需求

Amazon FSx for NetApp ONTAP

NetApp
November 28, 2023

目錄

需求

設定FSXfor ONTAP Sfor Sfor的權限

若要建立或管理適用於 ONTAP 工作環境的 FSX 、您需要將 AWS 認證新增至 BlueXP 、方法是提供 IAM 角色的 ARN 、讓 BlueXP 擁有為 ONTAP 工作環境建立 FSX 所需的權限。

設定IAM角色

設定IAM角色、讓BlueXP能夠承擔角色。

步驟

1. 前往目標帳戶中的IAM主控台。
2. 授予 BlueXP AWS 帳戶存取權。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。
   - 在*信任的實體類型*下、選取* AWS帳戶*。
   - 選擇 * 其他 AWS 帳戶 * 並輸入 BlueXP * 帳戶 ID* ：
     - 適用於BlueXP SaaS：952013314444
     - AWS GovCloud（美國）：033442085313

     為了提高安全性、建議您指定 "外部 ID_"。若要存取 AWS 帳戶、 BlueXP 必須提供角色 ARN （Amazon 資源名稱）和您指定的外部 ID 。這可防止 "混亂的副問題"。
3. 視需要建立包含下列必要最低權限和選用權限的原則。

必要權限

以下是允許 BlueXP 為 NetApp ONTAP 檔案系統建立 FSX 所需的最低權限。

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

自動容量

啟用時需要下列額外權限 "自動容量管理"。

```
"cloudwatch:GetMetricData",
"cloudwatch:GetMetricStatistics"
```

安全性群組

需要下列額外權限才能允許 BlueXP "產生安全性群組"。

```
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:RevokeSecurityGroupEgress",
"ec2:RevokeSecurityGroupIngress",
"ec2:CreateSecurityGroup",
"ec2:DeleteSecurityGroup",
"cloudformation:CreateStack",
"cloudformation:ValidateTemplate",
"cloudformation:DescribeStacks",
"cloudformation:DescribeStackEvents"
```

4. 複製 IAM 角色的角色 ARN 、以便在下一步將其貼到 BlueXP 中。

結果

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BlueXP。

開始之前

如果您剛建立 IAM 角色、請稍候幾分鐘、讓新認證可供使用。

步驟

1. 在BlueXP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 > BlueXP*。
   b. * 定義認證 * ：提供 * 認證名稱 * 、以及您在建立時所建立的 * 角色 ARN* 和 * 外部 ID* （若有指定） 設定IAM角色。

      - 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*。

結果

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

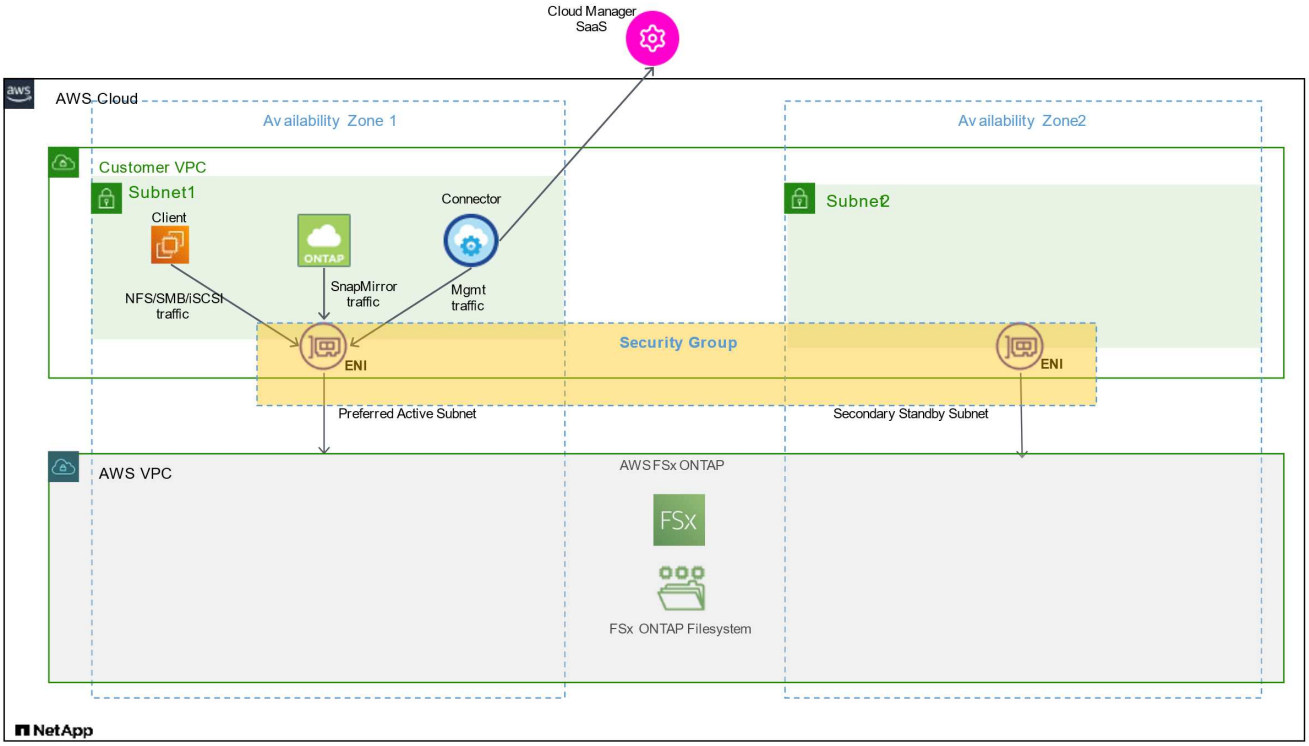
- "AWS 認證與權限"
- "管理適用於BlueXP的AWS認證資料"

FSXfor ONTAP Sfor Sf.的安全群組規則

BlueXP會建立AWS安全性群組、其中包含BlueXP和FSXfor ONTAP the支援功能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。

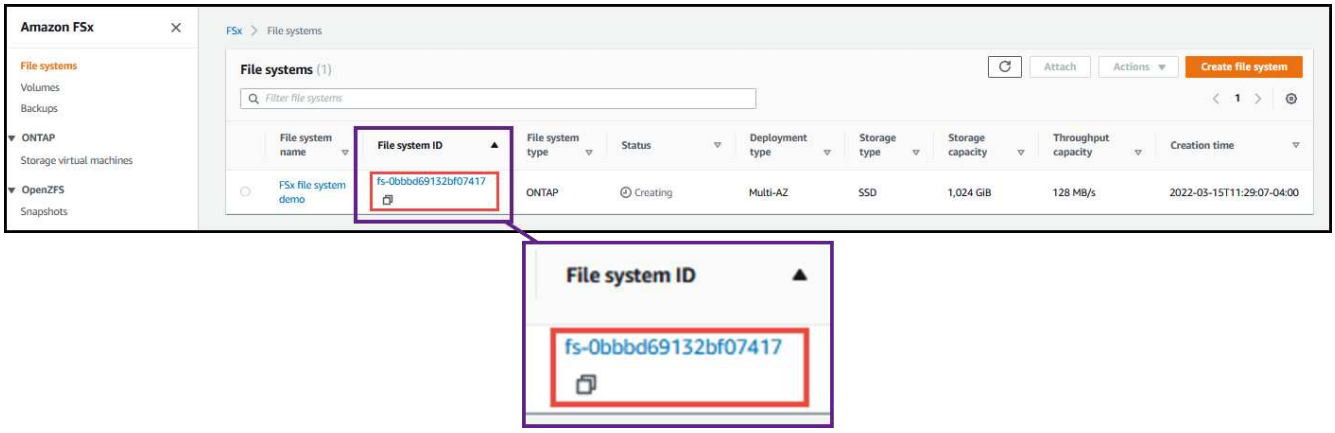


開始之前

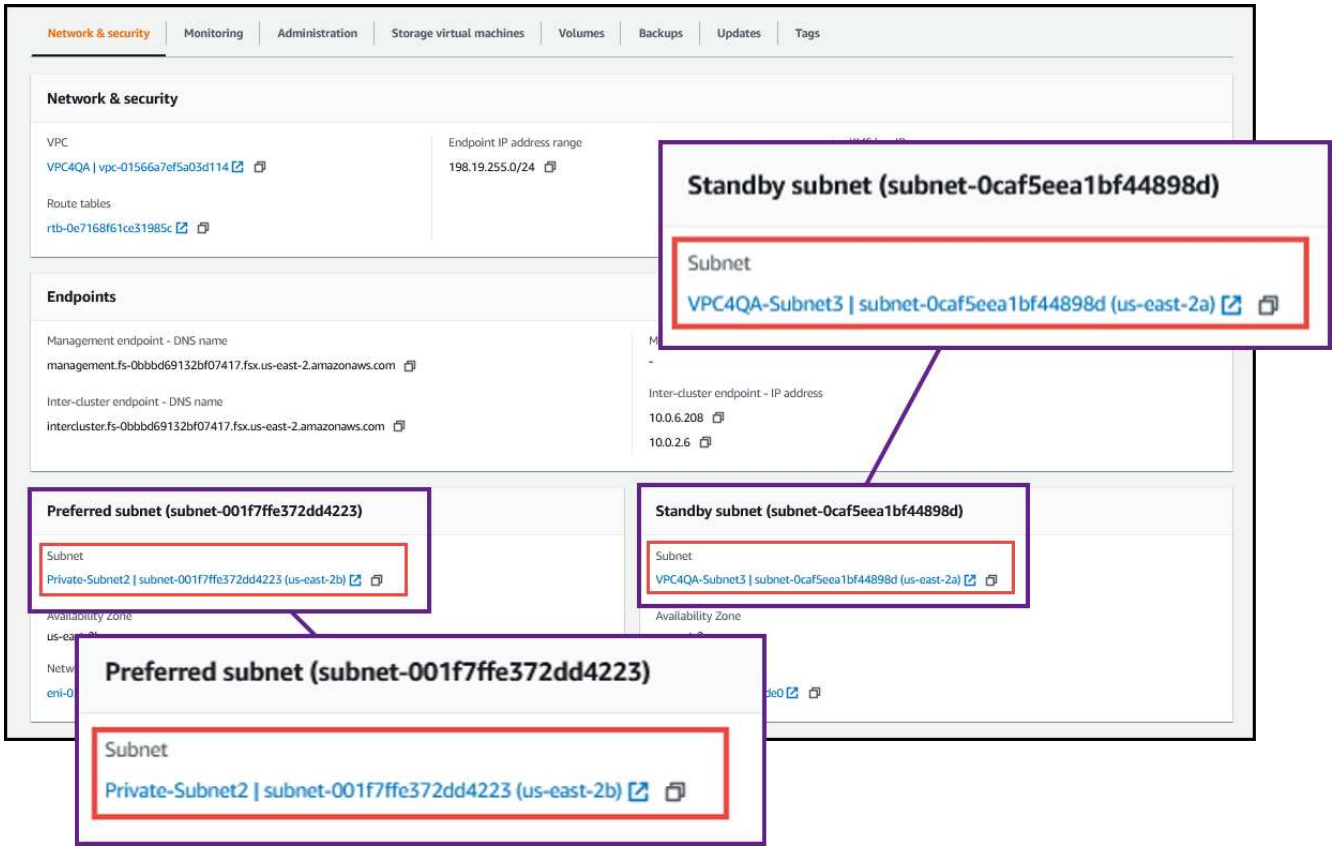
您需要使用AWS管理主控台來找出與Enis相關的安全性群組。

步驟

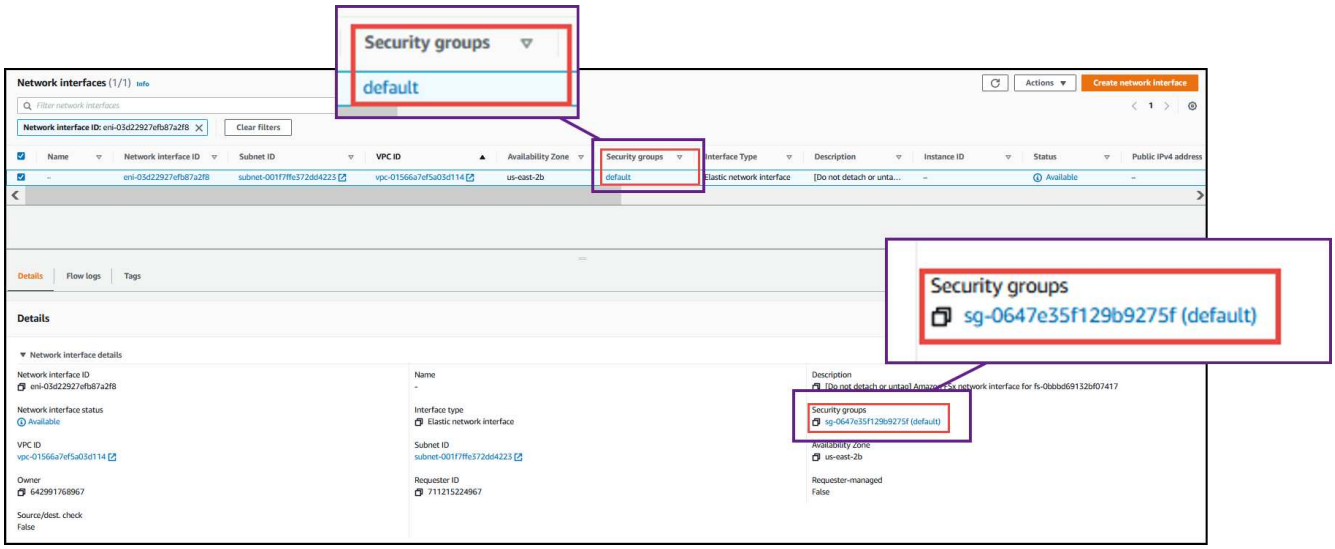
1. 在ONTAP AWS管理主控台開啟FSXfor S廳 檔案系統、然後按一下檔案系統ID連結。



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

傳輸協定	連接埠	目的
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
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

服務	傳輸協定	連接埠	來源	目的地	目的
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
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	提供從用戶端網頁瀏覽器到本機使用者介面的 HTTP 存取、以及從 BlueXP 分類執行個體的連線
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 網路未使用 NAT 或 Proxy 、則提供可存取網際網路的 BlueXP 分類執行個體

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BlueXP的DNS解析
BlueXP 分類	HTTP	80	BlueXP 分類	Cloud Volumes ONTAP 的 BlueXP 分類