開始使用
Amazon FSx for ONTAP

NetApp
July 19, 2022

目錄

開始使用 1
深入瞭解Amazon FSX for ONTAP Sf 1
Amazon FSX for ONTAP Sfor Sf.入門 2
設定FSXfor ONTAP Sfor Sfor的權限 2
FSXfor ONTAP Sfor Sf.的安全群組規則 4

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 Sfor Sfor支援帳戶由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的ID。
  - 適用於Cloud Manager SaaS：952013314444
  - AWS GovCloud（美國）：
- 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": "*"
        }
    ]
}
```

從檢視Connector部署原則 "Cloud Manager 原則頁面"。

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）。

      - 如果您使用AWS GovCloud（US）帳戶、請勾選*我使用AWS GovCloud（US）帳戶*。

      - 使用AWS GovCloud驗證將會停用SaaS平台。這是對您帳戶的永久變更、無法復原。

   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

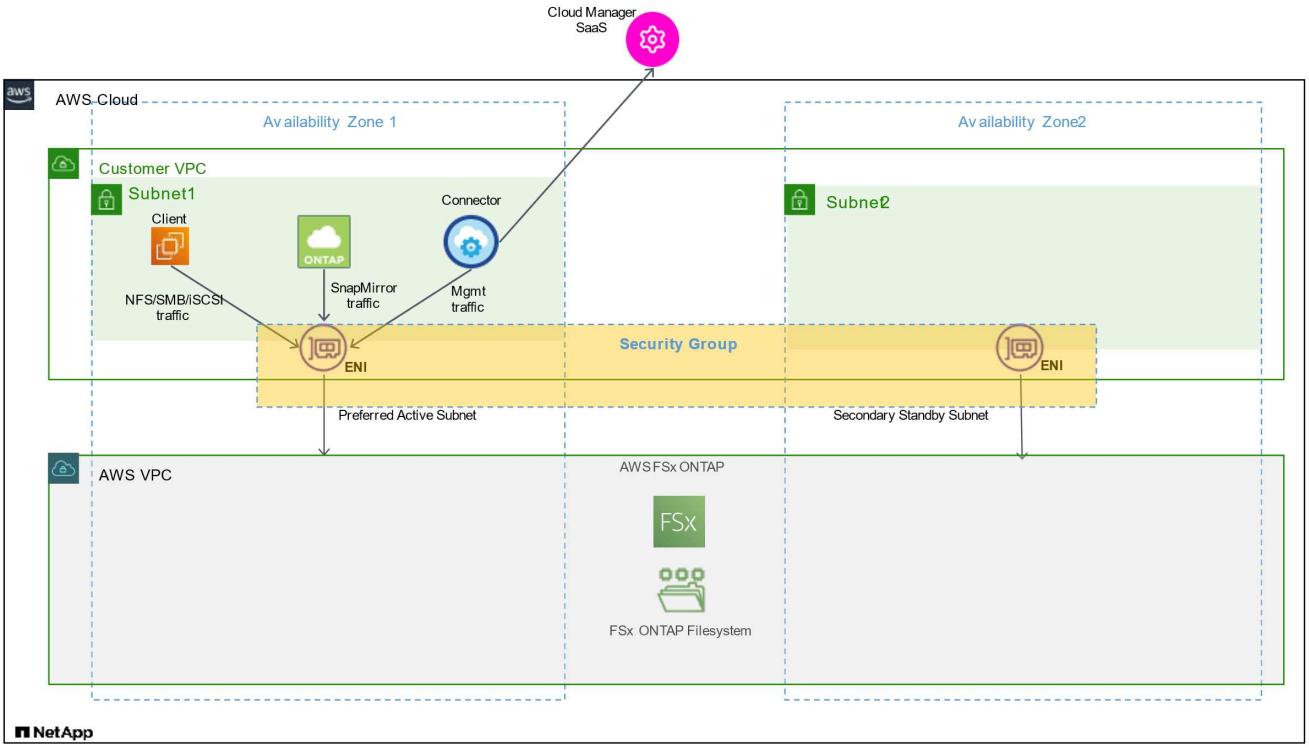
- "AWS 認證與權限"
- "管理Cloud Manager的AWS認證資料"

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 Sfor Sf.的規則

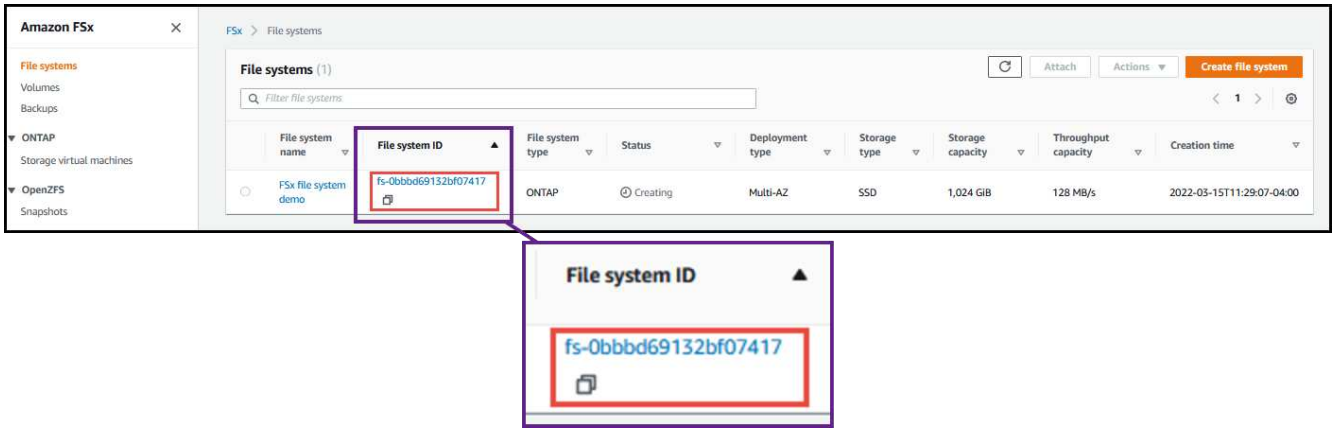
FSX for ONTAP Sfor Sfor Sfor Sfor Security群組需要傳入和傳出規則。此圖說明FSXfor ONTAP EfuS網路 組態和安全性群組需求。



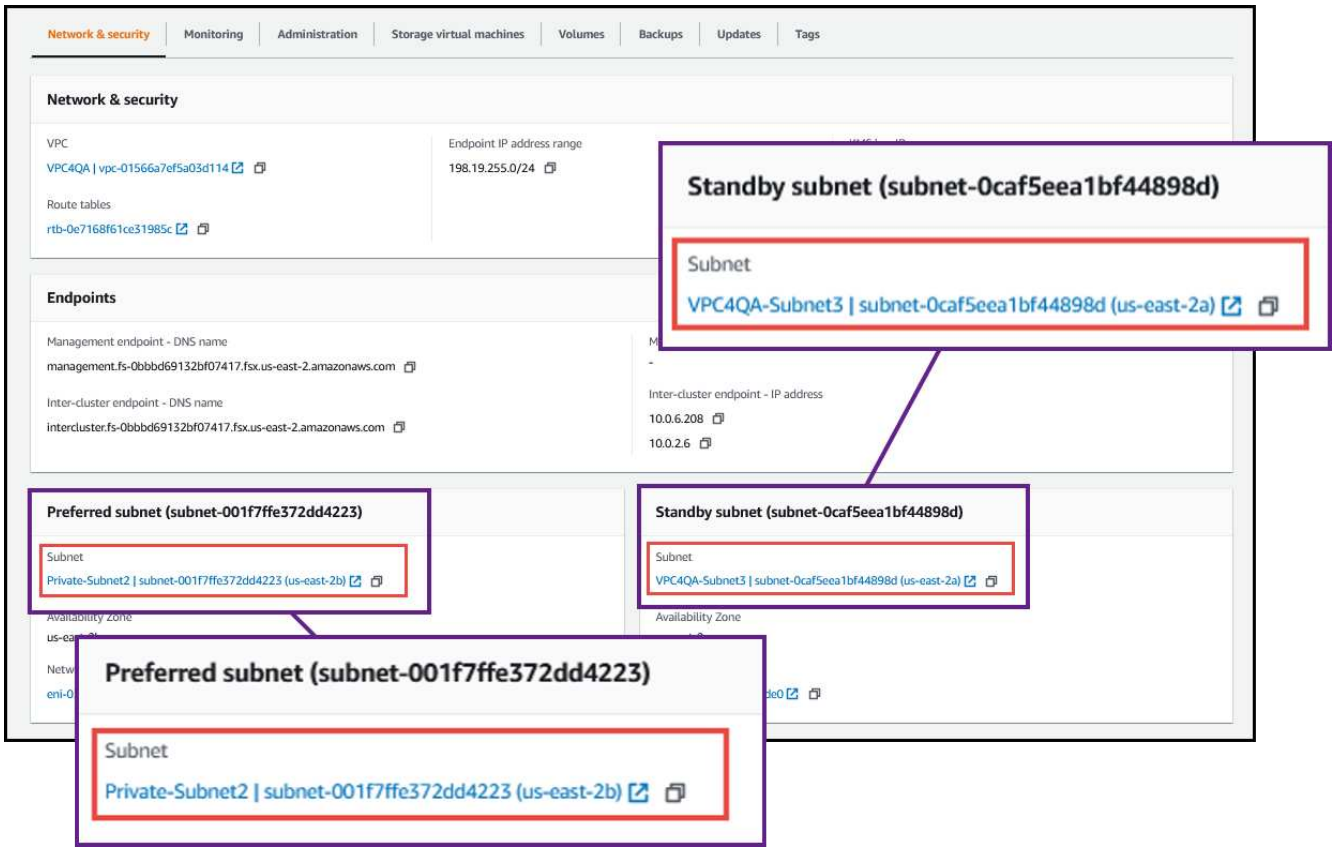
您需要使用AWS管理主控台來找出與Enis相關的安全性群組。

步驟

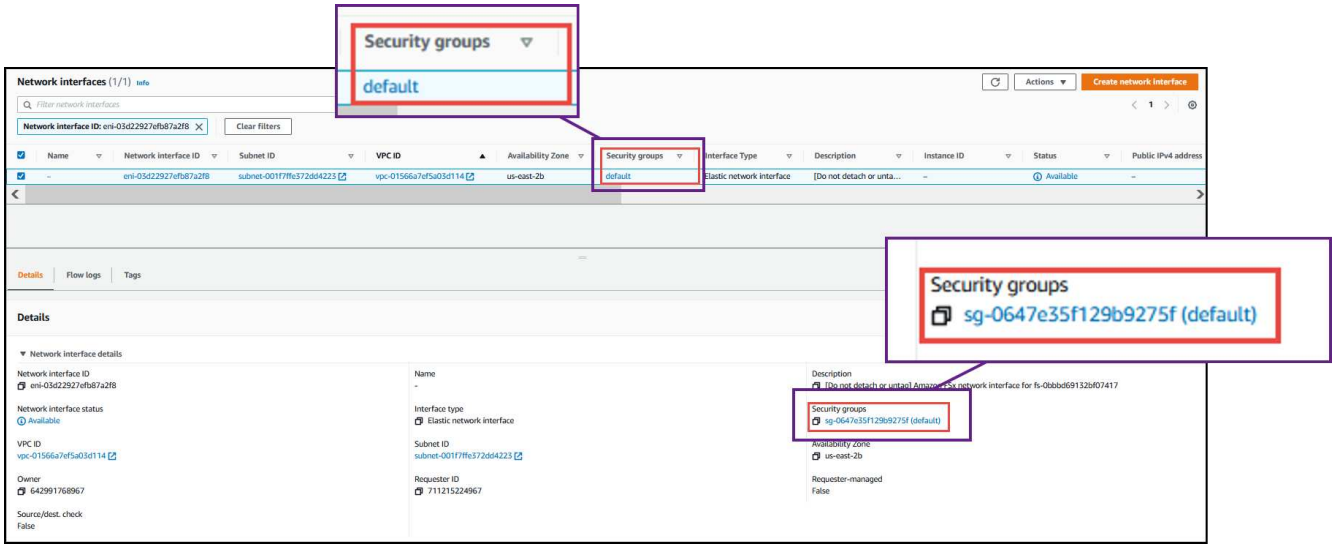
1. 在ONTAP AWS管理主控台開啟FSXfor S廳 檔案系統、然後按一下檔案系統ID連結。



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

傳輸協定	連接埠	目的
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
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、也不需要在FSXfor ONTAP Sfor Sf/節點之間開啟。

來源是FSXfor ONTAP Sfor 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

服務	傳輸協定	連接埠	來源	目的地	目的
DNS	UDP	53.	節點管理 LIF 與資料 LIF （NFS 、 CIFS ）	DNS	DNS
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執行個體以存取網際網路

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

版權資訊

商標資訊