# 設定您的網路
## Cloud Volumes ONTAP

NetApp
July 26, 2024

# 目錄

# 設定您的網路

## AWS 的網路需求 Cloud Volumes ONTAP

BlueXP負責Cloud Volumes ONTAP 設定功能完善的網路元件、例如IP位址、網路遮罩和路由。您需要確保可以存取傳出網際網路、有足夠的私有IP位址可用、有適當的連線位置等等。

### 一般要求

AWS 必須符合下列要求。

#### 對節點的輸出網際網路存取 **Cloud Volumes ONTAP**

支援NetApp功能的支援節點需要外傳網際網路存取功能、此功能可主動監控系統健全狀況、並將訊息傳送給NetApp技術支援部門。Cloud Volumes ONTAP AutoSupport

路由和防火牆原則必須允許將 HTTP / HTTPS 流量傳送至下列端點、 Cloud Volumes ONTAP 才能讓下列端點傳送 AutoSupport 動態訊息：

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

如果您有 NAT 執行個體、則必須定義傳入安全性群組規則、以允許 HTTPS 流量從私有子網路傳入網際網路。

如果傳出的網際網路連線無法傳送AutoSupport 功能性訊息、則BlueXP會自動將Cloud Volumes ONTAP 您的功能性更新系統設定為使用Connector做為Proxy伺服器。唯一的需求是確保連接器的安全性群組允許連接埠3128上的傳入連線。部署Connector之後、您需要開啟此連接埠。

如果您定義了Cloud Volumes ONTAP 嚴格的傳出規則以供支援、那麼Cloud Volumes ONTAP 您也必須確保支援透過連接埠3128建立_Outbound _連線的安全性群組。

在您確認可以存取傳出網際網路之後、您可以測試AutoSupport 以確保能夠傳送訊息。如需相關指示、請參閱 "文件：設定檔ONTAP AutoSupport"。

如果BlueXP通知您AutoSupport 無法傳送資訊、 "疑難排解AutoSupport 您的VMware組態"。

#### **HA** 中介器的傳出網際網路存取

HA 中介執行個體必須具有 AWS EC2 服務的傳出連線、才能協助進行儲存容錯移轉。若要提供連線、您可以新增公用 IP 位址、指定 Proxy 伺服器或使用手動選項。

手動選項可以是從目標子網路到 AWS EC2 服務的 NAT 閘道或介面 VPC 端點。如需 VPC 端點的詳細資訊、請參閱 "AWS 文件：介面 VPC 端點（AWS Private Link）"。

#### 私有**IP**位址

BlueXP會自動分配所需的私有IP位址數量給Cloud Volumes ONTAP 整個過程。您必須確保網路有足夠的私有IP位址可用。

BlueXP分配Cloud Volumes ONTAP 給功能的生命量取決於您是部署單一節點系統或HA配對。LIF 是與實體連接埠相關聯的 IP 位址。

#### 單一節點系統的IP位址

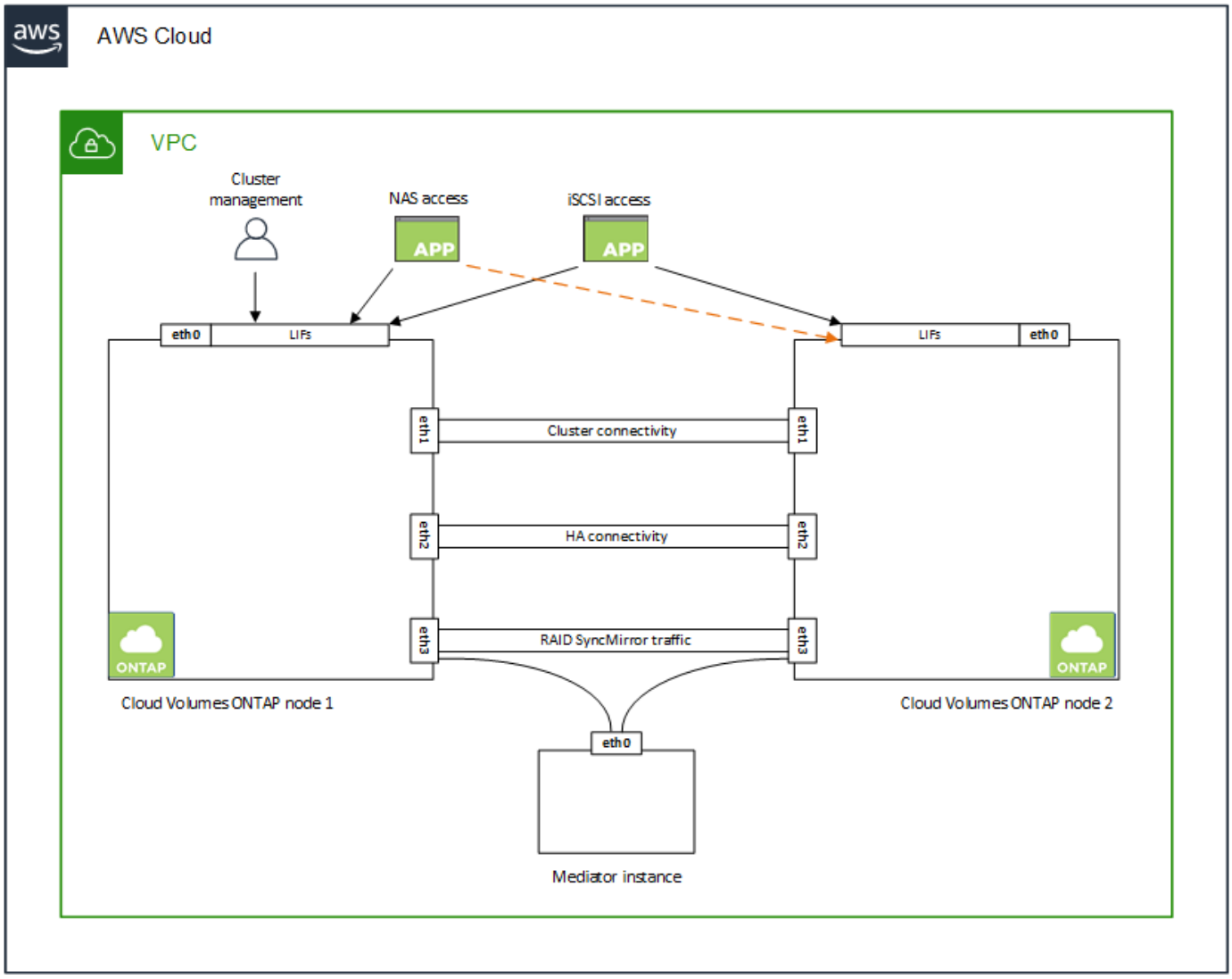
BlueXP會將6個IP位址分配給單一節點系統。

下表提供與每個私有IP位址相關聯的LIF詳細資料。

| LIF | 目的 |
| --- | --- |
| 叢集管理 | 整個叢集（HA配對）的管理管理。 |
| 節點管理 | 節點的管理管理。 |
| 叢集間 | 跨叢集通訊、備份與複寫。 |
| NAS資料 | 透過NAS傳輸協定進行用戶端存取。 |
| iSCSI資料 | 透過iSCSI傳輸協定進行用戶端存取。系統也用於其他重要的網路工作流程。此LIF為必填項目、不應刪除。 |
| 儲存VM管理 | 儲存VM管理LIF可搭配SnapCenter 使用諸如VMware等管理工具。 |

#### HA配對的IP位址

HA配對比單一節點系統需要更多IP位址。這些IP位址分佈在不同的乙太網路介面上、如下圖所示：




HA配對所需的私有IP位址數目取決於您選擇的部署模式。部署在_onle_ AWS可用區域（AZ）中的HA配對需要15個私有IP位址、而部署在_multi__ AZs中的HA配對則需要13個私有IP位址。

下表提供與每個私有IP位址相關聯的LIF詳細資料。

**HA**配對的生命週數、在單一**AZ**中

| **LIF** | 介面 | 節點 | 目的 |
|---|---|---|---|
| 叢集管理 | eth0 | 節點1 | 整個叢集（HA配對）的管理管理。 |
| 節點管理 | eth0 | 節點1和節點2 | 節點的管理管理。 |
| 叢集間 | eth0 | 節點1和節點2 | 跨叢集通訊、備份與複寫。 |
| NAS資料 | eth0 | 節點1 | 透過NAS傳輸協定進行用戶端存取。 |
| iSCSI資料 | eth0 | 節點1和節點2 | 透過iSCSI傳輸協定進行用戶端存取。系統也用於其他重要的網路工作流程。這些生命是必要的、不應刪除。 |
| 叢集連線能力 | eth1. | 節點1和節點2 | 可讓節點彼此通訊、並在叢集內移動資料。 |
| HA連線能力 | 道德 2 | 節點1和節點2 | 在發生容錯移轉時、兩個節點之間的通訊。 |

| LIF | 介面 | 節點 | 目的 |
| --- | --- | --- | --- |
| RSMiSCSI流量 | 道德 3 | 節點1和節點2 | RAID SyncMirror 支援iSCSI流量、以及兩Cloud Volumes ONTAP 個支援節點與中介器之間的通訊。 |
| 中介者 | eth0 | 中介者 | 節點與中介器之間的通訊通道、可協助進行儲存接管與恢復程序。 |

多個**AZs**中**HA**配對的**LIF**

| LIF | 介面 | 節點 | 目的 |
| --- | --- | --- | --- |
| 節點管理 | eth0 | 節點1和節點2 | 節點的管理管理。 |
| 叢集間 | eth0 | 節點1和節點2 | 跨叢集通訊、備份與複寫。 |
| iSCSI資料 | eth0 | 節點1和節點2 | 透過iSCSI傳輸協定進行用戶端存取。這些LIF也能管理節點之間的浮動IP位址移轉作業。這些生命是必要的、不應刪除。 |
| 叢集連線能力 | eth1. | 節點1和節點2 | 可讓節點彼此通訊、並在叢集內移動資料。 |
| HA連線能力 | 道德 2 | 節點1和節點2 | 在發生容錯移轉時、兩個節點之間的通訊。 |
| RSMiSCSI流量 | 道德 3 | 節點1和節點2 | RAID SyncMirror 支援iSCSI流量、以及兩Cloud Volumes ONTAP 個支援節點與中介器之間的通訊。 |
| 中介者 | eth0 | 中介者 | 節點與中介器之間的通訊通道、可協助進行儲存接管與恢復程序。 |

部署在多個可用度區域時、會與多個生命區建立關聯 "浮動 IP 位址"、不計入AWS私有IP限制。

安全性群組

您不需要建立安全性群組、因為BlueXP會為您建立安全性群組。如果您需要使用自己的、請參閱 "安全性群組規則"。

正在尋找Connector的相關資訊？ "檢視Connector的安全群組規則"

資料分層連線

如果您想要將 EBS 當作效能層、將 AWS S3 當作容量層、您必須確保 Cloud Volumes ONTAP 將該連接到 S3 。提供此連線的最佳方法是建立 VPC 端點至 S3 服務。如需相關指示、請參閱 "AWS 文件：建立閘道端點"。

當您建立 VPC 端點時、請務必選取與 Cloud Volumes ONTAP 該實例相對應的區域、 VPC 和路由表。您也必須修改安全性群組、以新增允許流量到 S3 端點的傳出 HTTPS 規則。否則 Cloud Volumes ONTAP 、無法連線至 S3 服務。

如果您遇到任何問題、請參閱 "AWS 支援知識中心：為什麼我無法使用閘道 VPC 端點連線至 S3 儲存區？"

連線**ONTAP** 至功能鏈接

若要在Cloud Volumes ONTAP AWS系統和ONTAP 其他網路中的更新系統之間複寫資料、您必須在AWS VPC和其他網路（例如您的公司網路）之間建立VPN連線。如需相關指示、請參閱 "AWS 文件：設定 AWS VPN 連線 "。

適用於 **CIFS** 的 **DNS** 和 **Active Directory**

如果您想要配置 CIFS 儲存設備、則必須在 AWS 中設定 DNS 和 Active Directory 、或將內部部署設定延伸至 AWS 。

DNS 伺服器必須為 Active Directory 環境提供名稱解析服務。您可以將 DHCP 選項集設定為使用預設 EC2 DNS 伺服器、此伺服器不得是 Active Directory 環境所使用的 DNS 伺服器。

如需相關指示、請參閱 "AWS 文件： AWS Cloud 上的 Active Directory 網域服務：快速入門參考部署"。

**VPC**共享

從9.11.1版開始、Cloud Volumes ONTAP AWS支援搭配VPC共享功能的更新版、VPC共用功能可讓您的組織與其他AWS帳戶共用子網路。若要使用此組態、您必須設定AWS環境、然後使用API部署HA配對。

"瞭解如何在共用子網路中部署HA配對"。

## 多個 **AZs** 的 **HA** 配對需求

其他 AWS 網路需求適用於 Cloud Volumes ONTAP 使用多個可用區域（AZs）的 SestHA 組態。在啟動HA配對之前、您應該先檢閱這些需求、因為在建立工作環境時、您必須在BlueXP中輸入網路詳細資料。

若要瞭解 HA 配對的運作方式、請參閱 "高可用度配對"。

可用度區域

此 HA 部署模式使用多個 AZs 來確保資料的高可用度。您應該使用專屬的 AZ 來處理每 Cloud Volumes ONTAP 個實例、並使用中介執行個體、以提供 HA 配對之間的通訊通道。

每個可用區域都應有一個子網路。

用於 **NAS** 資料和叢集 **/ SVM** 管理的浮動 **IP** 位址

多個 AZs 中的 HA 組態會使用浮動 IP 位址、在發生故障時在節點之間移轉。除非您的選擇、否則無法從 VPC 外部原生存取 "設定 AWS 傳輸閘道"。

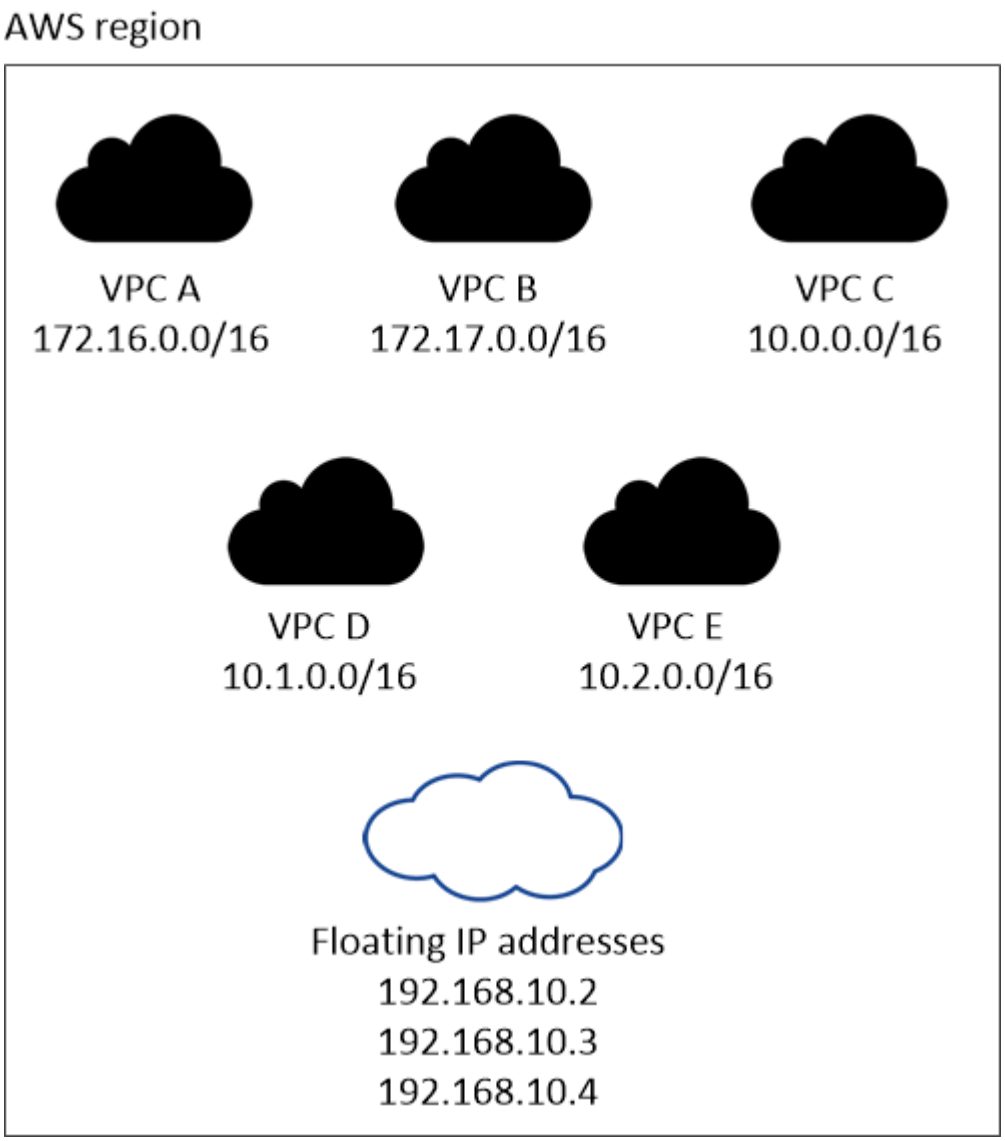
一個浮動 IP 位址是用於叢集管理、一個用於節點 1 上的 NFS/CIFS 資料、另一個用於節點 2 上的 NFS/CIFS 資料。SVM 管理的第四個浮動 IP 位址為選用項目。

> 如果您使用 SnapDrive 適用於 Windows 的 SHIP 或 SnapCenter 搭配 HA 配對的 SHIP 、則 SVM 管理 LIF 需要一個浮動 IP 位址。

建立Cloud Volumes ONTAP 一套功能完善的運作環境時、您需要在BlueXP中輸入浮動IP位址。在啟動系統時、BlueXP會將IP位址分配給HA配對。

在部署 HA 組態的 AWS 區域中、所有 VPC 的浮動 IP 位址都必須位於 CIDR 區塊之外。將浮動 IP 位址視為位於您所在地區 VPC 外部的邏輯子網路。

下列範例顯示 AWS 區域中浮動 IP 位址與 VPC 之間的關係。雖然浮動 IP 位址位於所有 VPC 的 CIDR 區塊之外、但仍可透過路由表路由傳送至子網路。




BlueXP會自動建立靜態IP位址、以供iSCSI存取及從VPC外部用戶端存取NAS。您不需要滿足這些類型 IP 位址的任何需求。

傳輸閘道、可從 **VPC** 外部啟用浮動 **IP** 存取

如有需要、 "設定 AWS 傳輸閘道" 可從 HA 配對所在的 VPC 外部存取 HA 配對的浮動 IP 位址。

路由表

在BlueXP中指定浮動IP位址之後、系統會提示您選取路由表、其中應包含通往浮動IP位址的路由。這可讓用戶端存取 HA 配對。

如果VPC中只有一個子網路路由表（主路由表）、則BlueXP會自動將浮動IP位址新增至該路由表。如果您有多個路由表、在啟動 HA 配對時、請務必選取正確的路由表。否則、部分用戶端可能無法存取 Cloud Volumes ONTAP 功能不完全。

例如、您可能有兩個子網路與不同的路由表相關聯。如果您選取路由表 A 而非路由表 B 、則與路由表 A 相關

聯的子網路中的用戶端可以存取 HA 配對、但與路由表 B 相關的子網路中的用戶端則無法存取。

如需路由表的詳細資訊、請參閱 "AWS 文件：路由表"。

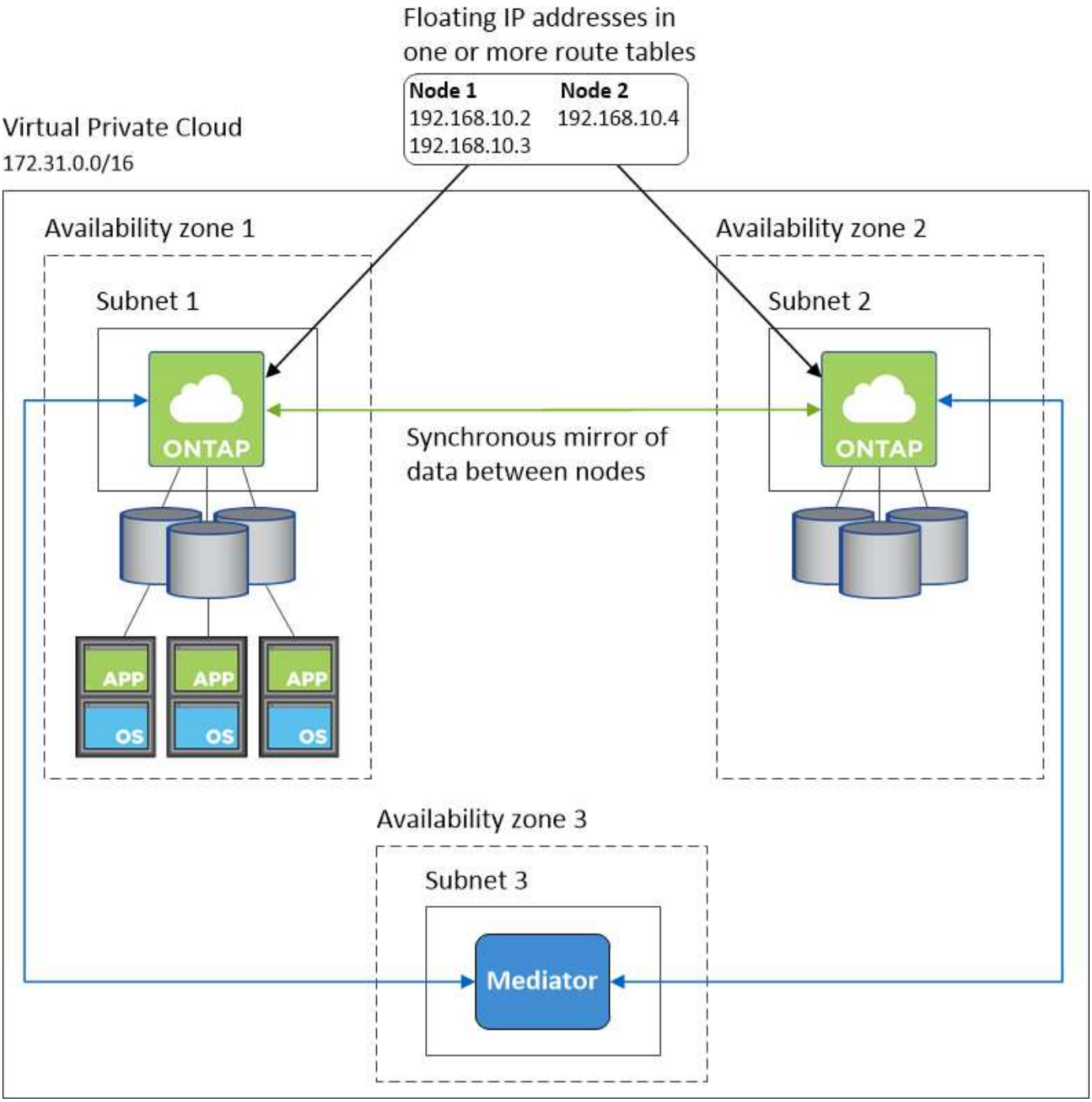
連線至 **NetApp** 管理工具

若要將 NetApp 管理工具搭配多個 AZs 中的 HA 組態使用、您有兩種連線選項：

1. 在不同的 VPC 和中部署 NetApp 管理工具 "設定 AWS 傳輸閘道"。閘道可讓您從 VPC 外部存取叢集管理介面的浮動 IP 位址。
2. 在與 NAS 用戶端相同的 VPC 中部署 NetApp 管理工具、其路由組態與 NAS 用戶端相似。

**HA** 組態範例

下圖說明多個AZs中HA配對的特定網路元件：三個可用度區域、三個子網路、浮動IP位址和路由表。




### 連接器需求

如果您尚未建立連接器、也應該檢閱連接器的網路需求。

- "檢視連接器的網路需求"
- "AWS中的安全群組規則"

## 在多個 AZs 中設定 HA 配對的 AWS 傳輸閘道

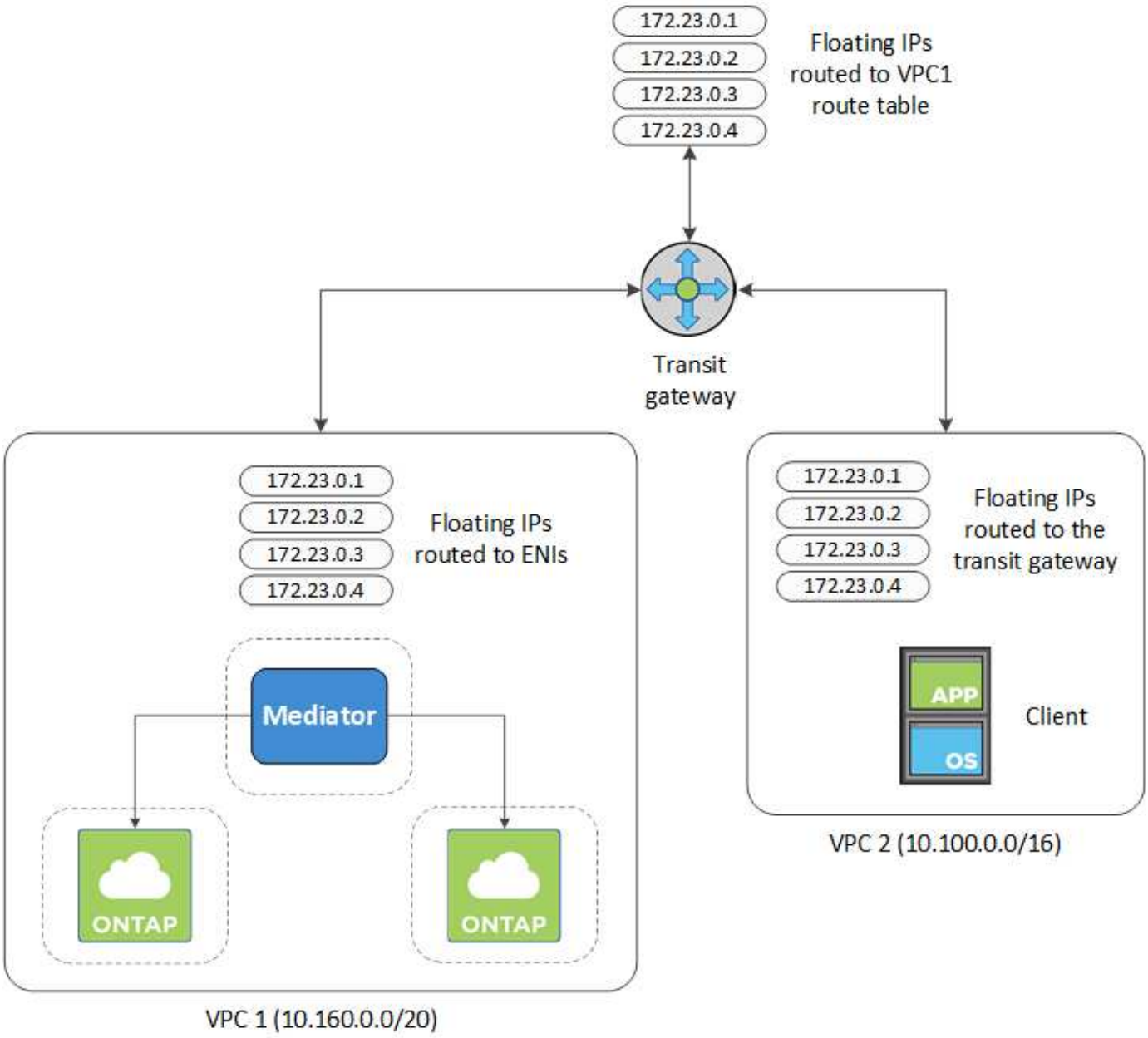
設定 AWS 傳輸閘道、以便存取 HA 配對 "浮動 IP 位址" 從 HA 配對所在的 VPC 外部。

當某個靜態 HA 組態分佈於多個 AWS 可用區域時、從 VPC 內部存取 NAS 資料時、需要使用浮動 IP 位址。Cloud Volumes ONTAP當發生故障時、這些浮動 IP 位址可在節點之間移轉、但無法從 VPC 外部原生存取。獨立的私有 IP 位址可從 VPC 外部存取資料、但無法提供自動容錯移轉功能。

叢集管理介面和選用的 SVM 管理 LIF 也需要浮動 IP 位址。

如果您設定 AWS 傳輸閘道、就能從 HA 配對所在的 VPC 外部存取浮動 IP 位址。這表示 VPC 以外的 NAS 用戶端和 NetApp 管理工具可以存取浮動 IP 。

以下範例顯示兩個透過傳輸閘道連線的 VPC 。HA 系統位於一個 VPC 、而用戶端位於另一個 VPC 。然後、您可以使用浮動 IP 位址、在用戶端上掛載 NAS Volume 。



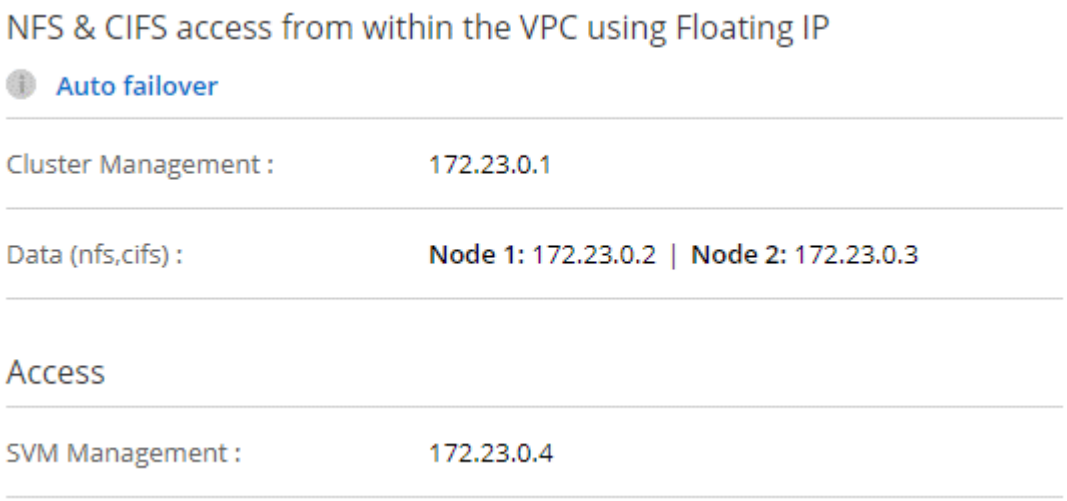

下列步驟說明如何設定類似的組態。

步驟

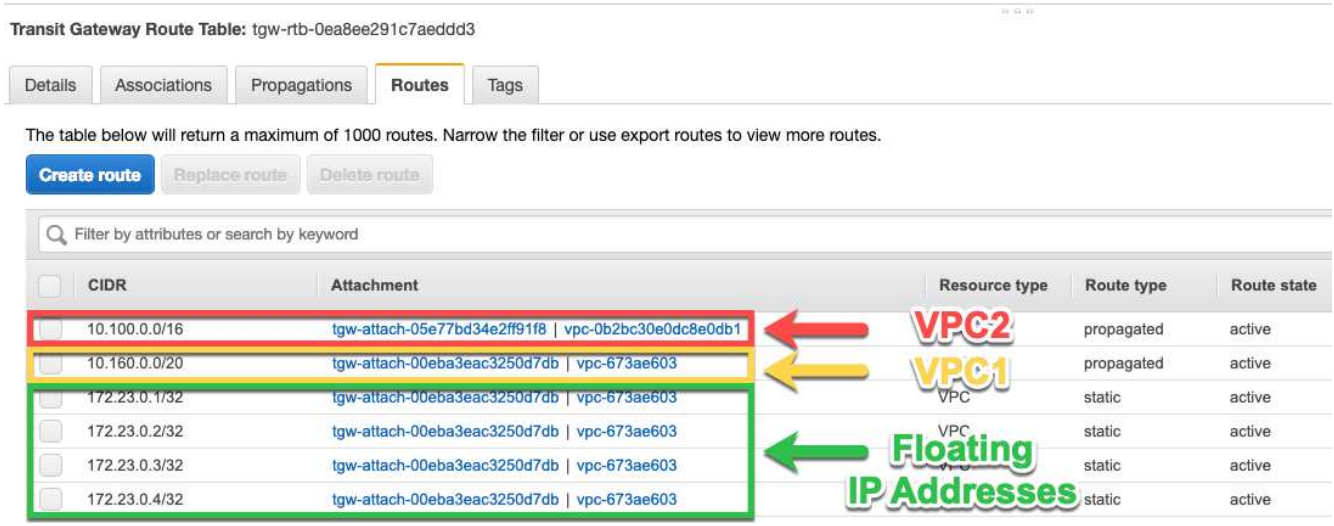
1. "建立傳輸閘道、並將 VPC 附加至閘道"。

2. 將VPC與傳輸閘道路由表建立關聯。
   a. 在* VPC*服務中、按一下* Transit Gateway Route Tables *。
   b. 選取路由表。
   c. 按一下「關聯」、然後選取「建立關聯」。
   d. 選擇要關聯的附件（VPC）、然後按一下*建立關聯*。
3. 指定 HA 配對的浮動 IP 位址、在傳輸閘道的路由表中建立路由。

   您可以在BlueXP的「工作環境資訊」頁面找到浮動IP位址。範例如下：

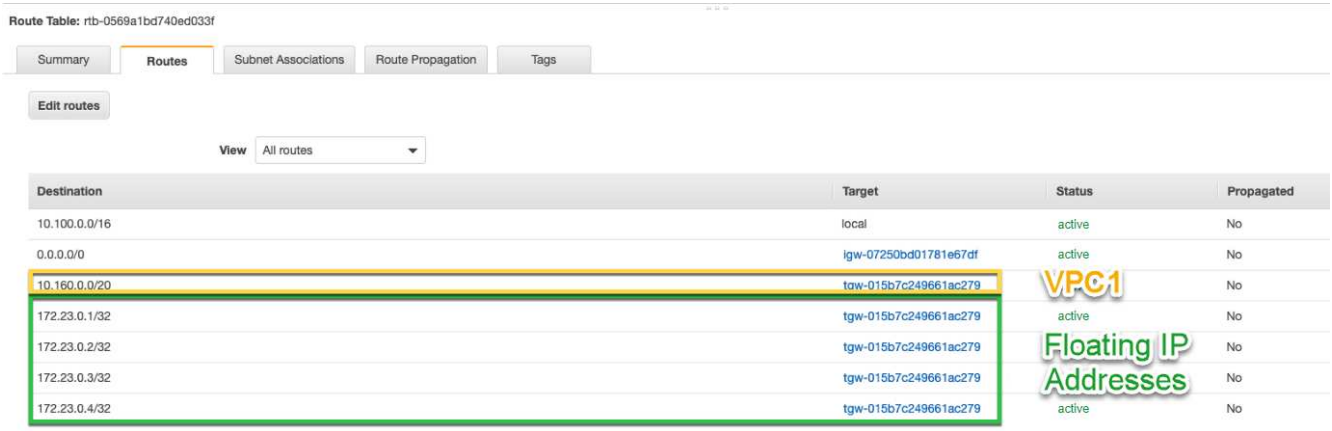



   下列範例影像顯示傳輸閘道的路由表。其中包括兩部 VPC 的 CIDR 區塊路由、 Cloud Volumes ONTAP 以及由 R1 使用的四個浮動 IP 位址。




4. 修改需要存取浮動 IP 位址的 VPC 路由表。
   a. 新增路由項目至浮動 IP 位址。
   b. 將路由項目新增至 HA 配對所在 VPC 的 CIDR 區塊。

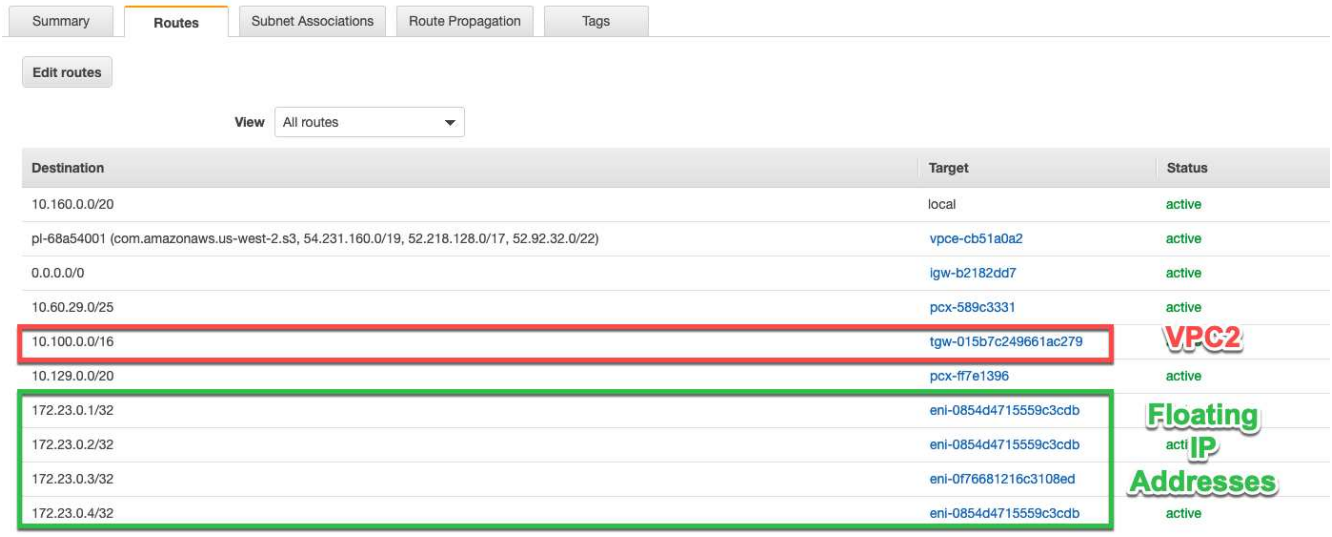
      下列範例影像顯示 VPC 2 的路由表、其中包括通往 VPC 1 的路由和浮動 IP 位址。




5. 將需要存取浮動 IP 位址的路由新增至 VPC 、以修改 HA 配對 VPC 的路由表。

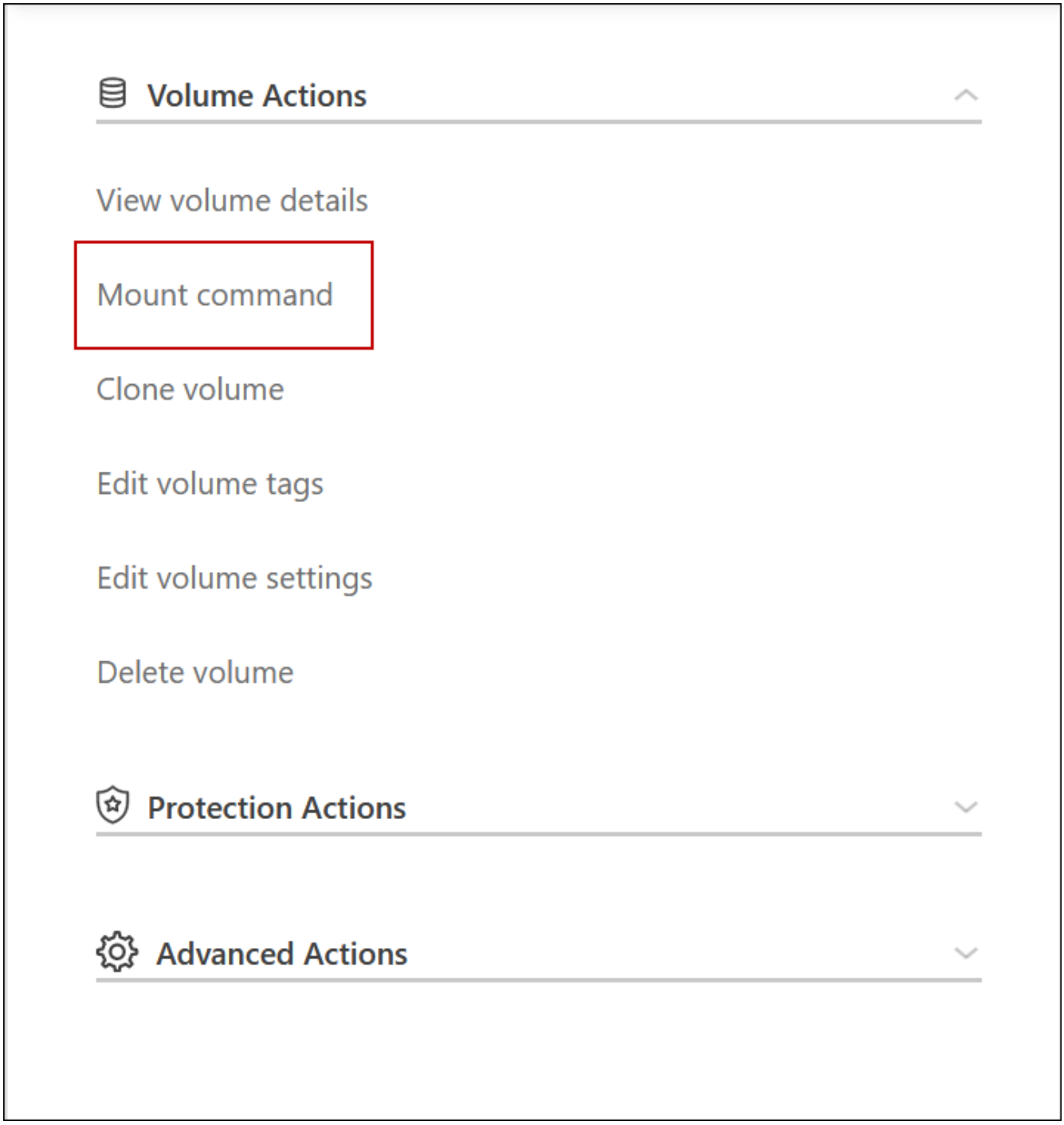
   此步驟非常重要、因為它會完成 VPC 之間的路由。

   下列範例影像顯示 VPC 1 的路由表。其中包括通往浮動 IP 位址和 VPC 2 的路由、而 VPC 2 是用戶端所在的位置。在部署HA配對時、BlueXP會自動將浮動IP新增至路由表。




6. 使用浮動 IP 位址將磁碟區掛載到用戶端。

   您可以透過 BlueXP 中「管理磁碟區」面板下的 * 掛載命令 * 選項、在 BlueXP 中找到正確的 IP 位址。




7. 如果您要掛載NFS Volume、請設定匯出原則以符合用戶端VPC的子網路。

   "瞭解如何編輯Volume"。

   - 相關連結 *
   - "AWS 中的高可用度配對"
   - "AWS 的網路需求 Cloud Volumes ONTAP"

# 在共享子網路中部署HA配對

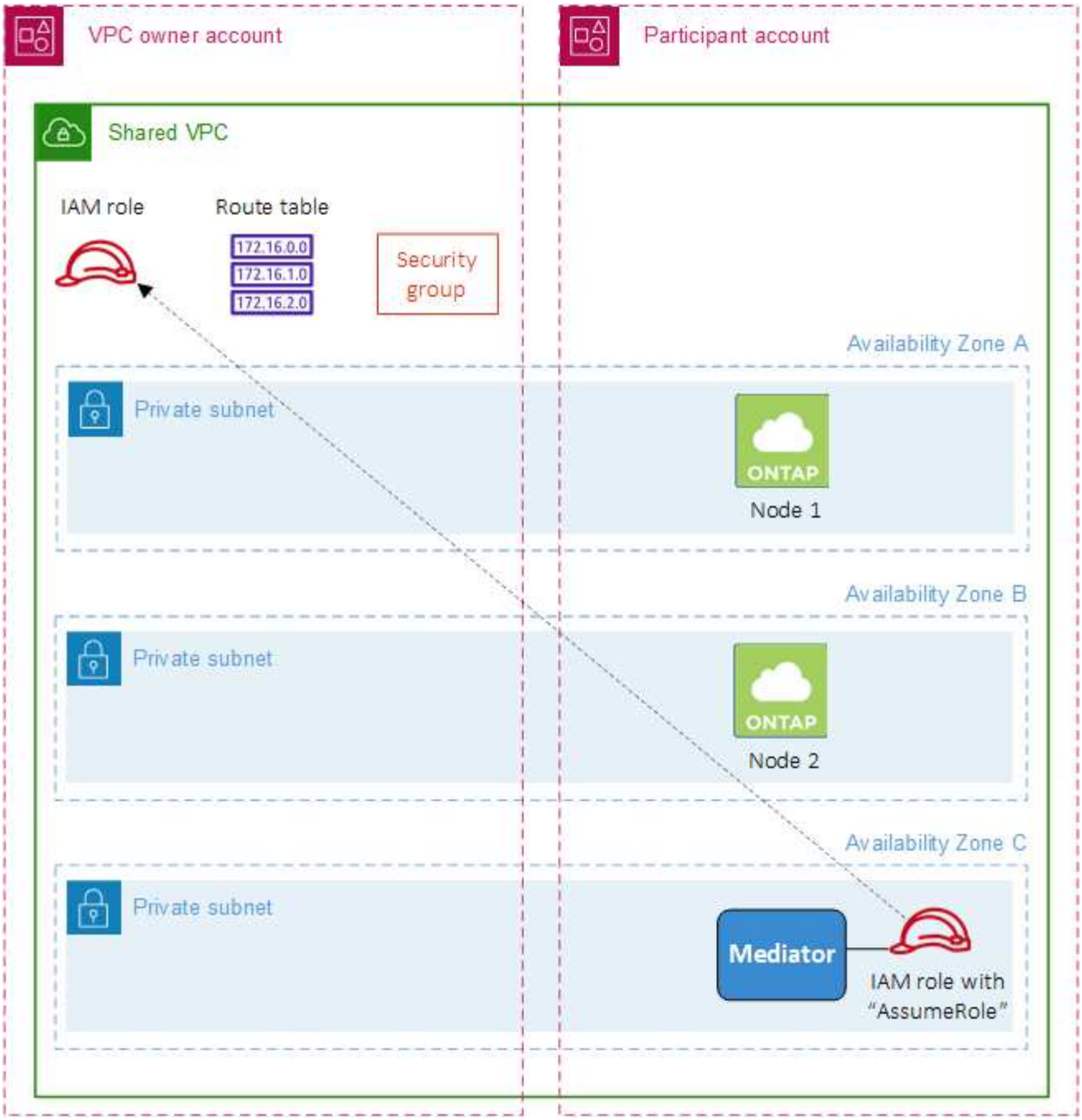
從9.11.1版開始、Cloud Volumes ONTAP AWS支援搭配VPC共享功能的更新版、VPC共用功能可讓您的組織與其他AWS帳戶共用子網路。若要使用此組態、您必須設定AWS環境、然後使用API部署HA配對。

與 "VPC共享"、將一個功能豐富的全功能HA組態分佈於兩個帳戶：Cloud Volumes ONTAP

- VPC擁有者帳戶、擁有網路（VPC、子網路、路由表和Cloud Volumes ONTAP 保密群組）
- 參與者帳戶、其中EC2執行個體部署在共享子網路中（包括兩個HA節點和中介器）

若將某個版本部署在多個可用度區域中、HA中介程式需要特定權限、才能寫入VPC擁有者帳戶中的路由表。Cloud Volumes ONTAP您必須設定協調員可以承擔的IAM角色、以提供這些權限。

下圖顯示此部署所涉及的元件：




如下列步驟所述、您必須與參與者帳戶共用子網路、然後在VPC擁有者帳戶中建立IAM角色和安全性群組。

當您建立Cloud Volumes ONTAP 不協調作業環境時、BlueXP會自動建立IAM角色、並將其附加至協調者。此角色會假設您在VPC擁有者帳戶中建立的IAM角色、以便變更與HA配對相關的路由表。

步驟

1. 與參與者帳戶共用VPC擁有者帳戶中的子網路。

   若要在共用子網路中部署HA配對、必須執行此步驟。

   "AWS文件：共用子網路"

2. 在VPC擁有者帳戶中、建立Cloud Volumes ONTAP 一個安全群組以供使用。

"請參閱Cloud Volumes ONTAP 安全性群組規則以瞭解相關資訊"。請注意、您不需要為HA中介者建立安全性群組。BlueXP能為您實現這項目標。

3. 在VPC擁有者帳戶中、建立包含下列權限的IAM角色：

```
Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
```

4. 使用BlueXP API建立新Cloud Volumes ONTAP 的功能不全的工作環境。

   請注意、您必須指定下列欄位：

   - "安全性群組Id"

     「安全性GroupId」欄位應指定您在VPC擁有者帳戶中建立的安全性群組（請參閱上述步驟2）。

   - 「haParam」物件中的「assugerme勞力Arn」

     「assume勞力arn」欄位應包含您在VPC擁有者帳戶中建立的IAM角色ARN（請參閱上述步驟3）。

     例如：

```
"haParams": {
     "assumeRoleArn":
"arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
}
```

+
"深入瞭Cloud Volumes ONTAP 解NetApp API"

# AWS 的安全群組規則

BlueXP會建立AWS安全性群組、其中包括Cloud Volumes ONTAP 需要順利運作的傳入和傳出規則。您可能需要參照連接埠進行測試、或是偏好使用自己的安全性群組。

## 規則 Cloud Volumes ONTAP

適用於此功能的安全性群組 Cloud Volumes ONTAP 需要傳入和傳出規則。

傳入規則

當您建立工作環境並選擇預先定義的安全性群組時、可以選擇允許下列其中一項的流量：

- *僅限選定VPC *：傳入流量的來源是VPC的子網路範圍（適用於Cloud Volumes ONTAP 整個系統）、以及連接器所在VPC的子網路範圍。這是建議的選項。
- 所有**VPC**：傳入流量的來源為0.00.0.0/0 IP範圍。

| 傳輸協定 | 連接埠 | 目的 |
|---|---|---|
| 所有ICMP | 全部 | Ping 執行個體 |
| HTTP | 80 | 使用叢集管理 LIF 的 IP 位址、以 HTTP 存取 System Manager Web 主控台 |
| HTTPS | 443.. | 使用叢集管理LIF的IP位址、連線到Connector和HTTPS、存取System Manager Web主控台 |
| 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 | 161-162-163. | 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 | 161-162-163. | 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

預先定義 Cloud Volumes ONTAP 的 Security Group for the 旅行團會開啟所有的傳出流量。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

適用於此功能的預先定義安全性群組 Cloud Volumes ONTAP 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

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 Cloud Volumes ONTAP 那些由真人進行傳出通訊所需的連接埠。

> 來源是 Cloud Volumes ONTAP 指在整個系統上的介面（ 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 ） |
| AutoSupport | HTTPS | 443.. | 節點管理 LIF | support.netapp.com | 支援（預設為HTTPS）AutoSupport |
| | HTTP | 80 | 節點管理 LIF | support.netapp.com | 僅當傳輸傳輸傳輸傳輸傳輸協定從HTTPS變更為HTTP 時、AutoSupport |
| | TCP | 3128 | 節點管理 LIF | 連接器 | 如果無法使用傳出的網際網路連線、請透過Connector上的Proxy伺服器傳送AutoSupport 功能介紹訊息 |

| 服務 | 傳輸協定 | 連接埠 | 來源 | 目的地 | 目的 |
|---|---|---|---|---|---|
| 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 |
| 叢集 | 所有流量 | 所有流量 | 一個節點上的所有 LIF | 其他節點上的所有 LIF | 叢集間通訊（Cloud Volumes ONTAP 僅限不含 HA） |
| | TCP | 3000 | 節點管理 LIF | HA 中介 | ZAPI 呼叫（Cloud Volumes ONTAP 僅限 RHA） |
| | ICMP | 1. | 節點管理 LIF | HA 中介 | Keepive Alive （Cloud Volumes ONTAP 僅限 HHA） |
| 組態備份 | HTTP | 80 | 節點管理 LIF | \http ： //// <connector-IP-address> occm/offboxconfig | 將組態備份傳送至Connector。 "深入瞭解組態備份檔案"。 |
| 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 | 162-1662 | 節點管理 LIF | 監控伺服器 | 透過 SNMP 設陷進行監控 |
| | UDP | 162-1662 | 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 |

## HA 協調器外部安全群組的規則

針對此功能、預先定義 Cloud Volumes ONTAP 的外部安全群組包括下列傳入和傳出規則。

#### 傳入規則

HA中介器的預先定義安全性群組包括下列傳入規則。

| 傳輸協定 | 連接埠 | 來源 | 目的 |
|---|---|---|---|
| TCP | 3000 | 連接器的CIDR | 從 Connector 進行 RESTful API 存取 |

#### 傳出規則

HA 中介器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

HA 中介器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、只開啟 HA 中介者傳出通訊所需的連接埠。

| 傳輸協定 | 連接埠 | 目的地 | 目的 |
|---|---|---|---|
| HTTP | 80 | AWS EC2執行個體上Connector的IP位址 | 下載中介程式升級 |
| HTTPS | 443.. | ec2.amazonaws.com | 協助進行儲存容錯移轉 |
| UDP | 53. | ec2.amazonaws.com | 協助進行儲存容錯移轉 |

您可以建立介面 VPC 端點、從目標子網路到 AWS EC2 服務、而非開啟連接埠 443 和 53 。

## HA組態內部安全性群組的規則

針對某個不穩定的HA組態、預先定義的內部安全群組Cloud Volumes ONTAP 包括下列規則。此安全性群組可在HA節點之間以及中介器與節點之間進行通訊。

BlueXP一律會建立此安全性群組。您沒有使用自己的選項。

#### 傳入規則

預先定義的安全性群組包含下列傳入規則。

| 傳輸協定 | 連接埠 | 目的 |
|---|---|---|
| 所有流量 | 全部 | HA 中介器與 HA 節點之間的通訊 |

傳出規則

預先定義的安全性群組包括下列傳出規則。

| 傳輸協定 | 連接埠 | 目的 |
| --- | --- | --- |
| 所有流量 | 全部 | HA 中介器與 HA 節點之間的通訊 |

## Connector 規則

"檢視Connector的安全群組規則"