



# 網路需求

## Cloud Manager 3.6

NetApp  
March 25, 2024

# 目錄

網路需求 .....	1
Cloud Manager的網路需求 .....	1
AWS 的網路需求 Cloud Volumes ONTAP .....	4
在多個 AZs 中設定 HA 配對的 AWS 傳輸閘道 .....	10
Azure 的網路需求 Cloud Volumes ONTAP .....	14

# 網路需求

## Cloud Manager的網路需求

您必須設定網路、Cloud Manager才能在Cloud Volumes ONTAP AWS或Microsoft Azure 中部署支援功能完善的系統。最重要的步驟是確保從網際網路存取各種端點。



如果您的網路使用Proxy伺服器來進行所有與網際網路的通訊、Cloud Manager會在設定期間提示您指定Proxy。您也可以從「設定」頁面指定Proxy伺服器。請參閱 ["設定Cloud Manager使用Proxy伺服器"](#)。

### 連線至目標網路

Cloud Manager需要網路連線至AWS VPC和Azure VNets、您可以在其中部署Cloud Volumes ONTAP

例如、如果您在公司網路中安裝Cloud Manager、則必須設定VPN連線至AWS VPC或Azure vnet、以便在其中啟動Cloud Volumes ONTAP 更新。

### 傳出網際網路存取

Cloud Manager需要存取外部網際網路、才能部署Cloud Volumes ONTAP 及管理功能。從網頁瀏覽器存取Cloud Manager時、以及在Linux主機上執行Cloud Manager安裝程式時、也需要外傳網際網路存取。

下列各節將說明特定的端點。

透過外傳網際網路存取功能、在**Cloud Volumes ONTAP AWS**中管理功能

Cloud Manager在Cloud Volumes ONTAP AWS中部署及管理功能時、需要透過外傳網際網路連絡下列端點：

端點	目的
AWS 服務 (amazonaws.com): <ul style="list-style-type: none"><li>• CloudFormation</li><li>• 彈性運算雲端 ( EC2 )</li><li>• 金鑰管理服務 ( KMS )</li><li>• 安全性權杖服務 ( STOS )</li><li>• 簡易儲存服務 ( S3 )</li></ul> 確切的端點取決於您部署 Cloud Volumes ONTAP 的區域。 <a href="#">"如需詳細資料、請參閱 AWS 文件。"</a>	讓Cloud Manager能夠在Cloud Volumes ONTAP AWS中部署及管理功能。
<a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a>	API 要求 NetApp Cloud Central 。
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>	提供軟體映像、資訊清單和範本的存取權限。

端點	目的
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a>	讓 Cloud Manager 能夠存取及下載資訊清單、範本及 Cloud Volumes ONTAP 升級影像。
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	讓 NetApp 能夠從稽核記錄串流資料。
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	與 Cloud Manager 服務（包括 Cloud Central 帳戶）進行通訊。
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	與 NetApp Cloud Central 通訊、以進行集中式使用者驗證。
<a href="https://support.netapp.com/aods/asupmessage">https://support.netapp.com/aods/asupmessage</a> <a href="https://support.netapp.com/asupprod/post/1.0/postAsup">https://support.netapp.com/asupprod/post/1.0/postAsup</a>	與 NetApp AutoSupport 通訊
<a href="https://support.netapp.com/svcgw">https://support.netapp.com/svcgw</a> <a href="https://support.netapp.com/ServiceGW/entitlement">https://support.netapp.com/ServiceGW/entitlement</a>	與 NetApp 溝通以取得授權與支援註冊。
<a href="https://packages.cloud.google.com/yum">https://packages.cloud.google.com/yum</a> <a href="https://github.com/NetApp/trident/releases/download/">https://github.com/NetApp/trident/releases/download/</a>	需要將 Cloud Volumes ONTAP 支援的系統與 Kubernetes 叢集連線。端點可安裝 NetApp Trident。
各種協力廠商位置、例如： <ul style="list-style-type: none"> <li>• <a href="https://repo1.maven.org/maven2">https://repo1.maven.org/maven2</a></li> <li>• <a href="https://oss.sonatype.org/content/repositories">https://oss.sonatype.org/content/repositories</a></li> <li>• <a href="https://repo.typesafe.org">https://repo.typesafe.org</a></li> </ul> <p>第三方據點可能會有所變更。</p>	在升級期間、Cloud Manager 會針對協力廠商相依性下載最新的套件。

#### 可在 **Cloud Volumes ONTAP Azure** 中管理不穩定功能的傳出網際網路存取

在 Cloud Volumes ONTAP Microsoft Azure 中部署及管理功能時、Cloud Manager 需要透過外傳網際網路連絡下列端點：

端點	目的
<a href="https://management.azure.com">https://management.azure.com</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>	讓 Cloud Manager 能夠在 Cloud Volumes ONTAP 大多數 Azure 地區部署及管理功能。
<a href="https://management.microsoftazure.de">https://management.microsoftazure.de</a> <a href="https://login.microsoftonline.de">https://login.microsoftonline.de</a>	讓 Cloud Manager 能夠在 Cloud Volumes ONTAP Azure Germany 地區部署及管理功能。
<a href="https://management.usgovcloudapi.net">https://management.usgovcloudapi.net</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>	讓 Cloud Manager 能夠在 Cloud Volumes ONTAP Azure US Gov 地區部署及管理功能。
<a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a>	API 要求 NetApp Cloud Central。
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>	提供軟體映像、資訊清單和範本的存取權限。

端點	目的
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> <a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a>	讓Cloud Manager能夠存取及下載資訊清單、範本及Cloud Volumes ONTAP 升級影像。
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	讓 NetApp 能夠從稽核記錄串流資料。
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	與 NetApp Cloud Central 通訊、以進行集中式使用者驗證。
<a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	與 NetApp AutoSupport 通訊
<a href="https://support.netapp.com/svcgw">https://support.netapp.com/svcgw</a> <a href="https://support.netapp.com/ServiceGW/entitlement">https://support.netapp.com/ServiceGW/entitlement</a>	與NetApp溝通以取得授權與支援註冊。
<a href="https://packages.cloud.google.com/yum">https://packages.cloud.google.com/yum</a> <a href="https://github.com/NetApp/trident/releases/download/">https://github.com/NetApp/trident/releases/download/</a>	需要將Cloud Volumes ONTAP 支援的系統與Kubernetes叢集連線。端點可安裝NetApp Trident。
各種協力廠商位置、例如： <ul style="list-style-type: none"> <li>• <a href="https://repo1.maven.org/maven2">https://repo1.maven.org/maven2</a></li> <li>• <a href="https://oss.sonatype.org/content/repositories">https://oss.sonatype.org/content/repositories</a></li> <li>• <a href="https://repo.typesafe.org">https://repo.typesafe.org</a></li> </ul> 第三方據點可能會有所變更。	在升級期間、Cloud Manager 會針對協力廠商相依性下載最新的套件。

#### 從網頁瀏覽器存取傳出網際網路

使用者必須從網頁瀏覽器存取 Cloud Manager。執行 Web 瀏覽器的機器必須連線至下列端點：

端點	目的
Cloud Manager主機	您必須從網頁瀏覽器輸入主機的 IP 位址、才能載入 Cloud Manager 主控台。  視您與雲端供應商的連線能力而定、您可以使用指派給主機的私有 IP 或公有 IP： <ul style="list-style-type: none"> <li>• 如果您有 VPN 並直接連線至虛擬網路、則私有 IP 可正常運作</li> <li>• 公有 IP 適用於任何網路情境</li> </ul> 無論如何、您應該確保安全群組規則僅允許從授權的 IP 或子網路存取、以確保網路存取安全。
<a href="https://auth0.com">https://auth0.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://services.cloud.netapp.com">https://services.cloud.netapp.com</a>	您的網頁瀏覽器會連線至這些端點、以便透過 NetApp Cloud Central 進行集中式使用者驗證。
<a href="https://widget.intercom.io">https://widget.intercom.io</a>	產品內對談可讓您與 NetApp 雲端專家交談。

可在Linux主機上安裝Cloud Manager的傳出網際網路存取

Cloud Manager安裝程式必須在安裝過程中存取下列URL：

- <http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm>
- <https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm>
- <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip>

## 連接埠和安全性群組

- 如果您從Cloud Central或市場映像部署Cloud Manager、請參閱下列內容：
  - ["AWS中Cloud Manager的安全群組規則"](#)
  - ["Azure中Cloud Manager的安全群組規則"](#)
- 如果您在現有的Linux主機上安裝Cloud Manager、請參閱 ["Cloud Manager主機需求"](#)。

# AWS 的網路需求 Cloud Volumes ONTAP

設定 AWS 網路功能、Cloud Volumes ONTAP 讓各個系統正常運作。

正在尋找Cloud Manager需要存取的端點清單？現在只需在單一位置進行維護。 ["請按一下此處以取得詳細資料"](#)。

## 一般AWS網路需求Cloud Volumes ONTAP

AWS 必須符合下列要求。

### 對節點的輸出網際網路存取 Cloud Volumes ONTAP

支援不需透過外部網際網路存取、即可將訊息傳送至 NetApp 解決方案、以主動監控儲存設備的健全狀況。 Cloud Volumes ONTAP AutoSupport

路由和防火牆原則必須允許 AWS HTTP / HTTPS 流量傳輸至下列端點、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。

### 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 \(AWS Private Link\)"](#)。

## 安全性群組

您不需要建立安全性群組、因為 Cloud Manager 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](#)"。

## 從 Cloud Volumes ONTAP 支援資料分層的功能、從功能鏈接至 AWS S3

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 至其他網路中的不二系統

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 和其他網路之間建立 VPN 連線、例如 Azure vnet 或公司網路。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](#)"。

## AWS 在 Cloud Volumes ONTAP 多個 AZs 中的功能需求

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、因為您必須在 Cloud Manager 中輸入網路詳細資料。

若要瞭解 HA 配對的運作方式、請參閱 "[高可用性配對](#)"。

### 可用性區域

此 HA 部署模式使用多個 AZs 來確保資料的高可用性。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。

### 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。



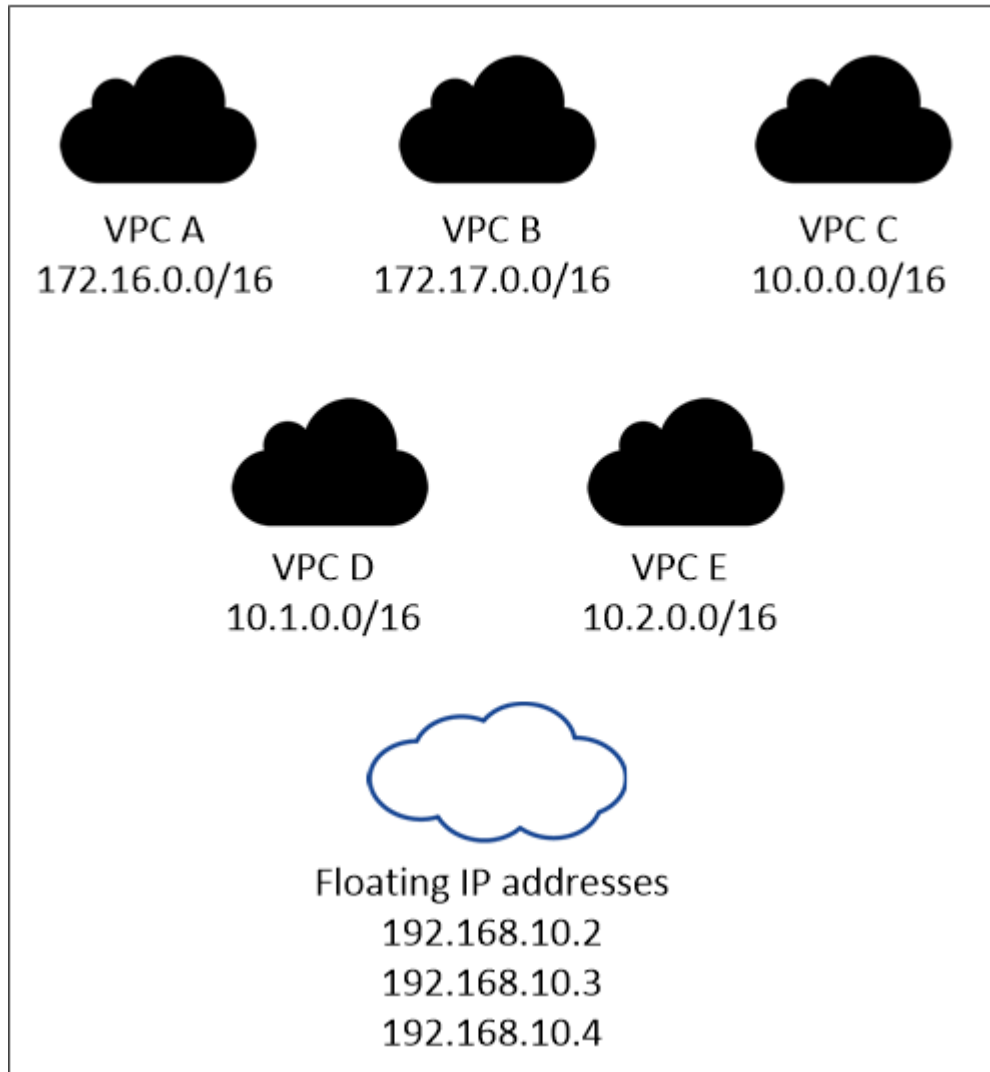
如果您使用 SnapDrive 適用於 Windows 的 SHIP 或 SnapCenter 搭配 HA 配對的 SHIP、則 SVM 管理 LIF 需要一個浮動 IP 位址。如果您在部署系統時未指定 IP 位址、您可以稍後建立 LIF。如需詳細資訊、請參閱 "[設定 Cloud Volumes ONTAP 功能](#)"。

當您建立 Cloud Volumes ONTAP 一個發揮作用的環境時、需要在 Cloud Manager 中輸入浮動 IP 位址。Cloud Manager 會在 HA 配對啟動系統時、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。

## AWS region



Cloud Manager 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

"[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 Cloud Manager 中指定浮動 IP 位址之後、您必須選取路由表、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）、Cloud Manager 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 相關聯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"](#)。

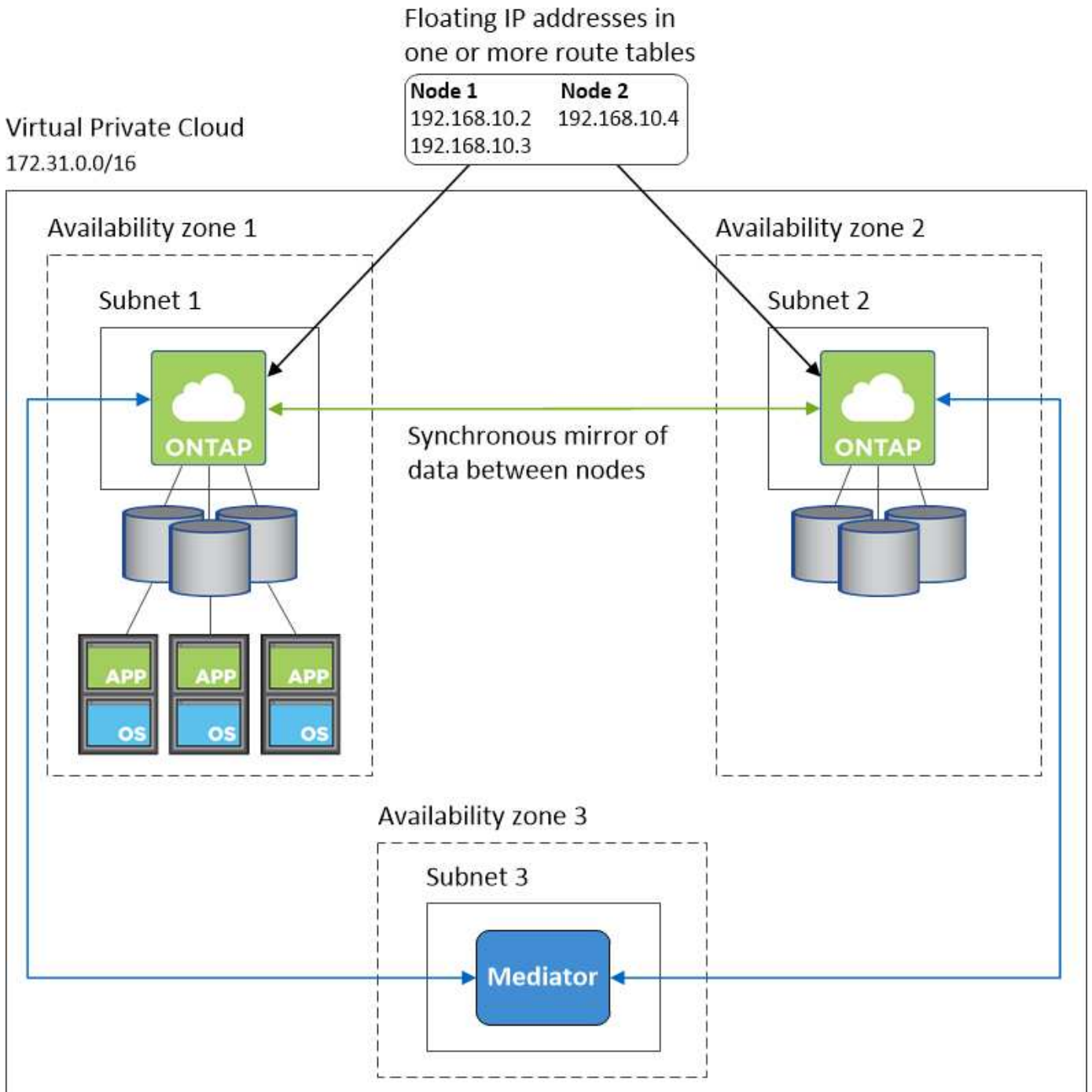
## 連線至 NetApp 管理工具

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。

## 組態範例

下圖顯示 AWS 以主動 - 被動式組態運作時的最佳 HA 組態：



## VPC組態範例

若要更深入瞭解Cloud Volumes ONTAP 解如何在AWS中部署Cloud Manager和功能、您應該檢閱最常見的VPC組態。

- 具有公有和私有子網路及NAT裝置的VPC
- 具有私有子網路和VPN連線的VPC、可連線至您的網路

### 具有公有和私有子網路及NAT裝置的VPC

此VPC組態包括公有和私有子網路、將VPC連接至網際網路的網際網路閘道、以及在公有子網路中啟用傳出網際網路流量的NAT閘道或NAT執行個體。在此組態中、您可以在公有子網路或私有子網路中執行Cloud

Manager、但建議使用公有子網路、因為它允許從VPC以外的主機存取。然後、您可以在Cloud Volumes ONTAP 私有子網路中啟動執行個體。

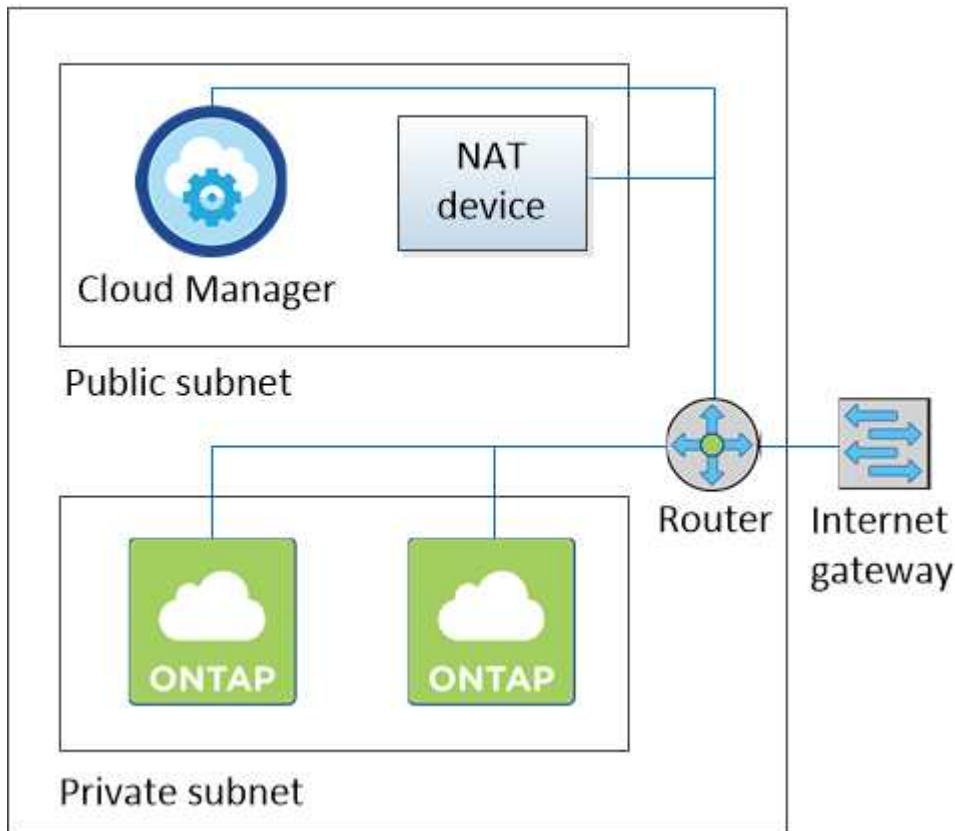


您可以使用HTTP Proxy來提供網際網路連線功能、而非使用NAT裝置。

如需此案例的詳細資訊、請參閱 "[AWS文件：情境2：VPC搭配公有和私有子網路（NAT）](#)"。

下圖顯示在公有子網路中執行的Cloud Manager、以及在私有子網路中執行的單一節點系統：

## Virtual Private Cloud



具有私有子網路和VPN連線的VPC、可連線至您的網路

這種VPC組態是混合雲組態、Cloud Volumes ONTAP 其中的功能是将效能提升到私有環境的延伸。此組態包括私有子網路和虛擬私有閘道、並可透過VPN連線至您的網路。透過VPN通道路由可讓EC2執行個體透過網路和防火牆存取網際網路。您可以在私有子網路或資料中心執行Cloud Manager。接著您會在Cloud Volumes ONTAP 私有子網路中啟動效能不均。



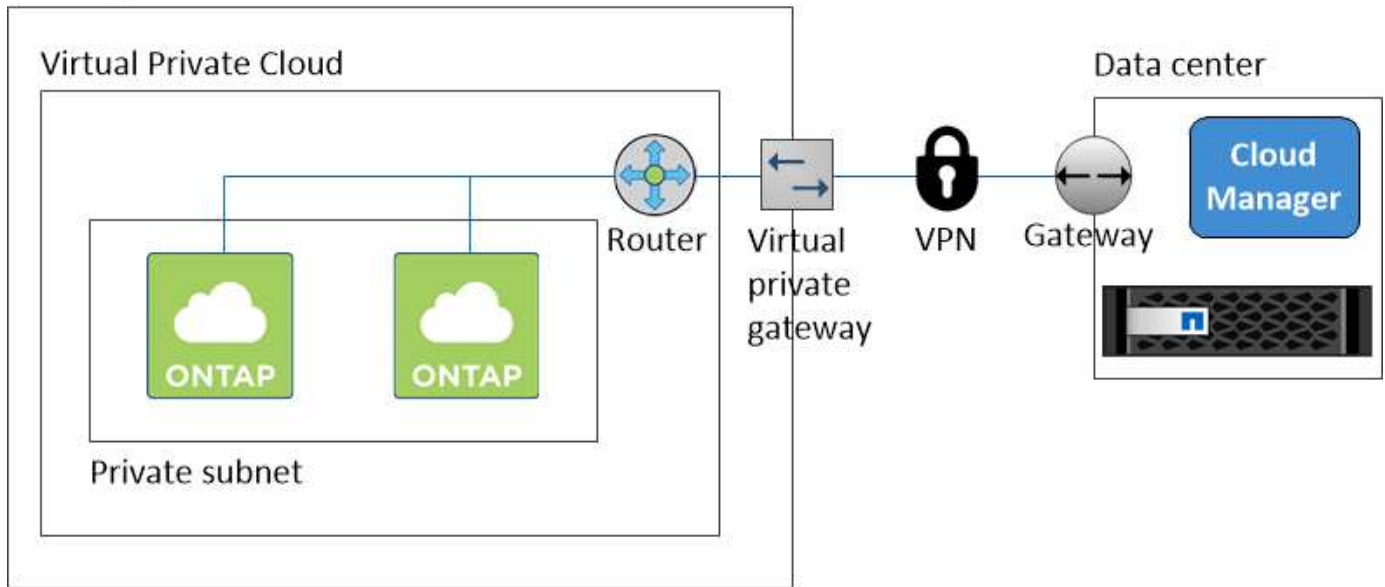
您也可以在此組態中使用Proxy伺服器來允許網際網路存取。Proxy伺服器可以位於您的資料中心或AWS中。

如果您想要在FAS 資料中心的支援系統和Cloud Volumes ONTAP AWS的支援系統之間複寫資料、您應該使用VPN連線、以確保連結安全無虞。

如需此案例的詳細資訊、請參閱 "[AWS文件：案例4：VPC僅含私有子網路和AWS託管VPN存取](#)"。

下圖顯示在資料中心執行的Cloud Manager、以及在私有子網路中執行的單一節點系統：

## AWS region



## 在多個 AZs 中設定 HA 配對的 AWS 傳輸閘道

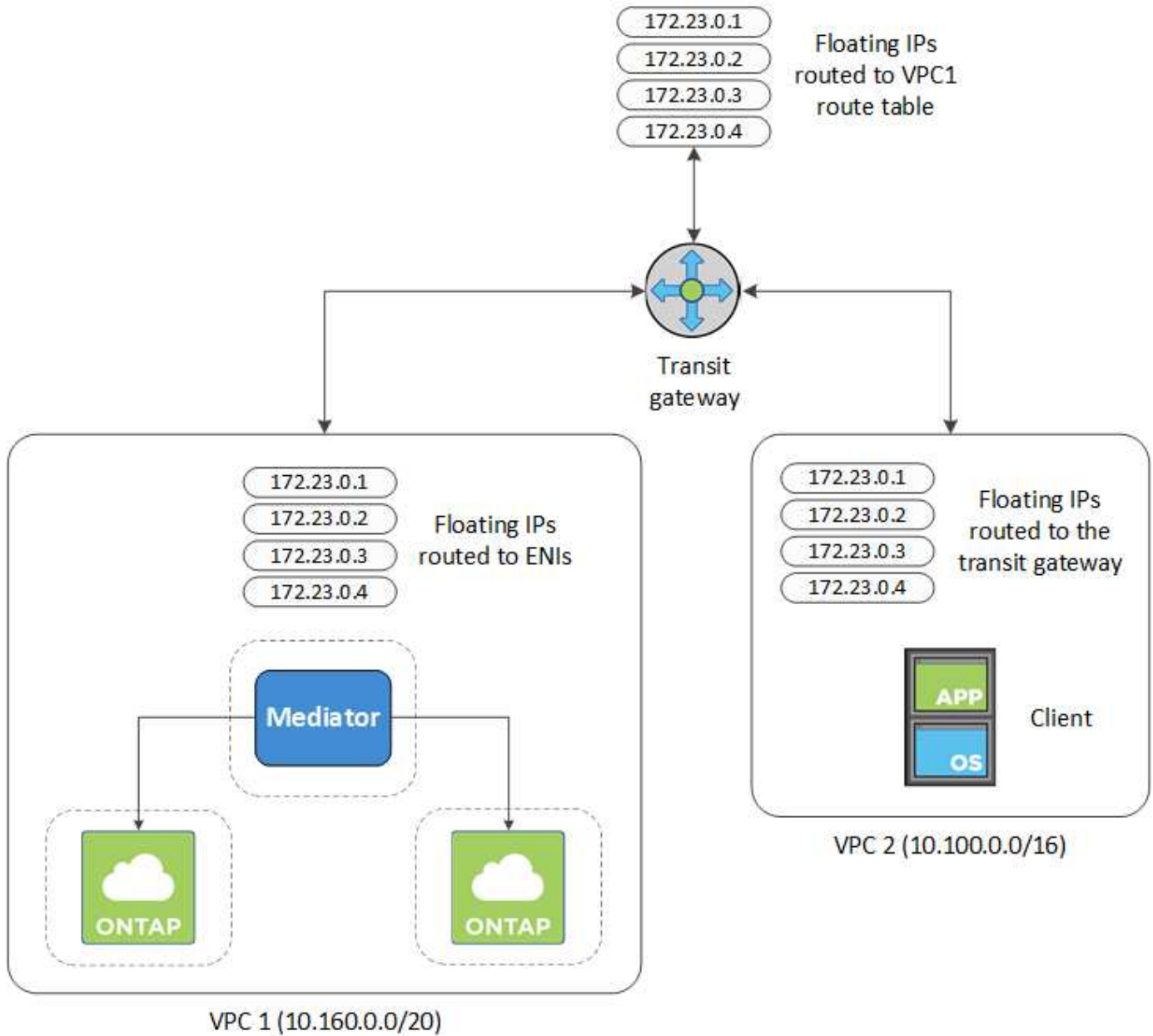
設定AWS傳輸閘道、以便從HA配對所在的VPC外部存取HA配對的浮動IP位址。

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. 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 Cloud Manager 的「工作環境資訊」頁面找到浮動 IP 位址。範例如下：

## NFS & CIFS access from within the VPC using Floating IP

### Auto failover

Cluster Management : 172.23.0.1

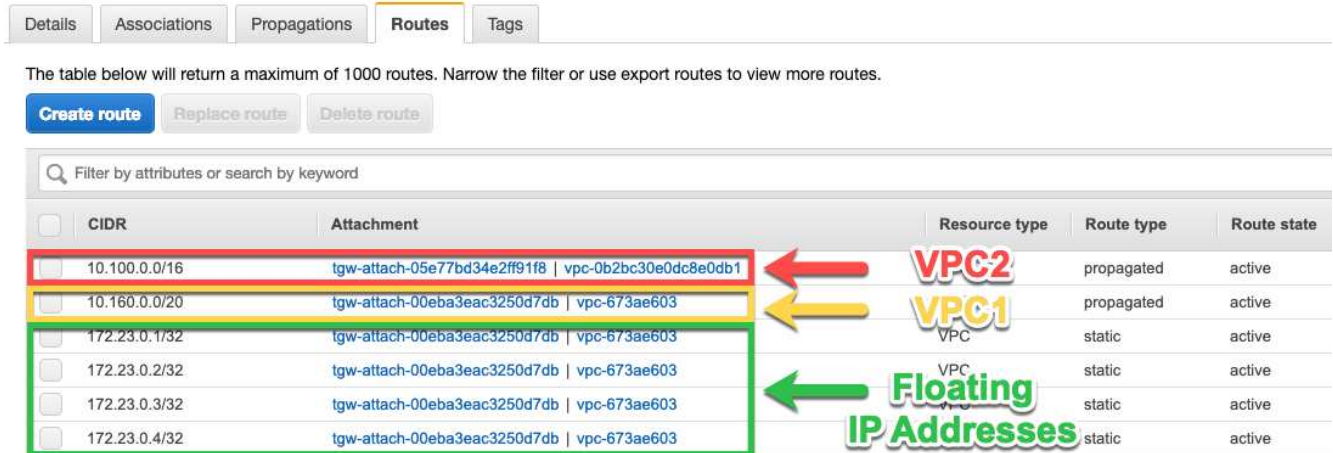
Data (nfs,cifs) : Node 1: 172.23.0.2 | Node 2: 172.23.0.3

### Access

SVM Management : 172.23.0.4

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。

Transit Gateway Route Table: tgw-rtb-0ea8ee291c7aeddd3



The screenshot shows the AWS Transit Gateway console interface for a route table. The 'Routes' tab is selected. The table below lists routes with columns for CIDR, Attachment, Resource type, Route type, and Route state. Annotations include a red arrow pointing to the VPC2 route, a yellow arrow pointing to the VPC1 route, and a green arrow pointing to the floating IP routes.

CIDR	Attachment	Resource type	Route type	Route state
10.100.0.0/16	tgw-attach-05e77bd34e2ff91f8   vpc-0b2bc30e0dc8e0db1	VPC2	propagated	active
10.160.0.0/20	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC1	propagated	active
172.23.0.1/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active
172.23.0.2/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active
172.23.0.3/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active
172.23.0.4/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active

3. 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。

Route Table: rtb-0569a1bd740ed033f

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	active	No
0.0.0.0/0	igw-07250bd01781e67df	active	No
10.160.0.0/20	tgw-015b7c249661ac279	active	No
172.23.0.1/32	tgw-015b7c249661ac279	active	No
172.23.0.2/32	tgw-015b7c249661ac279	active	No
172.23.0.3/32	tgw-015b7c249661ac279	active	No
172.23.0.4/32	tgw-015b7c249661ac279	active	No

VPC1  
Floating IP Addresses

4. 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。Cloud Manager 會在部署 HA 配對時、自動將浮動 IP 新增至路由表。

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status
10.160.0.0/20	local	active
pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22)	vpce-cb51a0a2	active
0.0.0.0/0	igw-b2182cd7	active
10.60.29.0/25	pcx-589c3331	active
10.100.0.0/16	tgw-015b7c249661ac279	active
10.129.0.0/20	pcx-f7e1396	active
172.23.0.1/32	eni-0854d4715559c3cdb	active
172.23.0.2/32	eni-0854d4715559c3cdb	active
172.23.0.3/32	eni-0f76681216c3108ed	active
172.23.0.4/32	eni-0854d4715559c3cdb	active

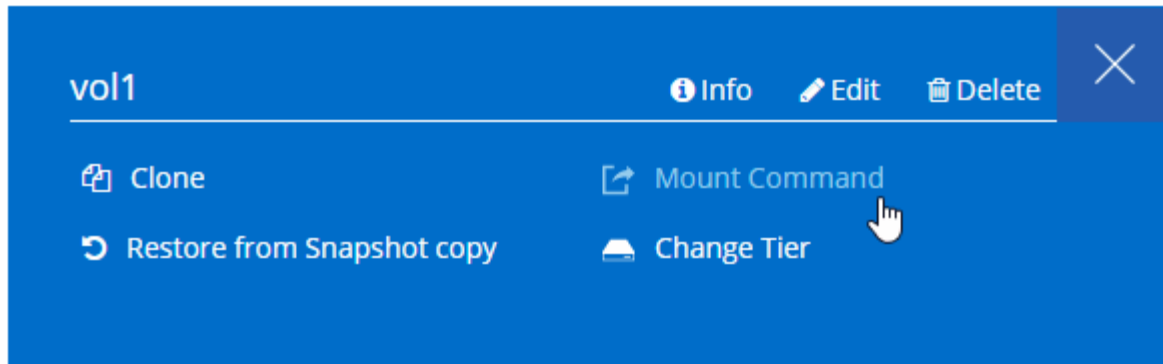
VPC2  
Floating IP Addresses

5. 使用浮動 IP 位址將磁碟區掛載到用戶端。

您可以在 Cloud Manager 中找到正確的 IP 位址、方法是選取磁碟區、然後按一下 \* Mount Command\* 。

# Volumes

2 Volumes | 0.22 TB Allocated | < 0.01 TB Used (0 TB in S3)



- 相關連結 \*
- "AWS 中的高可用性配對"
- "AWS 的網路需求 [Cloud Volumes ONTAP](#)"

## Azure 的網路需求 Cloud Volumes ONTAP

您必須設定 Azure 網路、Cloud Volumes ONTAP 才能使作業系統正常運作。

正在尋找 Cloud Manager 需要存取的端點清單？現在只需在單一位置進行維護。 ["請按一下此處以取得詳細資料"](#)。

### 輸出網際網路存取 **Cloud Volumes ONTAP** 功能

支援向 NetApp 支援部門傳送訊息、以便主動監控儲存設備的健全狀況。 Cloud Volumes ONTAP AutoSupport

路由和防火牆原則必須允許 AWS HTTP / HTTPS 流量傳輸至下列端點、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>

### 安全性群組

您不需要建立安全性群組、因為 Cloud Manager 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](#)"。

### 從邊到 **Azure Blob** 儲存設備的連線 **Cloud Volumes ONTAP**、可用於資料分層

如果您想要將冷資料分層至 Azure Blob 儲存設備、只要 Cloud Manager 具備必要權限、就不需要設定 vnet 服務端點：



```
"Microsoft.Network/virtualNetworks/subnets/write",  
"Microsoft.Network/routeTables/join/action",
```

這些權限包含在最新版本中 ["Cloud Manager 原則"](#)。

如需設定資料分層的詳細資訊、請參閱 ["將冷資料分層至低成本物件儲存設備"](#)。

#### 連線 **ONTAP** 至其他網路中的不二系統

若要在 Cloud Volumes ONTAP Azure 中的某個更新系統與 ONTAP 其他網路中的其他更新系統之間複寫資料、您必須在 Azure vnet 與其他網路（例如 AWS VPC 或公司網路）之間建立 VPN 連線。

如需相關指示、請參閱 ["Microsoft Azure 文件：在 Azure 入口網站中建立站台對站台連線"](#)。

## 版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

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。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

## 商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。