定稽核控制項，請使用 Windows File Explorer。在指定的檔案或資料夾上，開啟 Windows File Explorer，然後選取屬性 > 安全性 > 進階 > 稽核索引標籤。

下列稽核控制範例會稽核資料夾的成功事件。每當管理員使用者成功開啟該控制代碼以供讀取時，都會發出 Windows 事件日誌項目。



類型欄位指出您要稽核的動作。將此欄位設定為成功以稽核成功的嘗試、失敗的稽核失敗的嘗試，或全部以稽核成功和失敗的嘗試。

如需稽核項目欄位的詳細資訊，請參閱 Microsoft 文件中的對檔案或資料夾套用基本稽核政策。

使用 PowerShell 命令設定稽核存取權

您可以使用 Microsoft Windows `Set-Acl`命令，在任何檔案或資料夾上設定稽核 SACL。如需此命令的相關資訊，請參閱 Microsoft Set-Acl 文件。

以下是使用一系列 PowerShell 命令和變數來設定成功嘗試稽核存取權的範例。您可以調整這些範例命令，以符合檔案系統的需求。

```
$path = "C:\Users\TestUser\Desktop\DemoTest\"

$ACL = Get-Acl $path

$ACL | Format-List

$AuditUser = "TESTDOMAIN\TestUser"

$AuditRules = "FullControl"
```

```
$InheritType = "ContainerInherit,ObjectInherit"

$AuditType = "Success"

$AccessRule = New-Object System.Security.AccessControl.FileSystemAuditRule($AuditUser,
$AuditRules,$InheritType,"None",$AuditType)

$ACL.SetAuditRule($AccessRule)

$ACL | Set-Acl $path

Get-Acl $path -Audit | Format-List
```

管理檔案存取稽核

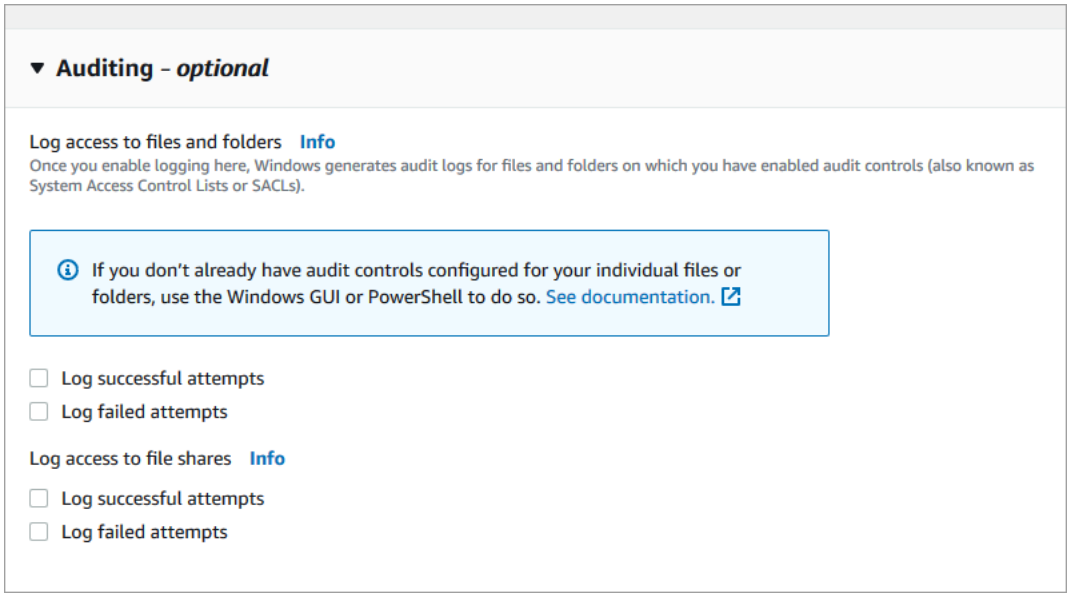
您可以在建立新的 Amazon FSx for Windows File Server 檔案系統時啟用檔案存取稽核。當您從 Amazon FSx 主控台建立檔案系統時，預設會關閉檔案存取稽核。

在已啟用檔案存取稽核的現有檔案系統上，您可以變更檔案存取稽核設定，包括變更檔案和檔案共用存取的存取嘗試類型，以及稽核事件日誌目的地。您可以使用 Amazon FSx 主控台 AWS CLI或 API 來執行這些任務。

> **Note**
>
> 僅在輸送量容量為 32 MBps 或更高的 Amazon FSx for Windows File Server 檔案系統上支援檔案存取稽核。如果啟用檔案存取稽核，則您無法建立或更新輸送量容量小於 32 MBps 的檔案系統。您可以在建立檔案系統之後隨時修改輸送量容量。如需詳細資訊，請參閱管理輸送量容量。

在建立檔案系統時啟用檔案存取稽核（主控台）

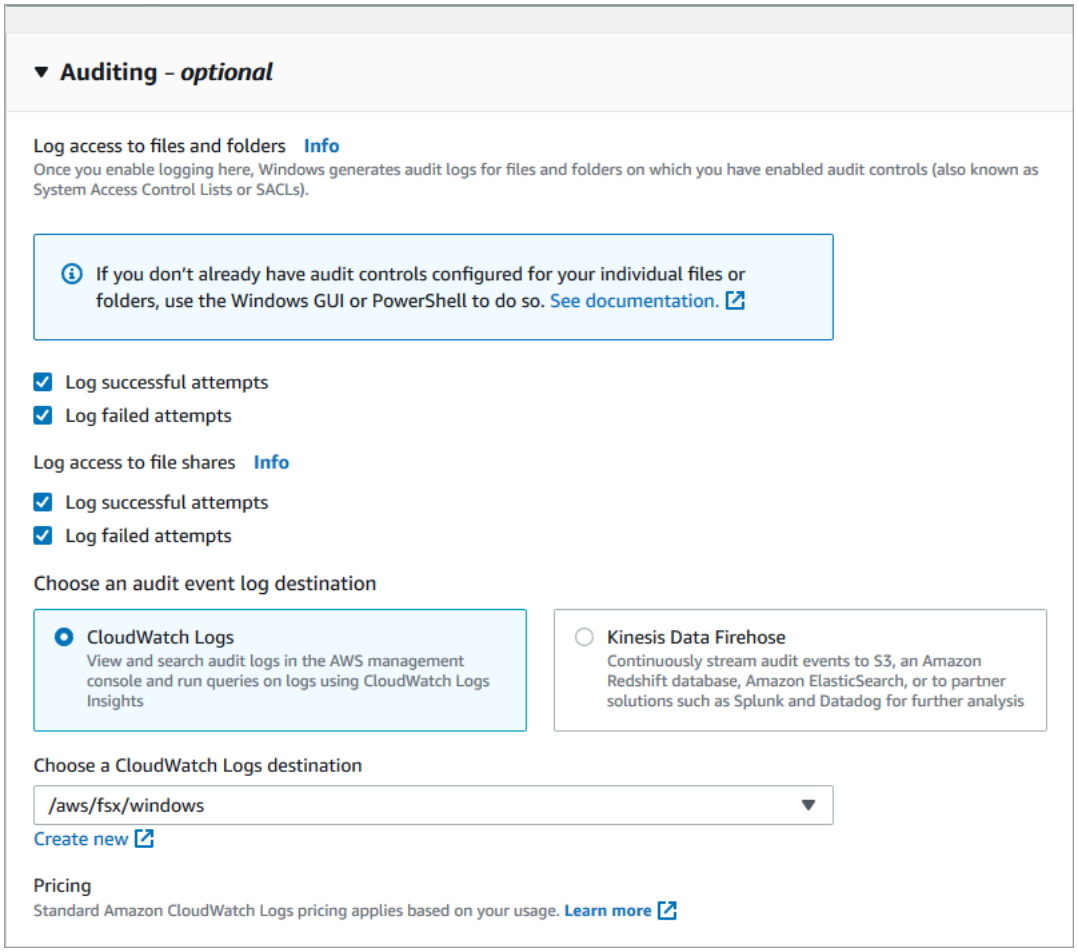
1. 開啟位於 https：//https://console.aws.amazon.com/fsx/ 的 Amazon FSx 主控台。
2. 請遵循 入門一節步驟 5. 建立您的檔案系統中所述建立新檔案系統的程序。
3. 開啟稽核 - 選用區段。檔案存取稽核預設為停用。



4. 若要啟用和設定檔案存取稽核，請執行下列動作。

   - 針對檔案和資料夾的日誌存取，選取成功和/或失敗嘗試的記錄。如果您不進行選擇，則會停用檔案和資料夾的記錄。
   - 針對檔案共享的日誌存取，選取成功和/或失敗嘗試的記錄。如果您不選擇檔案共享，則會停用記錄。
   - 針對選擇稽核事件日誌目的地，選擇 CloudWatch Logs 或 Firehose。然後選擇現有的日誌或交付串流，或建立新的日誌或交付串流。對於 CloudWatch Logs，Amazon FSx 可以在 CloudWatch Logs 日誌群組中建立和使用預設`/aws/fsx/windows`日誌串流。

   以下是檔案存取稽核組態的範例，該組態將稽核最終使用者對檔案、資料夾和檔案共用的成功和失敗存取嘗試。稽核事件日誌將傳送至預設 CloudWatch Logs `/aws/fsx/windows`日誌群組目的地。



5. 繼續執行檔案系統建立精靈的下一節。

當檔案系統可用時，會啟用檔案存取稽核功能。

在建立檔案系統 (CLI) 時啟用檔案存取稽核

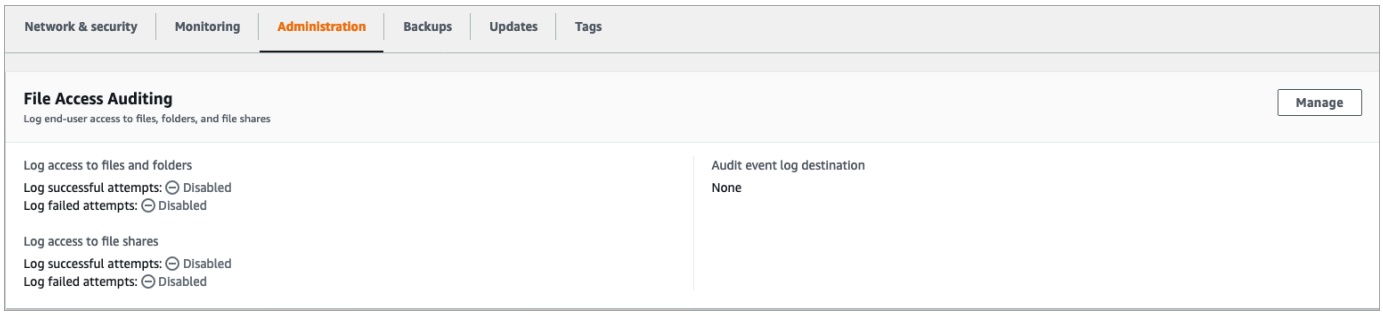
1. 建立新的檔案系統時，請使用 `AuditLogConfiguration` 屬性搭配 CreateFileSystem API 操作，以啟用新檔案系統的檔案存取稽核。

```
aws fsx create-file-system \
  --file-system-type WINDOWS \
  --storage-capacity 300 \
  --subnet-ids subnet-123456 \
  --windows-configuration
 AuditLogConfiguration='{FileAccessAuditLogLevel="SUCCESS_AND_FAILURE", \
    FileShareAccessAuditLogLevel="SUCCESS_AND_FAILURE", \
    AuditLogDestination="arn:aws:logs:us-east-1:123456789012:log-group:/aws/fsx/my-
customer-log-group"}'
```

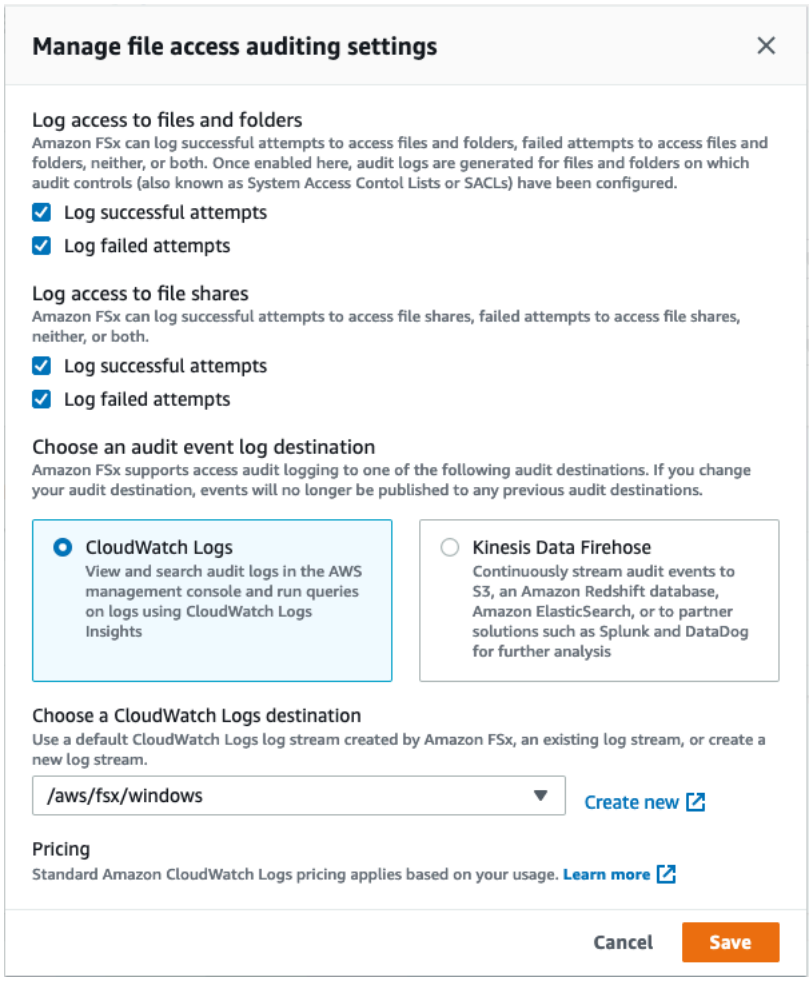
2. 當檔案系統可用時，會啟用檔案存取稽核功能。

變更檔案存取稽核組態（主控台）

1. 在 https://console.aws.amazon.com/fsx/：// 開啟 Amazon FSx 主控台。
2. 導覽至檔案系統，然後選擇您要管理檔案存取稽核的 Windows 檔案系統。
3. 選擇管理索引標籤。
4. 在檔案存取稽核面板上，選擇管理。



5. 在管理檔案存取稽核設定對話方塊中，變更所需的設定。



- 針對檔案和資料夾的日誌存取，選取成功和/或失敗嘗試的記錄。如果您不進行選擇，則會停用檔案和資料夾的記錄。
- 針對檔案共享的日誌存取，選取成功和/或失敗嘗試的記錄。如果您不選擇檔案共享，則會停用記錄。
- 針對選擇稽核事件日誌目的地，選擇 CloudWatch Logs 或 Firehose。然後選擇現有的日誌或交付串流，或建立新的日誌或交付串流。

6. 選擇儲存。

變更檔案存取稽核組態 (CLI)

- 使用 update-file-system CLI 命令或同等 UpdateFileSystem API 操作。

```
aws fsx update-file-system \
  --file-system-id fs-0123456789abcdef0 \
```

```
  --windows-configuration
 AuditLogConfiguration='{FileAccessAuditLogLevel="SUCCESS_ONLY", \
    FileShareAccessAuditLogLevel="FAILURE_ONLY", \
    AuditLogDestination="arn:aws:logs:us-east-1:123456789012:log-group:/aws/fsx/my-
customer-log-group"}'
```

Amazon FSx for Windows File Server 的身分和存取管理

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

主題

目標對象

如何使用 AWS Identity and Access Management (IAM) 會因您的角色而有所不同：

- 服務使用者 — 若無法存取某些功能，請向管理員申請所需許可 (請參閱 對 Amazon FSx for Windows File Server 身分和存取進行故障診斷)
- 服務管理員 — 負責設定使用者存取權並提交相關許可請求 (請參閱 Amazon FSx for Windows File Server 如何與 IAM 搭配使用)
- IAM 管理員 — 撰寫政策以管理存取控制 (請參閱 Amazon FSx for Windows File Server 的身分型政策範例)

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入 的方式。您必須驗證為 AWS 帳戶根使用者、IAM 使用者或擔任 IAM 角色。

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

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

AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從一個名為 AWS 帳戶 theroot 使用者的登入身分開始，該身分具有對所有 AWS 服務 和資源的完整存取權。強烈建議不要使用根使用者來執行日常任務。有關需要根使用者憑證的任務，請參閱《IAM 使用者指南》中的需要根使用者憑證的任務。

聯合身分

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

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

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

IAM 使用者和群組

IAM 使用者是一種身分，具備單一人員或應用程式的特定許可。建議以臨時憑證取代具備長期憑證的 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的要求人類使用者使用聯合身分提供者來 AWS 使用臨時憑證存取 。

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

IAM 角色

IAM 角色是一種具特定許可的身分，可提供臨時憑證。您可以透過從使用者切換到 IAM 角色 （主控台） 或呼叫 AWS CLI 或 AWS API 操作來擔任角色。如需詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

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

使用政策管理存取權

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

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

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

身分型政策

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

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

資源型政策

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

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用來自 IAM 的 AWS 受管政策。

其他政策類型

AWS 支援其他政策類型，可設定更多常見政策類型授予的最大許可：

- 許可界限 — 設定身分型政策可授與 IAM 實體的最大許可。如需詳細資訊，請參閱《 IAM 使用者指南》中的 IAM 實體許可界限。

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

多種政策類型

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

Amazon FSx for Windows File Server 如何與 IAM 搭配使用

使用 IAM 管理 FSx for Windows File Server 的存取權之前，請先了解哪些 IAM 功能可與 FSx for Windows File Server 搭配使用。

您可以搭配 Amazon FSx for Windows File Server 使用的 IAM 功能

IAM 功能	FSx 支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵 (服務特定)	是
ACL	否
ABAC (政策中的標籤)	是
臨時憑證	是
轉寄存取工作階段	是

IAM 功能	FSx 支援
服務角色	否
服務連結角色	是

若要全面了解 FSx 和其他 AWS 服務如何與大多數 IAM 功能搭配使用，請參閱《AWS IAM 使用者指南》中的與 IAM 搭配使用的 服務。

FSx 的身分型政策

支援身分型政策：是

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

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。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。

FSx 的身分型政策範例

若要檢視 FSx for Windows File Server 身分型政策的範例，請參閱 Amazon FSx for Windows File Server 的身分型政策範例。

FSx 中的資源型政策

支援資源型政策：否

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

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

FSx 的政策動作

支援政策動作：是

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

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

若要查看 FSx 動作清單，請參閱《服務授權參考》中的 Amazon FSx for Windows File Server 定義的動作。

FSx 中的政策動作在動作之前使用下列字首：

```
fsx
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

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

若要檢視 FSx for Windows File Server 身分型政策的範例，請參閱 Amazon FSx for Windows File Server 的身分型政策範例。

FSx 的政策資源

支援政策資源：是

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

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

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

若要查看 FSx 資源類型及其 ARNs，請參閱《服務授權參考》中的 Amazon FSx for Windows File Server 定義的資源。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 Amazon FSx for Windows File Server 定義的動作。

若要檢視 FSx for Windows File Server 身分型政策的範例，請參閱 Amazon FSx for Windows File Server 的身分型政策範例。

FSx 的政策條件索引鍵

支援服務特定政策條件金鑰：是

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

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

若要查看 FSx 條件金鑰清單，請參閱《服務授權參考》中的 Amazon FSx for Windows File Server 的條件金鑰。若要了解您可以使用條件金鑰的動作和資源，請參閱 Amazon FSx for Windows File Server 定義的動作。

若要檢視 FSx for Windows File Server 身分型政策的範例，請參閱 Amazon FSx for Windows File Server 的身分型政策範例。

FSx 中的 ACLs

支援 ACL：否

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

ABAC 搭配 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，依據稱為標籤的屬性來定義許可。您可以將標籤連接至 IAM 實體 AWS 和資源，然後設計 ABAC 政策，以便在委託人的標籤符合資源上的標籤時允許操作。

如需根據標籤控制存取，請使用 aws:ResourceTag/*key-name*、aws:RequestTag/*key-name* 或 aws:TagKeys 條件索引鍵，在政策的條件元素中，提供標籤資訊。

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

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

搭配 FSx 使用臨時登入資料

支援臨時憑證：是

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

轉送 FSx 的存取工作階段

支援轉寄存取工作階段 (FAS)：是

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

FSx 的服務角色

支援服務角色：否

服務角色是服務擔任的 IAM 角色，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可給 AWS 服務。

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

FSx 的服務連結角色

支援服務連結角色：是

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

如需建立或管理 FSx for Windows File Server 服務連結角色的詳細資訊，請參閱 針對 FSx for Windows File Server 使用服務連結角色。

Amazon FSx for Windows File Server 的身分型政策範例

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

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

如需 FSx 定義的動作和資源類型的詳細資訊，包括每種資源類型的 ARNs 格式，請參閱《服務授權參考》中的 Amazon FSx for Windows File Server 的動作、資源和條件索引鍵。

主題

- 政策最佳實務
- 使用 FSx 主控台
- 允許使用者檢視他們自己的許可

政策最佳實務

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

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需更多資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱《IAM 使用者指南》中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 等使用服務動作

AWS 服務，您也可以使用條件來授予其存取權 CloudFormation。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素：條件。

- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的透過 MFA 的安全 API 存取。

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

使用 FSx 主控台

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

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

為了確保使用者和角色仍然可以使用 FSx 主控台，也請將 FSx `AmazonFSxConsoleReadOnlyAccess` AWS 受管政策連接到實體。如需詳細資訊，請參閱《IAM 使用者指南》中的新增許可到使用者。

允許使用者檢視他們自己的許可

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
```

```
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Amazon FSx for Windows File Server 的 受管政策

AWS 受管政策是由 AWS AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住， AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義特定於使用案例的客戶管理政策，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新受 AWS 管政策中定義的許可，則更新會影響政策連接的所有主體身分（使用者、群組和角色）。 AWS 服務 當新的 啟動或新的 API 操作可供現有服務使用時， AWS 最有可能更新 AWS 受管政策。

如需詳細資訊，請參閱 IAM 使用者指南中的 AWS 受管政策。

AmazonFSxServiceRolePolicy

允許 Amazon FSx 代表您管理 AWS 資源。如需進一步了解，請參閱針對 FSx for Windows File Server 使用服務連結角色。

AWS 受管政策：AmazonFSxDeleteServiceLinkedRoleAccess

您不得將 AmazonFSxDeleteServiceLinkedRoleAccess 連接到 IAM 實體。此政策會連結至 服務，並僅用於該服務的服務連結角色。您無法連接、取消連接、修改或刪除此政策。如需詳細資訊，請參閱針對 FSx for Windows File Server 使用服務連結角色。

此政策授予管理許可，允許 Amazon FSx 刪除其 Amazon S3 存取的服務連結角色，僅供 Amazon FSx for Lustre 使用。

許可詳細資訊

此政策包含 中的許可iam，允許 Amazon FSx 檢視、刪除和檢視 FSx Service Linked Roles for Amazon S3 存取的刪除狀態。

若要檢視此政策的許可，請參閱《 AWS 受管政策參考指南》中的 AmazonFSxDeleteServiceLinkedRoleAccess。

AWS 受管政策：AmazonFSxFullAccess

您可以將 AmazonFSxFullAccess 連接至 IAM 實體。Amazon FSx 也會將此政策連接至允許 Amazon FSx 代表您執行動作的服務角色。

提供 Amazon FSx 的完整存取權和相關 AWS 服務的存取權。

許可詳細資訊

此政策包含以下許可。

- fsx – 允許主體完整存取以執行所有 Amazon FSx 動作，但 除外BypassSnaplockEnterpriseRetention。
- ds – 允許主體檢視 Directory Service 目錄的相關資訊。
- ec2
  - 允許主體在指定的條件下建立標籤。
  - 為所有可與 VPC 搭配使用的安全群組提供增強型安全群組驗證。

- `iam` – 允許原則代表使用者建立 Amazon FSx 服務連結角色。這是必要的，以便 Amazon FSx 可以代表使用者管理 AWS 資源。
- `firehose` – 允許主體將記錄寫入 Amazon Data Firehose。這是必要的，以便使用者可以透過傳送稽核存取日誌到 Firehose 來監控 FSx for Windows File Server 檔案系統存取。
- `logs` – 允許主體建立日誌群組、日誌串流，以及將事件寫入日誌串流。這是必要的，讓使用者可以透過傳送稽核存取日誌到 CloudWatch Logs 來監控 FSx for Windows File Server 檔案系統存取。

若要檢視此政策的許可，請參閱《 AWS 受管政策參考指南》中的 AmazonFSxFullAccess。

AWS 受管政策：AmazonFSxConsoleFullAccess

您可將 `AmazonFSxConsoleFullAccess` 政策連接到 IAM 身分。

此政策會授予管理許可，以允許完整存取 Amazon FSx 並透過 存取相關 AWS 服務 AWS 管理主控台。

許可詳細資訊

此政策包含以下許可。

- `fsx` – 允許主體在 Amazon FSx 管理主控台中執行所有動作，但 除外`BypassSnaplockEnterpriseRetention`。
- `cloudwatch` – 允許主體在 Amazon FSx 管理主控台中檢視 CloudWatch 警示和指標。
- `ds` – 允許主體列出 Directory Service 目錄的相關資訊。
- `ec2`
  - 允許主體在路由表上建立標籤、列出網路介面、路由表、安全群組、子網路以及與 Amazon FSx 檔案系統相關聯的 VPC。
  - 允許主體為所有可與 VPC 搭配使用的安全群組提供增強型安全群組驗證。
  - 允許主體檢視與 Amazon FSx 檔案系統相關聯的彈性網路介面。
- `kms` – 允許主體列出 AWS Key Management Service 金鑰的別名。
- `s3` – 允許主體列出 Amazon S3 儲存貯體中的部分或全部物件 （最多 1000 個）。
- `secretsmanager` – 允許主體在 中列出秘密 AWS Secrets Manager ，以選取網域加入服務帳戶登入資料。

- `iam` – 准許建立服務連結角色，以允許 Amazon FSx 代表使用者執行動作。

若要檢視此政策的許可，請參閱《 AWS 受管政策參考指南》中的 AmazonFSxConsoleFullAccess。

AWS 受管政策：AmazonFSxConsoleReadOnlyAccess

您可將 `AmazonFSxConsoleReadOnlyAccess` 政策連接到 IAM 身分。

此政策會將唯讀許可授予 Amazon FSx 和相關 AWS 服務，讓使用者可以在 中檢視這些服務的相關資訊 AWS 管理主控台。

許可詳細資訊

此政策包含以下許可。

- `fsx` – 允許主體在 Amazon FSx 管理主控台中檢視 Amazon FSx 檔案系統的相關資訊，包括所有標籤。
- `cloudwatch` – 允許主體在 Amazon FSx 管理主控台中檢視 CloudWatch 警示和指標。
- `ds` – 允許主體在 Amazon FSx 管理主控台 Directory Service 中檢視目錄的相關資訊。
- `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介面、安全群組、子網路和 VPC。
  - 允許主體為所有可與 VPC 搭配使用的安全群組提供增強型安全群組驗證。
  - 允許主體檢視與 Amazon FSx 檔案系統相關聯的彈性網路介面。
- `kms` – 允許主體在 Amazon FSx 管理主控台中檢視 AWS Key Management Service 金鑰的別名。
- `log` – 允許主體描述與提出請求的帳戶相關聯的 Amazon CloudWatch Logs 日誌群組。這是必要的，以便主體可以檢視 FSx for Windows File Server 檔案系統的現有檔案存取稽核組態。
- `secretsmanager` – 允許主體在 中列出秘密 AWS Secrets Manager ，以選取網域加入服務帳戶登入資料。
- `firehose` – 允許主體描述與提出請求的帳戶相關聯的 Amazon Data Firehose 交付串流。這是必要的，以便主體可以檢視 FSx for Windows File Server 檔案系統的現有檔案存取稽核組態。

若要檢視此政策的許可，請參閱《 AWS 受管政策參考指南》中的 AmazonFSxConsoleReadOnlyAccess。

AWS 受管政策：AmazonFSxReadOnlyAccess

您可將 AmazonFSxReadOnlyAccess 政策連接到 IAM 身分。

- fsx – 允許主體在 Amazon FSx 管理主控台中檢視 Amazon FSx 檔案系統的相關資訊，包括所有標籤。
- ec2 – 為所有可與 VPC 搭配使用的安全群組提供增強型安全群組驗證。

若要檢視此政策的許可，請參閱《 AWS 受管政策參考指南》中的 AmazonFSxReadOnlyAccess。

AWS 受管政策的 Amazon FSx 更新

檢視自此服務開始追蹤 Amazon FSx AWS 受管政策更新以來的詳細資訊。如需此頁面變更的自動提醒，請訂閱 Amazon FSx 文件歷史記錄頁面上的 RSS 摘要。

變更	描述	Date
AmazonFSxConsoleFullAccess – 更新現有政策	Amazon FSx 新增了新的許可，secretsmanager:ListSecrets 允許主體在中列出秘密 AWS Secrets Manager ，以選取網域加入服務帳戶憑證。	2025 年 11 月 5 日
AmazonFSxConsoleReadOnlyAccess – 更新至現有政策	Amazon FSx 新增了新的許可，secretsmanager:ListSecrets 允許主體在中列出秘密 AWS Secrets Manager ，以選取網域加入服務帳戶憑證。	2025 年 11 月 3 日
AmazonFSxServiceRolePolicy – 更新至現有政策	Amazon FSx 新增了新的許可，ec2:AssignIpv6Addresses 允許主體將 IPv6 地址指派給具有 AmazonFSx .FileSystemId 標籤的客戶網路介面。	2025 年 7 月 22 日

變更	描述	Date
AmazonFSxServiceRolePolicy – 更新至現有政策	Amazon FSx 新增了新的許可，ec2:UnassignIpv6Addresses 允許主體從具有 AmazonFSx.FileSystemId 標籤的客戶網路介面取消指派 IPv6 地址。	2025 年 7 月 22 日
AmazonFSxConsoleFullAccess – 更新現有政策	Amazon FSx 新增了新的許可，fsx:CreateAndAttachS3AccessPoint 允許主體建立 S3 存取點並將其連接到 FSx 磁碟區。	2025 年 6 月 25 日
AmazonFSxConsoleFullAccess – 更新現有政策	Amazon FSx 新增了新的許可，fsx:DescribeS3AccessPointAttachments 允許主體在 中列出 AWS 帳戶 中的所有 S3 存取點 AWS 區域。	2025 年 6 月 25 日
AmazonFSxConsoleFullAccess – 更新至現有政策	Amazon FSx 新增了fsx:DetachAndDeleteS3AccessPoint 允許主體刪除 S3 存取點的新許可。	2025 年 6 月 25 日
AmazonFSxFullAccess – 更新現有政策	Amazon FSx 新增了新的許可，fsx:CreateAndAttachS3AccessPoint 允許主體建立 S3 存取點並將其連接到 FSx 磁碟區。	2025 年 6 月 25 日
AmazonFSxFullAccess – 更新現有政策	Amazon FSx 新增了新的許可，fsx:DescribeS3AccessPointAttachments 允許主體在 中列出 AWS 帳戶 中的所有 S3 存取點 AWS 區域。	2025 年 6 月 25 日

變更	描述	Date
AmazonFSxFullAccess – 更新現有政策	Amazon FSx 新增了`fsx:DetachAndDeleteS3AccessPoint` 允許主體刪除 S3 存取點的新許可。	2025 年 6 月 25 日
AmazonFSxConsoleReadOnlyAccess – 更新至現有政策	Amazon FSx 新增了新的許可，`ec2:DescribeNetworkInterfaces` 允許主體檢視與其檔案系統相關聯的彈性網路介面。	2025 年 2 月 25 日
AmazonFSxConsoleFullAccess – 更新現有政策	Amazon FSx 新增了新的許可，`ec2:DescribeNetworkInterfaces` 允許主體檢視與其檔案系統相關聯的彈性網路介面。	2025 年 2 月 7 日
AmazonFSxServiceRolePolicy – 更新至現有政策	Amazon FSx 新增了新的許可，`ec2:GetSecurityGroupsForVpc` 允許主體為所有可與 VPC 搭配使用的安全群組提供增強型安全群組驗證。	2024 年 1 月 9 日
AmazonFSxReadOnlyAccess – 更新至現有政策	Amazon FSx 新增了新的許可，`ec2:GetSecurityGroupsForVpc` 允許主體為所有可與 VPC 搭配使用的安全群組提供增強型安全群組驗證。	2024 年 1 月 9 日
AmazonFSxConsoleReadOnlyAccess – 更新至現有政策	Amazon FSx 新增了新的許可，`ec2:GetSecurityGroupsForVpc` 允許主體為所有可與 VPC 搭配使用的安全群組提供增強型安全群組驗證。	2024 年 1 月 9 日

變更	描述	Date
AmazonFSxFullAccess – 更新現有政策	Amazon FSx 新增了新的許可，ec2:GetSecurityGroupsForVpc 允許主體為所有可與 VPC 搭配使用的安全群組提供增強型安全群組驗證。	2024 年 1 月 9 日
AmazonFSxConsoleFullAccess – 更新現有政策	Amazon FSx 新增了新的許可，ec2:GetSecurityGroupsForVpc 允許主體為所有可與 VPC 搭配使用的安全群組提供增強型安全群組驗證。	2024 年 1 月 9 日
AmazonFSxFullAccess – 更新現有政策	Amazon FSx 新增了新的許可，讓使用者能夠為 FSx for OpenZFS 檔案系統執行跨區域和跨帳戶資料複寫。	2023 年 12 月 20 日
AmazonFSxConsoleFullAccess – 更新至現有政策	Amazon FSx 新增了新的許可，讓使用者能夠為 FSx for OpenZFS 檔案系統執行跨區域和跨帳戶資料複寫。	2023 年 12 月 20 日
AmazonFSxFullAccess – 更新現有政策	Amazon FSx 新增了新的許可，讓使用者能夠執行 FSx for OpenZFS 檔案系統的隨需磁碟區複寫。	2023 年 11 月 26 日
AmazonFSxConsoleFullAccess – 更新現有政策	Amazon FSx 新增了新的許可，讓使用者能夠執行 FSx for OpenZFS 檔案系統的隨需磁碟區複寫。	2023 年 11 月 26 日

變更	描述	Date
AmazonFSxFullAccess – 更新現有政策	Amazon FSx 新增了新的許可，讓使用者能夠檢視、啟用和停用 FSx for ONTAP 多可用區域檔案系統的共用 VPC 支援。	2023 年 11 月 14 日
AmazonFSxConsoleFullAccess – 更新現有政策	Amazon FSx 新增了新的許可，讓使用者能夠檢視、啟用和停用 FSx for ONTAP 多可用區域檔案系統的共用 VPC 支援。	2023 年 11 月 14 日
AmazonFSxFullAccess – 更新現有政策	Amazon FSx 新增了新的許可，以允許 Amazon FSx 管理 FSx for OpenZFS 多可用區域檔案系統的網路組態。	2023 年 8 月 9 日
AWS 受管政策：AmazonFSxServiceRolePolicy – 更新現有政策	Amazon FSx 修改了現有的`cloudwatch:PutMetricData` 許可，以便 Amazon FSx 將 CloudWatch 指標發佈到`AWS/FSx`命名空間。	2023 年 7 月 24 日
AmazonFSxFullAccess – 更新現有政策	Amazon FSx 已更新政策以移除`fsx:*`許可並新增特定`fsx`動作。	2023 年 7 月 13 日
AmazonFSxConsoleFullAccess – 更新至現有政策	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
AmazonFSxConsoleReadOnlyAccess – 更新至現有政策	Amazon FSx 新增了新的許可，讓使用者能夠在 Amazon FSx 主控台中檢視 FSx for Windows File Server 檔案系統的增強效能指標和建議動作。	2022 年 9 月 21 日

變更	描述	Date
AmazonFSxConsoleFullAccess – 更新現有政策	Amazon FSx 新增了新的許可，讓使用者能夠在 Amazon FSx 主控台中檢視 FSx for Windows File Server 檔案系統的增強效能指標和建議動作。	2022 年 9 月 21 日
AmazonFSxReadOnlyAccess – 開始追蹤政策	此政策會授予所有 Amazon FSx 資源和與其關聯之任何標籤的唯讀存取權。	2022 年 2 月 4 日
AmazonFSxDeleteServiceLinkedRoleAccess – 開始追蹤政策	此政策會授予管理許可，允許 Amazon FSx 刪除其 Amazon S3 存取的服務連結角色。	2022 年 1 月 7 日
AmazonFSxServiceRolePolicy – 更新至現有政策	Amazon FSx 新增了新的許可，以允許 Amazon FSx 管理 Amazon FSx for NetApp ONTAP 檔案系統的網路組態。	2021 年 9 月 2 日
AmazonFSxFullAccess – 更新現有政策	Amazon FSx 新增了新的許可，以允許 Amazon FSx 在 EC2 路由表上為範圍縮小的呼叫建立標籤。	2021 年 9 月 2 日
AmazonFSxConsoleFullAccess – 更新至現有政策	Amazon FSx 新增了允許 Amazon FSx 為 NetApp ONTAP 多可用區域檔案系統建立 Amazon FSx 的許可。	2021 年 9 月 2 日
AmazonFSxConsoleFullAccess – 更新現有政策	Amazon FSx 新增了新的許可，以允許 Amazon FSx 在 EC2 路由表上為範圍縮小的呼叫建立標籤。	2021 年 9 月 2 日

變更	描述	Date
AmazonFSxServiceRolePolicy – 更新至現有政策	Amazon FSx 新增了允許 Amazon FSx 描述和寫入 CloudWatch Logs 日誌串流的許可。 這是必要的，讓使用者可以使用 CloudWatch Logs 檢視 FSx for Windows File Server 檔案系統的檔案存取稽核日誌。	2021 年 6 月 8 日
AmazonFSxServiceRolePolicy – 更新至現有政策	Amazon FSx 新增了允許 Amazon FSx 描述和寫入 Amazon Data Firehose 交付串流的許可。 這是必要的，讓使用者可以使用 Amazon Data Firehose 檢視 FSx for Windows File Server 檔案系統的檔案存取稽核日誌。	2021 年 6 月 8 日
AmazonFSxFullAccess – 更新現有政策	Amazon FSx 新增了新的許可，允許主體描述和建立 CloudWatch Logs 日誌群組、日誌串流，以及將事件寫入日誌串流。 這是必要的，以便主體可以使用 CloudWatch Logs 檢視 FSx for Windows File Server 檔案系統的檔案存取稽核日誌。	2021 年 6 月 8 日

變更	描述	Date
AmazonFSxFullAccess – 更新現有政策	Amazon FSx 新增了允許主體描述記錄並將其寫入 Amazon Data Firehose 的許可。 這是必要的，讓使用者可以使用 Amazon Data Firehose 檢視 FSx for Windows File Server 檔案系統的檔案存取稽核日誌。	2021 年 6 月 8 日
AmazonFSxConsoleFullAccess – 更新現有政策	Amazon FSx 新增了新的許可，允許主體描述與提出請求的帳戶相關聯的 Amazon CloudWatch Logs 日誌群組。 這是必要的，以便主體在設定 FSx for Windows File Server 檔案系統的檔案存取稽核時，可以選擇現有的 CloudWatch Logs 日誌群組。	2021 年 6 月 8 日
AmazonFSxConsoleFullAccess – 更新現有政策	Amazon FSx 新增了新的許可，允許主體描述與提出請求的帳戶相關聯的 Amazon Data Firehose 交付串流。 這是必要的，以便主體在設定 FSx for Windows File Server 檔案系統的檔案存取稽核時，可以選擇現有的 Firehose 交付串流。	2021 年 6 月 8 日

變更	描述	Date
AmazonFSxConsoleReadOnlyAccess – 更新至現有政策	Amazon FSx 新增了新的許可，允許主體描述與提出請求的帳戶相關聯的 Amazon CloudWatch Logs 日誌群組。 這是必要的，以便主體可以檢視 FSx for Windows File Server 檔案系統的現有檔案存取稽核組態。	2021 年 6 月 8 日
AmazonFSxConsoleReadOnlyAccess – 更新現有政策	Amazon FSx 新增了新的許可，允許主體描述與提出請求的帳戶相關聯的 Amazon Data Firehose 交付串流。 這是必要的，以便主體可以檢視 FSx for Windows File Server 檔案系統的現有檔案存取稽核組態。	2021 年 6 月 8 日
Amazon FSx 已開始追蹤變更	Amazon FSx 開始追蹤其 AWS 受管政策的變更。	2021 年 6 月 8 日

對 Amazon FSx for Windows File Server 身分和存取進行故障診斷

使用以下資訊來協助您診斷和修正使用 FSx for Windows File Server 和 IAM 時可能遇到的常見問題。

主題

- 我無權在 FSx 中執行動作
- 我未獲得執行 iam:PassRole 的授權
- 我想要允許 以外的人員 AWS 帳戶 存取我的 FSx 資源

我無權在 FSx 中執行動作

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

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

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

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

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，告知您無權執行 iam:PassRole動作，您的政策必須更新，以允許您將角色傳遞至 FSx for Windows File Server。

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

當名為 的 IAM marymajor 使用者嘗試使用主控台在 FSx for Windows File Server 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 沒有將角色傳遞給服務的許可。

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

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

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想要允許 以外的人員 AWS 帳戶 存取我的 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 FSx for Windows File Server 是否支援這些功能，請參閱 Amazon FSx for Windows File Server 如何與 IAM 搭配使用。

- 若要了解如何提供您擁有 AWS 帳戶 的資源存取權，請參閱《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個 中為 IAM 使用者提供存取權。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方 AWS 帳戶 擁有。
- 如需了解如何透過聯合身分提供存取權，請參閱《IAM 使用者指南》中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。

搭配 Amazon FSx 使用標籤

您可以使用標籤來控制對 Amazon FSx 資源的存取，以及實作屬性型存取控制 (ABAC)。使用者需要有許可，才能在建立期間將標籤套用至 Amazon FSx 資源。

在建立期間授予標籤資源的許可

有些建立資源的 FSx for Windows File Server API 動作可讓您在建立資源時指定標籤。您可以使用資源標籤來實作屬性型存取控制 (ABAC)。如需詳細資訊，請參閱《IAM 使用者指南》中的什麼是 ABAC for AWS。

使用者若要在建立時標記資源，他們必須具備建立資源動作 (如 `fsx:CreateFileSystem` 或 `fsx:CreateBackup`) 的使用許可。若標籤於資源建立動作指定，Amazon 會針對 `fsx:TagResource` 動作執行其他授權，以確認使用者具備建立標籤的許可。因此，使用者必須同時具備使用 `fsx:TagResource` 動作的明確許可。

下列範例示範的政策可讓使用者在特定 中建立檔案系統，並將標籤套用至檔案系統 AWS 帳戶。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateFileSystem",
         "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/*"
    }
  ]
}
```

同樣地，以下政策允許使用者在特定檔案系統上建立備份，並在備份建立期間將任何標籤套用至備份。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateBackup"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/file-system-id*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:backup/*"
    }
  ]
}
```

只有在資源建立動作中套用了標籤時，才評估 `fsx:TagResource` 動作。因此，在沒有標記條件的情況下，若請求中未指定標籤，則具備資源建立許可的使用者不需要使用 `fsx:TagResource` 動作的許可。然而，若該使用者試圖建立具有標籤的資源卻未具備使用 `fsx:TagResource` 動作的許可，則該請求會失敗。

如需標記 Amazon FSx 資源的詳細資訊，請參閱 標記 Amazon FSx 資源。如需使用標籤控制 FSx 資源存取的詳細資訊，請參閱 使用標籤來控制對 Amazon FSx 資源的存取。

使用標籤來控制對 Amazon FSx 資源的存取

若要控制對 Amazon FSx 資源和動作的存取，您可以根據標籤使用 AWS Identity and Access Management (IAM) 政策。您可以透過兩個方式提供控制：

1. 根據這些資源上的標籤控制對 Amazon FSx 資源的存取。
2. 控制您可以在 IAM 請求條件中傳遞哪些標籤。

如需有關如何使用標籤來控制 AWS 資源存取的資訊，請參閱《IAM 使用者指南》中的使用標籤控制存取。如需在建立時標記 Amazon FSx 資源的詳細資訊，請參閱 在建立期間授予標籤資源的許可。如需標記資源的詳細資訊，請參閱 標記 Amazon FSx 資源。

根據資源的標籤控制存取

若要控制使用者或角色可以在 Amazon FSx 資源上執行的動作，您可以在資源上使用標籤。例如，您可能想要根據資源上標籤的金鑰值組，允許或拒絕檔案系統資源上的特定 API 操作。

Example 政策 – 提供特定標籤時在 上建立檔案系統

此政策僅允許使用者在以特定標籤索引鍵值對標記檔案系統時建立檔案系統，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 政策 – 僅建立具有特定標籤的 Amazon FSx 檔案系統的備份

此政策允許使用者僅建立以金鑰值對 標記的檔案系統的備份`key=Department, value=Finance`，並使用標籤 建立備份`Deparment=Finance`。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
            "Condition": {
                "StringEquals": {
```

```
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example 政策 – 從具有特定標籤的備份建立具有特定標籤的檔案系統

此政策允許使用者建立Department=Finance僅從使用 標記的備份加上 標記的檔案系統Department=Finance。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateFileSystemFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateFileSystemFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example 政策 – 刪除具有特定標籤的檔案系統

此政策允許使用者僅刪除以 標記的檔案系統Department=Finance。如果他們建立最終備份，則必須使用 標記Department=Finance。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteFileSystem"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

針對 FSx for Windows File Server 使用服務連結角色

Amazon FSx for Windows File Server 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是一種獨特的 IAM 角色類型，可直接連結至 FSx for Windows File Server。服務連結角色由 FSx for Windows File Server 預先定義，並包含該服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓您更輕鬆地設定 FSx for Windows File Server，因為您不必手動新增必要的許可。FSx for Windows File Server 會定義其服務連結角色的許可，除非另有定義，否則只有 FSx for Windows File Server 可以擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

您必須先刪除服務連結角色的相關資源，才能將其刪除。這可保護您的 FSx for Windows File Server 資源，因為您不會不小心移除存取資源的許可。

如需關於支援服務連結角色的其他服務的資訊，請參閱可搭配 IAM 運作的AWS 服務，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (是) 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

FSx for Windows File Server 的服務連結角色許可

FSx for Windows File Server 使用名為 的服務連結角色 `AWSServiceRoleForAmazonFSx` – 在您的帳戶中執行特定動作，例如在您的 VPC 中為您的檔案系統建立彈性網路界面。

角色許可政策允許 FSx for Windows File Server 在所有適用的 AWS 資源上完成下列動作：

您無法將 AmazonFSxServiceRolePolicy 連接至 IAM 實體。此政策會連接到服務連結角色，允許 FSx 代表您管理 AWS 資源。如需詳細資訊，請參閱針對 FSx for Windows File Server 使用服務連結角色。

如需更新此政策，請參閱「AmazonFSxServiceRolePolicy」。

此政策會授予管理許可，允許 FSx 代表使用者管理 AWS 資源。

許可詳細資訊

AmazonFSxServiceRolePolicy 角色許可是由 AmazonFSxServiceRolePolicy AWS 受管政策所定義。AmazonFSxServiceRolePolicy 具有下列許可：

> **Note**
>
> 所有 Amazon FSx 檔案系統類型都會使用 AmazonFSxServiceRolePolicy；某些列出的許可可能不適用於 FSx for Windows。

- `ds` – 允許 FSx 檢視、授權和取消授權 Directory Service 目錄中的應用程式。
- `ec2` – 允許 FSx 執行下列動作：
  - 檢視、建立和取消關聯與 Amazon FSx 檔案系統相關聯的網路介面。
  - 檢視與 Amazon FSx 檔案系統相關聯的一或多個彈性 IP 地址。
  - 檢視與 Amazon FSx 檔案系統相關聯的 Amazon VPCs、安全群組和子網路。
  - 將 IPv6 地址指派給具有 `AmazonFSx.FileSystemId`標籤的客戶網路介面。
  - 從具有 `AmazonFSx.FileSystemId`標籤的客戶網路介面取消指派 IPv6 地址。
  - 為所有可與 VPC 搭配使用的安全群組提供增強型安全群組驗證。
  - 為 AWS授權使用者建立許可，以在網路界面上執行特定操作。
- `cloudwatch` – 允許 FSx 在 AWS/FSx 命名空間下將指標資料點發佈至 CloudWatch。
- `route53` – 允許 FSx 將 Amazon VPC 與私有託管區域建立關聯。
- `logs` – 允許 FSx 描述和寫入 CloudWatch Logs 日誌串流。如此一來，使用者可以將 FSx for Windows File Server 檔案系統的檔案存取稽核日誌傳送至 CloudWatch Logs 串流。
- `firehose` – 允許 FSx 描述和寫入 Amazon Data Firehose 交付串流。這是為了讓使用者可以將 FSx for Windows File Server 檔案系統的檔案存取稽核日誌發佈至 Amazon Data Firehose 交付串流。

JSON

```
{
```

```
    "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-*"
        }
    ]
}
```

此政策的任何更新都會在 中說明AWS 受管政策的 Amazon FSx 更新。

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的服務連結角色許可。

為 FSx for Windows File Server 建立服務連結角色

您不需要手動建立服務連結角色，當您在 AWS 管理主控台、IAM CLI 或 IAM API 中建立檔案系統時，FSx for Windows File Server 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，FSx for Windows File Server 會再次為您建立服務連結角色。

編輯 FSx for Windows File Server 的服務連結角色

FSx for Windows File Server 不允許您編輯服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的編輯服務連結角色。

刪除 FSx for Windows File Server 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 FSx for Windows File Server 服務在您嘗試刪除資源時正在使用 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 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。

FSx for Windows File Server 服務連結角色支援的區域

FSx for Windows File Server 支援在提供服務的所有區域中使用服務連結角色。如需詳細資訊，請參閱 AWS 區域與端點。

Amazon FSx for Windows File Server 的合規驗證

若要了解 AWS 服務 是否在特定合規計劃範圍內，請參閱AWS 服務 合規計劃範圍內然後選擇您感興趣的合規計劃。如需一般資訊，請參閱AWS 合規計劃。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載報告 in AWS Artifact

您使用 時的合規責任 AWS 服務 取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。如需使用 時合規責任的詳細資訊 AWS 服務，請參閱 AWS 安全文件。

Amazon FSx for Windows File Server 和介面 VPC 端點

您可以將 Amazon FSx 設定為使用介面 VPC 端點，以改善 VPC 的安全狀態。介面 VPC 端點採用 AWS PrivateLink技術，可讓您在沒有網際網路閘道、NAT 裝置、VPN 連接或 Direct Connect 連線的情況下私下存取 Amazon FSx APIs。VPC 中的執行個體不需要公有 IP 地址，即可與 Amazon FSx APIs 通訊。VPC 和 Amazon FSx 之間的流量不會離開 AWS 網路。

每個介面 VPC 端點由子網路中的一或多個彈性網路介面表示。網路介面提供私有 IP 地址，做為 Amazon FSx API 流量的進入點。Amazon FSx 支援使用IPv4-only和雙堆疊 (IPv4 和 IPv6) IP 地址類型設定的 VPC 端點。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的建立介面 VPC 端點。

Amazon FSx 介面 VPC 端點的考量事項

為 Amazon FSx 設定介面 VPC 端點之前，請務必檢閱《Amazon VPC 使用者指南》中的介面 VPC 端點屬性和限制。

您可以從 VPC 呼叫任何 Amazon FSx API 操作。例如，您可以從 VPC 內呼叫 CreateFileSystem API，以建立 FSx for Windows File Server 檔案系統。如需 Amazon FSx APIs 的完整清單，請參閱《Amazon FSx API 參考》中的動作。

VPC 對等互連考量

您可以使用 VPCs對等互連，透過介面 VPC 端點將其他 VPC 連接至 VPC。VPC 對等互連是兩個 VPC 之間的網路連線。您可以在自己的兩個 VPC 之間建立 VPCs 對等互連，或在另一個 VPC 中建立 VPC AWS 帳戶。VPCs 也可以位於兩個不同的 中 AWS 區域。

對等 VPCs之間的流量會保留在 AWS 網路上，而不會周遊公有網際網路。一旦 VPCs 對等互連，兩個 VPCs 中的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體等資源可以透過其中一個 VPCs 中建立的介面 VPC 端點來存取 Amazon FSx API。

為 Amazon FSx API 建立介面 VPC 端點

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface () 為 Amazon FSx API 建立 VPC 端點AWS CLI。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的建立介面 VPC 端點。

若要為 Amazon FSx 建立介面 VPC 端點，請使用下列其中一項：

- **com.amazonaws.*region*.fsx** – 建立 Amazon FSx API 操作的端點。
- **com.amazonaws.*region*.fsx-fips** – 為 Amazon FSx API 建立符合聯邦資訊處理標準 (FIPS) 140-2 的端點。

若要使用私有 DNS 選項，您必須設定 VPC 的 `enableDnsHostnames`和 `enableDnsSupport` 屬性。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的檢視和更新 VPC 的 DNS 支援。

AWS 區域 在中國除外，如果您為端點啟用私有 DNS，則可以使用 VPC 端點的預設 DNS 名稱向 Amazon FSx 提出 API 請求 AWS 區域，例如 `fsx.us-east-1.amazonaws.com`。對於中國（北京）和中國（寧夏）AWS 區域，您可以`fsx-api.cn-northwest-1.amazonaws.com.cn`分別使用 `fsx-api.cn-north-1.amazonaws.com.cn`和 使用 VPC 端點提出 API 請求。

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的透過介面 VPC 端點存取服務。

為 Amazon FSx 建立 VPC 端點政策

若要進一步控制對 Amazon FSx API 的存取，您可以選擇將 AWS Identity and Access Management (IAM) 政策連接至 VPC 端點。此政策會指定以下項目：

- 可執行動作的主體。
- 可執行的動作。
- 可對其執行動作的資源。

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。

使用其他 服務

除了 Amazon CloudWatch AWS Identity and Access Management AWS CloudTrail、 和 AWS DataSync之外，適用於 Windows File Server 的 FSx 也會與下列項目整合 AWS 服務：

- Amazon WorkSpaces 應用程式 – WorkSpaces Applicationsis 是一種全受管應用程式串流服務，可讓使用者從任何地方立即存取其桌面應用程式。WorkSpaces 應用程式可管理託管和執行應用程式所需的 AWS 資源、自動擴展，以及隨需提供使用者存取權。了解如何為個別使用者建立持久性儲存，並使用 WorkSpaces 應用程式在 FSx for Windows File Server 檔案系統上與許多使用者共用儲存。如需詳細資訊，請參閱搭配使用 Amazon FSx 與 Amazon WorkSpaces 應用程式。
- Amazon Kendra – Amazon Kendra 是一種智慧型搜尋服務，使用自然語言處理和進階機器學習演算法傳回從資料搜尋問題的特定答案。使用 Amazon Kendra，您可以透過將多個資料儲存庫連接到索引，以及擷取和爬取文件，來建立統一的搜尋體驗。如需搭配 FSx for Windows File Server 使用 Amazon Kendra 的詳細資訊，請參閱 搭配 Amazon Kendra 使用 FSx for Windows File Server。

主題

搭配使用 Amazon FSx 與 Amazon WorkSpaces 應用程式

透過支援伺服器訊息區塊 (SMB) 通訊協定，Amazon FSx for Windows File Server 支援從 Amazon EC2、VMware Cloud on AWS、Amazon WorkSpaces 和 Amazon WorkSpaces 應用程式執行個體存取您的檔案系統。WorkSpaces 應用程式是全受管應用程式串流服務。您可以集中管理 WorkSpaces 應用程式上的桌面應用程式，並將其安全地交付到任何電腦上的瀏覽器。如需 WorkSpaces 應用程式的詳細資訊，請參閱 Amazon WorkSpaces 應用程式管理指南。如需有關如何簡化 Amazon WorkSpaces 應用程式映像和機群管理的說明，請參閱 AWS 部落格文章自動建立自訂 AppStream 2.0 Windows 映像。

下列程序說明如何使用 Amazon FSx 搭配 WorkSpaces 應用程式，為每個使用者提供個人持久性儲存，並提供共用資料夾，讓多個使用者可以存取常見檔案。

為每個使用者提供個人持久性儲存

您可以使用 Amazon FSx 為組織中的每個使用者提供 WorkSpaces 應用程式串流工作階段中唯一的儲存磁碟機。使用者將擁有僅存取其資料夾的許可。磁碟機會在串流工作階段開始時自動掛載，而新增至或更新至磁碟機的檔案會在串流工作階段之間自動保留。

您需要執行三個程序才能完成此任務。

使用 Amazon FSx 為網域使用者建立主資料夾

1. 建立 Amazon FSx 檔案系統。如需詳細資訊，請參閱Amazon FSx for Windows File Server 入門。
2. 檔案系統可用後，請為 Amazon FSx 檔案系統中的每個網域 WorkSpaces 應用程式使用者建立一個資料夾。以下範例使用 使用者的網域使用者名稱做為對應資料夾的名稱。這樣做意味著您可以建置檔案共享的 UNC 名稱，以便使用 Windows 環境變數 輕鬆映射`%username%`。
3. 將每個資料夾共用為共用資料夾。如需詳細資訊，請參閱建立、更新、移除檔案共用。

啟動加入網域的 WorkSpaces 應用程式映像建置器

1. 登入 WorkSpaces 應用程式主控台：https：//https://console.aws.amazon.com/appstream2
2. 從導覽功能表中選擇目錄組態，然後建立目錄組態物件。如需詳細資訊，請參閱《Amazon WorkSpaces 應用程式管理指南》中的搭配使用 Active Directory 與 WorkSpaces 應用程式。Amazon WorkSpaces
3. 選擇映像、映像建置器，然後啟動新的映像建置器。
4. 選擇先前在映像建置器啟動精靈中建立的目錄組態物件，將映像建置器加入您的 Active Directory 網域。
5. 在與 Amazon FSx 檔案系統相同的 VPC 中啟動映像建置器。請務必將映像建置器與加入 Amazon FSx 檔案系統的相同 AWS Managed Microsoft AD 目錄建立關聯。您與映像建置器建立關聯的 VPC 安全群組必須允許存取您的 Amazon FSx 檔案系統。
6. 一旦映像建置器可用，請連線至映像建置器，並使用網域管理員帳戶登入。
7. 安裝您的應用程式。

將 Amazon FSx 檔案共用與 WorkSpaces 應用程式連結

1. 在映像建置器中，使用下列命令建立批次指令碼，並將其存放在已知的檔案位置 （例如：C：\Scripts\map-fs.bat)。下列範例使用 S： 做為磁碟機代號，以映射 Amazon FSx 檔案系統上的共

用資料夾。您可以在此指令碼中使用 Amazon FSx 檔案系統的 DNS 名稱或與檔案系統相關聯的 DNS 別名，您可以從 Amazon FSx 主控台中的檔案系統詳細資訊檢視取得。

如果您使用的是檔案系統的 DNS 名稱：

```
@echo off
net use S: /delete
net use S: \\file-system-DNS-name\users\%username%
```

如果您使用的是與檔案系統相關聯的 DNS 別名：

```
@echo off
net use S: /delete
net use S: \\fqdn-DNS-alias\users\%username%
```

2. 開啟 PowerShell 提示並執行 `gpedit.msc`。
3. 從使用者組態選擇 Windows 設定，然後選擇登入。
4. 導覽至您在此程序的第一個步驟中建立的批次指令碼，然後選擇它。
5. 在電腦組態中，選擇 Windows 管理範本、系統，然後選擇群組政策。
6. 選擇政策設定登入指令碼延遲。啟用政策並減少 的時間延遲0。此設定有助於確保在使用者啟動串流工作階段時立即執行使用者登入指令碼。
7. 建立映像並將其指派給 WorkSpaces 應用程式機群。請確定您也將 WorkSpaces 應用程式機群加入您用於映像建置器的相同 Active Directory 網域。在 Amazon FSx 檔案系統所使用的相同 VPC 中啟動機群。您與機群建立關聯的 VPC 安全群組必須提供 Amazon FSx 檔案系統的存取權。
8. 使用 SAML SSO 啟動串流工作階段。若要連線至加入 Active Directory 的機群，請使用 SAML 供應商設定單一登入聯合。如需詳細資訊，請參閱《Amazon WorkSpaces 應用程式管理指南》中的使用 SAML 2.0 對 AppStream 2.0 的單一登入存取。
9. 您的 Amazon FSx 檔案共享會映射至串流工作階段中的 S： 磁碟機代號。

提供跨使用者的共用資料夾

您可以使用 Amazon FSx 為組織中的使用者提供共用資料夾。共用資料夾可用來維護所有使用者所需的常見檔案（例如，示範檔案、程式碼範例、指示手冊等）。

您需要執行三個程序才能完成此任務。

使用 Amazon FSx 建立共用資料夾

1. 建立 Amazon FSx 檔案系統。如需詳細資訊，請參閱Amazon FSx for Windows File Server 入門。
2. 根據預設，每個 Amazon FSx 檔案系統都包含共用資料夾，您可以使用地址 *file-system-DNS-name*\share 或 *fqdn-DNS-alias*\share 來存取。您可以使用預設共用或建立不同的共用資料夾。如需詳細資訊，請參閱建立、更新、移除檔案共用。

啟動 WorkSpaces 應用程式映像建置器

1. 從 WorkSpaces 應用程式主控台，啟動新的映像建置器或連線至現有的映像建置器。在 Amazon FSx 檔案系統所使用的相同 VPC 中啟動映像建置器。您與映像建置器建立關聯的 VPC 安全群組必須允許存取您的 Amazon FSx 檔案系統。
2. 一旦映像建置器可用，請以管理員使用者身分連線至映像建置器。
3. 以管理員身分安裝或更新您的應用程式。

將共用資料夾與 WorkSpaces 應用程式連結

1. 如先前程序所述建立批次指令碼，以便在使用者啟動串流工作階段時自動掛載共用資料夾。若要完成指令碼，您需要檔案系統的 DNS 名稱或與檔案系統相關聯的 DNS 別名（您可以從 Amazon FSx 主控台中的檔案系統詳細資訊檢視取得），以及存取共用資料夾的登入資料。

   如果您使用的是檔案系統的 DNS 名稱：

   ```
   @echo off
   net use S: /delete
   net use S: \\file-system-DNS-name\share /user:username password
   ```

   如果您使用的是與檔案系統相關聯的 DNS 別名：

   ```
   @echo off
   net use S: /delete
   net use S: \\fqdn-DNS-alias\share /user:username password
   ```

2. 建立群組政策，在每次使用者登入時執行此批次指令碼。您可以遵循上一節所述的相同指示。
3. 建立映像並將其指派給機群。

4. 啟動串流工作階段。您現在應該會看到共用資料夾自動映射至磁碟機代號。

搭配 Amazon Kendra 使用 FSx for Windows File Server

Amazon Kendra 是一種高度準確且智慧型的搜尋服務。FSx for Windows File Server 檔案系統可以用作 Amazon Kendra 的資料來源，可讓您索引和智慧搜尋存放在檔案系統中的文件所包含的資訊。

- 如需 Amazon Kendra 的詳細資訊，請參閱《Amazon Kendra 開發人員指南》中的什麼是 Amazon Kendra。
- 如需如何將檔案系統新增為 Amazon Kendra 資料來源的詳細資訊，請參閱《Amazon Kendra 開發人員指南》中的 Amazon FSx 資料來源（主控台）入門。
- 如需 Amazon Kendra 的概觀資訊，請參閱 Amazon Kendra 網站。
- 如需如何使用 Amazon Kendra 搜尋檔案系統的逐步解說，請參閱AWS Machine Learning部落格中的使用適用於 Amazon FSx for Windows File Server 的 Amazon Kendra 連接器在 Windows 檔案系統上安全地搜尋非結構化資料。

檔案系統效能

當您新增 FSx for Windows File Server 檔案系統做為資料來源時，Amazon Kendra 會以定期同步頻率編目檔案系統上的檔案和資料夾，以建立和維護其搜尋索引。（您可以在建立整合時選取同步頻率。）此來自 Amazon Kendra 的檔案存取活動會耗用檔案系統資源，類似於您自有工作負載存取檔案系統的活動。

確保您的檔案系統已設定足夠的資源，讓您的工作負載效能不受影響。具體而言，如果您打算為大量檔案編製索引，我們建議您使用具有 SSD 儲存類型的檔案系統，為需要存取儲存磁碟區的請求提供更高的最大輸送量和 IOPS 層級。如需 Amazon FSx 效能模型的詳細資訊，請參閱 FSx for Windows File Server 效能。

配額

接下來，您可以了解使用 Amazon FSx for Windows File Server 時的配額。

主題

您可以提高的配額

以下是 AWS 帳戶 AWS 區域每個您可以增加的 Amazon FSx for Windows File Server 配額。

資源	預設	描述
Windows 檔案系統	100	您可以在此帳戶中建立的 Amazon FSx for Windows Server 檔案系統數目上限。
Windows 輸送量容量	10240	此帳戶中所有 Amazon FSx for Windows 檔案系統允許的輸送量總容量 (MBps)。
Windows HDD 儲存容量	524288	此帳戶中所有 Amazon FSx for Windows File Server 檔案系統允許的 HDD 儲存容量上限（以 GiB 為單位）。
Windows SSD 儲存容量	524288	此帳戶中所有 Amazon FSx for Windows File Server 檔案系統允許的 SSD 儲存容量上限（以 GiB 為單位）。

資源	預設	描述
Windows SSD IOPS 總計	500,000	此帳戶中所有 Amazon FSx for Windows File Server 檔案系統允許的 SSD IOPS 總量。
Windows 備份	500	您在此帳戶中可以擁有的所有 Amazon FSx for Windows File Server 檔案系統的使用者啟動備份數量上限。

請求提高配額

1. 開啟 Service Quotas 主控台。
2. 在導覽窗格中，選擇 AWS services (AWS 服務)。
3. 選擇 Amazon FSx。
4. 選擇配額。
5. 選擇增加請求配額，然後依照指示請求增加配額。
6. 若要檢視配額請求的狀態，請在主控台導覽窗格中選擇配額請求歷史記錄。

如需詳細資訊，請參閱「Service Quotas 使用者指南」中的請求提高配額。

每個檔案系統的資源配額

以下是 中每個檔案系統的 Amazon FSx for Windows File Server 資源配額 AWS 區域。

資源	每個檔案系統的限制
標籤數量上限	50
自動備份的最長保留期間	90 天
每個帳戶的單一目的地區域正在進行的備份複製請求數量上限。	5
最低儲存容量、SSD 檔案系統	32 GiB

資源	每個檔案系統的限制
最低儲存容量、HDD 檔案系統	2，000 GiB
最大儲存容量、SSD 和 HDD	64 TiB
最低 SSD IOPS	96
SSD IOPS 上限	400,000
最小輸送量	8 MBps
最大輸送量	12，288 MBps
檔案共用數目上限	100,000

其他考量

此外，請注意下列事項：

- 您可以在最多 125 個 Amazon FSx 檔案系統上使用每個 AWS Key Management Service (AWS KMS) 金鑰。
- 如需 AWS 區域 可建立檔案系統的清單，請參閱 中的 Amazon FSx 端點和配額AWS 一般參考。
- 您可以將來自虛擬私有雲端 (VPC) 中 Amazon EC2 執行個體的檔案共用與其網域名稱服務 (DNS) 名稱進行映射。

Microsoft Windows 特定的配額

如需詳細資訊，請參閱 Microsoft Windows Dev Center 上的 NTFS 限制。

Amazon FSx 故障診斷

使用下列各節來協助您對 Amazon FSx 的問題進行疑難排解。

如果您在使用 Amazon FSx 時遇到以下未列出的問題，請嘗試在 Amazon FSx 論壇中提出問題。

主題

您無法存取您的檔案系統

有許多潛在原因導致無法存取您的檔案系統，每個系統都有自己的解決方案，如下所示。

主題

檔案系統彈性網路界面已修改或刪除

您不得修改或刪除檔案系統的彈性網路界面。修改或刪除網路界面可能會導致 VPC 和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 彈性網路介面。如需詳細資訊，請參閱使用 Amazon VPC 的檔案系統存取控制。

已刪除連接至檔案系統彈性網路界面的彈性 IP 地址

Amazon FSx 不支援從公有網際網路存取檔案系統。Amazon FSx 會自動分離任何彈性 IP 地址，這是可從網際網路連線的公有 IP 地址，連接到檔案系統的彈性網路界面。如需詳細資訊，請參閱存取您的資料。

檔案系統安全群組缺少必要的傳入或傳出規則。

檢閱 中指定的傳入規則Amazon VPC 安全群組，並確保與您檔案系統相關聯的安全群組具有對應的傳入規則。

運算執行個體的安全群組缺少必要的傳出規則

檢閱 中指定的傳出規則Amazon VPC 安全群組，並確認與運算執行個體相關聯的安全群組具有對應的傳出規則。

運算執行個體未加入 Active Directory

您的運算執行個體可能無法正確加入兩種 Active Directory 類型之一：

- 檔案系統加入的 AWS Managed Microsoft AD 目錄。
- 與目錄建立單向樹系信任關係的 AWS Managed Microsoft AD Microsoft Active Directory 目錄。

請確定您的運算執行個體已加入兩種目錄類型的其中之一。其中一種類型是檔案系統加入的 AWS Managed Microsoft AD 目錄。另一種類型是 Microsoft Active Directory 目錄，具有與 AWS Managed Microsoft AD 目錄建立的單向樹系信任關係。如需詳細資訊，請參閱搭配 使用 Amazon FSx AWS Directory Service for Microsoft Active Directory。

檔案共用不存在

您嘗試存取的 Microsoft Windows 檔案共用不存在。

如果您使用的是現有的檔案共享，請確定檔案系統 DNS 名稱和共享名稱已正確指定。若要管理您的檔案共享，請參閱 建立、更新、移除檔案共用。

Active Directory 使用者缺少必要的許可

您存取檔案共享的 Active Directory 使用者缺少必要的存取許可。

確定共用資料夾的檔案共用和 Windows 存取控制清單 ACLs) 的存取許可允許存取需要存取它的 Active Directory 使用者。

允許移除完全控制 NTFS ACL 許可

如果您在共用的資料夾上移除 SYSTEM 使用者的允許完全控制 NTFS ACL 許可，該共用可能會變得無法存取，而且從該時間點起取得的任何檔案系統備份可能無法使用。

您需要重新建立受影響的檔案共享。如需詳細資訊，請參閱建立、更新、移除檔案共用。重新建立資料夾或共用之後，您可以從運算執行個體映射並使用 Windows 檔案共用。

無法使用現場部署用戶端存取檔案系統

您使用 Direct Connect 或 VPN 從內部部署使用您的 Amazon FSx 檔案系統，並且使用內部部署用戶端的非私有 IP 地址範圍。

Amazon FSx 僅支援從在 2020 年 12 月 17 日之後建立的檔案系統上具有非私有 IP 地址的內部部署用戶端存取。

如果您需要使用非私有 IP 地址範圍存取 2020 年 12 月 17 日之前建立的 FSx for Windows File Server 檔案系統，您可以透過還原檔案系統的備份來建立新的檔案系統。如需詳細資訊，請參閱使用備份保護您的資料。

新的檔案系統未在 DNS 中註冊

對於加入自我管理 Active Directory 的檔案系統，Amazon FSx 不會在建立檔案系統 DNS 時註冊，因為客戶網路不使用 Microsoft DNS。

如果您的網路使用第三方 DNS 服務而非 Microsoft DNS，Amazon FSx 不會在 DNS 中註冊檔案系統。您必須手動設定 Amazon FSx 檔案系統的 DNS A 項目。對於單一可用區 1 檔案系統，您需要新增一個 DNS A 項目；對於單一可用區 2 和多可用區檔案系統，您需要新增兩個 DNS A 項目。使用下列程序取得手動新增 DNS A 項目時要使用的檔案系統 IP 地址。

1. 在 https://console.aws.amazon.com/fsx/ 中，選擇要取得 IP 地址的檔案系統，以顯示檔案系統詳細資訊頁面。
2. 在網路與安全索引標籤中，執行下列其中一項操作：

- 對於單一可用區 1 檔案系統：
  - 在子網路面板中，選擇網路界面下方顯示的彈性網路界面，以在 Amazon EC2 中開啟網路界面頁面。
  - 要使用的單一可用區 1 檔案系統的 IP 地址會顯示在主要私有 IPv4 IP 欄中。
- 對於單一可用區 2 或多可用區檔案系統：
  - 在偏好的子網路面板中，選擇網路界面下方顯示的彈性網路界面，以在 Amazon EC2 中開啟網路界面頁面。
  - 要使用之偏好子網路的 IP 地址會顯示在次要私有 IPv4 IP 欄中。
  - 在 Amazon FSx 待命子網路面板中，選擇網路界面下方顯示的彈性網路界面，以在 Amazon EC2 主控台中開啟網路界面頁面。
  - 要使用的待命子網路 IP 地址會顯示在次要私有 IPv4 IP 欄中。

無法使用 DNS 別名存取檔案系統

如果您無法使用 DNS 別名存取檔案系統，請使用下列程序對問題進行疑難排解。

1. 執行下列其中一個步驟，確認別名與檔案系統相關聯：

   a. 使用 Amazon FSx 主控台 – 選擇您嘗試存取的檔案系統。在檔案系統詳細資訊頁面上，DNS 別名會顯示在網路與安全索引標籤上。

   b. 使用 CLI 或 API – 使用 `describe-file-system-aliases` CLI 命令或 DescribeFileSystemAliases API 操作來擷取目前與檔案系統相關聯的別名。
2. 如果未列出 DNS 別名，您必須將其與檔案系統建立關聯。如需詳細資訊，請參閱管理現有檔案系統的 DNS 別名。
3. 如果 DNS 別名與檔案系統相關聯，請確認您已設定下列必要項目：

   - 建立與 Amazon FSx 檔案系統 Active Directory 電腦物件上 DNS 別名對應的服務主體名稱 (SPNs)。

     如需詳細資訊，請參閱設定 Kerberos 的服務主體名稱 (SPNs)。
   - 為解析為 Amazon FSx 檔案系統預設 DNS 名稱的 DNS 別名建立 DNS CNAME 記錄。

     如需詳細資訊，請參閱更新或建立 DNS CNAME 記錄。
4. 如果您建立了有效的 SPNs和 DNS CNAME 記錄，請確認用戶端的 DNS 具有解析為正確檔案系統的 DNS CNAME 記錄。

a. 執行 nslookup 以確認記錄存在，並解析為檔案系統的預設 DNS 名稱。

b. 如果 DNS CNAME 解析為另一個檔案系統，請等待用戶端的 DNS 快取重新整理，然後再次檢查 CNAME 記錄。您可以使用下列命令來排清用戶端的 DNS 快取，以加速程序。

```
ipconfig /flushdns
```

5. 如果 DNS CNAME 記錄解析為 Amazon FSx 檔案系統的預設 DNS，且用戶端仍然無法存取檔案系統，請參閱 您無法存取您的檔案系統 以取得其他故障診斷步驟。

無法使用 IP 地址存取檔案系統

如果您無法使用 IP 地址存取檔案系統，請嘗試改用 DNS 名稱或相關聯的 DNS 別名。

您可以選擇 Windows File Server、Network & Security，在 Amazon FSx 主控台上尋找檔案系統的 DNS 名稱和任何相關聯的 DNS 別名。或者，您可以在 CreateFileSystem 或 DescribeFileSystems API 操作的回應中找到它們。如需使用 DNS 別名的詳細資訊，請參閱 管理 DNS 別名。

- 對於加入 AWS 受管 Microsoft Active Directory 的單一可用區檔案系統，DNS 名稱如下所示。

```
fs-0123456789abcdef0.ad-domain.com
```

- 對於加入自我管理 Active Directory 的所有多可用區域檔案系統和單一可用區域檔案系統，DNS 名稱如下所示。

```
amznfsxaa11bb22.ad-domain.com
```

建立新的 Amazon FSx 檔案系統失敗

當檔案系統建立請求失敗時，有許多潛在原因，如下節所述。

主題

- 設定錯誤的 VPC 安全群組和網路 ACLs
- 重複的檔案系統管理員群組名稱
- 無法連線 DNS 伺服器或網域控制站
- 無效的服務帳戶登入資料
- Amazon FSx 無法存取 中的 Active Directory 服務帳戶登入資料 AWS Secrets Manager

- 服務帳戶許可不足
- 超過服務帳戶容量
- Amazon FSx 無法存取組織單位 (OU)
- 服務帳戶無法存取管理員群組
- 網域中的 Amazon FSx 連線中斷
- 服務帳戶沒有正確的許可
- 用於建立參數的 Unicode 字元
- 在還原備份時切換儲存體類型至 HDD 失敗

設定錯誤的 VPC 安全群組和網路 ACLs

確保使用建議的安全群組組態來設定 VPC 安全群組和網路 ACLs。如需詳細資訊，請參閱建立安全群組。

重複的檔案系統管理員群組名稱

建立加入自我管理 Active Directory 的檔案系統失敗，並顯示下列錯誤訊息：

```
File system creation failed. Amazon FSx is unable to apply your Microsoft Active
 Directory configuration with the
specified file system administrators group. Please ensure that your Active Directory
 does not contain multiple domain
groups with the name: domain_group.
```

Amazon FSx 未建立檔案系統，因為網域中有多個管理員群組具有相同的名稱。

如果您未指定群組名稱，Amazon FSx 會嘗試使用預設值「網域管理員」做為管理員群組。如果有一個以上的群組使用預設的「網域管理員」名稱，則請求將會失敗。

使用下列步驟來解決問題。

1. 檢閱將檔案系統加入自我管理 Active Directory 的先決條件。
2. 在建立加入自我管理 Active Directory 的 FSx for Windows File Server 檔案系統之前，請使用 Amazon FSx Active Directory 驗證工具來驗證您的自我管理 Active Directory 組態。
3. 使用 AWS 管理主控台 或 建立新的檔案系統 AWS CLI。如需詳細資訊，請參閱將 Amazon FSx 檔案系統加入自我管理的 Microsoft Active Directory 網域。
4. 針對自我管理 Active Directory，提供網域中唯一的檔案系統管理員群組名稱。

無法連線 DNS 伺服器或網域控制站

建立加入自我管理 Active Directory 的檔案系統失敗，並顯示下列錯誤訊息：

```
Amazon FSx can't reach the DNS servers provided or the domain controllers for your
 self-managed directory in Microsoft Active Directory.
File system creation failed. Amazon FSx is unable to communicate with your Microsoft
 Active Directory domain controllers.
This is because Amazon FSx can't reach the DNS servers provided or domain controllers
 for your domain.
To fix this problem, delete your file system and create a new one with valid DNS
 servers and networking configuration that allows
traffic from the file system to the domain controller.
```

使用下列步驟來疑難排解和解決問題。

1. 確認您已遵循在建立 Amazon FSx 檔案系統的子網路與自我管理 Active Directory 之間建立網路連線和路由的先決條件。如需詳細資訊，請參閱先決條件。

   使用 Amazon FSx Active Directory 驗證工具來測試和驗證這些網路設定。

   > **Note**
   >
   > 如果您定義了多個 Active Directory 站點，請確保與 Amazon FSx 檔案系統相關聯的 VPC 中的子網路在 Active Directory 站點中定義，並且 VPC 中的子網路與其他站點中的子網路之間不存在 IP 衝突。您可以使用 Active Directory Sites and Services MMC 嵌入式檢視和變更這些設定。

2. 確認您已設定與 Amazon FSx 檔案系統相關聯的 VPC 安全群組，以及任何 VPC 網路 ACLs，以允許所有連接埠上的傳出網路流量。

   > **Note**
   >
   > 如果您想要實作最低權限，您只能允許傳出流量到與 Active Directory 網域控制站通訊所需的特定連接埠。如需詳細資訊，請參閱 Microsoft Active Directory 文件。

3. 確認 Microsoft Windows 檔案伺服器或網路管理屬性的值不包含non-Latin-1 字元。例如，如果您使用 `Domänen-Admins`做為檔案系統管理員群組的名稱，則檔案系統建立會失敗。
4. 確認 Active Directory 網域的 DNS 伺服器和網域控制站處於作用中狀態，並且能夠回應所提供網域的請求。

5. 請確定 Active Directory 網域的功能層級是 Windows Server 2008 R2 或更高版本。
6. 請確定 Active Directory 網域網域控制站上的防火牆規則允許來自 Amazon FSx 檔案系統的流量。如需詳細資訊，請參閱 Microsoft Active Directory 文件。

無效的服務帳戶登入資料

建立加入自我管理 Active Directory 的檔案系統失敗，並顯示下列錯誤訊息：

```
Amazon FSx is unable to establish a connection with your Microsoft Active Directory
 domain controllers
because the service account credentials provided are invalid. To fix this problem,
 delete your file
system and create a new one using a valid service account.
```

使用下列步驟來疑難排解和解決問題。

案例 1：如果您使用 AWS Secrets Manager 秘密來存放 Active Directory 登入資料

1. 檢閱 使用 存放 Active Directory 登入資料 AWS Secrets Manager。
2. 秘密 ARN 的 是正確的，並遵循正確的格式：`arn:aws:secretsmanager:region:account-id:secret:secret-name-6chars`。
3. 確認秘密包含具有非空白值的兩個必要欄位：
   - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME` – 您的 AD 服務帳戶使用者名稱。
   - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD` – 您的 AD 服務帳戶密碼。
4. 確認秘密和金鑰具有以資源為基礎的政策，授予 Amazon FSx 服務主體擷取秘密值的`fsx.amazonaws.com`許可。

案例 2：如果您使用純文字登入資料來加入 Active Directory

1. 確認您在自我管理 Active Directory 組態`ServiceAcct`中僅輸入使用者名稱做為服務帳戶使用者名稱的輸入，例如 。

> **Important**
>
> 輸入服務帳戶使用者名稱時，請勿包含網域字首 (`corp.com\ServiceAcct`) 或網域尾碼 (`ServiceAcct@corp.com`)。

輸入服務帳戶使用者名稱時，請勿使用辨別名稱 (DN) (CN=ServiceAcct，OU=example，DC=corp，DC=com)。

2. 確認您提供的服務帳戶存在於 Active Directory 網域中。
3. 請確定您已將所需的許可委派給您提供的服務帳戶。服務帳戶必須能夠在您加入檔案系統的網域中建立和刪除 OU 中的電腦物件。服務帳戶至少也需要具有執行下列動作的許可：

   - 重設密碼
   - 限制帳戶讀取和寫入資料
   - 驗證寫入 DNS 主機名稱的能力
   - 已驗證能夠寫入服務主體名稱

   如需建立具有正確許可之服務帳戶的詳細資訊，請參閱 Amazon FSx 服務帳戶。

Amazon FSx 無法存取 中的 Active Directory 服務帳戶登入資料 AWS Secrets Manager

下列各節說明常見問題以及如何解決這些問題。

將檔案系統加入自我管理 Active Directory 失敗，並顯示下列錯誤訊息：

```
You can't provide both username/password and a domain join service account
secret to connect to your Active Directory. Provide only one set of
credentials.
```

解決此問題

1. 選擇您要提供存放在 Secrets Manager 秘密還是純文字中的登入資料。
2. 加入 Active Directory 時，僅提供其中一個參數，不提供兩者。

將檔案系統加入自我管理 Active Directory 失敗，並顯示下列錯誤訊息：

```
The domain join service account secret ARN format you entered isn't
valid. Use the format: arn:partition:secretsmanager:region:account-
id:secret:secret-name-6chars
```

解決此問題

1. 檢閱 使用 存放 Active Directory 登入資料 AWS Secrets Manager。
2. 確認您輸入的 ARN 格式正確。正確的格式範例為 `arn:aws:secretsmanager:us-east-1:123456789012:secret:MyDatabaseSecret-Ab3d5f`。

將檔案系統加入自我管理 Active Directory 失敗，並顯示下列錯誤訊息：

```
Amazon FSx can't access the domain join service account secret [ARN]. Add a resource permission to the secret that grants the FSx service principal (fsx.amazonaws.com) permission to access it.
```

解決此問題

1. 檢閱 使用 存放 Active Directory 登入資料 AWS Secrets Manager。
2. 確認您提供的 Secrets Manager 秘密具有允許 Amazon FSx 使用秘密的正確政策。

將檔案系統加入自我管理 Active Directory 失敗，並顯示下列錯誤訊息：

```
You don't have permission to access the domain join service account secret [ARN]. A resource permission needs to be added to the secret to grant you access.
```

解決此問題

- Secrets Manager 秘密擁有者或管理員需要授予您的帳戶使用此秘密的存取權。如需詳細資訊，請參閱身分型政策。

將檔案系統加入自我管理 Active Directory 失敗，並顯示下列錯誤訊息：

```
The domain join service account secret format or content isn't valid. Make sure the secret includes both CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME and CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD fields with non-empty values.
```

解決此問題

1. 檢閱 使用 存放 Active Directory 登入資料 AWS Secrets Manager。
2. 確認您提供的 Secrets Manager 秘密具有兩個必要欄位。

服務帳戶許可不足

建立加入自我管理 Active Directory 的檔案系統失敗，並顯示下列錯誤訊息：

```
Amazon FSx is unable to establish a connection with your
Microsoft Active Directory domain controllers. This is because the service account
 provided does not
have permission to join the file system to the domain with the specified organizational
 unit.
To fix this problem, delete your file system and create a new one using a service
 account with
permission to join the file system to the domain with the specified organizational
 unit.
```

使用下列程序來疑難排解和解決問題。

- 請確定您已將所需的許可委派給您提供的服務帳戶。服務帳戶必須能夠在您加入檔案系統的網域中建立和刪除 OU 中的電腦物件。服務帳戶至少也需要具有執行下列動作的許可：
  - 重設密碼
  - 限制帳戶讀取和寫入資料
  - 驗證寫入 DNS 主機名稱的能力
  - 已驗證能夠寫入服務主體名稱

  如需建立具有正確許可之服務帳戶的詳細資訊，請參閱 Amazon FSx 服務帳戶。

超過服務帳戶容量

建立加入自我管理 Active Directory 的檔案系統失敗，並顯示下列錯誤訊息：

```
Amazon FSx can't establish a connection with your Microsoft Active Directory
domain controllers. This is because the service account provided has reached the
maximum number of computers that it can join to the domain. To fix this problem,
delete your file system and create a new one, supplying a service account that
is able to join new computers to the domain.
```

若要解決此問題，請確認您提供的服務帳戶已達到可加入網域的電腦數量上限。如果已達到上限，請建立具有正確許可的新服務帳戶。使用新的服務帳戶並建立新的檔案系統。如需詳細資訊，請參閱Amazon FSx 服務帳戶。

Amazon FSx 無法存取組織單位 (OU)

建立加入自我管理 Active Directory 的檔案系統失敗，並顯示下列錯誤訊息：

```
Amazon FSx can't establish a connection with your Microsoft Active Directory domain
 controller(s).
This is because the organizational unit you specified either doesn't exist or isn't
 accessible
to the service account provided. To fix this problem, delete your file system and
 create a new one specifying an
organizational unit to which the service account can join the file system.
```

使用下列步驟來疑難排解和解決問題。

1. 確認您提供的 OU 位於 Active Directory 網域中。
2. 請確定您已將所需的許可委派給您提供的服務帳戶。服務帳戶必須能夠在您加入檔案系統的網域中建立和刪除 OU 中的電腦物件。服務帳戶至少也需要具有執行下列動作的許可：

   - 重設密碼
   - 限制帳戶讀取和寫入資料
   - 驗證寫入 DNS 主機名稱的能力
   - 已驗證能夠寫入服務主體名稱
   - 委派控制來建立和刪除電腦物件
   - 驗證讀取和寫入帳戶限制的能力

   如需建立具有正確許可之服務帳戶的詳細資訊，請參閱 Amazon FSx 服務帳戶。

服務帳戶無法存取管理員群組

建立加入自我管理 Active Directory 的檔案系統失敗，並顯示下列錯誤訊息：

```
Amazon FSx is unable to apply your Microsoft Active Directory configuration. This is
 because the file system
administrators group you provided either doesn't exist or isn't accessible to the
 service account you
provided. To fix this problem, delete your file system and create a new one specifying
 a file
system administrators group in the domain that is accessible to the service account
```

```
provided.
```

使用下列步驟來疑難排解和解決問題。

1. 請確定您只提供群組的名稱做為管理員群組參數的字串。

   > **Important**
   >
   > 提供群組名稱參數時，請勿包含網域字首 (`corp.com\FSxAdmins`) 或網域尾碼 (`FSxAdmins@corp.com`)。
   > 請勿對群組使用辨別名稱 (DN)。辨別名稱的範例為 CN=FSxAdmins，OU=example，DC=corp，DC=com。

2. 確保提供的管理員群組與您要加入檔案系統的管理員位於相同的 Active Directory 網域中。
3. 如果您未提供管理員群組參數，Amazon FSx 會嘗試在您的 Active Directory 網域中使用`Builtin Domain Admins`群組。如果此群組的名稱已變更，或者您使用不同的群組進行網域管理，則需要為群組提供該名稱。

網域中的 Amazon FSx 連線中斷

建立加入自我管理 Active Directory 的檔案系統失敗，並顯示下列錯誤訊息：

```
Amazon FSx is unable to apply your Microsoft Active Directory configuration. To fix
 this problem, delete your file system and create a new one
meeting the pre-requisites described in the Amazon FSx user guide.
```

建立檔案系統時，Amazon FSx 能夠連線到 Active Directory 網域的 DNS 伺服器和網域控制站，並將檔案系統成功加入 Active Directory 網域。不過，在完成檔案系統建立時，Amazon FSx 失去與您網域中 或 成員資格的連線。使用下列步驟來疑難排解和解決問題。

1. 確保您的 Amazon FSx 檔案系統和 Active Directory 之間持續存在網路連線。此外，透過使用路由規則、VPC 安全群組規則、VPC 網路 ACLs 和網域控制站防火牆規則，確保網路流量在其之間持續受到允許。
2. 請確定 Amazon FSx 為您 Active Directory 網域中的檔案系統建立的電腦物件仍處於作用中狀態，且未被刪除或以其他方式操作。

服務帳戶沒有正確的許可

建立加入自我管理 Active Directory 的檔案系統失敗，並顯示下列錯誤訊息：

```
File system creation failed. Amazon FSx is unable to establish a connection with your
 Microsoft Active Directory domain controller(s).
This is because the service account provided does not have permission to join the file
 system to the domain with the specified
organizational unit (OU). To fix this problem, delete your file system and create a new
 one using a service account with permission
to create computer objects and reset passwords within the specified organizational
 unit.
```

請確定您已將所需的許可委派給您提供的服務帳戶。使用下列步驟來疑難排解和解決問題。

服務帳戶至少需要具有下列許可：

- 受委派控制，以建立和刪除您聯結檔案系統的目標 OU 中的電腦物件
- 在您加入檔案系統的 OU 中擁有下列許可：
  - 能夠重設密碼
  - 能夠限制帳戶讀取和寫入資料
  - 驗證寫入 DNS 主機名稱的能力
  - 已驗證能夠寫入服務主體名稱
  - 能夠（可委派）建立和刪除電腦物件
  - 驗證讀取和寫入帳戶限制的能力
  - 修改許可的能力

  如需建立具有正確許可之服務帳戶的詳細資訊，請參閱 Amazon FSx 服務帳戶。

用於建立參數的 Unicode 字元

建立加入自我管理 Active Directory 的檔案系統失敗，並顯示下列錯誤訊息：

```
File system creation failed. Amazon FSx is unable to create a file system within the
 specified
Microsoft Active Directory. To fix this problem, please delete your file system and
 create a new one
meeting the pre-requisites described in the FSx for ONTAP User Guide.
```

Amazon FSx 不支援 Unicode 字元。確認沒有任何建立參數具有 Unicode 字元，例如重音標記。這包括可保留空白的參數，其中會自動填入預設值。請確定 Active Directory 中的對應預設值也不包含 Unicode 字元。

在還原備份時切換儲存體類型至 HDD 失敗

從備份建立檔案系統失敗，並顯示下列錯誤訊息：

```
Switching storage type to HDD while creating a file system from backup backup_id is not supported because a storage scaling activity was still under way on the source file system to increase storage capacity from less than 2000 GiB when the backup backup_id was taken, and the minimum storage capacity for HDD storage is 2000 GiB.
```

還原備份時發生此問題，而且您已將儲存類型從 SSD 變更為 HDD。從備份還原失敗，因為在原始檔案系統上儲存容量增加時，已進行您還原的備份。在增加請求之前，檔案系統的 SSD 儲存容量小於 2000 GiB，這是建立 HDD 檔案系統所需的最低儲存容量。

請使用下列程序來解決此問題。

1. 等待儲存容量增加請求完成，且檔案系統至少具有 2000 GiB 的 SSD 儲存容量。如需詳細資訊，請參閱監控儲存容量增加。
2. 對檔案系統進行使用者啟動的備份。如需詳細資訊，請參閱使用使用者啟動的備份。
3. 使用 HDD 儲存將使用者啟動的備份還原至新的檔案系統。如需詳細資訊，請參閱將備份還原至新的檔案系統。

檔案系統處於設定錯誤狀態

由於 Active Directory 環境中的變更，FSx for Windows File Server 檔案系統可能會進入設定錯誤的狀態。在此狀態下，您的檔案系統目前無法使用，或有失去可用性的風險，而且備份可能無法成功。

設定錯誤狀態包含錯誤訊息，以及您可以使用 Amazon FSx 主控台、API 或 存取的建議修正動作 AWS CLI。採取修正動作後，請確認檔案系統的狀態最終會變更為 `Available`- 請注意，此變更可能需要幾分鐘才能完成。

您的檔案系統可能會因多種原因而進入設定錯誤狀態，例如：

- DNS 伺服器 IP 地址不再有效。
- 服務帳戶登入資料不再有效，或缺少必要的許可。

- 由於網路連線問題，例如無效的 VPC 安全群組、VPC 網路 ACL 或路由表組態，或網域控制器防火牆設定，無法連線到 Active Directory 網域控制器。

> **Important**
>
> 建立檔案系統後，請勿移動 Amazon FSx 在 OU 中建立的電腦物件。這樣做會導致您的檔案系統設定錯誤。

（如需 Active Directory 需求的完整清單，請參閱 先決條件。 您也可以使用 Amazon FSx Active Directory 驗證工具，驗證 Active Directory 環境是否已正確設定以符合這些要求。）

解決其中一些問題需要直接更新檔案系統 Active Directory 組態中的一或多個參數，例如變更 DNS 伺服器 IP 地址，或變更服務帳戶使用者名稱或密碼。在這些情況下，您的修正動作必然涉及使用 Amazon FSx 主控台、API 或 AWS CLI 來更新所需的組態參數。

其他問題可能不需要變更任何 Active Directory 組態參數，例如變更網域控制器防火牆設定或 VPC 安全群組。不過，在這些情況下，您將需要採取進一步的動作，檔案系統才能成為 `Available`。確保 Active Directory 環境設定正確後，請在 Amazon FSx 主控台中選取錯誤設定狀態旁的嘗試復原按鈕，或在 Amazon FSx 主控台、API 或 中使用 `StartMisconfiguredStateRecovery`命令 AWS CLI。

主題

設定錯誤的檔案系統：Amazon FSx 無法連接網域的 DNS 伺服器或網域控制站。

當 Amazon FSx 無法與您的 Microsoft Active Directory 網域控制站或控制站通訊時，檔案系統將進入 `Misconfigured` 狀態。

若要解決這種情況，請執行下列動作：

1. 請確定您的聯網組態允許從檔案系統到網域控制器的流量。
2. 使用 Amazon FSx Active Directory 驗證工具來測試和驗證自我管理 Active Directory 的網路設定。如需詳細資訊，請參閱使用自我管理的 Microsoft Active Directory。
3. 在 Amazon FSx 主控台中檢閱檔案系統的自我管理 Active Directory 組態。
4. 若要更新檔案系統的自我管理 Active Directory 組態，您可以使用 Amazon FSx 主控台。

   a. 在導覽窗格中，選擇檔案系統，然後選擇要更新的檔案系統；檔案系統詳細資訊頁面隨即出現。

   b. 在檔案系統詳細資訊頁面上，選擇網路和安全性索引標籤上的更新。

   您也可以使用 Amazon FSx CLI `update-file-system`命令或 API 操作 UpdateFileSystem。

設定錯誤的檔案系統：服務帳戶登入資料無效

Amazon FSx 無法與您的 Microsoft Active Directory 網域控制站或控制站建立連線。這是因為所提供的服務帳戶登入資料無效。如需詳細資訊，請參閱使用自我管理的 Microsoft Active Directory。

若要解決組態錯誤，請執行下列動作：

1. 確認您使用的是正確的服務帳戶，而且您使用該帳戶的正確登入資料。
2. 然後使用 Amazon FSx 主控台，使用正確的服務帳戶或帳戶登入資料更新檔案系統的組態。

   a. 在導覽窗格中，選擇檔案系統，然後選擇設定錯誤的檔案系統進行更新。

   b. 在檔案系統詳細資訊頁面上，選擇網路和安全性索引標籤中的更新。

   您也可以使用 Amazon FSx API 操作 `update-file-system`。若要進一步了解，請參閱《Amazon FSx API 參考》中的 UpdateFileSystem。

設定錯誤的檔案系統：未正確設定 AWS Secrets Manager 秘密或 KMS 金鑰

Amazon FSx 無法與您的 Microsoft Active Directory 網域控制站或控制站建立連線。這是因為您的 AWS Secrets Manager 秘密 AWS KMS key 或未正確設定。如需詳細資訊，請參閱使用 存放 Active Directory 登入資料 AWS Secrets Manager。

若要解決組態錯誤，請執行下列動作：

1. 驗證秘密 ARN 是否正確，並遵循正確的格式：`arn:aws:secretsmanager:region:account-id:secret:secret-name-6chars`。
2. 確認秘密包含具有非空白值的兩個必要欄位：
   - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME` – 您的 AD 服務帳戶使用者名稱。
   - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD` – 您的 AD 服務帳戶密碼。
   - 確認秘密和金鑰具有以資源為基礎的政策，授予 Amazon FSx 服務主體擷取秘密值的`fsx.amazonaws.com`許可。

設定錯誤的檔案系統：提供的服務帳戶沒有將檔案系統加入網域的許可

Amazon FSx 無法建立與 Microsoft Active Directory 網域控制站的連線。這是因為提供的服務帳戶沒有使用指定 OU 將檔案系統加入網域的許可。

若要解決組態錯誤，請執行下列動作：

1. 將所需的許可新增至 Amazon FSx 服務帳戶，或建立具有所需許可的新服務帳戶。如需執行此操作的詳細資訊，請參閱 Amazon FSx 服務帳戶。
2. 然後使用新的服務帳戶憑證更新檔案系統的自我管理 Active Directory 組態。若要更新組態，您可以使用 Amazon FSx 主控台。
   a. 在導覽窗格中，選擇檔案系統，然後選擇要更新的檔案系統；檔案系統詳細資訊頁面隨即出現。
   b. 在檔案系統詳細資訊頁面上，選擇網路和安全性索引標籤上的更新。

   您也可以使用 Amazon FSx API 操作 `update-file-system`。若要進一步了解，請參閱《Amazon FSx API 參考》中的 UpdateFileSystem。

設定錯誤的檔案系統：服務帳戶無法再將任何電腦加入網域

Amazon FSx 無法建立與 Microsoft Active Directory 網域控制站的連線。在此情況下，這是因為提供的服務帳戶已達到可加入網域的電腦數量上限。

若要解決組態錯誤，請執行下列動作：

1. 識別另一個服務帳戶或建立新的服務帳戶，以將新電腦加入網域。

2. 然後使用 Amazon FSx 主控台，使用新的服務帳戶登入資料更新檔案系統的自我管理 Active Directory 組態。

   a. 在導覽窗格中，選擇檔案系統，然後選擇要更新的檔案系統；檔案系統詳細資訊頁面隨即出現。
   b. 在檔案系統詳細資訊頁面上，選擇網路和安全性索引標籤上的更新。

   您也可以使用 Amazon FSx API 操作 `update-file-system`。若要進一步了解，請參閱《Amazon FSx API 參考》中的 UpdateFileSystem。

設定錯誤的檔案系統：服務帳戶無法存取 OU

Amazon FSx 無法建立與 Microsoft Active Directory 網域控制站的連線，因為提供的服務帳戶無法存取指定的 OU。

若要解決組態錯誤，請執行下列動作：

1. 識別另一個服務帳戶或建立新的可存取 OU 的服務帳戶。
2. 然後使用新的服務帳戶憑證更新檔案系統的自我管理 Active Directory 組態。

   a. 在導覽窗格中，選擇檔案系統，然後選擇要更新的檔案系統；檔案系統詳細資訊頁面隨即出現。
   b. 在檔案系統詳細資訊頁面上，選擇網路和安全性索引標籤上的更新。

   您也可以使用 Amazon FSx API 操作 `update-file-system`。若要進一步了解，請參閱《Amazon FSx API 參考》中的 UpdateFileSystem。

您無法在多可用區或單一可用區 2 檔案系統上設定 DFS-R

多可用區域和單一可用區域 2 檔案系統不支援 Microsoft 分散式檔案系統複寫 (DFS-R)。

多可用區域檔案系統已設定為原生跨多個存取區域的備援。使用異地同步備份部署類型，在多個可用區域中實現高可用性。如需詳細資訊，請參閱可用性和耐久性：單一可用區和多可用區檔案系統。

儲存或輸送量容量更新失敗

檔案系統儲存和輸送量容量更新請求失敗有許多潛在原因，每個請求都有自己的解決方案。

儲存容量增加失敗，因為 Amazon FSx 無法存取檔案系統的 AWS KMS key

儲存容量增加請求失敗，因為 Amazon FSx 無法存取用來加密檔案系統的 KMS 金鑰。

您需要確保 Amazon FSx 可以存取用來加密檔案系統的 KMS 金鑰，以執行管理動作。使用下列資訊來解決金鑰存取問題。

- 如果已刪除 KMS 金鑰，則使用已刪除 KMS 金鑰的檔案系統和其任何備份將無法復原。如需詳細資訊，請參閱AWS KMS key《 開發人員指南》中的刪除 。 AWS Key Management Service
- 如果 KMS 金鑰已停用，且它是客戶受管金鑰，您將需要重新啟用它，然後重試儲存容量增加請求。如需詳細資訊，請參閱《 AWS Key Management Service 開發人員指南》中的啟用和停用金鑰。
- 如果金鑰因為待刪除而無效，您必須在金鑰仍處於 `PendingDeletion` 狀態時取消金鑰刪除。一旦 KMS 金鑰為 ，您可以重試請求`Enabled`。
- 如果金鑰因為待匯入而無效，您必須等到匯入完成，然後重試儲存增加請求。
- 如果超過金鑰的授予限制，您必須請求增加金鑰的授予數量。如需詳細資訊，請參閱《 AWS Key Management Service 開發人員指南》中的資源配額。授予配額增加時，請重試儲存增加請求。

儲存或輸送量容量更新失敗，因為自我管理 Active Directory 設定錯誤

儲存容量或輸送量容量更新請求失敗，因為您檔案系統的自我管理 Active Directory 處於設定錯誤的狀態。

若要解決特定設定錯誤的狀態，請參閱 檔案系統處於設定錯誤狀態。

由於輸送量容量不足，儲存容量增加失敗

儲存容量增加請求失敗，因為檔案系統的輸送量容量設定為 8 MBps。

將檔案系統的輸送量容量增加到至少 16 MBps，然後重試請求。如需詳細資訊，請參閱管理輸送量容量。

傳輸量容量更新至 8 MBps 失敗

將檔案系統的輸送量容量修改為 8 MBps 的請求失敗。

當儲存容量增加請求處於待定狀態或進行中時，可能會發生這種情況。增加儲存容量需要至少 16 MBps 的輸送量。等待儲存容量增加請求完成，然後重試輸送量容量修改請求。

文件歷史記錄

- API 版本：2018-03-01
- 文件最近更新時間：2025 年 9 月 30 日

下表說明 Amazon FSx Windows 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
新增 AWS Secrets Manager 整合的支援	Amazon FSx 現在與 整合，AWS Secrets Manager 以增強 Active Directory 憑證的管理。如需詳細資訊，請參閱使用 存放 Active Directory 登入 AWS Secrets Manager資料。	2025 年 11 月 5 日
AmazonFSxConsoleFullAccess – 更新現有政策	Amazon FSx 新增了新的許可 `secretsmanager:ListSecrets` ，允許主體在中列出秘密 AWS Secrets Manager ，以選取網域加入服務帳戶憑證。如需詳細資訊，請參閱 AWS 受管政策：AmazonFSxFullAccess。	2025 年 11 月 5 日
新增網際網路通訊協定第 6 版 (IPv6) 的支援	FSx for Windows File Server 檔案系統現在支援兩種網路類型選項：IPv4-only和雙堆疊 （適用於 IPv4 和 IPv6)。建立檔案系統時，您必須指定其中一個選項。您可以隨時變更現有 FSx for Windows File Server 檔案系統的網路類型。如需詳細資訊，請參閱管理網路類型。	2025 年 9 月 30 日

Amazon FSx 已更新 AmazonFSxServiceRolePolicy AWS 受管政策	Amazon FSx 已將 `ec2:AssignIpv6Addresses` 和 `ec2:UnassignIpv6Addresses` 許可新增至 AmazonFSxServiceRolePolicy。如需詳細資訊，請參閱 AmazonFSxServiceRolePolicy。	2025 年 7 月 22 日
Amazon FSx 已更新 AmazonFSxFullAccess AWS 受管政策	AmazonFSxFullAccess 受管政策已更新，以新增 `fsx:CreateAndAttachS3AccessPoint`、`fsx:DescribeS3AccessPointAttachments` 和 `fsx:DetachAndDeleteS3AccessPoint` 許可。	2025 年 6 月 25 日
Amazon FSx 已更新 AmazonFSxConsoleFullAccess AWS 受管政策	AmazonFSxConsoleFullAccess 受管政策已更新，以新增 `fsx:CreateAndAttachS3AccessPoint`、`fsx:DescribeS3AccessPointAttachments` 和 `fsx:DetachAndDeleteS3AccessPoint` 許可。	2025 年 6 月 25 日
Amazon FSx 已更新 AmazonFSxConsoleReadOnlyAccess AWS 受管政策	Amazon FSx 已更新 AmazonFSxConsoleReadOnlyAccess 政策來新增`ec2:DescribeNetworkInterfaces` 許可。如需詳細資訊，請參閱 AmazonFSxConsoleReadOnlyAccess 政策。	2025 年 2 月 25 日

新增對 Amazon FSx 雙堆疊 VPC 介面端點的支援	您現在可以使用 IPv4 和 IPv6 IP 地址和 DNS 名稱為 Amazon FSx 建立雙堆疊 VPC 介面端點。如需詳細資訊，請參閱 FSx for Windows File Server 和界面 VPC 端點。	2025 年 2 月 7 日
新增對雙堆疊 API 端點的支援	用於建立和管理檔案系統的 Amazon FSx 服務 API 具有新的雙堆疊端點。如需詳細資訊，請參閱《Amazon FSx API 參考》中的 API 端點。	2025 年 2 月 7 日
Amazon FSx 已更新 AmazonFSxConsoleFullAccess AWS 受管政策	Amazon FSx 已更新 AmazonFSxConsoleFullAccess 政策以新增`ec2:DescribeNetworkInterfaces` 許可。如需詳細資訊，請參閱 AmazonFSxConsoleFullAccess 政策。	2025 年 2 月 7 日
FSx for Windows File Server Active Directory 驗證工具的更新版本	FSx for Windows File Server Active Directory 驗證工具的更新版本已推出。如需詳細資訊，請參閱驗證 Active Directory 組態	2024 年 11 月 6 日

在輸送量容量為 4 GBps 或更高的檔案系統上新增了更高層級 IOPS 的支援	對於輸送量容量為 4 GBps 或更高的檔案系統，FSx for Windows File Server 會將最大 IOPS 從 130K 增加到 150K，對於輸送量容量為 6 GBps或更高的檔案系統，從 175K 增加到 200K，對於輸送量容量為 9 GBps或更高的檔案系統，從 260K 增加到 300K，對於輸送量容量為 12 GBps或更高的檔案系統，從 350K 增加到 400K。如需詳細資訊，請參閱 FSx for Windows File Server 效能。	2024 年 1 月 17 日
Amazon FSx 已更新 AmazonFSxFullAccess、AmazonFSxConsoleFullAccess、AmazonFSxReadOnlyAccess、AmazonFSxConsoleReadOnlyAccess 和 AmazonFSxServiceRolePolicy AWS 受管政策	Amazon FSx 已更新 AmazonFSxFullAccess、AmazonFSxConsoleFullAccess、AmazonFSxReadOnlyAccess、AmazonFSxConsoleReadOnlyAccess 和 AmazonFSxServiceRolePolicy 政策以新增`ec2:GetSecurityGroupsForVpc` 許可。如需詳細資訊，請參閱 Amazon FSx AWS 受管政策的更新。	2024 年 1 月 9 日

Amazon FSx 已更新 AmazonFSxFullAccess 和 AmazonFSxConsoleFullAccess AWS 受管政策	Amazon FSx 已更新 AmazonFSxFullAccess 和 AmazonFSxConsoleFullAccess 政策來新增`ManageCrossAccountDataReplication` 動作。如需詳細資訊，請參閱 Amazon FSx AWS 受管政策的更新。	2023 年 12 月 20 日
Amazon FSx 已更新 AmazonFSxFullAccess 和 AmazonFSxConsoleFullAccess AWS 受管政策	Amazon FSx 已更新 AmazonFSxFullAccess 和 AmazonFSxConsoleFullAccess 政策以新增`fsx:CopySnapshotAndUpdateVolume` 許可。如需詳細資訊，請參閱 Amazon FSx AWS 受管政策的更新。	2023 年 11 月 26 日
Amazon FSx 已更新 AmazonFSxFullAccess 和 AmazonFSxConsoleFullAccess AWS 受管政策	Amazon FSx 已更新 AmazonFSxFullAccess 和 AmazonFSxConsoleFullAccess 政策，以新增 `fsx:DescribeSharedVPCConfiguration` 和 `fsx:UpdateSharedVPCConfiguration` 許可。如需詳細資訊，請參閱 Amazon FSx AWS 受管政策的更新。	2023 年 11 月 14 日
新增更新檔案系統儲存類型的支援	FSx for Windows File Server 檔案系統現在支援從 HDD 儲存類型更新為 SSD 儲存類型。如需詳細資訊，請參閱管理儲存類型。	2023 年 8 月 9 日

新增對更高最大輸送量容量的支援	FSx for Windows File Server 檔案系統現在支援高達 12 GBps 的輸送量。如需詳細資訊，請參閱 FSx for Windows File Server 效能。	2023 年 8 月 9 日
新增對 SSD IOPS 佈建的支援	FSx for Windows File Server 檔案系統現在支援獨立於儲存容量的 SSD IOPS 佈建，最高可達 350，000 IOPS。如需詳細資訊，請參閱管理 SSD IOPS。	2023 年 8 月 9 日
Amazon FSx 已更新 AmazonFSxServiceRolePolicy AWS 受管政策	Amazon FSx 已更新 AmazonFSxServiceRolePolicy 中的`cloudwatch:PutMetricData` 許可。如需詳細資訊，請參閱 AmazonFSxServiceRolePolicy。	2023 年 7 月 24 日
Amazon FSx 已更新 AmazonFSxFullAccess AWS 受管政策	Amazon FSx 已更新 AmazonFSxFullAccess 政策，以移除`fsx:*`許可並新增特定`fsx`動作。如需詳細資訊，請參閱 AmazonFSxFullAccess 政策。	2023 年 7 月 13 日
Amazon FSx 已更新 AmazonFSxConsoleFullAccess AWS 受管政策	Amazon FSx 已更新 AmazonFSxConsoleFullAccess 政策，以移除`fsx:*`許可並新增特定`fsx`動作。如需詳細資訊，請參閱 AmazonFSxConsoleFullAccess 政策。	2023 年 7 月 13 日

新增對 Amazon FSx for Windows File Server 新 CloudWatch 指標的支援	FSx for Windows File Server 現在提供額外的 CloudWatch 指標，可監控檔案伺服器和儲存磁碟區效能和容量使用量。如需詳細資訊，請參閱指標和維度。	2022 年 9 月 22 日
新增檔案系統效能警告的支援	當任何一組 CloudWatch 指標接近或跨預先決定的這些指標閾值時，Amazon FSx 現在會在效能和監控視窗中提供警告。每個警告也提供可行的建議，以改善檔案系統的效能。如需詳細資訊，請參閱效能警告和建議。	2022 年 9 月 22 日
新增增強型檔案系統效能監控的支援	適用於 FSx for Windows File Server 檔案系統的 Amazon FSx 主控台檔案系統監控儀表板包含新的摘要、儲存和效能區段。這些區段會顯示新 CloudWatch 指標的圖表，為您提供增強的效能監控。如需詳細資訊，請參閱使用 CloudWatch 監控指標。	2022 年 9 月 22 日
新增 AWS PrivateLink 介面 VPC 端點的支援。	您現在可以使用介面 VPC 端點從 VPC 存取 Amazon FSx API，而無需透過網際網路傳送流量。如需詳細資訊，請參閱 Amazon FSx 和界面 VPC 端點。	2022 年 4 月 5 日

新增對 Amazon Kendra 的支援	您現在可以使用 FSx for Windows File Server 檔案系統做為 Amazon Kendra 的資料來源，讓您可以索引和搜尋存放在檔案系統上文件中的資訊。如需詳細資訊，請參閱搭配使用 FSx for Windows File Server 與 Amazon Kendra。	2022 年 3 月 26 日
新增對檔案存取稽核的支援	您現在可以在檔案、資料夾和檔案共享上啟用最終使用者存取的稽核。您可以選擇將稽核事件日誌傳送至 Amazon CloudWatch Logs 或 Amazon Data Firehose 服務。如需詳細資訊，請參閱檔案存取稽核。	2021 年 6 月 8 日
新增複製備份的支援	您現在可以使用 Amazon FSx 將相同 AWS 帳戶中的備份複製到另一個 AWS 區域（跨區域複本）或相同 AWS 區域（區域內複本）。如需詳細資訊，請參閱複製備份。	2021 年 4 月 12 日
自動增加檔案系統的儲存容量	使用 AWS開發的可自訂 CloudFormation 範本，在其容量達到您指定的閾值時，自動增加檔案系統的儲存容量。如需詳細資訊，請參閱動態增加儲存容量。	2021 年 2 月 17 日

新增使用非私有 IP 地址存取用戶端的支援	您可以使用非私有 IP 地址，透過內部部署用戶端存取 FSx for Windows File Server 檔案系統。如需詳細資訊，請參閱支援的環境。您可以使用使用非私有 IP 地址的 DNS 伺服器和 AD 網域控制站，將 FSx for Windows File Server 檔案系統加入自我管理的 Microsoft Active Directory。如需詳細資訊，請參閱搭配您的自我管理 Microsoft Active Directory 使用 Amazon FSx。	2020 年 12 月 17 日
新增使用 DNS 別名的支援	您現在可以將 DNS 別名與 FSx for Windows File Server 檔案系統建立關聯，以便用來存取檔案系統上的資料。如需詳細資訊，請參閱管理 DNS 別名和逐步解說 5：使用 DNS 別名存取您的檔案系統。	2020 年 11 月 9 日
新增對 Amazon Elastic Container Service 的支援	您現在可以將 FSx for Windows File Server 與 Amazon ECS 搭配使用。如需詳細資訊，請參閱支援的用戶端。	2020 年 11 月 9 日
Amazon FSx 現在已與 整合 AWS Backup	除了使用原生 Amazon FSx 備份之外 AWS Backup ，您現在可以使用 備份和還原 FSx 檔案系統。如需詳細資訊，請參閱搭配使用 AWS Backup 與 Amazon FSx。	2020 年 11 月 9 日

新增了輸送量容量擴展的支援	您現在可以隨著輸送量需求的變化，修改現有 FSx for Windows File Server 檔案系統的輸送量容量。如需詳細資訊，請參閱管理輸送量容量。	2020 年 6 月 1 日
新增儲存容量擴展的支援	您現在可以隨著儲存需求的變化，增加現有 FSx for Windows File Server 檔案系統的儲存容量。如需詳細資訊，請參閱管理儲存容量。	2020 年 6 月 1 日
新增硬碟 (HDD) 儲存的支援	HDD 儲存可讓您在使用 FSx for Windows File Server 時享有價格和效能彈性。如需詳細資訊，請參閱使用 Amazon FSx 最佳化成本。	2020 年 3 月 26 日
新增使用 傳輸檔案的支援 AWS DataSync	您現在可以使用 AWS DataSync 在 FSx for Windows File Server 之間傳輸檔案。如需詳細資訊，請參閱使用 AWS DataSync 將檔案遷移至 Amazon FSx for Windows File Server。	2020 年 2 月 4 日
FSx for Windows File Server 版本支援其他 Windows 檔案系統管理任務	您現在可以使用 Amazon FSx CLI 在 PowerShell 上進行遠端管理，來管理檔案共享、重複資料刪除、儲存配額和傳輸中加密。如需詳細資訊，請參閱管理檔案系統。	2019 年 11 月 20 日

FSx for Windows File Server 發行原生多可用區支援	您可以使用 FSx for Windows File Server 的異地同步備份部署，更輕鬆地建立跨多個可用區域 (AZs) 的高可用性檔案系統。如需詳細資訊，請參閱可用性和耐久性：單一可用區和異地同步備份檔案系統。	2019 年 11 月 20 日
FSx for Windows File Server 版本支援管理使用者工作階段和開啟檔案	您現在可以使用 Microsoft Windows 原生的共用資料夾工具，在 FSx for Windows File Server 檔案系統上管理使用者工作階段和開啟檔案。如需詳細資訊，請參閱管理使用者工作階段和開啟檔案。	2019 年 10 月 17 日
Amazon FSx 版本支援 Microsoft Windows 影子複本	您現在可以在 FSx for Windows File Server 檔案系統上設定 Windows 陰影複本。陰影副本可讓您的使用者輕鬆復原檔案變更，並透過將檔案還原至先前的版本來比較檔案版本。如需詳細資訊，請參閱使用陰影複本。	2019 年 7 月 31 日
Amazon FSx 發行共用的 Microsoft Active Directory 支援	您現在可以將 FSx for Windows File Server 檔案系統加入到位於不同 VPC 中的 AWS Managed Microsoft AD 目錄，或與檔案系統 AWS 帳戶 不同的目錄。如需詳細資訊，請參閱 Active Directory Support。	2019 年 6 月 25 日

Amazon FSx 發行增強版 Microsoft Active Directory 支援	您現在可以將 FSx for Windows File Server 檔案系統加入自我管理的 Microsoft Active Directory 網域，無論是內部部署或雲端。如需詳細資訊，請參閱 Active Directory Support。	2019 年 6 月 24 日
Amazon FSx 符合 SOC 認證	Amazon FSx 已經過評估，符合 SOC 認證。如需詳細資訊，請參閱安全和資料保護。	2019 年 5 月 16 日
新增有關 VPN Direct Connect 和區域間 VPC 互連連線支援的釐清備註	2019 年 2 月 22 日之後建立的 Amazon FSx 檔案系統可使用 Direct Connect、VPN 和區域間 VPC 對等互連存取。如需詳細資訊，請參閱支援的存取方法。	2019 年 2 月 25 日
Direct Connect新增 、VPN 和區域間 VPC 對等互連支援	您現在可以從內部部署資源和不同 Amazon VPC 或 中的資源存取 Amazon FSx for Windows File Server 檔案系統 AWS 帳戶。如需詳細資訊，請參閱支援的存取方法。	2019 年 2 月 22 日
Amazon FSx 現已正式推出	Amazon FSx for Windows File Server 提供完全受管的 Microsoft Windows 檔案伺服器，並由完全原生的 Windows 檔案系統提供支援。Amazon FSx for Windows File Server 提供功能、效能和相容性，可輕鬆提升和轉移企業應用程式 AWS。	2018 年 11 月 28 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。