



# **Amazon FSX以取得ONTAP 相關文件**

## **Amazon FSx for ONTAP**

NetApp  
May 20, 2022

# 目錄

Amazon FSX以取得ONTAP 相關文件	1
Amazon FSX for ONTAP Sfor Sf2的新功能	2
2022年2月27日	2
2021年10月31日	2
2021年10月4日	2
2021年9月2日	2
開始使用	4
深入瞭解Amazon FSX for ONTAP Sf	4
Amazon FSX for ONTAP Sfor Sf.入門	5
設定FSXfor ONTAP Sfor Sf的權限	5
FSXfor ONTAP Sfor Sf的安全群組規則	7
使用Amazon FSX ONTAP for Sfuse	14
建立及管理Amazon FSX以利ONTAP 實現不工作環境	14
為Amazon FSX建立Volume ONTAP for Sf	22
管理Amazon FSX ONTAP for Sf的Volume	27
知識與支援	29
註冊以取得支援	29
取得協助	30
法律聲明	32
版權	32
商標	32
專利	32
隱私權政策	32
開放原始碼	32

# Amazon FSX以取得ONTAP 相關文件

# Amazon FSX for ONTAP Sfor Sf2的新功能

瞭解Amazon FSX for ONTAP Sf2的新功能。

## 2022年2月27日

### 承擔IAM角色

當您建立FSXfor ONTAP the Sfor the Syn可使用 環境時、您現在必須提供IAM角色的ARN、Cloud Manager可用來建立FSXfor ONTAP the Synfrole工作環境。您先前需要提供AWS存取金鑰。

["瞭解如何設定FSX for ONTAP Sfor Sfor Sfor的權限"](#)。

## 2021年10月31日

### 使用Cloud Manager API建立iSCSI Volume

您可以ONTAP 使用Cloud Manager API為FSX建立iSCSI Volume以供使用、並在工作環境中加以管理。

### 建立Volume時、請選取Volume單位

您可以 ["建立磁碟區時、請選取Volume單位（GiB或TiB）"](#) FSX ONTAP for Sfor Sf.

## 2021年10月4日

### 使用Cloud Manager建立CIFS Volume

現在您可以了 ["使用ONTAP Cloud Manager在FSXF中建立CIFS Volume以供其使用"](#)。

### 使用Cloud Manager編輯Volume

現在您可以了 ["使用ONTAP Cloud Manager編輯FSXfor Sf2 Volume"](#)。

## 2021年9月2日

### 支援Amazon FSX for ONTAP Sfy

- ["Amazon FSX for ONTAP Sf"](#) 是一項完整的託管服務、可讓客戶啟動及執行採用NetApp ONTAP 的一套資訊儲存作業系統的檔案系統。FSX for ONTAP VMware提供NetApp客戶在內部部署所使用的相同功能、效能和管理功能、以及原生AWS服務的簡易性、敏捷度、安全性和擴充性。

["深入瞭解Amazon FSX for ONTAP Sf"](#)。

- 您可以在ONTAP Cloud Manager中設定FSXfor Sfor Sfor Sfor Sf有效 工作環境。

["建立Amazon FSX以利ONTAP 不工作環境"](#)。

- 使用AWS和Cloud Manager中的Connector、您可以建立及管理磁碟區、複寫資料、並將FSX for ONTAP 效益與NetApp雲端服務整合、例如Data Sense和Cloud Sync Sf4。

["開始瞭解Cloud Data Sense for Amazon FSX ONTAP for Sf"](#)。

# 開始使用

## 深入瞭解Amazon FSX for ONTAP Sf

"Amazon FSX for ONTAP Sf" 是一項完整的託管服務、可讓客戶啟動及執行採用NetApp ONTAP 的一套資訊儲存作業系統的檔案系統。FSX for ONTAP VMware提供NetApp客戶在內部部署所使用的相同功能、效能和管理功能、以及原生AWS服務的簡易性、敏捷度、安全性和擴充性。

### 功能

- 無需設定或管理儲存設備、軟體或備份。
- 支援CIFS、NFSv3、NFSv4.x及SMB v2.0 - v3.1.1傳輸協定。
- 使用不常存取（IA）的可用儲存層、以低成本、幾乎不受限制的方式儲存資料容量。
- 通過認證、可在對延遲敏感的應用程式（包括Oracle RAC）上執行。
- 可選擇搭售和隨用隨付定價。

### Cloud Manager 的其他功能

- 使用AWS和Cloud Manager中的Connector、您可以建立及管理磁碟區、複寫資料、並將FSX for ONTAP 效益與NetApp雲端服務整合、例如Data Sense和Cloud Sync Sf4。
- Cloud Data Sense採用人工智慧（AI）導向技術、可協助您瞭解資料內容、並識別位於FSX中的敏感資料、以利ONTAP 實現效益。"深入瞭解"。
- 使用NetApp Cloud Sync 解決方案、您可以將資料移轉自動化、移轉至雲端或內部部署的任何目標。"深入瞭解"

### 成本

您的FSX for ONTAP Sf由AWS維護、而非由Cloud Manager維護。"Amazon FSX for ONTAP Sf入門 指南"

使用AWS中的Connector以及Cloud Sync 選用的資料服務（例如、支援功能和Data Sense）、需要額外的成本。

### 支援的地區

"檢視支援的Amazon地區。"

### 取得協助

Amazon FSX ONTAP for Sf1是AWS的第一方解決方案。如有任何疑問或技術支援問題、請使用AWS FSX檔案系統、基礎架構或任何使用此服務的AWS解決方案、使用AWS主控台的Support Center開啟AWS的支援案例。選取「FSXfor ONTAP Sf1」服務和適當的類別。提供建立AWS支援案例所需的其餘資訊。

對於Cloud Manager或Cloud Manager微服務的一般問題、您可以從線上Cloud Manager聊天開始。

如需Cloud Manager或內部微服務專屬的技術支援問題、您可以使用Cloud Manager帳戶層級序號來開啟NetApp支援服務單。您需要註冊Cloud Manager序號、才能啟動支援。

## 限制

- Cloud Manager只能從內部部署或Cloud Volumes ONTAP 從功能複製資料到ONTAP 功能複製功能以供參考的FSX。
- 此時、您可以使用ONTAP 支援的CLI、ONTAP 介紹API或Cloud Manager API來建立iSCSI磁碟區。
- 目前、來自FSXfor ONTAP Sfor Sfis的SnapMirror複寫 "[支援ONTAP 使用CLI](#)"。

## Amazon FSX for ONTAP Sfor Sf.入門

Amazon FSX ONTAP for Sfin入門指南（僅需幾個步驟）。

只ONTAP 要幾個步驟、就能開始使用FSXfor Sfor而已。

在新增Volume之前、您必須先建立Amazon FSX for ONTAP Szing工作環境。您需要 "[設定IAM角色、讓Cloud Manager SaaS能夠承擔角色](#)"。

您必須擁有 "[AWS連接器](#)" 若要開啟FSXfor ONTAP the Sfor the Sfor the Sf12工作環境、建立磁碟區或執行其他動作。需要Connector時、Cloud Manager會在尚未新增連接器時提示您。

您可以ONTAP 使用Cloud Manager建立適用於SfSX Volume的FSX。

使用Cloud Manager來管理磁碟區、並設定其他服務、例如複寫、Cloud Sync 鏡像和Data Sense。

### 相關連結

- "[從 Cloud Manager 建立 Connector](#)"
- "[從 AWS Marketplace 啟動 Connector](#)"
- "[在 Linux 主機上安裝 Connector 軟體](#)"

## 設定FSXfor ONTAP Sfor Sfor的權限

若要建立或管理Amazon FSX for ONTAP the Sfor the Synfrole工作環境、您需要提供IAM角色的ARN、讓Cloud Manager擁有建立FSX for ONTAP the Synfrole環境所需的權限、才能將AWS認證新增至Cloud Manager。

### 設定IAM角色

設定IAM角色、讓Cloud Manager SaaS能夠承擔角色。

#### 步驟

1. 前往目標帳戶中的IAM主控台。
2. 在「存取管理」下、按一下\*「角色」>「建立角色」\*、然後依照步驟建立角色。

請務必執行下列動作：

- 在\*信任的實體類型\*下、選取\* AWS帳戶\*。
- 選取\*其他AWS帳戶\*、然後輸入Cloud Manager SaaS的ID：952013314444。
- 建立包含下列權限的原則：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "fsx:*",
        "ec2:Describe*",
        "ec2:CreateTags",
        "kms:Describe*",
        "kms:List*",
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*"
    }
  ]
}
```

3. 複製IAM角色的角色ARN、以便在下一步將其貼到Cloud Manager中。

IAM角色現在擁有所需的權限。

## 新增認證資料

在您提供IAM角色所需的權限之後、請將角色ARN新增至Cloud Manager。

如果您剛建立IAM角色、可能需要幾分鐘的時間才能使用。請稍候幾分鐘、再將認證資料新增至Cloud Manager。

### 步驟

1. 在 Cloud Manager 主控台右上角、按一下「設定」圖示、然後選取 \* 認證 \*。



2. 按一下\*「Add Credential\*（新增認證\*）」、然後依照精靈中的步驟進行。
  - a. 認證資料位置：選取\* Amazon Web Services > Cloud Manager\*。
  - b. 定義認證資料：提供IAM角色的ARN（Amazon資源名稱）。



c. 審查：確認新認證資料的詳細資料、然後按一下\*新增\*。

您現在可以在建立FSXfor ONTAP the Sfor the Sfor the Sfuse環境時使用認證資料。

## 相關連結

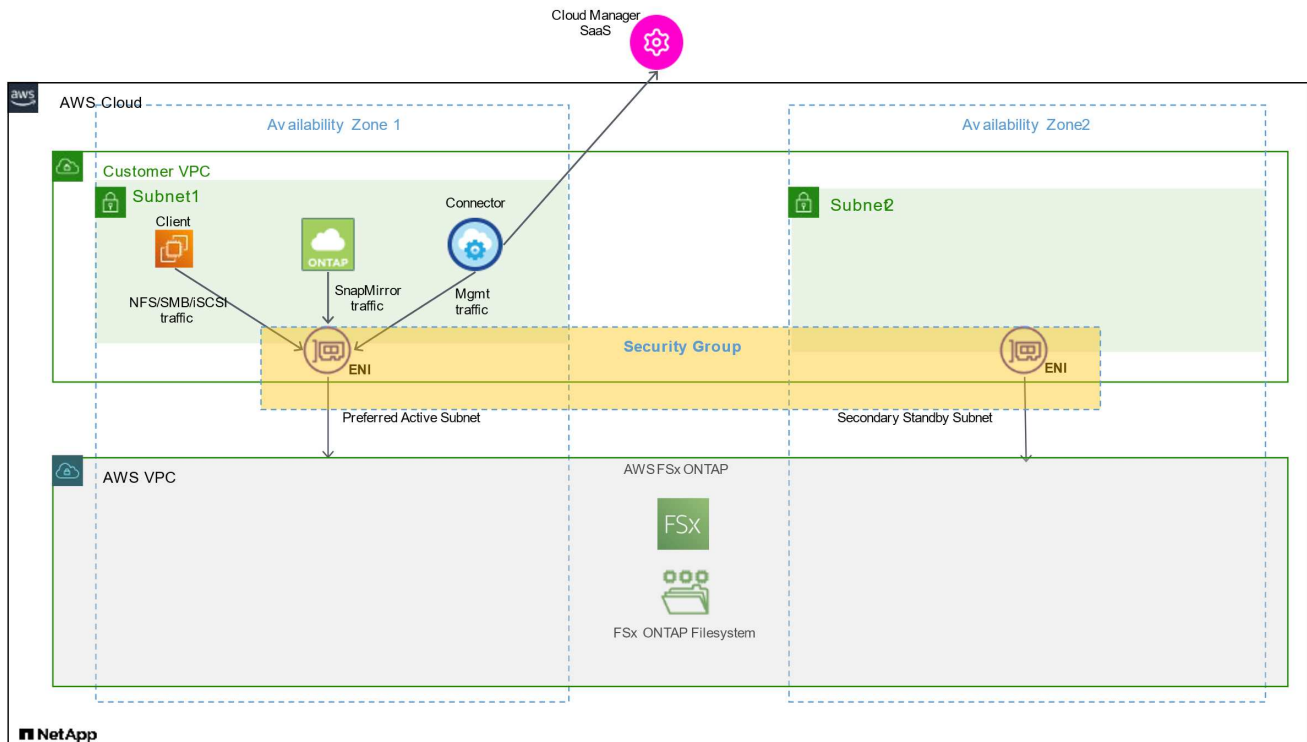
- ["AWS 認證與權限"](#)
- ["管理Cloud Manager的AWS認證資料"](#)

## FSXfor ONTAP Sfor Sf.的安全群組規則

Cloud Manager會建立AWS安全性群組、其中包含Cloud Manager和FSXfor ONTAP the支援成功運作所需的傳入和傳出規則。您可能需要參照連接埠進行測試、或是需要使用自己的連接埠。

### FSXfor ONTAP Sfor Sf.的規則

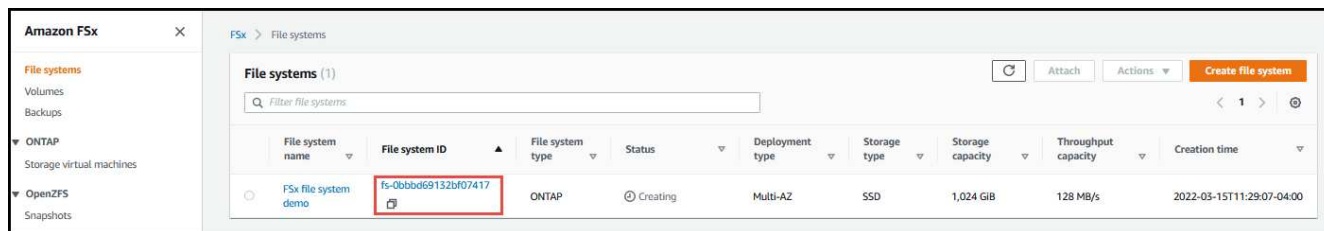
FSX for ONTAP Sfor Sfor Sfor Sfor Security群組需要傳入和傳出規則。此圖說明FSXfor ONTAP EfuS網路 組態和安全性群組需求。



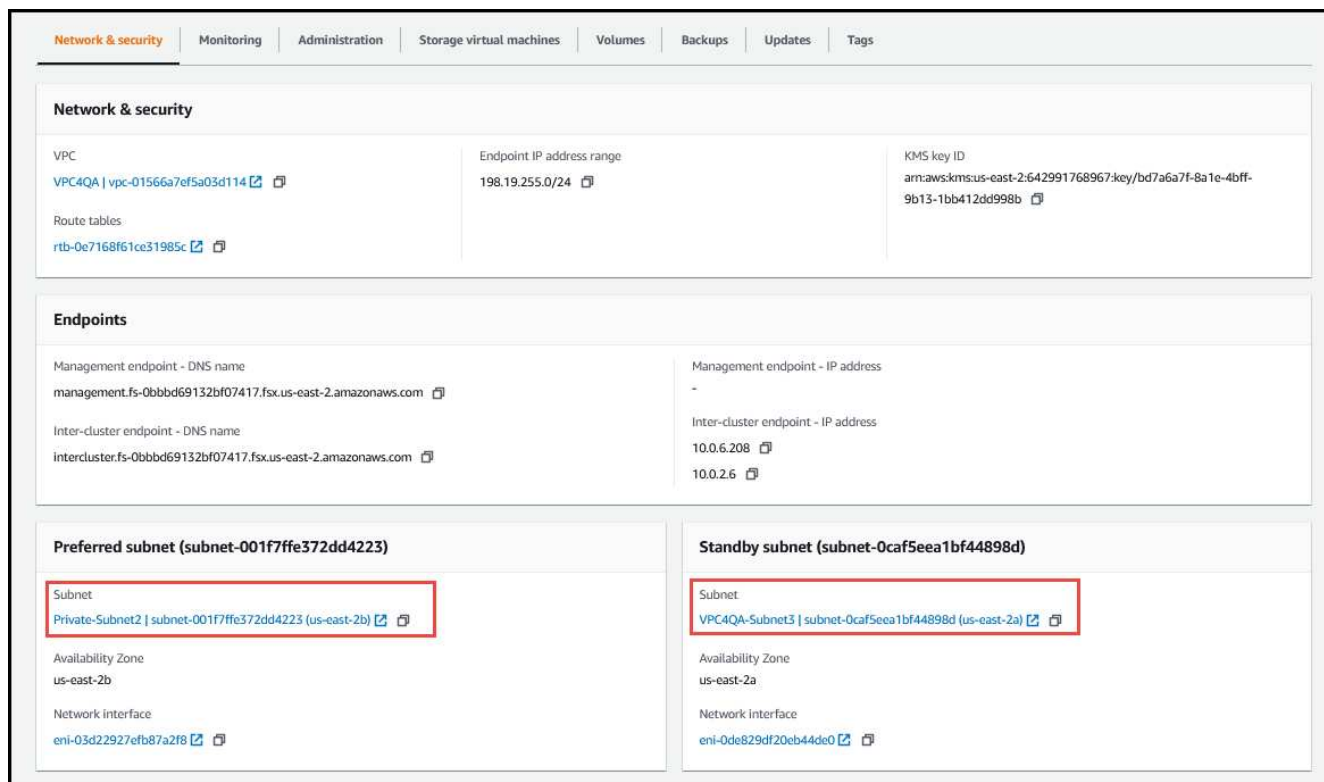
您需要使用AWS管理主控台來找出與Enis相關的安全性群組。

## 步驟

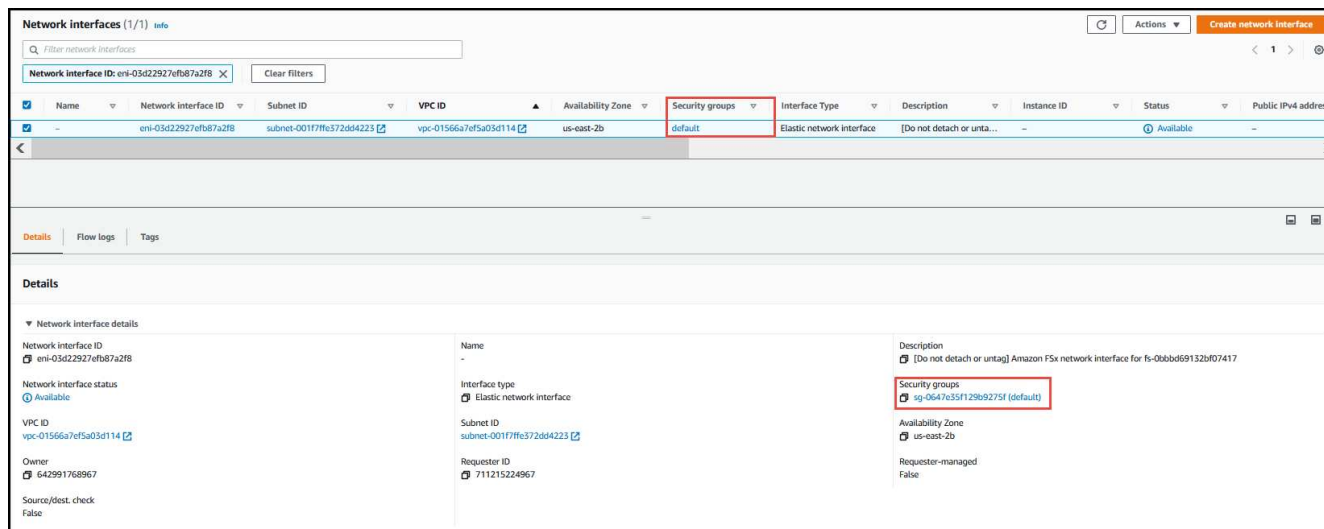
1. 在ONTAP AWS管理主控台開啟FSXfor S應 檔案系統、然後按一下檔案系統ID連結。



2. 在\*網路與安全性\*索引標籤上、按一下偏好的或待命子網路的網路介面ID。



3. 按一下網路介面表中的安全性群組或網路介面的\*詳細資料\*區段。



## 傳入規則

傳輸協定	連接埠	目的
所有 ICMP	全部	Ping 執行個體
HTTPS	443..	從Connector存取fsxadmin管理LIF、將API呼叫傳送至FSX
SSH	22	SSH 存取叢集管理 LIF 的 IP 位址或節點管理 LIF
TCP	111.	遠端程序需要 NFS
TCP	139.	CIFS 的 NetBios 服務工作階段
TCP	161-162	簡單的網路管理傳輸協定
TCP	445	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
TCP	635	NFS 掛載
TCP	749	Kerberos
TCP	2049	NFS 伺服器精靈
TCP	3260	透過 iSCSI 資料 LIF 存取 iSCSI
TCP	4045	NFS 鎖定精靈
TCP	4046	NFS 的網路狀態監控
TCP	10000	使用 NDMP 備份
TCP	11104.	管理 SnapMirror 的叢集間通訊工作階段
TCP	11105.	使用叢集間生命體進行 SnapMirror 資料傳輸
UDP	111.	遠端程序需要 NFS
UDP	161-162	簡單的網路管理傳輸協定
UDP	635	NFS 掛載
UDP	2049	NFS 伺服器精靈
UDP	4045	NFS 鎖定精靈
UDP	4046	NFS 的網路狀態監控
UDP	4049	NFS rquotad 傳輸協定

## 傳出規則

針對FSXfor ONTAP Sfor Sfor支援的預先定義安全性群組會開啟所有傳出流量。如果可以接受、請遵循基本的傳出規則。如果您需要更嚴格的規則、請使用進階的傳出規則。

### 基本傳出規則

針對FSXfor ONTAP Sfor Sfor FSfor的預先定義安全性群組包括下列傳出規則。

傳輸協定	連接埠	目的
所有 ICMP	全部	所有傳出流量

傳輸協定	連接埠	目的
所有 TCP	全部	所有傳出流量
所有的 udp	全部	所有傳出流量

#### 進階傳出規則

您不需要開啟特定的連接埠來進行中介、也不需要為 FSX for ONTAP S for S 節點之間開啟。



來源是 FSX for ONTAP S for the 系統上的介面（IP 位址）。

服務	傳輸協定	連接埠	來源	目的地	目的
Active Directory	TCP	88	節點管理 LIF	Active Directory 樹系	Kerberos V 驗證
	UDP	137.	節點管理 LIF	Active Directory 樹系	NetBios 名稱服務
	UDP	138	節點管理 LIF	Active Directory 樹系	NetBios 資料報服務
	TCP	139.	節點管理 LIF	Active Directory 樹系	NetBios 服務工作階段
	TCP 與 UDP	389	節點管理 LIF	Active Directory 樹系	LDAP
	TCP	445	節點管理 LIF	Active Directory 樹系	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
	TCP	464.64	節點管理 LIF	Active Directory 樹系	Kerberos V 變更及設定密碼 ( Set_change )
	UDP	464.64	節點管理 LIF	Active Directory 樹系	Kerberos 金鑰管理
	TCP	749	節點管理 LIF	Active Directory 樹系	Kerberos V 變更與設定密碼 ( RPCSEC_GSS )
	TCP	88	資料 LIF ( NFS 、 CIFS 、 iSCSI )	Active Directory 樹系	Kerberos V 驗證
	UDP	137.	資料 LIF ( NFS 、 CIFS )	Active Directory 樹系	NetBios 名稱服務
	UDP	138	資料 LIF ( NFS 、 CIFS )	Active Directory 樹系	NetBios 資料報服務
	TCP	139.	資料 LIF ( NFS 、 CIFS )	Active Directory 樹系	NetBios 服務工作階段
	TCP 與 UDP	389	資料 LIF ( NFS 、 CIFS )	Active Directory 樹系	LDAP
	TCP	445	資料 LIF ( NFS 、 CIFS )	Active Directory 樹系	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
	TCP	464.64	資料 LIF ( NFS 、 CIFS )	Active Directory 樹系	Kerberos V 變更及設定密碼 ( Set_change )
	UDP	464.64	資料 LIF ( NFS 、 CIFS )	Active Directory 樹系	Kerberos 金鑰管理
	TCP	749	資料 LIF ( NFS 、 CIFS )	Active Directory 樹系	Kerberos V 變更及設定密碼 ( RPCSEC_GSS )
備份至 S3	TCP	5010 .	叢集間 LIF	備份端點或還原端點	備份與還原備份至 S3 功能的作業
DHCP	UDP	68	節點管理 LIF	DHCP	第一次設定的 DHCP 用戶端
DHCPs	UDP	67	節點管理 LIF	DHCP	DHCP 伺服器
DNS	UDP	53.	節點管理 LIF 與資料 LIF ( NFS 、 CIFS )	DNS	DNS

服務	傳輸協定	連接埠	來源	目的地	目的
NDMP	TCP	18600 – 18699	節點管理 LIF	目的地伺服器	NDMP 複本
SMTP	TCP	25	節點管理 LIF	郵件伺服器	可以使用 SMTP 警示 AutoSupport 來執行功能
SNMP	TCP	161.	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	UDP	161.	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	TCP	162 %	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
	UDP	162 %	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控
SnapMirror	TCP	11104.	叢集間 LIF	叢集間 LIF ONTAP	管理 SnapMirror 的叢集間通訊工作階段
	TCP	11105.	叢集間 LIF	叢集間 LIF ONTAP	SnapMirror 資料傳輸
系統記錄	UDP	514	節點管理 LIF	系統記錄伺服器	系統記錄轉送訊息

## Connector 規則

Connector 的安全性群組需要傳入和傳出規則。

### 傳入規則

傳輸協定	連接埠	目的
SSH	22	提供對 Connector 主機的 SSH 存取權
HTTP	80	提供HTTP存取、從用戶端網頁瀏覽器存取本機使用者介面、以及從Cloud Data Sense連線
HTTPS	443..	提供 HTTPS 存取、從用戶端網頁瀏覽器存取本機使用者介面
TCP	3128	如果您的AWS網路不使用NAT或Proxy、則可提供Cloud Data Sense執行個體以存取國際網路

### 傳出規則

Connector 的預先定義安全性群組會開啟所有傳出流量。如果可以接受、請遵循基本的傳出規則。如果您需要更嚴格的規則、請使用進階的傳出規則。

#### 基本傳出規則

Connector 的預先定義安全性群組包括下列傳出規則。

傳輸協定	連接埠	目的
所有 TCP	全部	所有傳出流量
所有的 udp	全部	所有傳出流量

#### 進階傳出規則

如果您需要嚴格的傳出流量規則、可以使用下列資訊、僅開啟連接器傳出通訊所需的連接埠。



來源 IP 位址為 Connector 主機。

服務	傳輸協定	連接埠	目的地	目的
Active Directory	TCP	88	Active Directory 樹系	Kerberos V 驗證
	TCP	139.	Active Directory 樹系	NetBios 服務工作階段
	TCP	389	Active Directory 樹系	LDAP
	TCP	445	Active Directory 樹系	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構
	TCP	464.64	Active Directory 樹系	Kerberos V 變更及設定密碼 (Set_change)
	TCP	749	Active Directory 樹系	Active Directory Kerberos V 變更及設定密碼 (RPCSEC_GSS)
	UDP	137.	Active Directory 樹系	NetBios 名稱服務
	UDP	138	Active Directory 樹系	NetBios 資料報服務
	UDP	464.64	Active Directory 樹系	Kerberos 金鑰管理
API 呼叫與 AutoSupport 功能	HTTPS	443..	傳出網際網路和 ONTAP 叢集管理 LIF	API 呼叫 AWS 和 ONTAP es供、並傳送 AutoSupport 不只是功能的訊息給 NetApp
API 呼叫	TCP	8088	備份至 S3	API 呼叫備份至 S3
DNS	UDP	53.	DNS	用於 Cloud Manager 的 DNS 解析
雲端資料感測	HTTP	80	Cloud Data Sense執行個體	Cloud Data Sense for Cloud Volumes ONTAP 功能

# 使用Amazon FSX ONTAP for Sfuse

## 建立及管理Amazon FSX以利ONTAP 實現不工作環境

使用Cloud Manager、您可以建立及管理FSXfor ONTAP Sfor Sfor Sfor Sfor Sfor Sfor Sfor Sfor Sfor營運環境、以新增及管理磁碟區及其他資料服務。

### 建立Amazon FSX以利ONTAP 不工作環境

第一步是建立FSX,以利ONTAP 實現不二的工作環境。如果您已在ONTAP AWS管理主控台建立FSXfor the S廳檔案系統、您可以 "使用Cloud Manager探索IT"。

在ONTAP Cloud Manager中建立FSXfor Sfor Sfor Sf有效 作業環境之前、您需要：

- IAM角色的ARN賦予Cloud Manager建立FSX以利ONTAP 運作環境所需的權限。請參閱 "將AWS認證資料新增至Cloud Manager" 以取得詳細資料。
- 您將在其中建立FSX以利ONTAP 執行個體的區域和VPN資訊。

#### 步驟

1. 在Cloud Manager中、新增工作環境、選取位置\* Amazon Web Services\*、然後按一下\* Next\*。
2. 選擇\* Amazon FSX\* for ONTAP Sfor Sfor Sfor 、然後按一下 Next\*（下一步）。

The screenshot displays the 'Add Working Environment' wizard in AWS Cloud Manager. It is divided into two main sections: 'Choose a Location' and 'Choose Type'. In the 'Choose a Location' section, four options are shown: Microsoft Azure, Amazon Web Services (selected with a blue checkmark), Google Cloud Platform, and On-Premises. In the 'Choose Type' section, four options are shown: Cloud Volumes ONTAP (Single Node), Cloud Volumes ONTAP HA (High Availability), Amazon FSx for ONTAP (selected with a blue checkmark, with 'High Availability' chosen from the dropdown), and Kubernetes Cluster (Managed). A search bar at the bottom suggests clicking a link to discover existing Amazon FSx for ONTAP in AWS. A 'Next' button is located at the bottom right.

3. 在ONTAP Cloud Manager中驗證FSXfor的功能。
  - a. 如果您的帳戶中現有的IAM角色具有正確的FSXfor ONTAP 支援AWS權限、請從下拉式清單中選取該角色。



- b. 如果您的帳戶中沒有IAM角色、請按一下\*認證頁面\*、然後依照精靈中的步驟、為AWS IAM角色新增ARN、並使用FSX來取得ONTAP 資訊證明。請參閱 "將AWS認證資料新增至Cloud Manager" 以取得詳細資料。

4. 提供有關FSXfor ONTAP Sfor Sfinstance的資訊：
- a. 輸入您要使用的工作環境名稱。
  - b. 您也可以按一下加號、然後輸入標記名稱和值、藉此建立標記。
  - c. 輸入並確認ONTAP 您想要使用的「叢集」密碼。
  - d. 選取此選項、即可為SVM使用者使用相同的密碼、或設定不同的密碼。

e. 單擊 \* 下一步 \* 。

The screenshot shows the 'Add FSx for ONTAP' wizard at the 'Details and Credentials' step. The interface is divided into two main sections: 'Details' and 'Credentials'. In the 'Details' section, the 'Working Environment Name' is set to 'myfsxenvironment'. There is an 'Add Tags' link with a plus icon. In the 'Credentials' section, the 'User Name' is 'fsxadmin'. The 'ONTAP Cluster Password' and 'Confirm ONTAP Cluster Password' fields are both masked with dots. A checkbox labeled 'Use the same password for SVM user (vsadmin)' is checked. At the bottom, there are 'Previous' and 'Next' buttons.

5. 提供地區與VPC資訊：

- 選取一個區域和VPC、子網路位於至少兩個可用度區域中、因此每個節點都位於專用可用度區域中。
- 接受預設的安全性群組、或選取不同的安全性群組。"AWS安全群組" 控制傳入和傳出流量。這些設定是由AWS管理員設定、並與相關聯 "AWS彈性網路介面 (ENI)" 。
- 為每個節點選取可用度區域和子網路。
- 單擊 \* 下一步 \* 。

The screenshot shows the 'Add FSx for ONTAP' wizard at the 'Region and VPC' step. At the top, there are three dropdown menus: 'Region' (set to 'us-east-2 | US East (Ohio)'), 'VPC' (set to 'VPC4QA - 10.0.0.0/16'), and 'Security Group' (set to 'Default security group'). Below these are two panels for 'Node 1' and 'Node 2'. Each panel has an 'Availability Zone' dropdown (Node 1 is 'us-east-2b', Node 2 is 'us-east-2c') and a 'Subnet' dropdown (Node 1 is '10.0.4.0/24', Node 2 is '10.0.3.0/24'). At the bottom, there are 'Previous' and 'Next' buttons.

6. 將\_CIDR range保留空白、然後按一下\* Next\*自動設定可用範圍。您也可以選擇使用 "AWS Transit閘道" 手動設定範圍。

Add FSx for ONTAP
Floating IP

Floating IP addresses are required for cluster and SVM access and for NFS and CIFS data access.

Floating IPs can migrate between HA nodes if failures occur. To access the data from outside the VPC, you can set up an [AWS transit gateway](#).

CIDR Range

Optional

Example: 10.10.10.10/24

**Notice:** You must specify a CIDR block that is outside of the CIDR blocks for all VPCs in the selected AWS region.

Previous

Next

7. 選取包含通往浮動IP位址路由的路由表。如果VPC中只有一個子網路路由表（主路由表）、Cloud Manager 會自動將浮動IP位址新增至該路由表。單擊 \* 下一步 \* 繼續。

Add FSx for ONTAP
Route Tables

Select the route tables that should include routes to the floating IP addresses. This enables client access to volumes. Clients associated with unselected route tables won't have access to volumes.

[Learn More](#)

2 Route table

<input type="checkbox"/>	Name	Main	ID	Associate with Subnets	Tags	
<input checked="" type="checkbox"/>	VPC4QA	Yes	rtb-0880ec9d aeb55d630	2 Subnets	2	▼
<input type="checkbox"/>	No tag name	No	rtb-0e0c7d9e a4cf05d66	1 Subnet	1	▼


**Notice:** The main route table is the default for the VPC

Previous

Next

8. 接受預設的AWS主金鑰、或按一下\*變更金鑰\*以選取不同的AWS客戶主金鑰（CMK）。如需CMK的詳細資訊、請參閱 "[設定 AWS KMS](#)"。單擊 \* 下一步 \* 繼續。

Add FSx for ONTAP
Data Encryption


AWS Managed Encryption

AWS is responsible for data encryption and decryption operations. Key management is handled by AWS key management services.

---

Default Master Key: aws/fsx [Change Key](#)


Previous
Next

## 9. 設定儲存設備：

- 選取處理量、容量和單位。
- 您可以選擇性地指定IOPS值。如果您未指定IOPS值、Cloud Manager會根據輸入的總容量每GiB 3 IOPS設定預設值。例如、如果您輸入2000 GiB作為總容量、而沒有輸入IOPS值、則有效IOPS值將設為6000。

如果您指定的IOPS值不符合最低需求、則在新增工作環境時會收到錯誤訊息。





Failed to create FSx for ONTAP systems [Show Less](#)

Invalid SSD IOPS provided: 400 IOPS. Amazon FSx does not support provisioning fewer than 3 IOPS per GB of SSD storage capacity on a ONTAP file system.

- 單擊 \* 下一步 \*

Add FSx for ONTAP
Storage Configuration


SSD Disk Properties

Throughput
512 MBps

Capacity
3
Unit
TiB

IOPS Value
400
Optional ⓘ


**Notice:** The current version of FSx does not allow changing the capacity after creation. Also, note that the capacity drives the cost of the service.

Previous
Next

10. 檢閱您的組態：

- 按一下這些索引標籤、檢視ONTAP 您的資訊功能、供應商屬性和網路組態。
- 按一下\*上一個\*以變更任何設定。
- 按一下「新增」以接受設定並建立您的工作環境。

### Review

**myfsxenvironment**  
FSx for ONTAP | HA | Multiple AZs

#### Overview

ONTAP Properties	Provider Properties	Networking
HA Deployment Model	Multiple Availability Zone	
Capacity	3 TiB	
Throughput	512 MBps	

PreviousAdd

Cloud Manager會ONTAP 在「畫版」頁面上顯示您的FSXfor支援的組態設定。



您現在ONTAP 可以使用Cloud Manager、將Volume新增至FSXfor Sfor Sfor Sfor工作環境。

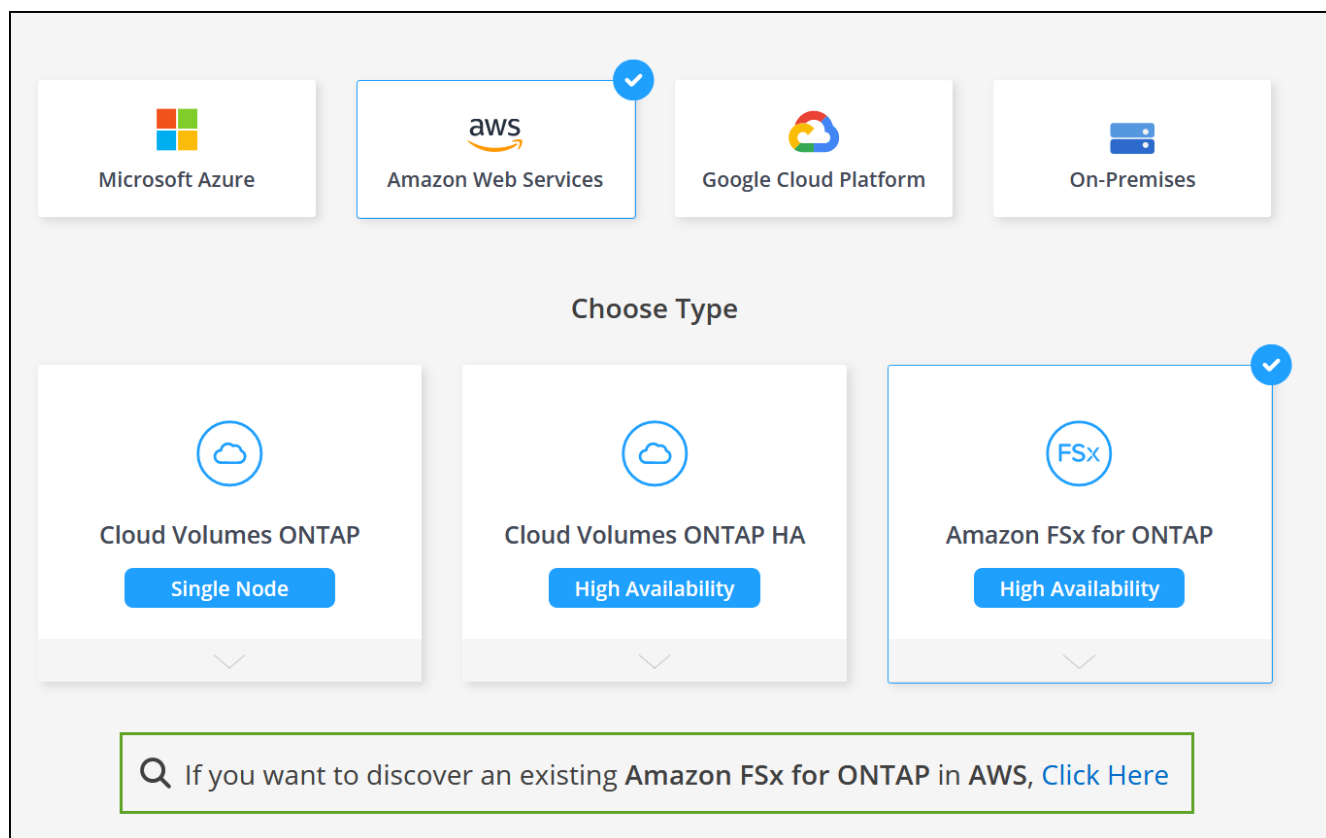
## 探索現有ONTAP 的FSX for Sf供 資料系統使用

如果ONTAP 您使用AWS管理主控台建立FSX for S廳 檔案系統、或是想要還原先前移除的工作環境、您可以使用Cloud Manager來探索它。

### 步驟

- 在Cloud Manager中、按一下\*新增工作環境\*、然後選取\* Amazon Web Services\*。

2. 選擇\* Amazon FSX\* for ONTAP Sfor Sfor Sfor 、然後按一下\*按一下此處。



3. 選取現有認證或建立新認證。單擊 \* 下一步 \* 。

4. 選取您要新增的AWS區域和工作環境。



5. 按一下「\* 新增 \*」。

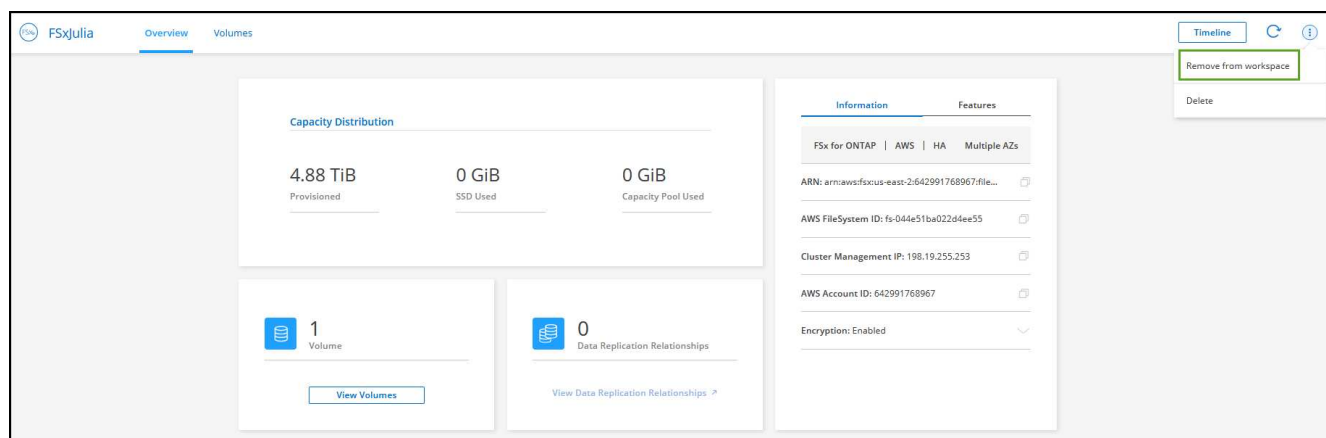
Cloud Manager會顯示您探索到的FSX ONTAP for Sfor Sficity檔案系統。

## 從ONTAP 工作區中移除FSXfor Sfor

您可以從ONTAP Cloud Manager移除FSXfor Sfor支援、而不需刪除FSX for ONTAP S庫 帳戶或磁碟區。您可以ONTAP 隨時將FSX for the Sfor the Sfor the Sfor the Sfor the Sf有效 工作環境新增回Cloud Manager。

步驟

1. 開啟工作環境。如果AWS中沒有Connector、您會看到提示畫面。您可以忽略這一點、然後繼續移除工作環境。
2. 在頁面右上角、選取「動作」功能表、然後按一下「從工作區移除」。



3. 按一下「移除」、從ONTAP Cloud Manager移除FSX for Sfor

## 刪除FSX以利ONTAP 執行作業環境

您可以從ONTAP Cloud Manager刪除FSXfor Sfor

開始之前

- 您必須 "刪除所有Volume" 與檔案系統相關聯。



您將需要AWS中的作用中連接器來移除或刪除磁碟區。

- 您無法刪除包含故障磁碟區的工作環境。在刪除FSX for ONTAP Sfi檔案系統之前、必須先使用AWS管理主控台或CLI刪除故障的磁碟區。



此動作將會刪除與工作環境相關的所有資源。此動作無法復原。

步驟

1. 開啟工作環境。如果AWS中沒有Connector、您會看到提示畫面。您可以忽略這一點、然後繼續刪除工作環境。
2. 在頁面右上角、選取「動作」功能表、然後按一下「刪除」。



3. 輸入工作環境的名稱、然後按一下\*刪除\*。

## 為Amazon FSX建立Volume ONTAP for S

設定工作環境之後、您可以建立及掛載ONTAP 適用於SfSX Volume的FSX。

### 建立磁碟區

您可以在ONTAP Cloud Manager中、從FSX建立及管理NFS和CIFS磁碟區、以利執行運作環境。使用ONTAP Sfxi建立的NFS和CIFS磁碟區也會顯示在您的FSX中ONTAP 、以利執行各種作業環境。

您可以使用ONTAP SfxCLI、ONTAP fisc進API或Cloud Manager API來建立iSCSI磁碟區、並在FSXfor ONTAP 支援功能的環境中使用Cloud Manager來管理這些磁碟區。

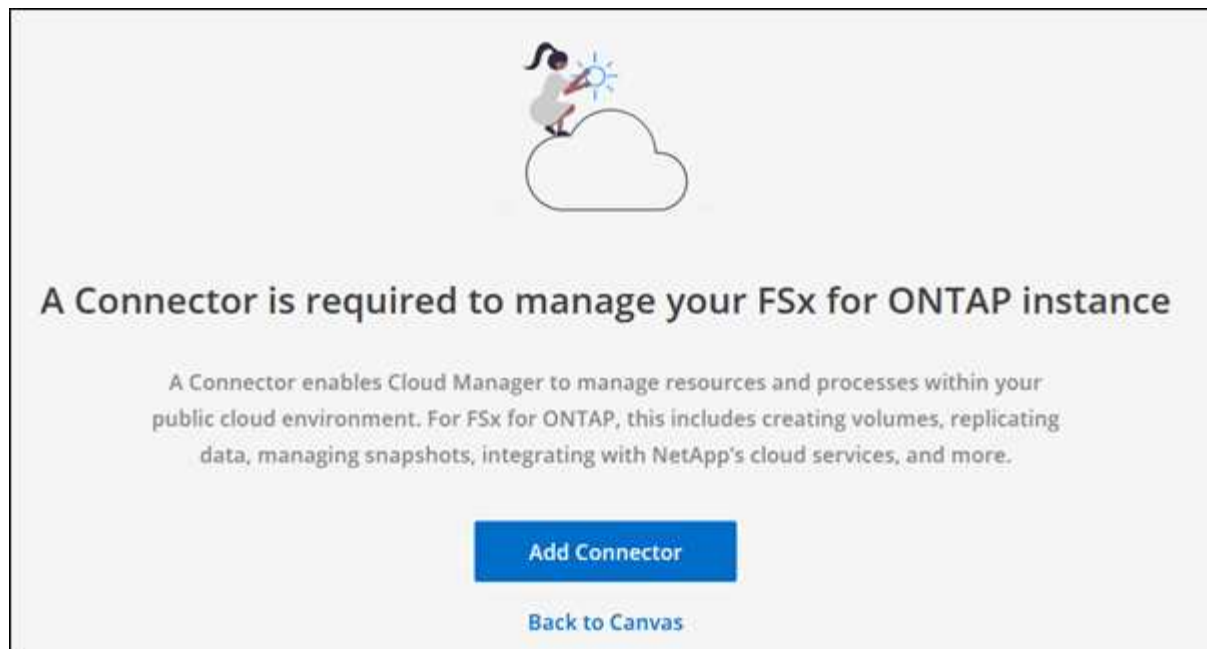
您需要：

- 使用中 "[AWS的連接器](#)"。
- 若要使用SMB、您必須設定DNS和Active Directory。如需DNS和Active Directory網路組態的詳細資訊、請參閱 "[AWS：使用自我管理的Microsoft AD的必要條件](#)"。

### 步驟

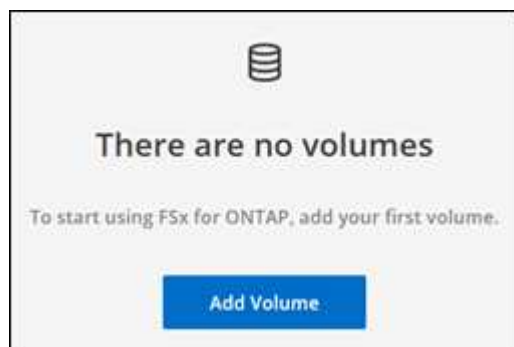
1. 開啟FSX,以利ONTAP 執行不工作環境。
2. 如果您未啟用Connector、系統會提示您新增一個。





3. 按一下「\* Volumes（\*磁碟區

4. 按一下 \* 新增 Volume \*。



5. \* Volume詳細資料與保護\*：

- 輸入新磁碟區的名稱。
- Storage VM（SVM）欄位會根據您工作環境的名稱、自動填入SVM。
- 輸入Volume大小、然後選取單位（GiB或TiB）。請注意、磁碟區大小會隨著使用量而增加。
- 選取快照原則。根據預設、每小時（保留最後六個複本）、每天（保留最後兩個複本）和每週（保留最後兩個複本）會擷取快照。
- 單擊 \* 下一步 \*。

1 Details and Protection   2 Protocol   3 Usage Profile & Tiering Policy   4 Review

### Volume Details & Protection

Volume Name i A

Storage VM (SVM) v  
svm\_FSxJulia

Volume Size i Unit v

1-100000 u GiB

TiB

GiB

Snapshot Policy v  
default

default policy i

6. 傳輸協定：選取NFS或CIFS磁碟區傳輸協定。

a. NFS：

- 選取存取控制原則。
- 選取NFS版本。
- 選取自訂匯出原則。按一下資訊圖示以取得有效的值準則。

✓ Details & Protection   2 Protocol   3 Usage Profile & Tiering Policy   4 Review

### Volume Protocol

Select the volume's protocol: ☒ NFS Protocol ☐ CIFS Protocol

Access Control v  
Custom\_export\_policy

Select NFS Version

☒ NFSv3 ☒ NFSv4

Custom Export Policy i  
10.20.0.0/16

b. CIFS：

- 輸入共用名稱。
- 輸入以分號分隔的使用者或群組。
- 選取磁碟區的權限等級。



如果這是此工作環境的第一個CIFS磁碟區、系統會提示您使用 \_Active Directory 或 \_Workgroup\_ 設定來設定CIFS連線。

- 如果您選取Active Directory設定、則需要提供下列組態資訊。

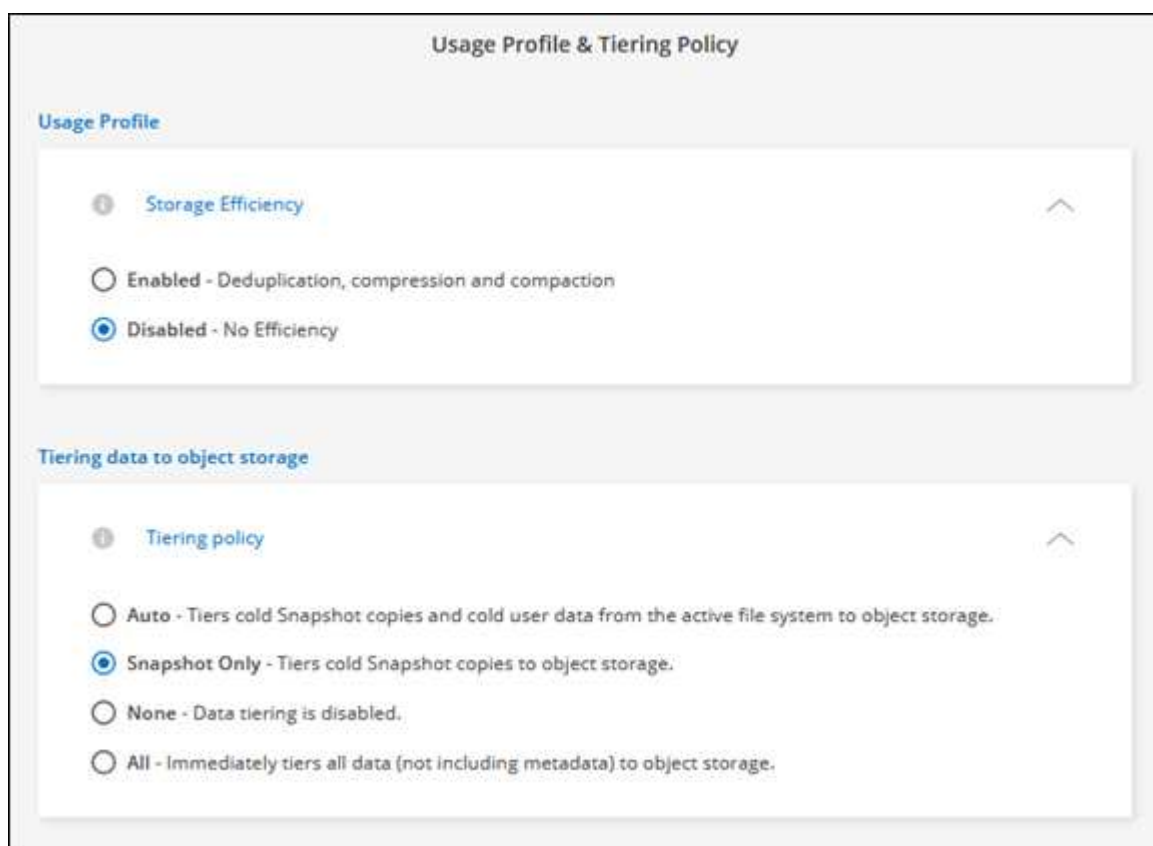
欄位	說明
DNS 主要 IP 位址	提供CIFS伺服器名稱解析的DNS伺服器IP位址。列出的DNS伺服器必須包含所需的服務位置記錄 (SRV),才能找到CIFS伺服器要加入之網域的Active Directory LDAP伺服器和網域控制器。
要加入的 Active Directory 網域	您要CIFS伺服器加入之Active Directory (AD) 網域的FQDN。
授權加入網域的認證資料	具有足夠權限的 Windows 帳戶名稱和密碼、可將電腦新增至 AD 網域內的指定組織單位 (OU)。
CIFS 伺服器 NetBios 名稱	AD 網域中唯一的 CIFS 伺服器名稱。
組織單位	AD 網域中與 CIFS 伺服器相關聯的組織單位。預設值為「CN= 電腦」。
DNS 網域	儲存虛擬機器 (SVM) 的DNS網域。在大多數情況下、網域與 AD 網域相同。
NTP 伺服器	選取*啟用NTP伺服器組態*、以使用Active Directory DNS設定NTP伺服器。如果您需要使用不同的位址來設定 NTP 伺服器、則應該使用 API。請參閱 <a href="#">"Cloud Manager自動化文件"</a> 以取得詳細資料。

- 如果您選取「工作群組」設定、請輸入設定為CIFS的工作群組的伺服器和工作群組名稱。
  - a. 單擊 \* 下一步 \*。

#### 7. 使用設定檔與分層：

- a. 預設會停用\*儲存效率\*。您可以變更此設定以啟用重複資料刪除和壓縮。
- b. 根據預設、\*分層原則\*設為\*僅Snapshot\*。您可以根據需求選擇不同的分層原則。

c. 單擊 \* 下一步 \* 。



8. 審查：檢閱您的Volume組態。按一下\*上一步\*變更設定、或按一下\*新增\*建立磁碟區。

新磁碟區會新增至工作環境。

## 掛載磁碟區

從 Cloud Manager 存取掛載指示、以便將磁碟區掛載至主機。

### 步驟

1. 開啟工作環境。
2. 開啟Volume功能表、然後選取\* Mount the volume \*。



3. 請依照指示來掛載磁碟區。

# 管理Amazon FSX ONTAP for Sfor的Volume

您可以使用ONTAP Cloud Manager來管理Volume、複製和快照、以及變更FSXfor Sfor的分層原則。

## 編輯Volume

建立磁碟區之後、您可以隨時加以修改。

### 步驟

1. 開啟工作環境。
2. 開啟Volume功能表、然後選取\*編輯\*。
  - a. 對於NFS、您可以修改大小和標記。
  - b. 對於CIFS、您可以視需要修改共用名稱、使用者、權限及Snapshot原則。
3. 按一下「\* 套用 \*」。

## 複製磁碟區

建立磁碟區之後、您可以從新的Snapshot建立新的讀寫磁碟區。

### 步驟

1. 開啟工作環境。
2. 開啟Volume功能表、然後選取\* Clone（複製）\*。
3. 輸入複製磁碟區的名稱。
4. 按一下\* Clone（複製）\*。

## 管理Snapshot複本

Snapshot 複本提供磁碟區的時間點複本。建立Snapshot複本、並將資料還原至新磁碟區。

### 步驟

1. 開啟工作環境。
2. 開啟Volume功能表、然後選擇其中一個可用選項來管理Snapshot複本：
  - \* 建立 Snapshot 複本 \*
  - 從**Snapshot**複本還原
3. 依照提示完成選取的動作。

## 變更分層原則

變更磁碟區的分層原則。

### 步驟

1. 開啟工作環境。

2. 開啟Volume功能表、然後選取\*變更分層原則\*。
3. 選取新的磁碟區分層原則、然後按一下\*變更\*。

## 複寫及同步資料

您可以使用Cloud Manager在儲存環境之間複寫資料。若要設定FSXfor ONTAP Sfor Sfor S供 複寫、請參閱 ["在系統之間複寫資料"](#)。

您可以使用Cloud Sync Cloud Manager中的功能、建立同步關係。若要設定同步關係、請參閱 ["建立同步關係"](#)。

## 刪除Volume

刪除不再需要的磁碟區。

您無法使用Cloud Manager刪除先前屬於SnapMirror關係的磁碟區。SnapMirror磁碟區必須使用AWS管理主控台或CLI刪除。

### 步驟

1. 開啟工作環境。
2. 開啟Volume功能表、然後選取\*刪除\*。
3. 輸入工作環境名稱、然後確認您要刪除該磁碟區。從Cloud Manager完全移除磁碟區可能需要一小時的時間。



如果您嘗試刪除複製的Volume、將會收到錯誤訊息。

# 知識與支援

## 註冊以取得支援

在您透過NetApp技術支援開啟支援案例之前、您必須先將NetApp支援網站帳戶新增至Cloud Manager、然後註冊以取得支援。

### 新增一個NSS帳戶

「支援儀表板」可讓您從單一位置新增及管理所有NetApp支援網站帳戶。

#### 步驟

1. 如果您還沒有 NetApp 支援網站帳戶、"[註冊一項](#)"。
2. 在Cloud Manager主控台右上角、按一下「說明」圖示、然後選取\*「支援」\*。



3. 按一下「」**nss管理**」>「新增**nssAccount**」。
4. 出現提示時、按一下\*繼續\*以重新導向至Microsoft登入頁面。

NetApp使用Microsoft Azure Active Directory做為身分識別供應商、提供專為支援與授權所設計的驗證服務。

5. 在登入頁面上、提供您的NetApp支援網站註冊電子郵件地址和密碼、以執行驗證程序。

此動作可讓Cloud Manager使用您的NSS帳戶。

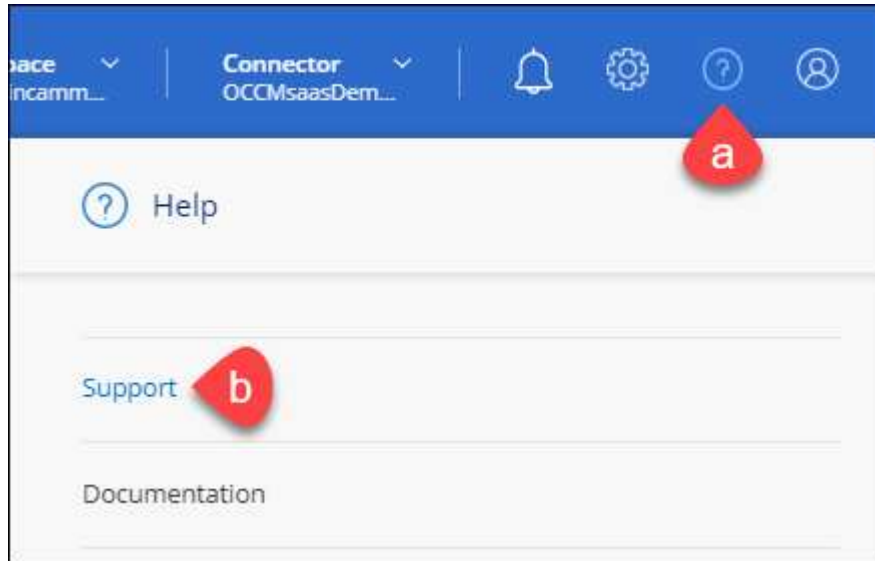
附註：帳戶必須是客戶層級的帳戶（非來賓帳戶或臨時帳戶）。

### 註冊您的帳戶以取得支援

支援註冊可從支援儀表板的Cloud Manager取得。

#### 步驟

1. 在Cloud Manager主控台右上角、按一下「說明」圖示、然後選取\*「支援」\*。



2. 在\* Resources（資源）選項卡中，單擊 Register for Support\*（註冊以獲得支持\*）。
3. 選取您要登錄的NSS認證、然後按一下「登錄」。

## 取得協助

NetApp以多種方式支援Cloud Manager及其雲端服務。我們全年無休提供豐富的免費自助支援選項、例如知識庫（KB）文章和社群論壇。您的支援註冊包括透過網路票證提供遠端技術支援。

### 自我支援

這些選項可供免費使用、一天24小時、一週7天：

- "知識庫"

請搜尋Cloud Manager知識庫、找出有助於疑難排解問題的文章。

- "社群"

加入Cloud Manager社群、追蹤後續討論或建立新討論。

- 文件

您目前正在檢視的Cloud Manager文件。

- mailto：[ng-cloudmanager-feedback@netapp.com](mailto:ng-cloudmanager-feedback@netapp.com) [意見反應電子郵件]

我們非常重視您的意見。提交意見反應、協助我們改善Cloud Manager。

### NetApp支援

除了上述的自我支援選項、您也可以與NetApp支援工程師合作、在您啟動支援之後解決任何問題。



## 步驟

1. 在Cloud Manager中、按一下\*「說明」>「支援」\*。
2. 在「Technical Support（技術支援）」下選擇可用的選項之一：
  - a. 按一下\*致電我們\*以尋找NetApp技術支援的電話號碼。
  - b. 按一下「開啟問題」、選取其中一個選項、然後按一下「傳送」。

NetApp代表將審查您的案例、並盡快回覆您。

# 法律聲明

法律聲明提供版權聲明、商標、專利等存取權限。

## 版權

<http://www.netapp.com/us/legal/copyright.aspx>

## 商標

NetApp、NetApp 標誌及 NetApp 商標頁面上列出的標章均為 NetApp、Inc. 的商標。其他公司與產品名稱可能為其各自所有者的商標。

<http://www.netapp.com/us/legal/netapptmlist.aspx>

## 專利

如需最新的 NetApp 擁有專利清單、請參閱：

<https://www.netapp.com/us/media/patents-page.pdf>

## 隱私權政策

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

## 開放原始碼

通知檔案提供有關 NetApp 軟體所使用之協力廠商版權與授權的資訊。

- ["Cloud Manager 3.9 注意事項"](#)
- ["雲端備份注意事項"](#)
- ["關於本產品的注意事項 Cloud Sync"](#)
- ["雲端分層注意事項"](#)
- ["Cloud Data Sense 注意事項"](#)

## 版權資訊

Copyright©2022 NetApp、Inc.版權所有。美國印製本文件中版權所涵蓋的任何部分、不得以任何形式或任何方式（包括影印、錄製、在未事先取得版權擁有者書面許可的情況下、在電子擷取系統中進行錄音或儲存。

衍生自受版權保護之NetApp資料的軟體必須遵守下列授權與免責聲明：

本軟體係由NetApp「依現狀」提供、不含任何明示或暗示的保證、包括但不限於適售性及特定用途適用性的暗示保證、特此聲明。在任何情況下、NetApp均不對任何直接、間接、偶發、特殊、示範、或衍生性損害（包括但不限於採購替代商品或服務；使用損失、資料或利潤損失；或業務中斷）、無論是在合約、嚴格責任或侵權行為（包括疏忽或其他）中、無論是因使用本軟體而產生的任何責任理論（包括疏忽或其他）、即使已被告知可能造成此類損害。

NetApp保留隨時變更本文所述之任何產品的權利、恕不另行通知。除非NetApp以書面明確同意、否則NetApp不承擔因使用本文所述產品而產生的任何責任或責任。使用或購買本產品並不代表NetApp擁有任何專利權利、商標權利或任何其他智慧財產權。

本手冊所述產品可能受到一或多個美國國家/地區的保護專利、國外專利或申請中。

限制權利圖例：政府使用、複製或揭露受DFARS 252.277-7103（1988年10月）和FAR 52-227-19（1987年6月）技術資料與電腦軟體權利條款（c）（1）（ii）分段所述限制。

## 商標資訊

NetApp、NetApp標誌及所列的標章 <http://www.netapp.com/TM> 為NetApp、Inc.的商標。其他公司和產品名稱可能為其各自所有者的商標。