aws

視窗使用者指南

Amazon FSx for Windows File Server

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

Table of Contents

什麼是 FSx 的 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 的功能、效能和相容性，可輕鬆地將企業應用程式移至. 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 針對中的企業應用程式進行了最佳化 AWS 雲端，具有原生 Windows 相容性、企業效能和功能，以及低於一毫秒的延遲。

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。適用於 Amazon FSx 的 Windows 應用程式和工作負載包括商業應用程式、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 還能讓 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。它還提供了與其他 AWS 服務的豐富集成 AWS Directory Service for Microsoft Active Directory，如 AWS IAM WorkSpaces，Amazon 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。檔案系統是您儲存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 (單位為 GiB)、SSD IOPS 和輸送量容量 (以 MB/s 為單位)。建立檔案系統之後，您可以根據需求變更來修改這些屬性。如需詳細資訊，請參閱管理儲存容量、管理固態硬碟 IOPS及管理輸送量容量。

FSx for Windows File Server 的備份非 file-system-consistent常耐用且增量。為了確保檔案系統的一致性，Amazon FSx 在 Microsoft 視窗中使用磁碟區陰影複製服務 (VSS)。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。

Windows 檔案共用是檔案系統內的特定資料夾 (及其子資料夾)，您可以透過 SMB 讓運算執行個體存取此資料夾。您的檔案系統已隨附一個名為的預設 Windows 檔案共用`\share`。您可以使用 Windows 上的共用資料夾圖形使用者介面 (GUI) 工具來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 Microsoft 視窗檔案共用。

您可以使用檔案系統的 DNS 名稱或與檔案系統相關聯的 DNS 別名來存取檔案共用。如需詳細資訊，請參閱 管理 DNS 別名。

存取檔案共用

Amazon FSx 可從具有中小企業通訊協定的運算執行個體存取 (支援 2.0 至 3.1.1 版)。您可以從視窗伺服器 2008 和視窗 7 開始的所有視窗版本，也可以從目前的 Linux 版本存取您的共用資料。您可以在 Amazon 彈性運算雲端 (Amazon EC2) 執行個體以及 AWS 虛擬機器上的執行個體、亞馬遜 AppStream 2.0 WorkSpaces 執行個體和 VMware 雲端上映射您的 Amazon FSx 檔案共用。

您可以使用或從內部部署運算執行個體存取檔案共 AWS Direct Connect 用 AWS VPN。除了存取與檔案系統位於相同 VPC、 AWS 帳戶和 AWS 區域的檔案共用之外，您還可以存取位於不同 Amazon VPC、帳戶或區域的運算執行個體上的共用。您可以使用 VPC 對等或傳輸閘道來執行此操作。如需詳細資訊，請參閱 Support 的存取方法。

安全性與資料保護

Amazon FSx 提供多層級的安全性和合規性，以協助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 (適用於檔案系統和備份 AWS Key Management Service 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，並符合 HIPAA 資格。

Amazon FSx 透過 Windows 存取控制清單 (ACL) 在檔案和資料夾層級提供存取控制。它使用 Amazon 虛擬私有雲 (Amazon VPC) 安全群組在檔案系統層級提供存取控制。此外，它還使用 AWS Identity and Access Management (IAM) 存取政策在 API 層級提供存取控制。訪問文件系統的用戶與 Microsoft 活動目錄進行身份驗證。Amazon FSx 與整合 AWS CloudTrail 以監控和記錄您的 API 呼叫，讓您查看使用者在 Amazon FSx 資源上採取的動作。

此外，它還可以通過每天自動對文件系統進行高度耐用的備份來保護您的數據，並允許您隨時進行額外的備份。如需詳細資訊，請參閱 Amazon FSx 中的安全。

可用性與持久性

FSx for Windows File Server 的檔案系統具有兩個層級的可用性和耐久性。單一可用區檔案可自動偵測並解決元件故障，確保單一可用區域 (AZ) 內的高可用性。此外，異 AWS 地同步備份檔案系統透過在區域內的獨立可用區域中佈建和維護備用檔案伺服器，在多個可用區域提供高可用性和容錯移轉支援。若要深入了解單一可用區和異地同步備份檔案系統部署，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

管理檔案系統

您可以使用自訂遠端管理 PowerShell 命令或在某些情況下使用 Windows 原生 GUI 來管理適用於 Windows 檔案伺服器檔案系統的 FSx。若要進一步了解管理 Amazon FSx 檔案系統的相關資訊，請參閱管理檔案系統。

價格與效能彈性

FSx Windows 檔案伺服器提供固態硬碟 (SSD) 和硬碟 (HDD) 儲存類型，為您提供價格與效能彈性。HDD 儲存裝置專為廣泛的工作負載而設計，包括主目錄、使用者和部門共用，以及內容管理系統。SSD 儲存裝置專為效能最高且延遲最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。

透過 FSx for Windows File Server，您可以獨立佈建檔案系統儲存裝置、SSD IOPS 和輸送量，以達到適當的成本與效能組合。您可以修改檔案系統的儲存裝置、SSD IOPS 和輸送量容量，以滿足不斷變化的工作負載需求，讓您只需按需要付費。如需詳細資訊，請參閱 使用亞馬遜 FSx 優化成本。

Amazon FSx 的定價

使用 Amazon FSx 時，無需預付硬體或軟體成本。您只需為使用的資源付費，沒有最低承諾、設定成本或額外費用。如需與服務相關聯的定價和費用的詳細資訊，請參閱 Amazon FSx for Windows File Server 定價。

前提

若要使用 Amazon FSx，您需要擁有 Amazon EC2 執行個體、執行個體、 AppStream 2.0 執行個 WorkSpaces 體或在 VMware 雲端中執行的虛擬機器的 AWS 帳戶，並在受支援類型的 AWS 環境中執行。

在本指南中，我們做出了以下假設：

- 如果您使用的是 Amazon EC2，我們假設您熟悉 Amazon EC2。如需如何使用 Amazon EC2 的詳細資訊，請參閱 Amazon 彈性運算雲端文件。
- 如果您使用的是 WorkSpaces，我們假設您熟悉 WorkSpaces。如需有關如何使用的詳細資訊 WorkSpaces，請參閱 Amazon 使用 WorkSpaces 者指南。
- 如果您正在使用 VMware 雲端服務 AWS，我們假設您已熟悉此功能。如需詳細資訊，請參閱上的 VMware 雲端 AWS。

- 我們假設您熟悉 Microsoft 活動目錄的概念。

必要條件

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 執行個體所需許可的 AWS 帳戶。如需詳細資訊，請參閱 設定您的 AWS 帳戶。
- 在虛擬私有雲 (VPC) 中執行 Microsoft 視窗伺服器的亞馬 Amazon EC2 執行個體，該執行個體是以您想要與 Amazon FSx 檔案系統建立關聯的 Amazon VPC 服務為基礎。如需如何建立執行個體的詳細資訊，請參閱 Amazon EC2 使用者指南中的開始使用 Amazon EC2 Windows 執行個體。
- Amazon FSx 與 Microsoft 活動目錄合作，以執行用戶身份驗證和訪問控制。你加入你的 Amazon FSx 文件系統到 Microsoft 活動目錄，同時創建它。如需詳細資訊，請參閱 使用 Microsoft 活動目錄在 FSx for Windows File Server。
- 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。如果有，您需要確保新增必要的規則，以允許從 Amazon EC2 執行個體傳輸到 Amazon FSx 檔案系統的網路流量。如需詳細資訊，請參閱Amazon FSx 中的安全。
- 安裝並設定 AWS Command Line Interface (AWS CLI)。支援的版本為 1.9.12 及更新版本。若要取得更多資訊，請參閱《AWS Command Line Interface 使用指南》 AWS CLI中的〈安裝、更新和解除安裝〉。

> **Note**
>
> 您可以使用`aws --version`命令檢查 AWS CLI 您正在使用的版本。

FSx for Windows File Server 論壇的 Amazon FSx

如果您在使用 Amazon FSx 時遇到問題，請使用論壇。

您是 Amazon FSx 的首次使用者嗎？

如果您是 Amazon FSx 的首次使用者，建議您依序閱讀下列各節：

1. 如果您已準備好建立第一個 Amazon FSx 檔案系統，請嘗試使用開始使用適用於 FSx for Windows File Server 的 Amazon FSx.

2. 如需有關效能的詳細資訊，請參閱FSx 適用於 FSx for Windows File Server 效能。
3. 如需 Amazon FSx 安全性詳細資訊，請參閱Amazon FSx 中的安全。
4. 如需有關 Amazon FSx API 的資訊，請參閱 Amazon FSx 應用程式介面參考。

適用於 FSx for Windows File Server 最佳作法

我們建議您在使用適用於 Windows 檔案伺服器的 Amazon FSx 時遵循這些最佳實務。請點選下列連結，進一步瞭解所討論的主題。

主題

一般最佳實務

在移至生產環境之前測試工作負載

我們建議您使用與生產環境具有相同組態的測試環境來測試您的工作負載。例如，使用相同的 Active Directory (AD) 和網路組態、檔案系統大小和組態，以及 Windows 功能，例如重複資料刪除和陰影複製。在模擬所需生產流量的測試環境中執行測試工作負載，有助於確保程序順利執行。

我們也建議您檢閱檔案系統的可用性模型，並確保在檔案系統維護、輸送量容量變更和意外服務中斷等事件期間，您的工作負載能夠回復您的檔案系統類型的預期復原行為。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。

建立監視計劃

您可以使用檔案系統指標來監控儲存空間和效能使用情況、瞭解使用模式，並在使用量接近檔案系統的儲存空間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，可讓您快速偵錯任何可能影響效能的問題。

確保您的檔案系統有足夠的資源

資源不足可能會增加延遲並排入佇列 I/O 要求，這可能會顯示為檔案系統完整或部分無法使用。如需監視效能和存取效能警告和建議的詳細資訊，請參閱監督 FSx 的 FSx for Windows File Server。

定期備份您的檔案系統

定期備份可讓您滿足資料保留、業務和合規性需求。我們建議您使用預設為檔案系統啟用的每日自動備份，並將其用 AWS Backup 於中央備份解決方案 AWS 服務。 AWS Backup 可讓您設定不同頻率的其他備份計劃 (例如，一天、每天或每週多次) 和保留期。

安全最佳實務

我們建議您遵循這些最佳作法來管理檔案系統的安全性和存取控制。如需設定 Amazon FSx 以符合安全和合規目標的詳細資訊，請參閱Amazon FSx 中的安全。

網路安全

請勿修改或刪除與檔案系統相關聯的 ENI

Amazon FSx 檔案系統可透過 elastic network interface (ENI) 存取，該界面位於與檔案系統關聯的虛擬私有雲 (VPC) 中。修改或刪除網路介面可能會導致 VPC 與檔案系統之間的連線永久中斷。

使用安全群組和網路 ACL

您可以使用安全性群組和網路存取控制清單 (ACL) 來限制對檔案系統的存取。對於 VPC 安全群組，預設安全性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性群組和網路 ACL 允許連接埠上的流量。如需詳細資訊，請參閱 Amazon VPC 安全群組。

Active Directory

建立 Amazon FSx 檔案系統時，可以將其加入 Microsoft AD 網域，以提供使用者身份驗證，以及共用、檔案和資料夾層級存取控制授權。您的使用者可以使用現有的 AD 帳戶連線至檔案共用，以及存取其中的檔案和資料夾。此外，您可以將現有的安全 ACL 組態移轉到 Amazon FSx，而無需進行任何修改。Amazon FSx 為您提供活動目錄兩個選項：Microsoft AWS 託管 AD 或自我管理 Microsoft AD。

如果您使用的是AWS 受管理的 Microsoft AD，建議您保留 AD 安全性群組的預設設定。如果您確實修改了這些設定，請務必維護符合網路需求的網路組態。如需詳細資訊，請參閱 網路必要條。

如果您使用自我管理的 Microsoft AD，您還有其他選項可供您設定檔案系統。在搭配自我管理的 Microsoft AD 使用 Amazon FSx 時，我們建議您採用下列最佳實務來進行初始設定：

- 將子網路指派給單一 AD 站台：如果您的 AD 環境具有大量網域控制站，請使用 Active Directory 站台和服務，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 AD 站點。請確定 VPC 安全群組、VPC 網路 ACL、網路 ACL、Windows 防火牆規則，以及您在 AD 基礎設施中擁有的任何其他網路路由控制項，都允許 Amazon FSx 在所需連接埠上進行通訊。如果 Windows 無法使用指派的 AD 網站，這可讓 Windows 還原為其他網域控制站。如需詳細資訊，請參閱 使用 Amazon VPC 進行檔案系統存取控制。
- 使用單獨的組織單位 (OU)：針對 Amazon FSx 檔案系統使用 OU，這個 OU 與您可能擁有的任何其他組織單位不同。

- 以所需的最低權限設定您的服務帳戶：以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 活動目錄的先決條件 及 將權限委派給您的 Amazon FSx 服務帳戶 。
- 持續驗證您的 AD 組態 ：在建立 Amazon FSx 檔案系統之前，針對 AD 組態執行 Amazon FSx 活動目錄驗證工具，以確認您的組態可與 Amazon FSx 搭配使用，並發現該工具可能暴露的任何警告和錯誤。

避免因 AD 設定錯誤而喪失可用性

將 Amazon FSx 與自我管理的 Microsoft AD 搭配使用時，不僅要在建立檔案系統期間擁有有效的 AD 組態，還要有持續的作業和可用性。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 AD 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，而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 AD 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之任何檔案系統的組態。
- 監控 AD 配置錯誤：為您自己設置錯誤的狀態通知，以便在必要時重置文件系統的 AD 配置。如需使用 Lambda 解決方案來達成此目標的範例，請參閱使用 Amazon 和監控 Amazon FSx 檔案系統的運作狀態。 EventBridge AWS Lambda
- 定期驗證 AD 組態：如果您想要主動偵測 AD 錯誤設定，建議您持續針對 AD 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訊息，表示您的檔案系統可能有設定錯誤的風險。
- 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 AD 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檔案系統設定錯誤。

視窗 ACL

使用 Amazon FSx 時，您可以使用標準的 Windows 存取控制清單 (ACL) 進行精細的共用、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的使用者登入資料，以強制執行這些 Windows ACL。

- 請勿變更系統使用者的 NTFS ACL 許可：Amazon FSx 要求系統使用者對檔案系統中所有資料夾擁有完全控制 NTFS ACL 許可。變更 SYSTEM 使用者的 NTFS ACL 權限可能會導致檔案系統變得無法存取，而且 future 的檔案系統備份可能會變得無法使用。

配置和調整檔案系統的大小

選取部署類型

Amazon FSx 提供兩種部署選項：單一可用區和異地同步備份。我們建議針對需要高可用性的共用 Windows 檔案資料的大多數生產工作負載使用異地同步備份檔案系統。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。

選取儲存類型

SSD 儲存裝置適用於大多數具有高效能需求和延遲敏感性的生產工作負載。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。對於涉及大量使用者、高層級 I/O 或具有大量小檔案的資料集的使用案例，我們也建議使用 SSD。最後，如果您打算啟用陰影複製，我們建議您使用 SSD 儲存體。您可以針對具有 SSD 儲存裝置的檔案系統設定和擴充 SSD IOPS，但不能使用 HDD 儲存裝置。

如果您決定使用 HDD 儲存空間，請測試您的檔案系統，以確保檔案系統能夠符合您的效能需求。相對於 SSD 儲存，HDD 儲存的成本較低，但延遲時間較高，每單位儲存裝置的磁碟輸送量和磁碟 IOPS 也較低。它可能適用於一般用途的使用者共用和 I/O 需求較低的主目錄、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 儲存設定與效能。

您可以隨時使用 Amazon FSx 主控台或 Amazon FSx API 將儲存類型從硬碟升級為固態硬碟。如需詳細資訊，請參閱 管理儲存區類型。

選取輸送量容量

將檔案系統設定為足夠的輸送量容量，不僅可以滿足工作負載的預期流量，還可以滿足您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功能，您選擇的輸送量容量必須提供足夠的記憶體，以根據您擁有的儲存體執行重複資料刪除。如果您正在使用陰影複製，請將輸送量容量增加到至少三倍於工作負載預期驅動值的值，以避免 Windows Server 刪除陰影複製。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空間不足，或者您預期儲存需求將大於目前的儲存限制時，請增加檔案系統的儲存容量。我們建議您始終在檔案系統上維持至少 10% 的可用儲存容量。我們也建議您在擴充儲存空間之前，將儲存容量增加至少 20%，因為在程序進行期間，您將無法增加儲存容量。您可以使用FreeStorage容 CloudWatch 量指標來監視可用的可用儲存空間數量，並瞭解其趨勢。如需詳細資訊，請參閱 管理儲存容量。

如果您的工作負載受到目前效能限制的限制，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「監視和效能」頁面來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。

若要將儲存擴展的持續時間降至最低並避免寫入效能降低，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，然後在儲存容量增加完成後調整輸送量容量。大部分的工作負載在儲存擴展期間對效能的影響最小，但具有大量使用中資料集的寫入量應用程式可能會暫時降低高達一半的寫入效能。

在閒置期間修改輸送量容量

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，並導致異地同步備份檔案系統的容錯移轉和容錯回復。對於異地同步備份檔案系統，如果在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處理。對於大量寫入和 IOPS 繁重的工作負載，資料同步處理程序可能需要長達數小時的時間。雖然您的檔案系統在此期間仍可繼續使用，但我們建議您排定維護時段，並在檔案系統負載最小的閒置期間執行輸送量容量更新，以減少資料同步處理的持續時間。如需進一步了解，請參閱管理輸送量容量。

開始使用適用於 FSx for Windows File Server 的 Amazon FSx

接下來，您可以學習如何開始使用 FSx for Windows File Server。此入門練習包括以下步驟。

1. 註冊 AWS 帳戶 並在帳戶中建立系統管理使用者。
2. 使用建立 AWS 受管理的 Microsoft AD 活動目錄 AWS Directory Service。您將加入您的檔案系統和計算執行個體至作用中目錄。
3. 創建一個運行 Microsoft Windows 服務器的 Amazon 彈性計算雲計算實例。您將使用此執行個體來存取您的檔案系統。
4. 使用 Amazon FSx 主控台建立適用於 FSx for Windows File Server 的 Amazon FSx 檔案系統。
5. 將您的檔案系統對應至 EC2 執行個體
6. 將資料寫入您的檔案系統。
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

第一次使用 Amazon FSx 之前，請先完成下列任務：

1. 註冊一個 AWS 帳戶
2. 建立具有管理權限的使用者

註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

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

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

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

AWS 註冊過程完成後，會向您發送確認電子郵件。您可以隨時登錄 https://aws.amazon.com/ 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立具有管理權限的使用者

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

保護您的 AWS 帳戶根使用者

1. 選擇 Root 使用者並輸入您的 AWS 帳戶 電子郵件地址，以帳戶擁有者身分登入。AWS Management Console在下一頁中，輸入您的密碼。

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

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

建立具有管理權限的使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱 AWS IAM Identity Center 使用者指南中的啟用 AWS IAM Identity Center。
2. 在 IAM 身分中心中，將管理存取權授予使用者。

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

以具有管理權限的使用者身分登入

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

  如需使用 IAM 身分中心使用者登入的說明，請參閱使用AWS 登入 者指南中的登入 AWS 存取入口網站。

指派存取權給其他使用者

1. 在 IAM 身分中心中，建立遵循套用最低權限許可的最佳做法的權限集。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「建立權限集」。
2. 將使用者指派給群組，然後將單一登入存取權指派給群組。

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

建立您的檔案系統

若要建立您的 Amazon FSx 檔案系統，您必須建立您的視窗亞馬遜彈性運算雲端 (Amazon EC2) 執行個體和目 AWS Directory Service 錄。如果您尚未設定，請參閱演練 1：開始使用的先決條件。

若要建立您的檔案系統 (主控台)

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 在儀表板上，選擇 Create file system (建立檔案系統) 以啟動檔案系統建立精靈。
3. 在 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. 針對建立方式，選擇「標準建立」

檔案系統詳情

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，尋找和管理檔案系統會比較容易。您最多可以使用 256 個 Unicode 字母、空格和數字，再加上 +-= 的特殊字元。_:/
2. 對於部署類型，請選擇異地同步備份或單一可用

   - 選擇異地同步備份以部署容忍可用區域無法使用的檔案系統。此選項支持 SSD 和硬盤存儲。
   - 選擇單一可用區域以部署在單一可用區域中部署的檔案系統。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：單一可用區和異地同步備份檔案系。
3. 對於存儲類型，您可以選擇 SSD 或 HDD。

   FSx for Windows File Server 提供固態驅動器（SSD）和硬盤驅動器（HDD）存儲類型。SSD 儲存裝置專為效能最高且延遲最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 儲存是專為廣泛的工作負載所設計，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 使用儲存類型最佳化成本。
4. 針對佈建的 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，以維持每 GiB 儲存容量的 3 個固態硬碟 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。將 SSD IOPS 擴展到 80,000 以上，可在美國東部 (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) 使用。如需詳細資訊，請參閱 管理固態硬碟 IOPS。
5. 對於儲存容量，請輸入檔案系統的儲存容量 (以 GiB 為單位)。如果您使用的是固態硬碟儲存空間，請輸入介於 32 到 65,536 範圍內的任何整數。如果您使用的是硬碟儲存空間，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。輸送量容量是代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] 設定是根據您選擇的儲存容量量而定。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]，然後選擇一個值。如需詳細資訊，請參閱 FSx 適用於 FSx for Windows File Server 效能。

> **Note**
>
> 如果您要啟用檔案存取稽核，則必須選擇 32 MB/s 或以上的輸送量容量。如需詳細資訊，請參閱 檔案存取稽核。

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。

網路與安全性

1. 在「網路與安全性」區段中，選擇您要與檔案系統建立關聯的 Amazon VPC。在此入門練習中，請選擇您為 AWS 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。如果您沒有使用預設的安全性群組，請確定您選擇的安全性群組與您的檔案系統位於 AWS 區域 相同的安全性群組。為確保您可以將 EC2 執行個體與檔案系統連接，您需要將下列規則新增至選擇的安全群組：

   a. 新增下列輸入和輸出規則，以允許下列連接埠。

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

   新增與您要存取檔案系統之用戶端運算執行個體相關聯的 IP 位址或安全群組 ID。

   b. 新增輸出規則，以允許您加入檔案系統之 Active Directory 的所有流量。若要執行此操作，請執行以下其中一項操作：

   - 允許輸出流量連至與您 AWS 受管理 AD 目錄相關聯的安全群組 ID。
   - 允許輸出流量傳送至與您自我管理的 Active Directory 網域控制站相關聯的 IP 位址。

> **Note**
>
> 在某些情況下，您可能已經從預設設定中修改了 AWS Managed Microsoft AD 安全性群組的規則。如果是這樣，請確定此安全群組具有必要的輸入規則，以允許來自 Amazon FSx 檔案系統的流量。如需必要輸入規則的詳細資訊，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 進行檔案系統存取控制。

3. 異地同步備份檔案系統在自己的可用區域和子網路中都有一個主要和待命檔案伺服器。如果您要建立異地同步備份檔案系統 (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，請為您的檔案系統選擇子網路。

視窗驗證

- 對於 Windows 驗證，您可以使用下列選項：

  如果您想要將您的檔案系統加入由所AWS 管理的 Microsoft Active Directory 網域，請選擇受管理的 Microsoft 作用中目錄 AWS，然後從清單中選擇您的 AWS Directory Service 目錄。如需詳細資訊，請參閱 使用 Microsoft 活動目錄在 FSx for Windows File Server。

  如果您想要將您的檔案系統加入自我管理的 Microsoft Active Directory 網域，並提供下列詳細資料，請選擇自我管理的 Microsoft 作用中目錄。如需更多資訊，請參閱使用 Amazon FSx 與您的自我管理 Microsoft 活動目錄。

  - 您的活動目錄的完整網域名稱。

  > **Important**
  >
  > 對於單一可用區 2 和所有異地同步備份檔案系統，Active Directory 網域名稱不得超過 47 個字元。此限制適用於 AWS Directory Service 和自我管理的活動目錄網域名稱。Amazon FSx 需要直接連接到您的 DNS IP 地址的內部流量。不支援透過網際網路閘道進行連線。而是使用 AWS Virtual Private Network VPC 對等互連或 AWS Transit Gateway 關聯。 AWS Direct Connect

- DNS 伺服器 IP 位址 — 您網域的 DNS 伺服器的 IPv4 位址

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

- 服務帳戶使用者名稱 — 現有 Active Directory 中服務帳戶的使用者名稱。請勿包含網域前置字元或尾碼。
- 服務帳戶密碼 — 服務帳戶的密碼。
- (選擇性) 組織單位 (OU) — 您要加入檔案系統之組織單位的辨別路徑名稱。
- (選擇性) 委派檔案系統管理員群組 — Active Directory 中可以管理您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 將權限委派給您的 Amazon FSx 服務帳戶 。

加密、稽核和存取 (DNS 別名)

1. 對於「加密」，請選擇用於加密靜 AWS KMS key 態檔案系統上資料的加密金鑰。您可以指定金鑰的 ARN AWS KMS，選擇由管理的預設 aws/fsx (預設值)、現有金鑰或客戶管理的金鑰。如需詳細資訊，請參閱 靜態加密。
2. 針對稽核-選用，依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資訊，請參閱若要在建立檔案系統時啟用檔案存取稽核 (主控台)。
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。

Backup 與維護

如需有關自動每日備份和本節中設定的詳細資訊，請參閱使用備份。

1. 對於每日自動備份，預設為啟用。如果您不希望 Amazon FSx 每天自動備份檔案系統，可以停用此設定。
2. 如果啟用了自動備份，則會在稱為備份時段的期間內進行。您可以使用預設視窗，或選擇自動備份視窗開始時間。
3. 對於自動備份保留期，您可以使用預設設定 30 天，或設定介於 1 到 90 天之間的值，Amazon FSx 會保留檔案系統的每日自動備份。此設定不適用於使用者起始的備份或由所取得的備份 AWS Backup。

4. 在「標籤-選用」中，輸入鍵和值，以將標籤新增至檔案系統。標籤是區分大小寫的索引鍵值組，可協助您管理、篩選及搜尋檔案系統。如需詳細資訊，請參閱 標記您的 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。在建立檔案系統之後，您可以查看哪些檔案系統設定可以及無法修改哪些檔案系統設定，以供參考。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 [網路與安全性] 索引標籤中記下檔案系統的 DNS 名稱。您需要在下列程序中將共用對應至 EC2 執行個體。

將您的檔案共用對應至執行 Windows 伺服器的 EC2 執行個體

您現在可以將 Amazon FSx 檔案系統掛載到加入目錄的基於 Microsoft 視窗的亞馬遜 EC2 執行個體。AWS Directory Service 檔案共用的名稱與檔案系統的名稱不同。

使用圖形用戶界面在 Amazon EC2 Windows 實例上映射文件共享

1. 在 Windows 執行個體上掛載檔案共用之前，您必須先啟動 EC2 執行個體並將其加入 AWS Directory Service for Microsoft Active Directory. 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到 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) 功能表，然後選擇 [對應網路磁碟機
5. 為「雲端硬碟」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 別名來對應檔案系統。此程序說明使用預設 DNS 名稱對應檔案共用。如果您要使用 DNS 別名對應檔案共用，請參閱逐步解說 5：使用 DNS 別名存取您的檔案系統。

在資料夾中，輸入檔案系統 DNS 名稱和共用名稱。默認的 Amazon FSx 共享被調\share用。您可以在 Amazon FSx 控制台，https://console.aws.amazon.com/fsx/，視窗文件服務器 > 網絡和安全部分，或在CreateFileSystem或 DescribeFileSystems API 命令的響應中找到 DNS 名稱。

- 對於加入 AWS 管理 Microsoft 活動目錄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，以及任何異地同步備份檔案系統，DNS 名稱如下所示。

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

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

7. 選擇是否要在登入時重新連線檔案共用，然後選擇 [完成]。

將資料寫入檔案共用

現在您已將檔案共用對應至執行個體，您可以像使用 Windows 環境中的任何其他目錄一樣使用檔案共用。

將資料寫入檔案共用

1. 開啟 [記事本] 文字編輯器。
2. 在文本編輯器中寫一些內容。例如：*######*
3. 將檔案儲存至檔案共用的磁碟機代號。
4. 使用 [檔案總管]，瀏覽至您的檔案共用，並尋找剛儲存的文字檔案。

備份您的檔案系統

現在您已經有機會使用 Amazon FSx 檔案系統及其檔案共用，您可以對其進行備份。依預設，每日備份會在檔案系統的 30 分鐘備份時段自動建立。不過，您可以隨時建立使用者啟動的備份。備份有相關的額外費用。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. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 從主控台儀表板中，選擇您為本練習建立的檔案系統名稱。
3. 在檔案系統的「概覽」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，以便還原檔案系統或刪除備份，請選擇「備份」。

當您建立新備份時，其狀態會在建立時設定為 [建立]。這可能需要幾分鐘的時間。備份可供使用時，其狀態會變更為「可用」。

清除資源

完成這個練習之後，您應該依照下列步驟清理資源並保護您的 AWS 帳戶。

清理資源

1. 在 Amazon EC2 主控台上，終止您的執行個體。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的終止執行個體。
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。但是，您仍然需要刪除手動創建的備份。以下步驟概述了此過程：

   a. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
   b. 從主控台儀表板中，選擇您為本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，決定是否要建立最終備份。如果這樣做，請提供最終備份的名稱。也會刪除任何自動建立的備份。

      > **Important**
      >
      > 可以從備份中創建新的文件系統。我們建議您建立最終備份作為最佳作法。如果您發現在一段時間後不需要它，則可以刪除此備份和其他手動創建的備份。

   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，其在儀表板中的狀態會變更為 DELETE。刪除檔案系統後，該檔案系統將不再出現在儀表板中。

h. 現在，您可以刪除任何手動為文件系統創建的備份。在左側導覽中，選擇「備份」。

i. 從儀表板中，選擇與您刪除的檔案系統具有相同檔案系統 ID 的任何備份，然後選擇 [刪除備份]。

j. 刪除備份」對話方塊隨即開啟。保持核取所選備份 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在會被刪除。

3. 如果您在中建立了此練習的 AWS Directory Service 目錄演練 1：開始使用的先決條件，您現在可以將其刪除。如需詳細資訊，請參閱《AWS Directory Service 管理指南》中的刪除目錄。

Amazon FSx 文件系統狀態

您可以使用 Amazon FSx 主控台、 AWS CLI 指令描述檔案系統或 API 作業系統來檢視 Amazon FSx 檔案系統的狀態。DescribeFile

檔案系統狀態	描述
AVAILABLE	檔案系統狀態良好，可存取和使用。
CREATING	Amazon FSx 正在創建一個新的文件系統。
DELETING	Amazon FSx 正在刪除現有的檔案系統。
UPDATING	檔案系統正在進行客戶啟動的更新。
配置錯誤	由於您的 Active Directory 環境發生變更，檔案系統處於受損狀態。您的檔案系統目前無法使用，或有遺失可用性的風險，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錯誤設定的狀態。
設定錯誤 (_U) 無法使用	檔案系統目前無法使用，因為您的 Active Directory 環境發生變更。如需還原可用性的資訊，請參閱檔案系統處於錯誤設定的狀態。

檔案系統狀態	描述
失敗	• 建立新檔案系統時，Amazon FSx 無法建立新的檔案系統。 • 檔案系統無法使用。 • 檔案系統發生故障，Amazon FSx 無法復原。 • Amazon FSx 無法建立備份。

FSx for Windows File Server 支援的用戶端、存取方法和環境

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

主題

用戶端支援

Amazon FSx 支援從各種運算執行個體和作業系統連線到您的檔案系統。它通過支持通過服務器消息塊（SMB）協議的訪問，從 2.0 到 3.1.1 版來實現這一點。

以下AWS運算執行個體支援搭配 Amazon FSx 使用：

- Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，包括 Microsoft Windows Server (Amazon EC2) 執行個體，如需詳細資訊，請參閱 存取檔案共用。
- Amazon Elastic Container Service (Amazon ECS) 容器 如需詳細資訊，請參閱FSx for Windows File Server 磁碟區在Amazon Elastic Container Service 開發人員指南。
- WorkSpaces 執行個體 — 如需進一步了解，請參閱AWS部落格文章搭配 Amazon 使用 FSx for Windows File Server WorkSpaces。
- 亞馬遜 AppStream 2.0 執行個體 — 如需進一步了解，請參閱AWS部落格文章使用 Amazon FSx 搭配 Amazon FSx 與 Amazon AppStream 2.0。
- 在 VMware 雲端上執行的虛擬機器AWS環境 — 如需進一步了解，請參閱AWS部落格文章在 VMware 雲端中使用 FSx 儲存和共用檔案 (適用於 Windows 檔案伺服器)AWS環境。

Amazon FSx 支援以下作業系統：

- Windows Server 2008 年，Windows Server 2008 R2、Windows Server 2012、Windows Server 2012、Windows Server 2012、Windows Server 2012 (Windows Server 2012 R2) Windows Server 2008 (Windows Server)，Windows Server 2008 (Windows Server)
- 視窗遠景, 視窗 7, 視窗 8, 視窗 8.1, 視窗 10（包括視窗 7 和視窗 10 桌面體驗 WorkSpaces) 和視窗 11.

- Linux, 使用`cifs-utils`工具。
- macOS

Support 的存取方法

您可以搭配 Amazon FSx 使用下列存取方法和方法。

使用預設 DNS 名稱存取檔案系統

FSx for Windows File Server 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對應至 Amazon FSx 檔案共用，以存取 FSx for Windows 檔案伺服器檔案系統。如需進一步了解，請參閱 使用 Microsoft 視窗檔案共用。

> **Important**
>
> 如果您使用微軟 DNS 做為預設 DNS，Amazon FSx 只會為檔案系統註冊 DNS 記錄。如果您使用的是第三方 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之正確 IP 地址的資訊，請參閱取得要用於 DNS 的正確檔案系統 IP 位址。

如需尋找 DNS 名稱：

- 在 Amazon FSx 主控台，選擇檔案系統，然後選擇詳細資訊。在「」中檢視 DNS 名稱網路與安全區域。
- 或者，查看它的響應CreateFileSystem或者DescribeFileSystemsAPI 指令。

適用於所有加入至AWS託管 Microsoft Active Directory，DNS 名稱如下所示：`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，以及任何異地同步備份檔案系統，DNS 名稱如下所示：`amznfsxaa11bb22.`*`ad-domain`*`.com`

搭配 Kerberos 身份驗證使用 DNS 名稱

我們建議您在傳輸過程中使用 Kerberos 型身份驗證和加密搭配 Amazon FSx。Kerberos 為存取檔案系統的用戶端提供最安全的驗證。若要為您的 SMB 工作階段啟用 Kerberos 型身份驗證和傳輸中的資料加密，請使用 Amazon FSx 提供的檔案系統 DNS 名稱來存取您的檔案系統。

如果您在AWS託管微軟活動目錄和您的現場活動目錄，使用亞馬遜 FSx 遠程 PowerShell 使用 Kerberos 驗證時，您必須在用戶端上針對樹系搜尋順序設定本機群組原則。如需詳細資訊，請參閱設定凱伯洛斯森林搜尋順序 (KFSO)在微軟文檔中。

使用 DNS 別名存取檔案系統

FSx for Windows File Server 的每個檔案系統都會提供 DNS 名稱，讓您用來存取檔案共用。您也可以透過為 Windows 檔案伺服器檔案系統的 FSx 註冊別名，以便從 Amazon FSx 建立的預設 DNS 名稱以外的 DNS 名稱存取 Amazon FSx。

使用 DNS 別名，您可以將 Windows 檔案共用資料移至 Amazon FSx，然後繼續使用您現有的 DNS 名稱存取 Amazon FSx 上的資料。DNS 別名也可讓您使用有意義的名稱，以便更輕鬆地管理工具和應用程式以連接到 Amazon FSx 檔案系統。如需詳細資訊，請參閱 管理 DNS 別名。

搭配 Kerberos 身份驗證使用 DNS 別名

我們建議您在傳輸過程中使用 Kerberos 型身份驗證和加密搭配 Amazon FSx。Kerberos 為存取檔案系統的用戶端提供最安全的驗證。若要為使用 DNS 別名存取 Amazon FSx 的用戶端啟用 Kerberos 身份驗證，您必須新增服務主體名稱 (SPN)，這些名稱與 Amazon FSx 檔案系統的作用中目錄電腦物件上的 DNS 別名相對應。

您可以選擇性地強制使用 DNS 別名存取檔案系統的用戶端以使用 Kerberos 驗證和加密，方法是在您的 Active Directory 中設定下列群組原則物件 (GPO)：

- 限制 NTLM：傳出 NTLM 流量至遠端伺服器-使用此原則設定可拒絕或稽核從電腦到執行 Windows 作業系統之任何遠端伺服器的傳出 NTLM 流量。
- 限制 NTLM：新增 NTLM 驗證的遠端伺服器例外-使用此原則設定可建立允許用戶端裝置使用 NTLM 驗證的遠端伺服器例外清單，如果網路安全 限制 NTLM：傳出 NTLM 流量至遠端伺服器已設定原則設定。

如需詳細資訊，請參閱 逐步解說 5：使用 DNS 別名存取您的檔案系統。

使用 FSx for Windows File Server 檔案系統

FSx FSx for Windows File Server 支援使用微軟分散式檔案系統 (DFS) 命名空間。您可以使用 DFS 命名空間，將多個檔案系統上的檔案共用組織成一個用來存取整個檔案資料集的共用資料夾結構 (命名空間)。您可以使用 DFS 命名空間中的名稱來存取 Amazon FSx 檔案系統，方法是將其連結目標設定為檔案系統的 DNS 名稱。如需詳細資訊，請參閱 使用 DFS 命名空間分組多個檔案系統。

支援的環境

您可以從與檔案系統位於相同 VPC 中的資源存取檔案系統。如需詳細資訊和詳細說明，請參閱演練 1：開始使用的先決條件。

您也可以從內部部署資源和位於不同 VPC 的資源存取 2019 年 2 月 22 日之後建立的檔案系統，AWS 帳戶，或AWS區域 下表說明 Amazon FSx 支援在每個受支援環境中從用戶端存取的環境，具體取決於檔案系統的建立時間。

客戶位於...	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	✓	✓	✓
建立檔案系統之 VPC 的主要 CIDR 區塊	✓	✓	✓
建立檔案系統之 VPC 的次要 CIDR		具有 IP 位址的用戶端RFC 1918私有 IP 位址範圍： • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	IP 位址超出下列 CIDR 封鎖範圍的用戶端：198.19.0.0/16
其他 CIDR 或對等網路			

> **Note**
>
> 在某些情況下，您可能想要使用非私有 IP 位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。若要這麼做，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。

接下來，您可以找到有關如何從內部部署和不同 VPC 存取您的 FSx for Windows 檔案伺服器檔案系統的資訊，AWS帳戶，或AWS區域

從內部部署存取 FSx for Windows File Server 檔案系統

FSx for Windows File Server 支援AWS Direct Connect或者AWS VPN從內部部署運算執行個體存取您的檔案系統。隨著支援AWS Direct Connect的 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。隨著支援AWS VPN的 FSx for Windows File Server 可讓您透過安全且私密的通道，從內部部署裝置存取檔案系統。

將現場部署環境連接到與 Amazon FSx 檔案系統關聯的 VPC 後，您可以使用檔案系統的 DNS 名稱或 DNS 別名來存取檔案系統。您可以這樣做，就像從 VPC 內的運算執行個體執行個體一樣。如需詳細資訊AWS Direct Connect，請參閱AWS Direct Connect使用者指南。如需設定的詳細資訊AWS VPN連線，請參閱VPN 連線在Amazon VPC User Guide。

FSx for Windows File Server 也支援使用 Amazon FSx 檔案閘道，從現場部署運算執行個體對 Windows 檔案伺服器檔案共用的雲端 FSx 提供低延遲且順暢的存取。如需詳細資訊，請參閱亞馬遜 FSx 檔案閘道使用者指南。

從其他 VPC、帳戶存取 FSx for Windows File Server 檔案系統AWS 區域

您可以從不同 VPC 中的計算執行個體存取 FSx for Windows File Server 檔案系統AWS帳戶，或AWS與您檔案系統相關聯的區域。若要這麼做，您可以使用 VPC 對等或傳輸閘道。當您使用 VPC 對等連接或傳輸閘道連接 VPC 時，位於一個 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 VPC 屬於不同的帳戶，並且 VPC 位於不同的帳戶中，也可以執行此存取AWS區域

一個VPC 對等連線是指兩個 VPC 之間的聯網連線，您可以使用私有 IPv4 或 IP 第 6 (IPv6) 地址在兩者之間路由流量。您可以使用 VPC 對等連接相同的 VPCAWS地區或之間AWS區域 如需 VPC 互連的詳細資訊，請參閱什麼是 VPC 互連？在Amazon VPC Peering Guide。

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 VPC 傳輸閘道的詳細資訊，請參閱「VPC 傳輸閘道」。開始使用傳輸閘道在Amazon VPC 傳輸閘道。

設定 VPC 對等或傳輸閘道連線後，您可以使用檔案系統的 DNS 名稱來存取檔案系統。您可以這樣做，就像從關聯 VPC 內的運算執行個體執行個體一樣。

可用性和耐久性：單一可用區和異地同步備份檔案系

適用於 Windows 檔案伺服器的 Amazon FSx 提供兩種檔案系統部署類型：單一同步備份和異地同步備份。以下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 (服務等級協議) 的相關資訊，請參閱 Amazon FSx 服務水準協議。

單一可用區域檔案系統是由單一 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，以防止單一元件在大多數情況下發生故障。Amazon FSx 會持續監控硬體故障，並透過更換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離線 (通常不超過 20 分鐘)，在這些故障復原事件期間，以及在您為檔案系統設定的維護時段內規劃的檔案系統維護期間。使用單一可用區檔案系統時，檔案系統故障可能無法復原，在極少數情況下，例如由於多個元件故障，或是由於單一檔案伺服器發生非正常故障而導致檔案系統失敗而使檔案系統處於不一致的狀態，在這種情況下，您可以從最近的備份中復原檔案系統。

異地同步備份檔案系統是由一個高可用性的 Windows 檔案伺服器叢集組成，分散在兩個 AZ (偏好的 AZ 和備用 AZ)，利用 Windows Server 容錯移轉叢集 (WSFC) 技術，以及兩個 AZ 上的一組儲存磁碟區。資料會在每個個別 AZ 內以及兩個 AZ 之間同步複製。相對於單一可用區部署，異地同步備份部署可透過進一步跨 AZ 複寫資料來提供增強的耐久性，並透過自動容錯移轉至備用 AZ，在計劃的系統維護和意外服務中斷期間提升可用性。這可讓您繼續存取資料，並協助保護資料免受執行個體故障和 AZ 中斷的影響。

選擇單一備份或異地同步備份檔案系統部署

鑑於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異地同步備份檔案系統。單一可用區部署是針對測試和開發工作負載、應用程式層內建複寫且不需要額外儲存層級備援的特定生產工作負載，以及放寬可用性和復原點目標 (RPO) 需求的生產工作負載而設計成本效益的解決方案。具有放鬆可用性需求的工作負載可在計劃的檔案系統維護或意外服務中斷的情況下，容忍最多 20 分鐘的可用性暫時喪失，而且 RPO 需求放鬆的工作負載可以容忍自最近備份以來的資料更新遺失。

依部署類型提供功能支援

下表摘要說明 FSx for Windows File Server 系統部署類型的功能：

部署類型	固态盘存储	硬碟儲存	DFS 命名空間	DFS 複寫	自訂 DNS 名稱	加拿大股票
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 2 檔案系統上建立連續可用的 (CA) 共用，但您應該在異地同步備份檔案系統上使用 CA 共用來進行 SQL Server HA 部署。

FSx for Windows File Server FSx 的容錯移轉程序

如果發生下列任何一種情況，異地同步備份檔案系統會自動從偏好的檔案伺服器容錯移轉到待命檔案伺服器：

- 發生可用區域中斷。
- 首選的文件服務器變為不可用。
- 偏好的檔案伺服器會經過計劃的維護作業。

當從某個檔案伺服器容錯移轉至另一個檔案伺服器時，新的使用中檔案伺服器會自動開始提供所有檔案系統讀取和寫入要 當偏好子網路中的資源可用時，Amazon FSx 會自動容錯回偏好子網路中的慣用檔案伺服器。容錯移轉通常在 30 秒內完成，從偵測到使用中檔案伺服器上的故障，到將待命檔案伺服器升級為使用中狀態。原始異地同步備份組態的容錯回復也會在不到 30 秒的時間內完成，而且只有在偏好子網路中的檔案伺服器完全復原時才會發生。

在檔案系統容錯移轉和故障回復的短暫期間，I/O 可能會暫停，並且 Amazon CloudWatch 指標可能暫時無法使用。

對於異地同步備份檔案系統，如果在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處理。此程序可能需要長達數小時才能處理大量寫入和 IOPS 繁重的工作負載。建議您在檔案系統負載較輕的情況下，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

當從某個檔案伺服器容錯移轉至另一個檔案伺服器時，新的使用中檔案伺服器會自動開始提供所有檔案系統讀取和寫入要 偏好子網路中的資源可用後，Amazon FSx 會自動故障返回偏好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 應用程式來說是透明的，因此 Windows 應用程式會繼續檔案系統作業，而不需要手動 容錯移轉通常在 30 秒內完成，從偵測到使用中檔案伺服器上的故障，到將待命檔案伺服器升級為使用中狀態。原始異地同步備份組態的容錯回復也會在 30 秒內完成，而且只有在偏好子網路中的檔案伺服器完全復原之後才會發生。

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。異地同步備份檔案系統失敗回到偏好子網路中的檔案伺服器後，它們將自動恢復檔案系統作業。

在檔案系統上測試容錯移轉

您可以透過修改異地同步備份檔案系統的輸送量容量來測試容錯移轉。修改檔案系統的輸送量容量時，Amazon FSx 會切換出檔案系統的檔案伺服器。異地同步備份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到新的主要伺服器，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。一旦更新順利完成，您的檔案系統就會容錯移轉至次要伺服器，並且失敗回到主要伺服器。如需修改檔案系統輸送量容量和監視要求進度的詳細資訊，請參閱管理輸送量容量。

使用單一和異地同步備份檔案系統資源

子網

當您建立 VPC 時，它會跨越該區域中的所有可用區域 (AZ)。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一個子網路。各個子網必須完全位於某一可用區域內，不得跨越多個區域。建立單一可用區 Amazon FSx 檔案系統時，請為檔案系統指定單一子網路。您選擇的子網路會定義在其中建立檔案系統的可用區域。

建立異地同步備份檔案系統時，您可以指定兩個子網路，一個用於偏好的檔案伺服器，另一個用於待命檔案伺服器。您選擇的兩個子網路必須位於相同區域內的不同可用區 AWS 域中。

對於內部AWS 應用程式，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，以將延遲降到最低。

文件系统弹性网络接口

當您建立 Amazon FSx 檔案系統時，Amazon FSx 會在 Amazon V irtual Private Cloud (VPC) 佈建一個或多個彈性網路界面，這些界面會與您的檔案系統建立關聯。網路介面可讓您的用戶端與 Windows 檔案伺服器檔案系統的 FSx 進行通訊。儘管是帳戶 VPC 的一部分，但網路界面仍被視為 Amazon FSx 的服務範圍內。異地同步備份檔案系統具有兩個彈性網路介面，每個檔案伺服器各一個。單一可用區檔案系統具有一個 elastic network interface。

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

下表摘要說明適用於 Windows 檔案伺服器檔案系統部署類型之 FSx 的子網路、elastic network interface 和 IP 位址資源：

檔案系統部署類型	子網路數目	彈性網路介面數	IP 位址數目
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，檔案系統在刪除檔案系統之前不會變更其 IP 位址。

> **Important**
>
> Amazon FSx 不支援從公用網際網路存取檔案系統或公開檔案系統。如果彈性 IP 位址 (可從網際網路存取的公用 IP 位址) 連接到檔案系統的 elastic network interface，Amazon FSx 會自動將其分離。

使用亞馬遜 FSx 優化成本

FSx Windows 檔案伺服器提供多種功能，可協助您根據應用程式需求，將總體擁有成本 (TCO) 最佳化。您可以選擇儲存類型 (HDD 或 SSD)，在應用程式的成本與效能需求之間取得適當平衡。您可以彈性地從儲存容量中選擇輸送量容量，以最佳化您的成本。此外，您還可以使用重複資料刪除功能，消除檔案系統上的冗餘資料，將儲存成本最佳化。

主題

靈活選擇儲存和輸送量

使用 FSx 適用於 Windows 檔案伺服器，您可以獨立設定檔案系統的儲存裝置、SSD IOPS 和輸送量容量。這為您提供了靈活性，以實現正確的成本和性能組合。例如，您可以為冷 (通常是非作用中) 工作負載選擇具有相對較小的輸送量容量的大量儲存體，以節省不需要的輸送量成本。或者，作為另一個例子，您可以選擇為相對較小的儲存容量提供大量的輸送量容量。較高的輸送量容量會在檔案伺服器上進行快取的記憶體數量較高。您可以利用檔案伺服器上的快速快取，針對主動存取的資料最佳化效能。如需詳細資訊，請參閱FSx 適用於 FSx for Windows File Server 效能。

您可以在建立檔案系統之後隨時增加儲存容量。如需詳細資訊，請參閱管理儲存容量。您可以在建立檔案系統之後隨時隨地擴充 SSD IOPS，而不受儲存容量影響。如需詳細資訊，請參閱管理固態硬碟 IOPS。您可以隨時增加或減少輸送量容量，提供滿足不斷變化的效能需求的彈性。如需詳細資訊，請參閱管理輸送量容量。

將儲存體成本最佳化

您可以使用 Amazon FSx 以多種方式優化儲存成本，如下所述。

使用儲存類型最佳化成本

FSx Windows 檔案伺服器提供兩種類型的儲存裝置 — 硬碟 (HDD) 和固態硬碟 (SSD)，可讓您將成本最佳化，滿足您的工作負載需求。HDD 儲存裝置專為廣泛的工作負載而設計，包括主目錄、使用者和部門共用，以及內容管理系統。SSD 儲存裝置專為效能最高且延遲最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。如需詳細資訊，請參閱Latency (延遲)和視窗檔案伺服器專用亞馬遜 FSx 定價。

使用重複資料刪除最佳化儲存成本

大型資料集通常具有冗餘資料，因此會增加資料儲存成本。例如，使用者檔案共用可以有同一個檔案的多個副本，由多個使用者儲存。軟體開發共用可以包含許多二進位檔案，這些二進位檔案從組建到建置之間 您可以開啟以降低資料儲存成本重复数据删除用於您的文件系統。重複資料刪除功能開啟後，重複資料刪除功能只會儲存一次資料集的重複部分，自動減少或消除多餘的資料。如需有關 Amazon FSx 檔案系統輕鬆開啟重複資料刪除的詳細資訊，請參閱重复数据删除。

複查用量與帳單

您可以檢閱檔案系統使用情況，包括儲存容量、輸送量容量、備份和資料傳輸。AWS Billing儀表板或 AWS Cost Explorer。這些工具可讓您檢閱資源的使用情況，並依使用類型、地區和其他相關條件篩選和分組。請注意，若要檢視單一檔案系統或單一檔案系統備份的使用情況，您必須啟用該特定資源的標籤，並啟用以標籤為基礎的計費報告。如需詳細資訊，請參閱使用AWS成本分配標籤在AWS Billing用戶指南。

使用 Microsoft 活動目錄在 FSx for Windows File Server

Amazon FSx 的工作與 Microsoft 活動目錄與您現有的 Microsoft Windows 環境集成。Active Directory 是 Microsoft 目錄服務，用於存儲有關網絡上的對象的信息，並使這些信息易於管理員和用戶查找和使用。這些物件通常包括共用資源，例如檔案伺服器和網路使用者和電腦帳戶。

使用 Amazon FSx 建立檔案系統時，請將其加入 Active Directory 網域，以提供使用者身份驗證以及檔案和資料夾層級存取控制。然後，您的使用者可以使用他們在 Active Directory 中現有的使用者身分來驗證自己並存取 Amazon FSx 檔案系統。使用者也可以使用現有的身分來控制對個別檔案和資料夾的存取。此外，您可以將現有的檔案和資料夾以及這些項目的安全存取控制清單 (ACL) 組態移轉至 Amazon FSx，而無需進行任何修改。

Amazon FSx 提供兩個選項，可讓您將 FSx FSx for Windows File Server 檔案系統與活動目錄搭配使用：使用 Amazon FSx AWS Directory Service for Microsoft Active Directory和。使用 Amazon FSx 與您的自我管理 Microsoft 活動目錄

> **Note**
>
> Amazon FSx 支持 Microsoft Azure 活動目錄域服務，您可以加入到 Microsoft Azure 活動目錄。

為檔案系統建立連結的 Active Directory 組態之後，您只能更新下列屬性：

- 服務使用者認證
- DNS 伺服器 IP 位址

建立檔案系統之後，您就無法為加入的 Microsoft AD 變更下列屬性：

- DomainName
- OrganizationalUnitDistinguishedName
- FileSystemAdministratorsGroup

不過，您可以從備份建立新的檔案系統，並在 Microsoft Active Directory 整合組態中為新檔案系統變更這些屬性。如需詳細資訊，請參閱 演練 2：從備份建立檔案系統。

> **Note**
>
> Amazon FSx 不支持活動目錄連接器和簡單的活動目錄。

如果您的作用中目錄組態發生變更而中斷與檔案系統的連線，Windows 檔案伺服器的 FSx 可能會變成設定錯誤。若要將檔案系統返回「可用」狀態，請選取 Amazon FSx 主控台中的「嘗試復原」按鈕，或使用 Amazon FSx API 或主控台中的`StartMisconfiguredStateRecovery`命令。如需更多資訊，請參閱檔案系統處於錯誤設定的狀態。

主題

- 使用 Amazon FSx AWS Directory Service for Microsoft Active Directory
- 使用 Amazon FSx 與您的自我管理 Microsoft 活動目錄

使用 Amazon FSx AWS Directory Service for Microsoft Active Directory

AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) 在雲端中提供完全受控、高可用性、實際的 Active Directory 目錄。您可以在工作負載部署中使用這些作用中目錄。

如果您的組織用 AWS Managed Microsoft AD 於管理身分和裝置，建議您將 Amazon FSx 檔案系統與 AWS Managed Microsoft AD. 這樣，您就可以獲得使用 Amazon FSx 的統包解決方案。 AWS Managed Microsoft AD AWS 處理這兩項服務的部署、作業、高可用性、可靠性、安全性以及無縫整合，讓您能夠專注於有效地運作自己的工作負載。

若要在 AWS Managed Microsoft AD 設定中使用 Amazon FSx，您可以使用 Amazon FSx 主控台。當您在主控台中建立新的 Windows 檔案伺服器檔案系統 FSx 時，請在 [Windows 驗證] 區段下選擇 [AWS 受管理的作用中目錄]。您也可以選擇要使用的特定目錄。如需詳細資訊，請參閱 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) 上管理身分識別和裝置。如果是這樣，您可以將 Amazon FSx 檔案系統直接加入您現有的自我管理活動目錄網域。如需詳細資訊，請參閱 使用 Amazon FSx 與您的自我管理 Microsoft 活動目錄。

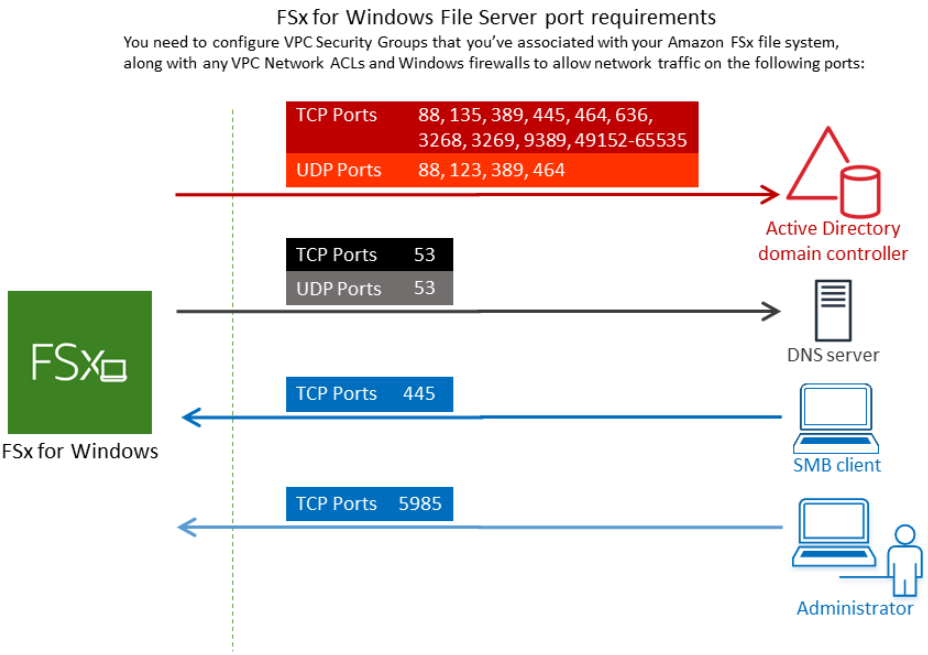
此外，您也可以設定系統以受益於資源樹系隔離模型。在此模型中，您可以將資源 (包括 Amazon FSx 檔案系統) 隔離到個別的活動目錄樹系中，與使用者所在的樹系中。

> **Important**
>
> 對於單一可用區 2 和所有異地同步備份檔案系統，Active Directory 網域名稱不得超過 47 個字元。

網路必要條

在您建立加入 AWS Microsoft 受管理的使用中目錄網域的 Windows 檔案伺服器檔案系統 FSx 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。請確定您要建立 FSx 檔案系統之子網路的安全性群組和 VPC Network ACL 允許連接埠上的流量，並遵循下圖所示的指示。



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 全球編錄

通訊協定	連接埠	角色
TCP	3269	通過 SSL Micros 全局類別目錄
TCP	5985	Micros 視窗遠端管理
TCP	9389	Micros AD DS 網絡服務 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 和所有異地同步備份檔案系統部署都需要在 TCP 連接埠 9389 上允許輸出流量。

> **Note**
>
> 如果您使用 VPC 人雲端網路 ACL，您也必須允許 FSx 檔案系統的動態連接埠 (49152-65535) 上的輸出流量。

- 如果您要將 Amazon FSx 檔案系統連接到不同虛擬私人雲端或帳戶中的 AWS 受管 Microsoft Active Directory，請確保該 VPC 人雲端與您要建立檔案系統的 Amazon VPC 之間的連線。如需詳細資訊，請參閱 在不同的 VPC 或帳戶 AWS Managed Microsoft AD 中使用 Amazon FSx。

> **Important**
>
> 雖然 Amazon VPC 安全群組要求連接埠只能以網路流量起始的方向開啟，但 VPC 網路 ACL 要求連接埠雙向開放。

使用 Amazon FSx 網路驗證工具來驗證您活動目錄網域控制站的連線能力。

使用資源樹系隔離模型

您可以將檔案系統加入安 AWS Managed Microsoft AD 裝程式。然後，您可以在您建立的網域與現有的自我管理 Active Directory AWS Managed Microsoft AD 網域之間建立單向樹系信任關係。對於 Amazon FSx 中的 Windows 身份驗證，您只需要單向性樹系信任，其中 AWS 受管樹系會信任公司網域樹系。

您的公司網域扮演信任網域的角色，而受 AWS Directory Service 管理的網域則是信任網域的角色。經過驗證的驗證要求只會在一個網域之間傳送，讓您公司網域中的帳戶可以針對受管理網域中共用的資源進行驗證。在這種情況下，Amazon FSx 只會與受管網域互動。受管理的網域接著會將驗證要求傳遞至您的公司網域。

測試您的活動目錄配置

建立 Amazon FSx 檔案系統之前，我們建議您使用 Amazon FSx 網路驗證工具驗證活動目錄網域控制站的連線。如需詳細資訊，請參閱 驗證連線到您的作用中目錄網域控制站。

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

- AWS Directory Service 管理指南中的 AWS Directory Service 是什麼
- 在《AWS 管理指南》中建立受AWS Directory Service 管理的活動目錄
- 何時建立《AWS Directory Service 管理指南》中的信任關係
- 演練 1：開始使用的先決條件

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

您可以使用 VPC 對等互連，將 FSx for Windows 檔案伺服器檔案系統加入至相同帳戶內不同 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**
>
> 您只能選擇與您的文件系統 AWS 區域 相同的 AWS Managed Microsoft AD 內容。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 Amazon FSx 與您的自我管理 Microsoft 活動目錄。

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

1. 設定您的網路環境。
2. 分享您的目錄。
3. 將您的檔案系統加入共用目錄。

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

若要設定您的網路環境，您可以使用 AWS Transit Gateway 或 Amazon VPC 並建立 VPC 對等連線。此外，請確定兩個 VPC 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。如需有關使用 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人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) 位址，在它們之間路由流量。您可以使用 VPC 對等連接相同 AWS 區域內或區域之間的 VPC。 AWS 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帳戶不同的 AWS Managed Microsoft AD 目錄時，還有另一個先決條件。您還需要與其他帳戶共享您的 Microsoft 活動目錄。要做到這一點，你可以使用 AWS 管理 Microsoft 活動目錄的目錄共享功能。若要深入了解，請參閱《AWS Directory Service 管理指南》中的共用目錄。

驗證連線到您的作用中目錄網域控制站

在您建立加入作用中目錄的 Windows 檔案伺服器檔案系統 FSx 之前，請使用 Amazon FSx 作用中目錄驗證工具來驗證您的作用中目錄網域的連線。您可以使用此測試，無論您是使用帶有 AWS 受管理 Microsoft 活動目錄的 FSx for Windows File Server，還是使用自我管理的作用中目錄組態。網域控制站網路連線性測試 (TEST-FSxadControllerConnection) 不會針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。請改為使用此測試，針對特定的網域控制站集執行網路連線驗證。

驗證與您的作用中目錄網域控制站的連線

1. 在相同的子網路中啟動 Amazon EC2 Windows 執行個體，並使用您將用於 Windows 檔案伺服器檔案系統 FSx 的相同 Amazon VPC 安全群組。對於異地同步備份部署類型，請使用偏好的作用中檔案伺服器的子網路。
2. 將您的 EC2 視窗執行個體加入您的活動目錄。如需詳細資訊，請參閱《管理指南》中的〈手動加入 Windows 執行個體AWS Directory Service 〉。

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到 Windows 執行個體。
4. 在 EC2 執行個體上開啟 Windows PowerShell 視窗 (使用「以系統管理員身分執行」)。

   若要測試 Windows 所需的使用中目錄模組 PowerShell 是否已安裝，請使用下列測試指令。

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

   如果以上返回錯誤，請使用以下命令進行安裝。

   ```
   PS C:\> Install-WindowsFeature RSAT-AD-PowerShell
   ```
5. 使用下列指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. 將亞馬遜 FSxad 驗證模塊添加到當前會話中。

   ```
   PS C:\> Import-Module .\AmazonFSxADValidation
   ```
8. 設定使用中目錄網域控制站 IP 位址的值，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

使用 Amazon FSx 與您的自我管理 Microsoft 活動目錄

如果您的組織在自我管理的 Active Directory 內部部署或雲端中管理身分識別和裝置，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。若要搭配使用 Amazon FSx AWS Managed Microsoft AD，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] 下的 [自我管理 Microsoft 作用中目錄]。為您的自我管理作用中目錄提供下列詳細資料：

- 自我管理目錄的完整網域名稱

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

> **Note**
>
> 對於單一可用區 2 和異地同步備份檔案系統，Active Directory 網域名稱不得超過 47 個字元。

- 您網域的 DNS 伺服器 IP 位址

  DNS 伺服器 IP 位址、使用中目錄網域控制站 IP 位址和用戶端網路必須符合下列需求：

適用於 2020 年 12 月 17 日之前建立的檔案系統	適用於 2020 年 12 月 17 日之後建立的檔案系統
IP 位址必須在 RFC 1918 私有 IP 位址範圍內： • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	IP 位址可以在任何範圍內，但下列情況除外： • 與 Amazon Web Services 衝突的 IP 地址在該 AWS 區域擁有的 IP 地址。如需依地區分類的 AWS 擁有 IP 位址清單，請參閱 AWS IP 位址範圍。 • 位於下列 CIDR 區塊範圍內的 IP 位址：

> **Note**
>
> 您的使用中目錄網域控制站必須是可寫入的。

- 您活動目錄網域上服務帳戶的使用者名稱和密碼，供 Amazon FSx 用來將檔案系統加入您的活動目錄網域
- (選擇性) 您要加入檔案系統的網域中的組織單位 (OU)
- (選擇性) 您想要委派權限以在檔案系統上執行管理動作的網域群組。例如，此網域群組可能會管理 Windows 檔案共用、管理檔案系統根資料夾上的存取控制清單 (ACL)、取得檔案和資料夾的擁有權等等。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您的作用中目錄中必須是唯一的。在下列情況下，Windows 檔案伺服器的 FSx 將不會建立網域群組：
>
> - 如果您指定的名稱已存在群組
> - 如果您沒有指定名稱，且您的 Active Directory 中已經存在名為「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 活動目錄網域。

> **Important**
>
> 如果您使用 Microsoft DNS 做為預設 DNS 服務，Amazon FSx 只會為檔案系統註冊 DNS 記錄。如果您使用的是第三方 DNS，則必須在建立 Amazon FSx 檔案系統之後手動設定 DNS 項目。

當您將檔案系統直接加入自我管理的 Active Directory 時，Windows 檔案伺服器的 FSx 位於相同的作用中目錄樹系 (包含網域、使用者和電腦的 Active Directory 組態中的最上層邏輯容器)，以及與使用者和現有資源 (包括現有檔案伺服器) 相同的 Active Directory 網域中。

> **Note**
>
> 您可以將資源 (包括 Amazon FSx 專案系統) 隔離到個別的活動目錄樹系中，與使用者所在的樹系中。若要這麼做，請將您的系統加入 AWS 受管理的 Active Directory，並在您建立的受管理 Active Directory 與現有的自我 AWS 管理 Active Directory 之間建立單向樹系信任關係。

主題

使用自我管理的 Microsoft 活動目錄的先決條件

建立加入自我管理 Microsoft 活動目錄網域的 Amazon FSx 檔案系統之前，請先檢閱下列先決條件。

主題

內部部署組

請確定您擁有可以加入 Amazon FSx 檔案系統的現場部署或其他自我管理的 Microsoft Active Directory。您的內部部署作用中目錄應具有下列組態：

- 您的作用中目錄網域控制站在 Windows 伺服器 2008 R2 或更高版本的網域功能層級。
- DNS 伺服器 IP 位址和使用中的目錄網域控制站 IP 位址如下所示，視您的檔案系統建立時間而定：

適用於 2020 年 12 月 17 日之前建立的檔案系統	適用於 2020 年 12 月 17 日之後建立的檔案系統
IP 位址必須在 RFC 1918 私有 IP 位址範圍內： • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	IP 位址可以在任何範圍內，但下列情況除外： • 與 Amazon Web Services 衝突的 IP 地址在該 AWS 區域擁有的 IP 地址。如需依地區分類的 AWS 擁有 IP 位址清單，請參閱 AWS IP 位址範圍。 • 位於下列 CIDR 區塊範圍內的 IP 位址：

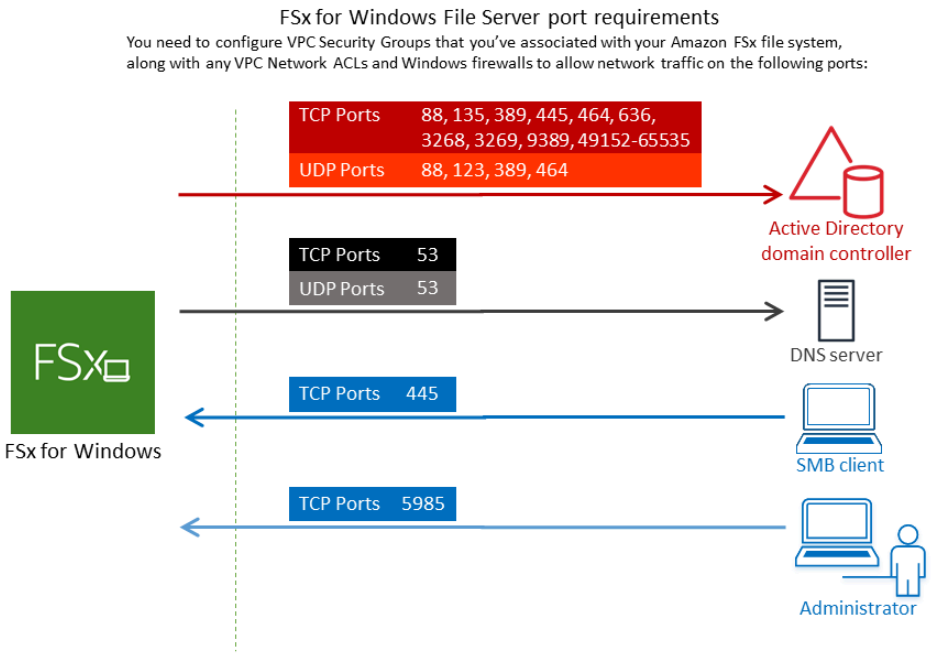
  如果您需要使用非私有 IP 位址範圍存取在 2020 年 12 月 17 日之前建立的 Windows 檔案伺服器檔案系統 FSx，您可以透過還原檔案系統的備份來建立新的檔案系統。如需詳細資訊，請參閱 使用備份。
- 非單一標籤網域 (SLD) 格式的網域名稱。Amazon FSx 不支持 SLD 域。
- 對於單一可用區 2 和所有異地同步備份檔案系統，Active Directory 網域名稱不得超過 47 個字元。
- 如果您已定義 Active Directory 站台，則 VPC 中與 Amazon FSx 檔案系統相關聯的子網路必須定義在 Active Directory 站台中，且 VPC 中的子網路與其他網站中的子網路之間不得發生衝突。
- 您可能需要將規則新增到防火牆，以允許您的作用中目錄網域控制站和 Amazon FSx 之間的 ICMP 流量。

網路組態

本節說明將檔案系統加入您自我管理的 Active Directory 所需的網路組態。

我們建議您先使用 Amazon FSx 活動目錄驗證工具來測試您的網路設定，然後再嘗試將檔案系統加入自我管理的活動目錄。

- 必須在您要建立檔案系統的 Amazon VPC 和自我管理的 Active Directory 之間設定連線能力。您可以使用 AWS Direct Connect、、AWS Virtual Private NetworkVPC 對等互連或來設定此連線。AWS Transit Gateway
- 對於 VPC 安全群組，必須將預設 Amazon VPC 的預設安全群組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性群組和 VPC Network ACL 允許連接埠上的流量，並按照下圖所示的指示進行流量。



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	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)

通訊協定	連接埠	角色
TCP	135	分散式計算環境/端點對應器 (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 全球編錄
TCP	3269	通過 SSL Microsoft 全局類別目錄
TCP	5985	Microsoft 視窗遠端管理
TCP	9389	Microsoft 活動目錄 DS Web 服務, PowerShell
TCP	49152 - 65535	適用於 RPC 的暫時性連接埠

請確定這些流量規則也會鏡像到適用於每個 Active Directory 網域控制站、DNS 伺服器、FSx 用戶端和 FSx 系統管理員的防火牆上。

Important

單一可用區 2 和異地同步備份檔案系統部署需要在 TCP 連接埠 9389 上允許輸出流量。

Note

如果您使用 VPC 人雲端網路 ACL，您也必須允許 FSx 檔案系統的動態連接埠 (49152-65535) 上的輸出流量。

Important

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

服務帳戶權限

請確定您在自我管理的 Microsoft Active Directory 中有一個具有委派權限的服務帳戶，以將電腦加入網域。服務帳戶是指已委派特定工作的自我管理 Microsoft Active Directory 中的使用者帳戶。

服務帳戶必須至少委派您加入檔案系統的 OU 中的下列權限：

- 能夠重置密碼
- 限制帳戶讀取和寫入資料的能力
- 已驗證能夠寫入 DNS 主機名稱
- 已驗證能夠寫入服務主體名稱
- 建立和刪除電腦物件的能力 (可委派)
- 經過驗證的讀取和寫入帳戶限制功能
- 修改權限的能力

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

如需使用正確權限建立服務帳戶的詳細資訊，請參閱 將權限委派給您的 Amazon FSx 服務帳戶 。

Amazon FSx 需要在 Amazon FSx 檔案系統整個生命週期內擁有有效的服務帳戶。Amazon FSx 必須能夠完全管理檔案系統，並執行需要使用服務帳戶取消加入和重新加入 Active Directory 網域的任務。這些工作包括取代失敗的檔案伺服器或修補 Windows 伺服器軟體。您必須使用 Amazon FSx 更新您的活動目錄組態 (包括服務帳戶登入資料)。如需詳細資訊，請參閱 保持您的活動目錄配置更新。

Amazon FSx 需要連線到活動目錄環境中的所有網域控制站。如果您有多個網域控制站，請確定所有網域控制站都符合上述需求，並確定您的服務帳戶的任何變更都會傳播到所有的網域控制站。

您可以使用 Amazon FSx 作用中目錄驗證工具來驗證您的作用中目錄組態，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目，您也可以在內部部署網域控制站和 AWS Managed Microsoft AD. 如需詳細資訊，請參閱 使用資源樹系隔離模型。

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

將 FSx FSx for Windows File Server 檔案系統加入自我管理的 Microsoft 活動目錄網域的最佳作法

當您將 Amazon FSx FSx for Windows File Server 加入系統到您自我管理的 Microsoft 活動目錄時，我們建議您使用這些最佳實務。

將權限委派給您的 Amazon FSx 服務帳戶

請務必以所需的最低權限設定您提供給 Amazon FSx 的服務帳戶。此外，請將組織單位 (OU) 與其他網域控制站問題隔離。

若要將 Amazon FSx 檔案系統加入您的網域，請確定服務帳戶具有委派的權限。網域管理員群組的成員擁有足夠的權限來執行此工作。不過，最佳作法是使用僅具有執行此操作所需最低權限的服務帳戶。下列程序示範如何僅委派將 Amazon FSx 檔案系統加入您的網域所需的權限。

您可以使用 [使用中的目錄使用者和電腦 MMC 嵌入式管理單元中的委派控制項或進階功能來指派這些權限。

在已加入 Active Directory 且已安裝Active Directory User and Computers MMC嵌入式管理單元的電腦上執行下列任一程序。

使用委派控制將權限指派給服務帳戶或群組

1. 以您的作用中目錄網域的網域系統管理員身分登入您的系統。
2. 開啟使用中目錄使用者和電腦 MMC 嵌入式管理單元。
3. 在工作窗格中，展開網域節點。
4. 找出並開啟您要修改之 OU 的內容 (按一下滑鼠右鍵) 功能表，然後選擇 [委派控制]。
5. 在 [委派控制精靈] 頁面上，選擇 [下一步]。
6. 選擇 [新增] 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. 選擇資料夾中的 [只有下列物件]，然後選擇 [電腦物件]。
9. 選擇在此資料夾中建立選取的物件，然後選擇刪除此資料夾中的選取物 然後選擇下一步。
10. 對於「權限」，請選擇下列項目：

    - 重設密碼
    - 讀取和寫入帳戶限制

- 已驗證寫入 DNS 主機名稱
- 已驗證的寫入服務主要名稱

11. 選擇 Next (下一步)，然後選擇 Finish (完成)。
12. 關閉使用中目錄使用者和電腦 MMC 嵌入式管理單元。

使用進階功能指派權限

1. 以您的作用中目錄網域的網域系統管理員身分登入您的系統。
2. 開啟使用中目錄使用者和電腦 MMC 嵌入式管理單元。
3. 從功能表列選取 [檢視]，並確定已啟用 [進階功能] (如果啟用此功能，旁邊會出現核取記號)。
4. 在工作窗格中，展開網域節點。
5. 找出並開啟 (按一下滑鼠右鍵) 您要修改之 OU 的內容功能表，然後選擇 [內容]。
6. 在 [OU 內容] 窗格中，選取 [安全性] 索引標籤。
7. 在「安全性」標籤中，選取「進階」。然後選取 [新增]。
8. 在權限輸入頁面上，選擇選取主體，然後輸入 Amazon FSx 服務帳戶或群組的名稱。針對「套用至:」，選擇「子系電腦」物件。請確定已選取下列項目：

   - 修改權限
   - 建立電腦物件
   - 刪除電腦物件

9. 選取 [套用]，然後選取 [確定]。
10. 關閉使用中目錄使用者和電腦 MMC 嵌入式管理單元。

> **Important**
>
> 建立檔案系統之後，請勿移動 Amazon FSx 在 OU 中建立的電腦物件。這樣做會導致您的檔案系統設定錯誤。如果您使用新的服務帳戶更新檔案系統，請確定新的服務帳戶具有與檔案系統相關聯之現有電腦物件的「完全控制」權限。

保持您的活動目錄配置更新

為了確保 Amazon FSx 檔案系統的持續不中斷可用性，您需要在變更自我管理的 Active Directory 設定時更新檔案系統的 Active Directory 組態。

例如，如果您的 Active Directory 使用以時間為基礎的密碼重設政策，一旦密碼重設，請務必使用 Amazon FSx 更新服務帳戶密碼。同樣地，如果您的作用中目錄網域的 DNS 伺服器 IP 位址變更，一旦發生變更，請使用 Amazon FSx 更新 DNS 伺服器 IP 位址。如需詳細資訊，請參閱 更新自我管理的作用中目錄組態。

當您更新 Amazon FSx 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]。在套用更新之後，確認狀態切換回 [可用] — 請注意，更新可能需要數分鐘才能完成。如需詳細資訊，請參閱 監視自我管理作用中目錄更新。

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為 [設定錯誤]。此狀態會在主控台、API 和 CLI 中的檔案系統說明旁顯示錯誤訊息和建議的更正動作。採取建議的更正動作之後，請確認檔案系統的狀態最終變更為「可用」。

若要深入了解疑難排解可能的自我管理 Active Directory 錯誤設定，請參閱。檔案系統處於錯誤設定的狀態

使用安全群組限制 VPC 內的流量

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

為檔案系統的網路介面建立輸出安全性群組規則

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

驗證您的活動目錄配置

在您建立連接到活動目錄的 Windows 檔案伺服器檔案系統 FSx 之前，我們建議您使用 Amazon FSx 作用中目錄驗證工具來驗證您的作用中目錄組態。請注意，輸出網際網路連線需要成功驗證 Active Directory 組態。

若要驗證您的作用中目錄組態

1. 在相同的子網路中啟動 Amazon EC2 Windows 執行個體，並使用您用於 Windows 檔案伺服器檔案系統 FSx 的相同 Amazon VPC 安全群組。確保您的 EC2 執行個體具有所需的 `AmazonEC2ReadOnlyAccess` IAM 許可。您可以使用 IAM 政策模擬器驗證 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. 將您的 EC2 視窗執行個體加入您的活動目錄。如需詳細資訊，請參閱《管理指南》中的〈手動加入 Windows 執行個體AWS Directory Service〉。
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到 Windows 執行個體。
4. 在 EC2 執行個體上開啟 Windows PowerShell 視窗 (使用「以系統管理員身分執行」)。

   若要測試 Windows 所需的使用中目錄模組 PowerShell 是否已安裝，請使用下列測試指令。

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

   如果以上返回錯誤，請使用以下命令進行安裝。

   ```
   PS C:\> Install-WindowsFeature RSAT-AD-PowerShell
   ```
5. 使用下列指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模塊添加到當前會話。

   ```
   PS C:\> Import-Module .\AmazonFSxADValidation
   ```
8. 通過替換以下命令來設置所需的參數：

   - 活動目錄域名（*## .COM*）
   - 使用下列其中一個選項為服務帳戶密碼準備$Credential物件。
     - 若要以互動方式產生認證物件，請使用下列命令。

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

     - 若要使用 AWS Secrets Manager 資源產生認證物件，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 ### IP ## (IP ## 1#IP ## 2)*
- 您打算在其中建立 Amazon FSx 檔案系統的子網路識別碼 (例如，*SUBNET_2*)。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. (選擇性) 在執行驗證工具之前 DomainControllersMaxCount，依照內含README.md檔案中的指示，設定組織單位、委派管理員群組，並啟用服務帳戶權限驗證。

> **Note**
>
> 如果作業系統不是英文，Domain Admins群組會有不同的名稱。例如，群組以法文作業系統版本命名Administrateurs du domaine。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. 下面是一個成功的測試結果的例子。

```
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
```

以下是含有錯誤之測試結果的範例。

```
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中包含的疑難排解指南 (TROUBLESHOOTING.md) 和疑難排解 Amazon FSx。

將 Amazon FSx 檔案系統加入自我管理的 Microsoft 活動目錄網域

當您建立新的 FSx for Windows File Server 系統時，您可以設定 Microsoft 活動目錄整合，使其加入到您自我管理的 Microsoft 活動目錄網域。若要這麼做，請為您的 Microsoft 作用中目錄提供下列資訊：

- 內部部署 Microsoft 活動目錄目錄的完整網域名稱。

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

- 您網域之 DNS 伺服器的 IP 位址。
- 內部部署 Microsoft 活動目錄網域中服務帳戶的認證。Amazon FSx 使用這些登入資料加入您的自我管理作用中目錄。

或者，您也可以指定以下內容：

- 您希望 Amazon FSx 檔案系統加入的網域內的特定組織單位 (OU)。
- 其成員被授與 Amazon FSx 檔案系統管理權限之網域群組的名稱。

> **Note**
>
> 您提供的網域群組名稱在您的作用中目錄中必須是唯一的。在下列情況下，Windows 檔案伺服器的 FSx 將不會建立網域群組：
>
> - 如果您指定的名稱已存在群組
> - 如果您沒有指定名稱，且您的 Active Directory 中已經存在名為「網域管理員」的群組。

指定此資訊之後，Amazon FSx 會使用您提供的服務帳戶，將您的新檔案系統加入您的自我管理 Active Directory 網域。

> **Important**
>
> Amazon FSx 僅在您加入檔案系統的使用中目錄網域使用 Microsoft DNS 作為預設 DNS 時，才會註冊該檔案系統的 DNS 記錄。如果您使用的是第三方 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。如需選擇用於檔案系統之正確 IP 位址的詳細資訊，請參閱取得要用於 DNS 的正確檔案系統 IP 位址。

開始之前

請確定您已完成中的使用自我管理的 Microsoft 活動目錄的先決條件詳細資訊使用 Amazon FSx 與您的自我管理 Microsoft 活動目錄。

若要建立連接到自我管理的作用中目錄 (主控台) 的 Windows 檔案伺服器檔案系統 FSx

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 在儀表板上，選擇 Create file system (建立檔案系統) 以啟動檔案系統建立精靈。
3. 針對 Windows 檔案伺服器選擇「FSx」，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，再加上 +-= 的特殊字元。_:/
5. 對於儲存容量，請輸入檔案系統的儲存容量 (以 GiB 為單位)。如果您使用的是固態硬碟儲存空間，請輸入介於 32 到 65,536 範圍內的任何整數。如果您使用的是硬碟儲存空間，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。

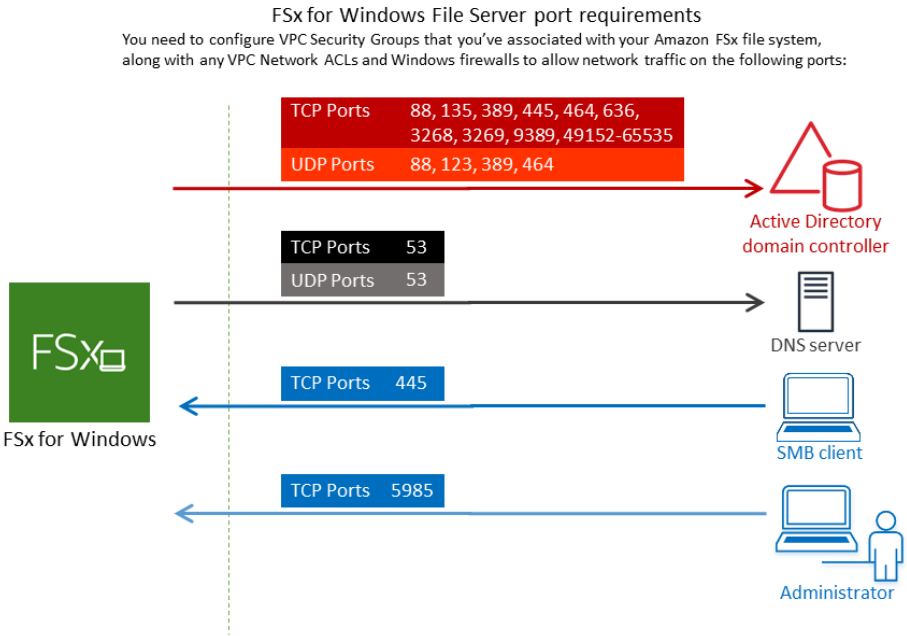
6. 保留 Throughput capacity (輸送容量) 的預設設定。輸送量容量是代管檔案系統的檔案伺服器可以提供資料的持續速度。[建議的輸送量容量] 設定是根據您選擇的儲存容量量而定。如果您需要超過建議的輸送量容量，請選擇 [指定輸送量容量]，然後選擇一個值。如需詳細資訊，請參閱 FSx 適用於 FSx for Windows File Server 效能。

   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關聯的 VPC。為了進行此入門練習的目的，請選擇與 AWS 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。請確定您要建立 FSx 檔案系統之子網路的安全性群組和 VPC Network ACL 允許連接埠上的流量，並按照下圖所示的指示進行流量。



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 全球編錄

通訊協定	連接埠	角色
TCP	3269	通過 SSL Micros 全局類別目錄
TCP	5985	Micros 視窗遠端管理
TCP	9389	Micros 活動目錄 DS Web 服務, Power

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 和所有異地同步備份檔案系統部署都需要在 TCP 連接埠 9389 上允許輸出流量。

Note

如果您使用 VPC 人雲端網路 ACL，您也必須允許 FSx 檔案系統的動態連接埠 (49152-65535) 上的輸出流量。

- 輸出規則，允許所有流量傳送至與您自我管理的 Microsoft Active Directory 網域的 DNS 伺服器和網域控制站相關聯的 IP 位址。如需詳細資訊，請參閱 Microsoft 關於設定防火牆以進行作用中目錄通訊的文件。
- 請確定這些流量規則也會鏡像到適用於每個 Active Directory 網域控制站、DNS 伺服器、FSx 用戶端和 FSx 系統管理員的防火牆上。

> **Note**
>
> 如果您已定義 Active Directory 站台，則必須確保 VPC 中與 Amazon FSx 檔案系統相關聯的子網路已定義在 Active Directory 站台中，且 VPC 中的子網路與其他網站中的子網路之間沒有衝突。您可以使用 [使用中的目錄站台和服務 MMC 嵌入式管理單元來檢視和變更這些設定。

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

10. 對於 Windows 驗證，請選擇自我管理 Microsoft 活動目錄。
11. 為自我管理的 Microsoft 活動目錄目錄的完整網域名稱輸入一個值。

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

> **Important**
>
> 對於單一可用區 2 和所有異地同步備份檔案系統，Active Directory 網域名稱不得超過 47 個字元。

12. 為自我管理的 Microsoft 活動目錄目錄的組織單位輸入值。

> **Note**
>
> 請確定您提供的服務帳戶具有委派給您在此處指定的 OU 或預設 OU 的權限 (如果未指定 OU)。

13. 為自我管理的 Microsoft 活動目錄目錄的 DNS 服務器 IP 地址輸入至少一個值，但不超過兩個值。
14. 為您自我管理的 Active Directory 網域上的帳戶輸入服務帳戶使用者名稱的字串值，例如`ServiceAcct`。Amazon FSx 使用此用戶名加入到您的 Microsoft 活動目錄域。

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

15. 輸入您自我管理的 Active Directory 網域上帳戶的服務帳戶密碼值。Amazon FSx 使用此密碼加入到您的 Microsoft 活動目錄域。
16. 在確認密碼中重新輸入密碼以確認密碼。
17. 對於委派檔案系統管理員群組，請指定Domain Admins群組或自訂委派檔案系統管理員群組 (如果您已建立群組)。您指定的群組應具有委派的授權，可以在檔案系統上執行管理工作。如果您沒有提供值，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Domain Admins擁有 Delegated file system administrators group (您指定的群組或自訂群組)。

> **Important**
>
> 如果您未提供委派的檔案系統管理員群組，Amazon FSx 預設會嘗試在您的 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，或是您使用不同的群組進行網域管理，您必須在此提供該群組的名稱。

> **Important**
>
> 提供群組名稱參數時，請勿包含網域前置詞 (corp.com\ FSxAdmins) 或網域尾碼 (F SxAdmins @corp .com)。
> 請勿使用群組的辨別名稱 (DN)。辨別名稱的範例為 CN=F SxAdmins、OU = 範例、DC = 公司、DC = COM。

若要建立連接到自我管理的作用中目錄的 Windows 檔案伺服器檔案系統的 FSx ()AWS CLI

下列範例會SelfManagedActiveDirectoryConfiguration在us-east-2可用區域中建立適用於 Windows 檔案伺服器檔案系統的 FSx。

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

取得要用於 DNS 的正確檔案系統 IP 位址

如果您使用 Microsoft DNS 做為預設 DNS 服務，Amazon FSx 只會為檔案系統註冊 DNS 記錄。如果您使用的是第三方 DNS，則需要為 Amazon FSx 檔案系統手動設定 DNS 項目。本節說明如果您必須手動將檔案系統新增至 DNS，如何取得要使用的正確檔案系統 IP 位址。請注意，一旦建立檔案系統，其 IP 位址必須等到檔案系統被刪除才會變更。

如何取得要用於 DNS A 項目的檔案系統 IP 位址

1. 在 https://console.aws.amazon.com/fsx/ 中，選擇您要取得 IP 位址的檔案系統，以顯示檔案系統詳細資訊頁面。
2. 在 [網路與安全性] 索引標籤中，執行下列其中一項動作

   - 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 位址會顯示在主要私人 IPv4 IP 欄中。
   - 對於單一可用區 2 或異地同步備份檔案系統：
     - 在「偏好的子網路」面板中，選擇「網路界面」下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。

- 要使用的偏好子網路的 IP 位址會顯示在次要私人 IPv4 IP 欄中。
- 在 Amazon FSx 待命子網路面板中，選擇網路界面下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的 IP 位址會顯示在次要私人 IPv4 IP 欄中。

> **Note**
>
> 如果您需要為單一可用區 2 或異地同步備份檔案系統的 Windows 遠 PowerShell 端端點設定 DNS 項目，您應該為偏好的子網路的 elastic network interface 使用主要私人 IPv4 位址。如需詳細資訊，請參閱 使用 Amazon FSx CLI PowerShell。

更新自我管理的作用中目錄組態

您可以使用 Amazon FSx API AWS Management Console，或更新服務帳戶使 AWS CLI 用者名稱和密碼，以及檔案系統自我管理的使用中目錄組態的 DNS 伺服器 IP 位址。您可以隨時使用 CLI 和 API 追蹤自我管理的 Active Directory 組態更新的進度。 AWS Management Console如需詳細資訊，請參閱 監視自我管理作用中目錄更新。

更新自我管理的作用中目錄組態 (主控台)

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 瀏覽至 [檔案系統]，然後選擇您要更新其自我管理的使用中目錄組態的 Windows 檔案系統。
3. 在 [網路與安全性] 索引標籤中，然後針對 DNS 伺服器 IP 位址或服務帳戶使用者名稱選擇 [更新]，視您要更新的 Active Directory 內容而定。
4. 在出現的對話方塊中輸入新的 DNS 伺服器 IP 位址或新的服務帳戶認證。
5. 選擇「更新」以起始「作用中目錄」組態更新。

   您可以使用 AWS Management Console 或監視更新進度 AWS CLI。

若要更新自我管理的作用中目錄組態 (CLI)

- 若要更新 Windows 檔案伺服器檔案系統 FSx 的自我管理作用中目錄組態，請使用 AWS CLI 指令更新檔案系統。設定下列參數：
  - `--file-system-id`到您正在更新的文件系統的 ID。

- `UserName`自我管理的 Active Directory 服務帳戶的新使用者名稱。
- `Password`自我管理作用中目錄服務帳戶的新密碼。
- `DnsIps`自我管理的作用中目錄 DNS 伺服器的 IP 位址。

```
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。響應中的`AdminstrativeActions`對象描述了請求及其狀態。

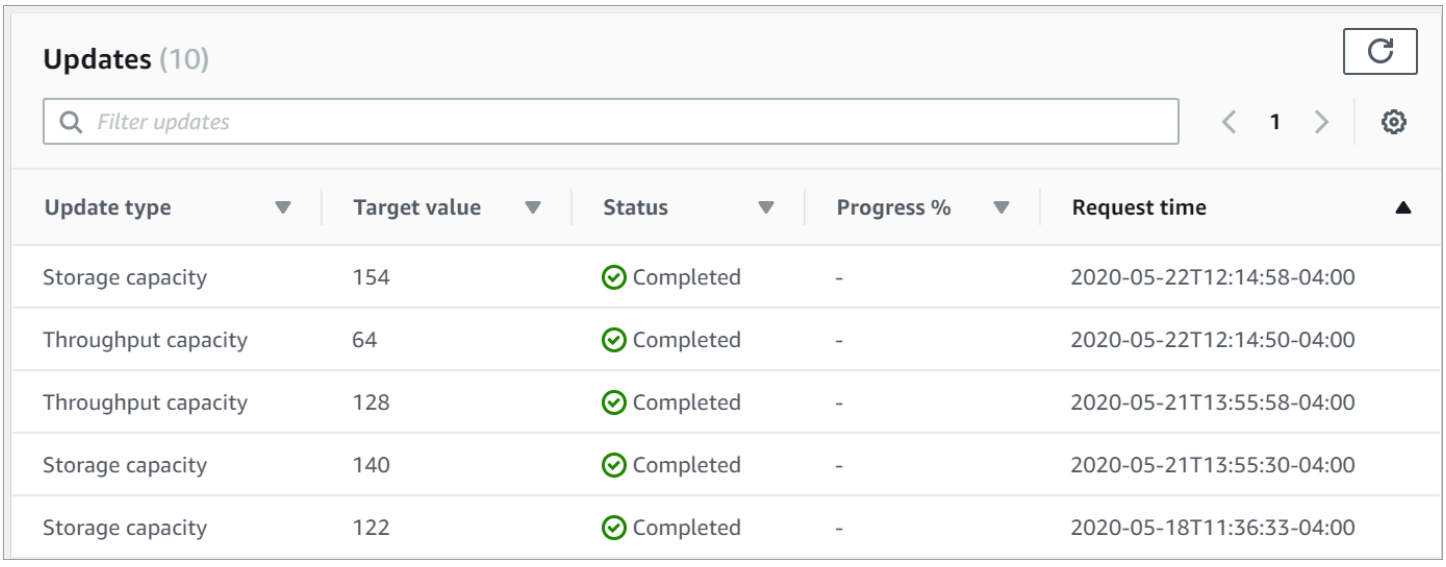
監視自我管理作用中目錄更新

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] 切換為 [更新]。更新完成後，狀態會切換回「可用」— 請注意，更新最多可能需要數分鐘才能完成。

您可以使用 API 或下列各節中所述 AWS Management Console，監視自我管理的 Active Directory 組態更新的進度。 AWS CLI

在主控台中監視更新

在 [檔案系統詳細資料] 視窗的 [更新] 索引標籤中，您可以檢視每種更新類型的 10 個最新更新。



對於自我管理的 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
- 服務帳戶認證

目標值

要將檔案系統屬性更新為的所需值。對於服務帳戶認證更新，只會顯示使用者名稱，服務帳戶密碼永遠不會包含在此欄位中。

狀態

更新的目前狀態。對於自我管理的使用中目錄更新，可能的值如下所示：

- 擱置中 — Amazon FSx 已收到更新要求，但尚未開始處理更新要求。
- 進行中 — Amazon FSx 正在處理更新請求。
- 已完成 — 檔案系統更新順利完成。
- 失敗 — 檔案系統更新失敗。選擇問號 (?)，以查看有關失敗的詳細資訊。

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 收到更新動作要求的時間。

使用 AWS CLI 和 API 監控更新

您可以使用描述檔案系統 AWS CLI 命令和「系統 API」動作來檢視和監視正在進行的檔案系統更新要求。DescribeFileAdministrativeActions陣列會列出每個管理動作類型的 10 個最新更新動作。

下列範例會顯示 describe-file-systems CLI 命令回應的摘錄，顯示兩個自我管理的 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."
                    }
                }
            ],
        .
        .
        .
```

使用 Microsoft 視窗檔案共用

Microsoft Windows 檔案共用是檔案系統中的特定資料夾。它包含該資料夾的子資料夾，您可以透過伺服器訊息區 (SMB) 通訊協定讓您的運算執行個體存取這些子資料夾。您的檔案系統隨附一個預設的 Windows 檔案共用，名為`share`. 您可以使用名為共用資料夾的 Windows 圖形使用者介面 (GUI) 工具來建立和管理任意數量的其他 Windows 檔案共用。

存取檔案共用

若要存取檔案共用，您可以使用 Windows Map 網路磁碟機功能，將運算執行個體上的磁碟機代號對應至 Amazon FSx 檔案共用。將檔案共用對應至運算執行個體上的磁碟機的程序稱為在 Linux 中掛載檔案共用。這個程序會根據運算執行個體的類型和作業系統而有所不同。對應檔案共用之後，您的應用程式和使用者可以存取檔案共用上的檔案和資料夾，就像是本機檔案和資料夾一樣。

以下是在不同支援的運算執行個體上對應檔案共用的程序。

主題

在 Amazon EC2 窗口實例上映射文件共享

您可以使用 Windows 檔案總管或命令提示字元，在 EC2 Windows 執行個體上對應檔案共用。

若要在 Amazon EC2 Windows 執行個體 (主控台) 上對應檔案共用

1. 啟動 EC2 視窗執行個體，並將其連接到您加入 Amazon FSx 檔案系統的 Microsoft 活動目錄。若要執行此操作，請從《AWS Directory Service 管理指南》中選擇下列其中一個程序：
   - 無縫加入執行個體
   - 手動聯結視窗執行個體
2. 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到您的 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) 功能表，然後選擇 [對應網路磁碟機]。
5. 在「磁碟機」中，選擇磁碟機代號。
6. 在資料夾中，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。

> **Important**
>
> 在異地同步備份檔案系統的容錯移轉程序期間，使用 IP 位址而非 DNS 名稱可能會導致無法使用。此外，異地同步備份和單一可用區檔案系統中的 Kerberos 型驗證也需要 DNS 名稱或相關聯的 DNS 別名。

您可以選擇 Windows 檔案伺服器、網路和安全性，在 Amazon FSx 主控台上找到檔案系統的 DNS 名稱和任何相關的 DNS 別名。或者，您可以在CreateFile系統或系DescribeFile統 API 操作的響應中找到它們。如需有關使用 DNS 別名的詳細資訊，請參閱管理 DNS 別名。

- 對於加入 AWS 管理 Microsoft 活動目錄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，以及任何異地同步備份檔案系統，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，請在資料夾中輸入以下內容。

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

若要使用異地同步備份檔案系統的 DNS 名稱，請在「資料夾」中輸入以下內容。

```
\\famznfsxaa11bb22.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」中輸入以下內容。

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

7. 選擇登入時重新連線的選項，指出是否應在登入時重新連線檔案共用，然後選擇 [完成]。

若要在 Amazon EC2 Windows 執行個體上對應檔案共用 (命令提示字元)

1. 啟動 EC2 視窗執行個體，並將其連接到您加入 Amazon FSx 檔案系統的 Microsoft 活動目錄。若要執行此操作，請從《AWS Directory Service 管理指南》中選擇下列其中一個程序：
   - 無縫加入執行個體
   - 手動聯結視窗執行個體
2. 以 AWS Managed Microsoft AD 目錄中的使用者身分 Connect 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到您的 Windows 執行個體。
3. 連線後，開啟命令提示字元視窗。
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 檔案伺服器、網路和安全性，使用 Amazon FSx 主控台找到 DNS 名稱。或者，您可以在`CreateFileSystem`或 `DescribeFileSystems` API 作業的回應中找到它們。
   - 對於加入 AWS 管理 Microsoft 活動目錄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，以及任何異地同步備份檔案系統，DNS 名稱如下所示。

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

   以下是掛載檔案共用的範例命令。

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

   您還可以使用任何支持的`net use`命 PowerShell 令來掛載文件共享，而不是命令。

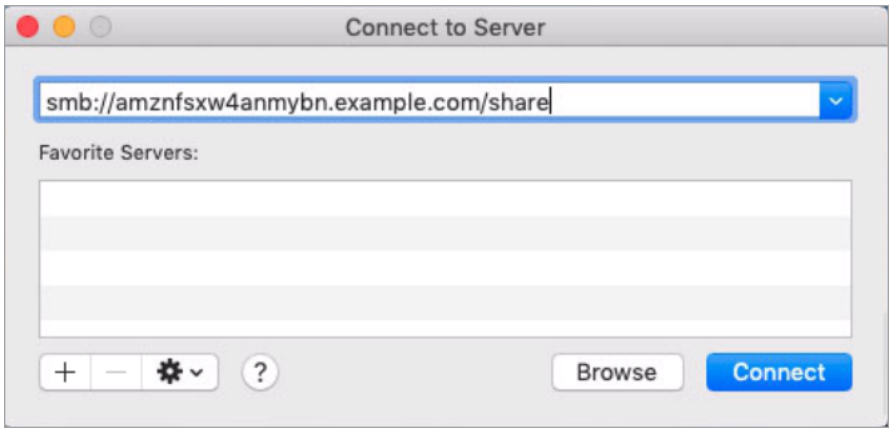
在 Amazon EC2 Mac 執行個體上掛載檔案共用

您可以在加入您的活動目錄或未加入的 Amazon EC2 Mac 執行個體上掛載檔案共用。如果執行個體未加入您的作用中目錄，請務必更新為執行個體所在的 Amazon Virtual Private Cloud (Amazon VPC) 設定的 DHCP 選項，以包含您活動目錄網域的 DNS 名稱伺服器。然後重新啟動執行個體。

若要在 Amazon EC2 Mac 執行個體 (GUI) 上掛載檔案共用

1. 啟動 Mac 執行個體。若要這麼做，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
   - 啟動 Mac 執行個體，使用 AWS CLI
2. 使用虛擬網路運算 (VNC) Connect 至您的 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 Connect 到執行個體。
3. 在 EC2 Mac 執行個體上，連接到您的 Amazon FSx 檔案共用，如下所示：
   a. 開啟 [Finder]，選擇 [執行]，然後選擇 [Connect 至伺服器]。
   b. 在 [Connect 到伺服器] 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 檔案伺服器、網路和安全性，在 Amazon FSx 主控台上找到檔案系統的 DNS 名稱和任何相關的 DNS 別名。或者，您可以在CreateFile系統或系DescribeFile統 API 操作的響應中找到它們。如需有關使用 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 [Connect] 以繼續。
   d. 為 Amazon FSx 服務帳戶輸入您的 Microsoft 活動目錄 (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，您可以在搜尋工具視窗中的位置下看到 Amazon FSx 共用。

若要在 Amazon EC2 Mac 執行個體 (命令列) 上掛載檔案共用

1. 啟動 Mac 執行個體。若要這麼做，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
   - 啟動 Mac 執行個體，使用 AWS CLI
2. 使用虛擬網路運算 (VNC) Connect 至您的 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 Connect 到執行個體。
3. 使用以下命令掛載文件共享。

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

您可以選擇 Windows 檔案伺服器、網路和安全性，在 Amazon FSx 主控台上找到 DNS 名稱。或者，您可以在`CreateFileSystem`或 `DescribeFileSystems` API 作業的回應中找到它們。

- 對於加入 AWS 管理 Microsoft 活動目錄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，以及任何異地同步備份檔案系統，DNS 名稱如下所示。

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

此程序中使用的 mount 指令會在指定時間點執行下列作業：

- *//file_system_dns_name/file_share*— 指定要掛載之檔案系統的 DNS 名稱和共用。
- *mount_point* — 您要將檔案系統掛載到的 EC2 執行個體上的目錄。

在 Amazon EC2 Linux 執行個體上掛載檔案共用

您可以在已加入您的活動目錄或未加入的 Amazon EC2 Linux 執行個體上掛載 FSx 適用於 Windows 檔案伺服器的檔案共用。

> **Note**
>
> - 下列命令僅將 SMB 通訊協定、快取以及讀取和寫入緩衝區大小等參數指定為範例。Linux `cifs` 命令的參數選擇以及所使用的 Linux 核心版本可能會影響用戶端和 Amazon FSx 檔案系統之間網路操作的輸送量和延遲。如需詳細資訊，請參`cifs`閱您所使用之 Linux 環境的說明文件。
> - 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。

在加入您的活動目錄的 Amazon EC2 Linux 實例上掛載文件共享

1. 如果您尚未將執行中的 EC2 Linux 執行個體加入您的 Microsoft Active Directory，請參閱《AWS Directory Service 管理指南》中的手動加入 Linux 執行個體以取得相關指示。
2. Connect 至您的執行個體。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的 Connect 到 Linux 執行個體。
3. 若要安裝此 `cifs-utils` 套件，請執行下列命令：該軟件包用於在 Linux 上安裝像 Amazon FSx 的網絡文件系統。

   ```
   $ 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. 使用以下命令與 kerberos 進行身份驗證。

```
$ kinit
```

6. 使用以下命令掛載文件共享。

```
$ 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 檔案伺服器、網路和安全性，在 Amazon FSx 主控台上找到 DNS 名稱。或者，您可以在`CreateFileSystem`或 `DescribeFileSystems` API 操作的響應中找到它們。

- 對於加入 AWS 管理 Microsoft 活動目錄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，以及任何異地同步備份檔案系統，DNS 名稱如下所示。

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

*CIFSMaxBufSize*替換為內核允許的最大值。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)
```

輸出顯示最大緩衝區大小為 130048。

7. 執行下列指令，確認檔案系統是否已掛載，該指令只會傳回通用網際網路檔案系統 (CIFS) 類型的檔案系統。

```
$ 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 mount 指令會在指定時間點執行下列作業：

- *//file_system_dns_name/file_share*— 指定要掛載之檔案系統的 DNS 名稱和共用。
- *mount_point* — 您要將檔案系統掛載到的 EC2 執行個體上的目錄。
- `-t cifs vers=`*SMB_version*— 將檔案系統類型指定為 CIFS 和 SMB 通訊協定版本。FSx for Windows File Server 專用的 Amazon FSx 支援中小企業 2.0 至 3.1.1 版本。
- `sec=krb5`— 指定使用 Kerberos 版本 5 進行驗證。
- `cache=`*cache_mode*— 設定快取模式。CIFS 快取的這個選項可能會影響效能，因此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 說明文件)。建議使`none`用選項`strict`和，因為`loose`可能會導致數據不一致，由於較寬鬆的協議語義。
- `cruid=`*ad_user*— 將憑證快取擁有者的 uid 設定為 AD 目錄管理員。
- */mnt/fsx*— 指定 EC2 執行個體上 Amazon FSx 檔案共用的掛接點。
- `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*替換為內核允許的最大值。`CIFSMaxBufSize`透過執行下列命令來判斷。

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

  輸出顯示最大緩衝區大小為 130048。
- `ip=`*preferred-file-server-Ip*— 將目標 IP 位址設定為檔案系統偏好檔案伺服器的 IP 位址。

  您可以擷取檔案系統偏好的檔案伺服器 IP 位址，如下所示：
  - 使用 Amazon FSx 主控台，在檔案系統詳細資訊頁面的「網路和安全性」索引標籤上。
  - 在 `describe-file-systems` CLI 命令或等效的DescribeFile系統 API 命令的響應中。

若要在未加入您的作用中目錄的 Amazon EC2 Linux 執行個體上掛載檔案共用

下列程序會將 Amazon FSx 檔案共用掛接到未加入您的作用中目錄 (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 位址來掛載適用於 Windows 檔案伺服器檔案共用的 FSx。您可以使用 Amazon FSx 主控台的「網路與安全」索引標籤的「慣用檔案伺服器 IP 位址」取得檔案系統的私有 IP 位址。

此範例使用 NTLM 驗證。若要這麼做，您可以將檔案系統掛載為使用者，該使用者身為 Windows 檔案伺服器檔案系統的 FSx 所加入的 Microsoft 作用中目錄網域的成員。使用者帳戶的登入資料會以您在 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
```

若要啟動和設定 Amazon 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. Connect 到您的 Amazon EC2 執行個體。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的 Connect 到 Linux 執行個體。
3. 若要安裝此 `cifs-utils` 套件，請執行下列命令：該軟件包用於在 Linux 上安裝像 Amazon FSx 的網絡文件系統。

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

4. 建立您計劃掛**`/mnt/fsxx`**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`認證檔案。
6. 設置`creds.txt`文件權限，以便只有您（所有者）可以通過運行以下命令來讀取和寫入文件。

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

掛載檔案系統

1. 您可以使用其私人 IP 位址來裝載未加入您使用中目錄的檔案共用。您可以使用 Amazon FSx 主控台的「網路與安全性」索引標籤的「慣用檔案伺服器 IP 位址」取得檔案系統的私有 IP 位址。
2. 使用下列指令掛載檔案系統：

   ```
   $ 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`*替換為內核允許的最大值。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)
```

輸出顯示最大緩衝區大小為 130048。

3. 執行下列指令 (僅傳回 CIFS 檔案系統)，以確認檔案系統是否已掛載。

```
$ 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 mount 指令會在指定時間點執行下列作業：

- *//file-system-IP-address/file_share*— 指定您正在掛載的檔案系統的 IP 位址和共用。
- `-t cifs vers=`*SMB_version*— 將檔案系統類型指定為 CIFS 和 SMB 通訊協定版本。FSx for Windows File Server 專用的 Amazon FSx 支援中小企業 2.0 至 3.1.1 版本。
- `sec=ntlmsspi`— 指定使用 NT 區域網路管理員安全性 Support 提供者介面 (NTLMSSPI) 進行驗證。
- `cache=`*cache_mode*— 設定快取模式。CIFS 快取的這個選項可能會影響效能，因此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 說明文件)。建議使`none`用選項`strict`和，因為`loose`可能會導致數據不一致，由於較寬鬆的協議語義。
- `cred=/home/ec2-user/creds.txt`— 指定取得使用者認證的位置。
- */mnt/fsx*— 指定 EC2 執行個體上 Amazon FSx 檔案共用的掛接點。
- `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*替換為內核允許的最大值。`CIFSMaxBufSize`透過執行下列命令來判斷。

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

在未加入活動目錄的 Amazon Linux EC2 實例上自動掛接文件共享

您可以在安裝該檔案伺服器的 Amazon EC2 Linux 執行個體重新啟動時，自動掛載 FSx 用於 Windows 檔案伺服器的檔案共用。若要這麼做，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的指令`mount -a`會掛載檔案中列出的`/etc/fstab`檔案系統。

對於未加入您的作用中目錄的 Amazon EC2 Linux 執行個體，您只能使用其私有 IP 位址來掛接 Windows 檔案伺服器檔案共用的 FSx。您可以使用 Amazon FSx 主控台的「網路與安全」索引標籤的「慣用檔案伺服器 IP 位址」取得檔案系統的私有 IP 位址。

下列程序使用 Microsoft NTLM 驗證。您可以將檔案系統掛載為使用者，該使用者是 Windows 檔案伺服器檔案系統所加入的 FSx 的 Microsoft 作用中目錄網域的成員。使用者帳戶的認證會在文字檔中提供`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
```

若要在未加入您的活動目錄的 Amazon Linux EC2 執行個體上自動掛載檔案共用

若要啟動和設定 Amazon 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 Connect 到 Linux 執行個體。
3. 若要安裝此 `cifs-utils` 套件，請執行下列命令：該軟件包用於在 Linux 上安裝像 Amazon FSx 的網絡文件系統。

   ```
   $ 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`認證檔案。
6. 設置文件權限，以便只有您（所有者）可以通過運行以下命令來讀取文件。

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

自動掛載檔案系統

1. 您可以使用其私有 IP 位址，自動掛載未加入您使用中目錄的檔案共用。您可以使用 Amazon FSx 主控台的「網路與安全」索引標籤的「慣用檔案伺服器 IP 位址」取得檔案系統的私有 IP 位址。
2. 若要使用其私人 IP 位址自動掛載檔案共用，請將下列行新增至/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
```

*CIFSMaxBufSize*替換為內核允許的最大值。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)
```

輸出顯示最大緩衝區大小為 130048。

3. 通過使用帶有「偽造」選項的mount命令以及「全部」和「詳細」選項來測試fstab條目。

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

4. 若要掛載檔案共用，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，確認檔案系統已掛載。

```
$ 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檔案的行會在指定時間點執行下列動作：

- *//file-system-IP-address/file_share*— 指定您要掛載之 Amazon FSx 檔案系統的 IP 位址和共用率。
- /mnt/fsx— 指定 EC2 執行個體上 Amazon FSx 檔案系統的掛載點。

- `cifs vers=`*`SMB_version`*— 將檔案系統類型指定為 CIFS 和 SMB 通訊協定版本。FSx for Windows File Server 專用的 Amazon FSx 支援中小企業 2.0 至 3.1.1 版本。
- `sec=ntlmsspi`— 指定使用 NT 區域網路管理員安全性 Support 提供者介面，以促進 NTLM 挑戰回應驗證。
- `cache=`*`cache_mode`*— 設定快取模式。CIFS 快取的這個選項可能會影響效能，因此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 說明文件)。建議使none用選項strict和，因為loose可能會導致數據不一致，由於較寬鬆的協議語義。
- `cred=/home/ec2-user/creds.txt`— 指定取得使用者認證的位置。
- `_netdev`— 告訴作業系統檔案系統位於需要網路存取的裝置上。使用此選項可防止執行個體掛載檔案系統，直到用戶端上啟用網路服務為止。
- `0`— 指示檔案系統應該由dump備份 (如果它是非零值)。對於 Amazon FSx，這個值應該是0。
- `0`— 指定開機時fsck檢查檔案系統的順序。對於 Amazon FSx 檔案系統，此值應0表示不fsck應在啟動時執行。

將現有的檔案儲存遷移到 Amazon FSx

FSx for Windows File Server 的功能、效能和相容性，可協助您輕鬆地將企業應用程式提升並轉移到 Amazon Web Services 雲端。遷移到 FSx 的 Windows 文件服務器的過程包括以下步驟：

1. 將您的檔案移轉至 FSx (適用於 FSx for Windows File Server)。如需詳細資訊，請參閱 將現有的檔案儲存移轉至 FSx for Windows File Server。
2. 將您的檔案共用組態移轉至 FSx for Windows File Server)。如需詳細資訊，請參閱 將檔案共用組態遷移到 Amazon FSx。
3. 將您現有的 DNS 名稱建立為 Amazon FSx 檔案系統的 DNS 別名建立關聯。如需詳細資訊，請參閱將 DNS 別名與 Amazon FS x 建立關聯。
4. 切換成 FSx 適用於 FSx for Windows File Server。如需詳細資訊，請參閱 切割到 Amazon FSx。

您可以在以下各節中找到流程中每個步驟的詳細資訊。

主題

- 將現有的檔案儲存移轉至 FSx for Windows File Server
- 將檔案共用組態遷移到 Amazon FSx
- 遷移 DNS 組態以使用 Amazon FSx
- 切割到 Amazon FSx

將現有的檔案儲存移轉至 FSx for Windows File Server

若要將現有檔案移轉至 FSx for Windows File Server 檔案系統，我們建議您使用線上資料傳輸服務 AWS DataSync，其設計目的是簡化、自動化及加速在 AWS 儲存服務之間複製大量資料。 DataSync 通過互聯網或複製數據 AWS Direct Connect。作為完全受控的服務， DataSync 不再需要修改應用程式、開發指令碼或管理基礎結構。如需詳細資訊，請參閱 將現有檔案移轉至 FSx for Windows File Server 使用) AWS DataSync。

作為替代解決方案，您可以使用強大的文件複製或 Robocopy，這是 Microsoft Windows 的命令行目錄和文件複製命令集。如需如何使用 Robocopy 將檔案儲存移轉至 FSx (適用於 Windows 檔案伺服器) 的詳細程序，請參閱。使用機器人複製將現有檔案移轉至 FSx

將現有檔案儲存裝置移轉至適用於 Windows 檔案伺服器的 FSx 的最佳作法

若要盡快將大量資料遷移到 FSx for Windows File Server，請使用設定為固態硬碟 (SSD) 儲存體的 Amazon FSx 檔案系統。遷移完成後，如果這是您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 SDD 儲存將資料從 Amazon FSx 檔案系統移至硬碟儲存，您可以執行下列步驟。請注意，HDD 檔案系統至少有 2TB 的儲存容量，並且從備份還原時無法變更儲存容量。)

1. 備份您的 SSD 文件系統。如需詳細資訊，請參閱 建立使用者初始備份。
2. 使用 HDD 存儲將備份還原到文件系統。如需詳細資訊，請參閱 還原備份。

將現有檔案移轉至 FSx for Windows File Server 使用) AWS DataSync

我們建議使用 AWS DataSync 在 FSx 之間傳輸資料，適用於 Windows 檔案伺服器的檔案系統。DataSync 是一種資料傳輸服務，可透過網際網路或其他儲存服務，簡化、自動化及加速內部部署儲存系統與其他 AWS 儲存服務之間的資料移動和複寫速度。 AWS Direct Connect DataSync 可以傳輸您的檔案系統資料和中繼資料，例如擁有權、時間戳記和存取權限。

DataSync 支援複製 NTFS 存取控制清單 (ACL)，並且還支援複製檔案稽核控制資訊，也稱為 NTFS 系統存取控制清單 (SACL)，系統管理員會使用這些清單來控制使用者嘗試存取檔案的稽核記錄。

您可 DataSync 以使用在 Windows 檔案伺服器檔案系統的兩個 FSx 之間傳輸檔案，也可以將資料移至不同 AWS 區域 或 AWS 帳戶中的檔案系統。您可以 DataSync 搭配 FSx 使用 Windows 檔案伺服器檔案系統來執行其他工作。例如，您可以執行一次性資料移轉、定期擷取分散式工作負載的資料，以及排程複寫以進行資料保護和復原。

在中 AWS DataSync，適用於 FSx for Windows File Server 位置是適用於 FSx for Windows File Server 端點。您可以在 Windows 檔案伺服器的 FSx 位置與其他檔案系統的位置之間傳輸檔案。若要取得資訊，請參閱《使用指南》中的〈AWS DataSync 使用位置〉。

DataSync 使用伺服器訊息區 (SMB) 通訊協定存取 Windows 檔案伺服器的 FSx。它會使用您在 AWS DataSync 主控台或中設定的使用者名稱和密碼進行驗證。 AWS CLI

必要條件

若要將資料遷移到 Amazon FSx for Windows File Server 的設定中，您需要符合需 DataSync 求的伺服器和網路。若要深入瞭解，請參閱《AWS DataSync 使用者指南》 DataSync中的「的需求」。

如果您要執行大型資料遷移，或是涉及許多小型檔案的遷移，建議您使用具有 SSD 儲存類型的 Amazon FSx 檔案系統。這是因為 DataSync 任務涉及文件元數據的掃描，這可能會耗盡 HDD 文件系統的磁盤 IOPS 限制，從而導致長時間運行的遷移和文件系統性能影響。如需詳細資訊，請參閱 將現有檔案儲存裝置移轉至適用於 Windows 檔案伺服器的 FSx 的最佳作法。

如果您的資料集大部分是小型檔案、檔案總數 (以百萬計)，或者您的可用網路頻寬超過單一 DataSync 工作的使用量，您也可以使用向外擴充架構加速資料傳輸。如需詳細資訊，請參閱：如何使用橫向 AWS DataSync 擴充架構加速資料傳輸。

您可以使用 FSx 效能測量結果來監督檔案系統的磁碟 I/O 使用率。

使用移轉檔案的基本步驟 DataSync

若要使用將檔案從來源位置傳輸到目標位置 DataSync，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，請參閱使用者指南中的自我管理儲存體之間的資料傳輸和 AWS建立 SMB 位置和建立適用於 Windows 檔案伺服器的 Amazon FSx 位置。AWS DataSync

若要了解如何將檔案從現有雲端檔案系統傳輸到適用 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 檔案系統之間進行遷移

您可以使 DataSync 用在兩個 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，例如從單一可用區組態移至異地同步備份組態，此功能會很有幫助。您也可以使用 DataSync 在兩個檔案系統之間分割工作負載。

以下是移轉程序的概觀範例：

1. 建立來源檔案系統和目標檔案系統的 DataSync 位置。請注意，來源和目的地必須屬於相同的 Active Directory (AD) 網域，或在其網域之間具有 AD 信任關係。
2. 建立並設定 DataSync 工作，將資料從來源傳輸到目的地。您可以將工作作為一次性執行個體執行，或將工作設定為根據您設定的排程自動執行。

3. 工作順利完成之後，目的地檔案系統中的資料就是來源的精確副本。請注意，您必須暫時暫停來源檔案系統上的任何寫入活動或檔案更新，才能完成工作。然後，您可以切換到目標文件系統並刪除源文件系統。

從生產檔案系統移轉之前，您可以在從最近備份還原的檔案系統上測試移轉程序。這可讓您估計資料傳輸程序需要多長時間，並事先對 DataSync 錯誤進行疑難排解。

若要將切換時間縮到最短，您可以事先 DataSync 執行工作，將大部分資料從來源檔案系統移至目的檔案系統。停止來源檔案系統的流量之後，您可以執行一次最後的工作傳輸，以同步處理因為您停止流量後新更新的任何資料，然後切換到目的地檔案系統。

您可以將 DataSync 工作設定為僅在特定目錄中執行，或包含或排除特定路徑。如果您要同時執 parallel 多個工作，或者想要遷移資料的子集，這會很有用。

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。這可讓您的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：逐步解說 5：使用 DNS 別名存取您的檔案系統。

執行此類型的移轉時，我們建議您執行下列動作：

- 排程您的移轉，以避免任何檔案系統備份、每週維護時段和`Data Deduplication`工作。具體來說，如果`Data Deduplication GarbageCollection`工作與您計劃的移轉重合，我們建議您停用該工作。
- 您的來源和目的檔案系統都使用 SSD 儲存類型。您可以通過從備份還原來在 HDD 和 SSD 存儲類型之間切換。如需詳細資訊，請參閱：將現有的檔案儲存移轉至 FSx for Windows File Server。
- 針對您需要傳輸的資料量，設定您的來源和目的地檔案系統，具有足夠的輸送量容量。在 DataSync 工作程序期間，監視來源檔案系統和目的檔案系統的效能使用率。如需詳細資訊，請參閱 使用 Amazon 監控指標 CloudWatch。
- 設置DataSync 監視以幫助您了解正在進行的任務的進度。您也可以將 DataSync 日誌傳送到 Amazon CloudWatch 日誌群組，以協助您在遇到任何錯誤時對任務進行除錯。

使用機器人複製將現有檔案移轉至 FSx

以 Microsoft 視窗伺服器為基礎，Amazon FSx for Windows File Server，可讓您將現有的資料集完全遷移到 Amazon FSx 檔案系統中。您可以移轉每個檔案的資料。您也可以移轉所有相關的檔案中繼資料，包括屬性、時間戳記、存取控制清單 (ACL)、擁有者資訊和稽核資訊。透過這項全面的移轉支援，Amazon FSx 可將依賴這些檔案資料集的 Windows 型工作負載和應用程式移至 Amazon Web Services 雲端。

使用下列主題做為複製現有檔案資料程序的指南。執行此副本時，您會保留現場部署資料中心或 Amazon EC2 上自我管理檔案伺服器的所有檔案中繼資料。

必要條件

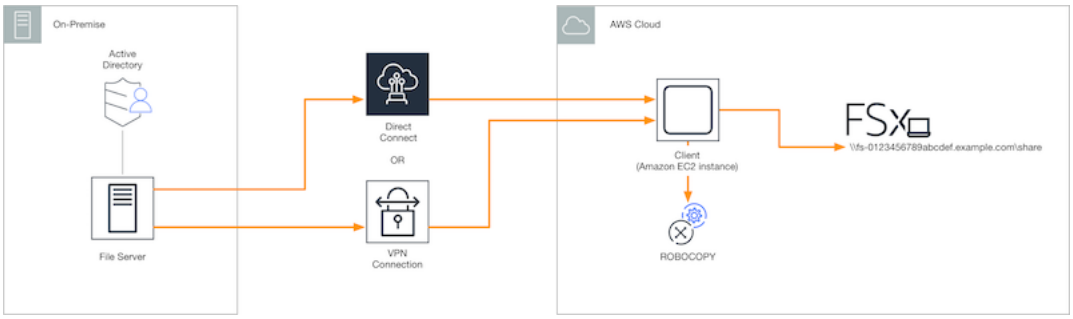
在開始之前，請確定您已執行下列動作：

- 在您要建立 Amazon FSx 檔案系統的現場部署作用中目錄和 VPC 私人雲端之間建立網路連線 (使用 AWS Direct Connect 或 VPN)。
- 在您的 Active Directory 上建立具有委派權限的服務帳戶，以將電腦加入網域。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，並加入您的自我管理 (現場部署) Microsoft AD 目錄。
- 請記下包含要傳輸到 Amazon FSx 的現有檔案的檔案共用位置 (例如，`\\Source\Share`內部部署或中 AWS)。
- 請記下您想要透過現有檔案傳輸到的 Amazon FSx 檔案系統上檔案共用的位置 (例如，`\\Target\Share`)。

下表摘要說明三種移轉使用者存取模式的來源和目標檔案系統可存取性需求。

移轉使用者存取模式	來源檔案系統存取性需求	目標 FSx 檔案伺服器可存取性需求
直接讀/寫權限模型	使用者必須對要移轉的檔案和資料夾具有至少讀取權限 (NTFS ACL)。	使用者必須至少擁有要移轉之檔案和資料夾的寫入權限 (NTFS ACL)。
備份/還原權限模型以覆蓋存取權限	使用者必須是內部部署 Active Directory 的 Backup 操作員群組的成員，並搭配 RoboCopy使用 /b 旗標。	使用者必須是 Amazon FSx 檔案系統管理員群組 * 的成員，並搭配使用 /b 旗標。 RoboCopy
覆寫存取權限的網域管理員 (完整) 權限模型	使用者必須是內部部署 Active Directory 的網域系統管理員群組的成員。	使用者必須是 Amazon FSx 檔案系統管理員群組的成員 *，並使用 /b 旗標 RoboCopy

> **Note**
>
> * 對於加入 AWS 受管 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。在您的自我管理 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指定用於管理的自訂群組。



如何使用 Robocopy 將現有文件遷移到 Amazon FSX

您可以使用下列程序將現有檔案移轉到 Amazon FSx。

將現有檔案遷移到 Amazon FSx

1. 在與您的 Amazon FSx 檔案系統相同的 Amazon VPC 中啟動視窗伺服器 2016 年亞馬遜 EC2 執行個體。
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 (內部部署或中 AWS) 上的來源檔案共用對應至磁碟機代號 (例如，*Y*:)，如下所示。在此過程中，您會為內部部署 Active Directory 的網域系統管理員群組的成員提供認證。

```
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對應至不同的磁碟機代號 (例如，*Z*:) Amazon EC2 如下所示。在此過程中，您需要為身為現場部署 Active Directory 網域管理員群組成員的使用者帳戶和 Amazon FSx 檔案系統的管理員群組提供登入資料。對於加入 AWS 管理 Microsoft AD 的檔

案系統而言，該群組為**AWS Delegated FSx Administrators**。在自我管理的 Microsoft AD 中，該群組是**Domain Admins**您在建立檔案系統時指定用於管理的自訂群組。

如需詳細資訊，請參閱中的來源檔案系統協助工具需求表格必要條件。

```
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. 從內容功能表選擇「以管理員身分執行」。以系統管理員身分開啟命令提示字元或 Windows PowerShell，然後執行下列 Robocopy 命令，將檔案從來源共用複製到目標共用。

   該ROBOCOPY命令是一個靈活的文件傳輸實用程序，具有多個選項來控制數據傳輸過程。由於這個ROBOCOPY命令程序，來源共用中的所有檔案和目錄都會複製到 Amazon FSx 目標共用。副本會保留檔案和資料夾 NTFS ACL、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
   ```

   前面的示例命令使用以下元素和選項：

   - Y — 指位於內部部署作用中目錄樹系 mydata.com 中的來源共用。
   - Z — 是指在 Amazon FSX 上的目標共享。
   - /copy — 指定下列要複製的檔案內容：
     - ð-數據
     - A-屬性
     - T — 時間戳
     - S — NTFS ACL
     - O — 所有者信息
     - U — 稽核資訊。
   - /secfix — 修正所有檔案的檔案安全性，甚至是略過的檔案。
   - /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 ACL 拒絕目前使用者的權限。

- /MT: 8 — 指定用於執行多執行緒副本的執行緒數目。

> **Note**
>
> 如果您要透過緩慢或不可靠的連線來複製大型檔案，您可以使用選項來取代/zb選項來啟用可重新啟動模式。robocopy /b使用可重新啟動模式時，如果大型檔案的傳輸中斷，後續的 Robocopy 作業可能會在傳輸中間執行，而不必從頭開始重新複製整個檔案。啟用可重新啟動模式可以降低資料傳輸速度。

將檔案共用組態遷移到 Amazon FSx

您可以使用下列程序將現有的檔案共用組態遷移到 Amazon FSx。在此程序中，來源檔案伺服器是您要將其檔案共用組態遷移到 Amazon FSx 的檔案伺服器。

> **Note**
>
> 在移轉檔案共用組態之前，請先將檔案移轉到 Amazon FSx。如需詳細資訊，請參閱 將現有的檔案儲存移轉至 FSx for Windows File Server。

若要將現有的檔案共用移轉至 Windows 檔案伺服器的 FSx

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」。 PowerShell以系統管理員身分開啟視窗。
2. SmbShares.xml透過在中執行下列指令，將來源檔案伺服器的檔案共用匯出到名為的檔案 PowerShell。在此範例中，將 F: 替換為您要從中匯出檔案共用的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: (您的磁碟機代號) 的所有參照取代為 D:\share，因為 Amazon FSx 檔案系統駐留在 D:\share.
4. 將現有的檔案共用組態匯入至 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。然後使用以下命令將其導入到變量中。

```
$shares = Import-Clixml -Path F:\SmbShares.xml
```

5. 使用下列其中一個選項，準備在 FSx for Windows 檔案伺服器檔案伺服器上建立檔案共用所需的認證物件。

   若要以互動方式產生認證物件，請使用下列命令。

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

   若要使用 AWS Secrets Manager 資源產生認證物件，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到 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 }
   }
   ```

遷移 DNS 組態以使用 Amazon FSx

FSx for Windows File Server 每個可用來存取檔案系統資料的檔案系統提供預設的網域名稱系統 (DNS) 名稱。您也可以將替代 DNS 名稱設定為 Amazon FSx 檔案系統的 DNS 別名，使用您選擇的任何 DNS 名稱存取檔案系統。

透過 DNS 別名，您可以在將檔案系統儲存從現場部署遷移到 Amazon FSx 時，繼續使用現有的 DNS 名稱存取儲存在 Amazon FSx 上的資料。這有助於在遷移到 Amazon FSx 時，無需更新任何使用 DNS 名稱的工具或應用程式。當您建立新檔案系統時，以及當您從備份建立新檔案系統時，您可以將 DNS 別名與 Windows 檔案伺服器檔案系統的現有 FSx 產生關聯。您一次最多可以將 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 別名必須符合下列需求：

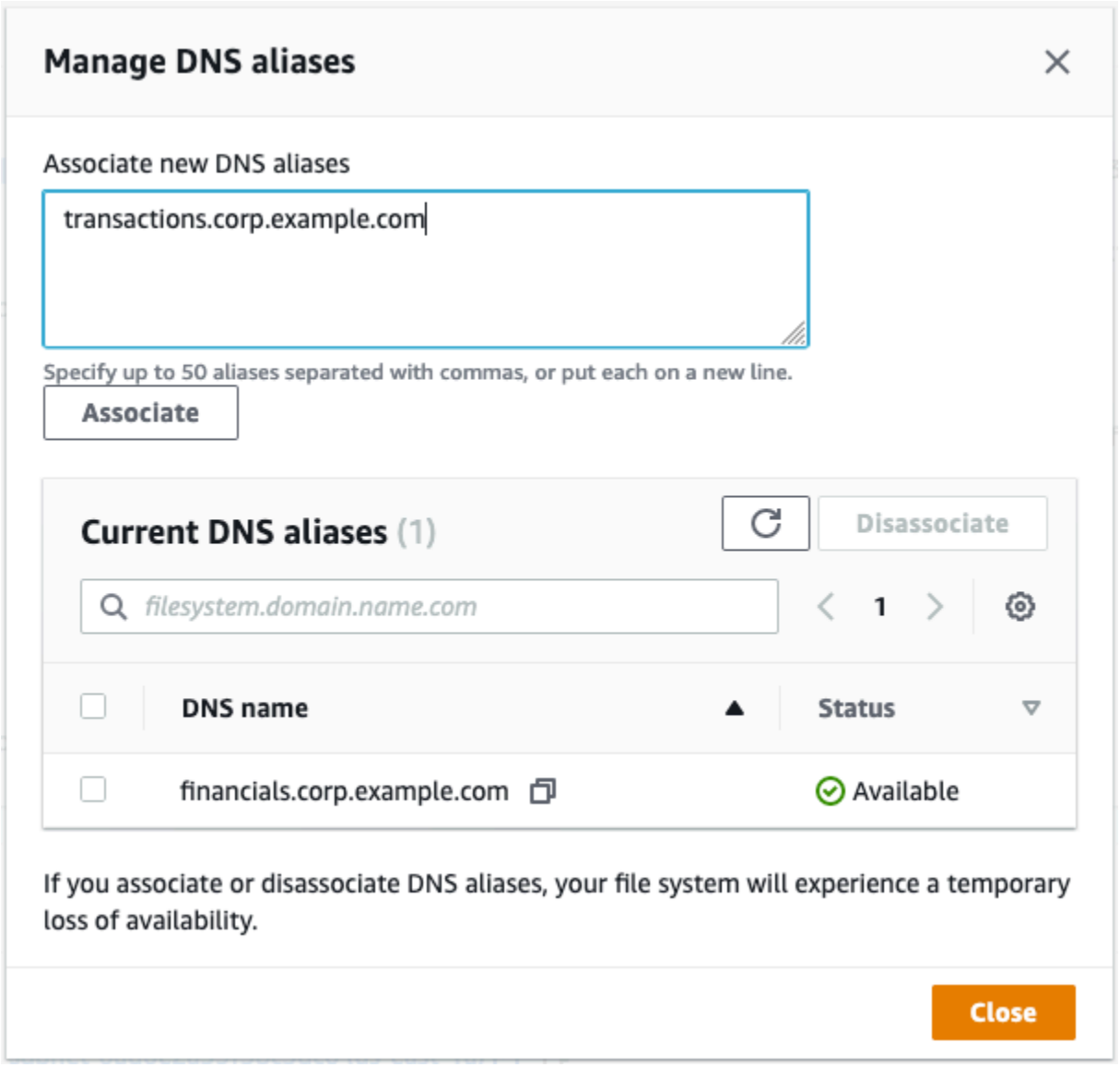
- 必須格式化為完整網域名稱 (FQDN)，例如。`accounting.example.com`
- 可以包含英數字元和連字號 (-)。
- 名稱開頭或結尾不能為連字號 (-)。
- 可以從數字開頭。

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 別名與您現有的 Windows 檔案伺服器檔案系統建立關聯。如需在建立新檔案系統時關聯 DNS 別名的詳細資訊，包括備份中的新檔案系統，請參閱建立 DNS 別名與檔案系統的關聯。

建立 DNS 別名與現有檔案系統 (主控台) 的關聯

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 瀏覽至 [檔案系統]，然後選擇您要與 DNS 別名建立關聯的 Windows 檔案系統。
3. 在 [網路與安全性] 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。

   您可以監視剛在「目前別名」清單中關聯的別名狀態。當狀態顯示為「可用」時，別名會與檔案系統相關聯 (這個程序最多可能需要 2.5 分鐘)。

建立 DNS 別名與現有檔案系統 (CLI) 的關聯

- 使用 `associate-file-system-aliases` CLI 命令或 AssociateFileSystemAliasesAPI 作業，將 DNS 別名與現有檔案系統建立關聯。

  下列 CLI 要求會將兩個別名與指定的檔案系統產生關聯。

```
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 與檔案系統關聯的別名狀態。

```
{
      "Aliases": [
          {
              "Name": "financials.corp.example.com",
              "Lifecycle": CREATING
          },
          {
              "Name": "transfers.corp.example.com",
              "Lifecycle": CREATING
          }
      ]
  }
```

若要監視要關聯之別名的狀態，請使用 `describe-file-system-aliases` CLI 命令 (這DescribeFileSystemAliases是對等的 API 作業)。當別名的值`Lifecycle`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)。

切割到 Amazon FSx

若要切換至 Windows 檔案伺服器檔案系統的 FSx，請執行下列步驟：

- 準備切過來。
  - 暫時中斷 SMB 用戶端與原始檔案系統的連線。
  - 執行最終檔案與檔案共用設定同步。
- 為您的 Amazon FSx 檔案系統設定服務主體名稱 (SPN)。
- 更新 DNS CNAME 記錄以指向您的 Amazon FSx 檔案系統。

以下各節提供了執行上述每個步驟的程序。

主題

準備切換到 Amazon FSx

若要準備轉換至 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。
- 使用 AWS DataSync 或 Robocopy 執行最終檔案同步。如需詳細資訊，請參閱 將現有的檔案儲存移轉至 FSx for Windows File Server。
- 執行最終檔案共用設定同步。如需詳細資訊，請參閱 將檔案共用組態遷移到 Amazon FSx。

設定用於 Kerberos 驗證的 SPN

我們建議您在傳輸過程中使用 Kerberos 型身份驗證和加密與 Amazon FSx。Kerberos 為存取檔案系統的用戶端提供最安全的驗證。若要為使用 DNS 別名存取 Amazon FSx 的用戶端啟用 Kerberos 身份驗證，您必須新增服務主體名稱 (SPN)，這些名稱與 Amazon FSx 檔案系統的作用中目錄電腦物件上的 DNS 別名相對應。

Kerberos 驗證有兩個必要的 SPN。

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

例如，如果別名是`finance.domain.com`，則兩個必要的 SPN 如下。

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

SPN 一次只能與單一作用中目錄電腦物件相關聯。如果為原始檔案系統的使用中目錄電腦物件設定了 DNS 名稱的現有 SPN，則必須先刪除它們，然後才能為 Amazon FSx 檔案系統建立 SPN。

下列程序說明如何尋找任何現有的 SPN、刪除它們，以及如何為 Amazon FSx 檔案系統的使用中目錄電腦物件建立新的 SPN。

若要安裝所需的 PowerShell 使用中目錄模組

1. 登入加入 Amazon FSx 檔案系統所加入的作用中目錄的 Windows 執行個體。
2. PowerShell 以管理員身份打開。
3. 使用以下命令安裝 PowerShell 活動目錄模塊。

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

尋找和刪除原始檔案系統的作用中目錄電腦物件上現有的 DNS 別名 SPN

1. 使用下列命令尋找任何現有的 SPN。以您在中*alias_fqdn*與檔案系統相關聯的 DNS 別名取代遷移 DNS 組態以使用 Amazon FSx。

```
## 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 SPN。

   - 以您*alias_fqdn*與中的檔案系統相關聯的完整 DNS 別名取代遷移 DNS 組態以使用 Amazon FSx。
   - *file_system_DNS_name*以原始檔案系統的 DNS 名稱取代。

```
## 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 別名重複這些步驟遷移 DNS 組態以使用 Amazon FSx。

在 Amazon FSx 檔案系統的作用中目錄電腦物件上設定 SPN

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

   - 以 Amazon FSx 指派給檔案系統的 DNS 名稱取*file_system_DNS_name*代。

     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料頁面的 [網路和安全性] 窗格。您也可以在DescribeFile系統 API 作業的回應中取得 DNS 名稱。

   - 以您*alias_fqdn*與中的檔案系統相關聯的完整 DNS 別名取代遷移 DNS 組態以使用 Amazon FSx。

```
## 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**
   >
   > 如果原始檔案系統電腦物件的 AD 中存在 DNS 別名的 SPN，則為您的 Amazon FSx 檔案系統設定 SPN 將會失敗。如需尋找和刪除現有 SPN 的資訊，請參閱尋找和刪除原始檔案系統的作用中目錄電腦物件上現有的 DNS 別名 SPN。

2. 使用下列範例指令碼確認已針對 DNS 別名設定新 SPN。請確定回應包含兩個主機 SPN HOST/*alias* 和HOST/*alias_fqdn*。

   取代*file_system_DNS_name*為 Amazon FSx 指派給您檔案系統的 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]，選擇您的檔案系統，然後在檔案系統詳細資料頁面上選擇 [網路和安全性] 窗格。

   您也可以在DescribeFile系統 API 作業的回應中取得 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. 針對與中的檔案系統相關聯的每個 DNS 別名重複上述步驟遷移 DNS 組態以使用 Amazon FSx。

> **Note**
>
> 您可以在 Active Directory 中設定下列群組原則物件 (GPO)，以便在使用 DNS 別名連線至您檔案系統的用戶端強制執行 Kerberos 驗證和加密傳輸中：
>
> - 限制 NTLM：傳出 NTLM 流量至遠端伺服器
> - 限制 NTLM：為 NTLM 驗證新增遠端伺服器例外
>
> 如需詳細資訊，請參閱逐步解說 5：使用 DNS 別名存取您的檔案系統使用 GPO 強制執行 Kerberos 驗證中的。

更新 Amazon FSx 檔案系統的 DNS CNAME 記錄

為檔案系統正確設定 SPN 之後，您可以將解析為原始檔案系統的每個 DNS 記錄取代解析為原始檔案系統的 DNS 記錄，以解析為 Amazon FSx 檔案系統預設 DNS 名稱的 DNS 記錄來切換為 Amazon FSx。

若要安裝必要的 PowerShell 指令程式

1. 登入加入 Active Directory 的 Windows 執行個體，您的 Amazon FSx 檔案系統所加入的使用者身分屬於具有 DNS 管理權限的群組成員 (AWS 受管 Microsoft Active Directory 中的AWS 委派網域名稱系統管理員，以及您已在自我管理的 Active Directory 中委派 DNS 管理權限的其他群組)

   如需詳細資訊，請參閱 Amazon EC2 使用者指南中的連線到 Windows 執行個體。
2. PowerShell 以管理員身份打開。
3. 執行此程序中的指示需要 PowerShell DNS 伺服器模組。使用以下命令安裝它。

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

若要更新現有的 DNS CNAME 記錄

1. 下列指令碼會更新 Amazon FSx 檔案系統電腦物件的任何現有 DNS CNAME 記錄。*alias_fqdn*如果找不到任何項目，它會為解析為 Amazon FSx 檔案系統預設 DNS 名稱的 DNS 別*alias_fqdn*名建立新的 DNS CNAME 記錄。

   執行指令碼：

   - 以您*alias_fqdn*與檔案系統相關聯的 DNS 別名取代。
   - 以 Amazon FSx 指派給檔案系統的預設 DNS 名稱取*file_system_DNS_name*代。

   ```
   $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. 針對與中的檔案系統相關聯的每個 DNS 別名重複上一個步驟遷移 DNS 組態以使用 Amazon FSx。

搭配使用 FSx for Windows File Server 與 Microsoft Server

高可用性 (HA) 微軟 SQL Server 通常部署在 Windows 伺服器容錯移轉叢集 (WSFC) 中的多個資料庫節點，每個節點都可以存取共用的檔案儲存。您可以透過兩種方式使用 FSx for Windows File Server 作為高可用性 (HA) Microsoft SQL Server 部署的共用儲存裝置：做為使用中資料檔案的儲存，以及 SMB 檔案共用見證。

> **Note**
>
> 目前，亞馬遜 FSx 不支持微軟 SQL 服務器 IFI（即時文件初始化）功能。

建議 SQL 伺服器使用固態硬碟儲存裝置。SSD 儲存裝置專為效能最高且延遲最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相關資訊，請參閱AWS儲存部落格上的下列文章：

- 使用適用於 Windows 檔案伺服器的亞馬遜 FSx 簡化您的微軟 SQL 伺服器高可用性部署
- 將您的高可用性 SQL Server 部署的成本最佳化AWS
- 使用AWS Launch Wizard 和亞馬遜 FSx 簡化 SQL 伺服器永遠在線部署

使用亞馬遜 FSx 處理活動 SQL 服務器數據文件

微軟 SQL Server 可以部署 SMB 文件共享作為活動數據文件的存儲選項。Amazon FSx 經過最佳化，可透過支援持續可用 (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 等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 共用，但是無論是否 HA，都必須在異地同步備份檔案系統上使用 CA 共用。

建立持續可用的共用

您可以在上使用 Amazon FSx CLI 建立 CA 共用，以進行遠端管理 PowerShell。若要指定共用為連續可用的共用，請使`New-FSxSmbShare`用將選`-ContinuouslyAvailable`項設定為`$True`。若要深入了解如何建立新 CA 共用，請參閱建立持續可用 (CA) 共用。

設定 SMB 逾時設定

如中所述FSx for Windows File Server FSx 的容錯移轉程序，異地同步備份的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。您的 SQL Server 應用程式可能對逾時設定有不同的敏感度，具體取決於它的設定方式。

您可以調整 SMB 用戶端組態工作階段逾時，以確保應用程式能夠復原異地同步備份檔案系統容錯移轉。您可以更新檔案系統的輸送量容量 (啟動自動容錯移轉和容錯回復)，以測試應用程式在容錯移轉期間的行為。

使用亞馬遜 FSx 做為中小企業檔案共用見證

Windows Server 容錯移轉叢集部署通常會部署 SMB 檔案共用見證，以維護叢集資源的仲裁。見證檔案共用只需要少量的儲存以取得仲裁資訊。Amazon FSx 檔案系統可用作 Windows 伺服器容錯移轉叢集部署的 SMB 檔案共用見證。

搭配使用 FSx for Windows File Server 與 Amazon Kendra

Amazon Kendra 是一個高精度和智能的搜索服務。適用於 Windows 文件服務器文件系統的 FSx 可用作 Amazon Kendra 的數據源，允許您索引並智能地搜索存儲在文件系統中的文檔中包含的信息。

- 如需 Amazon Kendra 的詳細資訊，請參什麼是 Amazon Kendra中的Amazon Kendra 開發者指南。
- 如需如何將您的檔案系統作為 Amazon Kendra 數據源的詳細資訊，請參開始使用亞馬遜 FSX 數據源（控制台）中的Amazon Kendra 開發者指南。
- 如需 Amazon Kendra 的概述資訊，請參Amazon Kendra 網站。
- 如需使用 Amazon Kendra 搜索您的檔案系統的演練，請參使用適用於 Windows 文件服務器的亞馬遜 FSX 的 Amazon Kendra 連接器安全地搜索 Windows 文件系統上的非結構化數據在AWSMachine Learning 博客。

檔案系統性能

將 FSx for Windows File Server 系統添加為數據源時，Amazon Kendra 會以常規同步頻率抓取文件系統上的文件和文件夾，以創建和維護其搜索索引。（您可以在建立集成時選擇同步頻率。）Amazon Kendra 提供的此文件訪問活動將佔用文件系統資源，類似於您自己訪問文件系統的工作負載中的活動。

確保您的文件系統配置了足夠的資源，以便您的工作負載性能不受影響。具體而言，如果您計劃為大量文件編制索引，我們建議使用具有 SSD 存儲類型的文件系統，該文件系統為需要訪問存儲卷的請求提供更高的最大吞吐量和 IOPS 級別。

如需 Amazon FSx 績效模型的詳細資訊，請參FSx 適用於 FSx for Windows File Server 效能。

使用備份、陰影複製和排程複製來保護您的資料

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

- 原生 Amazon FSx 備份可支援您在 Amazon FSx 中的備份保留和合規需求。
- AWS Backup Amazon FSx 檔案系統的備份是跨雲端和內部部署 AWS 服務的集中式自動備份解決方案的一部分。
- Windows 陰影複製可讓您的使用者輕鬆還原檔案變更，並透過將檔案還原為舊版來比較檔案版本。
- AWS DataSync 將 Amazon FSx 檔案系統的排程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

使用 Amazon FSx 時，備份具有 file-system-consistent高度耐用性和增量功能。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。為了確保檔案系統的一致性，Amazon FSx 在 Microsoft 視窗中使用磁碟區陰影複製服務 (VSS)。為了確保高耐用性，Amazon FSx 將備份存放在亞馬遜簡單儲存服務 (Amazon S3) 中。

Amazon FSx 備份都是增量備份，無論是使用自動每日備份還是使用者啟動的備份功能產生。這表示只會儲存最近一次備份後，檔案系統上已變更的資料。如此可將建立備份所需的時間降至最低，並透過不複製資料來節省儲存成本。

在備份過程中的某個時候，存儲 I/O 可能會暫停，通常會持續幾秒鐘。由於 VSS 服務需要在繼續 I/O 之前清除任何快取的磁碟寫入，因此如果工作負載每秒有大量寫入作業 ()`DataWriteOperations`，則暫停的持續時間可能會更長。大多數終端使用者和應用程式會在短暫的 I/O 暫停時間中遇到此 I/O 暫停。您的應用程式對逾時設定的敏感度可能會有不同的設定。

為檔案系統建立定期備份是最佳實務，可補充 Amazon FSx for Windows File Server 系統執行的複寫作業。Amazon FSx 備份有助於支援您的備份保留和合規需求。無論是建立備份、複製備份、從備份還原檔案系統或刪除備份，都能輕鬆使用 Amazon FSx 備份。請注意，若要檢視單一檔案系統備份的使用情況，您必須啟用該特定備份的標籤，並啟用以標籤為基礎的帳單報告。

主題

使用自動每日備份

根據預設，Amazon FSx 會每日自動備份您的檔案系統。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視窗期間進行。當您選擇每日備份時段時，我們建議您選擇一天中方便的時間。對於使用檔案系統的應用程式，最理想的情況下，這個時間超出正常的作業時間。

自動每日備份會保留一段時間，稱為保留期。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。預設保留期在 Amazon FSx API 和 CLI 中有所不同。您可以將保留期設定為介於 0-90 天之間。將保留期限設定為 0 (零) 天會關閉每日自動備份。刪除檔案系統時，會刪除自動每日備份。

> **Note**
>
> 將保留期限設定為 0 天，表示您的檔案系統永遠不會自動備份。我們強烈建議您針對具有任何關聯重要功能層級的檔案系統，使用自動每日備份。

您可以使用 AWS CLI 或其中一個 AWS SDK 來變更檔案系統的備份時段和備份保留期。使用 `UpdateFileSystem`API 作業或 `update-file-system`CLI 指令。如需詳細資訊，請參閱 演練 3：更新現有的檔案系統。

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 (AWS CLI) 來執行這項操作。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，就可以使用這些備份。即使刪除已備份的檔案系統，仍會保留

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

如果在修改檔案系統 (例如更新輸送量容量期間，或在檔案系統維護期間) 初始化備份，則備份要求會排入佇列，並在活動完成時繼續執行。

建立使用者初始備份

下列程序會引導您如何在 Amazon FSx 主控台中為現有檔案系統建立使用者啟動的備份。

建立使用者啟動的檔案系統備份

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 從主控台儀表板中，選擇您要備份的檔案系統名稱。
3. 從 [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。Backup 名稱最多可包含 256 個 Unicode 字元，包括字母、空格、數字和特殊字元。+-= _:/
5. 選擇 Create backup (建立備份)。

現在，您已經創建了文件系統備份。您可以在 Amazon FSx 主控台中找到所有備份的表格，方法是在左側導覽中選擇備份。您可以搜尋備份的名稱，以及僅顯示相符結果的表格篩選器。

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

AWS Backup 與 Amazon FSx 一起使用

AWS Backup 這是一種簡單且符合成本效益的方式，可透過備份 Amazon FSx 檔案系統來保護資料。AWS Backup 是一種統一的備份服務，旨在簡化備份的創建、複製、還原和刪除，同時提供更好的報告和審計。 AWS Backup 可以更輕鬆地制定集中式備份策略，以實現法律、法規和專業合規性。 AWS Backup 同時提供一個集中的位置，讓您可以執行下列作業，讓保護 AWS 儲存磁碟區、資料庫和檔案系統變得更加簡單：

- 設定及稽核您要備份的 AWS 資源。
- 自動化備份排程。
- 設定保留政策。
- 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 的內置備份功能。從 AWS Backup 主控台進行的備份具有相同層級的檔案系統一致性和效能，以及與透過 Amazon FSx 主控台進行的備份相同的還原選項。從中取得的備份 AWS Backup 是相對於您採取的任何其他 Amazon FSx 備份 (使用者啟動的還是自動備份) 的增量備份。

如果您使用 AWS Backup 來管理這些備份，您將獲得額外的功能，例如無限制的保留選項，以及每小時一次建立排程備份的能力。此外，即使刪除來源檔案系統， AWS Backup 仍會保留不可變的備份。這可防止意外或惡意刪除的情形發生。

採取的備份視 AWS Backup 為使用者啟動的備份，並計入使用者啟動的 Amazon FSx 備份配額中。您可以在 Amazon FSx 主控台、CLI 和 API AWS Backup 中查看和還原所取得的備份。不過，您無法刪除 Amazon FSx 主控台、CLI 或 API AWS Backup 中所取得的備份。如需有關如何使用 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 手動將同一 AWS 帳戶內的備份複製到另一個 AWS 區域 (跨區域副本) 或同一區域內 (AWS 區域內副本)。您只能在相同的 AWS 磁碟分割內建立跨區域副本。您可以使用 Amazon FSx 主控台或 API 建立使用者啟動的備份副本。 AWS CLI當您建立使用者啟動的備份副本時，它會有類型`USER_INITIATED`。

您也可以使 AWS Backup 用跨 AWS 區域和跨 AWS 帳戶複製備份。 AWS Backup 是一項完全受控的備份管理服務，可為原則型備份計劃提供中央介面。透過跨帳戶管理功能，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。

跨區域備份副本對於跨區域災難復原特別有用。您可以進行備份並將其複製到另一個 AWS 區域，以便在主要 AWS 區域發生災難時，您可以從備份還原，並在其他 AWS 區域快速復原可用性。您也可以使用備份副本將檔案資料集複製到另一個 AWS 區域或同一 AWS 區域內。您可以使用 Amazon FSx 主控台或 Amazon FSx API， AWS CLI在同一個 AWS 帳戶 (跨區域或區域內) 製作備份副本。您也可以使用AWS Backup來執行隨選或原則型備份複本。

跨帳戶備份副本對於符合法規遵循要求，將備份複製到隔離帳戶非常有用。它們還提供額外的資料保護層，有助於防止意外或惡意刪除備份、遺失認證或 AWS KMS 金鑰洩漏。跨帳戶備份支援扇入 (將備份從多個主要帳戶複製到一個隔離的備份副本帳戶) 和散發 (將備份從一個主要帳戶複製到多個隔離備份副本帳戶)。

您可以使用 AWS Backup AWS Organizations 支援來製作跨帳戶備份副本。跨帳戶副本的帳戶界限由 AWS Organizations 策略定義。如需使用 AWS Backup 建立跨帳戶備份副本的詳細資訊，請參閱AWS Backup 開發人員指南 AWS 帳戶中的跨帳戶建立備份副本。

Backup 副本限制

以下是複製備份時的一些限制：

- 只有在中國 (北京) 和中國 (寧夏) 區 AWS 域之間的任何兩個商業區域之間、(美國東部) 和 AWS GovCloud (美國西部) 區域之間支援跨區域備份副本，但不支援跨這些區域集。 AWS GovCloud
- 選擇加入的區域不支援跨區域備份副本。
- 您可以在任何區域內製作區 AWS 域內備份副本。
- 來源備份的狀態必須為，AVAILABLE才能複製備份。
- 如果正在複製來源備份，則無法刪除該備份。目的地備份可用到允許您刪除來源備份之間，可能會有短暫的延遲。如果您重試刪除來源備份，請記住此延遲。
- 每個帳戶最多可以有五個備份副本請求正在處理到一個目的地 AWS 區域。

跨區域備份副本的權限

您可以使用 IAM 政策聲明授予執行備份副本操作的許可。若要與來源 AWS 區域通訊以請求跨區域備份副本，請求者 (IAM 角色或 IAM 使用者) 必須具有來源備份和來源區域的存取權。 AWS

您可以使用此原則來授與備份複製作業CopyBackup動作的權限。您可以在策略的Action欄位中指定動作，然後在策略的Resource欄位中指定資源值，如下列範例所示。

```
{
    "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

當您從來源備份將備份複製到不同的目的地 AWS 區域或目的地 AWS 帳戶時，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，第一個複本仍是完整備份副本。

在第一次備份副本之後，所有後續備份副本到同一個 AWS 帳戶內相同目的地區域都是增量的，前提是您尚未刪除該區域中所有先前複製的備份，並且使用相同 AWS KMS 的金鑰。如果不符合任一條件，複製作業會產生完整 (非增量) 備份副本。

使用主控台複製相同帳戶（跨區域或區域內）內的備份

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
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，選擇要將備份複製到的目的地 AWS 區域。目的地可以位於另一個 AWS 區域 (跨區域副本) 或同一區域內 (AWS 區域內副本)。
   - (選擇性) 選取複製標籤，將標籤從來源備份複製到目的地備份。如果您選取「複製標籤」並在步驟 6 中新增標籤，則會合併所有標籤。
5. 對於「加密」，請選擇要 AWS KMS 加密複製備份的加密金鑰。
6. 在「標籤-選用」中，輸入金鑰和值，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 中選取了「複製標籤」，則會合併所有標籤。
7. 選擇複製備份。

您的備份會在同一 AWS 帳戶內複製到所選 AWS 區域。

使用 CLI 在同一帳戶內複製備份 (跨區域或區域內)

- 使用 `copy-backup` CLI 命令或 CopyBackupAPI 作業，跨 AWS 區域或區域內的相同 AWS 帳戶複製備份。 AWS

  下列指令會複製`backup-0abc123456789cba7`來自「`us-east-1`區域」的 ID 的備份。

  ```
  aws fsx copy-backup \
    --source-backup-id backup-0abc123456789cba7 \
    --source-region us-east-1
  ```

  回應會顯示複製備份的說明。

  您可以在 Amazon FSx 主控台上檢視備份，或使用 `describe-backups` CLI 命令或 DescribeBackupsAPI 作業以程式設計方式檢視備份。

還原備份

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。您可以使用主控台或其中一個 AWS SDK 還原備份。 AWS CLI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至檔案系統，在此期間，您將會遇到稍高的延遲時間。

若要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相關聯的 Active Directory 網域與原始檔案系統的網域相同，或受到原始檔案系統的 AD 網域信任。如需有關使用中目錄的詳細資訊，請參閱使用 Microsoft 活動目錄在 FSx for Windows File Server。

下列程序會引導您如何使用主控台還原備份，以建立新的檔案系統。

> **Note**
>
> 您只能將備份還原至與原始備份相同部署類型和儲存容量的檔案系統。您可以在還原的檔案系統可供使用之後增加其儲存容量。如需詳細資訊，請參閱 管理儲存容量。

從備份還原檔案系統

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 在控制台儀表板中，從左側導航中選擇「備份」。
3. 從「備份」表中選擇要還原的備份，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完全相同，但部署類型和儲存容量已設定且無法變更。但是，您可以變更輸送量容量、關聯的 VPC 和其他設定以及儲存區類型。儲存類型預設為 SSD，但您可以在下列情況下將其變更為 HDD：

   - 檔案系統部署類型為異地同步備份或單一可用區 2。
   - 儲存容量至少為 2,000 GiB。
4. 像建立新檔案系統時一樣完成精靈。
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]。

您已從備份還原，而且正在建立新的檔案系統。當其狀態變更為時`AVAILABLE`，您可以正常使用檔案系統。

刪除備份

刪除備份是永久且無法復原的動作。刪除備份中的任何資料也會被刪除。除非您確定 future 來不再需要該備份，否則請勿刪除備份。您無法在 Amazon FSx 主控台 AWS Backup、CLI 或 API 中刪除具有 AWS Backup 類型的備份所取得的備份。

刪除備份

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 在控制台儀表板中，從左側導航中選擇「備份」。
3. 從 [備份] 表格中選擇要刪除的備份，然後選擇 [刪除備份]。
4. 在開啟的 [刪除備份] 對話方塊中，確認備份的 ID 識別您要刪除的備份。
5. 確認已勾選要刪除之備份的核取方塊。
6. 選擇刪除備份。

您的備份和所有包含的資料現在都會永久刪除，且無法復原。

備份大小

備份大小是使用檔案系統中已使用的儲存體來決定，而非佈建的儲存容量總計。備份的大小取決於使用的儲存容量以及檔案系統上的資料流失量。視資料在檔案系統儲存磁碟區的分佈方式以及變更頻率而定，您的總備份使用量可能大於或少於已使用的儲存容量。刪除備份時，只會移除該備份專屬的資料。使用 Amazon FSx，可節省重複資料刪除和壓縮的儲存效率，不僅適用於您的主要 SSD/HDD 儲存，也適用於備份。

為了提供 file-system-consistent持久性和增量備份，Amazon FSx 會在區塊層級備份資料。根據寫入或覆寫的模式，檔案系統儲存磁碟區上的資料可能會儲存在多個區塊中。因此，備份使用量的總大小可能與檔案系統上檔案和目錄的確切大小不相符。

您可以在 AWS Billing 儀表板或中找到您的整體備份使用量和成本 AWS Cost Management Console。若要計算個別檔案系統備份的大小和成本，您可以標記個別備份，並啟用以標籤為基礎的計費報告。

使用陰影複製保護您的資料

Microsoft 視窗陰影複製是 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儲存在網路上的已刪除或變更的檔案，並比較檔案版本。儲存區管理員可以輕鬆地排程陰影複製，以便使用 Windows PowerShell 命令定期進行。

陰影副本與您的系統資料一起儲存，並且只會針對已變更部分的影片消耗系統儲存容量。存儲在您的 Fine 系統中的所有卷影副本都包含在 FILE 系統備份中。

> **Note**
>
> 依預設，不會在適用 FSx for Windows File Server 上啟用陰影複製。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 設定陰影複製以使用預設儲存區和排程。

> **Warning**
>
> 陰影複製不能替代備份。如果您啟用陰影複製，請確定您繼續執行定期備份。

主題

使用陰影複製時的最佳作法

您可以為檔案系統啟用陰影複製，以允許使用者從 Windows 檔案總管中的先前快照檢視及還原個別檔案或資料夾。Amazon FSx 使用由 Microsoft 視窗服務器提供的卷影複製功能。請使用下列陰影複製的最佳作法：

- 確保您的檔案系統具有足夠的效能資源：根據設計，Microsoft Windows 會使用 copy-on-write 方法來記錄自最近陰影複製點以來的變更，而且此 copy-on-write 活動可能會針對每個檔案寫入作業產生最多三個 I/O 作業。
- 使用 SSD 儲存並增加輸送量容量：由於 Windows 需要高等級的 I/O 效能來維護陰影複製，因此建議您使用 SSD 儲存裝置，並將輸送容量提高到預期工作負載的三倍。這有助於確保您的檔案系統擁有足夠的資源，以避免不必要的陰影複製刪除等問題。
- 只維護您需要的陰影複製數目：如果您在單一檔案系統上有大量的陰影複本 (例如，超過 64 個最新的陰影複本)，或者在單一檔案系統上佔用大量儲存區 (TB-規模) 的陰影複製，例如容錯移轉和容錯回復可能需要一些額外的時間。這是因為 Windows 版 FSx 需要在陰影複製儲存區上執行一致性檢查。由於 Windows 的 FSx 需要在維護陰影複製的同時執行 copy-on-write 活動，因此您也可能會遇到較高的 I/O 作業延遲。若要將陰影複製的可用性和效能影響降到最低，請手動刪除未使用的陰影複製，或將指令碼設定為自動刪除檔案系統上的舊陰影複製。

> **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，要求在新的使用中檔案伺服器上線之前掃描檔案系統上的陰影複製儲存。一致性檢查的持續時間與檔案系統上的陰影複製數目以及使用的儲存空間有關。若要避免延遲的容錯移轉和容錯回復事件，建議您在檔案系統上維護少於 64 個陰影複本，並依照下列步驟定期監視和刪除最舊的陰影複本。

設定陰影複製

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 Windows 檔案伺服器檔案系統的 FSx 上設定陰影複製時的三個主要設定：

- 設定陰影複製可在檔案系統上使用的最大儲存容量
- (選擇性) 設定檔案系統上可儲存的陰影複製數目上限。預設值為 20。
- (選擇性) 設定排程，以定義要擷取陰影複製的時間和間隔，例如每日、每週和每月

您可以在任何時間點，每個檔案系統最多儲存 500 個陰影複本；不過，我們建議您隨時維護少於 64 個陰影複本，以確保可用性和效能。達到此限制時，您採取的下一個陰影複製會取代最舊的陰影複製。同樣地，當達到最大陰影複製儲存量時，會刪除一或多個最舊的陰影複本，以便為下一個陰影複製提供足夠的儲存空間。

如需如何使用預設 Amazon FSx 設定快速啟用和排程定期陰影複製的詳細資訊，請參閱設定陰影複製以使用預設儲存區和排程。

配置陰影複製儲存的考量

陰影複製是自上次陰影複製後所做的檔案變更的區塊層級複本。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量可能會根據您的工作負載而有所不同。修改檔案時，陰影複製所使用的儲存空間取決於您的工作負載。當您決定要配置多少儲存空間給陰影複製時，您應該考慮工作負載的檔案系統使用模式。

啟用陰影複製時，您可以指定陰影複製可在檔案系統上使用的最大儲存容量。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，建議您增加限制。將限制設定得太小可能會導致刪除最舊的陰影複本的頻率比使用者預期的要高。

您可以將陰影複製儲存設定為無界 (`Set-FsxShadowStorage -Maxsize "UNBOUNDED"`)。不過，無限制的組態可能會導致大量陰影複製耗用您的檔案系統儲存空間。這可能會導致您的工作負載沒有足夠的儲存容量。如果您設定了無限制的儲存裝置，請務必在達到陰影複製限制時擴展儲存容量。如需有關將陰影複製儲存設定為特定大小或無限制的資訊，請參閱設定陰影複製儲存的最大數量。

啟用陰影複製之後，您可以監視陰影複製所耗用的儲存空間量。如需詳細資訊，請參閱 檢視陰影複製儲存。

設定陰影複製數目上限時的考量

啟用陰影複製時，您可以指定檔案系統上儲存的陰影複製數目上限。預設限制為 20，為了將陰影複製的可用性和效能影響降到最低，Microsoft 建議將陰影複製的數目上限設定為小於 64 個。由於 Windows 需要高等級的 I/O 效能來維護陰影複製，因此我們建議您使用 SSD 儲存體，並將輸送量容量提高到預期工作負載的三倍。這有助於確保您的檔案系統擁有足夠的資源，以避免不必要的陰影複製刪除等問題。

您可以將陰影複製的最大數目設定為 500。不過，如果您在單一檔案系統上有大量陰影複製或陰影複製佔用大量儲存空間 (TB 級)，則容錯移轉和容錯回復之類的處理程序可能需要比預期更長的時間。這是因為 Windows 需要在陰影複製儲存區上執行一致性檢查。由於 Windows 需要在維護陰影複製的同時執行 copy-on-write 活動，因此您也可能會遇到較高的 I/O 作業延遲。

陰影複製的檔案系統建議

以下是使用陰影複製的檔案系統建議。

- 請務必針對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 視窗服務器提供的卷影複製功能。根據設計，Microsoft Windows 會使用一 copy-on-write 種方法來記錄自最近陰影複製點以來的變更，而且此 copy-on-write 活動最多可能會針對每個檔案寫入作業產生三個 I/O 作業。如果 Windows 無法跟上每秒 I/O 作業的傳入速率，則可能會造成刪除所有陰影複製，因為它無法再透過維護陰影複製 copy-on-write。因此，請務必針對檔案系統上的工作負載需求佈建足夠的 I/O 效能容量 (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)。
- 當您啟用陰影複製時，我們通常建議您使用設定為 SSD 儲存的檔案系統，而不是 HDD 儲存體，因為 Windows 會耗用較高的 I/O 效能來維護陰影複製，並且 HDD 儲存體可提供較低的 I/O 作業效能容量。
- 除了已設定的最大陰影複製儲存容量 (MaxSpace) 之外，您的檔案系統應該至少有 320 MB 的可用空間。例如，如果您將 5 GB 配置MaxSpace給陰影複製，除了 5 GB 之外，您的檔案系統應該至少有 320 MB 的可用空間MaxSpace。

> **Warning**
>
> 設定陰影複製排程時，請確定在移轉資料或排定執行重複資料刪除工作時，不要排程陰影複製。當您預期檔案系統處於閒置狀態時，您應該排程陰影複製。如需有關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。

設定陰影複製以使用預設儲存區和排程

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消耗最多 10% 的檔案系統儲存容量。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空間數量不會類似地增加。

預設排程會在每個星期一、星期二、星期三、星期四和星期五 (UTC) 上午 7:00 和下午 12:00 自動擷取陰影複製。

設定陰影複製儲存的預設層級

1. Connect 線至與檔案系統具有網路連線的 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 計算執行個體。在中 AWS Managed Microsoft AD，該群組為 AWS 「委派的 FSx 管理員」。在您自我管理的 Microsoft AD 中，該群組是網域系統管理員或您在建立檔案系統時指定管理的自訂群組。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的連線到 Windows 執行個體。
3. 使用下列命令設定預設陰影儲存量。取代*FSxFileSystem-Remote-PowerShell-Endpoint*為您要管理之檔案系統的 Windows 遠 PowerShell 端端點。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」區段中，或在 DescribeFileSystem API 作業的回應中找到 Windows 遠 PowerShell 端端點。

```
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. Connect 線至與檔案系統具有網路連線的 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 計算執行個體。在中 AWS Managed Microsoft AD，該群組是AWS 委派的 FSx 管理員。在您自我管理的 Microsoft AD 中，該群組是網域系統管理員或您在建立檔案系統時指定管理的自訂群組。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的連線到 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}
```

回應會顯示現在已設定的預設排程。

```
FSx Shadow Copy Schedule
```

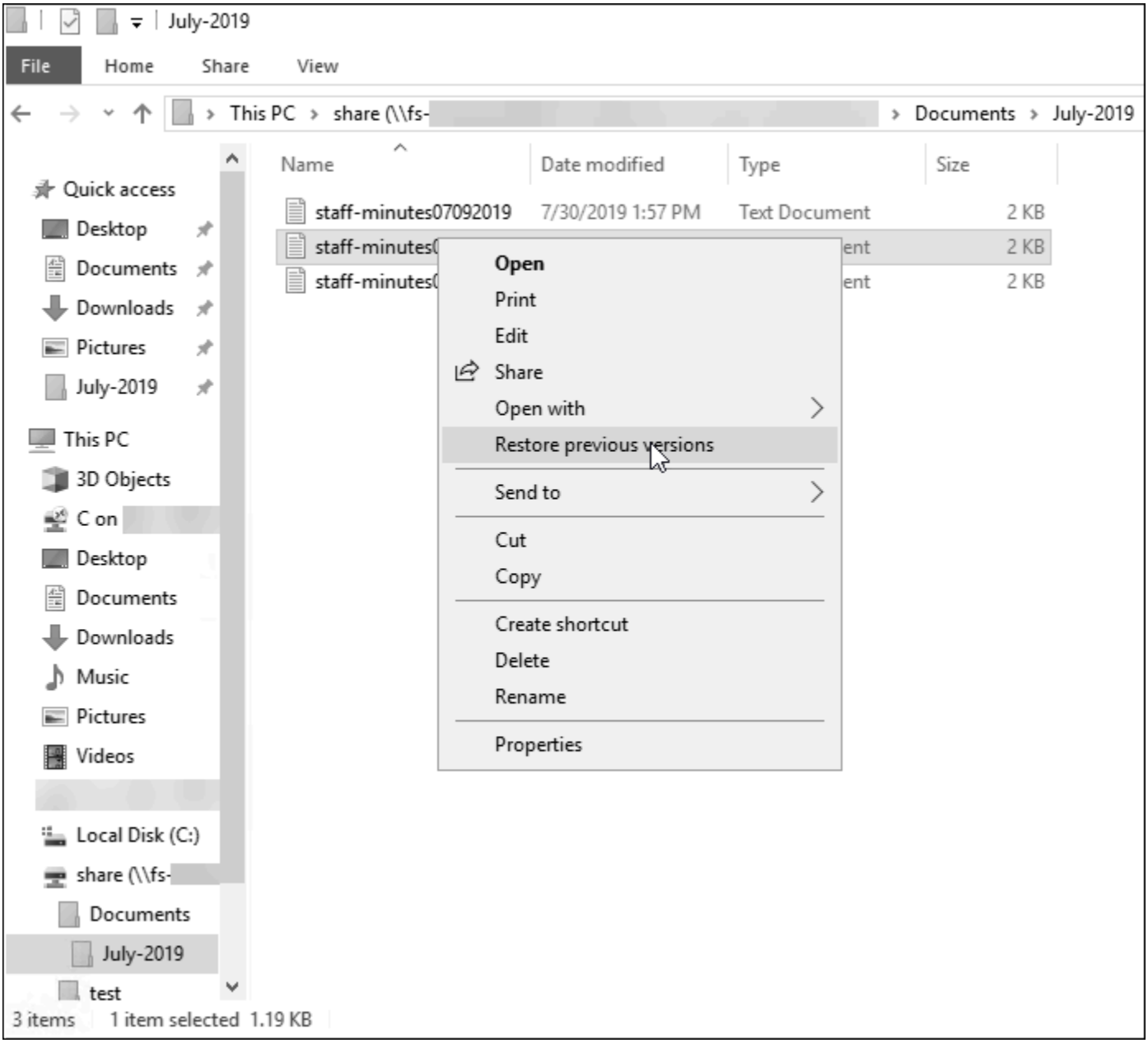
```
Start Time                Days of week                              WeeksInterval
----------                ------------                              -------------
2019-07-16T07:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
2019-07-16T12:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
```

若要瞭解其他選項及建立自訂陰影複製排程，請參閱建立自訂陰影複製排程。

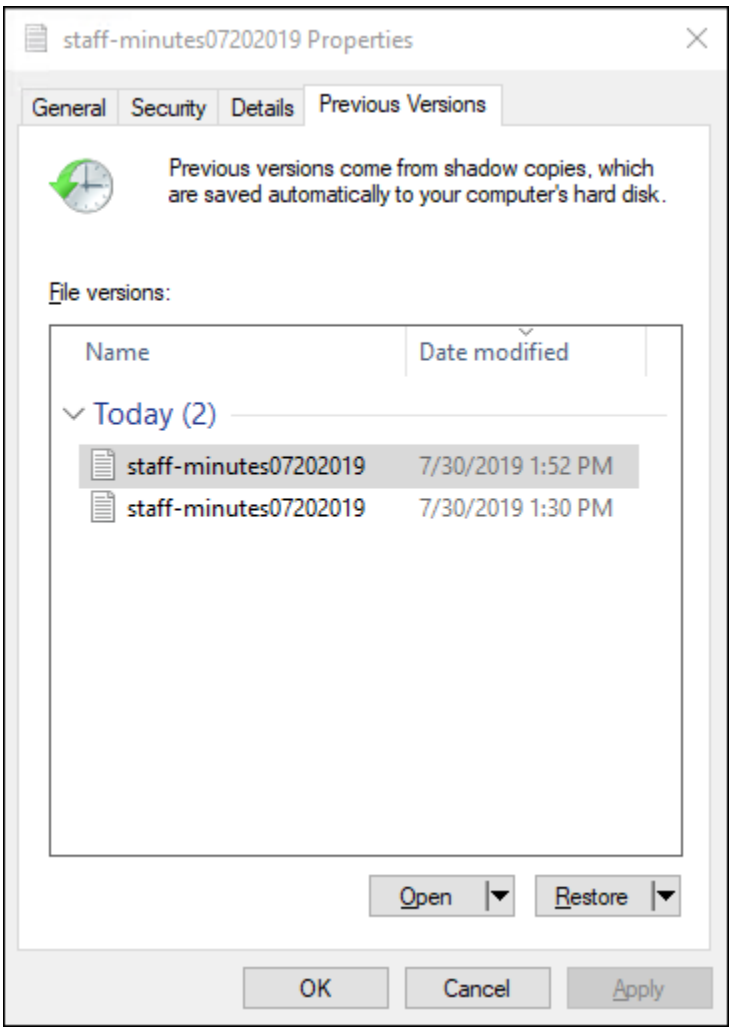
還原個別檔案和資料夾

在 Amazon FSx 檔案系統上設定陰影複製後，使用者可以快速還原個別檔案或資料夾的先前版本，以及復原已刪除的檔案。

使用者使用熟悉的 Windows 檔案總管介面將檔案還原至舊版本。若要還原檔案，請選擇要還原的檔案，然後從內容選單中選擇 [還原舊版] (按一下滑鼠右鍵)。



然後，使用者可以從「舊版」清單中檢視和還原先前的版本。



設定陰影複製儲存的最大數量

您可以使用 Set-FsxShadowStorage Custom PowerShell 指令，定義陰影複製可在檔案系統上使用的最大儲存容量。您可以使用或-Default參數來指定陰影複製可成長的大小-Maxsize上限。「使用」可將檔案系統儲存容量的最大值Default設定為 10%。您無法在相同-Maxsize的指令中指定和-Default參數。

使用-Maxsize，您可以定義陰影複製儲存，如下所示：

- 以字節為單位：Set-FsxShadowStorage -Maxsize 2500000000
- 以千字節，兆字節，千兆字節或其他單位為單位：或 Set-FsxShadowStorage -Maxsize (2500MB) Set-FsxShadowStorage -Maxsize (2.5GB)
- 以整體儲存空間的百分比表示：Set-FsxShadowStorage -Maxsize "20%"
- 作為無界：Set-FsxShadowStorage -Maxsize "UNBOUNDED"

用-Default於將陰影儲存設定為使用最多 10% 的檔案系統：Set-FsxShadowStorage -Default。若要進一步瞭解如何使用預設選項，請參閱設定陰影複製以使用預設儲存區和排程。

在 Windows 檔案伺服器檔案系統的 FSx 上設定陰影複製儲存的數量

1. 以身為檔案系統管理員群組成員的使用者身分，Connect 線至與檔案系統具有網路連線的運算執行個體。在中 AWS Managed Microsoft AD，該群組是AWS 委派的 FSx 管理員。在您自我管理的 Microsoft AD 中，該群組是網域系統管理員或您在建立檔案系統時指定管理的自訂群組。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的連線到 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 Amazon FSx 檔案系統上開啟遠端 PowerShell 工作階段。取代*FSxFileSystem-Remote-PowerShell-Endpoint*為您要管理之檔案系統的 Windows 遠 PowerShell 端端點。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」區段中，或在 DescribeFileSystem API 作業的回應中找到 Windows 遠 PowerShell 端端點。

```
PS C:\Users\delegateadmin> enter-pssession -computername FSxFileSystem-Remote-
PowerShell-Endpoint -configurationname fsxremoteadmin
```

4. 使用下列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體積的 10%，並將陰影對應的最大數量設定為 20。

```
[fs-1234567890abcef12]: PS>Set-FsxShadowStorage -Default
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- ------------------
             0         0 32530536858                 20
```

您可以使用指Set-FSxShadowStorage令搭配-MaxShadowCopyNumber參數並指定 1-500 之間的值，來限制檔案系統上允許的陰影複製數目上限。根據預設，陰影複製的最大數目設定為 20，如 Microsoft 針對作用中工作負載的建議。

檢視陰影複製儲存

您可以使用檔案系統上遠端 PowerShell 工作階段中的Get-FsxShadowStorage指令，檢視檔案系統上陰影複製目前使用的儲存空間量。如需在檔案系統上啟動遠端 PowerShell 工作階段的指示，請參閱使用 Amazon FSx CLI 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配置，如下所示：

- AllocatedSpace— 檔案系統上目前配置給陰影複製的儲存空間 (位元組)。最初，此值為 0。
- UsedSpace— 陰影複製目前使用的儲存容量 (以位元組為單位)。最初，此值為 0。
- MaxSpace— 陰影儲存可成長的最大儲存容量 (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— 檔案系統可以擁有的最大陰影複製數量，從 1-500 開始。

當UsedSpace量達到已設定的陰影複製儲存量上限 (MaxSpace) 或陰影複製數目達到已設定的最大陰影複製數目 (MaxShadowCopyNumber) 時，您下一次採取的陰影複製會取代最舊的陰影複製。如果您不想遺失最舊的陰影複製，請監視陰影複製儲存區，以確定您有足夠的儲存空間來儲存新的陰影複製。如果您需要更多空間，可以刪除現有的陰影複製或增加陰影複製儲存的最大容量。

> **Note**
>
> 自動或手動建立陰影複製時，它們會使用您設定為儲存限制的陰影複製儲存容量。陰影複製的大小隨著時間的推移而增加，並使用 CloudWatch FreeStorageCapacity度量所顯示的可用儲存空間，最多可達所設定的陰影複製儲存量上限 (MaxSpace)。

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，以及陰影複製排程。同時，您可以釋放檔案系統上的陰影複製儲存。

若要這麼做，請在檔案系統的遠端 PowerShell工作階段中輸入Remove-FsxShadowStorage指令。如需在檔案系統上啟動遠端 PowerShell 工作階段的指示，請參閱使用 Amazon FSx CLI 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.
```

建立自訂陰影複製排程

陰影複製排程會使用 Microsoft Windows 中的排程工作觸發程序來指定何時自動擷取陰影複製。陰影複製排程可以有多個觸發程序，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的數量，才能建立陰影複製排程。

在檔案系統上執行Set-FsxShadowCopySchedule命令時，會覆寫任何現有的陰影複製排程。如果您的用戶端電腦是 UTC 時區，您也可以使用 Windows 時區和-TimezoneId選項來指定觸發器的時區。如需 Windows 時區的清單，請參閱微軟的預設時區文件，或在 Windows 命令提示字元中執行下列指令：tzutil /l。若要深入了解 Windows 工作觸發程序，請參閱 Microsoft 開發人員中心中的工作觸發程序說明文件。

您也可以使用此-Default選項快速設定預設陰影複製排程。如需進一步了解，請參閱設定陰影複製以使用預設儲存區和排程。

建立自訂陰影複製排程

1. 建立一組 Windows 排程工作觸發程序，以定義何時在陰影複製排程中採取陰影複製。在本機電腦PowerShell上使用中的new-scheduledTaskTrigger指令來設定多個觸發器。

   下列範例會建立自訂陰影複製排程，該排程會在 UTC 時間每週一至週五的上午 6:00 及下午 6:00 執行陰影複製。根據預設，除非您在您建立的 Windows 排程工作觸發器中指定時區，否則時間為 UTC。

```
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. 用invoke-command於執行指scriptblock令。這麼做會寫入指令碼，使用您剛建立的new-scheduledTaskTrigger值來設定陰影複製排程。取代*FSxFileSystem-Remote-PowerShell-Endpoint*為您要管理之檔案系統的 Windows 遠 PowerShell 端端點。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」區段中，或在 DescribeFileSystem API 作業的回應中找到 Windows 遠 PowerShell 端端點。

```
PS C:\Users\delegateadmin> invoke-command -ComputerName FSxFileSystem-Remote-
PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {
```

3. 在>>提示下輸入以下行，以使用set-fsxshadowcopyschedule指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陰影複製排程，請在檔案系統的遠端 PowerShell 工作階段中輸入下列指令。如需在檔案系統上啟動遠端 PowerShell 工作階段的指示，請參閱使用 Amazon FSx CLI 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
```

刪除陰影複製排程

若要刪除檔案系統上現有的陰影複製排程，請在檔案系統的遠端 PowerShell 工作階段中輸入下列指令。如需在檔案系統上啟動遠端 PowerShell 工作階段的指示，請參閱使用 Amazon FSx CLI 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>
```

建立陰影複製

若要手動建立陰影複製，請在檔案系統的遠端 PowerShell 工作階段中輸入下列指令。如需在檔案系統上啟動遠端 PowerShell 工作階段的指示，請參閱使用 Amazon FSx CLI PowerShell。

```
[fs-0123456789abcdef1]PS>New-FsxShadowCopy

Shadow Copy {ABCDEF12-3456-7890-ABCD-EF1234567890} taken successfully
```

檢視現有的陰影複製

若要檢視檔案系統上現有的陰影複製集，請在檔案系統的遠端 PowerShell 工作階段中輸入下列指令。如需在檔案系統上啟動遠端 PowerShell 工作階段的指示，請參閱使用 Amazon FSx CLI 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
```

刪除卷影複製

您可以在檔案系統上使用遠端 PowerShell 工作階段中的`Remove-FsxShadowCopies`指令，刪除檔案系統上的一或多個現有陰影複本。如需在檔案系統上啟動遠端 PowerShell 工作階段的指示，請參閱使用 Amazon FSx CLI PowerShell。

使用下列其中一個必要選項指定要刪除的陰影複製：

- `-Oldest`刪除最舊的陰影複製
- `-All`刪除所有現有的陰影複製
- `-ShadowCopyId`依 ID 刪除特定的陰影複製。

您只能搭配指令使用一個選項。如果您未指定要刪除的陰影複製、指定多個陰影複製 ID，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陰影複製，請在檔案系統的遠端 PowerShell 工作階段中輸入下列指令。

```
[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陰影複製，請在檔案系統的遠端 PowerShell 工作階段中輸入下列指令。

```
[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特定數目最舊的陰影複本，請將-MaxShadowCopyNumber參數更新為您想要保留的陰影複製數目。但是，當系統自動刪除多餘的陰影複製複製時，此變更只會在下一個陰影複製快照集後生效。在檔案系統的遠端 PowerShell 工作階段中使用下列指令。

```
[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
```

排程複製使用 AWS DataSync

您可以使 AWS DataSync 用排程將 FSx for Windows File Server 系統的定期複製到第二個檔案系統。此功能適用於區域內部署和跨區域部署。若要進一步了解，請參閱本指南將現有檔案移轉至 FSx for Windows File Server 使用) AWS DataSync中的〈AWS DataSync 使用者指南〉中的〈AWS 儲存服務之間的資料傳輸〉。

管理檔案系統

本章說明如何存取 Amazon FSx CLI 以進行遠端管理 PowerShell，以及如何執行可用的檔案系統管理任務。您也可以使用 Microsoft 視窗原生圖形使用者介面 (GUI) 來執行某些系統管理工作。

主題

使用 Amazon FSx CLI PowerShell

用於遠端管理的 Amazon FSx CLI PowerShell 可為檔案系統管理員群組中的使用者啟用檔案系統管理功能。若要在 FSx for Windows File Server 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 Windows 檔案伺服器檔案系統的 FSx 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。如果您正在使用 AWS Managed Microsoft AD，則為「AWS 委派的 FSx 管理員」群組。如果您使用自我管理的 Microsoft Active Directory，也就是網域系統管理員群組或您在建立檔案系統時指定要管理的自訂群組。如需詳細資訊，請參閱 自我管理的活動目錄最佳實踐。
- 檔案系統的 VPC 安全群組輸入規則允許連接埠 5985 上的流量。

適用於遠端管理的 Amazon FSx CLI PowerShell 使用下列安全功能：

- 使用者認證會使用 Kerberos 驗證進行驗證。
- 連線的用戶端與檔案系統之間的管理工作階段通訊會使用 Kerberos 加密。

您有兩個選項可以在 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。`Invoke-Command`

如果要設置變量並將其作為參數傳遞給遠程管理命令，則需要使用`Invoke-Command`。

> **Note**
>
> 對於異地同步備份檔案系統，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 進行遠端管理。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。

使用遠端時，您需要使用檔案系統的 Windows 遠 PowerShell 端端點 PowerShell。使用 AWS Management Console，您可以在 [檔案系統詳細資料] 頁面的 [網路與安全性] 索引標籤中找到端點。使用 AWS CLI `describe-file-systems`命令，會在回應中傳回`RemoteAdministrationEndpoint`屬性。遠端管理端點會使用格式`amznfsxctlyaa1k.`*`ActiveDirectory-DNS-name`*，例如`amznfsxctlyaa1k.corp.example.com`。

您可以使用指`Get-Command`令程式取得中可用之指令程式、函數和別名的相關資訊。 PowerShell如需詳細資訊，請參閱 Microsoft 取得命令文件。

您也可以使用下列語法，使用指令`Invoke-Command`程式在檔案系統上的 PowerShell 命令上執行適用於遠端管理 CLI 的 Amazon FSx CLI。

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

如需有關如何在 FSx for Windows File Server 系統上啟動長期遠端 PowerShell 工作階段的指示，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 上啟動長效遠端 PowerShell 工作階段的指示。

在檔案系統上啟動遠端 PowerShell 工作階段

1. 以您建立檔案系統時所選擇之委派 FSx 管理員群組成員身分的使用者身分，Connect 線至與檔案系統具有網路連線的運算執行個體。
2. 在運算執行個體上開啟 Windows PowerShell 視窗。
3. 在中輸入下列命令 PowerShell，在 Amazon FSx 檔案系統上開啟長期存留的遠端工作階段。取代*Remote-PowerShell-Endpoint*為您要管理之檔案系統的 Windows 遠 PowerShell 端端點。作`FsxRemoteAdmin`為階段作業組態名稱使用。

   ```
   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 作用中目錄網域，系統會提示您在快顯視窗中輸入使用者登入資料。輸入身為 FSx 管理員群組成員之使用者的證明資料。如果您的執行個體已加入網域，系統就不會要求您提供憑證。

管理 DNS 別名

FSx for Windows File Server 每個可用來存取檔案系統資料的檔案系統提供預設的網域名稱系統 (DNS) 名稱。您也可以使用您選擇的 DNS 別名來存取檔案系統。透過 DNS 別名，您可以在將檔案系統儲存從現場部署遷移到 Amazon FSx 時，繼續使用現有的 DNS 名稱存取儲存在 Amazon FSx 上的資料，而無需更新任何工具或應用程式。如需詳細資訊，請參閱 將現有的檔案儲存遷移到 Amazon FSx。

> **Note**
>
> Support DNS 別名，適用於 Windows 檔案伺服器檔案系統在 2020 年 11 月 9 日下午 12 點之後建立的 FSx 上。若要在 2020 年 11 月 9 日下午 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. 將備份還原到新的檔案系統。如需詳細資訊，請參閱 還原備份。

一旦新的檔案系統可用，您就可以使用本節中提供的資訊，使用 DNS 別名來存取它。

> **Note**
>
> 這裡顯示的資訊假設您完全在 Active Directory 中工作，而且您沒有使用外部 DNS 提供者。第三方 DNS 提供者可能會導致非預期的行為。
> Amazon FSx 只會在您加入檔案系統的 AD 網域使用 Microsoft DNS 做為預設 DNS 時，才會註冊該檔案系統的 DNS 記錄。如果您使用的是第三方 DNS，則需要在建立檔案系統後手動設定 Amazon FSx 檔案系統的 DNS 項目。如需選擇用於檔案系統之正確 IP 位址的詳細資訊，請參閱取得要用於 DNS 的正確檔案系統 IP 位址。

當您建立新檔案系統時，以及當您從備份建立新檔案系統時，您可以將 DNS 別名與 Windows 檔案伺服器檔案系統的現有 FSx 產生關聯。您一次最多可以將 50 個 DNS 別名與檔案系統建立關聯。

除了將 DNS 別名與檔案系統產生關聯之外，若要讓用戶端使用 DNS 別名連線到檔案系統，您還必須執行下列動作：

- 為 Kerberos 驗證和加密設定服務主體名稱 (SPN)。
- 為解析為您的 Amazon FSx 檔案系統預設 DNS 名稱的 DNS 別名設定 DNS 別名的 DNS CNAME 記錄。

如需詳細資訊，請參閱 逐步解說 5：使用 DNS 別名存取您的檔案系統。

Windows 檔案伺服器檔案系統 FSx 的 DNS 別名必須符合下列需求：

- 必須格式化為完整網域名稱 (FQDN)。
- 可以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相關聯的別名建立關聯，則沒有任何作用。如果您嘗試取消別名與檔案系統無關聯的檔案系統之間的關聯，Amazon FSx 會回應錯誤的請求錯誤。

> **Note**
>
> 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，並會自動重新連線至檔案系統。用戶端在中斷連線時對應非連續可用 (非 CA) 共用的任何用戶端開啟的檔案，都必須由用戶端重新開啟。

主題

DNS 別名狀態

DNS 別名可以具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。
- 正在建立 — 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 驗證使用 DNS 別名

我們建議您在傳輸過程中使用 Kerberos 型身份驗證和加密與 Amazon FSx。Kerberos 為存取檔案系統的用戶端提供最安全的驗證。若要為使用 DNS 別名存取 Amazon FSx 檔案系統的用戶端啟用 Kerberos 身份驗證，您必須設定與檔案系統活動目錄電腦物件上的 DNS 別名相對應的服務主體名稱 (SPN)。

如果您已將 SPN 設定為您指派給 Active Directory 中電腦物件上另一個項目系統的 DNS 別名，則必須先移除這些 SPN，然後再將 SPN 新增至您的電腦物件。如需詳細資訊，請參閱 逐步解說 5：使用 DNS 別名存取您的檔案系統。

檢視檔案系統和備份的 DNS 別名

您可以使用 Amazon FSx 主控台、 AWS CLI 和 API 查看目前與檔案系統和備份相關聯的 DNS 別名。本主題提供如何檢視檔案系統和備份之 DNS 別名的指示。

若要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 [網路與安全性] 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 DescribeFileSystemAliasesAPI 作業。

若要檢視與備份相關聯的 DNS 別名

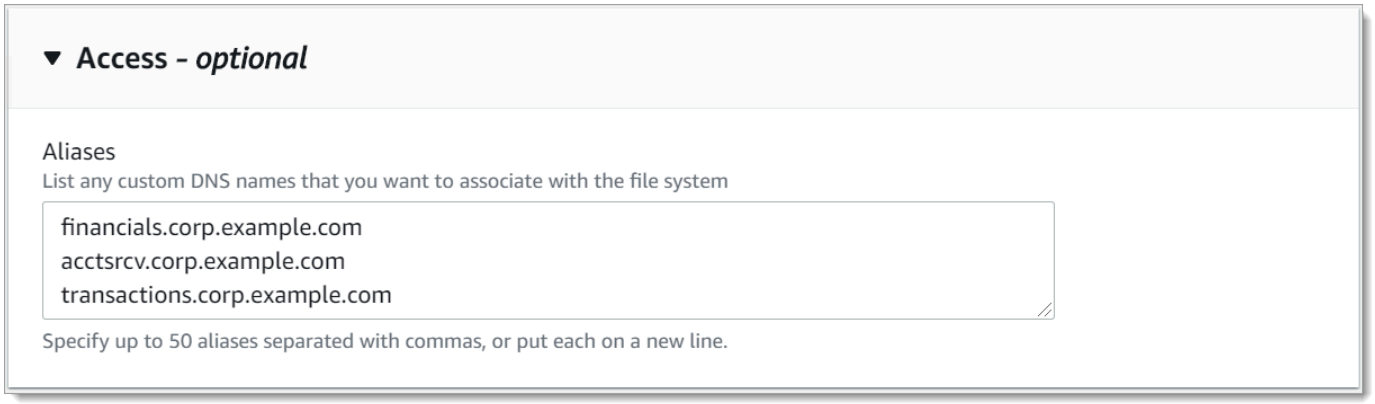
- 使用主控台 — 在功能窗格中，選擇 [備份]，然後選擇您要檢視的備份。在 [摘要] 窗格中，檢視 [DNS 別名] 欄位。
- 使用 CLI 或 API — 使用 `describe-backups` CLI 命令或 DescribeBackupsAPI 作業。

建立 DNS 別名與檔案系統的關聯

本主題說明當從頭開始建立新 FSx for Windows File Server 案系統時，或使用、和 API 從備份建立檔案系統時，如何關聯 DNS 別名。 AWS Management Console AWS CLI

建立新檔案系統時建立 DNS 別名的關聯 (主控台)

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 請遵循〈入門〉一節中所述的建立您的檔案系統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 (SPN)，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 逐步解說 5：使用 DNS 別名存取您的檔案系統。

在建立新的 Amazon FSx 檔案系統 (CLI) 時建立 DNS 別名的關聯

1. 建立新檔案系統時，請使用 Alias 屬性搭配 CreateFileSystemAPI 作業，將 DNS 別名與新檔案系統建立關聯。

```
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 (SPN)，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 逐步解說 5：使用 DNS 別名存取您的檔案系統。

若要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檔案系統時，您可以將 A li as 屬性與 CreateFileSystemFromBackupAPI 作業搭配使用，如下所示：

   - 依預設，與備份相關聯的所有別名都會與新檔案系統相關聯。
   - 若要建立檔案系統而不保留備份中的任何別名，請使用具有空白集的`Aliases`屬性。

若要關聯其他 DNS 別名，請使用內`Aliases`容，並同時包含與備份相關聯的原始別名以及要關聯的新別名。

下列 CLI 命令會將兩個別名與 Amazon FSx 從備份建立的檔案系統相關聯。

```
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]
```

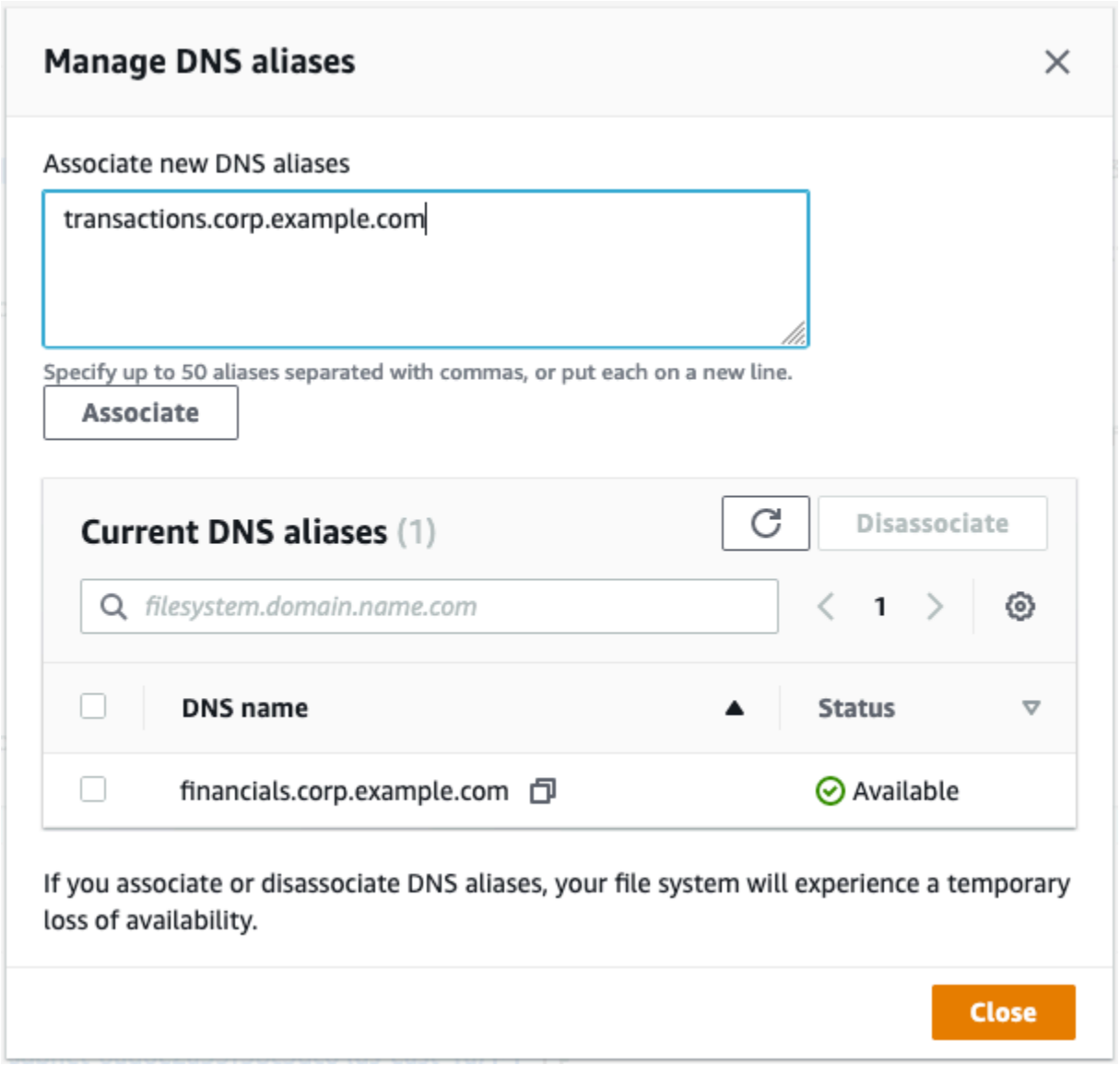
2. 當檔案系統可用時，您可以透過設定服務主體名稱 (SPN)，以及更新或建立別名的 DNS CNAME 記錄，使用 DNS 別名來存取它。如需詳細資訊，請參閱 逐步解說 5：使用 DNS 別名存取您的檔案系統。

管理現有檔案系統上的 DNS 別名

本主題說明如何使用 AWS Management Console 和 AWS CLI 在現有檔案系統上新增和移除別名。

管理檔案系統 DNS 別名 (主控台)

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 瀏覽至檔案系統，然後選擇您要管理 DNS 別名的 Windows 檔案系統。
3. 在 [網路與安全性] 索引標籤上，選擇 [管理 DNS 別名] 以顯示 [管理 DNS 別名] 對話方塊。



- 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。
- 取消關聯 DNS 別名 — 在 [目前別名] 清單中，選擇要取消關聯的別名。選擇取消關聯。

您可以監視在「目前別名」清單中管理的別名狀態。重新整理清單以更新狀態。別名最多需要 2.5 分鐘才能與檔案系統產生關聯或取消關聯。

4. 當別名可用時，您可以設定服務主體名稱 (SPN)，以及更新或建立別名的 DNS CNAME 記錄，使用 DNS 別名來存取檔案系統。如需詳細資訊，請參閱 逐步解說 5：使用 DNS 別名存取您的檔案系統。

將 DNS 別名與現有檔案系統產生關聯 (CLI)

1. 使用 `associate-file-system-aliases` CLI 命令或 AssociateFileSystemAliasesAPI 作業，將 DNS 別名與現有檔案系統建立關聯。

   下列 CLI 要求會將兩個別名與指定的檔案系統產生關聯。

   ```
   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 與檔案系統關聯的別名狀態。

   ```
   {
       "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 (這DescribeFileSystemAliases是對等的 API 作業) 來監視要關聯之別名的狀態。

3. 當值`Lifecycle`為可用 (最多需要 2.5 分鐘的程序) 時，您可以設定服務主要名稱 (SPN)，以及更新或建立別名的 DNS CNAME 記錄，使用 DNS 別名來存取檔案系統。如需詳細資訊，請參閱 逐步解說 5：使用 DNS 別名存取您的檔案系統。

取消 DNS 別名與檔案系統的關聯 (CLI)

- 使用 `disassociate-file-system-aliases` CLI 命令或 DisassociateFileSystemAliasesAPI 作業取消 DNS 別名與現有檔案系統的關聯。

  下列指令會取消某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 與檔案系統中斷關聯的別名狀態。

```
{
    "Aliases": [
        {
            "Name": "financials.corp.example.com",
            "Lifecycle": DELETING
        }
    ]
}
```

使用 `describe-file-system-aliases` CLI 命令 (DescribeFileSystemAliases是等效的 API 作業) 來監視別名的狀態。刪除別名最多需要 2.5 分鐘。

管理 FSx 上適用於 Windows 檔案伺服器檔案系統的檔案共用

本主題說明如何透過執行下列工作來管理檔案共用。

- 建立新檔案共用
- 修改現有的檔案共用
- 移除現有的檔案共用

您可以使用視窗原生共用資料夾圖形用戶界面和 Amazon FSx CLI 進行遠端管理，以管理 FSx 上 PowerShell 的 Windows 檔案伺服器檔案系統上的檔案共用。第一次開啟位於不同檔案系統上共用的內容功能表時，使用共用資料夾 GUI (fsmgmt.msc) 時，您可能會遇到延遲的情況。若要避免這些延遲，請使用 PowerShell 來管理位於多個檔案系統上的檔案共用。

請注意，Windows 支持的所有文件系統對文件和目錄的名稱都存在規則和限制。」。為了確保您可以成功地建立和存取資料，您應該根據這些 Windows 準則命名檔案和目錄。如需詳細資訊，請參閱命名慣例。

> **Warning**
>
> Amazon FSx 要求系統使用者必須在您建立 SMB 檔案共用的每個資料夾上擁有完全控制 NTFS ACL 許可。請勿變更資料夾上此使用者的 NTFS ACL 權限，因為這樣做可能會導致檔案共用無法存取。

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 提供管理 Windows 伺服器上所有共用資料夾的集中位置。下列程序說明如何管理檔案共用。

將共用資料夾連線到您的 FSx for Windows File Server) 檔案系統

1. 啟動您的 Amazon EC2 實例，並將其連接到您的 Amazon FSx 文件系統加入的 Microsoft 活動目錄。若要執行此操作，請從《AWS Directory Service 管理指南》中選擇下列其中一個程序：

   - 無縫加入執行個體
   - 手動聯結視窗執行個體

2. 以身為檔案系統管理員群組成員的使用者身分 Connect 至執行個體。在 AWS 受管理的 Microsoft 活動目錄中，這個群組稱為 AWS 委派的 FSx 系統管理員。在您自我管理的 Microsoft Active Directory 中，此群組稱為網域系統管理員，或是您在建立期間所提供之系統管理員群組的自訂名稱。如需詳細資訊，請參閱 Amazon 彈性運算雲端使用者指南中的 Windows 執行個體 Connect 到您的 Windows 執行個體。
3. 開啟 [開始] 功能表，並使用 [以系統管理員身分執行] 來執行 fsmgmt.msc。這麼做會開啟共用資料夾 GUI 工具。
4. 針對「動作」，選擇「Connect 到另一台電腦」
5. 例如**`amznfsxabcd0123.corp.example.com`**，如果是其他電腦，請輸入 Amazon FSx 檔案系統的網域名稱系統 (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]，選擇您的檔案系統，然後檢查檔案系統詳細資料頁面的 [網路和安全性] 區段。您也可以在DescribeFile系統 API 作業的回應中取得 DNS 名稱。
6. 選擇確定。然後，您 Amazon FSx 檔案系統的項目會顯示在共用資料夾工具的清單中。

現在共用資料夾已連線到 Amazon FSx 檔案系統，您可以在檔案系統上管理 Windows 檔案共用。會呼叫預設共用`\share`。您可以使用以下動作來執行此操作：

- 建立新的檔案共用 — 在共用資料夾工具中，選擇左窗格中的 [共用] 以查看 Amazon FSx 檔案系統的使用中共用。選擇 [新增共用] 並完成 [建立共用資料夾] 精靈。

  在建立新檔案共用之前，您必須先建立本端資料夾。你可以這樣做，如下所示：

  - 使用共用資料夾工具：在指定本機資料夾路徑時按 [瀏覽] ，然後按 [建立新資料夾] 以建立本機資料夾。
  - 使用命令行：

    ```
    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，在右窗格中開啟您要修改之檔案共用的內容 (按一下滑鼠右鍵) 選單，然後選擇「內容」。修改屬性，然後選擇「確定」。
- 移除檔案共用 — 在「共用資料夾」工具中，開啟右窗格中要移除之檔案共用的內容 (按一下滑鼠右鍵) 功能表，然後選擇「停止共用」。

> **Note**
>
> 對於單一可用區 2 和異地同步備份檔案系統，只有在使用 Amazon FSx 檔案系統的 DNS 名稱連線到 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 位址或 DNS 別名連線，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 檔案系統上的共用，當您第一次為位於不同檔案系統上的共用開啟檔案共用內容功能表時，可能會遇到延遲。PowerShell 為了避免這些延遲，您可以使用以下說明來管理檔案共用。

管理檔案共用 PowerShell

您可以使用的自訂遠端管理命令來管理檔案共用。 PowerShell這些指令可協助您更輕鬆地將這些工作自動化：

- 將現有檔案伺服器上的檔案共用移轉至 Amazon FSx

- 跨 AWS 區域的檔案共用同步處理以進行災難復原
- 以程式設計方式管理持續工作流程的檔案共用，例如團隊檔案共用佈建

若要了解如何使用 Amazon FSx CLI 進行遠端管理 PowerShell，請參閱使用 Amazon FSx CLI 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適用於 Windows 檔案伺服器檔案系統的 FSx 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	設定共用的屬性。
Get-FSxSmbShareAccess	擷取共用的存取控制清單 (ACL)。
Grant-FSxSmbShareAccess	將受託人的允許存取控制項目 (ACE) 新增至共用的安全性描述元。
Revoke-FSxSmbShareAccess	從共用的安全性描述元移除受託人的所有允許 ACE。
Block-FSxSmbShareAccess	將受託人的拒絕 ACE 新增至共用的安全性描述元。
Unblock-FSxSmbShareAccess	從共用的安全性描述元移除受託人的所有拒絕 ACE。

每個指令的線上說明提供了所有指令選項的參考。若要存取此說明，請使用執行指令-?，例如New-FSxSmbShare -?。

將憑據傳遞給 New-F 共享 SxSmb

您可以將認證傳遞給 New-F，以SxSmbShare 便您可以在循環中運行它以創建數百或數千個共享，而無需每次重新輸入憑據。

使用下列其中一個選項，準備在 FSx for Windows 檔案伺服器檔案伺服器上建立檔案共用所需的認證物件。

- 若要以互動方式產生認證物件，請使用下列命令。

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

- 若要使用 AWS Secrets Manager 資源產生認證物件，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 (CA) 共用

您可以在 PowerShell上使用 Amazon FSx CLI 建立持續可用的 (CA) 共用，以進行遠端管理。在 FSx 適用於 Windows 檔案伺服器異地同步備份檔案系統上建立的 CA 共用具有高耐用性和高可用性。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，但並非高可用性。在將`-ContinuouslyAvailable`選項設定為的情況下使`$True`用指`New-FSxSmbShare`令，以指定共用為連續可用的共用。以下是建立 CA 共用的範例命令。

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

您可以使用`Set-FSxSmbShare`指令修改現有檔案共用上的`-ContinuouslyAvailable`選項。

判斷現有的檔案共用是否持續可用

使用以下指令可檢視既有檔案共用的「連續可用」性質的值。

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

如果啟用 CA，輸出將包括以下行：

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

如果未啟用 CA，輸出將包含以下行：

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

若要在現有檔案共用上啟用持續可用，請使用下列命令：

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

檔案存取稽核

適用於 Windows 檔案伺服器的 Amazon FSx 支援稽核最終使用者對檔案、資料夾和檔案共用的存取。您可以選擇將檔案系統的稽核事件記錄傳送至其他提供豐富功能的 AWS 服務。其中包括啟用查詢、處理、儲存和封存記錄、發出通知，以及觸發動作，以進一步推進您的安全性與合規目標。

如需有關使用檔案存取稽核取得存取模式的深入資訊，並針對使用者活動實作安全性通知，請參閱檔案儲存存取模式深入解析和實作使用者活動的安全性通知。

檔案存取稽核可讓您根據您定義的稽核控制，記錄使用者對個別檔案、資料夾和檔案共用的存取。稽核控制項也稱為 NTFS 系統存取控制清單 (SACL)。如果您已在現有檔案資料上設定稽核控制，則可以透過建立新的 Amazon FSx for Windows 檔案伺服器檔案系統並移轉資料，以利用檔案存取稽核。

Amazon FSx 針對檔案、資料夾和檔案共用存取支援下列 Windows 稽核事件：

- 對於文件訪問，它支持：全部，遍歷文件夾/執行文件，列出文件夾/讀取數據，讀取屬性，創建文件/寫入數據，創建文件夾/附加數據，寫入屬性，刪除子文件夾和文件，刪除，讀取權限，更改權限和獲取所有權。
- 對於文件共享訪問，它支持：Connect 到文件共享。

Amazon FSx 跨檔案、資料夾和檔案共用存取，支援記錄成功嘗試 (例如擁有足夠權限的使用者成功存取檔案或檔案共用)、失敗嘗試或兩者皆可。

您可以設定是否只要對檔案和資料夾、僅對檔案共用或兩者進行存取稽核。您也可以設定應記錄哪些類型的存取 (僅限成功嘗試、僅嘗試失敗，或兩者皆記錄)。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一般使用者在啟用資料之後的存取資料。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使用者檔案、資料夾和檔案共用存取活動的稽核事件記錄。

支援的最大存取稽核事件速率為每秒 5,000 個事件。不會針對每個檔案讀取和寫入作業產生存取稽核事件，而是在每個檔案中繼資料作業 (例如使用者建立、開啟或刪除檔案時) 產生一次。

主題

稽核事件記錄目的地

啟用檔案存取稽核時，必須設定 Amazon FSx 向其傳送稽核事件日誌的 AWS 服務。您可以將稽核事件日誌傳送到 CloudWatch 日誌日誌群組中的 Amazon CloudWatch 日誌串流或 Amazon 資料 Firehose 交付串流。您可以在建立 Amazon FSx for Windows File Server 系統時，或在更新現有檔案系統後隨時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記錄檔目的地：

- 如果您要在 Amazon CloudWatch 主控台中存放、檢視和搜尋稽核事件日誌，請選擇「CloudWatch 記錄檔」、使用 CloudWatch 日誌深入解析在日誌上執行查詢，以及觸發 CloudWatch 警示或 Lambda 函數。
- 如果您想要將事件持續串流至 Amazon S3 中的儲存、Amazon Redshift 中的資料庫、Amazon OpenSearch 服務，或是 AWS 合作夥伴解決方案 (例如 Splunk 或 Datadog) 以進行進一步分析，請選擇 Firehose。

根據預設，Amazon FSx 會在您的帳戶中建立並使用預設的 CloudWatch 日誌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 記錄檔記錄群組或使用 Firehose 做為稽核事件記錄目的地，以下是稽核事件記錄目標的名稱和位置的需求：

- CloudWatch 記錄檔記錄群組的名稱必須以/aws/fsx/前置詞開頭。如果在主控台上建立或更新檔案系統時沒有現有的 CloudWatch 日誌日誌群組，Amazon FSx 可以在日誌日誌群組中建立和使用預設 CloudWatch 日/aws/fsx/windows誌串流。如果您不想使用預設的記錄群組，設定 UI 可讓您在主控台上建立或更新檔案系統時，建立 CloudWatch 記錄檔記錄群組。
- Firehose 傳送串流的名稱必須以aws-fsx-字首開頭。如果您沒有現有的 Firehose 傳遞串流，您可以在主控台建立或更新檔案系統時建立一個串流。
- Firehose 傳送串流必須設定Direct PUT為使用作為其來源。您無法使用現有的 Kinesis 資料串流作為交付串流的資料來源。
- 目的地 (CloudWatch 日誌記錄群組或 Firehose 交付串流) 必須與 AWS 帳戶 Amazon FSx 檔案系統位於相同的 AWS 分割區中。 AWS 區域

您可以隨時變更稽核事件記錄目的地 (例如，從 CloudWatch 記錄檔變更為 Firehose)。當您這麼做時，新的稽核事件記錄只會傳送至新的目的地。

最好的工作審核事件日誌傳遞

稽核事件記錄通常會在幾分鐘內傳遞至目的地，但有時候可能需要更長的時間。在極少數情況下，稽核事件記錄可能會遺漏。如果您的使用案例需要特定的語意 (例如，確保沒有遺漏稽核事件)，建議您在設計工作流程時將遺漏的事件列入考量。您可以掃描檔案系統上的檔案和資料夾結構來稽核遺漏的事件。

遷移稽核控制

如果現有檔案資料已設定稽核控制 (SACL)，則可以建立 Amazon FSx 檔案系統，然後將資料遷移到新的檔案系統。我們建議您 AWS DataSync 使用將資料和相關的 SACL 傳輸到 Amazon FSx 檔案系統。作為替代解決方案，您可以使用 Robocopy (強大的文件複製) 。如需詳細資訊，請參閱 將現有的檔案儲存遷移到 Amazon FSx。

檢視事件記錄

您可以在 Amazon FSx 開始發出稽核事件日誌後檢視這些日誌。檢視記錄的位置和方式取決於稽核事件記錄檔目的地：

- 您可以前往 CloudWatch 主控台並選擇要傳送稽核事件記 CloudWatch 錄檔的記錄群組和記錄資料流，以檢視記錄檔記錄。如需詳細資訊，請參閱 Amazon CloudWatch 日誌使用者指南中的檢視傳送至 CloudWatch 日誌的日誌資料。

  您可以使用 CloudWatch 日誌深入解析，以互動方式搜尋和分析記錄資料。如需詳細資訊，請參閱 Amazon CloudWatch 日誌使用者指南中的使用日誌洞察分析 CloudWatch 日誌資料。

您也可以將稽核事件日誌匯出到 Amazon S3。如需詳細資訊，請參閱 Amazon CloudWatch 日誌使用者指南中的將日誌資料匯出到 Amazon S3。

- 您無法在 Firehose 上檢視稽核事件記錄檔。不過，您可以設定 Firehose 將記錄檔轉寄至您可以讀取的目的地。目的地包括 Amazon S3、Amazon Redshift、Amazon OpenSearch 服務以及合作夥伴解決方案，如需詳細資訊，請參閱 Amazon 資料 Firehose 開發人員指南中的選擇目的地。

稽核事件欄位

本節提供稽核事件記錄檔中資訊的說明，以及稽核事件範例。

以下是 Windows 稽核事件中重要欄位的描述。

- 事件 ID 是指微軟定義的視窗事件記錄檔事件識別碼。如需檔案系統事件和檔案共用事件的相關資訊，請參閱 Microsoft 文件。
- SubjectUserName指執行存取的使用者。
- ObjectName指的是存取的目標檔案、資料夾或檔案共用。
- ShareName可用於針對檔案共用存取產生的事件。例如，`EventID 5140`在存取網路共用物件時產生。
- IpAddress是指針對檔案共用事件起始事件的用戶端。
- 關鍵字（如果可用）是指文件訪問成功還是失敗。對於成功的訪問，值是`0x8020000000000000`。對於失敗的存取，值為`0x8010000000000000`。
- TimeCreated SystemTime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 Windows 遠 PowerShell 端端點的 DNS 名稱，可用來識別檔案系統。
- AccessMask(如果可用) 是指執行的檔案存取類型 (例如， ReadData、 WriteData)。
- AccessList是指請求或授予對象的訪問權限。如需詳細資訊，請參閱下表和 Microsoft 文件 (例如在事件 4556 中)。

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

存取類型	存取遮罩	Value
附加資料或新增子目錄	0X4	%%4418
讀取延伸屬性	0X8	%%4419
寫入擴充屬性	0X10	%%4420
執行/周轉	0X20	%%4421
刪除子系	0X40	%%4422
讀取屬性	0x80	%%4423
寫入屬性	0X100	%%4424
Delete	0x10000	%%1537
讀取 ACL	0x20000	%%1538
寫入 ACL	0x40000	%%1539
寫入擁有者	0x80000	%%1540
同步	0x100000	%%1541
存取安全性 ACL	0x1000000	%%1542

以下是一些具有例子的關鍵事件。請注意，XML 已格式化以提高可讀性。

刪除物件時，會記錄事件識別碼 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>
```

刪除檔案的請求會記錄事件識別碼 4659。

```
<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>
```

對物件執行特定作業時，會記錄事件識別碼 4663。下面的例子顯示了從一個文件，它可以被解釋讀取數據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>
```

下面的例子顯示了從文件，它可以從解釋寫/追加數據。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>
```

事件識別碼 4656 表示已要求物件的特定存取權。在下列範例中，「讀取」要求初始化為 ObjectName 「最佳」，而且嘗試失敗，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>
```

變更物件的權限時，會記錄事件識別碼 4670。下列範例顯示使用者「管理員」修改了「權限測試」上的權限，以將權限新增至 SID ObjectName 「S-1-5-21-6584921-4185342820-3824891517-1113」。如需如何解譯權限的詳細資訊，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>
```

每次存取檔案共用時，都會記錄事件識別碼 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>
```

在檔案共用層級拒絕存取時，會記錄事件識別碼 5145。下面的例子顯示了訪問 ShareName 「demoshare01」被拒絕。

```
<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 搜尋記錄資料，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，請執行下列動作

```
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 日誌見解查詢語言的詳細資訊，請參閱 Amazon Logs 使用者指南中的「利用 CloudWatch 日誌洞察分析 CloudWatch 日誌資料」。

設定檔案和資料夾稽核控制

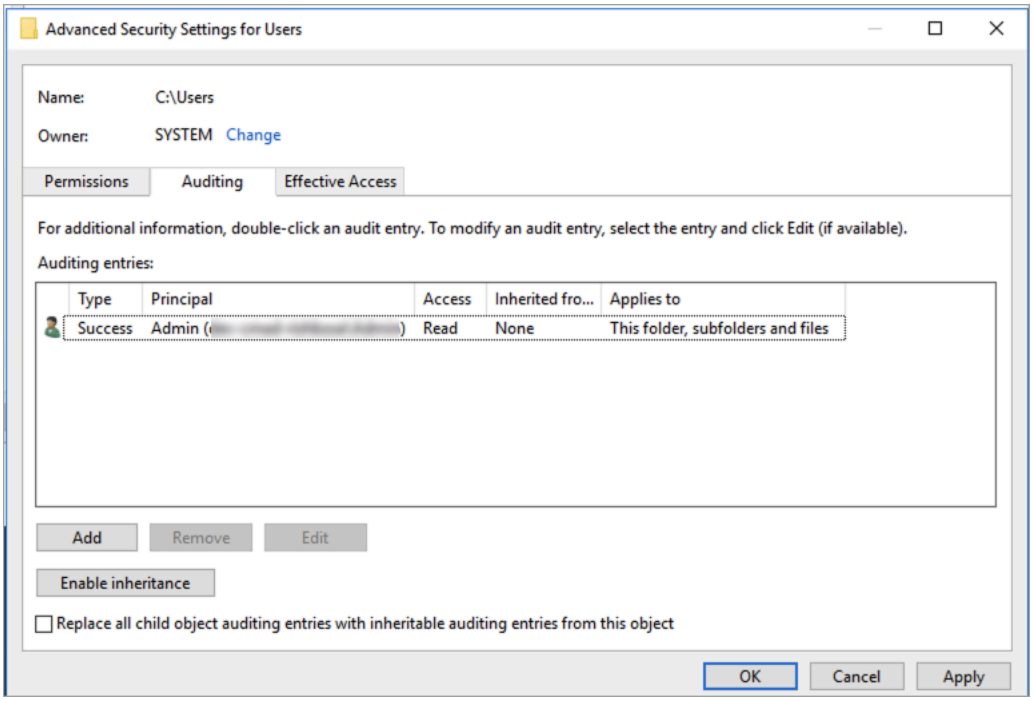
您需要針對要稽核使用者存取嘗試進行稽核的檔案和資料夾設定稽核控制。稽核控制項也稱為 NTFS 系統存取控制清單 (SACL)。

您可以使用 Windows 原生 GUI 介面或以程式設計方式使用 Windows PowerShell 命令來設定稽核控制項。如果啟用繼承，您通常只需要在要記錄存取的頂層資料夾上設定稽核控制。

使用視窗圖形用戶界面來設定稽核存取

若要使用 GUI 來設定檔案和資料夾的稽核控制項，請使用 Windows 檔案總管。在指定檔案或資料夾上，開啟 Windows 檔案總管，然後選取 [內容] > [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。每當管理員使用者開啟控制代碼以便成功讀取時，就會發出 Windows 事件記錄項目。



「類型」字段表示您要稽核的操作。將此欄位設定為「成功」以稽核成功嘗試，將無法稽核失敗的嘗試次數，或將「全部」設定為「全部」可稽核成功和失敗

如需稽核項目欄位的詳細資訊，請參閱 Microsoft 說明文件中的對檔案或資料夾套用基本稽核原則。

使用 PowerShell 指令設定稽核存取

您可以使用 Microsoft 視窗`Set-Acl`指令在任何檔案或資料夾上設定稽核 SACL。如需有關此命令的資訊，請參閱 Microsoft S et-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指令，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

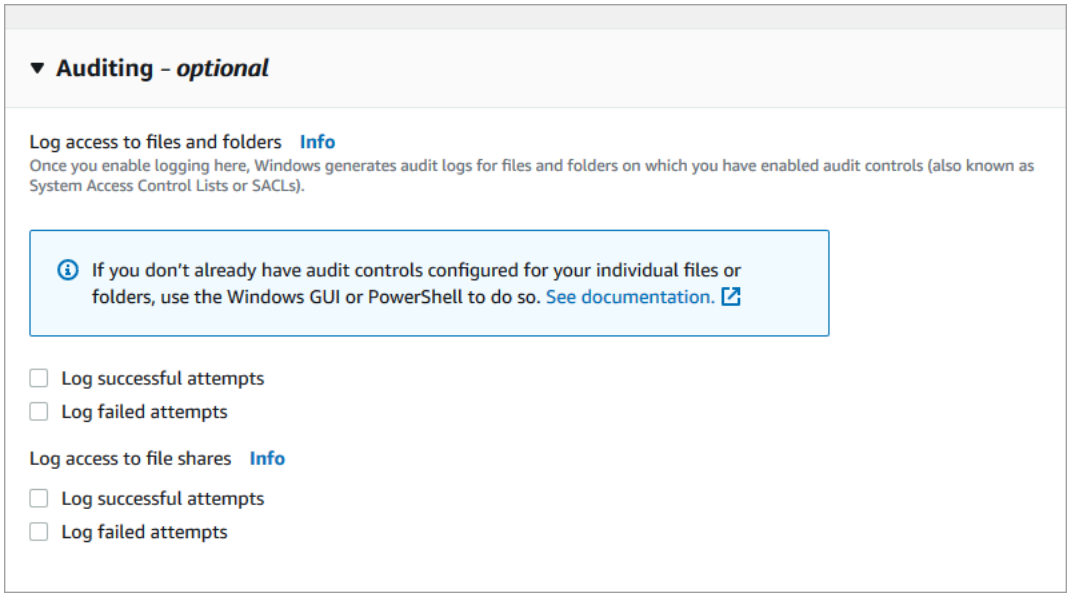
您可以在建立適用於 Windows 檔案伺服器檔案系統的新 Amazon FSx 時啟用檔案存取稽核。當您從 Amazon FSx 主控台建立檔案系統時，預設會關閉檔案存取稽核。

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，以及稽核事件記錄目的地。您可以使用 Amazon FSx 主控台或 API 來執行這些任務。 AWS CLI

> **Note**
>
> 只有輸送量容量為 32 MB/s 或以上的 Windows 檔案伺服器檔案系統的 Amazon FSx 才支援檔案存取稽核。如果啟用了檔案存取稽核，則無法建立或更新輸送容量小於 32 MB/s 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。

若要在建立檔案系統時啟用檔案存取稽核 (主控台)

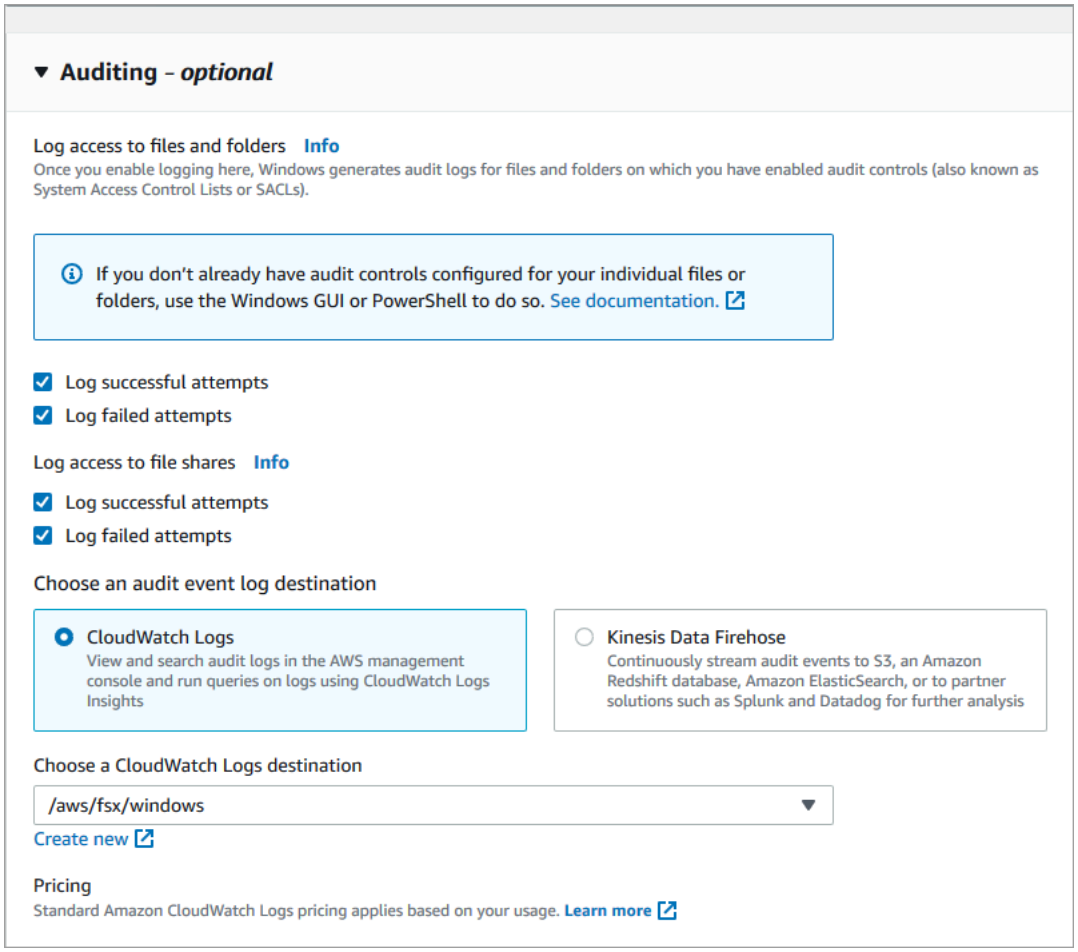
1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 請遵循〈入門〉一節中所述的建立您的檔案系統建立新檔案系統的程序。
3. 開啟 [稽核-選用] 區段。依預設，會停用檔案存取稽核。



4. 若要啟用和設定檔案存取稽核，請執行下列動作。

   - 對於檔案和資料夾的記錄存取，請選取成功和/或失敗嘗試的記錄。如果您未進行選取，則會停用檔案和資料夾的記錄功能。
   - 對於記錄檔案共用的存取，請選取成功和/或失敗嘗試的記錄。如果您未進行選取，則會停用檔案共用的記錄功能。
   - 針對 [選擇稽核事件記錄目的地]，選擇 [CloudWatch 記錄檔] 或 [Firehose]。然後選擇現有的記錄或傳送串流，或建立新的記錄檔或傳送串流。對於 CloudWatch 日誌，Amazon FSx 可以在日誌日誌群組中建立和使用預設 CloudWatch 日`/aws/fsx/windows`誌串流。

   以下是檔案存取稽核組態的範例，此設定將稽核一般使用者對檔案、資料夾和檔案共用的成功和失敗存取嘗試。稽核事件記錄檔將傳送至預設的 CloudWatch 記錄檔記`/aws/fsx/windows`錄群組目的地。



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。

若要在建立檔案系統 (CLI) 時啟用檔案存取稽核

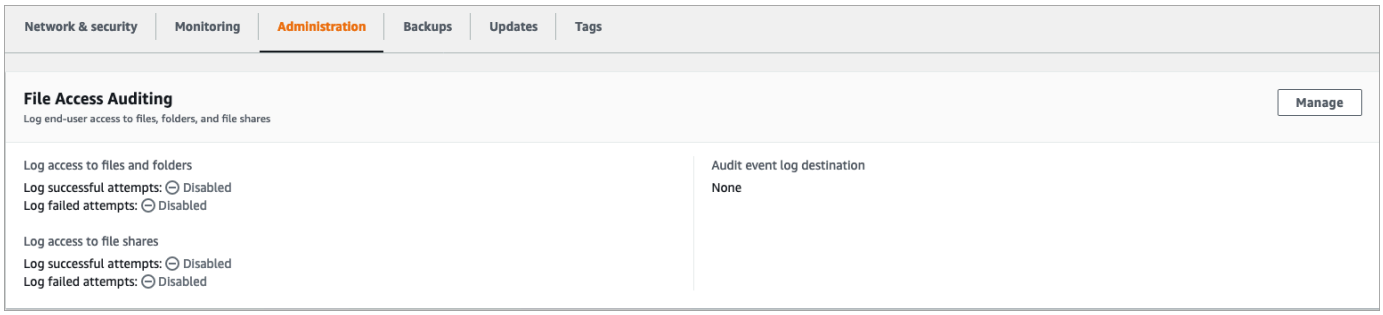
1. 建立新檔案系統時，請搭配 CreateFileSystemAPI 作業使用`AuditLogConfiguration`屬性，以啟用新檔案系統的檔案存取稽核功能。

```
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"}'
```

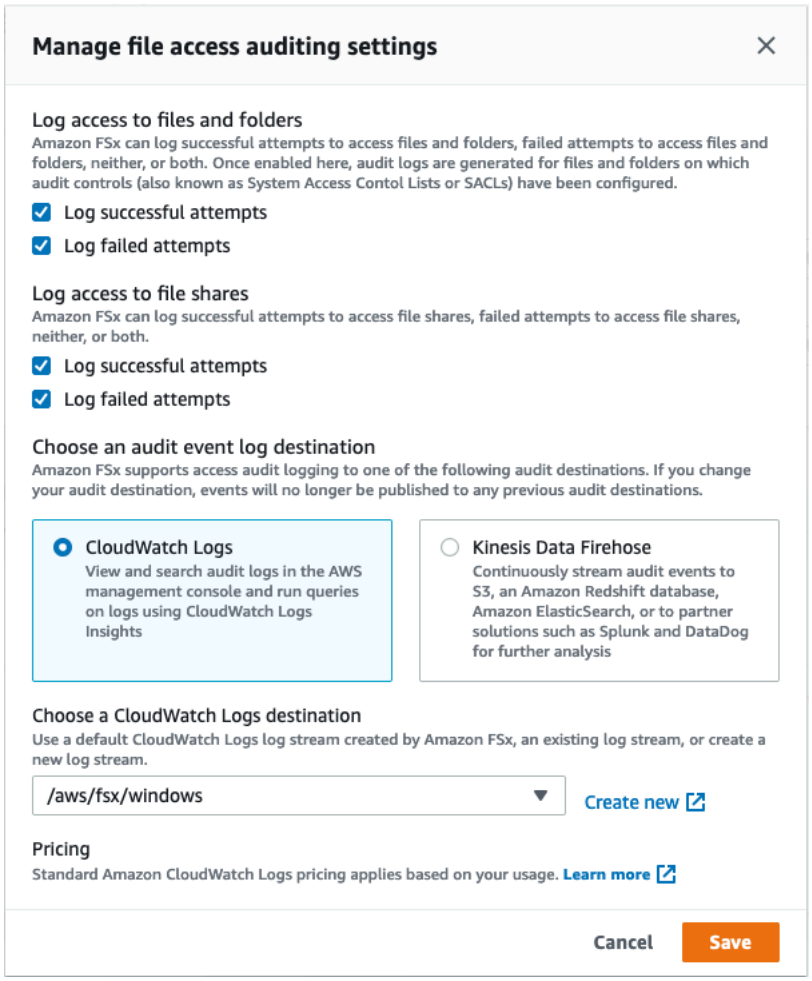
2. 當檔案系統可用時，會啟用檔案存取稽核功能。

若要變更檔案存取稽核組態 (主控台)

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 瀏覽至 [檔案系統]，然後選擇您要管理其檔案存取稽核的 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。



- 對於檔案和資料夾的記錄存取，請選取成功和/或失敗嘗試的記錄。如果您未進行選取，則會停用檔案和資料夾的記錄功能。
- 對於記錄檔案共用的存取，請選取成功和/或失敗嘗試的記錄。如果您未進行選取，則會停用檔案共用的記錄功能。
- 針對 [選擇稽核事件記錄目的地]，選擇 [CloudWatch 記錄檔] 或 [Firehose]。然後選擇現有的記錄或傳送串流，或建立新的記錄檔或傳送串流。

6. 選擇儲存。

變更檔案存取稽核組態 (CLI)

- 使用 update-file-systemCLI 命令或等效的 UpdateFileSystemAPI 作業。

```
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"}'
```

用戶會話和打開文件

您可以使用共用資料夾工具來監視連線的使用者工作階段，並在 FSx for Windows 檔案伺服器檔案系統上開啟檔案。共用資料夾工具提供一個集中位置，可以監控連線到檔案系統的使用者，以及開啟的檔案以及由誰開啟的檔案。您可以使用此工具執行以下操作：

- 恢復對鎖定文件的訪問權限。
- 中斷使用者工作階段的連線，這會關閉該使用者開啟的所有檔案。

您可以使用視窗原生共用資料夾 GUI 工具和 Amazon FSx CLI 進行遠端管理，以管理使 PowerShell 用者工作階段和開啟 FSx for Windows File Server 系統的檔案。

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。

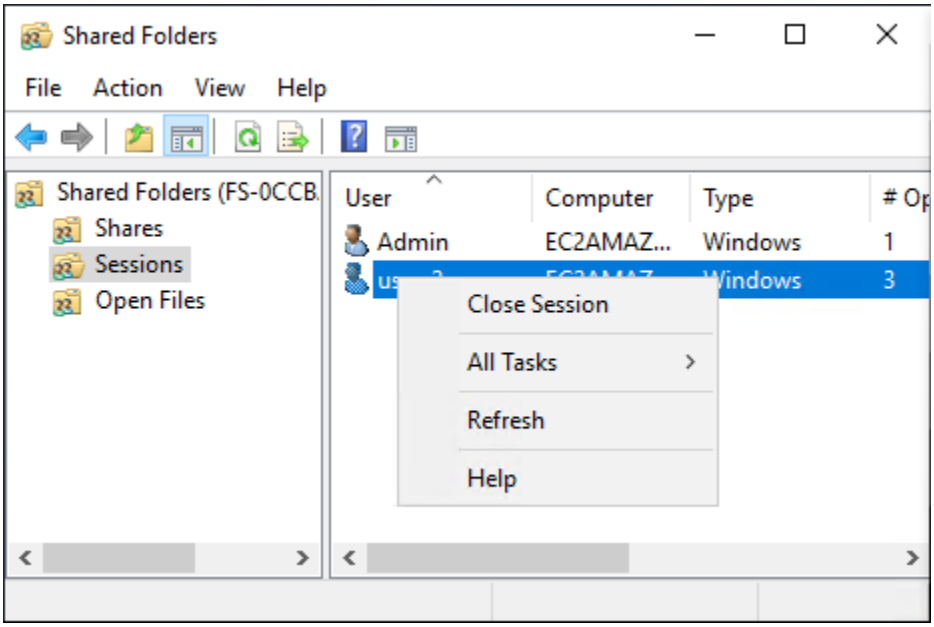
若要啟動共用資料夾工具

1. 啟動您的 Amazon EC2 實例，並將其連接到您的 Amazon FSx 文件系統加入的 Microsoft 活動目錄。若要執行此操作，請從《AWS Directory Service 管理指南》中選擇下列其中一個程序：
   - 無縫加入執行個體
   - 手動聯結視窗執行個體
2. 以身為檔案系統管理員群組成員的使用者身分 Connect 至執行個體。在 AWS 受管理的 Microsoft 活動目錄中，這個群組稱為 AWS 委派的 FSx 系統管理員。在您自我管理的 Microsoft Active Directory 中，此群組稱為網域系統管理員，或是您在建立期間所提供之系統管理員群組的自訂名稱。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的連線到 Windows 執行個體。
3. 打開開始菜單並使用運行 fsmg mt.msc。`Run As Administrator`這麼做會開啟共用資料夾 GUI 工具。
4. 針對「動作」，選擇「Connect 到另一台電腦」

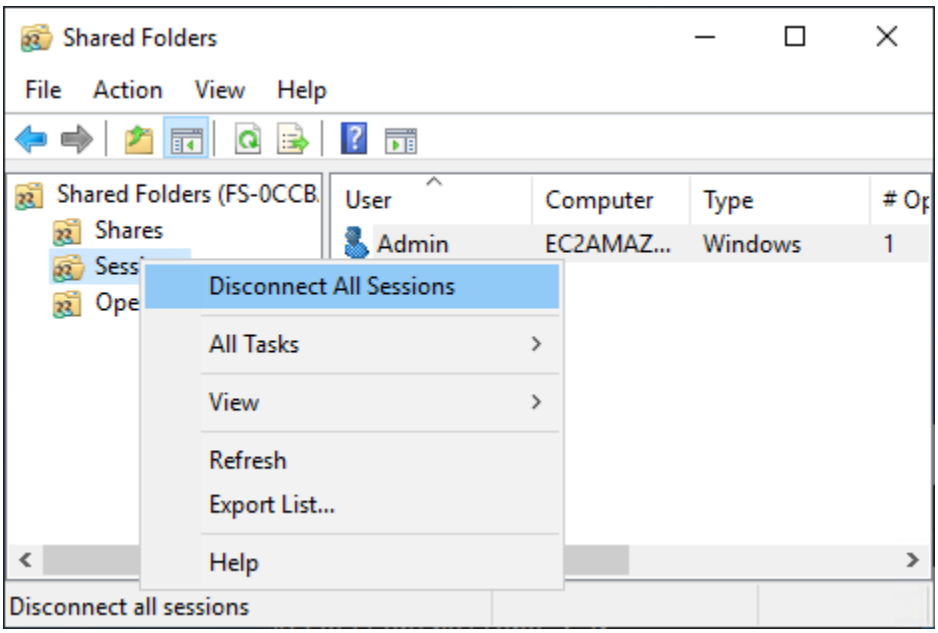
5. 例如fs-*01234567890123456*7.*ad-domain*.com，如果是其他電腦，請輸入 Amazon FSx 檔案系統的 DNS 名稱。
6. 選擇確定。然後，Amazon FSx 檔案系統的項目會顯示在共用資料夾工具的清單中。

若要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 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用，此嵌入式管理單元會顯示他們的工作階段。您可以開啟階段作業的前後關聯 (按一下滑鼠右鍵) 功能表，並選擇「關閉工作階段」來中斷

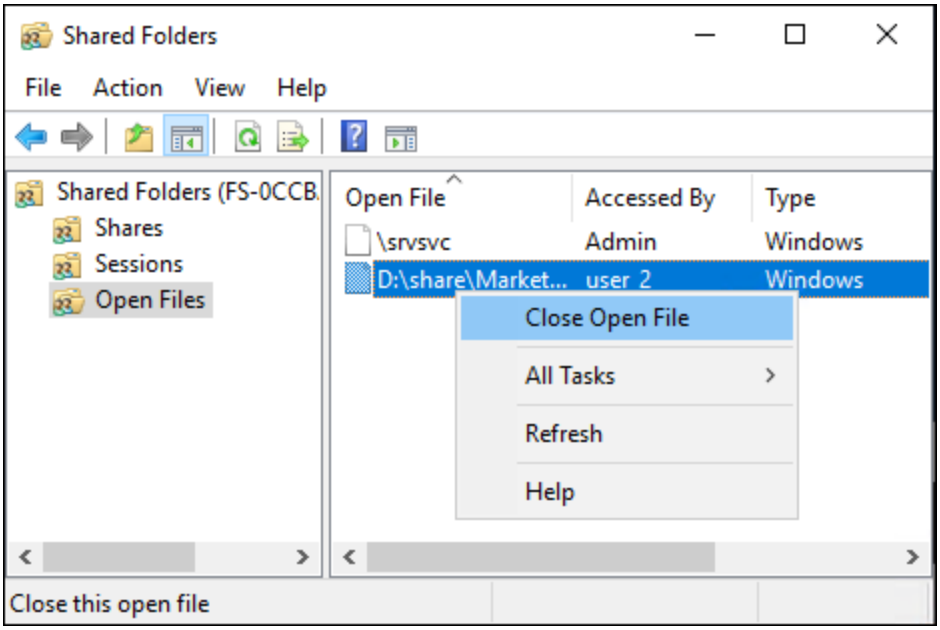


若要中斷所有開啟的工作階段，請開啟工作階段的內容 (按一下滑鼠右鍵) 功能表，選擇「中斷所有工作階段」的連線，

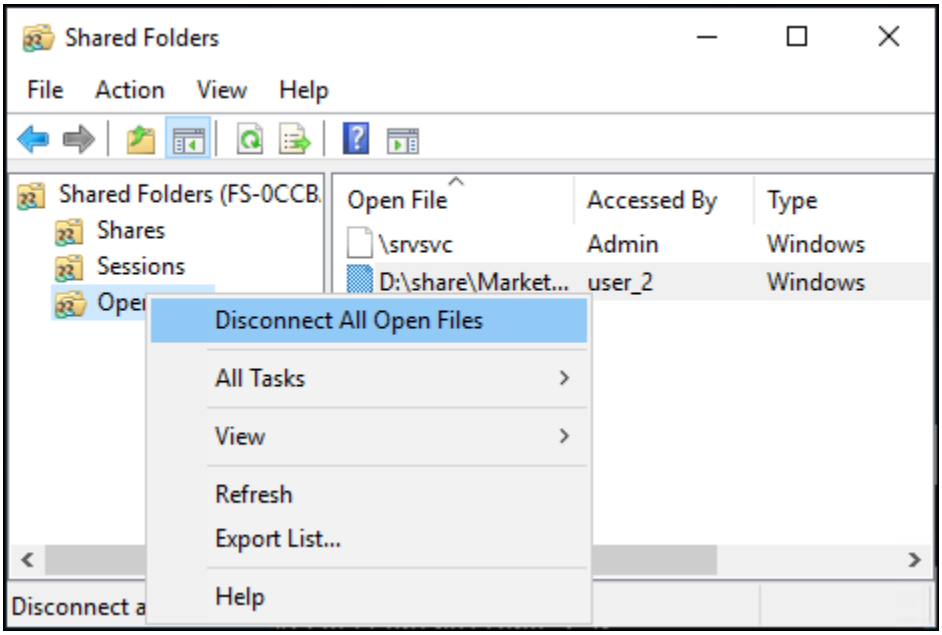


若要管理開啟的檔案 (GUI)

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。此檢視也會顯示開啟檔案或資料夾的使用者。此資訊有助於追蹤其他使用者無法開啟某些檔案的原因。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」，即可關閉任何使用者已開啟的任何檔案。



若要斷開檔案系統上所有開啟的檔案，請使用「開啟檔案」的內容 (按一下滑鼠右鍵) 功能表，然後選擇「中斷所有開啟的檔案」，並確認您的



用 PowerShell 於管理使用者工作階段和開啟檔案

您可以使用 Amazon FSx CLI 來管理作用中使用者工作階段，並在檔案系統上開啟檔案，進行遠端管理。 PowerShell若要瞭解如何使用此 CLI，請參閱使用 Amazon FSx CLI PowerShell。

以下是您可以使用用戶會話和打開文件管理命令。

Command	描述
Get-FSxSmbSession	擷取目前在檔案系統與相關用戶端之間建立之伺服器訊息區 (SMB) 工作階段的相關資訊。
Close-FSxSmbSession	結束 SMB 工作階段。
Get-FSxSmbOpenFile	擷取為連線至檔案系統的用戶端開啟的檔案相關資訊。
Close-FSxSmbOpenFile	關閉為 SMB 伺服器的其中一個用戶端開啟的檔案。

每個指令的線上說明提供了所有指令選項的參考。若要存取此說明，請使用執行指令-?，例如Get-FSxSmbSession -?。

重复数据删除

FSx 支援使用 Microsoft 重複資料刪除功能來識別和消除多餘的資料。大型資料集通常具有冗餘資料，這會增加資料儲存成本。例如，使用者檔案共用時，多個使用者可以儲存同一個檔案的多個副本或版本。使用軟體開發共用時，許多二進位檔案會在建置之間維持不變。

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。重複資料刪除功能只儲存一次資料集的重複部分，可減少或消除多餘的資料。使用重複資料刪除功能時，預設會啟用資料壓縮，藉由在重複資料刪除後壓縮資料，進一步減少資料儲存量。重複資料刪除作為背景程序執行，會持續且自動地掃描和最佳化您的檔案系統，而且對您的使用者和連線的用戶端來說是透明的。

重複資料刪除可節省的儲存空間取決於資料集的性質，包括檔案之間存在多少重複資料。一般用途檔案共用的典型平均節省 50% 至 60%。在共用範圍內，使用者文件可節省 30% 到 50% 的成本，到軟體開發資料集的 70—80% 不等。您可以使用下述`Measure-FSxDedupFileMetadata`指令測量可能節省的重複資料刪除功能。

您也可以自訂重複資料刪除功能，以滿足您的特定儲存需求。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，也可以建立自訂作業排程。由於重複資料刪除工作會消耗檔案伺服器資源，因此建議您使用下`Get-FSxDedupStatus`列指令來監控重複資料刪除工作的狀態。

如需有關重複資料刪除的詳細資訊，請參閱 Microsoft 了解重複資料刪除說明文件。

> **Note**
>
> 請參閱我們的最佳做法使用重複資料刪除的最佳做法。如果您在成功執行重複資料刪除工作時遇到問題，請參閱重複資料刪除故障診。

> **Warning**
>
> 不建議使用重複資料刪除功能來執行某些 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 重複資料刪除互通性說明文件。

使用重複資料刪除的最佳做法

以下是使用重複資料刪除的一些最佳作法：

- 排定在檔案系統閒置時執行重複資料刪除工作：預設排程包括星期六 UTC 2:45 的每週`GarbageCollection`工作。如果您的檔案系統有大量資料流失，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，請將此工作排定在預期檔案系統流量較低的時間執行。
- 設定足夠的輸送量容量以完成重複資料刪除：較高的輸送量容量可提供更高層級的記憶體。Microsoft 建議每 1 TB 的邏輯資料有 1 GB 的記憶體，以執行重複資料刪除功能。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滿足您的資料大小。
- 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：您可以限制最佳化在特定檔案類型或資料夾上執行，或設定最小檔案大小和保留時間以進行最佳化。如需進一步了解，請參閱重複数据删除。

管理重複資料刪除

您可以使用 Amazon FSx CLI 管理檔案系統上的重複資料刪除功能，進行遠端管理。 PowerShell若要瞭解如何使用此 CLI，請參閱使用 Amazon FSx CLI PowerShell。

以下是您可以使用重複數據刪除命令。

重複資料刪除指令	描述
Enable-FSxDedup	啟用檔案共用上的重複資料刪除功能。當您啟用重複資料刪除功能時，預設會啟用重複資料刪除後的資料壓縮。
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，包括最佳化的檔案大小和保留天數下限、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，包括最佳化的檔案大小和保留天數下限、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，描述檔案系統上最後一個工作的最佳化節省和狀態、時間和完成狀態。
Get-FSxDedupMetadata	擷取重複資料刪除最佳化中繼
Update-FSxDedupStatus	計算並擷取更新的重複資料刪除節省資訊。

重複資料刪除指令	描述
Measure-FSxDedupFileMetadata	如果您刪除資料夾群組，測量並擷取可在檔案系統上回收的潛在儲存空間。檔案通常具有在其他資料夾之間共用的區塊，而重複資料刪除引擎會計算哪些區塊是唯一且會被刪除的。
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。
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排入佇列的重複資料刪除工作的狀態和資訊。
Stop-FSxDedupJob	取消一或多個指定的重複資料刪除工作。

每個指令的線上說明提供了所有指令選項的參考。若要存取此說明，請使用執行指令-?，例如Enable-FSxDedup -?。

啟用重複資料刪除

您可以使用`Enable-FSxDedup`命令在 Amazon FSx 適用於 Windows 檔案伺服器的檔案共用上啟用重複資料刪除功能，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功能時，會建立預設排程和組態。您可以使用下列指令建立、修改及移除排程和組態。

您可以使用該`Disable-FSxDedup`命令完全禁用文件系統上的重複數據刪除。

建立重複資料刪除排程

即使預設排程在大多數情況下運作良好，您也可以使用`New-FsxDedupSchedule`指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
}
```

此命令會建立一個名為的排程，CustomOptimization該排程會在星期一、星期三和星期六的日子執行，並在每天上午 8:00 (UTC) 開始工作，最長持續時間為 7 小時，如果工作仍在執行，則工作會停止。

請注意，建立新的自訂重複資料刪除工作排程並不會覆寫或移除現有的預設排程。在建立自訂重複資料刪除工作之前，如果不需要預設工作，您可能會想要停用該工作。

您可以使用Set-FsxDedupSchedule指令停用預設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
 “BackgroundOptimization” -Enabled $false}
```

您可以使用Remove-FSxDedupSchedule -Name "ScheduleName"指令移除重複資料刪除排程。請注意，預設的BackgroundOptimization重複資料刪除排程無法修改或移除，必須改為停用。

修改重複資料刪除排程

您可以使用Set-FsxDedupSchedule指令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，以便在星期一至星期三和星期六的日子執行，在每天上午 9:00 (UTC) 開始工作，最長持續時間為 9 小時，如果工作仍在執行，則工作會停止。

若要在最佳化設定之前修改檔案保留時間下限，請使用Set-FSxDedupConfiguration指令。

檢視節省的空間量

若要檢視執行重複資料刪除所節省的磁碟空間量，請使用Get-FSxDedupStatus指令，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**
>
> 下列參數的指令回應中顯示的值不可靠，因此您不應使用下列值：容量 FreeSpace UsedSpace、 UnoptimizedSize、、和 SavingsRate。

重複資料刪除故障診

造成重複資料刪除問題的潛在原因有許多，如下節所述。

主題

- 重複資料刪除不起作用
- 重複資料刪除值意外設定為 0
- 刪除文件後，文件系統上的空間不會釋放

重複資料刪除不起作用

使用我們的重複資料刪除文件中的指示，執行`Get-FSxDedupStatus`命令以檢視最近重複資料刪除工作的完成狀態。如果一個或多個工作失敗，您可能看不到檔案系統上的可用儲存容量增加。

重複資料刪除工作失敗的最常見原因是記憶體不足。

- Microsoft 建議以最佳方式為每 1 TB 的邏輯資料擁有 1 GB 的記憶體 (或每 1 TB 的邏輯資料至少 300 MB + 50 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滿足您的資料大小。
- 重複資料刪除工作設定為 Windows 建議的預設值 25% 記憶體配置，也就是說，對於具有 32 GB 記憶體的檔案系統，可以使用 8 GB 進行重複資料刪除。記憶體配置是可設定的 (使用具有參數的`Set-FSxDedupSchedule`命令`-Memory`)，但消耗額外的記憶體可能會影響檔案系統的效能。

- 您可以修改重複資料刪除工作的組態，進一步降低記憶體需求。例如，您可以限制最佳化在特定檔案類型或資料夾上執行，或設定最小檔案大小和保留時間以進行最佳化。我們也建議您將重複資料刪除工作設定為在檔案系統負載最低的閒置期間執行。

如果重複資料刪除工作沒有足夠的時間完成，您也可能會看到錯誤。您可能需要變更工作的最長持續時間，如中所述修改重複資料刪除排程。

如果重複資料刪除工作長時間失敗，並且在此期間檔案系統上的資料發生了變更，後續的重複資料刪除工作可能需要更多資源才能成功完成第一次。

重複資料刪除值意外設定為 0

對於已設定重複資料刪除功能的檔案系統而言，SavedSpace和OptimizedFilesSavingsRate的值非預期為 0。

當您增加檔案系統的儲存容量時，可能會在儲存最佳化程序期間發生這種情況。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，這會將資料從舊磁碟移轉到新的較大磁碟。儲存最佳化任務完成後，Amazon FSx 會在檔案系統上恢復重複資料刪除。如需有關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。

刪除文件後，文件系統上的空間不會釋放

重複資料刪除的預期行為是，如果刪除的資料是 dedup 節省了空間，那麼在執行記憶體回收工作之前，實際上並不會釋放檔案系統上的空間。

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之後立即執行記憶體回收工作。記憶體回收工作完成之後，您可以將資源回收排程設定回其原始設定。這樣可確保您可以立即快速查看刪除中的空間。

使用下列程序將資源回收工作設定為在 5 分鐘內執行。

1. 若要確認已啟用重複資料刪除功能，請使用指Get-FSxDedupStatus令。如需指令及其預期輸出的詳細資訊，請參閱檢視節省的空間量。
2. 使用下列指令設定從現在起 5 分鐘執行資源回收工作的排程。

```
$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. 執行資源回收工作並釋放空間之後，請將排程設回其原始設定。

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空間量。設定配額後，您可以追蹤配額狀態以監控使用情況，並查看使用者何時超過其配額。

您也可以阻止達到配額的使用者寫入儲存空間，以強制執行配額。當您強制執行配額時，超出其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值設定下列臨界值：

- 警告-用於追蹤使用者或群組是否接近其配額限制，僅適用於追蹤。
- 限制-使用者或群組的儲存配額限制。

您可以設定預設配額，這些配額會套用至存取檔案系統的新使用者，以及套用至特定使用者或群組的配額。您也可以檢視每個使用者或群組使用多少儲存空間，以及他們是否超過其配額的報告。

系統會根據檔案擁有權追蹤使用者層級的儲存耗用量。儲存空間消耗是使用邏輯檔案大小計算的，而不是檔案佔用的實際實體儲存空間。在將資料寫入檔案時，會追蹤使用者儲存配額。

更新多個使用者的配額需要為每位使用者執行一次 update 命令，或將使用者組織到一個群組中，然後更新該群組的配額。

管理使用者儲存配額

您可以使用 Amazon FSx CLI 在上進行遠端管理，管理檔案系統上 PowerShell的使用者儲存配額。若要瞭解如何使用此 CLI，請參閱使用 Amazon FSx CLI PowerShell。

以下是可用來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，或同時執行兩者。
Disable-FSxUserQuotas	停止追蹤和強制執行使用者儲存配額。

使用者儲存配額命令	描述
Get-FSxUserQuotaSettings	擷取檔案系統目前的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。配額值以字節為單位指定。

每個指令的線上說明提供了所有指令選項的參考。若要存取此說明，請使用執行指令-?，例如Enable-FSxUserQuotas -?。

管理傳輸中的加密

您可以使用一組自訂 PowerShell 指令來控制 FSx for Windows 檔案伺服器檔案系統與用戶端之間傳輸中資料的加密。您可以將檔案系統存取限制為只有支援 SMB 加密的用戶端，以 data-in-transit 便永遠加密。為加密開啟強制執行時 data-in-transit，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而非檔案伺服器層級的加密。 data-in-transit 如果您想對某些具有敏感資料的檔案共用強制執行傳輸中加密，並允許所有使用者存取其他檔案共用，則可以使用檔案共用層級的加密控制，在同一個檔案系統上混合使用加密和未加密的檔案共用。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，您無法選擇性地停用某些共用的加密。

您可以使用 Amazon FSx CLI 在上進行遠端管理，在檔案系統上管理使用者傳輸中加密。 PowerShell 若要瞭解如何使用此 CLI，請參閱使用 Amazon FSx CLI PowerShell。

以下是可用來管理檔案系統上使用者傳輸中加密的指令。

傳輸中加密命令	描述
Get-FSxSmbServerConfiguration	擷取伺服器訊息區 (SMB) 伺服器組態。
Set-FSxSmbServerConfiguration	此指令有兩個設定傳輸中加密的選項： • `-EncryptData $True\|$False` — 將此參數設定為`True`以開啟傳輸中資料加密。將此參數設定`False`為可關閉傳輸中資料加密。

傳輸中加密命令	描述
	• `-RejectUnencryptedAccess $True\|$False` — 將此參數設定`True`為可禁止不支援加密的用戶端存取檔案系統。將此參數設定`False`為允許不支援加密的用戶端存取檔案系統。

每個指令的線上說明提供了所有指令選項的參考。若要存取此說明，請使用執行指令-?，例如Get-FSxSmbServerConfiguration -?。

管理儲存區組態

檔案系統的儲存配置包括儲存容量、儲存類型和 SSD IOPS。您可以在檔案系統建立期間和之後，設定這些資源和輸送量容量，以達到工作負載所需的效能等級。如需詳細資訊，請參閱下列主題。

主題

- 管理儲存容量
- 管理儲存區類型
- 管理固態硬碟 IOPS

管理儲存容量

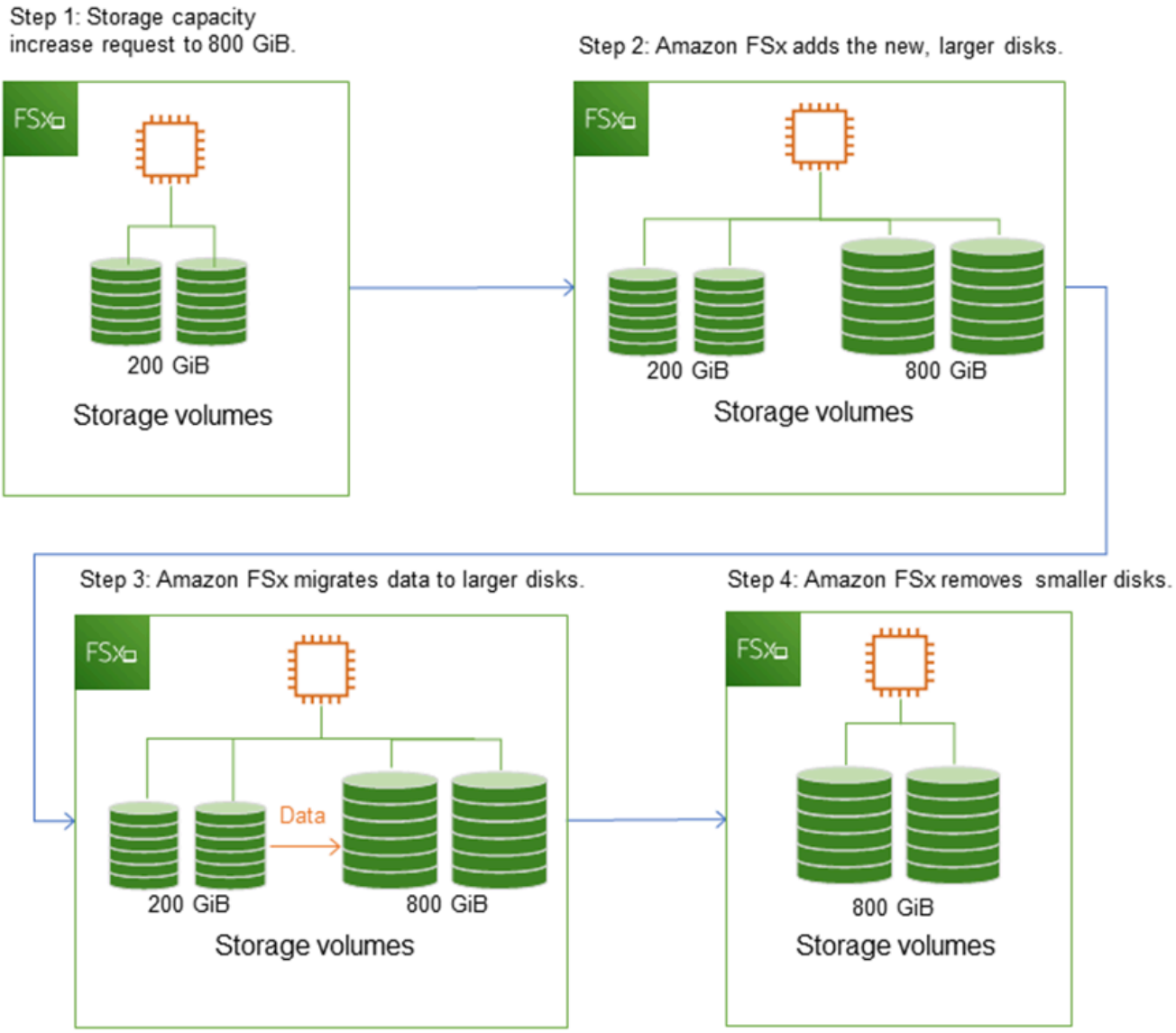
您可以視需要增加 FSx for Windows File Server 案系統的儲存容量。您可以使用亞馬遜 FSx 主控台、亞馬遜 FSx API 或 AWS Command Line Interface () AWS CLI 來執行此操作。您只能增加檔案系統的儲存容量；您無法減少儲存容量。

> **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，或是從屬於 2019 年 6 月 23 日之前建立之檔案系統的備份還原的檔案系統。

當您增加 Amazon FSx 檔案系統的儲存容量時，Amazon FSx 會在幕後向檔案系統新增一組更大的新磁碟。然後，Amazon FSx 會在背景執行儲存優化程序，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幾個小時到幾天的時間，對工作負載效能的明顯影響最小。在此最佳化期間，備份使用率會暫時提高，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地從備份擷取和還原。在備份歷史記錄中不再包含舊的

儲存磁碟區之後，備份使用量會回復到先前的基準層級。當新的儲存容量可用時，您只需支付新儲存容量的費用。

下圖顯示 Amazon FSx 在增加檔案系統儲存容量時所使用的四個主要程序步驟。



您可以隨時使用 Amazon FSx 主控台、CLI 或 API 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。

主題

增加儲存容量時要知道的重點

以下是增加儲存容量時需要考慮的幾個重要事項：

- 僅增加 — 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 — 每次增加的儲存容量必須至少為檔案系統目前儲存容量的 10%，最高可達 65,536 GiB 的最大允許值。
- 最小輸送量容量 — 若要增加儲存容量，檔案系統的最小輸送量容量必須為 16 MB/s。這是因為儲存最佳化步驟是輸送量密集的程序。
- 增加間隔時間 — 您無法在要求上次增加 6 小時後或儲存最佳化程序完成 (以較長的時間為準) 之前，在檔案系統上進一步增加儲存容量。儲存最佳化可能需要幾個小時到幾天才能完成。為了最大限度地減少完成儲存最佳化所需的時間，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 (儲存擴展完成後，輸送量容量可以縮減)，並在檔案系統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：
> 儲存容量擴充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，請參閱效能警告與建議。

何時增加儲存容量

當檔案系統的可用儲存容量不足時，請增加檔案系統的儲存容量。使用此`FreeStorageCapacity` CloudWatch 測量結果來監督檔案系統上可用的可用儲存空間量。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 監控指標 CloudWatch。

我們建議您始終在檔案系統上維持至少 10% 的可用儲存容量。使用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臨界值時，您可以自動增加檔案系統的儲存容量。使用AWS開發的自訂AWS CloudFormation範本，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。

增加儲存容量並提高檔案系統效能

大多數工作負載在新的儲存容量可用之後，Amazon FSx 會在背景執行儲存優化程序時，對效能的影響最小。具有大量使用中資料集的寫入量應用程式可能會暫時降低高達一半的寫入效能。在這些情況下，您可以先增加檔案系統的輸送量容量，然後再增加儲存容量。這可讓您繼續提供相同層級的輸送量，以符合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。

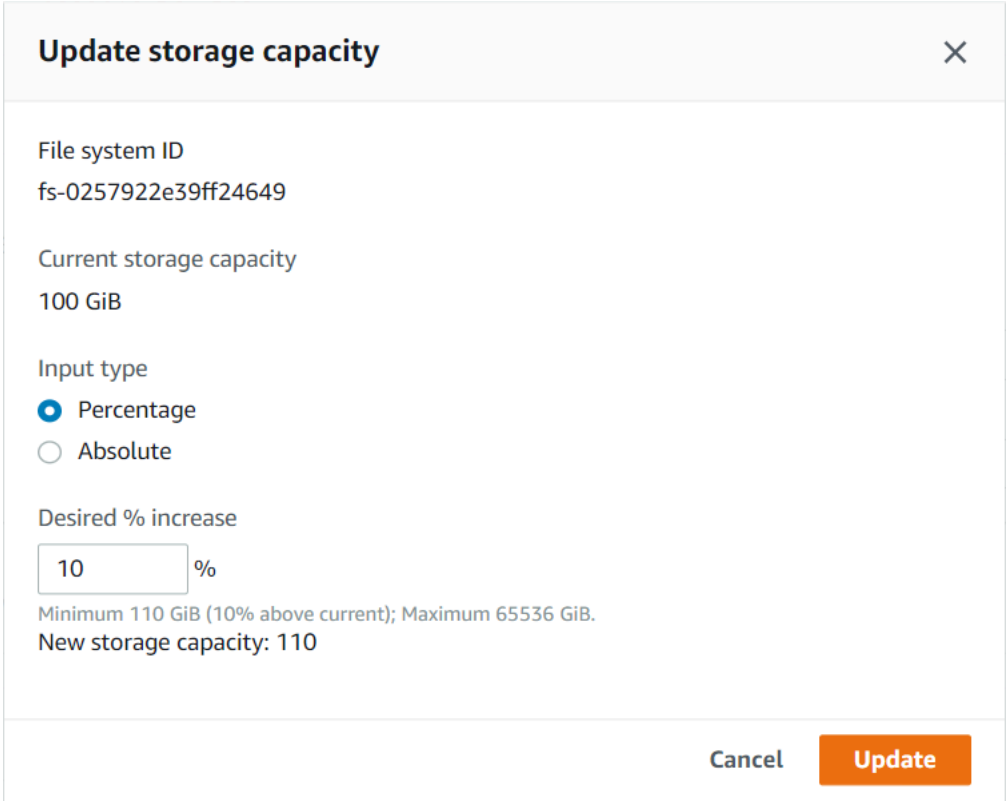
如何增加儲存容量

您可以使用 Amazon FSx 主控台、或 Amazon FSx API 來增加檔案系統的儲存容量。AWS CLI

增加檔案系統 (主控台) 的儲存容量

1. 開啟亞馬遜 FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 瀏覽至 [檔案系統]，然後選擇您要增加儲存容量的 Windows 檔案系統。
3. 針對 [動作]，選擇 [更新儲存區 或者，在「摘要」面板中，選擇檔案系統儲存容量旁邊的「更新」。

   [更新儲存容量] 視窗隨即出現。



4. 在 [輸入類型] 中，選擇 [百分比] 以從目前值變更的百分比輸入新儲存容量，或選擇 [絕對] 以在 GiB 中輸入新值。
5. 輸入所需的儲存容量。

> **Note**
>
> 所需容量值必須至少比目前值大 10%，最大值為 65,536 GiB。

6. 選擇 [更新] 以啟動儲存容量更新。
7. 您可以在 [檔案系統詳細資料] 頁面的 [更新] 索引標籤中監視更新進度。

增加檔案系統 (CLI) 的儲存容量

若要增加 Windows 檔案伺服器檔案系統 FSx 的儲存容量，請使用指AWS CLI令update-file-system。設定下列參數：

- `--file-system-id`到您正在更新的文件系統的 ID。
- `--storage-capacity`至少比目前值大 10% 的值。

您可以使用AWS CLI指令監視更新進度describe-file-systems。在輸出administrative-actions中尋找。

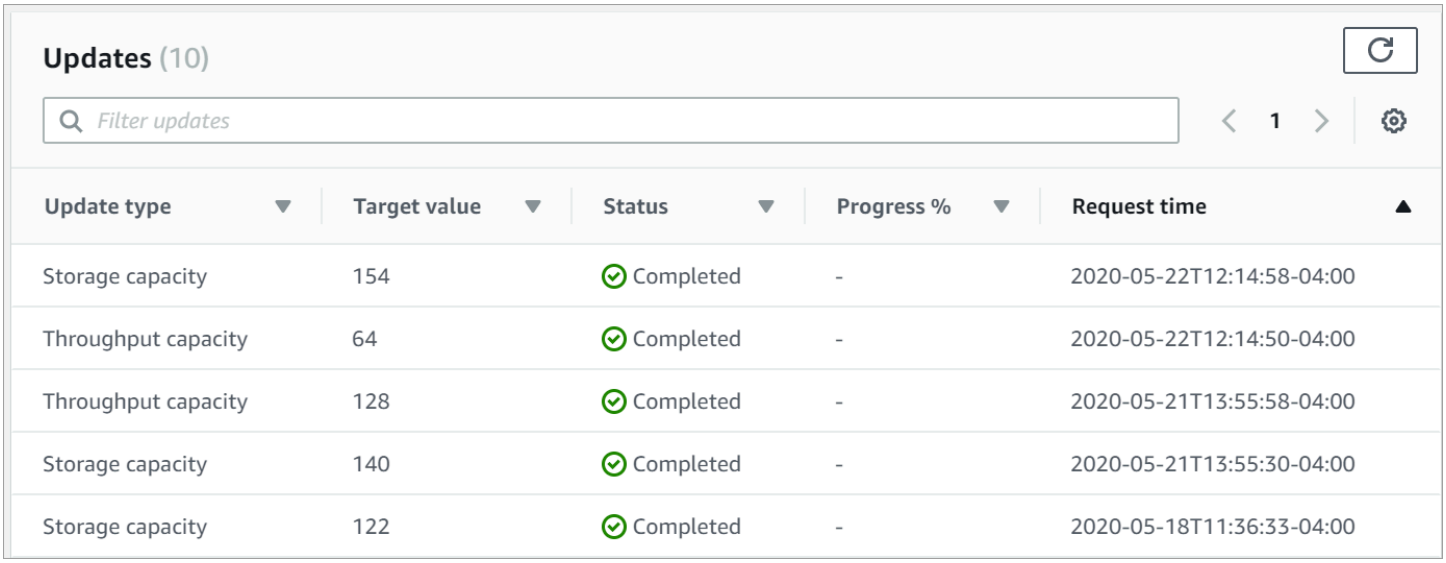
如需詳細資訊，請參閱AdministrativeAction。

監控儲存容量增加

您可以使用 Amazon FSx 主控台、API 或. AWS CLI

控制台中的監控增加

在 [檔案系統詳細資料] 視窗的 [更新] 索引標籤中，您可以檢視每種更新類型的 10 個最新更新。



對於儲存容量更新，您可以檢視下列資訊。

更新類型

可能的值為「儲存容量」。

目標值

將檔案系統的儲存容量更新為所需的值。

狀態

更新的目前狀態。對於儲存容量更新，可能的值如下：

- 擱置中 — Amazon FSx 已收到更新要求，但尚未開始處理。
- 進行中 — Amazon FSx 正在處理更新請求。

- 已更新最佳化 — Amazon FSx 增加了檔案系統的儲存容量。儲存最佳化程序現在正在將檔案系統資料移至新的較大磁碟。
- 已完成 — 儲存容量增加成功完成。
- 失敗 — 儲存容量增加失敗。選擇問號 (?) 以查看儲存區更新失敗原因的詳細資訊。

進度%

將儲存最佳化程序的進度顯示為完成百分比。

請求時間

Amazon FSx 收到更新動作要求的時間。

監控會隨著AWS CLI和 API 而增加

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

下列範例顯示 describe-file-systems CLI 命令回應的摘錄。檔案系統的儲存容量為 300 GB，而且有擱置中的系統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，並將新的較大儲存磁碟新增至檔案系統。檔案系統可使用新儲存區時，FILE_SYSTEM_UPDATE狀態會變更為UPDATED_OPTIMIZING。儲存容量會顯示更大的新值，而 Amazon FSx 則開始處理STORAGE_OPTIMIZATION管理動作。這顯示在下面的 describe-file-systems CLI 命令的響應摘錄中。

ProgressPercent屬性會顯示儲存區最佳化程序的進度。儲存區最佳化程序順利完成後，FILE_SYSTEM_UPDATE動作的狀態會變更為COMPLETED，且STORAGE_OPTIMIZATION動作不再顯示。

```
{
    "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,
                }
            ]
```

如果儲存區容量增加失敗，FILE_SYSTEM_UPDATE動作的狀態會變更為FAILED。FailureDetails屬性提供失敗的相關資訊，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
                }
            ]
```

如需疑難排解失敗動作的資訊，請參閱儲存或輸送量容量更新失敗。

動態增加 Windows 檔案伺服器檔案系統 FSx 的儲存容量

當可用儲存容量低於您指定的定義臨界值時，您可以使用下列解決方案來動態增加 FSx for Windows 檔案伺服器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、根據此閾值的 Amazon CloudWatch 警示，以及增加檔案系統儲存容量的AWS Lambda功能。

解決方案會自動部署所有必要的元件，並採用下列參數：

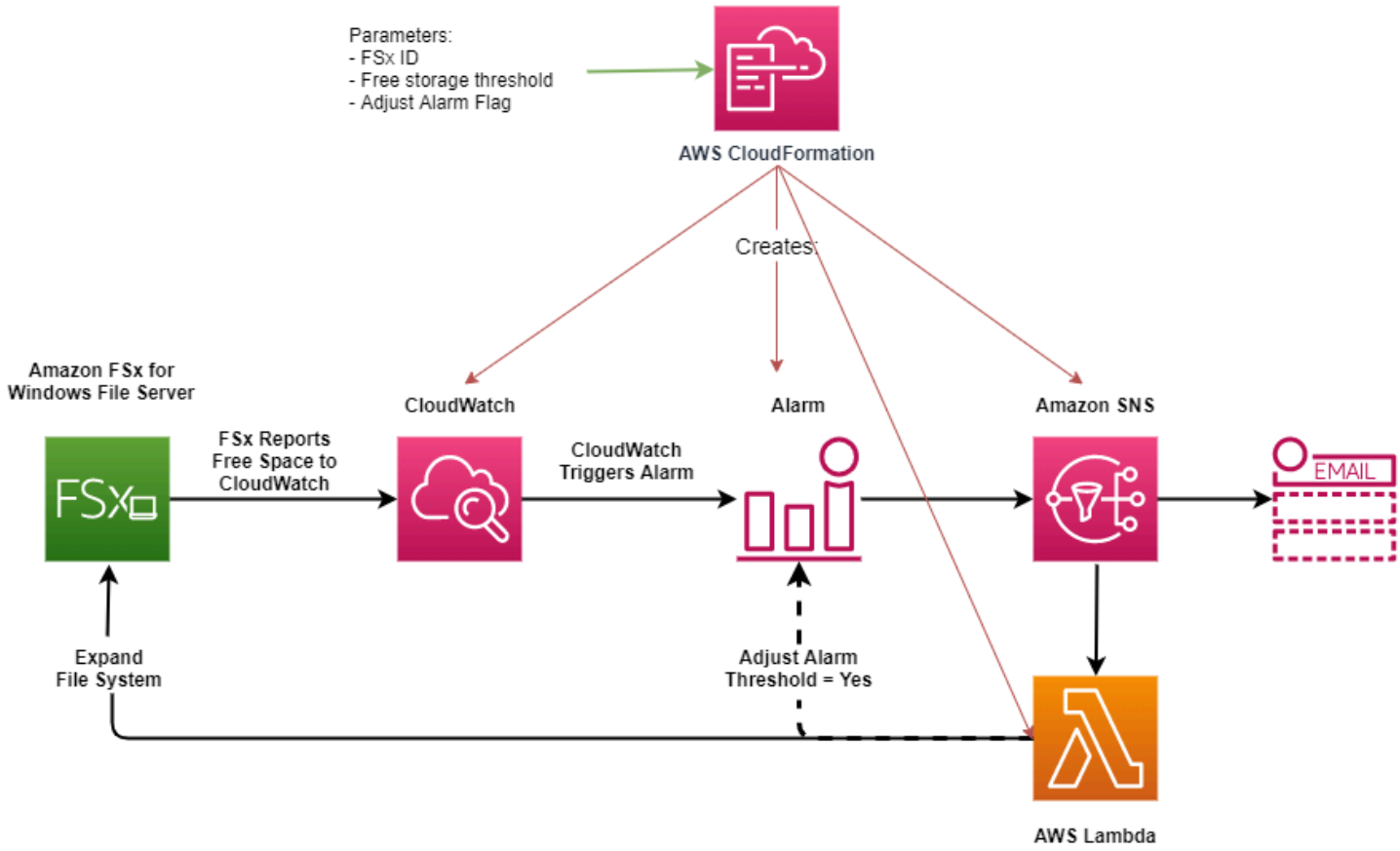
- 檔案系統識別碼
- 可用存儲容量閾值（數值）
- 測量單位（百分比 [預設] 或 GiB）
- 增加儲存容量的百分比 (%)
- SNS 訂閱的電子郵件地址
- 調整警報閾值 (是/否)

主題

- 架構概觀
- AWS CloudFormation 範本
- 自動化部署 AWS 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. AWS CloudFormation範本會部署 CloudWatch 警示、AWS Lambda函數、Amazon Simple Notification Service (Amazon SNS) 佇列，以及所有必要的 AWS Identity and Access Management (IAM) 角色。IAM 角色授予 Lambda 函數呼叫 Amazon FSx API 作業的權限。
2. CloudWatch 當檔案系統的可用儲存容量低於指定閾值時觸發警示，並將訊息傳送至 Amazon SNS 佇列。
3. 然後，解決方案會觸發訂閱此 Amazon SNS 主題的 Lambda 函數。
4. Lambda 函數會根據指定的增加百分比值計算新的檔案系統儲存容量，並設定新的檔案系統儲存容量。

5. Lambda 函數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. Lambda 函數作業的原始 CloudWatch 警示狀態和結果會傳送至 Amazon SNS 佇列。

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

AWS CloudFormation 範本

此解決方案AWS CloudFormation使用自動化部署元件，這些元件用於自動增加 Windows 檔案伺服器檔案系統的 FSx 儲存容量。若要使用此解決方案，請下載 In creaseF 範SxSizeAWS CloudFormation 本。

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

FileSystemId

沒有預設值。您要自動增加儲存容量之檔案系統的 ID。

LowFreeDataStorageCapacityThreshold

沒有預設值。指定初始可用儲存容量臨界值，在此臨界值時觸發警示並自動增加檔案系統的儲存容量 (以 GiB 指定) 或檔案系統目前儲存容量的百分比 (%)。以百分比表示時， CloudFormation 範本會重新計算為 GiB，以符合 CloudWatch 鬧鐘設定。

LowFreeDataStorageCapacityThresholdUnit

預設值為%。指定的單位`LowFreeDataStorageCapacityThreshold`，單位為 GiB 或目前儲存容量的百分比。

AlarmModificationNotification

預設值為 「是」。如果設定為「是」，則初始`LowFreeDataStorageCapacityThreshold`值會與後續警示臨界值的`PercentIncrease`值成比例增加。

例如，當`PercentIncrease`設定為 20 且 AlarmModificationNotification 設定為是時，GiB 中指定的可用空間臨界值 (`LowFreeDataStorageCapacityThreshold`) 會針對後續的儲存容量增加事件增加 20%。

EmailAddress

沒有預設值。指定要用於 SNS 訂閱的電子郵件地址，並接收儲存容量閾值警示。

PercentIncrease

沒有預設值。指定儲存容量的增加量，以目前儲存容量的百分比表示。

自動化部署 AWS CloudFormation

下列程序會設定並部署AWS CloudFormation堆疊，以自動增加適用於 Windows 檔案伺服器檔案系統的 FSx 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AWS服務的費用。如需詳細資訊，請參閱這些服務的定價詳細資料頁面。

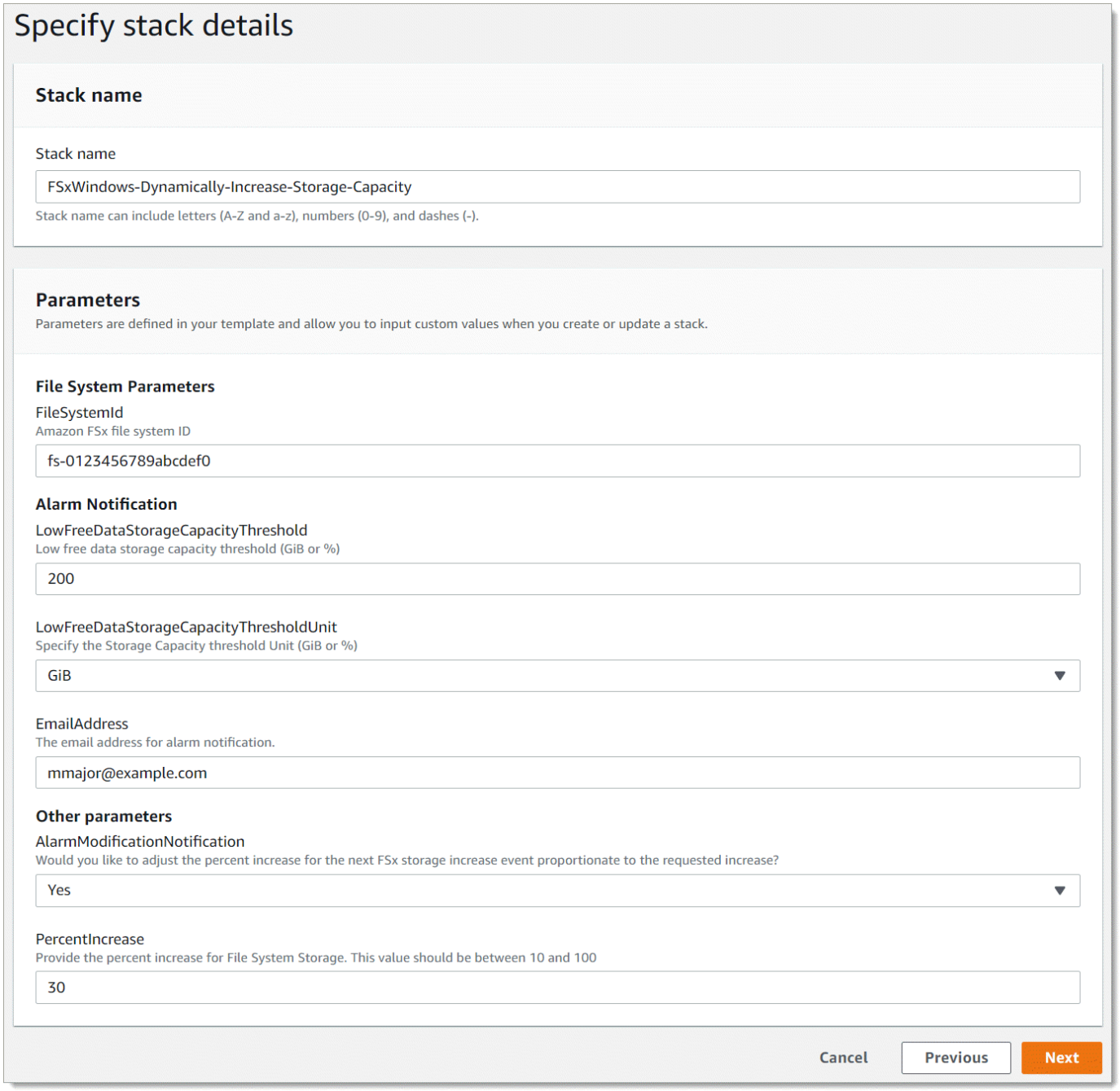
在開始之前，您的帳戶中必須具有在 Amazon 虛擬私有雲 (Amazon VPC) 中執行的 Amazon FSx 檔案系統的識別碼。AWS如需建立 Amazon FSx 資源的詳細資訊，請參閱開始使用適用於 FSx for Windows File Server 的 Amazon FSx。

啟動自動儲存容量增加解決方案堆疊

1. 下載增加模板SxSizeAWS CloudFormation。如需有關建立 CloudFormation 堆疊的詳細資訊，請參閱《使用指南》中的〈在AWS CloudFormation 主控台上建立堆疊AWS CloudFormation〉。

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

2. 在指定堆疊詳細資料中，輸入自動儲存容量增加解決方案的值。



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加以修改。然後選擇 Next (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. 對於「檢閱」，請檢閱並確認解決方案設定。您必須選取確認範本建立 IAM 資源的核取方塊。
7. 選擇建立以部署堆疊。

您可以在 AWS CloudFormation 主控台的狀態欄檢視堆疊的狀態。您應該會在大約 5 分鐘內看到「建立 _ 完成」狀態。

更新堆疊

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

管理儲存區類型

FSx for Windows File Server 提供固態驅動器（SSD）和磁性硬盤驅動器（HDD）存儲類型。SSD 儲存裝置專為效能最高且延遲最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 儲存是專為廣泛的工作負載所設計，包括主目錄、使用者和部門檔案共用，以及內容管理系統。

您可以使用 Amazon FSx 主控台或 Amazon FSx API 將檔案系統儲存類型從硬碟變更為固態硬碟。您無法將檔案系統儲存類型從 SSD 變更為 HDD。請記住，您無法再次更新檔案系統設定，直到要求最後一次更新 6 小時後，或直到儲存最佳化程序完成 (以較長的時間為準)。儲存最佳化可能需要幾個小時到幾天的時間才能完成。若要將這段時間縮到最短，建議您在檔案系統流量最少時更新儲存類型。

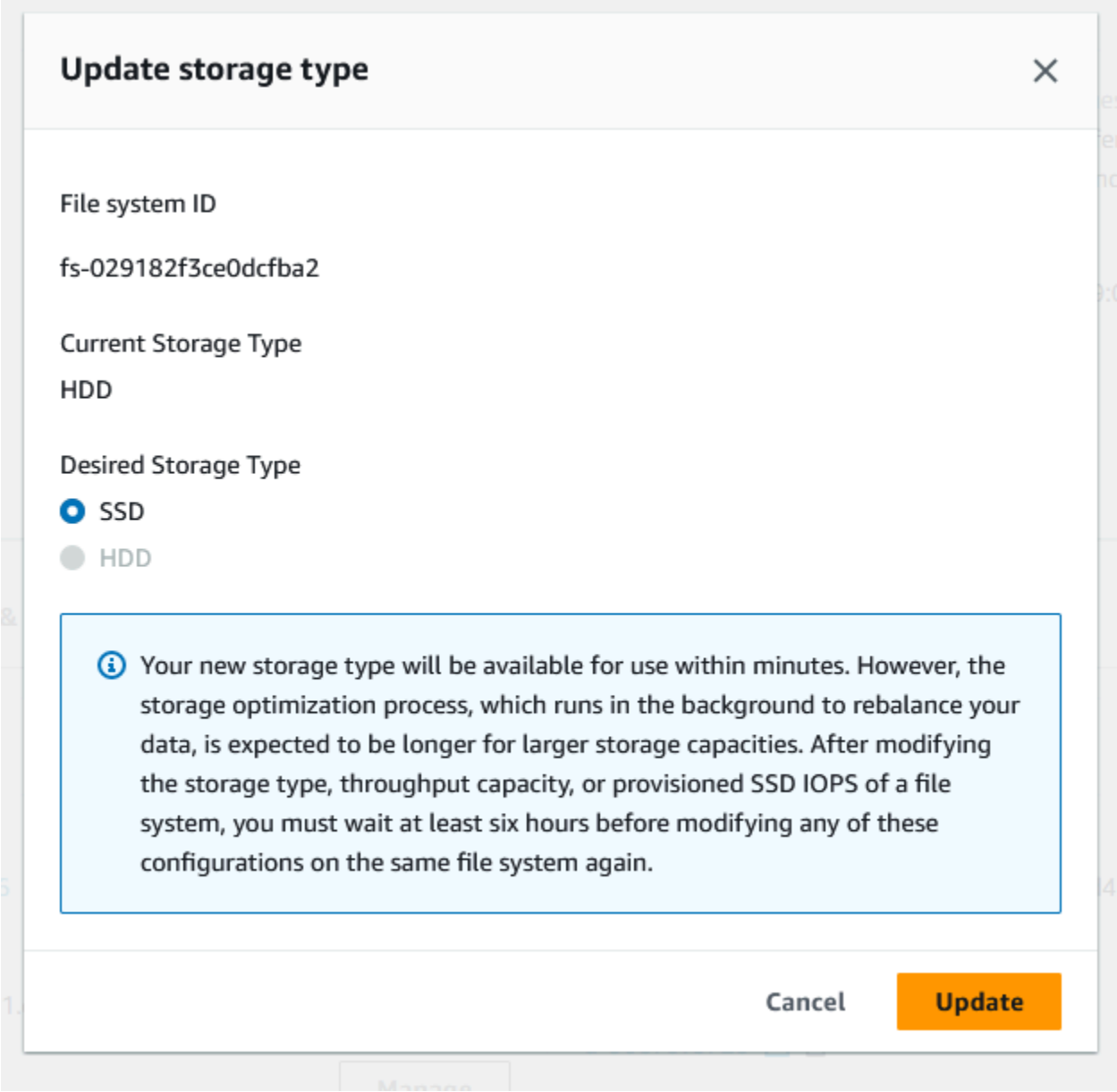
您也可以將檔案系統儲存類型從 HDD 變更為 SSD，方法是還原可用的備份以建立新的檔案系統並選取新的儲存類型。如需詳細資訊，請參閱還原備份。

如何更新儲存空間類型

您可以使用 Amazon FSx 主控台、或 Amazon FSx API 來更新檔案系統的儲存類型。AWS CLI

更新檔案系統 (主控台) 的儲存類型

1. 開啟亞馬遜 FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 瀏覽至 [檔案系統]，然後選擇您要更新其儲存類型的 Windows 檔案系統。
3. 在 [動作] 下，選擇 [更新儲存類型] 或者，在「摘要」面板中，選取 HDD 旁邊的「更新」按鈕。[更新儲存類型] 視窗隨即出現。



4. 針對 [想要的儲存類型] 選擇 [SSD]。選擇 [更新] 以起始儲存區類型更新。
5. 您可以在 [檔案系統詳細資料] 頁面的 [更新] 索引標籤上監視更新進度。

更新檔案系統 (CLI) 的儲存區類型

若要更新 Windows 檔案伺服器檔案系統 FSx 的儲存類型，請使用指AWS CLI令update-file-system。設定下列參數：

- `--file-system-id`到您要更新的文件系統的 ID。
- `--storage-type`到固態硬盤。您無法從 SSD 儲存類型切換為 HDD 儲存類型。

您可以使用AWS CLI指令來監視更新進度describe-file-systems。在輸出`administrative-actions`中尋找。

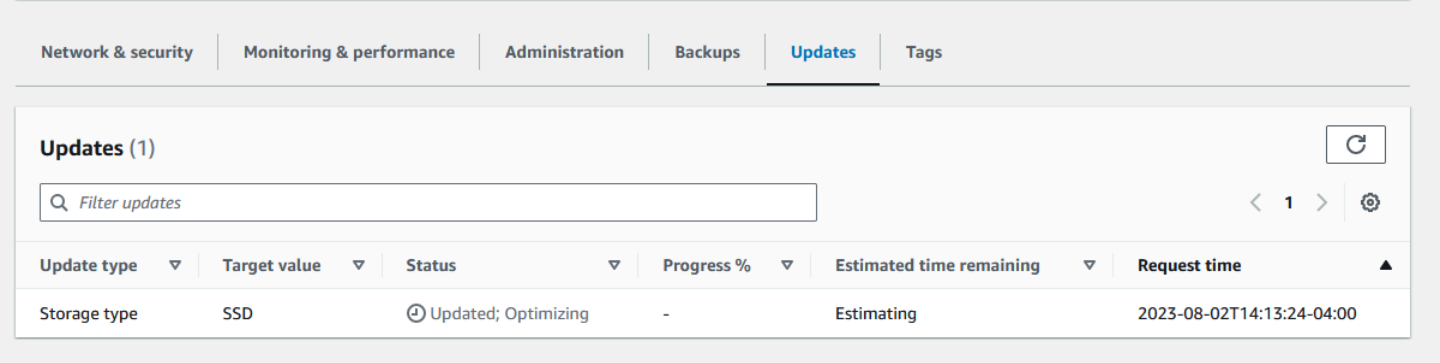
如需詳細資訊，請參閱AdministrativeAction。

監視儲存區類型更新

您可以使用 Amazon FSx 主控台、API 或. AWS CLI

在主控台中監視更新

在 [檔案系統詳細資料] 視窗的 [更新] 索引標籤上，您可以檢視每種更新類型的 10 個最新更新。



對於儲存區類型更新，您可以檢視下列資訊。

更新類型

可能的值為「儲存類型」。

目標值

固態硬

狀態

更新的目前狀態。對於儲存區類型更新，可能的值如下：

- 擱置中 — Amazon FSx 收到更新請求，但尚未開始處理更新請求。
- 進行中 — Amazon FSx 正在處理更新請求。
- 更新最佳化 — SSD 儲存效能可用於工作負載的寫入作業。您的更新會進入更新的最佳化狀態，通常會持續數小時，在此期間，工作負載的讀取作業會在 HDD 和 SSD 之間具有效能等級。更新動作完成後，您的新 SSD 效能即可用於讀取和寫入。
- 已完成 — 儲存類型更新順利完成。
- 失敗 — 儲存區類型更新失敗。選擇問號 (?) 以查看詳細資訊。

進度%

依完成百分比顯示儲存區最佳化程序的進度。

請求時間

Amazon FSx 收到更新動作要求的時間。

使用AWS CLI和 API 監控更新

您可以使用describe-file-systemsAWS CLI命令和 DescribeFileSystemsAPI 動作來檢視和監視檔案系統儲存類型更新要求。`AdministrativeActions`陣列會列出每個管理動作類型的 10 個最新更新動作。當您增加檔案系統的 SSD IOPS 時，會產生`AdministrativeActions`兩個：a `FILE_SYSTEM_UPDATE` 和一個`STORAGE_TYPE_OPTIMIZATION`動作。

管理固態硬碟 IOPS

對於 SSD 儲存磁碟區，您可以獨立於儲存容量來選擇和擴充 IOPS。您可以佈建的最大 SSD IOPS 取決於您為檔案系統選擇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所支援的限制，您可能需要增加輸送量容量，才能支援要求的 SSD IOPS 等級。如需詳細資訊，請參閱 FSx 適用於 FSx for Windows File Server 效能 及 管理輸送量容量。

主題

- 更新固態硬碟 IOPS 時要知道的重點
- 如何更新固態硬碟 IOPS
- 監控佈建的固態硬碟 IOPS 更新

更新固態硬碟 IOPS 時要知道的重點

以下是更新 SSD IOPS 時需要考慮的幾個重要事項：

- 若要為您的檔案系統指定佈建的 SSD IOPS 數量，您必須選擇以下兩種 IOPS 模式之一：
  - 自動 — Amazon FSx 會自動擴展您的固態硬碟 IOPS，以維持每 GiB 的儲存容量 3 個固態硬碟 IOPS，每個檔案系統最高可達 40 萬個固態硬碟 IOPS。
  - 使用者佈建 — 您可以指定介於 96—400,000 個範圍內的固態硬碟 IOPS 數目。針對所有AWS 區域提供 Amazon FSx 的儲存容量，指定每 GiB 3—50 IOPS 之間的數字，或者在美國東部 (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) 的每 GiB 儲存容量 3—500 IOPS 之間。如果固態硬碟 IOPS 數量不至少為每 GiB 3 IOPS，

則要求會失敗。針對較高層級的佈建 SSD IOPS，您需要支付每個檔案系統每 GiB 3 IOPS 以上的平均 IOPS 費用。

- 儲存容量更新 — 如果您增加儲存容量，而新容量需要比使用者佈建的 SSD IOPS 等級更高的 SSD IOPS 等級，Amazon FSx 會自動將您的檔案系統切換為自動模式。
- 輸送量容量更新 — 如果您增加輸送量容量，且新輸送量容量支援的最大 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。
- 間隔時間增加 — 您無法在要求上次增加 6 小時後或儲存最佳化程序完成儲存體最佳化程序完成 (以較長的時間為準)，才能在檔案系統上進一步增加 SSD IOPS、輸送量容量增加或更新儲存類型。儲存最佳化可能需要幾個小時到幾天才能完成。為了盡量減少完成儲存最佳化所需的時間，我們建議您在檔案系統流量最少時調整 SSD IOPS。

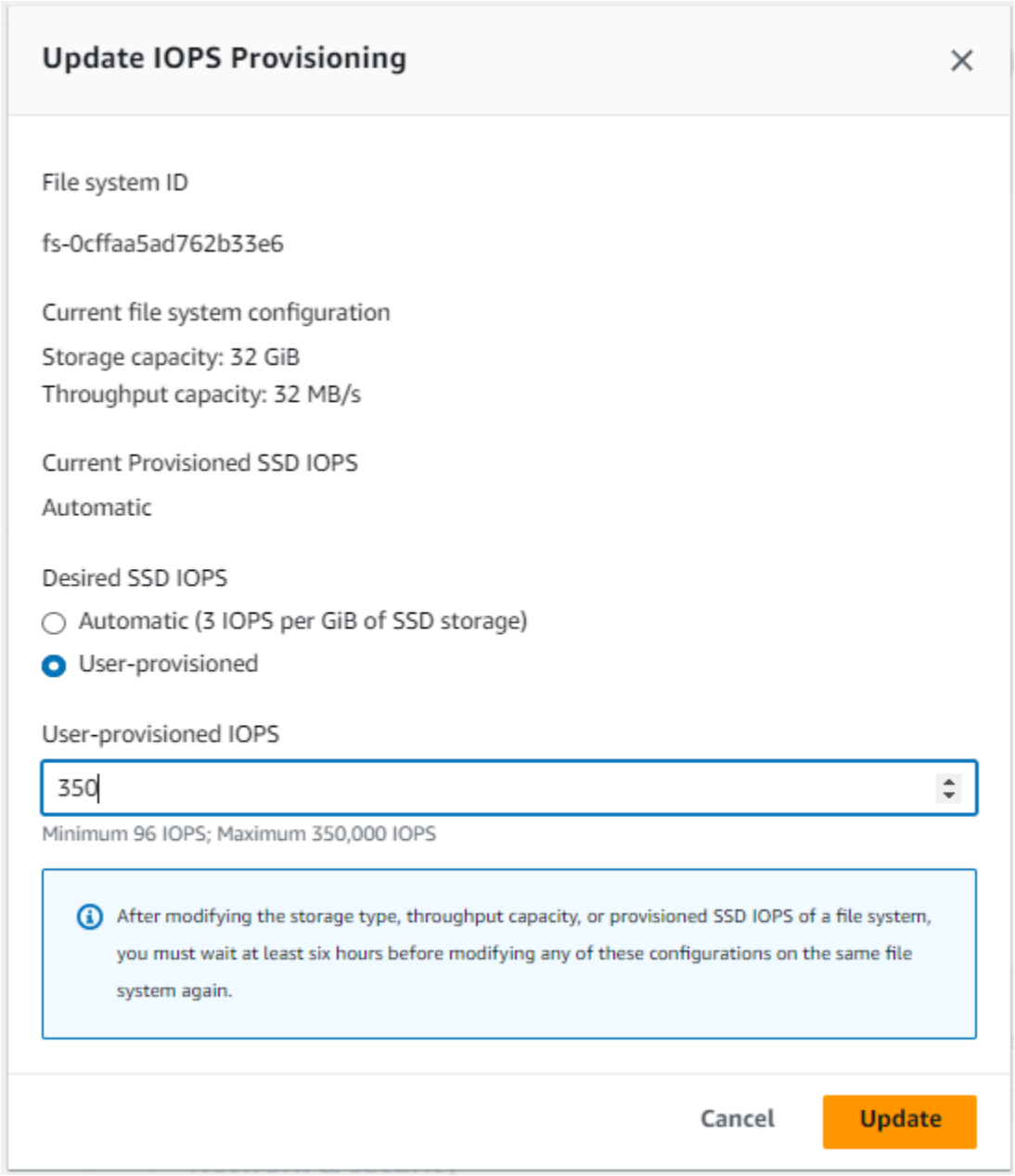
> **Note**
>
> 請注意，僅在下列情況支援 4,608 MBps 及更高的輸送量容量層級AWS 區域：美國東部 (維吉尼亞北部)、美國西部 (奧勒岡)、美國東部 (俄亥俄)、歐洲 (愛爾蘭)、亞太區域 (東京) 和亞太區域 (新加坡)。

如何更新固態硬碟 IOPS

您可以使用 Amazon FSx 主控台、或 Amazon FSx API 為檔案系統更新固態硬碟 IOPS。AWS CLI

更新檔案系統的固態硬碟 IOPS (主控台)

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 瀏覽至檔案系統，然後選擇您要為其更新固態硬碟 IOPS 的 Windows 檔案系統。
3. 在 [動作] 底下，選擇 [更新 SSD IOPS]。或者，在「摘要」面板中，選取佈建 SSD IOPS 旁邊的更新按鈕。更新 IOPS 佈建」視窗隨即開啟。



4. 在模式中，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佈建每 GiB 儲存容量 3 個固態硬碟 IOPS。如果您選擇使用者佈建，請輸入介於 96—400,000 範圍內的任何整數。
5. 選擇 [更新] 以起始佈建的 SSD IOPS 更新。
6. 您可以在 [檔案系統詳細資料] 頁面的 [更新] 索引標籤上監視更新進度。

若要更新檔案系統 (CLI) 的固態硬碟 IOPS

若要更新 FSx 適用於 Windows 檔案伺服器檔案系統的固態硬碟 IOPS，請使用內`--windows-configuration DiskIopsConfiguration`容。此屬性有兩個參數，`Iops`並且`Mode`：

- 如果您要指定固態硬碟 IOPS 的數目，請在支援的AWS區域中使用`Iops=`*`number_of_IOPS`*，最多可使用 400,000 個。`Mode=USER_PROVISIONED`
- 如果您希望 Amazon FSx 自動增加固態硬碟 IOPS，請使用`Mode=AUTOMATIC`且不要使用此`Iops`參數。Amazon FSx 會在您的檔案系統上，每一 GiB 的儲存容量自動維護 3 個固態硬碟 IOPS，在支援的區域中，最多可維護 40 萬個固態硬碟 IOPS。AWS

您可以使用AWS CLI指令來監視更新進度describe-file-systems。在輸出`administrative-actions`中尋找。

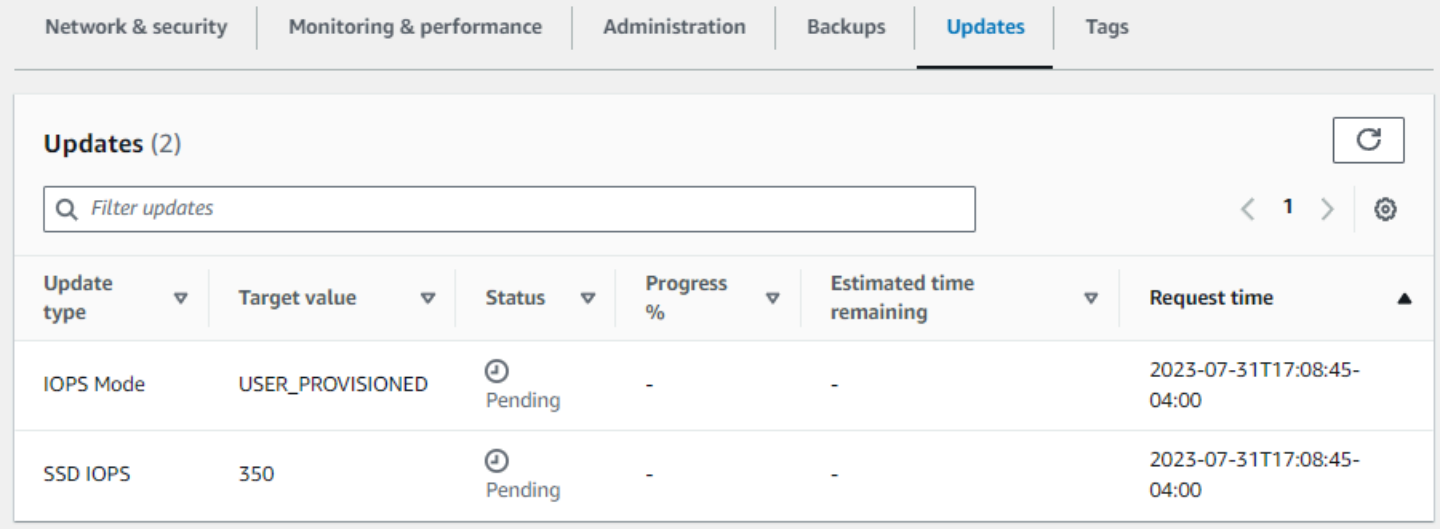
如需詳細資訊，請參閱AdministrativeAction。

監控佈建的固態硬碟 IOPS 更新

您可以使用 Amazon FSx 主控台、API 或. AWS CLI

在主控台中監視更新

在 [檔案系統詳細資料] 視窗的 [更新] 索引標籤中，您可以檢視每種更新類型的 10 個最新更新。



針對佈建的 SSD IOPS 更新，您可以檢視下列資訊。

更新類型

可能的值為 IOPS 模式和固態硬碟 IO PS。

目標值

將檔案系統的 IOPS 模式和 SSD IOPS 更新為所需的值。

狀態

更新的目前狀態。針對固態硬碟 IOPS 更新，可能的值如下：

- 擱置中 — Amazon FSx 已收到更新要求，但尚未開始處理。
- 進行中 — Amazon FSx 正在處理更新請求。
- 更新的最佳化 — 新的 IOPS 層級可用於工作負載的寫入作業。您的更新會進入已更新的最佳化狀態，通常會持續數小時，在此期間，工作負載的讀取作業會在上一層級與新層級之間具有 IOPS 效能。更新動作完成後，您的新 IOPS 層級即可用於讀取和寫入。
- 已完成 — SSD IOPS 更新已順利完成。
- 失敗 — 固態硬碟 IOPS 更新失敗。選擇問號 (?) 以查看儲存區更新失敗原因的詳細資訊。

進度%

將儲存最佳化程序的進度顯示為完成百分比。

請求時間

Amazon FSx 收到更新動作要求的時間。

使用AWS CLI和 API 監控更新

您可以使用describe-file-systemsAWS CLI命令和 DescribeFileSystemsAPI 動作來檢視和監視檔案系統 SSD IOPS 更新要求。`AdministrativeActions`陣列會列出每個管理動作類型的 10 個最新更新動作。當您增加檔案系統的 SSD IOPS 時，會產生`AdministrativeActions`兩個：a `FILE_SYSTEM_UPDATE` 和一個`IOPS_OPTIMIZATION`動作。

管理輸送量容量

每個 Windows 檔案伺服器檔案系統的 FSx 都具有在您建立檔案系統時設定的輸送量容量。您可以視需要隨時修改檔案系統的輸送量容量。輸送量容量是決定主控檔案系統的檔案伺服器可以提供檔案資料的速度之一。更高的輸送量容量層級也有更高的每秒 I/O 作業 (IOPS) 和更多的記憶體，可在檔案伺服器上快取資料。如需詳細資訊，請參閱FSx 適用於 FSx for Windows File Server 效能。

修改檔案系統的輸送量容量時，Amazon FSx 會在幕後切換檔案系統的檔案伺服器。對於異地同步備份檔案系統，這會導致自動容錯移轉和容錯回復，同時 Amazon FSx 切換偏好和次要檔案伺服器。對於

單一可用區系統，您的檔案系統在輸送量容量擴充期間將無法使用幾分鐘。檔案系統可使用新的輸送量容量時，我們會向您收取該容量的費用。

> **Note**
>
> 在後端進行維護作業期間，系統修改 (例如修改輸送量容量) 可能會延遲。維護可能會導致這些變更排入佇列狀態，直到下次處理完畢為止。

主題

何時修改輸送量容量

亞馬遜 FSx 與亞馬遜集成CloudWatch，可讓您監控檔案系統的持續輸送量使用量等級。除了檔案系統的輸送量容量、儲存容量和儲存類型外，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。您可以使用CloudWatch決定要變更哪些維度以提升效能的量度。如需詳細資訊，請參閱使用 Amazon 監控指標 CloudWatch。

對於異地同步備份檔案系統，輸送量容量擴展會導致自動容錯移轉和容錯回復，同時 Amazon FSx 切換偏好和次要檔案伺服器。在檔案伺服器取代期間 (在擴充輸送量容量以及檔案系統維護和意外服務中斷期間發生)，剩餘的檔案伺服器將會為檔案系統的任何持續流量提供服務。當被取代的檔案伺服器恢復上線時，FSx for Windows 會執行重新同步化工作，以確保資料會同步回新取代的檔案伺服器。

FSx for Windows 旨在將此重新同步處理活動對應用程式和使用者的影響降到最低。不過，重新同步處理程序需要同步處理大型區塊中的資料。這表示即使只更新一小部分，大型資料區塊也可能需要同步處理。因此，重新同步化的量不僅取決於資料流失量，還取決於檔案系統上資料流失的性質。如果您的工作負載大量寫入且需要大量 IOPS，則資料同步處理程序可能需要更長的時間，而且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化的持續時間，我們建議您在檔案系統負載最小的閒置期間修改輸送量容量。除了工作負載之外，我們也建議您確定檔案系統具有足夠的輸送量容量來執行同步處理工作，以減少資料同步化的持續時間。最後，我們建議您在檔案系統負載較輕的情況下測試容錯移轉的影響。

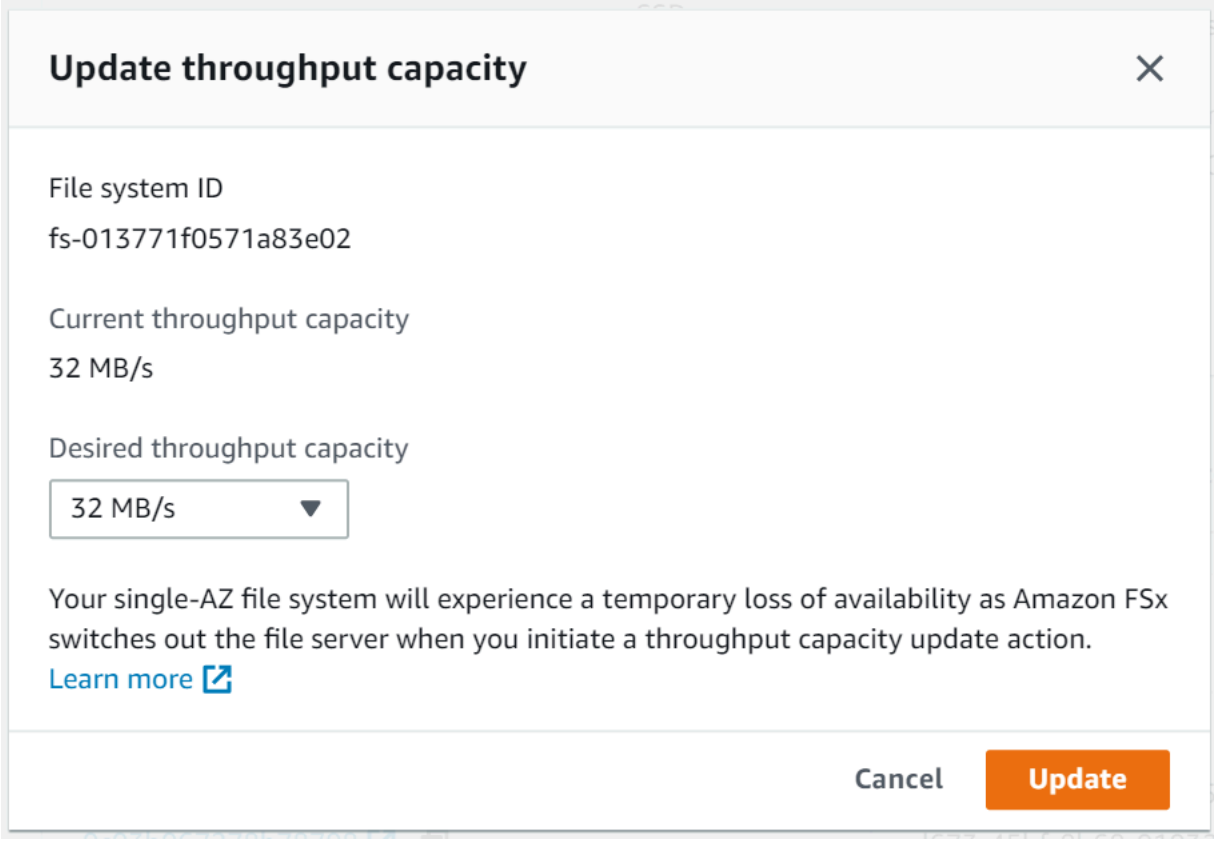
如何修改輸送量容量

您可以使用 Amazon FSx 主控台修改檔案系統的輸送量容量，AWS Command Line Interface(AWS CLI) 或亞馬遜 FSx 應用程式介面。

修改檔案系統的輸送量容量 (主控台)

1. 在以下位置打開亞馬遜 FSx 控制台https://console.aws.amazon.com/fsx/。
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. 對於動作，選擇更新輸送量。或者，在摘要」面板中，選擇更新文件系統的旁邊吞吐量容量。

   該更新輸送量容量窗口出現。
4. 為以下項目選擇新值吞吐量容量從列表中。



5. 選擇更新以啟動輸送量容量更新。

> **Note**
>
> 異地同步備份檔案系統在更新輸送量擴展時容錯移轉和容錯回復，且完全可用。單一可用區檔案系統在更新期間遇到非常短暫的無法使用時間。

6. 您可以在上監視更新進度檔案系統詳細資料頁面，在更新標籤。

   您可以使用 Amazon FSx 主控台監控更新進度，AWS CLI，以及應用程式介面。如需詳細資訊，請參閱監視輸送量容量變更。

修改檔案系統的輸送量容量 (CLI)

若要修改檔案系統的輸送量容量，請使用AWS CLI命令update-file-system。設定下列參數：

- `--file-system-id`至您正在更新之檔案系統的 ID。
- `ThroughputCapacity`到要將檔案系統更新為的所需值。

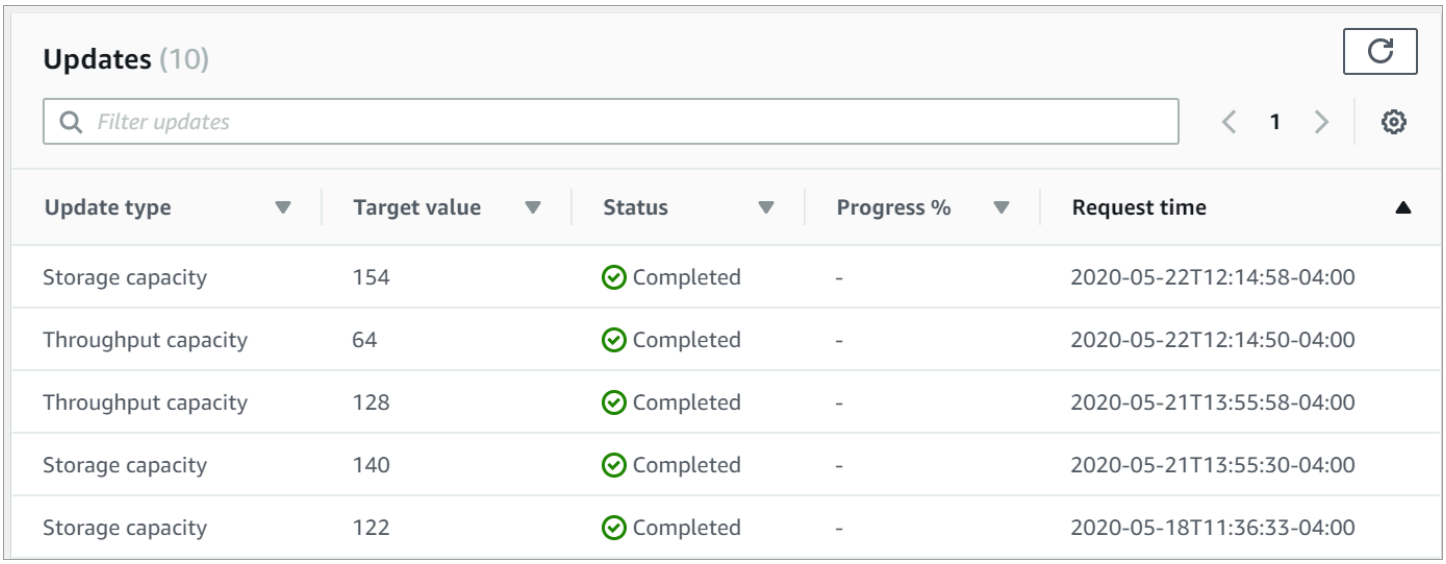
您可以使用 Amazon FSx 主控台監控更新進度，AWS CLI，以及應用程式介面。如需詳細資訊，請參閱監視輸送量容量變更。

監視輸送量容量變更

您可以使用 Amazon FSx 主控台、API 和AWS CLI。

監視主控台中的輸送量容量變更

在更新」頁籤中的檔案系統詳情視窗中，您可以檢視每個更新動作類型的 10 個最新更新動作。



對於輸送量容量更新動作，您可以檢視下列資訊。

更新類型

可能的值為吞吐量容量。

目標值

將檔案系統的輸送量容量變更為所需的值。

狀態

更新的目前狀態。對於輸送量容量更新，可能的值如下：

- 等待中— Amazon FSx 已收到更新要求，但尚未開始處理它。
- 進行中— 亞馬遜 FSx 正在處理更新請求。
- 更新優化— 亞馬遜 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 效能層級可用於寫入作業。您的讀取作業會看到上一層級與新層級之間的磁碟 I/O 效能，直到檔案系統不再處於此狀態為止。
- 已完成— 輸送量容量更新順利完成。
- 失敗— 輸送量容量更新失敗。選擇問號 (?) 以查看輸送量更新失敗原因的詳細資訊。

請求時間

亞馬遜 FSx 收到更新請求的時間。

使用監視變更AWS CLI和 API

您可以使用檢視和監視檔案系統輸送量容量修改要求describe-file-systemsCLI 指令和DescribeFileSystemsAPI 動作。該`AdministrativeActions`陣列列示每個管理動作類型的 10 個最新更新動作。當您修改檔案系統的輸送量容量時，`FILE_SYSTEM_UPDATE`系統管理動作已產生。

下面的例子顯示了一個的響應摘錄`describe-file-systems`使用 CLI 命令。檔案系統的輸送量容量為每秒 8 MB/s，目標輸送量容量為 256 MB/s。

```
.
.
.
    "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。新的輸送量容量隨後可供檔案系統使用，並顯示在ThroughputCapacity財產。這顯示在下面的響應摘錄describe-file-systems使用 CLI 命令。

```
.
.
.
    "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，和FailureDetails屬性提供有關失敗的資訊。如需疑難排解失敗動作的資訊，請參閱儲存或輸送量容量更新失敗。

標記您的 Amazon FSX 資源

為協助您管理您的文件系統和其他 Amazon FSX 資源，您可以用標籤形式將您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您的 AWS 資源，例如依據目的、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您的 AWS 資源，例如依據目的、擁有者或環境。例如，您可以為您賬户的 Amazon FSx 文件系統定義一組標籤，協助您追蹤每個實例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的管理您的資源。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 來説不具有任何語意義，並會嚴格解譯為字串。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。

若您使用卓越亞馬遜 FSx API，AWSCLI 或AWS軟體開發套件，您可以使用`TagResource`API 動作將標籤套用到現有資源。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

您可以為您賬户中存在的 Amazon FSX 資源新增標籤。若您使用 Amazon FSX 主控台，您可以透過使用位於相關資源畫面上的 Tags (標籤) 標籤套用標籤。創建資源時，可以應用帶有值的 Name 鍵，並且可以在創建新文件系統時應用所選標籤。主控台可能會根據 Name 標籤整理資源，但此標籤對 Amazon FSX 服務來説不具有任何語意義。

您可以在 IAM 政策中將標籤式的資源層級許可套用到支援在建立時新增標籤的 Amazon FSX API 動作，以對可在建立時為資源加上標籤的使用者和組實作精密控制。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到`TagResource`和`UntagResource`Amazon FSX API 動作，控制哪些標籤金鑰和值會在您現有的資源上設定。

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
- Amazon FSX 標籤允許的字元包括：可用 UTF-8 表示的字母、數字和空格，還有以下字元：+-=. _:/@。
- 標籤金鑰與值皆區分大小寫。
- 此 `aws:` 字首已保留供 AWS 使用。如果標籤具有此字首的標籤金鑰，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。

您無法僅根據標籤刪除資源；您必須指定資源標識符。例如，若要使用標籤金鑰標籤的文件系統，名為`DeleteMe`，您必須使用`DeleteFileSystem`操作與文件系統資源標識符，例如 fs-1234567890 的文件系統資源標識符。

當您標記公有或共享資源時，您指派的標籤僅適用於AWS 帳戶；無其他AWS 帳戶將有權訪問這些標籤。針對共享資源的標籤型存取控制，每個AWS 帳戶必須指派其自身的一組標籤，控制對資源的存取。

許可和標籤

如需在建立時為 Amazon FSX 資源新增標籤所需之許可的詳細資訊，請參在建立期間授予標籤資源的許可。如需使用標籤來限制對 IAM 政策中 Amazon FSX 資源的存取權的詳細資訊，請參使用標籤來控制對 Amazon FSx 資源的存取。

使用亞馬遜 FSx 維護窗口

適用於 Windows 檔案伺服器的 Amazon FSx 會針對其管理的微軟視窗伺服器軟體執行例行軟體修補。維護時段可讓您控制進行軟體修補的一週中的日期和時間。您可以在建立檔案系統期間選擇維護時段。如果您沒有時間偏好設定，則會指派 30 分鐘的預設視窗。

FSx Windows 檔案伺服器可讓您調整維護時段，以符合工作負載和作業需求。您可以視需要頻繁地移動維護時段，前提是至少每 14 天排定一次維護時段。如果修補程式已發行，而您尚未在 14 天內排定維護時段，則 Windows 檔案伺服器的 FSx 會繼續維護檔案系統，以確保其安全性和可靠性。

修補正在進行時，預期單一可用區檔案系統無法使用，通常不到 20 分鐘。您的異地同步備份檔案系統仍可使用，並自動容錯移轉和容錯回復偏好的檔案伺服器和待命檔案伺服器。如需詳細資訊，請參閱FSx for Windows File Server FSx 的容錯移轉程序。因為異地同步備份檔案系統的修補涉及容錯移轉和容錯回復，因此在此期間傳送至檔案系統的任何流量都必須在偏好的檔案伺服器和待命檔案伺服器之間同步。為了減少修補時間，我們建議您在檔案系統負載最小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 檔案伺服器會在維護開始之前，完成對託管檔案系統之基礎儲存磁碟區的任何擱置寫入操作。

您可以使用亞馬遜 FSx 管理主控台，AWS CLI,AWSAPI，或其中一個AWSSDK 可變更檔案系統的維護時段。

若要變更每週維護時段 (主控台)

1. 在以下位置開啟亞馬遜 FSx 主控台https://console.aws.amazon.com/fsx/。
2. 選擇檔案系統在左側導覽欄中。
3. 選擇您要變更每週維護時段的檔案系統。檔案系統詳細資訊頁面隨即顯示。
4. 選擇管理以顯示檔案系統管理設定面板。
5. 選擇更新以顯示變更維護視窗窗口。
6. 輸入您要每週維護時段開始的新日期與時間。
7. 選擇 Save (儲存) 儲存變更。新的維護開始時間會顯示在管理設定面板。

若要變更每週維護時段，請使用update-file-systemCLI 命令，請參閱演練 3：更新現有的檔案系統。

管理 Amazon FSx 檔案系統的最佳實務

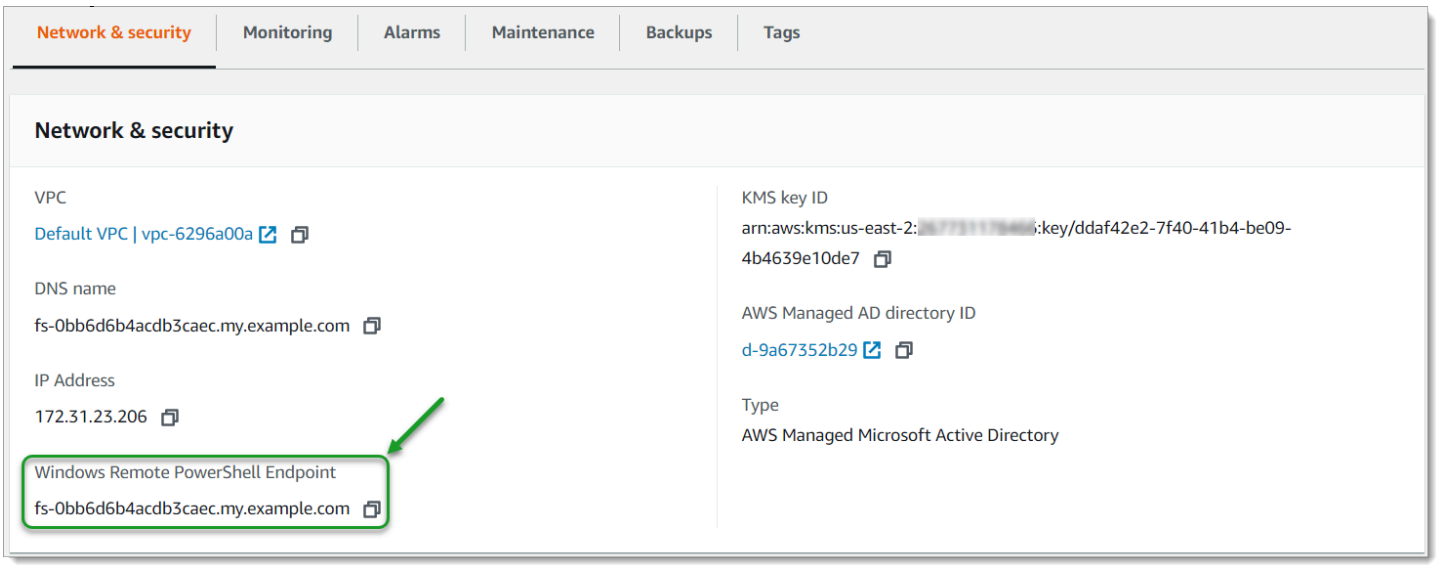
Amazon FSx 提供多種功能，可協助您實作管理檔案系統的最佳實務，包括：

- 最佳化儲存耗用
- 使最終用戶能夠將文件和文件夾恢復到以前的版本
- 對所有連線的用戶端強制執行加密

在 PowerShell命令上使用下列 Amazon FSx CLI 進行遠端管理，在檔案系統上快速實作這些最佳實務。

若要執行這些命令，您必須知道檔案系統的 Windows 遠 PowerShell端端點。若要尋找此端點，請依照下列步驟執行：

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 選擇您的檔案系統。在 [網路與安全性] 索引標籤上，找出 Windows 遠 PowerShell 端端點，如下所示。



如需詳細資訊，請參閱 管理檔案系統 及 使用 Amazon FSx CLI PowerShell。

主題

- 一次性管理設定工作
- 持續的管理工作以監控您的檔案系統

一次性管理設定工作

以下是您可以為檔案系統快速設定一次的工作。

管理儲存體使用

使用下列指令來管理您的檔案系統儲存空間耗用。

- 若要以預設排程開啟重複資料刪除功能，請執行下列命令。

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

  您也可以選擇使用下列指令，在建立檔案後立即在檔案上執行重複資料刪除作業，而不需要任何最低檔案保留時間。

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

  如需詳細資訊，請參閱 重复数据删除。

- 使用下列命令在「追蹤」模式下開啟使用者儲存配額，此模式僅用於報告目的，而不是用於強制執行。

```
$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 儲存配額。

開啟陰影複製，讓終端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) 開啟陰影複製，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 設定陰影複製以使用預設儲存區和排程。

在傳輸中強制執行加密

下列指令會強制為連線至檔案系統的用戶端強制加密。

```
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

```
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 用戶會話和打開文件。

持續的管理工作以監控您的檔案系統

下列進行中的工作可協助您監控檔案系統的磁碟使用情況、使用者配額和開啟的檔案。

監控重複刪除狀態

監控重複資料刪除狀態，包括在檔案系統上達到的節省率，如下所示。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -
ConfigurationName FsxRemoteAdmin -ScriptBlock { Get-FSxDedupStatus } | select
 OptimizedFilesCount,OptimizedFilesSize,SavedSpace,OptimizedFilesSavingsRate
```

監控使用者層級儲存耗用

取得目前使用者儲存配額項目的報告，包括使用多少空間，以及是否違反限制和警告臨界值。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Get-FSxUserQuotaEntries }
```

監視和關閉打開的文件

通過查找保持打開的文件並關閉它們來管理打開的文件。使用以下命令檢查打開的文件。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Get-FSxSmbOpenFile}
```

使用以下命令關閉打開的文件。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Close-FSxSmbOpenFile -Confirm:$false}
```

使用 DFS 命名空間分組多個檔案系統

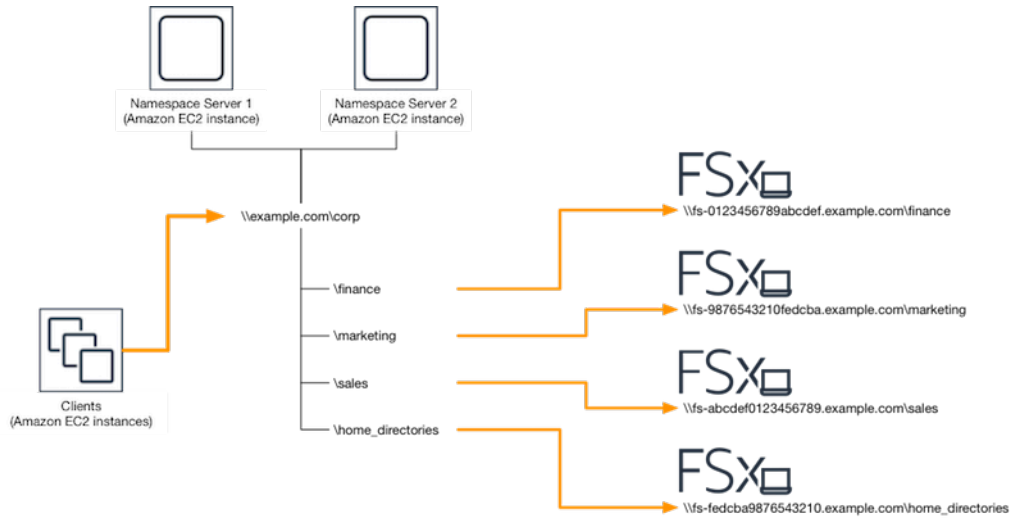
Amazon FSx FSx for Windows File Server 支援使用微軟的分散式檔案系統 (DFS) 命名空間。您可以使用 DFS 命名空間，將多個檔案系統上的檔案共用群組成一個共用資料夾結構 (命名空間)，您可以用來存取整個檔案資料集。DFS 命名空間可協助您組織和統一跨多個檔案系統對檔案共用的存取。DFS 命名空間也可協助擴充檔案資料儲存體，超越每個檔案系統支援的大型檔案資料集 (64 TB)，最高可達數百 PB。

設定 DFS 命名空間以分組多個檔案系統

您可以使用 DFS 命名空間來群組單一命名空間下的多個檔案系統。在以下範例中，以網域為基礎的命名空間 (example.com\ corp) 建立在兩個命名空間伺服器上，合併儲存在多個 Amazon FSx 檔案系統 (財務、行銷、銷售、home_目錄) 上的檔案共用。這可讓您的使用者使用一般命名空間存取檔案共用。鑑於此，他們不需要為每個託管檔案共用的檔案系統指定檔案系統 DNS 名稱。

> **Note**
>
> Amazon FSx 無法新增至 DFS 共用路徑的根目錄。

這些步驟會引導您在兩個命名空間伺服器上建立單一命名空間 (example.com\ corp)。您也可以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個別 Amazon FSx 檔案系統上託管的共用。



若要將多個檔案系統分組成共同的 DFS 命名空間

1. 如果您尚未執行 DFS 命名空間伺服器，您可以啟動一對使用設定 -DFSN-SERVER.Tem AWS CloudFormation plate 範本的高可用性 DFS 命名空間伺服器。如需有關建立 AWS CloudFormation 堆疊的詳細資訊，請參閱《使用指南》中的〈在 AWS CloudFormation 主控台上建立堆疊AWS CloudFormation〉。
2. Connect 至上一個步驟中以「AWS 委派管理員」群組中的使用者身分啟動的其中一個 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到 Windows 執行個體。
3. 開啟即可存取 DFS 管理主控台。開啟 [開始] 功能表並執行 [開始]。這將打開 DFS 管理圖形用戶界面工具。
4. 選擇動作，然後選擇新增命名空間，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. 在 [名稱] 中，輸入您要建立的命名空間 (例如 corp)。
6. 選擇 「編輯設定」，然後根據您的需求設定適當的權限。選擇下一步。
7. 保持預設以網域為基礎的命名空間選項保持選取狀態，保持選取啟用 Windows Server 2008 模式選項，然後選擇下一步。

   > **Note**
   >
   > 視窗伺服器 2008 年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後，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權限，然後選擇「確定」。
12. 開啟剛建立之命名空間的前後關聯 (按一下滑鼠右鍵) 選單，選擇「新增資料夾」，輸入資料夾的名稱 (例如，`finance`對於「名稱」，然後選擇 「確定」。
13. 輸入您希望 DFS 命名空間資料夾指向的檔案共用的 DNS 名稱，以 UNC 格式 (例如\ `\fs-0123456789abcdef0.example.com\finance`) 做為資料夾目標的路徑，然後選擇確定。
14. 如果該共享不存在：

    a. 選擇 [是] 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$ 底下建立新資料夾，然後選擇「確定」。

d. 設定適當的共用權限，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. 針對您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。

監督 FSx 的 FSx for Windows File Server

監控是維持 Amazon FSx 和 AWS 解決方案的可靠性、可用性和效能的重要組成部分。您應該從 AWS 解決方案的所有部分收集監視資料，以便在發生多點失敗時更輕鬆地偵錯。但是，在開始監控 Amazon FSx 之前，您應該建立一個監控計劃，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 Windows 檔案伺服器 FSx 中記錄和監視的相關資訊，請參閱下列主題。

主題

- 監控工具
- 使用 Amazon 監控指標 CloudWatch
- 記錄 Amazon FSx for Windows File Server API 呼叫AWS CloudTrail

監控工具

AWS 提供各種可用來監控 Amazon FSx 的工具。您可以配置其中一些工具來為您進行監視，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監控工具觀看 Amazon FSx，並在發生錯誤時回報：

- Amazon A CloudWatch lar ps — 觀看您指定期間內的單一指標，並根據指定臨界值在多個時段內相對於指定閾值的指標值執行一或多個動作。動作是傳送至亞馬遜簡單通知服務 (Amazon SNS) 主題或 Amazon EC2 Auto Scaling 政策的通知。 CloudWatch 警示不會僅因為處於特定狀態而叫用動作；狀態必須已變更並維持指定數目的期間。如需詳細資訊，請參閱 使用 Amazon 監控指標 CloudWatch。

- Amazon CloudWatch 日誌 — 監控、存放和存取來自 AWS CloudTrail 或其他來源的日誌檔。如需詳細資訊，請參閱什麼是 Amazon CloudWatch 日誌？ 在 Amazon CloudWatch 日誌用戶指南中。
- AWS CloudTrail 記錄監控 — 在帳戶之間共用記錄檔、即時監控記 CloudTrail 錄檔案，方法是將記錄檔傳送至 CloudWatch 記錄檔、使用 Java 撰寫記錄處理應用程式，以及驗證記錄檔在傳送之後是否未變更 CloudTrail。若要取得更多資訊，請參閱《使用指南》中的〈AWS CloudTrail 使用 CloudTrail 記錄檔〉。

手動監控工具

監控 Amazon FSx 的另一個重要部分涉及手動監控 Amazon CloudWatch 警報未涵蓋的項目。Amazon FSx 和其他 AWS 主控台儀表板可提供您 AWS 環境狀態的 at-a-glance 檢視。 CloudWatch

Amazon FSx 主控台的監控和效能儀表板顯示：

- 適用於 Windows 檔案伺服器的目前 FSx 警告與 CloudWatch 警示
- 顯示檔案系統活動摘要的圖形
- 檔案系統儲存容量與使用率的圖形
- 檔案伺服器與儲存磁碟區效能圖表
- CloudWatch 警報

CloudWatch 首頁顯示：

- 目前警示與狀態
- 警示與資源的圖表
- 服務運作狀態

此外，您可以使用執行 CloudWatch 以下操作：

- 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。
- 搜尋並瀏覽所有資 AWS 源指標。
- 建立與編輯要通知發生問題的警示。

如需 Amazon FSx 監控和效能儀表板的詳細資訊，請參閱如何將 FSx 用於 FSx for Windows File Server 的度量。

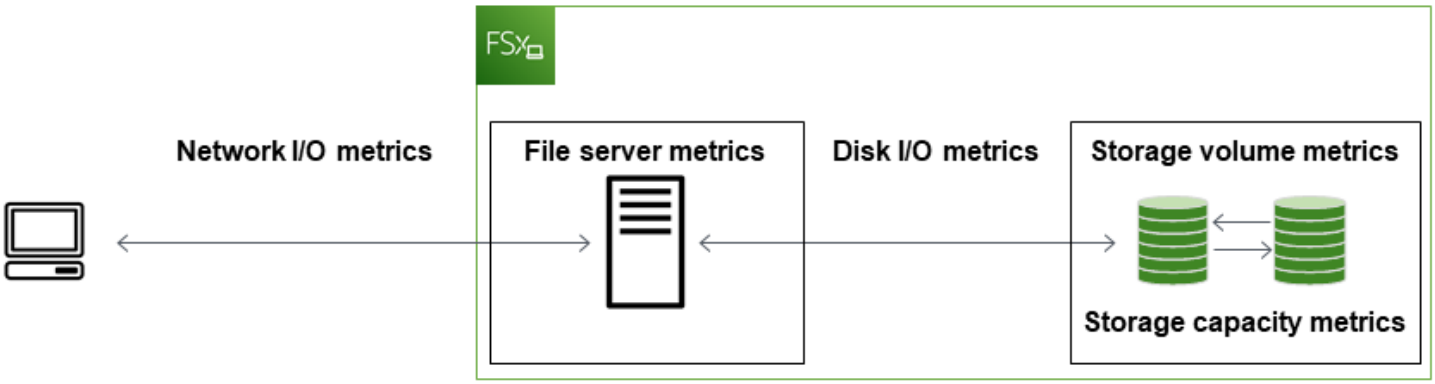
使用 Amazon 監控指標 CloudWatch

您可以使用 Amazon 監控適用於 Windows 檔案伺服器檔案系統的 FSx CloudWatch，Amazon 會從適用 FSx for Windows File Server 收集原始資料，並將其處理為可讀且近即時的指標。這些統計資料會保留 15 個月，因此您可以存取歷史資訊，並深入瞭解 Web 應用程式或檔案系統的執行情況。

FSx for Windows File Server 在下列網域中發佈 CloudWatch 測量結果：

- 網路 I/O 測量結果會測量存取檔案系統的從屬端與檔案伺服器之間的活動。
- 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 測量結果會測量檔案伺服器與儲存磁碟區之間的活動。
- 儲存體磁碟區指標可測量 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。
- 儲存容量指標可測量儲存使用量，包括因為重複資料刪除而節省儲存空間。

下圖說明 Windows 檔案伺服器檔案系統的 FSx、其元件及公制網域。



根據預設，Windows 檔案伺服器版 Amazon FSx 會在 1 分鐘的時間傳送量度資料至 CloudWatch ，但下列例外情況除外，以 5 分鐘為間隔發出：

- `FileServerDiskThroughputBalance`
- `FileServerDiskIopsBalance`

如需詳細資訊 CloudWatch，請參閱什麼是 Amazon CloudWatch？ 在 Amazon 用 CloudWatch 戶指南。

在進行系統維護或基礎架構元件更換期間，單一可用區 FILE 系統，以及在主要和次要檔案伺服器之間容錯移轉和容錯回復期間的異地同步備份檔案系統，可能不會發佈指標。

部分 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

指標與維度

FSx for Windows File Server 的所有檔案系統，將下列指標發佈到 Amazon CloudWatch 的AWS/FSx命名空間中：

- DataReadBytes
- DataWriteBytes
- DataReadOperations
- DataWriteOperations
- MetadataOperations
- FreeStorageCapacity

FSx 適用於 Windows 檔案伺服器，針對設定輸送容量至少 32 Mbps 的檔案系統，將以下所述的指標發佈到 Amazon CloudWatch 的AWS/FSx命名空間中。

主題

- FSx 適用於視窗儲存容量指標
- FSx (適用於視窗維度)

FSx 適用於視窗網路 I/O 測量結果

AWS/FSx命名空間包含下列網路 I/O 測量結果。

指標	描述
DataReadBytes	存取檔案系統之用戶端讀取作業的位元組數目。 單位：位元組 有效的統計資訊：Sum
DataWriteBytes	用戶端存取檔案系統之寫入作業的位元組數。 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作業數目。 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作業數目。 單位：計數 有效的統計資訊：Sum
MetadataOperations	存取檔案系統之用戶端的中繼資料作業數目。 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。

指標	描述
	單位：計數

FSx 檔案伺服器測量結果

AWS/FSx命名空間包含下列檔案伺服器測量結果。

指標	描述
NetworkThroughputUtilization	存取檔案系統之用戶端的網路輸送量，以佈建限制的百分比表示。 單位：百分比
CPUUtilization	檔案伺服器 CPU 資源的使用率百分比。 單位：百分比
MemoryUtilization	檔案伺服器記憶體資源的使用率百分比。 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，佔佈建限制的百分比，由輸送量容量決定。 單位：百分比
FileServerDiskThroughputBalance	檔案伺服器及其儲存磁碟區之間磁碟輸送量的可用突發積分百分比。對於傳輸量容量為 256 Mbps 或以下佈建的檔案系統有效。 單位：百分比
FileServerDiskIopsUtilization	檔案伺服器與儲存磁碟區之間的磁碟 IOPS，佔佈建限制的百分比 (由輸送量容量決定)。 單位：百分比

指標	描述
FileServerDiskIopsBalance	檔案伺服器及其儲存磁碟區之間磁碟 IOPS 的可用突發積分百分比。對於傳輸量容量為 256 Mbps 或以下佈建的檔案系統有效。 單位：百分比

FSx 適用於視窗磁碟 I/O 測量結果

AWS/FSx命名空間包含下列磁碟 I/O 測量結果。

指標	描述
DiskReadBytes	存取儲存磁碟區之讀取作業的位元組數目。 單位：位元組 有效的統計資訊：總和
DiskWriteBytes	存取儲存磁碟區之寫入作業的位元組數目。 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作業數目。 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作業數目。 單位：計數 有效的統計資訊：Sum

FSx 適用於視窗儲存體磁碟區指標

AWS/FSx命名空間包含下列儲存磁碟區測量結果。

指標	描述
DiskThroughputUtilization	(僅限 HDD) FILE 伺服器與其儲存磁碟區之間的磁碟輸送量，佔儲存磁碟區決定的佈建限制的百分比。 單位：百分比
DiskThroughputBalance	(僅限 HDD) 儲存磁碟區磁碟輸送量的可用突發積分百分比。 單位：百分比
DiskIopsUtilization	(僅適用於 SSD) 您的伺服器與儲存磁碟區之間的磁碟 IOPS，以儲存磁碟區決定的佈建 IOPS 限制的百分比。 單位：百分比

FSx 適用於視窗儲存容量指標

命AWS/FSx名空間包含下列儲存容量指標。

指標	描述
FreeStorageCapacity	可用儲存容量。 單位：位元組 有效的統計資訊：Average、Minimum
StorageCapacityUtilization	已使用的實體儲存容量佔總儲存容量的百分比。 單位：百分比
DeduplicationSavedStorage	重複資料刪除所節省的儲存空間 (如果已啟用)。 單位：位元組

FSx (適用於視窗維度)

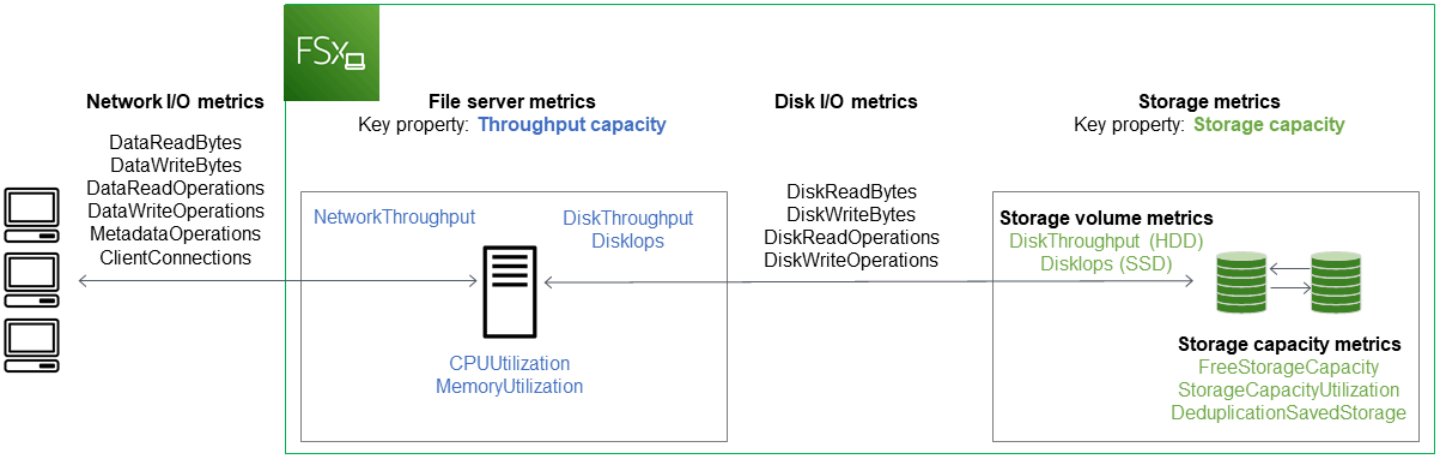
FSx for Windows File Server 度量會使用FSx命名空間，FileSystemId並提供單一維度的度量。您可以使用describe-file-systems AWS CLI 指令或 DescribeFileSystemsAPI 指令尋找檔案系統的 ID。檔案系統識別碼會採用 *fs-* 0123456789abcdef0 的形式。

如何將 FSx 用於 FSx for Windows File Server 的度量

每個 Amazon FSx 檔案系統都有兩個主要架構元件：

- 將資料提供給存取檔案系統的用戶端的檔案伺服器。
- 在檔案系統中裝載資料的儲存磁碟區。

FSx for Windows File Server 會報告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的度量。 CloudWatch 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。針對一組測量結果顯示的主要屬性是決定這些測量結果容量的檔案系統屬性。調整該屬性會修改該組度量的檔案系統效能。



使用 Amazon FSx 主控台中的監控和效能面板，檢視下表所述 FSx for Windows File Server CloudWatch 指標。

監控與效能面板	我該如何...	图表	相關指標
Summar	... 確定我的文件系統的 IOPS 總數？	總 IOPS	總和 (DataRead0 perations

監控與效能面板	我該如何...	图表	相關指標
			DataWriteOperations +MetadataOperations)/期間 (以秒為單位)
	... 確定我的文件系統的總吞吐量？	總輸送量	總和 (DataReadBytes +DataWriteBytes)/期間 (以秒為單位)
	... 判斷檔案系統上的可用儲存容量？	可用儲存容量	FreeStorageCapacity
	... 確定客戶端和文件服務器之間建立的連接數？	用戶端連線	ClientConnections
儲存	... 確定已使用的實體磁碟空間量佔檔案系統總儲存容量的百分比？	儲存容量使用率	StorageCapacityUtilization
	... 決定重複資料刪除所節省的實體磁碟空間量？	從重複資料刪除儲存	DeduplicationSavedStorage
	... 決定存取檔案系統之用戶端的網路輸送量，以檔案系統佈建輸送量的百分比為單位？	網路輸送量使用	NetworkThroughputUtilization
效能-檔案伺服器	... 判斷檔案伺服器與其儲存磁碟區之間的磁碟輸送量，是否為「輸送量容量」所決定的佈建限制的百分比？	磁碟輸送量使用	FileServerDiskThroughputUtilization
	... 決定檔案伺服器與其儲存磁碟區之間磁碟輸送量的可用突發積分百分比？	磁碟輸送量突增平衡	FileServerDiskThroughputBalance

監控與效能面板	我該如何...	图表	相關指標
	... 判斷檔案伺服器與儲存磁碟區之間的磁碟 IOPS 數量，是否為輸送量容量所決定的佈建限制的百分比？	磁碟 IOPS 使用率	`FileServerDiskIopsUtilization`
	... 決定檔案伺服器與儲存磁碟區之間磁碟 IOPS 的可用突發積分百分比？	磁碟 IOPS 突發平衡	`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？	內存使用率	`MemoryUtilization`
效能 — 儲存磁碟區	... 決定存取儲存磁碟區之作業的輸送量，是否為 HDD 儲存容量所決定的佈建限制百分比？	磁碟輸送量使用率 (HDD)	`DiskThroughputUtilization`
	... 決定存取 HDD 儲存磁碟區之作業輸送量的可用突發積分百分比？	磁碟輸送量突增平衡 (HDD)	`DiskThroughputBalance`
	... 決定存取儲存磁碟區之作業的 IOPS，是否為 SSD 儲存容量所決定的佈建限制的百分比？	磁碟 IOPS 使用率 (SSD)	`DiskIopsUtilization`

> **Note**
>
> 我們建議您將平均輸送量容量使用率維持在 50% 以下，以確保您擁有足夠的備用輸送量容量，以應付工作負載中的意外尖峰，以及任何背景 Windows 儲存體作業 (例如儲存同步處理、重複資料刪除或陰影複製)。

效能警告與建議

FSx 適用於 Windows 會針對設定輸送量容量至少 32 Mbps 的檔案系統，提供效能警告。每當其中一個 CloudWatch 指標接近或超過多個連續資料點的預定閾值時，Amazon FSx 就會顯示一組指標的警告。這些警告為您提供可行的建議，您可以使用這些建議來最佳化檔案系統的效能。

您可以在監視與效能儀表板的數個區域存取警告。所有使用中或最近的 Amazon FSx 效能警告，以及為處於 CloudWatch 警示狀態的檔案系統設定的任何警示，都會顯示在「摘要」區段的「監控與效能」面板中。警告也會顯示在顯示量度圖形的儀表板區段中。

您可以為任何 Amazon FSx 指標建立 CloudWatch 警示。如需詳細資訊，請參閱 創建 CloudWatch 警報以監控 Amazon FSx。

使用效能警告來改善檔案系統效能

Amazon FSx 提供可行的建議，您可以使用這些建議來優化檔案系統的效能。這些建議描述了如何解決潛在的性能瓶頸. 如果您希望活動繼續進行，或者它會對檔案系統效能造成影響，則可以採取建議的動作。視觸發警告的測量結果而定，您可以增加檔案系統的傳輸量容量或儲存體容量來解決此問題，如下表所述。

如果此量度有警告	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-成組分解平衡	
檔案伺服器 > 磁碟輸送量 — 突發平衡	
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 — 突發平衡 (HDD)	
儲存磁碟區 > 磁碟 IOPS — 使用率 (SSD)	增加固態硬碟 IOPS

> **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：
>
> - 儲存容量擴充的最佳化階段可產生更高的磁碟輸送量，如中所述 增加儲存容量並提高檔案系統效能
> - 對於異地同步備份檔案系統，輸送量容量擴充、硬體更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必須在主要和次要檔案伺服器之間進行同步處理，而 Windows Server 會執行可能會耗用磁碟 I/O 資源的資料同步化工作。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 適用於 FSx for Windows File Server 效能。

存取 FSx for Windows File Server 測量結果的 FSx

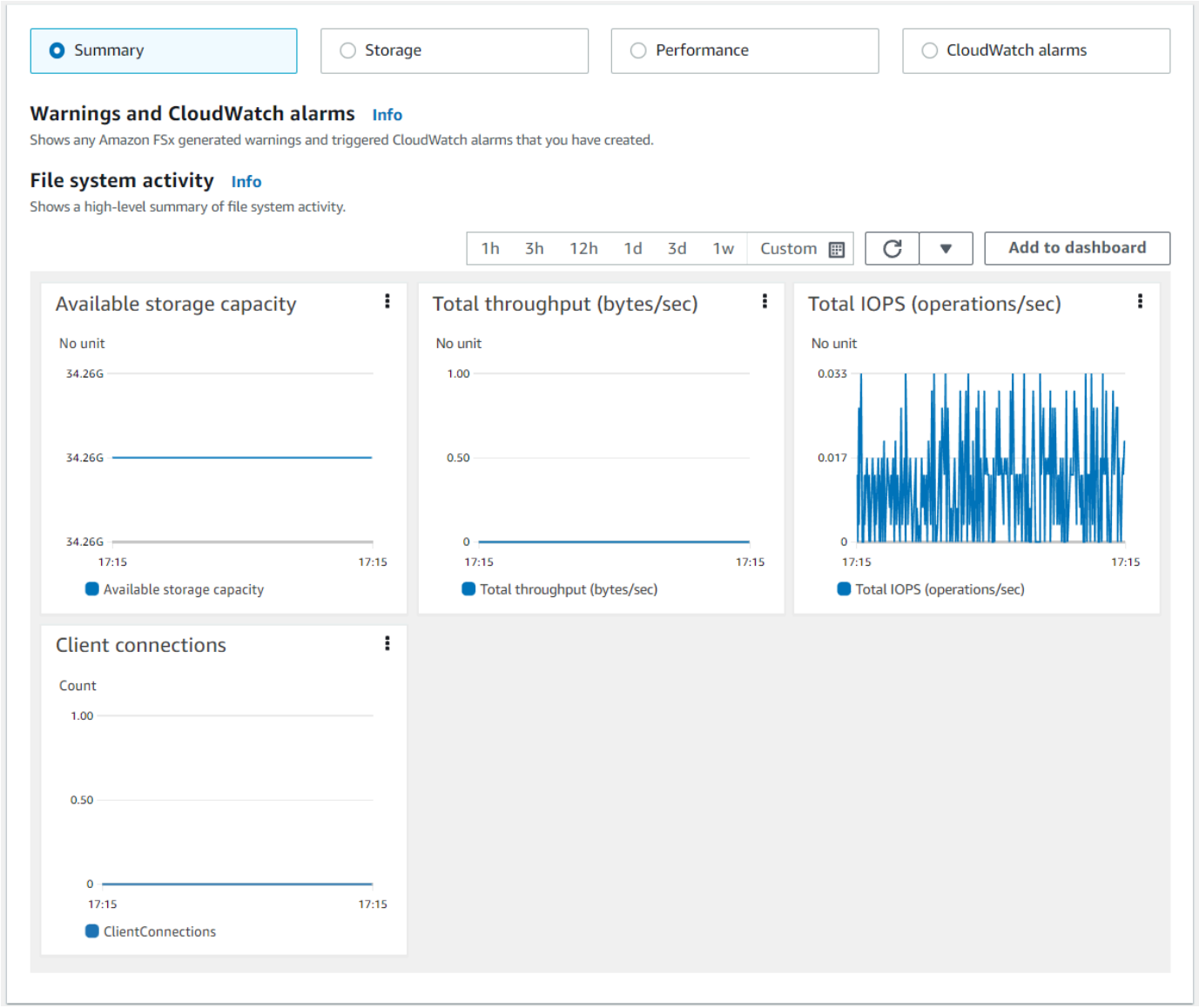
您可以透過下列方式查看的 Amazon FSx 指標。 CloudWatch

- Amazon FSx 控制台。
- 控 CloudWatch 制台。
- CloudWatch CLI（命令行界面）。
- CloudWatch 應用程式介面。

下列程序說明如何使用這些工具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. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 若要顯示 [檔案系統詳細資訊] 頁面，請在導覽窗格中選擇 [檔案系統]。
3. 選擇您要檢視其測量結果的檔案系統。
4. 若要檢視檔案系統度量的圖形，請選擇第二個面板上的 [監控與效能]。

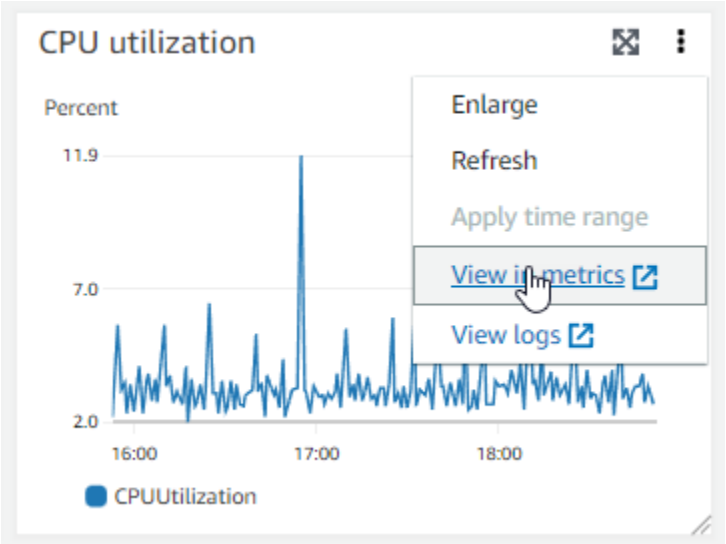


- 預設會顯示「摘要」量度，並顯示任何作用中的警告和 CloudWatch 警示，以及檔案系統活動量度。
- 選擇儲存體以檢視儲存容量和使用率指標。
- 選擇效能以檢視檔案伺服器和儲存體效能測量結
- 選擇CloudWatch 警示以檢視針對檔案系統設定之任何警示的圖形。

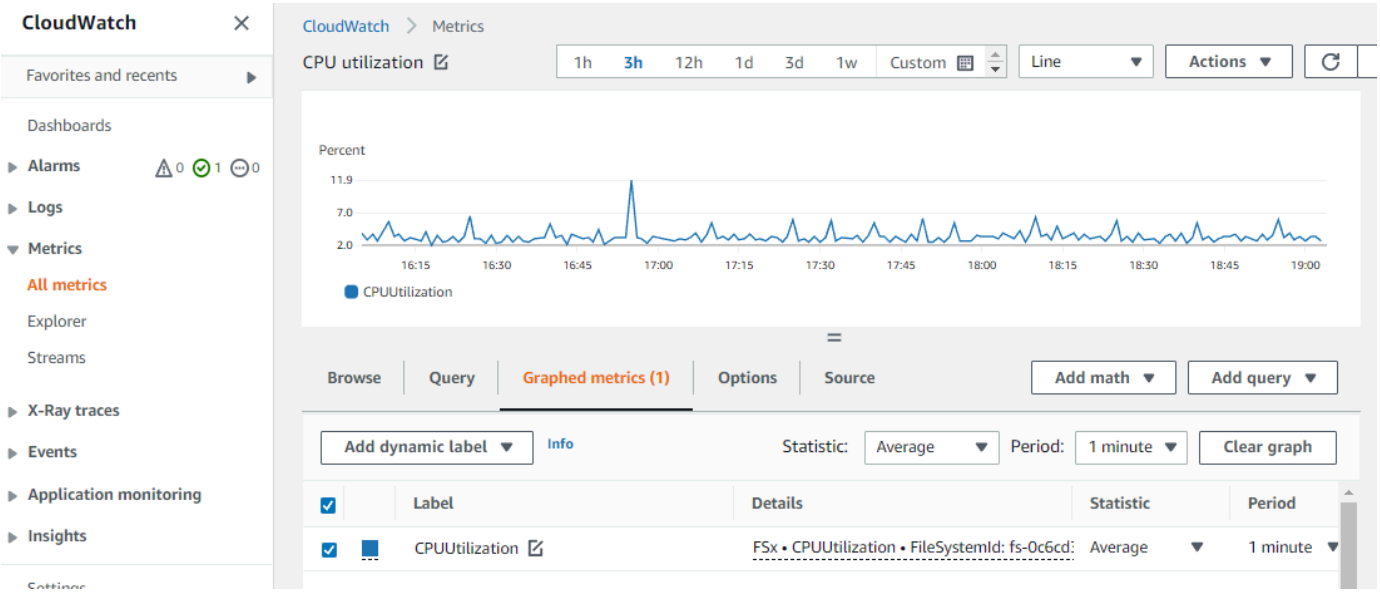
如需更多資訊，請參閱如何將 FSx 用於 FSx for Windows File Server 的度量

若要在 CloudWatch 主控台中檢視指標

1. 若要在 Amazon 主控台的「指標」頁面中檢視檔案系統指標，請導覽至 Amazon FSx CloudWatch 主控台的「監控和效能」面板中的指標。
2. 從量度圖表右上角的動作功能表中選擇檢視量度，如下圖所示。



這會在 CloudWatch 主控台中開啟「測量結果」頁面，並顯示量度圖表，如下圖所示。



若要將量度新增至 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「監控和效能」面板中選擇一組指標 (摘要、儲存或效能)。

2. 選擇面板右上角的「新增至儀表板」，這會開啟主 CloudWatch 控台。
3. 從清單中選取現有 CloudWatch 儀表板，或建立新儀表板。如需詳細資訊，請參閱 Amazon 使用 CloudWatch 者指南中的使用 Amazon CloudWatch 儀表板。

若要從存取度量 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/。

應用 CloudWatch 程式介面

若要從 CloudWatch API 存取指標

- 呼叫 `GetMetricStatistics`。如需詳細資訊，請參閱 Amazon CloudWatch API 參考資料。

創建 CloudWatch 警報以監控 Amazon FSx

您可以建立 CloudWatch 警示，在警示狀態變更時傳送 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。

警示只會呼叫持續狀態變更的動作。 CloudWatch 警報不會僅僅因為處於特定狀態而叫用動作；狀態必須已變更並維持指定數目的期間。您可以從 Amazon FSx 主控台或主控台建立警示。 CloudWatch

下列程序說明如何使用主控台和 API 為 Amazon FSx 建立警示。 AWS CLI

使用 Amazon FSx 主控台設定警示

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 在瀏覽窗格中，選擇 [檔案系統]，然後選擇您要建立警示的檔案系統。
3. 選擇「作業」功能表，然後選擇「檢視明細」。
4. 在 [摘要] 頁面上，選擇 [監視和效能]。
5. 選擇CloudWatch 鬧鐘。
6. 選擇 [建立 CloudWatch 鬧鐘]。您會被重新引導至 CloudWatch 主控台。
7. 選擇選取量度，然後選擇下一步。
8. 在「測量結果」段落中，選擇「FSX」。

9. 選擇 [檔案系統測量結果]，選擇您要設定警示的測量結果，然後選擇 [選取量度]。
10. 在「條件」區段中，選擇您要用於鬧鐘的條件，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，或在異地同步備份檔案系統的主要或次要伺服器的容錯移轉和容錯回復期間，不得發佈指標。若要避免不必要且誤導性的警示情況變更，並設定警示，以便對遺失的資料點有彈性，請參閱 Amazon CloudWatch 使用者指南中的設定 CloudWatch 警示如何處理遺失的資料。

11. 如果您想 CloudWatch 要在警示狀態觸發動作時傳送電子郵件或 SNS 通知給您，請為「無論何時此警示狀態為」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. 填入測量結果的「名稱」、「說明」和「時間」值，然後選擇「下一步」。
13. 在 [預覽並建立] 頁面上，檢閱您即將建立的鬧鐘，然後選擇 [建立鬧鐘]。

使用 CloudWatch 主控台設定鬧鐘

1. 請登入 AWS Management Console 並開啟 CloudWatch 主控台，網址為 https://console.aws.amazon.com/cloudwatch/。
2. 選擇 [建立警示] 以啟動 [建立警示精靈]。
3. 選擇 FSx 指標，然後捲動瀏覽 Amazon FSx 指標，找出您要放置警示的指標。若只要在此對話方塊中顯示 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. 如果您想要 CloudWatch 在到達鬧鐘狀態時傳送電子郵件給您，請針對「每當此警示」選擇「狀態為鬧鐘」。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，鬧鐘預覽區域讓您有機會預覽即將建立的鬧鐘。選擇建立警示 。

若要使用設定鬧鐘 AWS CLI

- 呼叫 `put-metric-alarm`。如需更多詳細資訊，請參閱 AWS CLI 命令參考。

使用 CloudWatch API 設定警示

- 呼叫 `PutMetricAlarm`。如需詳細資訊，請參閱 Amazon CloudWatch API 參考資料。

記錄 Amazon FSx for Windows File Server API 呼叫AWS CloudTrail

Amazon FSx for Windows File ServerAWS CloudTrail，提供由使用者、角色或使用者所採取之動作的服務AWS亞馬遜 FSx 中的服務。 CloudTrail 擷取 Amazon FSx 的 API 呼叫當作事件。擷取的呼叫包括來自 Amazon FSx 主控台的呼叫，以及對 Amazon FSx API 作業發出的程式碼呼叫。如果您建立追蹤記錄，就可以啟用持續傳送 CloudTrail Amazon S3 FSx 的事件。如果您不設定追蹤記錄，仍然可以透過 CloudTrail 主控台事件歷史。使用所收集的資訊 CloudTrail，您就可以判斷向 Amazon FSx 提出的請求、提出請求的時間，以及其他詳細資訊。

進一步了解 CloudTrail，請參閱AWS CloudTrail使用者指南。

Amazon FSx CloudTrail

CloudTrail 已在您的AWS 帳戶當您建立帳戶時。Amazon FSx 中發生活動時，該活動便會記錄在 CloudTrail 與其他一起事件AWS服務事件事件歷史。您可以檢視、搜尋和下載 AWS 帳戶 的最新事件。如需詳細資訊，請參閱檢視事件 CloudTrail 事件歷史。

如需您中正在進行事件的記錄AWS 帳戶，包括 Amazon FSx 的事件，請建立線索。一個線索啟用 CloudTrail 將日誌檔案交付到 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。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他AWS服務，以進一步分析和處理收集的事件資料 CloudTrail 日誌。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 的 Amazon SNS 通知 CloudTrail
- 接收 CloudTrail 來自多個區域的日誌檔案和接收 CloudTrail 來自多個帳戶的日誌檔案

會記錄所有 Amazon FSx CloudTrail 並記錄在Amazon FSx API 參考。例如，呼叫`CreateFileSystem`、`CreateBackup`和`TagResource`動作會產生項目 CloudTrail 日誌檔案。

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

- 該請求是否透過根或 AWS Identity and Access Management (IAM) 使用者憑證來提出。
- 提出該要求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 該請求是否由另一項 AWS 服務提出。

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

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至您指定的 Amazon S3 儲存貯體。 CloudTrail 日誌檔案包含一個或多個日誌項目。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 日誌檔案並非依公有 API 呼叫的堆疊追蹤，因此不會以任何特定順序出現。

以下範例顯示 CloudTrail 示範的記錄項目`TagResource`從控制台創建文件系統的標籤時的操作。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": “111122223333”,
        "arn": "arn:aws:sts::111122223333:root”,
        "accountId": “111122223333”,
```

```
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE”,
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T22:36:07Z"
            }
        }
    },
    "eventTime": "2018-11-14T22:36:07Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": “192.0.2.0”,
    "userAgent": “console.amazonaws.com”,
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789”
    },
    "responseElements": null,
    "requestID": “aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51”,
    "eventID": “bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p”,
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": “111122223333”
}
```

以下範例顯示 CloudTrail 示範的記錄項目UntagResource從主控台刪除檔案系統標籤時的動作。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": "111122223333",
        "arn": "arn:aws:sts::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T23:40:54Z"
            }
```

```
        }
    },
    "eventTime": "2018-11-14T23:40:54Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "UntagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789"
    },
    "responseElements": null,
    "requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
    "eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": "111122223333"
}
```

FSx 適用於 FSx for Windows File Server 效能

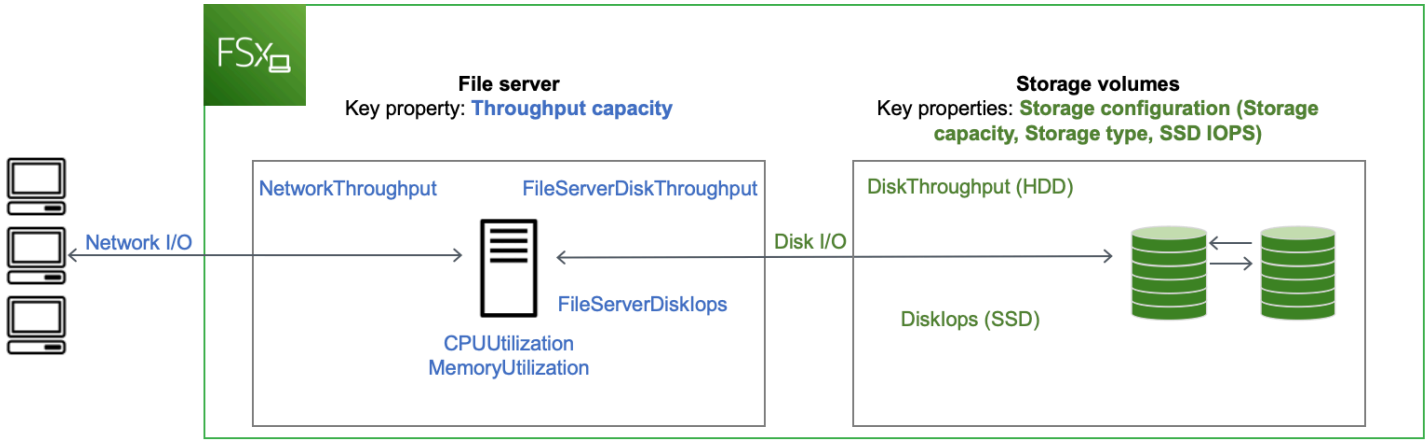
FSx for Windows File Server 提供檔案系統組態選項，以滿足各種效能需求。以下是 Amazon FSx 檔案系統效能的概觀，並討論可用的效能組態選項和有用的效能秘訣。

主題

檔案系統效能

Windows 檔案伺服器檔案系統的每個 FSx 都包含用戶端通訊的 Windows 檔案伺服器，以及連接至檔案伺服器的一組儲存磁碟區或磁碟。每個檔案伺服器都採用快速的記憶體內快取，以增強最常存取資料的效能。

下圖說明如何從 FSx 的 Windows 檔案伺服器檔案系統存取資料。



當用戶端存取儲存在記憶體內快取中的資料時，資料會以網路 I/O 的形式直接提供給要求的用戶端。檔案伺服器不需要從磁碟讀取或寫入磁碟。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 I/O 讀取或寫入磁碟。 然後，資料會以網路 I/O 的形式從檔案伺服器提供給從屬端。此資料存取的效能取決於網路 I/O 限制以及磁碟 I/O 限制。

網路 I/O 效能和檔案伺服器記憶體內快取是由檔案系統的輸送量容量決定。磁碟 I/O 效能由輸送量容量與儲存組態的組合決定。您的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) 是下列項目中較低的：

- 您的檔案伺服器所提供的磁碟 I/O 效能層級，視您為檔案系統選取的輸送量容量而定。
- 儲存組態所提供的磁碟 I/O 效能等級 (您為檔案系統選擇的儲存容量、儲存類型及 SSD IOPS 等級)。

其他效能考量

檔案系統效能通常是以其延遲、輸送量和每秒 I/O 作業數 (IOPS) 來衡量。

Latency (延遲)

FSx for Windows File Server 檔案伺服器採用快速的記憶體內快取，為主動存取的資料達到低於一毫秒的延遲。對於不在記憶體內快取中的資料，也就是說，對於需要透過在基礎儲存磁碟區執行 I/O 來處理的檔案操作，Amazon FSx 針對固態硬碟 (SSD) 儲存提供低於一毫秒的檔案操作延遲，以及硬碟機 (HDD) 儲存延遲 10 毫秒。

輸送量和 IOPS

Amazon FSx 檔案系統在提供 Amazon FSx 的所有位 AWS 區域 置提供高達 2 Gb/s 和 80,000 IOPS，以及在美國東部 (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 Gb/s 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 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 支援中小企業多通道。此功能可讓單一用戶端存取檔案系統，提供高達每秒 Gb/s 的

輸送量和數十萬個 IOPS。SMB 多通道在用戶端與伺服器之間同時使用多個網路連線，以彙總網路頻寬，達到最大的使用率。雖然 Windows 支援的 SMB 連線數目有理論上的限制，但這個限制是以百萬計，而且實際上您可以擁有無限數量的 SMB 連線。

爆裂性能

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

輸送量容量對效能的影響

輸送量容量決定下列類別中的檔案系統效能：

- 網路 I/O — 檔案伺服器可將檔案資料提供給存取檔案的用戶端的速度。
- 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 (例如重複資料刪除和陰影複製) 的資源。
- 磁碟 I/O — 檔案伺服器支援檔案伺服器與儲存磁碟區之間 I/O 的速度。

下表提供您可以使用每個佈建的輸送量容量組態來驅動的最大網路 I/O (輸送量和 IOPS) 層級 (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 (例如重複資料刪除和陰影複本) 的記憶體數量。雖然使用 Amazon FSx API 或 CLI 時，您可以選取低於每秒 32 MB (Mbps) 的輸送量容量層級，但請記住，這些等級適用於測試和開發工作負載，而非生產工作負載。

> **Note**
>
> 請注意，只有下列區域才支援 4,608 MBps 及更高的輸送量容量層級：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 與記憶體

FSx 輸送量容量 (百萬位元組/秒)	網路輸送量 (MB/秒)		網絡 IOPS	記憶體 (GB)
	基準線	爆裂（每天幾分鐘）		
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	–	百萬	192
6,144	12,500	–		256
9,216	18,750	–		384
12,288	21,250	–		512

磁碟 I/O

FSx 輸送量容量 (百萬位元組/秒)	磁碟輸送量 (每秒 MB)		磁碟 IOPS	
	基準線	爆裂（每天 30 分鐘）	基準線	爆裂（每天 30 分鐘）
32	32	260	2K	12 公里

FSx 輸送量容量 (百萬位元組/秒)	磁碟輸送量 (每秒 MB)		磁碟 IOPS	
64	64	350	4K	16 公里
128	128	600	6 公里	2 萬
256	256	600	10K	2 萬
512	512	–	2 萬	–
1,024	1,024	–	40K	–
2,048	2,048	–	八萬	–
4,608	4,608	–	150 萬	–
6,144	6,144	–	2 萬	–
9,216	9,216 [1]	–	三十	–
12,288	12,288 [1]	–	四十公里	–

> **Note**
>
> [1] 如果您擁有的異地同步備份檔案系統的輸送容量為 9,216 或 12,288 MBPS，則僅對於寫入流量，效能將限制為 9,000 MB 和 262,500 IOPS。否則，對於所有異地同步備份檔案系統上的讀取流量、所有單一可用區檔案系統上的讀取和寫入流量，以及所有其他輸送量容量層級，您的檔案系統將支援表格中顯示的效能限制。

選擇正確的輸送量容量層級

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量，自動為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滿足大多數工作負載，但您可以選擇覆寫建議並選取特定數量的輸送量容量來滿足應用程式的需求。例如，如果您的工作負載需要驅動 1Gbps 的流量到您的檔案系統，您應該選取至少 1,024 Mbps 的輸送量容量。

在決定要設定的輸送量層級時，您也應該考慮計劃在檔案系統上啟用的功能。例如，啟用陰影複製可能需要將輸送量容量增加到預期工作負載的三倍，以確保檔案伺服器能夠維護具有可用 I/O 效能容量的陰影複製。如果啟用「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容量，並確保此記憶體容量足以容納您的資料大小。

您可以在建立輸送量容量之後隨時調整輸送量容量。如需詳細資訊，請參閱 管理輸送量容量。

您可以透過檢視 Amazon FSx 主控台的監控與效能 > 效能索引標籤，監控工作負載對檔案伺服器效能資源的使用率，並取得選擇輸送量容量的建議。我們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。對於異地同步備份檔案系統，我們也建議您測試在檔案系統維護、輸送量容量變更以及工作負載意外服務中斷期間發生的容錯移轉程序所造成的影響，以及確保您已佈建足夠的輸送量容量以避免這些事件期間的效能影響。如需詳細資訊，請參閱 存取 FSx for Windows File Server 測量結果的 FSx。

儲存組態對效能的影響

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層級。

您可以隨時增加儲存容量並擴充固態硬碟 IOPS。如需詳細資訊，請參閱 管理儲存容量 及 管理固態硬碟 IOPS。您也可以將文件系統從 HDD 存儲類型升級為 SSD 存儲類型。如需詳細資訊，請參閱 管理儲存區類型。

您的檔案系統提供下列預設的磁碟輸送量和 IOPS 層級：

儲存體類型	磁碟輸送量 (每 TiB 儲存體的 MBP)	磁碟 IOPS (每個儲存體 TiB 的 IOP)
SSD	750	三千 *
HDD	12 個基準線；80 個突發 (每個檔案系統最多可達 1 Gb/s)	12 條基線；80 次爆裂

> **Note**
>
> * 對於具有 SSD 儲存類型的檔案系統，您可以佈建額外的 IOPS，最大比例為每 GiB 500 IOPS 和每個檔案系統 400,000 IOPS。

硬碟爆裂效能

對於硬碟儲存磁碟區，Amazon FSx 使用突發儲存貯體模型來提高效能。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 硬碟磁碟區，突發輸送量限制為 80 Mb/s，儲存貯體以 12 Mb/s 充滿點數，並且最多可容納 1 TIB 價值的點數。

範例：儲存容量和輸送量容量

下列範例說明儲存容量和輸送量容量如何影響檔案系統效能。

配置 2 TiB HDD 儲存容量和 32 Mbps 輸送量容量的檔案系統具有下列輸送量等級：

- 網路輸送量 — 32 Mbps 的基準線和 600 Mbps 突增 (請參閱輸送量容量表格)
- 磁碟輸送量 — 24 Mbps 的基準線和 160 兆比特突發，這是以下中較低的：
  - 根據檔案系統的輸送量容量，檔案伺服器支援的磁碟輸送量層級為 32 Mbps 基準和 260 Mbps 突增
  - 根據儲存區類型和容量，儲存磁碟區所支援的磁碟輸送量層級為 24 Mbps 基準 (每 TB 12 Mbps * 2 TiB) 和 160 MBPS 突增 (每 TiB 80 Mbps * 2 TiB)

因此，存取檔案系統的工作負載將能夠為檔案伺服器內快取中的主動存取資料執行檔案作業執行的檔案作業提供高達 32 Mbps 的基準線和 600 MBPS 突發輸送量，例如，由於快取遺漏而需要一直進入磁碟的檔案作業，最多可驅動 24 Mbps 基準和 160 MBPS 成組分解輸送量。

使用指標衡 CloudWatch 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 監控指標 CloudWatch。

解決效能問題

如需疑難排解常見效能問題的說明，請參閱解決檔案系統效能問題。

Amazon FSx 演練

下面，您可以找到一些面向任務的演練，指導您完成各種流程。

主題

演練 1：開始使用的先決條件

在完成入門練習之前，您必須已經將基於 Microsoft Windows 的 Amazon EC2 實例加入到您的AWS Directory Service目錄。您還必須以目錄的管理員用户身份通過 Windows 遠程桌面協議登錄到實例。以下的逐步解説明如何執行這些必要的先決條件操作。

主題

步驟 1：設置活動目錄

藉助 Amazon FSX，您可以為基於 Windows 的工作負載操作完全託管的文件存儲。同樣,AWS Directory Service提供用於工作負載部署的完全託管目錄。如果您有一個現有的公司 AD 域在AWS在使用 EC2 執行個體的虛擬私有雲端 (VPC) 中，您可以啟用基於使用者的身份驗證和訪問控制。您可以通過建立您之間的信任關係來執行個體AWS託管的微軟 AD 和您的公司域。對於 Amazon FSX 中的 Windows 身份驗證，您只需要單向林信任，其中AWS託管林信任公司域林。

您的公司域將擔任受信任域的角色，並且AWS Directory Service託管域接受信任域的角色。經過驗證的身份驗證請求僅在一個方向之間傳輸 — 允許公司域中的帳户根據託管域中共享的資源進行身份驗證。在這種情況下，Amazon FSX 僅與受管網域進行交互。然後，託管域將身份驗證請求傳遞到您的公司域。

> **Note**
>
> 您還可以將外部信任類型與 Amazon FSX 用於受信任域。

您的活動目錄安全組必須啟用來自 Amazon FSX 文件系統安全組的入站訪問。

建立AWS適用於 Microsoft AD 的目錄服務

- 如果您還沒有帳體，請使用AWS Directory Service建立您的AWS受管 Microsoft AD 目錄。如需詳細資訊，請參閱「」建立您的AWS受管 Microsoft AD 目錄中的AWS Directory Service管理指南。

  > **Important**
  >
  > 記住您分配給 Admin 用户的密碼；在本入門練習中稍後需要密碼。如果忘記密碼，則需要重複本練習中的步驟，使用新的AWS Directory Service目錄和管理員用户。

- 如果您擁有現有 AD，請在AWS託管微軟廣告和您現有的廣告。如需詳細資訊，請參閱「」建立信任關係的時機中的AWS Directory Service管理指南。

步驟 2：在 Amazon EC2 主控台中啟動 Windows 執行個體

您可以使用AWS Management Console如下列程序所述。這是為了幫助您快速啟動您的第一個執行個體，所以不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。選擇適用於 Windows Server 2016 Base 或 Windows Server 2012 R2 Base 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. 在檢閱執行個體的啟動頁面，在安全群組時，將顯示嚮導為您創建並選定的安全組。您可使用此安全組，或者使用下列步選取您在設定時建立的安全組：

   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。(如果隱藏 Public DNS (IPv4) (公有 DNS (IPv4)) 欄，請選擇頁面右上角的 Show/Hide Columns (顯示/隱藏欄) (齒輪狀圖示)，然後選取 Public DNS (IPv4) (公有 DNS (IPv4))。)
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**
>
> 請記下您在啟動此執行個體時建立的安全組的 ID。在建立 Amazon FSx 文件系統時會需要用到。

現在，您的執行個體已啟動，即可連線至您的執行個體。

步驟 3：連接至您的執行個體

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，對於英文來說，它是 Administrator，對於法文來說，它是 Admini戰略員，對於葡萄牙文來說，它是 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。

如果您將執行個體加入網域，則可以使用AWS Directory Service。在遠程桌面登錄屏幕上，不要使用本地計算機名稱和生成的密碼。而是使用管理員的完全限定用户名和此帳户的密碼。例如，**`corp.example.com\Admin`**。

Windows Server 操作系統 (OS) 的授權允許為了管理用途而同時有兩個遠端連線。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「」配置連接允許的同時遠程連接數。

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，然後選擇 Connect (連線)。
2. 在 中連結到您的執行個體對話方塊中，選擇取得密碼(在執行個體啟動後，需要幾分鐘的時間才能提供密碼)。
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)。主控台會在連結到您的執行個體對話框中，替換到取得密碼之前顯示的實際密碼。
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Close (關閉)以解除連結到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，選擇 Actions (動作)，然後選擇 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。

現在您已連接到您的實例，您可以將實例加入您的AWS Directory Service目錄。

步驟 4：將您的實例加入到您的AWS Directory Servicedirectory

以下程序示範如何將現有 Amazon EC2 Windows 執行個體手動加入您的AWS Directory Service目錄。

若要將 Windows 執行個體加入您的AWS Directory Servicedirectory

1. 使用任何遠端桌面協定用戶端連線到執行個體。
2. 在執行個體上開啟 TCP/IPv4 屬性內容對話方塊。
   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 (右鍵) 菜單，然後選擇屬性。
   c. 在連線內容對話方塊中，開啟 (按兩下) Internet Protocol Version 4 (網際網路協定第 4 版)。
3. (選用) 選擇使用下列 DNS 伺服器地址，請更改慣用 DNS 伺服器和其他 DNS 伺服器地址設置為AWS Directory Service提供的 DNS 服務器，然後選擇確定。
4. 開啟系統屬性對話框中，選擇計算機名稱選項卡，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 中成員方塊中，選擇網域，輸入您的AWS Directory Service目錄，然後選擇確定。
6. 當提示您輸入網域管理員的名稱和密碼時，輸入 Admin 帳戶的使用者名稱和密碼。

> **Note**
>
> 您可以輸入域的完全限定名稱或 NetBios 名稱，後面接着反斜線 (\)，接着使用者名稱 (在本例中為管理員。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. 通過 RDP 重新連線至您的執行個體，並使用AWS Directory Service目錄的管理員用户。

現在，您的執行個體已加入網域，即可建立 Amazon FSx 文件系統。然後，您可以繼續完成入門練習中的其他任務。如需詳細資訊，請參閱開始使用適用於 FSx for Windows File Server 的 Amazon FSx。

演練 2：從備份建立檔案系統

使用 Amazon FSx，您可以從備份建立檔案系統。執行此操作時，您可以更改以下任何元素，以更好地適應新創建的文件系統的使用案例：

- 儲存體類型
- 吞吐量容量
- VPC
- 可用區域
- Subnet (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
- 每週維護視窗

以下程序將帶您演練使用備份建立新檔案系統的過程。建立此檔案系統前，您必須擁有現有備份。如需詳細資訊，請參閱「」使用備份

從現有備份建立檔案系統

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

2. 從右側的導航列表中，選擇備份。
3. 從儀錶板上的表格中，選擇要用於創建新文件系統的備份。

> **Note**
>
> 您只能將備份還原到與原始存儲容量相同的文件系統。您可以在恢復的文件系統的存儲容量變為可用後增加其存儲容量。如需詳細資訊，請參閱 管理儲存容量。

4. 選擇 Restore backup (還原備份)。這將開始創建文件系統嚮導。
5. 選擇要為此新文件系統更改的設置。存儲類型設置為SSD，但您可以變更改為HDD在以下條件下：
   - 檔案系統部署類型為異地同步備份或者單一可用區 2。
   - 存儲容量至少為 2,000 GiB。
6. 選擇審核摘要以在創建文件系統之前查看您的設置。
7. 選擇 Create file system (建立檔案系統)。

現在，您已成功從現有備份建立新檔案系統。

演練 3：更新現有的檔案系統

您可以使用本演練中的過程更新三個元素。您可以從控制台執行更新的所有其他文件系統元素。這些過程假定您有AWS CLI在本機電腦上安裝和配置的。如需詳細資訊，請參閱「」安裝和設定中的AWS Command Line Interface使用者指南。

- AutomaticBackupRetentionDays— 您想要為您的文件系統保留自動備份的天數。
- DailyAutomaticBackupStartTime— 您想要開始每日自動備份時段 (國際標準時間 (UTC)) 的時間。窗口從此指定時間開始 30 分鐘。此時段不可與每週維護備份時段重疊。
- WeeklyMaintenanceStartTime– 您希望維護時段開始的一週中的時間。第 1 天為星期一，2 為星期二，依此類推。窗口從此指定時間開始 30 分鐘。此時段不可與每日自動備份時段重疊。

以下過程概述瞭如何使用AWS CLI。

更新為文件系統保留自動備份的時間

1. 在您的電腦上開啟命令提示字元或終端機。

2. 運行以下命令，將文件系統 ID 替換為文件系統的 ID，以及要保留自動備份的天數。

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration AutomaticBackupRetentionDays=30
```

更新文件系統的每日備份窗口

1. 在您的電腦上開啟命令提示字元或終端機。
2. 運行以下命令，將文件系統 ID 替換為文件系統的 ID，並將時間替換為您希望開始窗口的時間。

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration DailyAutomaticBackupStartTime=01:00
```

更新文件系統的每週維護時段

1. 在您的電腦上開啟命令提示字元或終端機。
2. 運行以下命令，將文件系統 ID 替換為文件系統的 ID，將日期和時間替換為要開始窗口的時間。

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration WeeklyMaintenanceStartTime=1:01:30
```

逐步解說 4：使用亞馬遜 FSx 與亞馬遜 AppStream 2.0

Amazon FSx FSx for Windows File Server 支援伺服器訊息區 (SMB) 通訊協定，支援從 Amazon EC2、VMware 雲端、亞馬遜和亞馬遜 WorkSpaces AppStream 2.0 執行個體存取您的檔案系統。AWS AppStream 2.0 是完全受控的應用程式串流服務。您可以在 AppStream 2.0 上集中管理桌面應用程式，並將其安全地傳送至任何電腦上的瀏覽器。如需 AppStream 2.0 的詳細資訊，請參閱亞馬遜 AppStream 2.0 管理指南。如需有關如何簡化 Amazon AppStream 2.0 映像和叢集管理的指示，請參閱AWS部落格文章：自動建立自訂的 AppStream 2.0 Windows 映像。

使用本逐步解說做為指南，說明如何在兩種使用案例中使用 Amazon FSx 和 AppStream 2.0：為每個使用者提供個人永久儲存，並為使用者提供共用資料夾以存取常見檔案。

為每個用戶提供個人持久性存儲

您可以使用 Amazon FSx 在 AppStream 2.0 個串流工作階段內為組織中的每個使用者提供唯一的儲存磁碟機。使用者將擁有僅存取其資料夾的權限。磁碟機會在串流工作階段開始時自動掛載，而新增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工作。

若要使用 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，請參閱開始使用適用於 FSx for Windows File Server 的 Amazon FSx。
2. 檔案系統可用之後，請為 Amazon FSx 檔案系統中的每個網域 AppStream 2.0 使用者建立一個資料夾。下列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。這樣做表示您可以建立檔案共用的 UNC 名稱，以便使用 Windows 環境變數輕鬆對應`%username%`。
3. 以共用資料夾的形式分享這些資料夾。如需詳細資訊，請參閱管理 FSx 上適用於 Windows 檔案伺服器檔案系統的檔案共用。

啟動加入網域的 AppStream 2.0 映像產生器

1. 登入 AppStream 2.0 主控台：https://console.aws.amazon.com/appstream2
2. 從導覽功能表選擇「目錄組態」，然後建立「目錄組 Config」物件。如需詳細資訊，請參閱《亞馬遜 AppStream 2.0 管理指南》中的〈搭配 AppStream 2.0 使用活動目錄〉。
3. 選擇 [影像]、[Image Builder]，然後啟動新的映像建立器。
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 Active Directory 網域。
5. 在您 Amazon FSx 檔案系統中使用相同的 VPC 中啟動映像建置器。請務必將映像產生器與 Amazon FSx 檔案系統加入的相同AWS Managed Microsoft AD目錄建立關聯。與映像產生器關聯的 VPC 安全群組必須允許存取 Amazon FSx 檔案系統。
6. 映像產生器可用後，請連線至映像產生器，並使用您的網域管理員帳戶登入。
7. 安裝您的應用程式。

將亞馬遜 FSx 文件共享與 AppStream 2.0 鏈接

1. 在映像產生器中，使用下列命令建立批次指令碼，並將其儲存在已知的檔案位置 (例如：C:\Scripts\map-fs.bat)。下列範例使用 S: 做為磁碟機代號，以對應 Amazon FSx 檔案系統上的共用資料

夾。您可以使用 Amazon FSx 檔案系統的 DNS 名稱，或與此指令碼中的檔案系統相關聯的 DNS 別名，您可以從 Amazon FSx 主控台的檔案系統詳細資料檢視中取得該別名。

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. 打開一個 PowerShell 提示並運行`gpedit.msc`。
3. 從使用者組態選擇 Windows 設定，然後選擇登入。
4. 瀏覽您在此程序的第一個步驟中建立的批次指令碼。
5. 從 [電腦設定] 中，選擇 [Windows 系統管理範本]、[系統]，然後選取 [群組
6. 選擇「設定登入指令碼延遲」原則。啟用原則並將延遲時間縮短至`0`。此設定有助於確保使用者啟動串流工作階段時，會立即執行使用者登入指令碼。
7. 建立映像並將其指派給 AppStream 2.0 叢集。請確定您也將 AppStream 2.0 叢集加入到您用於映像產生器的相同 Active Directory 網域。在您 Amazon FSx 檔案系統所使用的相同 VPC 中啟動叢集。與叢集關聯的 VPC 安全群組必須提供對 Amazon FSx 檔案系統的存取權。
8. 使用 SAML SSO 啟動串流工作階段。若要連線至已加入 Active Directory 的叢集，請使用 SAML 提供者設定單一登入同盟。如需詳細資訊，請參閱《Amazon AppStream 2.0 管理指南》中的使用 SAML 2.0 進行單一登入存取 AppStream 2.0。
9. 您的 Amazon FSx 檔案共用會對應至串流工作階段中的 S: 磁碟機代號。

跨使用者提供共用資料夾

您可以使用 Amazon FSx 提供共用資料夾給組織中的使用者。共用資料夾可用來維護所有使用者所需的一般檔案 (例如示範檔案、程式碼範例、說明手冊等)。

您需要執行三個程序才能完成此工作。

使用亞馬遜 FSx 創建共享文件夾

1. 建立 Amazon FSx 檔案系統。如需詳細資訊，請參閱開始使用適用於 FSx for Windows File Server 的 Amazon FSx。
2. 在預設情況下，每個 Amazon FSx 檔案系統都包含一個共用資料夾，您可以使用位址\\ *#### DNS ##*\ 共用或\\ *FQDN-* DNS-別名\ 共用 (如果您使用 DNS 別名) 來存取該資料夾。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，請參閱管理 FSx 上適用於 Windows 檔案伺服器檔案系統的檔案共用。

若要啟動 AppStream 2.0 映像建立器

1. 從 AppStream 2.0 主控台啟動新的映像產生器，或連線至現有的映像產生器。在 Amazon FSx 檔案系統所使用的相同 VPC 中啟動映像產生器。與映像產生器關聯的 VPC 安全群組必須允許存取 Amazon FSx 檔案系統。
2. 映像產生器可用後，請以管理員使用者身分連線至映像產生器。
3. 以管理員身份安裝或更新應用程式。

將共享資料夾與 AppStream 2.0 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 主控台的檔案系統詳細資料檢視中取得)，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. 建立群組原則，以便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描述的相同指示。
3. 建立映像並將其指派給您的叢集。
4. 啟動串流工作階段。現在，您應該會看到自動映射到驅動器號的共享文件夾。

逐步解說 5：使用 DNS 別名存取您的檔案系統

FSx for Windows File Server 每個可用來存取檔案系統資料的檔案系統提供預設的網域名稱系統 (DNS) 名稱。您也可以使用您選擇的 DNS 別名來存取檔案系統。透過 DNS 別名，您可以在將檔案系統儲存從現場部署遷移到 Amazon FSx 時，繼續使用現有的 DNS 名稱存取儲存在 Amazon FSx 上的資料，而無需更新任何工具或應用程式。您一次最多可以將 50 個 DNS 別名與檔案系統建立關聯。

若要使用 DNS 別名存取 Amazon FSx 檔案系統，您必須執行以下三個步驟：

1. 將 DNS 別名與您的 Amazon FSx 檔案系統建立關聯。
2. 設定檔案系統電腦物件的服務主體名稱 (SPN)。使用 DNS 別名存取您的檔案系統時，需要這麼做才能取得 Kerberos 驗證。)
3. 更新或建立檔案系統和 DNS 別名的 DNS CNAME 記錄。

主題

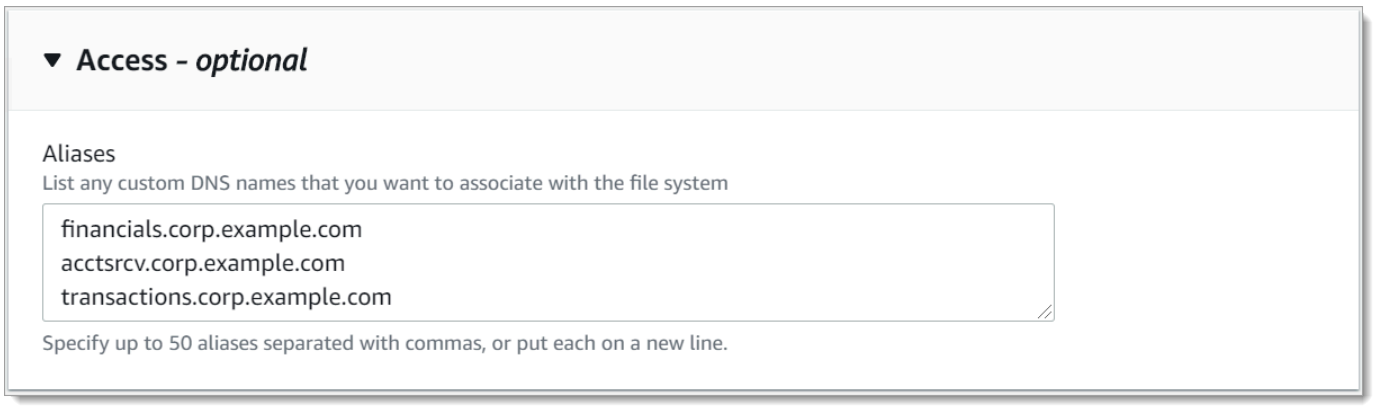
步驟 1：將 DNS 別名與您的 Amazon FSx 檔案系統建立關聯

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 FSx 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 (包括父網域) 以建立別名關聯。

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資訊，以及有關使用 CLI 和 API 的詳細資訊，請參閱管理 DNS 別名。

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

2. 依照〈入門〉一節中所述，建立新檔案系統建立您的檔案系統的程序進行。
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，請遵循下列準則：

- 必須格式化為完整網域名稱 (FQDN)*hostname.domain*，例如。`accounting.example.com`
- 可以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。

   當您的新檔案系統可用時，請繼續執行步驟 2。

步驟 2：設定 Kerberos 的服務主體名稱 (SPN)

我們建議您在傳輸過程中使用 Kerberos 型身份驗證和加密搭配 Amazon FSx。Kerberos 為存取檔案系統的用戶端提供最安全的驗證。

若要為使用 DNS 別名存取 Amazon FSx 的用戶端啟用 Kerberos 身份驗證，您必須新增服務主體名稱 (SPN)，這些名稱與 Amazon FSx 檔案系統的作用中目錄電腦物件上的 DNS 別名相對應。SPN 一次

只能與單一作用中目錄電腦物件相關聯。如果您已針對原始檔案系統的 Active Directory 電腦物件設定 DNS 名稱的現有 SPN，則必須先刪除它們。

Kerberos 驗證有兩個必要的 SPN：

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

如果別名是`finance.domain.com`，下列是兩個必要的 SPN：

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

> **Note**
>
> 在為 Amazon FSx 檔案系統的活動目錄 (AD) 電腦物件建立新的主機 SPN 之前，您必須先刪除與活動目錄電腦物件上 DNS 別名相對應的任何現有主機 SPN。如果 AD 中存在 DNS 別名的 SPN，嘗試為 Amazon FSx 檔案系統設定 SPN 將會失敗。

下列程序說明如何執行下列作業：

- 在原始檔案系統的作用中目錄電腦物件上尋找任何現有的 DNS 別名 SPN。
- 刪除找到的現有 SPN (如果有的話)。
- 為您的 Amazon FSx 檔案系統的作用中目錄電腦物件建立新的 DNS 別名 SPN。

若要安裝所需的 PowerShell 使用中目錄模組

1. 登入加入 Amazon FSx 檔案系統所加入的作用中目錄的 Windows 執行個體。
2. PowerShell 以管理員身份打開。
3. 使用以下命令安裝 PowerShell 活動目錄模塊。

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

尋找和刪除原始檔案系統的作用中目錄電腦物件上現有的 DNS 別名 SPN

1. 使用下列命令尋找任何現有的 SPN。以您在步驟 1 中*alias_fqdn*與檔案系統相關聯的 DNS 別名取代。

```
## 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 SPN。

   - 以您在步驟 1 中*alias_fqdn*與檔案系統相關聯的完整 DNS 別名取代。
   - *file_system_DNS_name*以原始檔案系統的 DNS 名稱取代。

```
## 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 檔案系統的作用中目錄電腦物件上設定 SPN

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

   - 以 Amazon FSx 指派給檔案系統的 DNS 名稱取*file_system_DNS_name*代。

     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]，選擇您的檔案系統，然後在檔案系統詳細資料頁面上選擇 [網路和安全性] 窗格。

     您也可以在DescribeFile系統 API 作業的回應中取得 DNS 名稱。
   - 以您在步驟 1 中*alias_fqdn*與檔案系統相關聯的完整 DNS 別名取代。

```
## 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 one of the following commands, not both:
Set-AdComputer -Identity $FSxAdComputer -Add @{"msDS-
AdditionalDnsHostname"="$Alias"}
##Or
SetSpn /S ("HOST/" + $Alias.Split('.')[0]) $FSxAdComputer.Name
SetSpn /S ("HOST/" + $Alias) $FSxAdComputer.Name
```

> **Note**
>
> 如果原始檔案系統電腦物件的 AD 中存在 DNS 別名的 SPN，則為您的 Amazon FSx 檔案系統設定 SPN 將會失敗。如需尋找和刪除現有 SPN 的資訊，請參閱尋找和刪除原始檔案系統的作用中目錄電腦物件上現有的 DNS 別名 SPN。

2. 使用下列範例指令碼確認已針對 DNS 別名設定新 SPN。請確定回應包含兩個 HOST SPN，以HOST/*alias*及HOST/*alias_fqdn*，如本程序先前所述。

   取代*file_system_DNS_name*為 Amazon FSx 指派給您檔案系統的 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]，選擇您的檔案系統，然後在檔案系統詳細資料頁面上選擇 [網路和安全性] 窗格。

   您也可以在DescribeFile系統 API 作業的回應中取得 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。

如需有關如何強制用戶端在連線至 Amazon FSx 檔案系統時使用 Kerberos 身份驗證和加密的詳細資訊，請參閱。使用 GPO 強制執行 Kerberos 驗證

步驟 3：更新或建立檔案系統的 DNS CNAME 記錄

為檔案系統正確設定 SPN 之後，您可以將解析為原始檔案系統的每個 DNS 記錄取代解析為原始檔案系統的 DNS 記錄，以解析為 Amazon FSx 檔案系統預設 DNS 名稱的 DNS 記錄來切換為 Amazon FSx。

若要執行本節中提供的指令，必須使用`dnsserver`和 `activedirectory` Windows 模組。

若要安裝必要的 PowerShell 指令程式

1. 登入加入 Active Directory 的 Windows 執行個體，您的 Amazon FSx 檔案系統所加入的使用者身分屬於具有 DNS 管理權限的群組成員 (AWS 受管 Active Directory 中的AWSAWS 委派網域名稱系統管理員，以及您已在自我管理 Active Directory 中委派 DNS 管理權限的其他群組)。

   如需詳細資訊，請參閱 Amazon EC2 使用者指南中的連線到 Windows 執行個體。
2. PowerShell 以管理員身份打開。
3. 需要 PowerShell DNS 伺服器模組才能執行此程序中的指示。使用以下命令安裝它。

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

更新或建立您的 Amazon FSx 檔案系統的自訂 DNS 名稱

1. 以具有 DNS 管理權限 (受管 Active Directory 中的AWS 委派網域名稱系統管理員，以及您已在自我 AWS 管理 Active Directory 中委派 DNS 管理權限的網域管理員或其他群組) 的使用者身分 Connect 線至 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到 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 記錄移轉至您的 Amazon FSx 檔案系統。如果找不到任何項目，它會為解析為 Amazon FSx 檔案系統預設 DNS 名稱的 DNS 別*alias_fqdn*名建立新的 DNS CNAME 記錄。

   執行指令碼：

   - 以您*alias_fqdn*與檔案系統相關聯的 DNS 別名取代。
   - 替換*file_system_DNS_name*為 Amazon FSx 已分配給文件系統的 DNS 名稱。

```
$Alias="alias_fqdn"
$FSxDnsName="file_system_dns_name"
$AliasHost=$Alias.Split('.')[0]
$ZoneName=((Get-WmiObject Win32_ComputerSystem).Domain)
$DnsServerComputerName = (Resolve-DnsName $ZoneName -Type NS | Where Type -eq 'A' |
 Select -ExpandProperty Name) | Select -First 1
foreach ($computer in $DnsServerComputerName)
{
Add-DnsServerResourceRecordCName -Name $AliasHost -ComputerName $computer -
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 別名重複上一個步驟。

您現在已經為您的 Amazon FSx 檔案系統新增了 DNS CNAME 值，其中包含 DNS 別名。您現在可以使用 DNS 別名來存取您的資料。

> **Note**
>
> 當更新 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，用戶端可能在短時間內無法與檔案系統連線。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 GPO 強制執行 Kerberos 驗證

您可以在存取檔案系統時強制執行 Kerberos 驗證，方法是在您的作用中目錄中設定下列群組原則物件 (GPO)：

- 限制 NTLM：遠端伺服器的外寄 NTLM 流量-使用此原則設定可拒絕或稽核從電腦到執行 Windows 作業系統之任何遠端伺服器的傳出 NTLM 流量。
- 限制 NTLM：新增 NTLM 驗證的遠端伺服器例外-如果網路安全性：限制 NTLM：已設定遠端伺服器的外寄 NTLM 流量原則設定，請使用此原則設定，建立允許用戶端裝置使用 NTLM 驗證的例外清單。

1. 登入加入作用中目錄的 Windows 執行個體，您的 Amazon FSx 檔案系統是以管理員身分加入的目錄。如果您要設定自我管理的作用中目錄，請將這些步驟直接套用至您的作用中目錄。

2. 選擇 [開始]、[系統管理工具]，然後選擇 [群組原則管理]。
3. 選擇群組原則物件。
4. 如果您的群組原則物件不存在，請建立它。
5. 找出現有的網路安全性：限制 NTLM：遠端伺服器的外寄 NTLM 流量原則。(如果沒有現有策略，請建立新策略。) 在 [本機安全性設定] 索引標籤中，開啟內容 (按一下滑鼠右鍵) 選單，然後選擇 [內容
6. 選擇 [全部拒絕]。
7. 選擇「套用」以儲存安全性設定。
8. 若要為用戶端的特定遠端伺服器設定 NTLM 連線的例外狀況，請找出「網路安全性：限制 NTLM：新增遠端伺服器例外」。

   打開上下文（右鍵單擊）菜單，然後在本地安全性設置選項卡中選擇屬性。
9. 輸入要新增至例外清單的任何伺服器的名稱。
10. 選擇「套用」以儲存安全性設定。

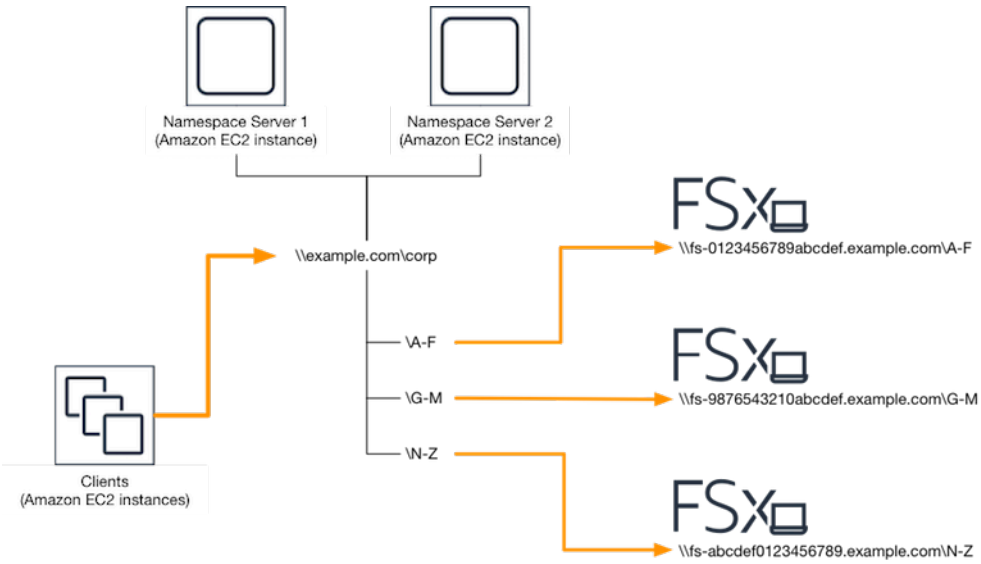
逐步解說 6：使用碎片擴展效能

Amazon FSx for Windows File Server 支持使用 Microsoft 分佈式文件系統（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，向外擴展效能 (讀取和寫入) 以處理 I/O 密集型工作負載。同時，您仍然可以在通用命名空間下向應用程式呈現統一檢視。此解決方案涉及將檔案資料分割成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 parallel 個體存取資料的應用程式可以同時讀取和寫入這些碎片，以達到高等級的效能。

當您的工作負載需要對檔案資料進行均勻分佈的讀取/寫入存取權時 (例如，如果每個計算執行個體子集存取檔案資料的不同部分)，您可以使用此解決方案。

為向外延展效能設定 DFS 命名空間

下列程序會引導您在 Amazon FSx 上建立 DFS 解決方案，以獲得向外擴充效能。在此範例中，儲存在 *corp* 命名空間中的資料會依字母順序分割。數據文件「A-F」，「G-M」和「N-Z」都存儲在不同的文件共享中。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用之間最佳分片資料。選擇一種分割慣例，將 I/O 平均分配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 個檔案共用和數百 PB 的儲存容量。



若要為向外延展效能設定 DFS 命名空間

1. 如果您尚未執行 DFS 命名空間伺服器，您可以啟動一對使用設定 -DFSN-SERVER.Tem AWS CloudFormation plate 範本的高可用性 DFS 命名空間伺服器。如需有關建立 AWS CloudFormation 堆疊的詳細資訊，請參閱《使用指南》中的〈在 AWS CloudFormation 主控台上建立堆疊AWS CloudFormation〉。
2. Connect 至上一個步驟中以「AWS 委派管理員」群組中的使用者身分啟動的其中一個 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到 Windows 執行個體。
3. 存取 DFS 管理主控台。開啟 [開始] 功能表並執行 [開始]。這會開啟 DFS 管理 GUI 工具。
4. 選擇動作，然後選擇新增命名空間，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. 在 [名稱] 中，輸入您要建立的命名空間 (例如 corp)。
6. 選擇 「編輯設定」，然後根據您的需求設定適當的權限。選擇下一步。
7. 保持預設以網域為基礎的命名空間選項保持選取狀態，保持選取啟用 Windows Server 2008 模式選項，然後選擇下一步。

   > **Note**
   >
   > 視窗伺服器 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後，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權限，然後選擇「確定」。
12. 開啟剛建立之命名空間的內容 (按一下滑鼠右鍵) 選單，選擇「新增資料夾」，輸入第一個碎片的資料夾名稱 (例如，針對「名稱」)，A-F然後選擇「新增」。
13. 在裝載此碎片的檔案共用的 DNS 名稱中，以 UNC 格式輸入資料夾目標的路徑，**\\fs-0123456789abcdef0.example.com\A-F**然後選擇確定。
14. 如果共用不存在：
    a. 選擇 [是] 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$ 底下建立新資料夾，然後選擇「確定」。
    d. 設定適當的共用權限，然後選擇 [確定]。
15. 現在為碎片新增資料夾目標後，選擇 [確定]。
16. 對要添加到相同命名空間的其他碎片重複最後四個步驟。

演練 7：複製備份到其他AWS 區域

使用 Amazon FSX，您可以將現有備份複製到同一AWS 帳戶到另一個AWS 區域（跨區域備份副本）或相同AWS 區域（區域內備份副本）。

下列程序會逐步解決如何在同一個AWS 帳戶。您必須具有現有備份，然後才能創建此備份副本。如需詳細資訊，請參閱 使用備份。

複製位於同一個AWS 帳戶（跨區域或區域內）

1. 開啟位於的 Amazon FSx 主控台https://console.aws.amazon.com/fsx/。
2. 在導覽窗格中，選擇 Backups (備份)。
3. 在 中備份表中，選擇您想要複製的備份。
4. 選擇 Copy backup (複製備份)。執行此操作會打開複製備份嚮導。
5. 在 中目的地區域列表中，選擇目標AWS 區域將備份複製到。目的地可以位於其他AWS 區域或在同一AWS 區域。
6. (選用) 選擇複製標籤將標籤從源備份複製到目標備份。如果您選擇複製標籤並在步驟 8 中添加標籤，所有標籤都將被合併。
7. 適用於Encryption (加密)中，選擇AWS KMS加密密鑰來加密複製的備份。
8. 適用於標籤-選用中，輸入密鑰和值以為複製備份添加標籤。如果您在此處添加標籤，並且還選擇複製標籤，則將合併所有標籤。

9. 選擇 Copy backup (複製備份)。

現在，您已成功地將備份複製到同一AWS 帳戶到另一個AWS 區域或在同一AWS 區域。

Amazon FSx 中的安全

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，該架構專為滿足對安全性最敏感的組織的需求而打造。

安全是 AWS 與您之間共同承擔的責任。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 網路 AWS 服務雲端中執行服務的基礎設施。 AWS 還為您提供可以安全使用的服務。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 Windows 檔案伺服器之 Amazon FSx 的合規計劃，請參閱合規計劃的AWS 服務範圍。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您瞭解如何在使用適用於 Windows 檔案伺服器的 Amazon FSx 時套用共同的責任模型。下列主題說明如何設定 Amazon FSx 以符合安全和合規目標。您也會學到如何使用其他可協助您監控和保護 Windows 檔案伺 AWS 服器專用 Amazon FSx 資源的服務。

主題

- Amazon FSx 中的數據加密
- 使用視窗 ACL 的檔案和資料夾層級存取控制
- 使用 Amazon VPC 進行檔案系統存取控制
- 適用於 Windows 檔案伺服器的 Amazon FSx 的 Identity and Access Management
- 適用於 FSx for Windows File Server 的 Amazon FSx 合規驗證
- Amazon FSx for Windows File Server 和界面 VPC 端點

Amazon FSx 中的數據加密

Amazon FSx for Windows File Server 支援兩種形式的檔案系統加密：傳輸中的資料加密和靜態加密。對應於支援 SMB 通訊協定 3.0 或更新版本的運算執行個體上的檔案共用，支援傳輸中的資料加密。建立 Amazon FSx 檔案系統時，系統會自動啟用靜態資料加密。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，而無需修改應用程式。

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。

如需使用適用於 Windows 檔案伺服器的 Amazon FSx 加密的詳細資訊，請參閱下列相關主題：

- 建立您的 FSx for Windows File Server 檔案系統的 Amazon FSx
- IAM 使用者指南中適用於 Amazon FSx 的動作、資源和條件金鑰

主題

- 靜態加密
- 傳輸中加密

靜態加密

所有 Amazon FSx 檔案系統都會使用 AWS Key Management Service (AWS KMS) 管理的金鑰在靜態時進行加密。數據在寫入文件系統之前會自動加密，並在讀取時自動解密數據。Amazon FSx 會透明地處理這些程序，因此您不必修改應用程式。

Amazon FSx 使用業界標準的 AES-256 加密演算法來加密 Amazon FSx 資料和靜態中繼資料。如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的密碼編譯基礎。

> **Note**
>
> AWS 金鑰管理基礎架構使用聯邦資訊處理標準 (FIPS) 140-2 核准的加密演算法。基礎設施符合國家標準技術研究所 (NIST) 800-57 的建議。

Amazon FSx 如何使用 AWS KMS

Amazon FSx 與 AWS KMS 金鑰管理整合。Amazon FSx 會使用一個 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 (包括資料和中繼資料) 的 KMS 金鑰。您可以啟用、停用或撤銷此 KMS 金鑰的授權。此 KMS 金鑰可以是下列兩種類型之一：

- AWS 受管金鑰— 這是默認的 KMS 密鑰，並且可以免費使用。

- 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，您可以啟用金鑰輪替。啟用金鑰輪換時， AWS KMS 每年會自動輪換金鑰一次。此外，使用客戶受管金鑰時，您可以隨時選擇停用、重新啟用、刪除或撤銷 KMS 金鑰存取權的時間。如需詳細資訊，請參閱 AWS Key Management Service 開發人員指南 AWS KMS keys中的旋轉。

靜態檔案系統加密和解密會以透明方式處理。不過，Amazon FSx 專屬的 AWS 帳戶 ID 會出現在與 AWS KMS 動作相關的 AWS CloudTrail 日誌中。

Amazon FSx 關鍵政策 AWS KMS

金鑰政策是控制對 KMS 金鑰之存取的主要方式。如需關鍵原則的詳細資訊，請參閱AWS Key Management Service 開發人員指南AWS KMS中的使用金鑰政策。下列清單說明 Amazon FSx 針對靜態檔案系統加密支援的所有 AWS KMS相關許可：

- kms:Encrypt：(選用) 將純文字加密為加密文字。此許可會納入預設的金鑰政策中。
- kms:Decrypt：(必要) 對密文進行解密。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，而不會在用戶端公開資料的純文字。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：GenerateDataKeyWithout純文字 — (必要) 傳回以 KMS 金鑰加密的資料加密金鑰。此權限包含在 kms: K GenerateData ey* 下的預設金鑰原則中。
- kms: CreateGrant — (必要) 將授權新增至金鑰，以指定誰可以使用金鑰，以及在何種情況下可以使用金鑰。授予是金鑰政策的備用許可機制。如需有關贈款的詳細資訊，請參閱AWS Key Management Service 開發人員指南中的使用贈款。此許可會納入預設的金鑰政策中。
- kms: DescribeKey — (必要) 提供有關指定 KMS 金鑰的詳細資訊。此許可會納入預設的金鑰政策中。
- kms: ListAliases — (選用) 列出帳戶中的所有金鑰別名。當您使用主控台建立加密的檔案系統時，此權限會填入 KMS 金鑰清單。我們建議您使用此許可，以提供最佳使用者體驗。此許可會納入預設的金鑰政策中。

傳輸中加密

對應於支援 SMB 通訊協定 3.0 或更新版本的運算執行個體上的檔案共用，支援傳輸中的資料加密。這包括所有從視窗伺服器 2012 和視窗 8 開始的視窗版本，以及所有使用 Samba 用戶端版本 4.2 或更新版本的 Linux 用戶端。當您存取檔案系統時，Amazon FSx 檔案伺服器會使用 SMB 加密自動加密傳輸中的資料，而無需修改應用程式。

中小企業加密會使用 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 工作階段金鑰進行簽署，藉此提供資料完整性。例如，透過加密的 SMB 連線複製大型檔案時，使用 AES-128-GCM 可提升效能提升 2 倍。

為了符合永遠加密的合規需求 data-in-transit，您可以將檔案系統存取限制為僅允許存取支援 SMB 加密的用戶端。您也可以啟用或停用每個檔案共用或整個檔案系統的傳輸中加密。這可讓您在同一個檔案系統上混合使用加密和未加密的檔案共用。若要進一步瞭解如何在檔案系統 encryption-in-transit 上進行管理，請參閱管理傳輸中的加密。

使用視窗 ACL 的檔案和資料夾層級存取控制

FSx for Windows File Server 的 Amazon FSx 支援透過伺服器訊息區 (SMB) 通訊協定透過 Microsoft 活動目錄進行身分識別驗證。Active Directory 是 Microsoft 目錄服務，用於存儲有關網絡上對象的信息，並使這些信息易於管理員和用戶查找和使用。這些物件通常包括共用資源，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 中的使用中目錄支援，請參閱使用 Microsoft 活動目錄在 FSx for Windows File Server。

加入網域的運算執行個體可以使用活動目錄登入資料存取 Amazon FSx 檔案共用。您可以使用標準 Windows 存取控制清單 (ACL) 來進行精細的檔案和資料夾層級存取控制。Amazon FSx 檔案系統會自動驗證使用者存取檔案系統資料的登入資料，以強制執行這些 Windows ACL。

每個 Amazon FSx 文件系統都帶有一個名為`share`的默認 Windows 文件共享。此共用資料夾的 Windows ACL 設定為允許網域使用者讀取/寫入存取權。它們也允許完全控制 Active Directory 中委派的系統管理員群組，這些管理員群組被委派可在您的檔案系統上執行系統管理動作。如果您要整合您的檔案系統與 AWS 受管理的 Microsoft AD，這個群組就是 AWS 委派的 FSx 系統管理員。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。也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 ACL，您可以將共用對應為委派系統管理員群組成員的使用者身分。

> **Warning**
>
> Amazon FSx 要求系統使用者對檔案系統中的所有資料夾擁有完全控制 NTFS ACL 許可。請勿變更資料夾上此使用者的 NTFS ACL 權限。這樣做可以使您的文件共享無法訪問，並防止文件系統備份可用。

相關連結

- 什麼是 AWS Directory Service？ 在《 AWS Directory Service 管理指南》中。
- 在《AWS 管理指南》中建立受AWS Directory Service 管理的 Microsoft AD 目錄。
- 何時建立《AWS Directory Service 管理指南》中的信任關係。
- 演練 1：開始使用的先決條件.

使用 Amazon VPC 進行檔案系統存取控制

您可以透過 elastic network interface 存取 Amazon FSx 檔案系統。此網路界面位於以您與檔案系統建立關聯之 Amazon Virtual Private Cloud (Amazon VPC) 服務為基礎的虛擬私有雲 (VPC) 中。您可以透過其網域名稱服務 (DNS) 名稱連線到 Amazon FSx 檔案系統。DNS 名稱會對應至 VPC 中檔案系統 elastic network interface 的私有 IP 位址。只有關聯 VPC 中的資源、與相關 VPC (AWS Direct Connect 或 VPN) 連線的資源，或對等 VPC 內的資源，才能存取檔案系統的網路介面。如需詳細資訊，請參閱什麼是 Amazon VPC？ 在 Amazon VPC 用戶指南中。

> **Warning**
>
> 您不得修改或刪除與檔案系統相關聯的 elastic network interface。修改或刪除網路介面可能會導致 VPC 與檔案系統之間的連線永久中斷。

FSx for Windows File Server 支援 VPC 共用，可讓您檢視、建立、修改和刪除其他帳戶所擁有的 VPC 中共用子網路中的資源。 AWS 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 中檔案系統 elastic network interface 的網路流量，請使用安全群組來限制對檔案系統的存取。安全群組是可設定狀態的防火牆，可控制進出其相關聯網路介面的流量。在此情況下，關聯的資源就是檔案系統的網路介面。

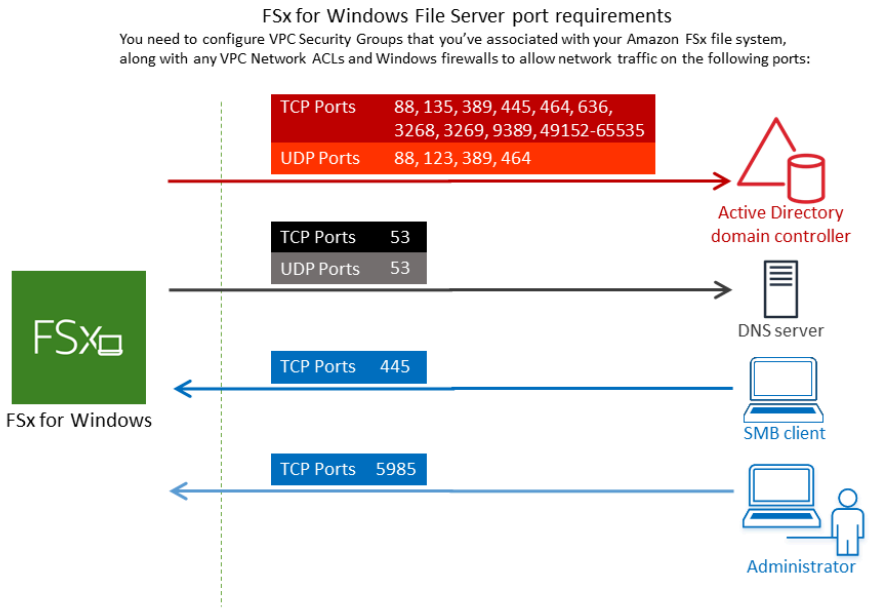
若要使用安全群組控制對 Amazon FSx 檔案系統的存取，請新增輸入和輸出規則。輸入規則可控制傳入流量，而輸出規則則會控制來自檔案系統的傳出流量。確保安全群組中有正確的網路流量規則，以將 Amazon FSx 檔案系統的檔案共用對應到受支援運算執行個體上的資料夾。

如需有關安全群組規則的詳細資訊，請參閱 Amazon EC2 使用者指南中的安全群組規則。

若要為 Amazon FSx 建立安全群組

1. 在以下位置打開 Amazon EC2 控制台 https://console.aws.amazon.com/ec2。
2. 在導覽窗格中，選擇 Security Groups (安全群組)。
3. 選擇 Create Security Group (建立安全群組)。
4. 指定安全群組的名稱和描述。
5. 對於虛擬私人雲端，請選擇與檔案系統關聯的 Amazon VPC，以在該 VPC 內建立安全群組。
6. 新增下列規則，以允許下列通訊埠上的輸出網路流量：

   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。請確定您要建立 FSx 檔案系統之子網路的安全性群組和 VPC Network ACL 允許連接埠上的流量，並按照下圖所示的指示進行流量。



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	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 全球編錄

通訊協定	連接埠	角色
TCP	3269	通過 SSL Microsoft 全局類別目錄
TCP	5985	Microsoft 視窗遠端管理
TCP	9389	Microsoft AD DS 網絡服務 PowerShell
TCP	49152 - 65535	適用於 RPC 的暫時性連接埠

> **Important**
>
> 單一可用區 2 和所有異地同步備份檔案系統部署都需要在 TCP 連接埠 9389 上允許輸出流量。

b. 請確定這些流量規則也會鏡像在套用至每個 AD 網域控制站、DNS 伺服器、FSx 用戶端和 FSx 系統管理員的防火牆上。

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

> **Note**
>
> 如果您已定義 Active Directory 站台，則必須確定 VPC 中與 Amazon FSx 檔案系統相關聯的子網路是在 Active Directory 站台中定義的，而且 VPC 中的子網路與其他站台中的子網路之間沒有衝突。您可以使用 [使用中的目錄站台和服務 MMC 嵌入式管理單元來檢視和變更這些設定。

> **Note**
>
> 在某些情況下，您可能已經從預設設定中修改了 AWS Managed Microsoft AD 安全性群組的規則。如果是這樣，請確定此安全群組具有必要的輸入規則，以允許來自 Amazon FSx

檔案系統的流量。如需必要輸入規則的詳細資訊，請參閱《AWS Directory Service 管理指南》中的AWS Managed Microsoft AD 先決條件。

現在您已經建立了安全群組，您可以將其與 Amazon FSx 檔案系統的 elastic network interface 建立關聯。

將安全群組與您的 Amazon FSx 檔案系統建立關聯

1. 開啟 Amazon FSx 主控台，網址為 https://console.aws.amazon.com/fsx/。
2. 在儀表板上，選擇您的檔案系統以檢視其詳細資料。
3. 選擇「網路與安全性」標籤，然後選擇檔案系統的網路介面，例如 ENI-01234567890123456。對於單一可用區檔案系統，您會看到單一網路介面。對於異地同步備份檔案系統，您會在首選子網路中看到一個網路介面，在待命子網路中看到一個網路介面。
4. 針對每個網路介面，選擇網路介面，然後在動作中選擇變更安全性群組。
5. 在 [變更安全性群組] 對話方塊中，選擇要使用的安全性群組，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的網路，您可以移除與檔案系統 elastic network interface 相關聯的所有安全性群組，並將其取代為沒有入站/輸出規則的群組。

Amazon VPC 網路 ACL

保護 VPC 內檔案系統存取的另一個選項是建立網路存取控制清單 (網路 ACL)。網路 ACL 與安全群組分開，但具有類似的功能，可為 VPC 中的資源增加額外的安全層。如需有關網路 ACL 的詳細資訊，請參閱 Amazon VPC 使用者指南中的網路 ACL。

適用於 Windows 檔案伺服器的 Amazon FSx 的 Identity and Access Management

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM 管理員控制哪些人可以通過身份驗證 (登入) 和授權 (具有許可) 來使用 Amazon FSx 資源。您可以使用 IAM AWS 服務 ，無需額外付費。

主題

物件

您使用 AWS Identity and Access Management (IAM) 的方式會有所不同，具體取決於您在 Amazon FSx 中執行的工作。

服務使用者 — 如果您使用 Amazon FSx 服務執行工作，則管理員會為您提供所需的登入資料和許可。當您使用更多 Amazon FSx 功能完成工作時，您可能需要額外的許可。瞭解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取 Amazon FSx 中的某個功能，請參閱針對 Windows 檔案伺服器身分識別和存取的 Amazon FSx 進行疑難。

服務管理員 — 如果您負責公司的 Amazon FSx 資源，您可能擁有 Amazon FSx 的完整存取權。判斷服務使用者應存取哪些 Amazon FSx 功能和資源是您的工作。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步了解貴公司如何將 IAM 與 Amazon FSx 搭配使用，請參閱FSx for Windows File Server 的 Amazon FSx 如何與 IAM 搭配使用。

IAM 管理員 — 如果您是 IAM 管理員，您可能想要了解如何撰寫政策以管理 Amazon FSx 存取權的詳細資訊。若要檢視可在 IAM 中使用的 Amazon FSx 身分型政策範例，請參閱。適用於 Windows 檔案伺服器的 Amazon FSx 的身分識別原則範例

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以 IAM 使用者身分或假設 IAM 角色進行驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM 身分中心) 使用者、貴公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料

都是聯合身分識別的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需有關登入的詳細資訊 AWS，請參閱《AWS 登入 使用指南》 AWS 帳戶中的如何登入您的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以加密方式簽署要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南中的簽署 AWS API 請求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。如需更多資訊，請參閱《AWS IAM Identity Center 使用者指南》中的多重要素驗證和《IAM 使用者指南》中的在 AWS 中使用多重要素驗證 (MFA)。

AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常作業。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱《IAM 使用者指南》中的需要根使用者憑證的任務。

聯合身分

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時認證 AWS 服務 來存取。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步到自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需 IAM Identity Center 的相關資訊，請參閱《AWS IAM Identity Center 使用者指南》中的什麼是 IAM Identity Center？。

IAM 使用者和群組

IAM 使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案

例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#rotate-credentials中的為需要長期憑證的使用案例定期輪換存取金鑰。

IAM 群組是一種指定 IAM 使用者集合的身分。您無法以群組身分登入。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的過程變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。如需進一步了解，請參閱《IAM 使用者指南》中的建立 IAM 使用者 (而非角色) 的時機。

IAM 角色

IAM 角色是您 AWS 帳戶 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以切換角色，在中暫時擔任 IAM 角色。 AWS Management Console 您可以透過呼叫 AWS CLI 或 AWS API 作業或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並取得由角色定義的許可。如需有關聯合角色的詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-idp.html中的為第三方身分供應商建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱《AWS IAM Identity Center 使用者指南》中的許可集。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳户存取權 – 您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的委託人) 存取您帳戶中的資源。角色是授予跨帳户存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。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 角色與資源類型政策的差異。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。當您使用某些服務時，您可能會執行一個動作，而該動作之後會在不同的服務中啟動另一個

動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。

- 服務角色：服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可給 AWS 服務 服務。
- 服務連結角色 — 服務連結角色是連結至. AWS 服務 服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

如需了解是否要使用 IAM 角色或 IAM 使用者，請參閱《IAM 使用者指南》中的建立 IAM 角色 (而非使用者) 的時機。

使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以 JSON 文件的形式儲存在中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱《IAM 使用者指南》中的 JSON 政策概觀。

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

預設情況下，使用者和角色沒有許可。若要授與使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或 AWS API 取得角色資訊。

身分型政策

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。如需瞭解如何在受管政策及內嵌政策間選擇，請參閱 IAM 使用者指南中的在受管政策和內嵌政策間選擇。

資源型政策

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

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

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

Amazon S3 和 Amazon VPC 是支援 ACL 的服務範例。 AWS WAF若要進一步了解 ACL，請參閱《Amazon Simple Storage Service 開發人員指南》中的存取控制清單 (ACL) 概觀。

其他政策類型

AWS 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授與您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可範圍的更多相關資訊，請參閱《IAM 使用者指南》中的 IAM 實體許可範圍。

- 服務控制策略（SCP）— SCP 是 JSON 策略，用於指定中組織或組織單位（OU）的最大權限。AWS Organizations AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 限制成員帳戶中實體的權限，包括每個 AWS 帳戶根使用者帳戶。如需組織和 SCP 的更多相關資訊，請參閱《AWS Organizations 使用者指南》中的 SCP 運作方式。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需更多資訊，請參閱《IAM 使用者指南》中的工作階段政策。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。要了解如何在涉及多個政策類型時 AWS 確定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

FSx for Windows File Server 的 Amazon FSx 如何與 IAM 搭配使用

在您使用 IAM 管理 Amazon FSx 的存取權限之前，請先了解哪些 IAM 功能可用於 Amazon FSx。

您可以搭配 FSx for Windows File Server 的 Amazon FSx 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

IAM 功能	FSx 支援
轉寄存取會話	是
服務角色	否
服務連結角色	是

若要深入瞭解 FSx 和其他 AWS 服務如何搭配大多數 IAM 功能運作，請參閱 IAM 使用者指南中的搭配 IAM 使用的AWS 服務。

FSx 的以身分識別為基礎的原則

支援身分型政策	是

身分型政策是可以連接到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要瞭解如何建立身分類型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。您無法在身分型政策中指定主體，因為這會套用至附加的使用者或角色。如要瞭解您在 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 的以識別為基礎的原則範例

若要檢視 Amazon FSx 身分識別型政策的範例，請參閱。適用於 Windows 檔案伺服器的 Amazon FSx 的身分識別原則範例

FSx 中以資源為基礎的政策

支援以資源基礎的政策	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。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執

行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。AWS 服務

若要啟用跨帳戶存取權，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，作為資源型政策的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主體和資源位於不同時 AWS 帳戶，受信任帳戶中的 IAM 管理員也必須授與主體實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策附加到實體來授予許可。不過，如果資源型政策會為相同帳戶中的主體授與存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM 角色與資源型政策有何差異。

FSx 的政策動作

支援政策動作	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼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。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些操作需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授與執行相關聯操作的許可。

若要查看 FSx 動作清單，請參閱服務授權參考資料中的 Amazon FSx for Windows File Server 服器定義的動作。

FSx 中的原則動作會在動作之前使用下列前置詞：

```
fsx
```

如需在單一陳述式中指定多個動作，請用逗號分隔。

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

若要檢視 Amazon FSx 身分識別型政策的範例，請參閱。適用於 Windows 檔案伺服器的 Amazon FSx 的身分識別原則範例

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哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素可指定要套用動作的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出作業)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

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

若要查看 FSx 資源類型及其 ARN 的清單，請參閱服務授權參考資料中的 Amazon FSx for Windows File Server 服器定義的資源。若要了解可以使用哪些動作指定每個資源的 ARN，請參閱 Amazon FSx for Windows File Server 定義的動作。

若要檢視 Amazon FSx 身分識別型政策的範例，請參閱。適用於 Windows 檔案伺服器的 Amazon FSx 的身分識別原則範例

FSx 的原則條件金鑰

支援服務特定政策條件索引鍵	是

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

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授與該 IAM 使用者。如需更多資訊，請參閱《IAM 使用者指南》中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

若要查看 FSx 條件金鑰清單，請參閱服務授權參考資料中適用於 Windows 檔案伺服器的 Amazon FSx 條件金鑰。若要了解可以使用條件金鑰的動作和資源，請參閱 Amazon FSx for Windows File Server 定義的動作。

若要檢視 Amazon FSx 身分識別型政策的範例，請參閱。適用於 Windows 檔案伺服器的 Amazon FSx 的身分識別原則範例

FSx 中的 ACL

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。

亚巴克与 FSx

支援 ABAC (政策中的標籤)	是

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在中 AWS，這些屬性稱為標籤。您可以將標籤附加到 IAM 實體 (使用者或角色) 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

若要根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，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索引鍵，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索引鍵，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的什麼是 ABAC?。如要查看含有設定 ABAC 步驟的教學課程，請參閱《IAM 使用者指南》中的使用屬性型存取控制 (ABAC)。

搭配 FSx 使用臨時登入資料

支援臨時憑證	是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配AWS 服務 使用，請參閱 IAM 使用者指南中的 IAM。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立暫時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱 IAM 使用者指南中的切換至角色 (主控台)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱 IAM 中的暫時性安全憑證。

FSx 的轉寄存取工作階段

支援轉寄存取工作階段 (FAS)	是

當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。當您使用某些服務時，您可能會執行一個動作，而該動作之後會在不同的服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。

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 服務。

> **Warning**
>
> 變更服務角色的權限可能會中斷 FSx 功能。僅在 FSx 提供指引時才編輯服務角色。

FSx 的服務連結角色

支援服務連結角色	是

服務連結角色是一種連結至. AWS 服務 服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理 Amazon FSx 服務連結角色的詳細資訊，請參閱。使用 Amazon FSx 的服務連結角色

適用於 Windows 檔案伺服器的 Amazon FSx 的身分識別原則範例

依預設，使用者和角色沒有建立或修改 Amazon FSx 資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。若要授與使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

如需 FSx 定義的動作和資源類型的詳細資訊，包括每種資源類型的 ARN 格式，請參閱服務授權參考中適用於 Windows 檔案伺服器的 Amazon FSx 動作、資源和條件金鑰。

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

以身分識別為基礎的政策可決定使用者是否可以在您的帳戶中建立、存取或刪除 Amazon FSx 資源。這些動作可能會讓您的 AWS 帳戶 產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的 AWS 受管政策。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需更多資訊，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

有關 IAM 中最佳實務的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 最佳安全實務。

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限度的許可。這些許可必須允許您 AWS 帳戶列出和檢視有關. 如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體（使用者或角色）而言，主控台就無法如預期運作。

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

若要確保使用者和角色仍可使用 FSx 主控台，請同時將 FSx `AmazonFSxConsoleReadOnlyAccess` AWS 受管理的原則附加至實體。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。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

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

AWS Amazon FSx 的受管政策

受 AWS 管理的策略是由建立和管理的獨立策略 AWS。 AWS 受管理的策略旨在為許多常見使用案例提供權限，以便您可以開始將權限指派給使用者、群組和角色。

請記住， AWS 受管理的政策可能不會為您的特定使用案例授與最低權限權限，因為這些權限可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法變更受 AWS 管理策略中定義的權限。如果 AWS 更新 AWS 受管理原則中定義的權限，則此更新會影響附加原則的所有主體識別 (使用者、群組和角色)。 AWS 當新的啟動或新 AWS 服務 的 API 操作可用於現有服務時，最有可能更新 AWS 受管理策略。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

亞馬遜 SxServiceRolePolicy

允許 Amazon FSx 代表您管理 AWS 資源。如需進一步了解，請參閱使用 Amazon FSx 的服務連結角色。

AWS 管理策略：亞馬遜 SxDeleteServiceLinkedRoleAccess

您不得將 AmazonFSxDeleteServiceLinkedRoleAccess 連接到 IAM 實體。此原則會連結至服務，且只能與該服務的服務連結角色搭配使用。您無法連接、取消連接、修改或刪除此政策。如需詳細資訊，請參閱 使用 Amazon FSx 的服務連結角色。

此政策授予管理許可，這些許可允許 Amazon FSx 刪除其用於 Amazon S3 存取的服務連結角色，這些角色僅供 Amazon FSx 用於 Lustre。

許可詳細資訊

此政策包含中iam允許 Amazon FSx 檢視、刪除和檢視 Amazon S3 存取 FSx 服務連結角色的刪除狀態的許可。

若要檢視此政策的權限，請參閱《 AWS 受管理策略參考指南》SxDeleteServiceLinkedRoleAccess中的 AmazonF。

AWS 管理策略：亞馬遜 SxFullAccess

您可以將亞馬遜 F 附加SxFullAccess 到您的 IAM 實體。Amazon FSx 也會將此政策附加到可讓 Amazon FSx 代表您執行動作的服務角色。

提供對 Amazon FSx 的完整存取權以及相關 AWS 服務的存取權。

許可詳細資訊

此政策包含以下許可。

- fsx— 允許主體完整存取權以執行除外的所有 Amazon FSx 動作。BypassSnaplockEnterpriseRetention

- ds— 允許主參與者檢視 AWS Directory Service 目錄的相關資訊。
- ec2
  - 允許主參與者在指定條件下建立標籤。
  - 為可與 VPC 搭配使用的所有安全群組提供增強的安全群組驗證。
- iam— 允許代表使用者建立 Amazon FSx 服務連結角色的原則。這是必要的，以便 Amazon FSx 可以代表使用者管理 AWS 資源。
- logs— 可讓主參與者建立記錄群組、記錄串流，以及將事件寫入記錄串流。這是必要的，以便使用者可以透過將稽核存取記錄傳送至 CloudWatch 記錄檔來監視 FSx 的 Windows 檔案伺服器檔案系統存取。
- firehose— 允許校長將記錄寫入 Amazon 資料 Firehose。這是必要的，以便使用者可以透過將稽核存取記錄傳送至 Firehose 來監控 FSx 的 Windows 檔案伺服器檔案系統存取。

若要檢視此政策的權限，請參閱《 AWS 受管理策略參考指南》SxFullAccess中的 AmazonF。

AWS 管理策略：亞馬遜 SxConsoleFullAccess

您可將 AmazonFSxConsoleFullAccess 政策連接到 IAM 身分。

此政策授予管理許可，允許完整存取 Amazon FSx，並 AWS 透過 AWS Management Console.

許可詳細資訊

此政策包含以下許可。

- fsx— 允許主體在 Amazon FSx 管理主控台中執行所有動作，但不包括。BypassSnaplockEnterpriseRetention
- cloudwatch— 允許主體在 Amazon FSx 管理主控台中檢視 CloudWatch 警示和指標。
- ds— 允許主參與者列出 AWS Directory Service 目錄的相關資訊。
- ec2
  - 允許主體在路由表上建立標籤、列出網路界面、路由表、安全群組、子網路以及與 Amazon FSx 檔案系統關聯的 VPC。
  - 為可與 VPC 搭配使用的所有安全群組提供增強的安全群組驗證。
- kms— 允許主參與者列出 AWS Key Management Service 金鑰的別名。
- s3— 允許主體列出 Amazon S3 儲存貯體中的部分或所有物件 (最多 1000 個)。
- iam— 授予建立服務連結角色的權限，以允許 Amazon FSx 代表使用者執行動作。

若要檢視此政策的權限，請參閱《 AWS 受管理策略參考指南》SxConsoleFullAccess中的 AmazonF。

AWS 管理策略：亞馬遜 SxConsoleReadOnlyAccess

您可將 AmazonFSxConsoleReadOnlyAccess 政策連接到 IAM 身分。

此政策授予 Amazon FSx 和相關 AWS 服務的唯讀許可，以便使用者可以在中檢視這些服務的相關資訊。 AWS Management Console

許可詳細資訊

此政策包含以下許可。

- fsx— 允許主體在 Amazon FSx 管理主控台中檢視有關 Amazon FSx 檔案系統的資訊，包括所有標籤。
- cloudwatch— 允許主體在 Amazon FSx 管理主控台中檢視 CloudWatch 警示和指標。
- ds— 允許主體在 Amazon FSx 管理主控台中檢視 AWS Directory Service 目錄的相關資訊。
- ec2
  - 允許主體在 Amazon FSx 管理主控台中檢視與 Amazon FSx 檔案系統相關聯的網路界面、安全群組、子網路以及 VPC 擬私人雲端。
  - 為可與 VPC 搭配使用的所有安全群組提供增強的安全群組驗證。
- kms— 允許主體在 Amazon FSx 管理主控台中檢視 AWS Key Management Service 金鑰的別名。
- log— 允許主體描述與提出請求的帳戶相關聯的 Amazon CloudWatch 日誌日誌群組。這是必要的，主體才能檢視 Windows 檔案伺服器檔案系統 FSx 的現有檔案存取稽核組態。
- firehose— 允許主體描述與提出請求的帳戶相關聯的 Amazon 資料 Firehose 交付串流。這是必要的，主體才能檢視 Windows 檔案伺服器檔案系統 FSx 的現有檔案存取稽核組態。

若要檢視此政策的權限，請參閱《 AWS 受管理策略參考指南》SxConsoleReadOnlyAccess中的 AmazonF。

AWS 管理策略：亞馬遜 SxReadOnlyAccess

您可將 AmazonFSxReadOnlyAccess 政策連接到 IAM 身分。

此政策授予允許對 Amazon FSx 進行唯讀存取的管理許可。

- `fsx`— 允許主體在 Amazon FSx 管理主控台中檢視有關 Amazon FSx 檔案系統的資訊，包括所有標籤。
- `ec2`— 為可與 VPC 搭配使用的所有安全群組提供增強的安全群組驗證。

若要檢視此政策的權限，請參閱《 AWS 受管理策略參考指南》SxReadOnlyAccess中的 AmazonF。

Amazon FSx 更新 AWS 受管政策

檢視 Amazon FSx AWS 受管政策更新的詳細資訊，因為此服務開始追蹤這些變更。如需有關此頁面變更的自動警示，請訂閱 Amazon FSx 文件歷史記錄 頁面上的 RSS 摘要。

變更	描述	日期
亞馬遜 SxServiceRolePolicy-更新到現有政策	Amazon FSx 新增了新權限，允`ec2:GetSecurityGroupsForVpc` 許主體對可搭配 VPC 使用的所有安全群組提供增強的安全群組驗證。	2024 年 1 月 9 日
亞馬遜 SxReadOnlyAccess-更新到現有政策	Amazon FSx 新增了新權限，允`ec2:GetSecurityGroupsForVpc` 許主體對可搭配 VPC 使用的所有安全群組提供增強的安全群組驗證。	2024 年 1 月 9 日
亞馬遜 SxConsoleReadOnlyAccess-更新到現有政策	Amazon FSx 新增了新權限，允`ec2:GetSecurityGroupsForVpc` 許主體對可搭配 VPC 使用的所有安全群組提供增強的安全群組驗證。	2024 年 1 月 9 日
亞馬遜 SxFullAccess-更新到現有政策	Amazon FSx 新增了新權限，允`ec2:GetSecurityGroupsForVpc` 許主體對可搭配 VPC 使用的所有安全群組提供增強的安全群組驗證。	2024 年 1 月 9 日

變更	描述	日期
亞馬遜 SxConsoleFullAccess-更新到現有政策	Amazon FSx 新增了新權限，允ec2:GetSecurityGroupsForVpc 許主體對可搭配 VPC 使用的所有安全群組提供增強的安全群組驗證。	2024 年 1 月 9 日
亞馬遜 SxFullAccess-更新到現有政策	Amazon FSx 新增了新的權限，讓使用者能夠針對 OpenZFS 檔案系統的 FSx 執行跨區域和跨帳戶資料複寫。	2023 年 12 月 20 日
亞馬遜 SxConsoleFullAccess-更新到現有政策	Amazon FSx 新增了新的權限，讓使用者能夠針對 OpenZFS 檔案系統的 FSx 執行跨區域和跨帳戶資料複寫。	2023 年 12 月 20 日
亞馬遜 SxFullAccess-更新到現有政策	Amazon FSx 新增了新的權限，讓使用者能夠針對 OpenZFS 檔案系統的 FSx 執行隨選磁碟區複寫。	2023 年 11 月 26 日
亞馬遜 SxConsoleFullAccess-更新到現有政策	Amazon FSx 新增了新的權限，讓使用者能夠針對 OpenZFS 檔案系統的 FSx 執行隨選磁碟區複寫。	2023 年 11 月 26 日
亞馬遜 SxFullAccess-更新到現有政策	Amazon FSx 新增了新的許可，讓使用者能夠檢視、啟用和停用針對 ONTAP 異地同步備份檔案系統 FSx 的共用 VPC 支援。	2023 年 11 月 14 日

變更	描述	日期
亞馬遜 SxConsoleFullAccess-更新到現有政策	Amazon FSx 新增了新的許可，讓使用者能夠檢視、啟用和停用針對 ONTAP 異地同步備份檔案系統 FSx 的共用 VPC 支援。	2023 年 11 月 14 日
亞馬遜 SxFullAccess-更新到現有政策	Amazon FSx 增加了新的許可，以允許 Amazon FSx 管理適用於 OpenZFS 異地同步備份檔案系統的 FSx 網路組態。	2023 年 8 月 9 日
AWS 管理策略：AmazonFSxServiceRolePolicy-更新到現有策略	Amazon FSx 修改了現有的`cloudwatch:PutMetricData` 許可，以便 Amazon FSx 將 CloudWatch 指標發佈到命名空間。`AWS/FSx`	2023 年 7 月 24 日
亞馬遜 SxFullAccess-更新到現有政策	Amazon FSx 已更新政策以移除`fsx:*`許可並新增特定`fsx`動作。	2023 年 7 月 13 日
亞馬遜 SxConsoleFullAccess-更新到現有政策	Amazon FSx 已更新政策以移除`fsx:*`許可並新增特定`fsx`動作。	2023 年 7 月 13 日
亞馬遜 SxFullAccess-更新到現有政策	Amazon FSx 增加了新的許可，以允許 Amazon FSx 管理適用於 OpenZFS 異地同步備份檔案系統的 FSx 網路組態。	2023 年 5 月 31 日
亞馬遜 SxConsoleReadOnlyAccess-更新到現有政策	Amazon FSx 新增了新的許可，讓使用者能夠在 Amazon FSx 主控台中檢視 Windows 檔案伺服器檔案系統 FSx 的增強效能指標和建議的動作。	2022 年 9 月 21 日

變更	描述	日期
亞馬遜 SxConsoleFullAccess-更新到現有政策	Amazon FSx 新增了新的許可，讓使用者能夠在 Amazon FSx 主控台中檢視 Windows 檔案伺服器檔案系統 FSx 的增強效能指標和建議的動作。	2022 年 9 月 21 日
亞馬遜 SxReadOnlyAccess-開始跟踪政策	此政策授予對所有 Amazon FSx 資源及其相關聯標籤的唯讀存取權。	2022 年 2 月 4 日
亞馬遜 SxDeleteServiceLinkedRoleAccess-開始跟踪政策	此政策授予管理許可，這些許可允許 Amazon FSx 刪除其適用於 Amazon S3 存取的服務連結角色。	2022 年 1 月 7 日
亞馬遜 SxServiceRolePolicy-更新到現有政策	Amazon FSx 添加了新的許可，以允許 Amazon FSx 管理 NetApp ONTAP 文件系統的 Amazon FSx 的網絡配置。	2021 年 9 月 2 日
亞馬遜 SxFullAccess-更新到現有政策	Amazon FSx 添加了新的許可，以允許 Amazon FSx 在 EC2 路由表上創建標籤以用於範圍關閉調用。	2021 年 9 月 2 日
亞馬遜 SxConsoleFullAccess-更新到現有政策	Amazon FSx 添加了新的許可，以允許 Amazon FSx 為 NetApp ONTAP 異地同步備份文件系統創建 Amazon FSx。	2021 年 9 月 2 日
亞馬遜 SxConsoleFullAccess-更新到現有政策	Amazon FSx 添加了新的許可，以允許 Amazon FSx 在 EC2 路由表上創建標籤以用於範圍關閉調用。	2021 年 9 月 2 日

變更	描述	日期
亞馬遜 SxServiceRolePolicy-更新到現有政策	Amazon FSx 添加了新的許可，以允許 Amazon FSx 描述和寫入日誌流 CloudWatch 日誌流。 這是必要的，以便使用者可以使用記錄檢視 Windows 檔案伺服器檔案系統 FSx 的檔案存取稽核記 CloudWatch 錄。	2021 年 6 月 8 日
亞馬遜 SxServiceRolePolicy-更新到現有政策	Amazon FSx 添加了新的許可，以允許 Amazon FSx 描述和寫入 Amazon 數據 Firehose 交付流。 這是必要的，以便使用者可以使用 Amazon 資料 Firehose 檢視 FSx 適用於 Windows 檔案伺服器檔案系統的檔案存取稽核日誌。	2021 年 6 月 8 日
亞馬遜 SxFullAccess-更新到現有政策	Amazon FSx 新增了新許可，允許主體描述和建立 CloudWatch 日誌日誌群組、日誌串流，以及將事件寫入日誌串流。 這是必要的，主體才能使 CloudWatch 用記錄來檢視 Windows 檔案伺服器檔案系統 FSx 的檔案存取稽核記錄。	2021 年 6 月 8 日

變更	描述	日期
亞馬遜 SxFullAccess-更新到現有政策	Amazon FSx 添加了新的許可，允許校長描述和寫入記錄到 Amazon 數據 Firehose。 這是必要的，以便使用者可以使用 Amazon 資料 Firehose 檢視 FSx 適用於 Windows 檔案伺服器檔案系統的檔案存取稽核日誌。	2021 年 6 月 8 日
亞馬遜 SxConsoleFullAccess-更新到現有政策	Amazon FSx 新增了新許可，允許主體描述與提出請求的帳戶相關聯的 Amazon CloudWatch 日誌日誌群組。 這是必要的，這樣主體才能在設定 Windows 檔案伺服器檔案系統的 FSx 檔案存取稽核時，選擇現有的 CloudWatch 記錄檔記錄群組。	2021 年 6 月 8 日
亞馬遜 SxConsoleFullAccess-更新到現有政策	Amazon FSx 新增了新的許可，允許校長描述與提出請求的帳戶相關聯的 Amazon 資料 Firehose 交付串流。 這是必要的，以便主體在為 Windows 檔案伺服器檔案系統設定檔案存取稽核時，可以選擇現有的 Firehose 傳遞串流。	2021 年 6 月 8 日

變更	描述	日期
亞馬遜 SxConsoleReadOnlyAccess-更新到現有政策	Amazon FSx 新增了新許可，允許主體描述與提出請求的帳戶相關聯的 Amazon CloudWatch 日誌日誌群組。 這是必要的，主體才能檢視 Windows 檔案伺服器檔案系統 FSx 的現有檔案存取稽核組態。	2021 年 6 月 8 日
亞馬遜 SxConsoleReadOnlyAccess-更新到現有政策	Amazon FSx 新增了新的許可，允許校長描述與提出請求的帳戶相關聯的 Amazon 資料 Firehose 交付串流。 這是必要的，主體才能檢視 Windows 檔案伺服器檔案系統 FSx 的現有檔案存取稽核組態。	2021 年 6 月 8 日
Amazon FSx 開始跟踪更改	Amazon FSx 開始追蹤其 AWS 受管政策的變更。	2021 年 6 月 8 日

針對 Windows 檔案伺服器身分識別和存取的 Amazon FSx 進行疑難

使用下列資訊協助您診斷和修正使用 Amazon FSx 和 IAM 時可能遇到的常見問題。

主題

- 我沒有在 FSx 中執行動作的授權
- 我沒有授權執行 iam：PassRole
- 我想允許我以外的人訪問我 AWS 帳戶 的 FSx 資源

我沒有在 FSx 中執行動作的授權

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登入憑證。

我沒有授權執行 iam：PassRole

如果您收到未獲授權執行iam:PassRole動作的錯誤訊息，則必須更新您的政策以允許您將角色傳遞給 Amazon FSx。

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

當名為的 IAM 使用者marymajor嘗試使用主控台在 Amazon FSx 中執行動作時，會發生下列範例錯誤。但是，該動作要求服務具備服務角色授與的許可。Mary 沒有將角色傳遞至該服務的許可。

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

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

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的登入憑證。

我想允許我以外的人訪問我 AWS 帳戶 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的組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 Amazon FSx 是否支援這些功能，請參閱FSx for Windows File Server 的 Amazon FSx 如何與 IAM 搭配使用。

- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱《IAM 使用者指南》中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限。
- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。
- 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 角色與資源型政策的差異。

使用標籤與 Amazon FSx

您可以使用標籤來控制對 Amazon FSx 資源的存取，以及實作以屬性為基礎的存取控制 (ABAC)。使用者需要在建立期間取得將標籤套用至 Amazon FSx 資源的權限。

在建立期間授予標籤資源的許可

某些資源建立 Amazon FSx 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以屬性為基礎的存取控制 (ABAC)。如需詳細資訊，請參閱 IAM 使用者指南 AWS中的 ABAC 是什麼。

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。

下列範例示範一項策略，該策略允許使用者在特定建立期間建立檔案系統並將標記套用至檔案系統 AWS 帳戶。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateFileSystem",
         "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/*"
    }
  ]
}
```

同樣地，下列原則允許使用者在特定檔案系統上建立備份，並在備份建立期間將任何標記套用至備份。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateBackup"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/file-system-id*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:backup/*"
    }
  ]
}
```

只有在資源建立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，請參閱標記您的 Amazon FSX 資源。如需使用標籤來控制 FSx 資源存取權的詳細資訊，請參閱使用標籤來控制對 Amazon FSx 資源的存取。

使用標籤來控制對 Amazon FSx 資源的存取

若要控制對 Amazon FSx 資源和動作的存取，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。

如需如何使用標籤來控制 AWS 資源存取權限的詳細資訊，請參閱 IAM 使用者指南中的使用標籤控制存取。如需有關在建立時標記 Amazon FSx 資源的詳細資訊，請參閱在建立期間授予標籤資源的許可。如需標記資源的詳細資訊，請參閱 標記您的 Amazon FSX 資源。

根據資源的標籤控制存取

若要控制使用者或角色可在 Amazon FSx 資源上執行的動作，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 原則 — 在提供特定標籤時建立檔案系統

此原則只允許使用者在使用特定標籤索引鍵值配對來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之 Amazon FSx 檔案系統的備份

此原則可讓使用者僅建立以金鑰值組標記之檔案系統的備份`key=Department, value=Finance`，而且會使用標籤建立備份`Deparment=Finance`。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
```

```
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }

    ]
}
```

Example 原則 — 從具有特定標籤的備份中建立具有特定標籤的檔案系統

此原則可讓使用者建立Department=Finance只有標記為備份的檔案系統Department=Finance。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateFileSystemFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example 原則 — 刪除具有特定標籤的檔案系統

此原則允許使用者僅刪除標記為的檔案系統Department=Finance。如果他們創建了最終備份，則必須使用標記Department=Finance。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteFileSystem"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

使用 Amazon FSx 的服務連結角色

FSx for Windows File Server 專用的 Amazon FSx 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 Amazon FSx 的唯一 IAM 角色類型。Amazon FSx 預先定義服務連結角色，並包含服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓您輕鬆設定 Amazon FSx，因為您不必手動新增必要的許可。Amazon FSx 會定義其服務連結角色的許可，除非另有定義，否則只有 Amazon FSx 可以擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

您必須先刪除服務連結角色的相關資源，才能將其刪除。這樣可以保護您的 Amazon FSx 資源，因為您無法意外移除存取資源的權限。

如需關於支援服務連結角色的其他服務的資訊，請參閱可搭配 IAM 運作的 AWS 服務，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (是) 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

適用於 Amazon FSx 的服務連結角色許可

Amazon FSx 使用名為的服務連結角色 `AWSServiceRoleForAmazonFSx` — 該角色會在您的帳戶中執行某些動作，例如為 VPC 中的檔案系統建立彈性網路界面。

角色許可政策允許 Amazon FSx 在所有適用 AWS 資源上完成下列動作：

您不能將亞馬遜 F 附加SxServiceRolePolicy 到您的 IAM 實體。此原則附加至服務連結角色，可讓 FSx 代表您管理 AWS 資源。如需詳細資訊，請參閱 使用 Amazon FSx 的服務連結角色。

如需此政策的更新，請參閱 亞馬遜 SxServiceRolePolicy

此原則會授與允許 FSx 代表使用者管理 AWS 資源的管理權限。

許可詳細資訊

AmazonF SxServiceRolePolicy 角色權限由 Amazon SxServiceRolePolicy AWS F 管理策略定義。亞馬遜SxServiceRolePolicy 擁有以下權限：

> **Note**
>
> 所有 Amazon FSx 檔案系統類型都使用了 AmazonFSxServiceRolePolicy ；某些列出的許可可可可可可不適用於視窗版 FSx。

- `ds`— 允許 FSx 檢視、授權和取消授權目錄中的應用程式 AWS Directory Service 。
- `ec2`— 允許 FSx 執行下列作業：
  - 檢視、建立和取消與 Amazon FSx 檔案系統相關聯的網路界面的關聯。
  - 檢視與 Amazon FSx 檔案系統關聯的一或多個彈性 IP 地址。
  - 檢視與 Amazon FSx 檔案系統相關聯的 Amazon VPC、安全群組和子網路。

  - 為可與 VPC 搭配使用的所有安全群組提供增強的安全群組驗證。
  - 建立 AWS授權使用者在網路介面上執行特定作業的權限。
- `cloudwatch`— 允許 FSx 將量度資料點發佈到 AWS /FSx 命名空間 CloudWatch 下。
- `route53`— 允許 FSx 將 Amazon VPC 與私有託管區域建立關聯。
- `logs`— 允許 FSx 描述及寫入 CloudWatch 記錄檔串流。這樣使用者可以將 FSx 適用於 Windows 檔案伺服器檔案系統的檔案存取稽核記錄傳送至 CloudWatch 記錄資料流。
- `firehose`— 允許 FSx 描述並寫入 Amazon 數據 Firehose 交付流。這樣使用者就可以將 FSx 適用於 Windows 檔案伺服器檔案系統的檔案存取稽核日誌發佈到 Amazon 資料 Firehose 交付串流。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateFileSystem",
            "Effect": "Allow",
            "Action": [
                "ds:AuthorizeApplication",
                "ds:GetAuthorizedApplicationDetails",
                "ds:UnauthorizeApplication",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAddresses",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVPCs",
                "ec2:DisassociateAddress",
                "ec2:GetSecurityGroupsForVpc",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PutMetrics",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
```

```
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/FSx"
                }
            }
        },

        {
            "Sid": "TagResourceNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "AmazonFSx.FileSystemId"
                }
            }
        },
        {
            "Sid": "ManageNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
                }
```

```
            }
        },
        {
            "Sid": "ManageRouteTable",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
                }
            }
        },
        {
            "Sid": "PutCloudWatchLogs",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
        },
        {
            "Sid": "ManageAuditLogs",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
        }
    ]
}
```

本政策的任何更新將在中說明Amazon FSx 更新 AWS 受管政策。

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的服務連結角色許可。

為 Amazon FSx 建立服務連結角色

您不需要手動建立一個服務連結角色。當您在 IAM CLI 或 IAM API 中 AWS Management Console建立檔案系統時，Amazon FSx 會為您建立服務連結角色。

> **Important**
>
> 此服務連結角色可以顯示在您的帳戶，如果您於其他服務中完成一項動作時，可以使用支援此角色的功能。若要進一步了解，請參閱我的 IAM 帳戶中出現的新角色。

若您刪除此服務連結角色然後需要再次建立，便可在帳戶中使用相同程序重新建立角色。當您建立檔案系統時，Amazon FSx 會再次為您建立服務連結角色。

編輯 Amazon FSx 的服務連結角色

Amazon FSx 不允許您編輯服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需更多資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

刪除 Amazon FSx 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。不過，您必須先刪除所有檔案系統和備份，才能手動刪除服務連結角色。

> **Note**
>
> 如果您嘗試刪除資源時，Amazon FSx 服務正在使用該角色，則刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台、IAM CLI 或 IAM API 刪除 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

支援 Amazon FSx 服務連結角色的區域

Amazon FSx 支援在提供服務的所有區域使用服務連結角色。如需詳細資訊，請參閱 AWS 區域與端點。

適用於 FSx for Windows File Server 的 Amazon FSx 合規驗證

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於您資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上架構 HIPAA 安全性與合規性 — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 用程式。

  > **Note**
  >
  > 並非所有人 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您滿足特定合規性架構所要求的入侵偵測需求，例如 PCI DSS 等各種合規性需求。

- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

Amazon FSx for Windows File Server 和界面 VPC 端點

您可以將 Amazon FSx 設定為使用介面 VPC 端點，進而提升 VPC 的安全狀態。界面 VPC 端點採用的技術AWS PrivateLink，這項技術可讓您以私有方式存取 Amazon FSx API，無需透過網際網路閘道、NAT 裝置、VPN 連接或AWS Direct Connect連線。VPC 中的執行個體不需要公有 IP 地址，即能與 Amazon FSx API 通訊。您的 VPC 與 Amazon FSx 之間的網路流量都不會在AWS網路。

每個介面 VPC 端點都由您子網路中的一或多個彈性網路介面表示。網路介面會提供一個私有 IP 地址，以作為 Amazon FSx API 的流量進入點。

Amazon FSx 介面 VPC 端點的考量事項

在設定 Amazon FSx 的界面 VPC 端點前，請務必檢界面 VPC 端點屬性和限制中的Amazon VPC User Guide。

您可以從 VPC 呼叫任何 Amazon FSx API 操作。例如對於您可以透過調用 CreateFileSystem API，從 VPC 內。如需 Amazon FSx API 的完整清單，請參動作在 Amazon FSx API 參考中。

VPC 互連的考量事項

您可以使用 VPC 對等互連透過界面 VPC 端點將其他 VPC 連線到 VPC。VPC 對等互連是兩個 VPC 之間的網路連線。您可以在自己的 VPC 之間建立 VPC 對等互連的連線，或與其他 VPC 建立對等互連的連線AWS 帳戶。VPC 也可以在兩個不同的AWS 區域。

對等互連的 VPC 之間的流量會保留在 AWS 網路上，且不會周遊公用網際網路。一旦 VPC 已對等互連，兩個 VPC 中的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體就可以透過在其中一個 VPC 中建立的建立的界面 VPC 端點存取 Amazon FSx API。

為 Amazon FSx API 建立界面 VPC 端點

您可以使用 Amazon VPC 主控台或AWS Command Line Interface(AWS CLI。如需詳細資訊，請參閱「」建立介面 VPC 端點中的Amazon VPC User Guide。

若要為 Amazon FSx 建立界面 VPC 端點，請使用以下其中一種方式：

- **com.amazonaws.*region*.fsx**— 為 Amazon FSx API 作業建立端點。

- **com.amazonaws.*region*.fsx-fips**— 為 Amazon FSx API 建立一個端點，該端點符合美國聯邦資訊處理標準 (FIPS) 140-2。

若要使用私有 DNS 選項，您必須設定enableDnsHostnames和enableDnsSupport屬 VPC。如需詳細資訊，請參閱「」檢視並更新 VPC 的 DNS 支援中的Amazon VPC User Guide。

排除AWS 區域在中國，如果您對該端點啟動私有 DNS，您可以使用 VPC 端點透過 VPC 端點透過其預設 DNS 名稱作為AWS 區域，例如fsx.us-east-1.amazonaws.com。中國 (北京) 和中國 (寧夏)AWS 區域，您可以使用 VPC 端點透過fsx-api.cn-north-1.amazonaws.com.cn和fsx-api.cn-northwest-1.amazonaws.com.cn分別。

如需詳細資訊，請參閱「」透過界面 VPC 端點存取服務中的Amazon VPC User Guide。

為 Amazon FSx 建立 VPC 端點政策

要進一步控制對亞馬遜 FSX API 的訪問，您可以選擇附加AWS Identity and Access Management(IAM) 政策添加到 VPC 端點。此政策會指定以下項目：

- 可執行動作的主體。
- 可執行的動作。
- 可供執行動作的資源。

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的使用 VPC 端點控制對服務的存取。

配額

接下來，您可以在使用適用於 Windows 檔案伺服器的 Amazon FSx 時找到有關配額的資訊。

主題

您可以提高的配額

以下是您可以增加的各個 AWS 帳戶 FSx for Windows File Server 的 Amazon FSx 配額。AWS 區域

資源	預設	描述
視窗檔案系統	100	您可以在此帳戶中建立的 Windows 伺服器檔案系統適用的 Amazon FSx 數目上限。
視窗吞吐量容量	10240	此帳戶中所有 Amazon FSx 適用於 Windows 檔案系統的輸送量容量總容量 (以 MBP 為單位)。
視窗硬碟儲存容量	524288	此帳戶中所有 Amazon FSx 適用於 Windows 檔案伺服器檔案系統的硬碟儲存容量上限 (以 GiB 為單位)。
視窗 SSD 儲存容量	524288	此帳戶中所有 Amazon FSx 適用於 Windows 檔案伺服器檔案系統所允許的 SSD 儲存容量上限 (以 GiB 為單位)。

資源	預設	描述
視窗總固態硬碟 IOPS	500,000	此帳戶中所有 Amazon FSX 適用於 Windows 檔案伺服器檔案系統允許的固態硬碟 IOPS 總量。
視窗備份	500	您可以在此帳戶中擁有的所有 Amazon FSx for Windows File Server 檔案系統的使用者啟動備份數目上限。

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 [要求增加配額]，然後依照指示要求提高配額。
6. 若要檢視配額要求的狀態，請在主控台瀏覽窗格中選擇配額要求歷程記錄。

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 檔案伺服器資源配額。AWS 區域

資源	每個檔案系統的限制
標籤的最大數量	50
自動備份的最長保留期	90 天
每個帳戶對單一目的地區域進行的備份複製要求數目上限。	5

資源	每個檔案系統的限制
最小儲存容量，SSD 檔案系統	32 GiB
最小儲存容量，HDD 檔案系統	2,000 GiB
最大存儲容量，SSD 和硬盤	64 TiB
最低固態硬碟 IOPS	96
最大固態硬碟 IOPS	400,000
最小輸送量容量	每秒 8 兆比特
最大輸送量容量	每秒 1288 兆比特
檔案共用數目上限	100,000

其他考量

此外，請注意下列事項：

- 您最多可以在 125 個 Amazon FSx 檔案系統上使用每個 AWS Key Management Service (AWS KMS) 金鑰。
- 如需可在AWS 區域其中建立檔案系統的清單，請參閱. AWS 一般參考
- 您可以將虛擬私有雲 (VPC) 中 Amazon EC2 執行個體的檔案共用與其網域名稱服務 (DNS) 名稱對應。

Microsoft 視窗特定配額

如需詳細資訊，請參閱 Microsoft 視窗開發人員中心的 NTFS 限制。

疑難排解 Amazon FSx

您可以使用下列各節來協助疑難排解您在使用 Amazon FSx 時遇到的問題。

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

無法存取檔案系統的可能原因有很多，每個原因都有自己的解析度，如下所示。

主題

- 無法使用 IP 位址存取檔案系統

文件系統 elastic network interface 被修改或刪除

您不得修改或刪除檔案系統的 elastic network interface。修改或刪除網路介面可能會導致 VPC 與檔案系統之間的連線永久中斷。建立新的檔案系統，請勿修改或刪除 Amazon FSx elastic network interface。如需詳細資訊，請參閱 使用 Amazon VPC 進行檔案系統存取控制。

刪除附加到文件系統 elastic network interface IP 地址

Amazon FSx 不支援從公用網際網路存取檔案系統。Amazon FSx 會自動分離任何彈性 IP 位址 (可從網際網路存取的公用 IP 位址)，並附加至檔案系統的 elastic network interface。如需詳細資訊，請參閱 FSx for Windows File Server 支援的用戶端、存取方法和環境。

檔案系統安全性群組缺少必要的輸入或輸出規則。

檢閱中指定的輸入規則Amazon VPC 安全群組，並確定與檔案系統關聯的安全性群組具有對應的輸入規則。

運算執行個體的安全性群組缺少必要的輸出規則

檢閱中指定的輸出規則Amazon VPC 安全群組，並確定與您的計算執行個體關聯的安全性群組具有對應的輸出規則。

計算執行個體未加入作用中目錄

您的運算執行個體可能無法正確連接到以下兩種類型的 Active Directory 中的一種：

- 您的檔案系統所連結的 AWS Managed Microsoft AD 目錄。
- 具有與目錄建立的單向樹系信任關係的 Microsoft 活動 AWS Managed Microsoft AD 目錄目錄。

請確定您的運算執行個體已結合到兩種類型的目錄中的一種。其中一種類型是 AWS Managed Microsoft AD 檔案系統所連結的目錄。另一種類型是具有與目錄建立的單向樹系信任關係的 Microsoft 活動 AWS Managed Microsoft AD 目錄目錄。如需詳細資訊，請參閱 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 視窗檔案共用不存在。

如果您使用現有的檔案共用，請確定已正確指定檔案系統 DNS 名稱和共用名稱。若要管理檔案共用，請參閱管理 FSx 上適用於 Windows 檔案伺服器檔案系統的檔案共用。

活動目錄用戶缺少必要的權限

您存取檔案共用的作用中目錄使用者缺少必要的存取權限。

請確定共用資料夾的檔案共用和 Windows 存取控制清單 (ACL) 的存取權限允許存取需要存取該資料夾的 Active Directory 使用者。

允許移除完全控制 NTFS ACL 權限

如果您移除您共用資料夾上 SYSTEM 使用者的 [允許完全控制 NTFS ACL] 權限，則該共用可能無法存取，而且從該點開始進行的任何檔案系統備份可能無法使用。

您必須重新建立受影響的檔案共用。如需詳細資訊，請參閱 管理 FSx 上適用於 Windows 檔案伺服器檔案系統的檔案共用。重新建立資料夾或共用之後，您可以從計算執行個體對應和使用 Windows 檔案共用。

無法使用內部部署用戶端存取檔案系統

您使用現場部署的 Amazon FSx 檔案系統使用 AWS Direct Connect 或 VPN，而且現場部署用戶端使用非私有 IP 地址範圍。

Amazon FSx 僅支援在 2020 年 12 月 17 日之後建立的檔案系統上使用非私有 IP 地址的現場部署用戶端進行存取。

如果您需要使用非私有 IP 位址範圍存取在 2020 年 12 月 17 日之前建立的 Windows 檔案伺服器檔案系統 FSx，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。

新的文件系統未在 DNS 中註冊

對於加入自我管理 Active Directory 的檔案系統，Amazon FSx 在建立檔案系統時並未註冊該檔案系統 DNS，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。您必須為您的 Amazon FSx 檔案系統手動設定 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 和異地同步備份檔案系統，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 位址。

1. 在 https://console.aws.amazon.com/fsx/ 中，選擇您要取得 IP 位址的檔案系統，以顯示檔案系統詳細資訊頁面。
2. 在 [網路與安全性] 索引標籤中，執行下列其中一項動作

   - 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 位址會顯示在主要私人 IPv4 IP 欄中。
   - 對於單一可用區 2 或異地同步備份檔案系統：
     - 在「偏好的子網路」面板中，選擇「網路界面」下顯示的彈性網路界面，以在 Amazon EC2 中開啟「網路界面」頁面。
     - 要使用的偏好子網路的 IP 位址會顯示在次要私人 IPv4 IP 欄中。
     - 在 Amazon FSx 待命子網路面板中，選擇網路界面下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的 IP 位址會顯示在次要私人 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，請使用下列程序來疑難排解問題。

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 [檔案系統詳細資料] 頁面上，DNS 別名會顯示在 [網路與安全性] 索引標籤上。

   b. 使用 CLI 或 API — 使用 `describe-file-system-aliases`CLI 命令或 DescribeFileSystemAliasesAPI 作業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 管理現有檔案系統上的 DNS 別名。
3. 如果 DNS 別名與檔案系統相關聯，請確認您也已設定下列必要項目：

   - 已建立與 Amazon FSx 檔案系統之作用中目錄電腦物件上 DNS 別名相對應的服務主體名稱 (SPN)。

     如需詳細資訊，請參閱 步驟 2：設定 Kerberos 的服務主體名稱 (SPN)。
   - 為 DNS 別名建立 DNS CNAME 記錄，該別名可解析為 Amazon FSx 檔案系統的預設 DNS 名稱。

如需詳細資訊，請參閱 步驟 3：更新或建立檔案系統的 DNS CNAME 記錄。

4. 如果您已建立有效的 SPN 和 DNS CNAME 記錄，請確認用戶端的 DNS 具有可解析為正確檔案系統的 DNS CNAME 記錄。

   a. 執行nslookup以確認記錄是否存在，並且解析為檔案系統的預設 DNS 名稱。

   b. 如果 DNS CNAME 解析為其他檔案系統，請等待用戶端的 DNS 快取重新整理，然後再次檢查 CNAME 記錄。您可以通過使用以下命令刷新客戶端的 DNS 緩存來加速該過程。

   ```
   ipconfig /flushdns
   ```

5. 如果 DNS CNAME 記錄解析為 Amazon FSx 檔案系統的預設 DNS，且用戶端仍無法存取檔案系統，請參閱以取得其他疑難排您無法存取您的檔案系統 解步驟。

無法使用 IP 位址存取檔案系統

如果您無法使用 IP 位址存取檔案系統，請改用 DNS 名稱或相關聯的 DNS 別名。

您可以選擇 Windows 檔案伺服器、網路和安全性，在 Amazon FSx 主控台上找到檔案系統的 DNS 名稱和任何相關的 DNS 別名。或者，您可以在CreateFileSystem或 DescribeFileSystemsAPI 作業的回應中找到它們。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 管理 Microsoft 活動目錄的單一可用區檔案系統，DNS 名稱如下所示。

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

- 對於所有異地同步備份檔案系統，以及加入自我管理 Active Directory 的單一可用區檔案系統，DNS 名稱如下所示。

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

建立新的 Amazon FSx 檔案系統失敗

檔案系統建立要求失敗時，有許多可能的原因，如下節所述。

主題

- 疑難排解加入 AWS 受管理 Microsoft 作用中目錄的檔案系統

- 建立加入自我管理的作用中目錄的檔案系統失敗

疑難排解加入 AWS 受管理 Microsoft 作用中目錄的檔案系統

您可以使用下列各節來協助疑難排解嘗試建立連結至自我管理作用中目錄的 Windows 檔案伺服器 FSx 檔案系統時發生的問題。

設定錯誤的 VPC 安全群組和網路 ACL

請確定 VPC 安全性群組和網路 ACL 是使用建議的安全群組組態設定來設定。如需詳細資訊，請參閱建立安全性群組。

建立加入自我管理的作用中目錄的檔案系統失敗

主題

- 重複檔案系統管理員群組名稱
- DNS 伺服器或網域控制站無法連線
- 無效的服務帳戶憑證
- 服務帳戶權限不足
- 超過服務帳戶容量
- Amazon FSx 無法存取組織單位 (OU)
- 服務帳戶無法訪問管理員組
- Amazon FSx 失去了域中的連接
- 服務帳戶沒有正確的權限
- 建立參數中使用的 Unicode 字元

重複檔案系統管理員群組名稱

建立加入您自我管理的 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，因為網域中有多個具有相同名稱的管理員群組。

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。如果有多個群組使用預設的「網域管理員」名稱，則要求將會失敗。

請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 的必要條件。
2. 使用 Amazon FSx 作用中目錄驗證工具來驗證您的自我管理作用中目錄組態，然後再建立連結至自我管理作用中目錄的 FSx 檔案伺服器檔案系統。
3. 使用 AWS Management Console 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 活動目錄網域。
4. 提供檔案系統管理員群組的名稱，該名稱在您自我管理的 Active Directory 網域中是唯一的。

DNS 伺服器或網域控制站無法連線

建立加入您自我管理的 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.
```

請使用下列步驟疑難排解並解決問題。

1. 確認您已遵循先決條件，在您要建立 Amazon FSx 檔案系統的子網路和您的自我管理 Active Directory 之間建立網路連線和路由。如需詳細資訊，請參閱 使用自我管理的 Microsoft 活動目錄的先決條件。

   使用 Amazon FSx 作用中目錄驗證工具來測試和驗證這些網路設定。

   > **Note**
   >
   > 如果您已定義多個 Active Directory 站台，請確定 VPC 中與 Amazon FSx 檔案系統相關聯的子網路已定義在 Active Directory 站台中，且 VPC 中的子網路與其他網站中的子網路之

間沒有 IP 衝突。您可以使用 [使用中的目錄站台和服務 MMC 嵌入式管理單元來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 ACL，以允許所有連接埠上的輸出網路流量。

> **Note**
>
> 如果您想要實作最低權限，您可以只允許輸出流量到與 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 作用中目錄文件。

3. 確認 Microsoft Windows 檔案伺服器或網路系統管理屬性的值不包含非拉丁字元。例如，如果您使用`Domänen-Admins`作為檔案系統管理員群組的名稱，則檔案系統建立會失敗。
4. 確認您的 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要求。
5. 請確定您的作用中目錄網域的功能層級是 Windows 伺服器 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 作用中目錄文件。

無效的服務帳戶憑證

建立加入自我管理的 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.
```

請使用下列步驟疑難排解並解決問題。

1. 確認您只輸入使用者名稱做為服務帳戶使用者名稱的輸入，例如`ServiceAcct`，在自我管理的 Active Directory 組態中。

> **Important**
>
> 輸入服務帳戶使用者名稱時，請勿包含網域前置詞 (`corp.com\ServiceAcct`或`ServiceAcct@corp.com`) 或網域尾碼 ()。

輸入服務帳戶使用者名稱時，請勿使用辨別名稱 (DN) (CN=ServiceAcct, OU = 範例、DC=Com)。

2. 確認您提供的服務帳戶存在於您的 Active Directory 網域中。
3. 請確定您已將必要權限委派給您提供的服務帳戶。服務帳戶必須能夠在您要加入檔案系統的網域中建立及刪除 OU 中的電腦物件。服務帳戶至少需要具有執行下列動作的權限：

   - 重設密碼
   - 限制帳戶讀取和寫入資料
   - 已驗證寫入 DNS 主機名稱的能力
   - 已驗證能夠寫入服務主體名稱

   如需使用正確權限建立服務帳戶的詳細資訊，請參閱 將權限委派給您的 Amazon FSx 服務帳戶 。

服務帳戶權限不足

建立加入您自我管理的 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.
```

請使用下列程序來疑難排解並解決問題。

- 請確定您已將必要權限委派給您提供的服務帳戶。服務帳戶必須能夠在您要加入檔案系統的網域中建立及刪除 OU 中的電腦物件。服務帳戶至少需要具有執行下列動作的權限：

  - 重設密碼
  - 限制帳戶讀取和寫入資料
  - 已驗證寫入 DNS 主機名稱的能力
  - 已驗證能夠寫入服務主體名稱

如需使用正確權限建立服務帳戶的詳細資訊，請參閱 將權限委派給您的 Amazon FSx 服務帳戶 。

超過服務帳戶容量

建立加入您自我管理的 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目上限。如果已達到上限，請使用正確的權限建立新的服務帳戶。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 將權限委派給您的 Amazon FSx 服務帳戶 。

Amazon FSx 無法存取組織單位 (OU)

建立加入您自我管理的 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.
```

請使用下列步驟疑難排解並解決問題。

1. 確認您提供的 OU 位於您的作用中目錄網域中。
2. 請確定您已將必要權限委派給您提供的服務帳戶。服務帳戶必須能夠在您要加入檔案系統的網域中建立及刪除 OU 中的電腦物件。服務帳戶還需要至少具有執行以下操作的權限：
   - 重設密碼
   - 限制帳戶讀取和寫入資料
   - 已驗證寫入 DNS 主機名稱的能力
   - 已驗證能夠寫入服務主體名稱

- 委派控制權以建立和刪除電腦物件
- 經過驗證的讀取和寫入帳戶限制功能

如需使用正確權限建立服務帳戶的詳細資訊，請參閱 將權限委派給您的 Amazon FSx 服務帳戶 。

服務帳戶無法訪問管理員組

建立加入您自我管理的 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.
```

請使用下列步驟疑難排解並解決問題。

1. 請確定您只提供群組名稱作為系統管理員群組參數的字串。

   > **Important**
   >
   > 提供群組名稱參數時，請勿包含網域前置詞 (corp.com \FSxAdminsFSxAdmins@corp.com) 或網域尾碼 ()。
   > 請勿使用群組的辨別名稱 (DN)。辨別名稱的範例為 CN=F SxAdmins、OU = 範例、DC = 公司、DC = COM。

2. 請確定提供的系統管理員群組與您要加入檔案系統的目標位於相同的 Active Directory 網域中。
3. 如果您未提供管理員群組參數，Amazon FSx 會嘗試使用您活動目錄網域中的Builtin Domain Admins群組。如果此群組的名稱已變更，或是您使用不同的群組進行網域管理，則必須為群組提供該名稱。

Amazon FSx 失去了域中的連接

建立加入您自我管理的 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 能夠連線到您的作用中目錄網域的 DNS 伺服器和網域控制站，並成功地將檔案系統加入您的作用中目錄網域。不過，在完成檔案系統建立時，Amazon FSx 會失去與您網域中的連線或成員資格。請使用下列步驟疑難排解並解決問題。

1. 確保您的 Amazon FSx 檔案系統和您的作用中目錄之間持續存在網路連線。此外，請使用路由規則、VPC 安全性群組規則、虛擬私人雲端網路 ACL 和網域控制站防火牆規則，確保它們之間繼續允許網路流量。
2. 請確定 Amazon FSx 為您的作用中目錄網域中的檔案系統建立的電腦物件仍處於作用中狀態，且未遭到刪除或以其他方式操控。

服務帳戶沒有正確的權限

建立加入您自我管理的 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.
```

請確定您已將必要權限委派給您提供的服務帳戶。請使用下列步驟疑難排解並解決問題。

服務帳戶至少需要具有下列權限：

- 委派控制權，以建立及刪除您要加入檔案系統之 OU 中的電腦物件
- 在您要加入檔案系統的 OU 中具有下列權限：
  - 能夠重置密碼
  - 限制帳戶讀取和寫入資料的能力
  - 已驗證寫入 DNS 主機名稱的能力
  - 已驗證能夠寫入服務主體名稱

- 建立及刪除電腦物件的能力 (可委派)
- 經過驗證的讀取和寫入帳戶限制功能
- 修改權限的能力

如需使用正確權限建立服務帳戶的詳細資訊，請參閱 將權限委派給您的 Amazon FSx 服務帳戶 。

建立參數中使用的 Unicode 字元

建立加入您自我管理的 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 不支持 Unicode 字符。確認所有建立參數都沒有 Unicode 字元，例如重音符號。這包括在自動填入預設值時可保留為空白的參數。確保活動目錄中的相應默認值也不包含 Unicode 字符。

如果您在使用 Amazon FSx 時遇到此處未列出的問題，請前往 Amazon FSx 論壇提出問題或聯絡 Amazon Web Services Support。

檔案系統處於錯誤設定的狀態

Windows 檔案伺服器檔案系統的 FSx 可能會因為您的使用中目錄環境中的變更而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可用性遺失的風險，而且備份可能無法成功。

「設定錯誤」狀態包括錯誤訊息和建議的更正動作，您可以使用 Amazon FSx 主控台、API 或存取。AWS CLI採取更正動作之後，請確認檔案系統的狀態最終變更為 `Available` — 請注意，此變更可能需要數分鐘才能完成。

您的檔案系統可能會因下列幾個原因而進入「設定錯誤」狀態：

- DNS 伺服器 IP 位址不再有效。
- 服務帳戶認證已不再有效，或缺少必要的權限。
- 無法連線 Active Directory 網域控制站，因為網路連線問題，例如無效的 VPC 安全性群組、VPC 網路 ACL 或路由表組態，或網域控制站防火牆設定。

如需使用中目錄需求的完整清單，請參閱使用自我管理的 Microsoft 活動目錄的先決條件。 您也可以使用 Amazon FSx 作用中目錄驗證工具來驗證您的作用中目錄環境是否已正確設定為符合這些需求。)

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 位址，或變更服務帳戶使用者名稱或密碼。在這些情況下，您的糾正動作必須涉及使用 Amazon FSx 主控台、API 或更新必 AWS CLI 要的組態參數。

其他問題可能不需要變更任何 Active Directory 組態參數，例如變更網域控制站防火牆設定或 VPC 安全性群組。但是，在這些情況下，您必須先採取進一步的處理行動，才能成為檔案系統`Available`。確保您的作用中目錄環境設定正確後，請選取 Amazon FSx 主控台中設定錯誤狀態旁的嘗試復原按鈕，或使用 Amazon FSx 主控台、API 或中的`StartMisconfiguredStateRecovery`命令。 AWS CLI

主題

- 設定錯誤的檔案系統：Amazon FSx 無法連線到您網域的 DNS 伺服器或網域控制站。
- 設定錯誤的檔案系統：服務帳戶認證無效
- 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權限
- 配置錯誤的文件系統：服務帳戶無法將任何其他計算機加入域
- 設定錯誤的檔案系統：服務帳戶無法存取 OU

設定錯誤的檔案系統：Amazon FSx 無法連線到您網域的 DNS 伺服器或網域控制站。

當 Amazon FSx 無法與您的 Microsoft 活動目錄域控制器或控制器通信時，文件系統將進入`Misconfigured`狀態。

若要解決此情況，請執行下列動作：

1. 請確定您的網路組態允許從檔案系統到網域控制站的流量。
2. 使用 Amazon FSx 活動目錄驗證工具來測試和驗證您自我管理的活動目錄的網路設定。如需詳細資訊，請參閱 使用 Amazon FSx 與您的自我管理 Microsoft 活動目錄。
3. 在 Amazon FSx 主控台中檢閱檔案系統的自我管理作用中目錄組態。
4. 若要更新檔案系統的自我管理作用中目錄組態，您可以使用 Amazon FSx 主控台。

    a. 在瀏覽窗格中，選擇 [檔案系統]，然後選擇要更新的檔案系統，就會顯示 [檔案系統詳細資訊] 頁面。

    b. 在 [檔案系統詳細資料] 頁面上，選擇 [網路和安全性] 索引標籤上的

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：服務帳戶認證無效

Amazon FSx 無法與您的 Microsoft 活動目錄域控制器或控制器建立連接。這是因為提供的服務帳戶憑據無效。如需詳細資訊，請參閱 使用 Amazon FSx 與您的自我管理 Microsoft 活動目錄。

若要解決組態錯誤，請執行下列動作：

1. 請確認您使用的是正確的服務帳戶，而且您使用的是該帳戶的正確認證。
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. 在瀏覽窗格中，選擇 [檔案系統]，然後選擇要更新的錯誤設定檔案系統。

   b. 在 [檔案系統詳細資料] 頁面上，選擇 [網路功能和安全性] 索引標籤中的

   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UpdateFileSystem中的。

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權限

Amazon FSx 無法建立到您的 Microsoft 活動目錄域控制站的連接。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權限。

若要解決組態錯誤，請執行下列動作：

1. 將必要的許可新增至 Amazon FSx 服務帳戶，或建立具有所需許可的新服務帳戶。如需執行此作業的詳細資訊，請參閱 將權限委派給您的 Amazon FSx 服務帳戶 。
2. 然後，使用新的服務帳戶認證來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. 在瀏覽窗格中，選擇 [檔案系統]，然後選擇要更新的檔案系統，就會顯示 [檔案系統詳細資訊] 頁面。

   b. 在 [檔案系統詳細資料] 頁面上，選擇 [網路和安全性] 索引標籤上的

   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UpdateFileSystem中的。

配置錯誤的文件系統：服務帳戶無法將任何其他計算機加入域

Amazon FSx 無法建立到您的 Microsoft 活動目錄域控制站的連接。在此情況下，這是因為所提供的服務帳戶已達到可加入網域的電腦數目上限。

若要解決組態錯誤，請執行下列動作：

1. 識別其他服務帳戶或建立可將新電腦加入網域的新服務帳戶。
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. 在瀏覽窗格中，選擇 [檔案系統]，然後選擇要更新的檔案系統，就會顯示 [檔案系統詳細資訊] 頁面。

   b. 在 [檔案系統詳細資料] 頁面上，選擇 [網路和安全性] 索引標籤上的

   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UpdateFileSystem中的。

設定錯誤的檔案系統：服務帳戶無法存取 OU

Amazon FSx 無法建立與您的 Microsoft 活動目錄網域控制站的連線，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. 識別其他服務帳戶或建立可存取 OU 的新服務帳戶。
2. 然後，使用新的服務帳戶認證來更新檔案系統的自我管理 Active Directory 組態。

   a. 在瀏覽窗格中，選擇 [檔案系統]，然後選擇要更新的檔案系統，就會顯示 [檔案系統詳細資訊] 頁面。

   b. 在 [檔案系統詳細資料] 頁面上，選擇 [網路和安全性] 索引標籤上的

   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UpdateFileSystem中的。

在 FSx 上使用 Windows 檔案伺服器的遠端電源殼層進行疑難排解

您可以使用自訂遠端 PowerShell 管理命令來管理 Windows 檔案伺服器檔案系統的 FSx。

主題

新-F SxSmbShare 命令因單向信任而失敗

如果您具有單向信任，且使用者所在的網域未設定為信任與 Amazon FSx 檔案系統關聯的網域，Amazon FSx 不支援執行`New-FSxSmbShare` PowerShell 命令。

您可以使用下列其中一種解決方案來解決此情況：

- 執行`New-FSxSmbShare`指令的使用者必須與 FSx 檔案系統位於相同的網域中。
- 您可以使用 fsmgmt.msc 圖形用戶界面在您的檔案系統上建立共用。如需詳細資訊，請參閱 使用共用資料夾 GUI 管理檔案共用。

您無法使用遠端存取檔案系統 PowerShell

有許多可能的原因導致無法使用 Remote 連線到您的檔案系統 PowerShell，每個原因都有各自的解析度，如下所示。

若要先確定您可以成功連線到 Windows 遠 PowerShell 端端點，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。

檔案系統的安全性群組缺少允許遠端 PowerShell 連線的必要輸入規則

檔案系統的安全性群組必須具有輸入規則，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 受管理的 Microsoft 作用中目錄與您的內部部署作用中目錄之間設定外部信任

若要使用 Amazon FSx 遠端 PowerShell 搭配 Kerberos 身分驗證，您需要在用戶端上設定本機群組原則以取得樹系搜尋順序。如需詳細資訊，請參閱 Microsoft 文件設定 Kerberos 森林搜尋順序 (KFSO)。

嘗試啟動遠端 PowerShell 工作階段時發生語言當地語系化錯誤

您需要將以下內容添加`-SessionOption`到命令中：`-SessionOption (New-PSSessionOption -uiCulture "en-US")`

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

```
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")
```

您無法在異地同步備份或單一可用區 2 檔案系統上設定 DFS-R

異地同步備份和單一可用區 2 檔案系統不支援 Microsoft 分散式檔案系統複寫 (DFS-R)。

異地同步備份檔案系統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，跨多個可用區域提供高可用性。如需詳細資訊，請參閱 可用性和耐久性：單一可用區和異地同步備份檔案系。

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要求失敗的可能原因有許多，每個原因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 KMS 加密金鑰

儲存容量增加請求失敗，因為 Amazon FSx 無法存取檔案系統的 AWS Key Management Service (AWS KMS) 加密金鑰。

您必須確保 Amazon FSx 能夠存取 AWS KMS 金鑰，才能執行管理動作。使用下列資訊來解決金鑰存取問題。

- 如果 KMS 金鑰已刪除，您必須使用新的 KMS 金鑰從備份建立新的檔案系統。如需詳細資訊，請參閱 演練 2：從備份建立檔案系統。您可以在新的檔案系統可用之後重試要求。
- 如果 KMS 金鑰已停用，請重新啟用該金鑰，然後重試增加儲存區容量的要求。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。

- 如果金鑰因為其擱置刪除而無效，您必須使用新的 KMS 金鑰從備份建立新的檔案系統。您可以在新的檔案系統可用之後重試要求。如需詳細資訊，請參閱 演練 2：從備份建立檔案系統。
- 如果金鑰因為其擱置匯入而無效，您必須等到匯入完成，然後重試增加儲存體的要求。
- 如果超過金鑰的授權限制，您必須要求增加金鑰的授權數目。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。授與配額增加時，請重試增加儲存體的要求。

儲存體或輸送量容量更新失敗，因為自我管理的 Active Directory 設定錯誤

儲存區容量或輸送量容量更新要求失敗，因為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錯誤設定的狀態。

儲存區容量增加失敗，因為輸送量容量不足

儲存區容量增加要求失敗，因為檔案系統的輸送量容量設定為 8 MB/s。

將檔案系統的輸送量容量增加至至少 16 MB/s，然後重試要求。如需詳細資訊，請參閱 管理輸送量容量。

輸送量容量更新為8MB/秒失敗

將檔案系統的輸送量容量修改為 8 MB/s 的要求失敗。

當儲存容量增加要求擱置中或正在進行中時，就可能會發生這種情況。增加儲存容量需要 16 MB/s 的最低輸送量。請等到儲存區容量增加要求完成，然後重試輸送量容量修改要求。

恢復備份失敗時將存儲類型切換到 HDD

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，而且您已將儲存類型從 SSD 變更為 HDD 時，就會發生這個問題。從備份還原失敗，因為您正在還原的備份是在原始檔案系統上增加儲存容量的同時進行中。檔案系統在增加要求前的 SSD 儲存容量低於 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，檔案系統至少擁有 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 存儲將用戶啟動的備份還原到新的文件系統。如需詳細資訊，請參閱 還原備份。

疑難排解卷影複

陰影複製遺失或無法存取時，有許多潛在原因，如下節所述。

主題

- 遺失最舊的陰影複製
- 我所有的影子副本都丟失了
- 無法在最近還原或更新的檔案系統上建立 Amazon FSx 備份或存取陰影複製

遺失最舊的陰影複製

在下列任一情況下，會刪除最舊的陰影複製：

- 如果您有 500 個陰影複本，則下一個陰影複製會取代最舊的陰影複製，無論陰影複製剩餘配置的儲存磁碟區空間為何。
- 如果已達到設定的最大陰影複製儲存容量，即使您的陰影複本少於 500 個，下一個陰影複製也會取代一或多個最舊的陰影複製。

這兩個結果都是預期的行為。如果您配置給陰影複製的儲存空間不足，請考慮增加已配置的儲存空間。

我所有的影子副本都丟失了

在您的檔案系統上 I/O 效能容量不足 (例如，因為您使用的是 HDD 儲存體，因為 HDD 儲存體已經用完了突發容量，或者輸送量容量不足) 可能會造成 Windows Server 刪除所有陰影複本，因為它無法維護具有可用 I/O 效能容量的陰影複本。請考慮下列建議，以協助避免此問題：

- 如果您使用的是硬碟儲存體，請使用 Amazon FSx 主控台或 Amazon FSx API 切換到使用固態硬碟儲存體。如需詳細資訊，請參閱 管理儲存區類型。
- 將檔案系統的輸送量容量增加到預期工作負載的三倍。

- 除了設定的最大陰影複製儲存容量之外，請確定您的檔案系統至少有 320 MB 的可用空間。
- 當您預期檔案系統處於閒置狀態時，排程陰影複製。

如需詳細資訊，請參閱 陰影複製的檔案系統建議。

無法在最近還原或更新的檔案系統上建立 Amazon FSx 備份或存取陰影複製

這是預期的行為。Amazon FSx 在最近還原的檔案系統上重建陰影複製狀態，並且在重建陰影複製狀態時不允許存取卷影複製或備份。

解決檔案系統效能問題

檔案系統效能取決於數個因素，包括您驅動到檔案系統的流量、如何佈建檔案系統，以及任何已啟用的功能，例如重複資料刪除或陰影複製。如需瞭解檔案系統效能的相關資訊，請參閱FSx 適用於 FSx for Windows File Server 效能。

主題

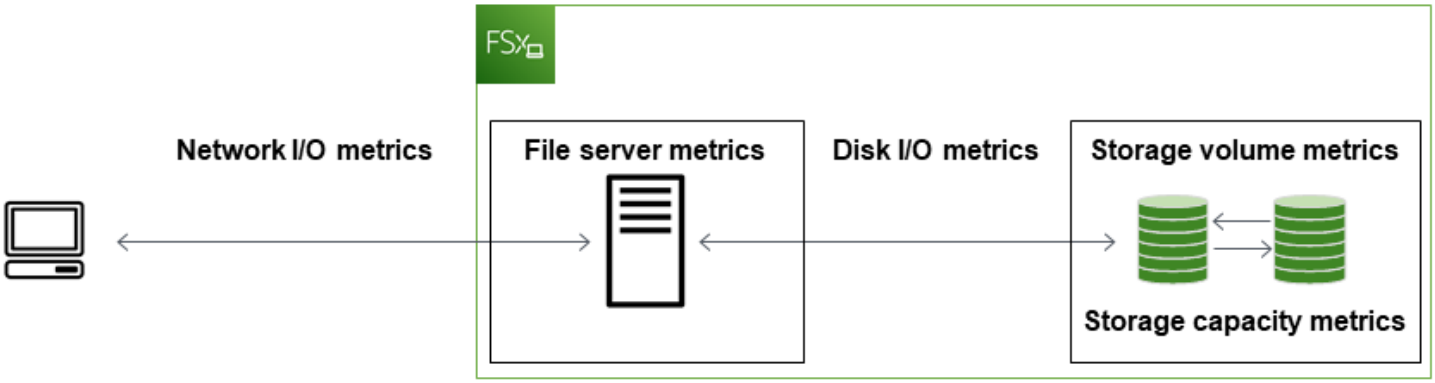
- 如何判斷檔案系統的輸送量和 IOPS 限制？
- 網絡 I/O 和磁盤 I/O 有什麼區別？ 為什麼我的網路 I/O 與磁碟 I/O 不同？
- 為什麼我的 CPU 或記憶體使用率很高，即使我的網路 I/O 很低？
- 什麼是爆裂？ 我的文件系統使用了多少爆發？ 爆發積分用完時會發生什麼？
- 我在 [監視與效能] 頁面上看到警告 — 是否需要變更檔案系統的設定？
- 我的指標暫時遺失了，我應該擔心嗎？

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，請參閱顯示以佈建輸送量容量量為基礎的效能層級表格。

網絡 I/O 和磁盤 I/O 有什麼區別？ 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，這些伺服器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記憶體，可增強最常存取之資料的效能。檔案伺服器也會將流量驅動到裝載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 監控指標 CloudWatch。

為什麼我的 CPU 或記憶體使用率很高，即使我的網路 I/O 很低？

檔案伺服器 CPU 和記憶體使用率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。設定和排程這些功能的方式可能會影響 CPU 和記憶體使用率。

進行中的重複資料刪除工作可能會消耗記憶體。您可以修改重複資料刪除工作的組態，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，或設定最小檔案大小和保留時間以進行最佳化。我們也建議您將重複資料刪除工作設定為在檔案系統負載最低的閒置期間執行。如需詳細資訊，請參閱 重复数据删除。

如果您已啟用以存取為基礎的列舉，當使用者檢視或列出檔案共用，或在儲存擴展工作的最佳化階段，您可能會看到高 CPU 使用率。如需詳細資訊，請參閱 Microsoft 儲存文件中的命名空間上啟用存取型列舉。

什麼是爆裂？ 我的文件系統使用了多少爆發？ 爆發積分用完時會發生什麼？

以檔案為基礎的工作負載通常是尖峰，其特點是短暫而密集的高 I/O 時間，以及突發之間的閒置時間。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外，Amazon FSx 還提供網路 I/O 和磁碟 I/O 作業在一段時間內提升到更高速度的功能。

Amazon FSx 使用 I/O 信用機制根據平均使用率分配輸送量和 IOPS — 檔案系統在輸送量和 IOPS 使用量低於其基準限制時會累積積分，而且可以在需要時使用這些積分超出基準限制 (達到突發限制)。如需檔案系統的成組分解限制和持續時間的詳細資訊，請參閱FSx 適用於 FSx for Windows File Server 效能。

我在 [監視與效能] 頁面上看到警告 — 是否需要變更檔案系統的設定？

[監視與效能] 頁面包含警告，指出最近的工作負載需求何時已接近或超過您設定檔案系統的方式所決定的資源限制。這並不一定表示您需要變更組態，不過如果您不採取建議的動作，您的檔案系統可能已針對工作負載佈建不足。

如果導致警告的工作負載是非典型的，並且您不希望它繼續下去，則不採取任何行動並密切監控您未來的使用情況可能是安全的。不過，如果造成警告的工作負載是一般的工作負載，而且您預期工作負載會持續下去，甚至加強，我們建議您遵循建議的動作來提高檔案伺服器效能 (藉由增加輸送量容量) 或增加儲存磁碟區效能 (藉由增加儲存容量，或從 HDD 切換至 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：
>
> - 儲存容量擴充的最佳化階段可產生更高的磁碟輸送量，如中所述 增加儲存容量並提高檔案系統效能
> - 對於異地同步備份檔案系統，輸送量容量擴充、硬體更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必須在主要和次要檔案伺服器之間進行同步處理，而 Windows Server 會執行可能會耗用磁碟 I/O 資源的資料同步化工作。如需詳細資訊，請參閱 管理輸送量容量。

我的指標暫時遺失了，我應該擔心嗎？

在檔案系統維護、基礎結構元件更換期間，以及無法使用可用區域時，單一可用區檔案系統將會無法使用。在這些時間內，度量將無法使用。

在異地同步備份部署中，Amazon FSx 會在不同的可用區域自動佈建和維護備用檔案伺服器。如果發生檔案系統維護或意外服務中斷，Amazon FSx 會自動容錯移轉至次要檔案伺服器，讓您無需手動介入即可繼續存取資料。在檔案系統容錯移轉和故障回復的短暫期間內，量度可能暫時無法使用。

其他資訊

本節提供支援但已淘汰的 Amazon FSx 功能的參考資料。

主題

設定自訂備份排程

我們建議您使用 AWS Backup 來設定檔案系統的自訂備份排程。如果您需要比使用時更頻繁地安排備份，則此處提供的資訊僅供參考 AWS Backup。

啟用後，Amazon FSx for Windows File Server 會在每日備份時段中，每天自動備份一次檔案系統。Amazon FSx 會強制執行您為這些自動備份指定的保留期。它還支持用戶啟動的備份，因此您可以隨時進行備份。

接下來，您可以找到資源和配置來部署自定義備份調度。自訂備份排程會根據您定義的自訂排程，在 Amazon FSx 檔案系統上執行使用者啟動的備份。例子可能是每六個小時一次，每週一次，依此類推。此指令碼也會設定刪除超過指定保留期間的備份。

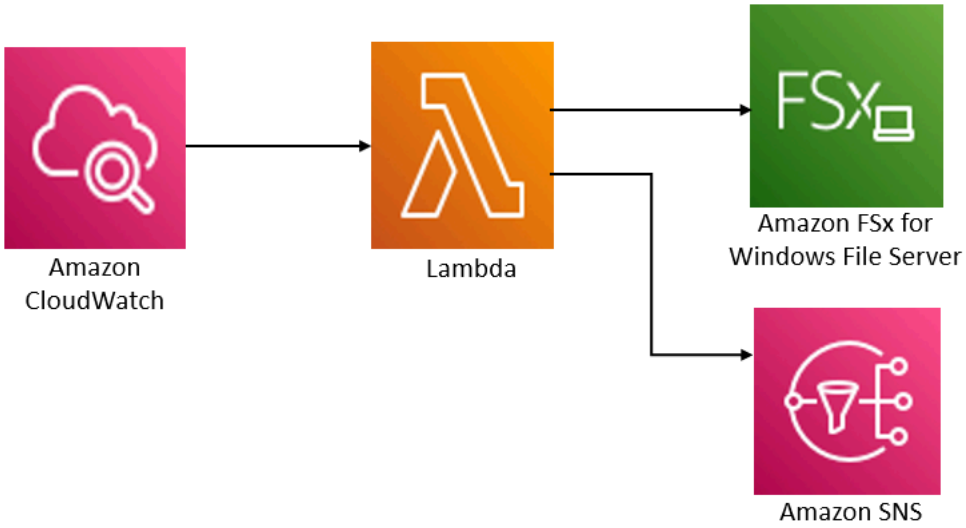
解決方案會自動部署所有必要的元件，並採用下列參數：

- 文件系統
- 用於執行備份的 CRON 排程模式
- 備份保留期 (以天為單位)
- 備份名稱標籤

如需 CRON 排程模式的詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的規則排程運算式。

架構概觀

部署此解決方案會在中建置下列資源 AWS 雲端。



此解決方案會執行下列作業：

1. AWS CloudFormation 範本會部署 CloudWatch 事件、Lambda 函數、Amazon SNS 佇列和 IAM 角色。IAM 角色授予 Lambda 函數呼叫 Amazon FSx API 操作的權限。
2. 在初始部署期間，CloudWatch 事件會依照您定義為 CRON 模式的排程執行。此事件會叫用解決方案的備份管理員 Lambda 函數，該函數會叫用 Amazon FSx `CreateBackup` API 作業以啟動備份。
3. 備份管理員會使用擷取指定檔案系統的現有使用`DescribeBackups`者啟動備份清單。然後，它會刪除比您在初始部署期間指定的保留期間更早的備份。
4. 如果您選擇在初始部署期間通知的選項，備份管理員會在成功備份時將通知訊息傳送到 Amazon SNS 佇列。發生故障時，永遠會傳送通知。

AWS CloudFormation 範本

此解決方案用 AWS CloudFormation 於自動化 Amazon FSx 自訂備份排程解決方案的部署。若要使用此解決方案，請下載 fsx 排程 AWS CloudFormation 備份範本。

自動化部署

下列程序會設定並部署此自訂備份排程解決方案。部署大約需要五分鐘。在開始之前，您的帳戶中必須具有在 Amazon 虛擬私有雲 (Amazon VPC) 中執行的 Amazon FSx 檔案系統的識別碼。 AWS 如需建立這些資源的詳細資訊，請參閱開始使用適用於 FSx for Windows File Server 的 Amazon FSx。

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

啟動自訂備份解決方案堆疊

1. 下載 fsx 排程 AWS CloudFormation 備份範本。如需有關建立 AWS CloudFormation 堆疊的詳細資訊，請參閱《使用指南》中的〈在 AWS CloudFormation 主控台上建立堆疊AWS CloudFormation〉。

   > **Note**
   >
   > 依預設，此範本會在美國東部 (維吉尼亞北部) AWS 區域啟動。Amazon FSx 目前僅在特定 AWS 區域的情況下提供。您必須在提供 Amazon FSx 的 AWS 區域啟動此解決方案。如需詳細資訊，請參閱中的 Amazon FSx 一節AWS 區域 和.AWS 一般參考

2. 對於「參數」，請檢閱範本的參數，並根據檔案系統的需求加以修改。此解決方案使用下列預設值。

參數	預設	描述
Amazon FSx 檔案系統識別碼	無預設值	您要備份之檔案系統的檔案系統 ID。
備份的 CRON 排程模式。	0 0/4 *? *	執行 CloudWatch 事件的排程，觸發新備份並刪除保留期以外的舊備份。
Backup 保留 (天數)	30	保留使用者啟動的備份的天數。Lambda 函數會刪除使用者啟動的備份時間超過此天數。
備份名稱	使用者排程備份	這些 Backup 的名稱，顯示在 Amazon FSx 管理主控台的「備份名稱」欄中。

參數	預設	描述
Backup 通知	是	選擇是否在成功起始備份時收到通知。如果發生錯誤，則始終會發送通知。
電子郵件地址	無預設值	訂閱 SNS 通知的電子郵件地址。

3. 選擇下一步。
4. 在「選項」中選擇「下一步」
5. 對於「檢閱」，請檢閱並確認設定。您必須選取確認範本建立 IAM 資源的核取方塊。
6. 選擇建立以部署堆疊。

您可以在 AWS CloudFormation 主控台的 [狀態] 欄中檢視堆疊的狀態。您應該會在大約五分鐘內看到「建立 _ 完成」狀態。

其他選項

您可以使用此解決方案建立的 Lambda 函數，對多個 Amazon FSx 檔案系統執行自訂排程備份。檔案系統識別碼會傳遞至 CloudWatch 事件輸入 JSON 中的 Amazon FSx 函數。傳遞至 Lambda 函數的預設 JSON 如下所示，其中的值`FileSystemId`和`SuccessNotification`從啟動 AWS CloudFormation 堆疊時指定的參數傳遞。

```
{
 "start-backup": "true",
 "purge-backups": "true",
 "filesystem-id": "${FileSystemId}",
 "notify_on_success": "${SuccessNotification}"
}
```

若要排程其他 Amazon FSx 檔案系統的備份，請建立另一個 CloudWatch 事件規則。您可以使用 Schedule 事件來源，並將此解決方案建立的 Lambda 函數做為目標。在「配置輸入」下選擇「常量（JSON 文本）」。對於 JSON 輸入，只需將 Amazon FSx 檔案系統的檔案系統識別碼替換為備份即可。`${FileSystemId}`另外，替換上面的 JSON `${SuccessNotification}` 中的一個`Yes`或`No`代替。

您手動建立的任何其他 CloudWatch 事件規則都不屬於 Amazon FSx 自訂排程備份解決方案 AWS CloudFormation 堆疊的一部分。因此，如果刪除堆棧，它們不會被刪除。

使用 Microsoft 分佈式文件系統複製

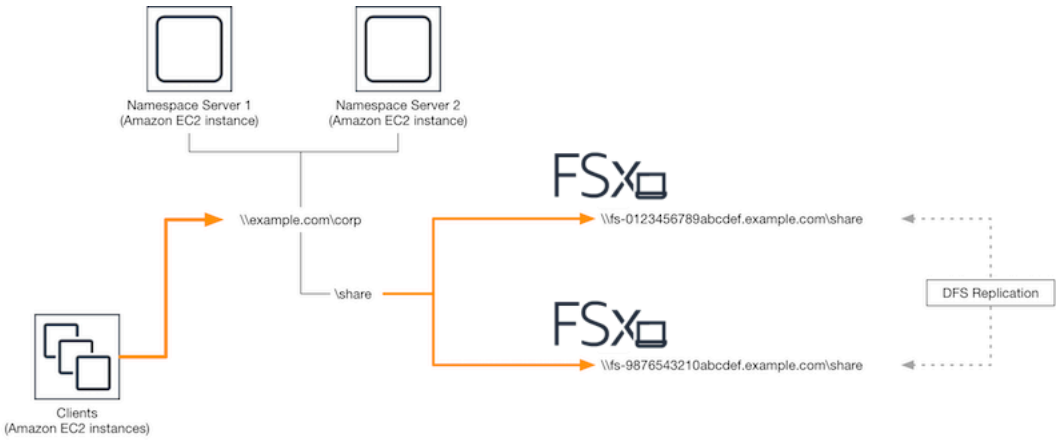
> **Note**
>
> 若要為 Windows 檔案伺服器實作 FSx 的高可用性，我們建議使用 Amazon FSx 異地同步備份。如需 Amazon FSx 異地同步備份的詳細資訊，請參閱 可用性和耐久性：單一可用區和異地同步備份檔案系

Amazon FSx 支援將 Microsoft 分散式檔案系統 (DFS) 用於跨多個可用區域 (AZ) 的檔案系統部署，以取得異地同步備份的可用性和耐久性。使用 DFS 複寫，您可以自動複寫兩個檔案系統之間的資料。使用 DFS 命名空間，您可以將一個檔案系統設定為主要檔案系統，另一個檔案系統設定為待命，並在主要檔案沒有回應時自動容錯移轉至待命。

使用 DFS 複寫之前，請執行下列步驟：

- 依照 Amazon FSx 入門指南中所述設定您Step 8的安全群組。
- 在一 AWS 個區域內的不同 AZ 中建立兩個 Amazon FSx 檔案系統。如需建立檔案系統的詳細資訊，請參閱將資料寫入檔案共用。
- 請確定兩個檔案系統都是相同的 AWS Directory Service for Microsoft Active Directory。
- 建立檔案系統之後，請記下它們的檔案系統 ID 以供稍後使用。

在下列主題中，您可以找到如何使用 Amazon FSx 在 AZ 之間設定和使用 DFS 複寫和 DFS 命名空間容錯移轉的說明。



設定 DFS 複寫

您可以使用 DFS 複寫在兩個 Amazon FSx 檔案系統之間自動複寫資料。此複製是雙向的，表示您可以寫入任一檔案系統，而變更會複製到另一個檔案系統。

> **Important**
>
> 您無法使用 DFS 管理使用者介面中的 Microsoft 視窗系統管理工具 (dfsmgmt.msc) 來設定您的 FSx for Windows File Server 統上的 DFS 複寫。

設定 DFS 複寫 (指令碼式)

1. 啟動執行個體並將其連接到您加入 Amazon FSx 檔案系統的 Microsoft 活動目錄，以開始管理 DFS 的程序。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. 以身為檔案系統管理員群組成員的 Active Directory 使用者身分 Connect 至執行個體。在 AWS 受管理 AD 中，此群組稱為 AWS 委派的 FSx 管理員。在您自我管理的 Microsoft AD 中，此群組稱為網域系統管理員，或是您在建立期間所提供之系統管理員群組的自訂名稱。

   此使用者也必須是具有委派給其 DFS 管理權限之群組的成員。在 AWS 受管理的 AD 中，此群組稱為「 AWS 委派分散式檔案系統管理員」。在您的自我管理 AD 中，此使用者必須是網域管理員的成員，或是您委派 DFS 管理權限的其他群組。

   如需詳細資訊，請參閱 Amazon EC2 使用者指南中的連線到 Windows 執行個體。

3. 下載 FSX-DFSR PowerShell 安裝程序檔。
4. 開啟 [開始] 功能表並輸入PowerShell。從清單中選擇「視窗」 PowerShell。
5. 使用下列指定參數執行指 PowerShell 令碼，以在兩個檔案系統之間建立 DFS 複寫：

   - DFS 複寫群組和資料夾的名稱
   - 要在檔案系統上複寫之資料夾的本機路徑 (例如，`D:\share`針對 Amazon FSx 檔案系統隨附的預設共用)
   - 您在先決條件步驟中建立的主要和備用 Amazon FSx 檔案系統的 DNS 名稱

Example

```
FSx-DFSr-Setup.ps1 -group Group -folder Folder -path ContentPath -
primary FSxFileSystem1-DNS-Name -standby FSxFileSystem2-DNS-Name
```

設定 DFS 複寫 (逐步執行)

1. 啟動執行個體並將其連接到您加入 Amazon FSx 檔案系統的 Microsoft 活動目錄，以開始管理 DFS 的程序。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. 以身為檔案系統管理員群組成員的 Active Directory 使用者身分 Connect 至執行個體。在 AWS 受管理 AD 中，此群組稱為 AWS 委派的 FSx 管理員。在您自我管理的 Microsoft AD 中，此群組稱為網域系統管理員，或是您在建立期間所提供之系統管理員群組的自訂名稱。

   此使用者也必須是具有委派給其 DFS 管理權限之群組的成員。在 AWS 受管理的 AD 中，此群組稱為「 AWS 委派分散式檔案系統管理員」。在您的自我管理 AD 中，此使用者必須是網域管理員的成員，或是您委派 DFS 管理權限的其他群組。

   如需詳細資訊，請參閱 Amazon EC2 使用者指南中的連線到 Windows 執行個體。

3. 開啟 [開始] 功能表並輸入PowerShell。從清單中選擇「視窗」 PowerShell。

4. 如果您尚未安裝 DFS 管理工具，請使用下列命令將它們安裝在執行個體上。

   ```
   Install-WindowsFeature RSAT-DFS-Mgmt-Con
   ```

5. 從 PowerShell 提示中，使用下列命令建立 DFS 複寫群組和資料夾。

   ```
   $Group = "Name of the DFS Replication group"
   $Folder = "Name of the DFS Replication folder"

   New-DfsReplicationGroup –GroupName $Group
   New-DfsReplicatedFolder –GroupName $Group –FolderName $Folder
   ```

6. 使用下列命令決定與每個檔案系統相關聯的 Active Directory 電腦名稱。

```
$Primary = "DNS name of the primary FSx file system"
$Standby = "DNS name of the standby FSx file system"

$C1 = (Get-ADObject -Filter "objectClass -eq 'Computer' -and ServicePrincipalName -
eq 'HOST/$Primary'").Name
$C2 = (Get-ADObject -Filter "objectClass -eq 'Computer' -and ServicePrincipalName -
eq 'HOST/$Standby'").Name
```

7. 將您的檔案系統新增為您使用下列命令建立的 DFS 複寫群組的成員。

```
Add-DfsrMember -GroupName $Group -ComputerName $C1
Add-DfsrMember -GroupName $Group -ComputerName $C2
```

8. 使用下列命令將每個檔案系統的本機路徑 (例如，D:\share) 新增至 DFS 複寫群組。在此程序中，做*file system 1*為主要成員，表示其內容一開始會同步至其他檔案系統。

```
$ContentPath1 = "Local path to the folder you want to replicate on file system 1"
$ContentPath2 = "Local path to the folder you want to replicate on file system 2"

Set-DfsrMembership -GroupName $Group -FolderName $Folder -ContentPath $ContentPath1
 -ComputerName $C1 -PrimaryMember $True
Set-DfsrMembership -GroupName $Group -FolderName $Folder -ContentPath $ContentPath2
 -ComputerName $C2 -PrimaryMember $False
```

9. 使用以下命令在文件系統之間添加連接。

```
Add-DfsrConnection -GroupName $Group -SourceComputerName $C1 -
DestinationComputerName $C2
```

在幾分鐘之內，兩個檔案系統都應該開始同步前面ContentPath指定的內容。

為容錯移轉設定 DFS 命名空間

您可以使用 DFS 命名空間將一個檔案系統視為您的主要檔案系統，另一個檔案系統視為您的待命名空間。如此一來，您就可以在主要項目沒有回應時，將自動容錯移轉設定為待命狀態。DFS 命名空間可讓您將不同伺服器上的共用資料夾群組成單一命名空間，其中單一資料夾路徑可導致儲存在多部伺服器上的檔案。DFS 命名空間由 DFS 命名空間伺服器管理，這些伺服器會將 DFS 命名空間資料夾對應至適當的檔案伺服器的計算執行個體。

若要設定容錯移轉的 DFS 命名空間 (UI)

1. 如果您尚未執行 DFS 命名空間伺服器，請啟動一對使用設定 -DFSN-SERVER.Tem AWS CloudFormation plate 範本範本的高可用性 DFS 命名空間伺服器。如需有關建立 AWS CloudFormation 堆疊的詳細資訊，請參閱《使用指南》中的〈在 AWS CloudFormation 主控台上建立堆疊AWS CloudFormation〉。
2. Connect 至上一個步驟中以「 AWS 委派管理員」群組中的使用者身分啟動的其中一個 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到 Windows 執行個體。
3. 開啟 DFS 管理主控台。打開開始菜單並運行`dfsmgmt.msc`。這麼做會開啟 DFS 管理 GUI 工具。
4. 在動作中，選擇新增命名空間，然後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. 在「名稱」中，輸入您要建立的命名空間 (例如**`corp`**)。
6. 選擇 「編輯設定」，然後根據您的需求設定適當的權限。選擇下一步。
7. 保持預設以網域為基礎的命名空間選項保持選取狀態，並保持選取啟用 Windows Server 2008 模式選項，然後選擇下一步。

   > **Note**
   >
   > 視窗伺服器 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底下選取新建立的命名空間後，選擇動作，然後選擇新增命名空間伺服器。
10. 在命名空間伺服器中，輸入您啟動的第二個 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權限，然後選擇「確定」。
12. ***## [##]#### Amazon FSx ############ UNC ################## [##]#***
13. ***## [##]#### Amazon FSx ############ UNC ################## [##]#***
14. 從「新建檔案夾」視窗中，選擇 「確定」。新資料夾是使用命名空間下的兩個資料夾目標建立的。
15. 針對您要新增至命名空間的每個檔案共用重複最後三個步驟。

若要設定容錯移轉的 DFS 命名空間 () PowerShell

1. 如果您尚未執行 DFS 命名空間伺服器，請啟動一對使用設定 -DFSN-SERVER.Tem AWS CloudFormation plate 範本範本的高可用性 DFS 命名空間伺服器。如需有關建立 AWS

CloudFormation 堆疊的詳細資訊，請參閱《使用指南》中的〈在 AWS CloudFormation 主控台上建立堆疊AWS CloudFormation〉。

2. Connect 至上一個步驟中以「AWS 委派管理員」群組中的使用者身分啟動的其中一個 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到 Windows 執行個體。
3. 開啟 [開始] 功能表並輸入PowerShell。視窗 PowerShell會出現在相符項目清單中。
4. 打開 Windows 的上下文（右鍵單擊）菜單， PowerShell然後選擇以管理員身份運行。
5. 如果您尚未安裝 DFS 管理工具，請使用下列命令將其安裝在執行個體上。

```
Install-WindowsFeature RSAT-DFS-Mgmt-Con
```

6. 如果您還沒有現有的 DFS 命名空間，您可以使用下列 PowerShell 命令建立一個。

```
$NSS1 = computer name of the 1st DFS Namespace server
$NSS2 = computer name of the 2nd DFS Namespace server

$DNSRoot = fully qualified Active Directory domain name (e.g. mydomain.com)
$Namespace = Namespace name you want to use
$Folder = Folder path you want to use within the Namespace
$FS1FolderTarget = Share path to Folder Target on File System 1
$FS2FolderTarget = Share path to Folder Target on File System 2

$NSS1,$NSS2 | ForEach-Object { Invoke-Command -ComputerName $_ -ScriptBlock { mkdir
 “C:\DFS\${using:Namespace}”;
New-SmbShare -Name ${using:Namespace} -Path “C:\DFS\${using:Namespace}” } }

New-DfsnRoot -Path "\\${DNSRoot}\${Namespace}" -TargetPath "\\${NSS1}.${DNSRoot}\
${Namespace}" -Type DomainV2
New-DfsnRootTarget -Path "\\${DNSRoot}\${Namespace}" -TargetPath "\\${NSS2}.
${DNSRoot}\${Namespace}"
```

7. 要在您的 DFS 命名空間中創建一個文件夾，您可以使用以下 PowerShell命令。這樣做會建立一個資料夾，依預設，將存取資料夾的運算執行個體引導至主要 Amazon FSx 檔案系統。

```
$FS1 = DNS name of primary FSx file system
New-DfsnFolder -Path “\\${DNSRoot}\${Namespace}\${Folder}" -TargetPath “\\${FS1}\
${FS1FolderTarget}” -EnableTargetFailback $True -ReferralPriorityClass GlobalHigh
```

8. 將您的備用 Amazon FSx 檔案系統新增至相同的 DFS 命名空間資料夾。如果存取資料夾的運算執行個體無法連線至主要 Amazon FSx 檔案系統，則會回復到此檔案系統。

```
$FS2 = DNS name of secondary FSx file system
New-DfsnFolderTarget -Path “\\${DNSRoot}\${Namespace}\${Folder}" -TargetPath “\\
${FS2}\${FS2FolderTarget}”
```

您現在可以使用前面指定的 DFS 命名空間資料夾的遠端路徑，從計算執行個體存取資料。這樣做會將運算執行個體導向主要 Amazon FSx 檔案系統 (如果主要執行個體沒有回應，則會導向待命檔案系統)。

例如，開啟 [開始] 功能表並輸入PowerShell。從清單中選擇Windows PowerShell並執行下列命令。

```
net use Z: \\${DNSRoot}\${Namespace}\${Folder} /persistent:yes
```

使用維護視窗和 FSx 異地同步備份

為了確保異地同步備份檔案系統部署的高可用性，建議您為異地同步備份部署中的兩個 Amazon FSx 檔案系統選擇不重疊的維護時段。這樣做有助於確保在系統維護期間，您的應用程式和使用者可以繼續使用您的檔案資料。

> **Note**
>
> 若要允許進出檔案系統的 DFS 複寫流量，請確定您新增 VPC 安全性群組輸入和輸出規則，如中Amazon VPC 安全群組所述。

文件歷史記錄

- 應用程式介面版本:
- 最新文件更新：2024 年 1 月 17 日

下表說明 Amazon FSx 視窗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
Support 更高層級的 IOPS，處理能力為 4 Gb/s 及更高的檔案系統	FSx for Windows File Server 的輸送量容量為 4 GB 或更高的檔案系統，最大 IOPS 將從 13 萬增加到 150 萬；對於具有 9 Gb/s 或更高輸送量容量的檔案系統，輸送量容量為 6 GB 或更高的檔案系統，從 260K 增加到 300K，而具有 9 Gb/s 或更高容量的檔案系統則從 350K 增加到 400K。如需詳細資訊，請參閱 FSx for Windows File Server 的效能。	2024年1月17日
Amazon FSx 更新了亞馬遜，亞馬遜，亞馬遜SxFullAccess，亞馬遜SxConsoleFullAccess和亞馬遜SxReadOnlyAccess管理政策SxConsoleReadOnlyAccess SxServiceRolePolicy AWS	Amazon FSx 更新了亞馬遜，亞馬遜SxFullAccess，亞馬遜SxConsoleFullAccess，亞馬遜和亞馬遜 F SxReadOnlyAccess 政策以添加許可。SxConsoleReadOnlyAccess SxServiceRolePolicy `ec2:GetSecurityGroupsForVpc` 如需詳細資訊，請參閱 Amazon FSx 更新受 AWS 管政策。	2024 年 1 月 9 日

Amazon FSx 更新了亞馬遜 SxFullAccess 和亞馬遜管理政策 SxConsoleFullAccess AWS	Amazon FSx 更新了亞馬遜 SxFullAccess 和亞馬遜SxConsoleFullAccess 政策以添加操作。`ManageCrossAccountDataReplication` 如需詳細資訊，請參閱 Amazon FSx 更新受 AWS 管政策。	2023 年 12 月 20 日
Amazon FSx 更新了亞馬遜 SxFullAccess 和亞馬遜管理政策 SxConsoleFullAccess AWS	Amazon FSx 更新了亞馬遜 SxFullAccess 和亞馬遜SxConsoleFullAccess 政策以添加許可。`fsx:CopySnapshotAndUpdateVolume` 如需詳細資訊，請參閱 Amazon FSx 更新受 AWS 管政策。	2023 年 11 月 26 日
Amazon FSx 更新了亞馬遜 SxFullAccess 和亞馬遜管理政策 SxConsoleFullAccess AWS	Amazon FSx 更新了亞馬遜 SxFullAccess 和亞馬遜 FSxConsoleFullAccess 政策以添加和許可。`fsx:DescribeSharedVPCConfiguration` `fsx:UpdateSharedVPCConfiguration` 如需詳細資訊，請參閱 Amazon FSx 更新受 AWS 管政策。	2023 年 11 月 14 日
增加了更新文件系統存儲類型的 Support	FSx for Windows File Server 的檔案系統現在支援從硬碟儲存類型更新為 SSD 儲存類型。如需詳細資訊，請參閱管理儲存區類型。	2023 年 8 月 9 日

增加了 Support 更高的最大吞吐量容量	FSx for Windows File Server 的檔案系統現在支援高達 12 Gbps 的輸送量容量。如需詳細資訊，請參閱 FSx for Windows File Server 的效能。	2023 年 8 月 9 日
針對固態硬碟 IOPS 佈建新增 Support	FSx for Windows File Server 的檔案系統現在支援固態硬碟 IOPS 佈建，而不受儲存容量影響，最高可達 35 萬 IOPS。如需詳細資訊，請參閱管理 SSD IOPS。	2023 年 8 月 9 日
Amazon FSx 更新了亞馬遜託管政策 SxServiceRolePolicy AWS	Amazon FSx 更新了亞馬遜SxServiceRolePolicy 的`cloudwatch:PutMetricData` 許可。有關更多信息，請參閱亞馬遜 F SxService RolePolicy。	2023 年 7 月 24 日
Amazon FSx 更新了亞馬遜託管政策 SxFullAccess AWS	Amazon FSx 更新了 AmazonF SxFullAccess 政策，以移除`fsx:*`許可並新增特定動作。`fsx`如需詳細資訊，請參閱 AmazonF 政策SxFullAccess。	2023 年 7 月 13 日
Amazon FSx 更新了亞馬遜託管政策 SxConsoleFullAccess AWS	Amazon FSx 更新了 AmazonF SxConsoleFullAccess 政策，以移除`fsx:*`許可並新增特定動作。`fsx`如需詳細資訊，請參閱 AmazonF 政策SxConsoleFullAccess。	2023 年 7 月 13 日

針 Support 適用於 Windows 檔案伺服器的 Amazon FSx 新 CloudWatch 指標增加了支援	FSx for Windows File Server 現在提供額外的 CloudWatch 度量來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，請參閱量度和維度。	2022 年 9 月 22 日
新 Support 檔案系統效能警告的支援	Amazon FSx 現在會在效能和監控視窗中提供警告，當任何一組 CloudWatch 指標方法或超過這些指標的預定閾值時。每個警告也會提供可行的建議，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
增加了增強文件系統性能監控的 Support	適用於 Windows 檔案伺服器檔案系統的 FSx 的 Amazon FSx 主控台檔案系統監控儀表板包括新的摘要、儲存和效能區段。這些段落會顯示新測 CloudWatch 量結果的圖形，可提供您增強的效能監控功能。如需詳細資訊，請參閱使用 CloudWatch.	2022 年 9 月 22 日
已新增 Support AWS PrivateLink 介面 VPC 端點的支援。	您現在可以使用介面虛擬私人雲端端點從 VPC 存取 Amazon FSx API，而無需透過網際網路傳送流量。如需詳細資訊，請參閱 Amazon FSx 和介面 VPC 端點。	2022 年 4 月 5 日

增加了對 Amazon Kendra 的 Support	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，讓您對檔案系統上儲存的文件中包含的資訊進行索引和搜尋。如需詳細資訊，請參閱搭配 Amazon Kendra 使用 FSx for Windows File Server。	2022年3月26日
新 Support 檔案存取稽核的支援	您現在可以啟用對檔案、資料夾和檔案共用之使用者存取的稽核功能。您可以選擇將稽核事件日誌傳送至 Amazon CloudWatch 日誌或 Amazon 資料 Firehose 服務。如需詳細資訊，請參閱檔案存取稽核。	2021 年 6 月 8 日
增加了複製備份的 Support	您現在可以使用 Amazon FSx 將同一帳戶內的備份複製到另一個 AWS 帳戶 AWS 區域 (跨區域副本) 或相同 AWS 區域 (區域內副本) 中的備份。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-developed 的可自訂 AWS CloudFormation 範本，當檔案系統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

Support 使用非私有 IP 位址進行用戶端存取	您可以使用非私人 IP 位址，透過內部部署用戶端存取 Windows 檔案伺服器檔案系統的 FSx。如需詳細資訊，請參閱支援的環境。您可以將 FSx FSx for Windows File Server 檔案系統加入自我管理的 Microsoft 作用中目錄與 DNS 伺服器和 AD 網域控制站使用非私人 IP 位址。如需詳細資訊，請參閱將 Amazon FSx 與您的自我管理 Microsoft 活動目錄搭配使用。	2020 年 12 月 17 日
增加了使用 DNS 別名的 Support	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 別名存取檔案系統。	2020 年 11 月 9 日
增加了 Amazon 彈性容器服務的 Support	您現在可以將 FSx 用於 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 AWS Backup	除了使用 AWS Backup 原生 Amazon FSx 備份之外，您現在還可以使用備份和還原 FSx 檔案系統。如需詳細資訊，請參閱AWS Backup 搭配 Amazon FSx 使用。	2020 年 11 月 9 日

新 Support 輸送量容量擴充的支援	您現在可以隨著輸送量需求的發展，修改 Windows 檔案伺服器檔案系統的現有 FSx 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 Support 儲存容量擴充的支援	您現在可以隨著儲存需求的演變，增加現有 FSx 適用於 Windows 檔案伺服器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
Support 硬盤驅動器（HDD）存儲	將 FSx 用於 Windows 檔案伺服器時，硬碟儲存可為您提供價格和效能彈性。如需詳細資訊，請參閱使用 Amazon FSx 將成本最佳化。	2020 年 3 月 26 日
增加了對文件傳輸的 Support AWS DataSync	您現在可以使 AWS DataSync 用在 FSx (適用於 Windows 檔案伺服器) 之間傳輸檔案。如需詳細資訊，請參閱將檔案移轉至 Amazon FSx for Windows File Server 使用 AWS DataSync)。	2020 年 2 月 4 日
FSx FSx for Windows File Server 版本支援其他 Windows 檔案系統管理工作	您現在可以使用 Amazon FSx CLI 進行遠端管理，管理檔案共用、重複資料刪除、儲存配額和傳輸中加密檔案共用。PowerShell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 的原生異地同步備份支援	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 (AZ) 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的檔案	您現在可以使用 Microsoft Windows 原生的共用資料夾工具來管理使用者工作階段，並在您的 FSx for Windows File Server 系統) 上開啟檔案。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 發布對 Microsoft 視窗卷影副本的支持	您現在可以在 FSx 上設定 Windows 檔案伺服器檔案系統的視窗陰影複製。陰影複製可讓您的使用者輕鬆還原檔案變更，並透過將檔案還原為舊版來比較檔案版本。如需詳細資訊，請參閱使用陰影複製。	2019 年 7 月 31 日
Amazon FSx 發布共享 Microsoft 活動目錄支持	您現在可以將 FSx for Windows File Server 檔案系統加入到不同 VPC 中或與檔案系統 AWS 帳戶 不同的 AWS Managed Microsoft AD 目錄。如需詳細資訊，請參閱使用中目錄 Support。	2019 年 6 月 25 日

Amazon FSx 發布增強的 Microsoft 活動目錄支持	您現在可以將 FSx for Windows File Server 的檔案系統加入自我管理的 Microsoft 活動目錄網域，無論是內部部署或雲端。如需詳細資訊，請參閱使用中目錄 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，請參閱安全性和資料保護。	2019 年 5 月 16 日
新增有關 VPN 和區域間 VPC 對 AWS Direct Connect等連線支援的澄清注意事項	在 2019 年 2 月 22 日之後建立的 Amazon FSx 檔案系統可使用 AWS Direct Connect VPN 和區域間虛擬私人雲 VPC 對等來存取。如需詳細資訊，請參閱支援的存取方法。	2019 年 2 月 25 日
AWS Direct Connect，VPN 和區域間 VPC 對等連接支持	您現在可以從現場部署資源和不同 Amazon VPC 或中的資源存取適用於 Windows 檔案伺服器的 Amazon FSx 檔案伺服器檔案系統。 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 FSx for Windows File Server 提供全受管的 Microsoft 視窗檔案伺服器，並由完全原生的 Windows 檔案系統支援。適用於 Windows 檔案伺服器的 Amazon FSx 提供各種功能、效能和相容性，可輕鬆地將企業應用程式移轉至 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。