



# 開始使用

## Cloud Volumes ONTAP

NetApp  
June 22, 2022

# 目錄

|                                |    |
|--------------------------------|----|
| 開始使用 .....                     | 1  |
| 深入瞭解 Cloud Volumes ONTAP ..... | 1  |
| Amazon Web Services入門 .....    | 2  |
| 開始使用Microsoft Azure .....      | 59 |
| 開始使用Google Cloud .....         | 83 |

# 開始使用

## 深入瞭解 Cloud Volumes ONTAP

利用 NetApp 技術、您可以最佳化雲端儲存成本與效能、同時強化資料保護、安全性與法規遵循。 Cloud Volumes ONTAP

不只是軟體的儲存應用裝置、可在雲端上執行功能完善的資料管理軟體。 Cloud Volumes ONTAP 它提供企業級儲存設備、具備下列主要功能：

- 儲存效率

運用內建的重複資料刪除技術、資料壓縮、精簡配置及複製技術、將儲存成本降至最低。

- 高可用度

確保雲端環境發生故障時、企業的可靠性和持續營運。

- 資料保護

利用 NetApp 領先業界的複寫技術 SnapMirror、將內部部署資料複寫到雲端、讓次要複本可輕鬆用於多種使用案例。 Cloud Volumes ONTAP

此外、還能與 Cloud Backup 整合、提供備份與還原功能、以保護雲端資料、並長期歸檔。 Cloud Volumes ONTAP

### "深入瞭解 Cloud Backup"

- 資料分層

在高效能與低效能儲存資源池之間隨需切換、而不需將應用程式離線。

- 應用程式一致性

使用 NetApp SnapCenter 功能確保 NetApp Snapshot 複本的一致性。

### "深入瞭解 SnapCenter 解功能"

- 資料安全

支援資料加密、並提供防範病毒和勒索軟體的功能。 Cloud Volumes ONTAP

- 隱私權法規遵循控管

與 Cloud Data Sense 整合可協助您瞭解資料內容並識別敏感資料。

### "深入瞭解 Cloud Data Sense"



不含適用於功能的授權 ONTAP。 Cloud Volumes ONTAP

["檢視支援 Cloud Volumes ONTAP 的支援的支援功能"](#)

["深入瞭解 Cloud Volumes ONTAP 解功能"](#)

## Amazon Web Services入門

### 在AWS中快速入門Cloud Volumes ONTAP

只要幾個步驟、Cloud Volumes ONTAP 就能開始使用AWS的功能。

如果您沒有 ["連接器"](#) 然而、帳戶管理員需要建立一個帳戶。 ["瞭解如何在 AWS 中建立 Connector"](#)。

當您建立第一個 Cloud Volumes ONTAP 運作環境時、如果您還沒有連接器、Cloud Manager 會提示您部署連接器。

Cloud Manager 提供符合工作負載需求的預先設定套件、您也可以建立自己的組態。如果您選擇自己的組態、應該瞭解可用的選項。 ["深入瞭解"](#)。

1. 確保您的 VPC 和子網路支援連接器與 Cloud Volumes ONTAP 支援之間的連線。

2. 啟用從目標 VPC 的傳出網際網路存取、讓 Connector 和 Cloud Volumes ONTAP 支援中心能夠連絡多個端點。

這個步驟很重要、因為連接器 Cloud Volumes ONTAP 無法在沒有外傳網際網路存取的情況下管理不穩定。如果您需要限制傳出連線、請參閱的端點清單 ["Connector 與 Cloud Volumes ONTAP the"](#)。

3. 設定 S3 服務的 VPC 端點。

如果您想要將冷資料從 Cloud Volumes ONTAP 不願儲存到低成本物件儲存設備、則需要 VPC 端點。

["深入瞭解網路需求"](#)。

如果您想搭配 Cloud Volumes ONTAP 使用 Amazon 加密搭配使用、則必須確保存在作用中的客戶主金鑰（CMK）。您也必須新增 IAM 角色、將連接器的權限提供給作為 `_key 使用者` 的連接器、以修改每個 CMK 的金鑰原則。 ["深入瞭解"](#)。

按一下「\* 新增工作環境 \*」、選取您要部署的系統類型、然後完成精靈中的步驟。 ["閱讀逐步指示"](#)。

#### 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"](#)
- ["Cloud Manager 使用 AWS 權限的功能"](#)

## 在Cloud Volumes ONTAP AWS中規劃您的不一樣組態

在 Cloud Volumes ONTAP AWS 中部署時、您可以選擇符合工作負載需求的預先設定系統、也可以建立自己的組態。如果您選擇自己的組態、應該瞭解可用的選項。

選擇**Cloud Volumes ONTAP** 一個不含功能的授權

有多種授權選項可供Cloud Volumes ONTAP 選擇。每個選項都能讓您選擇符合需求的消費模式。

- ["深入瞭解Cloud Volumes ONTAP 解適用於此功能的授權選項"](#)
- ["瞭解如何設定授權"](#)

選擇支援的地區

支援大部分 AWS 地區的支援。Cloud Volumes ONTAP ["檢視支援區域的完整清單"](#)。

您必須先啟用較新的 AWS 區域、才能在這些區域中建立及管理資源。 ["瞭解如何啟用地區"](#)。

選擇支援的執行個體

根據您選擇的授權類型、支援多種執行個體類型。 Cloud Volumes ONTAP

["AWS支援Cloud Volumes ONTAP 的支援組態"](#)

瞭解儲存限制

一個不含資源的系統的原始容量上限 Cloud Volumes ONTAP 與授權有關。其他限制會影響集合體和磁碟區的大小。在規劃組態時、您應該注意這些限制。

["AWS的儲存限制Cloud Volumes ONTAP"](#)

在**AWS**中調整系統規模

調整 Cloud Volumes ONTAP 您的支援規模、有助於滿足效能與容量的需求。在選擇執行個體類型、磁碟類型和磁碟大小時、您應該注意幾個關鍵點：

執行個體類型

- 將工作負載需求與每個 EC2 執行個體類型的最大處理量和 IOPS 配對。
- 如果有多位使用者同時寫入系統、請選擇有足夠 CPU 來管理要求的執行個體類型。
- 如果您的應用程式大多讀取、請選擇具有足夠 RAM 的系統。
  - ["AWS 文件：Amazon EC2 執行個體類型"](#)
  - ["AWS 文件：Amazon EBS 最佳化執行個體"](#)

**EBS** 磁碟類型

EBS磁碟類型之間的差異較高、如下所示。若要深入瞭解EBS磁碟的使用案例、請參閱 ["AWS 文件：EBS Volume 類型"](#)。

- 通用SSD（GP3） 磁碟是成本最低的SSD、可在各種工作負載的成本與效能之間取得平衡。效能是

以IOPS和處理量來定義。支援GP3磁碟Cloud Volumes ONTAP 的版本可搭配使用。9.7及更新版本。

當您選取GP3磁碟時、Cloud Manager會填入預設的IOPS和處理量值、這些值會根據選取的磁碟大小提供相當於gp2磁碟的效能。您可以提高價值、以更高的成本獲得更好的效能、但我們不支援較低的值、因為這樣可能導致效能低落。簡而言之、請保留預設值或增加預設值。請勿降低。"[深入瞭解GP3磁碟及其效能](#)"。

請注意Cloud Volumes ONTAP、此功能可搭配GP3磁碟支援Amazon EBS彈性磁碟區功能。"[深入瞭解彈性磁碟區支援](#)"。

- 通用SSD (gp2) 磁碟可平衡各種工作負載的成本與效能。效能是以 IOPS 定義。
- 資源配置的IOPS SSD (io1) 磁碟適用於需要以較高成本獲得最高效能的關鍵應用程式。

請注意Cloud Volumes ONTAP、支援Amazon EBS彈性Volume功能搭配IO1磁碟。"[深入瞭解彈性磁碟區支援](#)"。

- Throughput Optimized HDD (ST1) 磁碟適用於經常存取的工作負載、這些工作負載需要以較低的價格提供快速且一致的處理量。



使用處理量最佳化的HDD (ST1) 時、不建議將資料分層至物件儲存設備。

## EBS 磁碟大小

如果您選擇不支援的組態 "[Amazon EBS彈性磁碟區功能](#)"之後、您需要在啟動Cloud Volumes ONTAP 一套系統時選擇初始磁碟大小。之後、您就可以了 "[讓 Cloud Manager 為您管理系統容量](#)"但如果您想要的話 "[自行建立集合體](#)"請注意下列事項：

- 集合體中的所有磁碟大小必須相同。
- EBS 磁碟的效能與磁碟大小有關。大小決定 SSD 磁碟的基準 IOPS 和最大突發持續時間、以及 HDD 磁碟的基準和突發處理量。
- 最後、您應該選擇能提供所需 持續效能 的磁碟大小。
- 即使您選擇較大的磁碟（例如六個4 TiB磁碟）、也可能無法取得所有IOPS、因為EC2執行個體可能達到其頻寬限制。

如需 EBS 磁碟效能的詳細資訊、請參閱 "[AWS 文件：EBS Volume 類型](#)"。

如上所述、Cloud Volumes ONTAP 支援Amazon EBS彈性Volume功能的各種組態不支援選擇磁碟大小。"[深入瞭解彈性磁碟區支援](#)"。

請觀看下列影片、以瞭解如何在 Cloud Volumes ONTAP AWS 中調整您的更新功能：



### 檢視預設系統磁碟

Cloud Manager除了儲存使用者資料之外、也購買雲端儲存設備來儲存Cloud Volumes ONTAP 作業系統資料（開機資料、根資料、核心資料和NVRAM）。為了規劃目的、在部署Cloud Volumes ONTAP 完更新之前、您可能需要先檢閱這些詳細資料。

["在Cloud Volumes ONTAP AWS中檢視系統資料的預設磁碟"](#)。



連接器也需要系統磁碟。 ["檢視Connector預設組態的詳細資料"](#)。

### 準備在Cloud Volumes ONTAP AWS Outpost部署功能

如果您有 AWS Outpost、您可以 Cloud Volumes ONTAP 在「工作環境」精靈中選取 Outpost VPC、在該 Outpost 中部署功能不全。體驗與 AWS 中的任何其他 VPC 相同。請注意、您必須先在 AWS Outpost 部署 Connector。

有幾項限制可以指出：

- 目前僅 Cloud Volumes ONTAP 支援單一節點的不支援系統
- 您可以搭配 Cloud Volumes ONTAP 使用的 EC2 執行個體僅限於您的據點所提供的項目
- 目前僅支援通用SSD（gp2）

### 收集網路資訊

在 Cloud Volumes ONTAP AWS 中啟動時、您需要指定 VPC 網路的詳細資料。您可以使用工作表向系統管理員收集資訊。

#### 單一AZ中的單一節點或HA配對

| AWS 資訊          | 您的價值 |
|-----------------|------|
| 區域              |      |
| VPC             |      |
| 子網路             |      |
| 安全性群組（如果使用您自己的） |      |

#### 多個AZs中的HA配對

| AWS 資訊            | 您的價值 |
|-------------------|------|
| 區域                |      |
| VPC               |      |
| 安全性群組（如果使用您自己的）   |      |
| 節點 1 可用度區域        |      |
| 節點 1 子網路          |      |
| 節點 2 可用度區域        |      |
| 節點 2 子網路          |      |
| 中介可用度區域           |      |
| 中介子網路             |      |
| 中介器的金鑰配對          |      |
| 叢集管理連接埠的浮動 IP 位址  |      |
| 節點 1 上資料的浮動 IP 位址 |      |
| 節點 2 上資料的浮動 IP 位址 |      |
| 浮動 IP 位址的路由表      |      |

#### 選擇寫入速度

Cloud Manager 可讓您選擇 Cloud Volumes ONTAP 適合的寫入速度設定。在您選擇寫入速度之前、您應該先瞭解一般與高設定之間的差異、以及使用高速寫入速度時的風險與建議。 ["深入瞭解寫入速度"](#)。

#### 選擇Volume使用設定檔

包含多項儲存效率功能、可減少您所需的總儲存容量。ONTAP在 Cloud Manager 中建立 Volume 時、您可以選擇啟用這些功能的設定檔、或是停用這些功能的設定檔。您應該深入瞭解這些功能、以協助您決定要使用的設定檔。

NetApp 儲存效率功能提供下列效益：



## 資源隨需配置

為主機或使用者提供比實體儲存資源池實際擁有更多的邏輯儲存設備。儲存空間不會預先配置儲存空間、而是會在寫入資料時動態分配給每個磁碟區。

## 重複資料刪除

找出相同的資料區塊、並以單一共用區塊的參考資料取代這些區塊、藉此提升效率。這項技術可消除位於同一個磁碟區的備援資料區塊、進而降低儲存容量需求。

## 壓縮

藉由壓縮主儲存設備、次儲存設備和歸檔儲存設備上磁碟區內的資料、來減少儲存資料所需的實體容量。

## 設定您的網路

### AWS 的網路需求 Cloud Volumes ONTAP

Cloud Manager可處理Cloud Volumes ONTAP 有關功能的網路元件設定、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。

["瞭解如何設定 AutoSupport 功能"](#)。

### 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

Cloud Manager會自動分配所需數量的私有IP位址Cloud Volumes ONTAP 給各個方面。您必須確保網路有足夠的私有IP位址可用。

Cloud Manager分配Cloud Volumes ONTAP 給功能不全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

Cloud Manager會將6個IP位址分配給單一節點系統：

- 叢集管理LIF
- 節點管理 LIF
- 叢集間 LIF
- NAS資料LIF
- iSCSI資料LIF
- 儲存VM管理LIF

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。 |
| 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  | eth2 | 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 | eth3 | 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。此LIF也能管理節點之間的浮動IP位址移轉作業。                      |
| 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     | eth2 | 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 | eth3 | 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 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"](#)。

### 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。

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

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 Cloud Manager 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）、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"](#)。

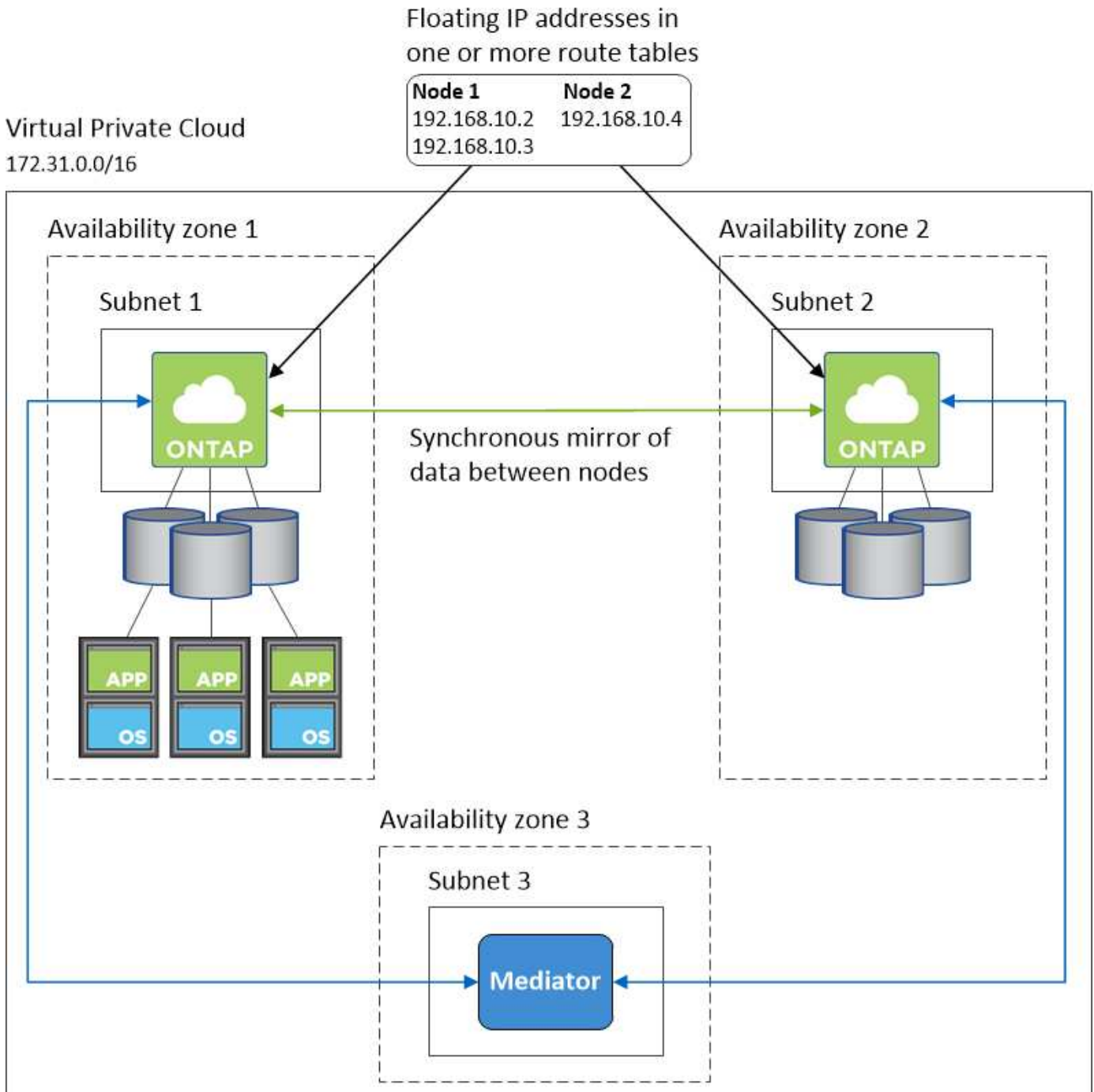
## 連線至 NetApp 管理工具

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。

## 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

設定您的網路、讓 Connector 能夠管理公有雲環境中的資源和程序。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、您可以從「設定」頁面指定 Proxy 伺服器。請參閱 ["將 Connector 設定為使用 Proxy 伺服器"](#)。

## 連線至目標網路

連接器需要網路連線至您要部署 Cloud Volumes ONTAP 的 VPC 和 VNets 。

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

## 傳出網際網路存取

連接器需要存取傳出網際網路、才能管理公有雲環境中的資源和程序。

| 端點   | 目的                                     |
|--|--|
| <a href="https://support.netapp.com">https://support.netapp.com</a>  | 以取得授權資訊、並將AutoSupport 資訊傳送給NetApp支援部門。 |
| <a href="https://*.cloudmanager.cloud.netapp.com">https://*.cloudmanager.cloud.netapp.com</a>  | 在Cloud Manager中提供SaaS功能與服務。            |
| <a href="https://cloudmanagerinfraproduct.azurecr.io">https://cloudmanagerinfraproduct.azurecr.io</a><br><a href="https://*.blob.core.windows.net">https://*.blob.core.windows.net</a> | 升級Connector及其Docker元件。                 |

## 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 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-0ea8ee291c7aedd3

Details Associations Propagations **Routes** Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route Replace route Delete route

Filter by attributes or search by keyword

| <input type="checkbox"/> | CIDR          | Attachment   | Resource type | Route type | Route state |
|--------------------------|---------------|--|---------------|------------|-------------|
| <input type="checkbox"/> | 10.100.0.0/16 | tgw-attach-05e77bd34e2ff91f8   vpc-0b2bc30e0dc8e0db1 | VPC2          | propagated | active      |
| <input type="checkbox"/> | 10.160.0.0/20 | tgw-attach-00eba3eac3250d7db   vpc-673ae603          | VPC1          | propagated | active      |
| <input type="checkbox"/> | 172.23.0.1/32 | tgw-attach-00eba3eac3250d7db   vpc-673ae603          | VPC           | static     | active      |
| <input type="checkbox"/> | 172.23.0.2/32 | tgw-attach-00eba3eac3250d7db   vpc-673ae603          | Floating IP   | static     | active      |
| <input type="checkbox"/> | 172.23.0.3/32 | tgw-attach-00eba3eac3250d7db   vpc-673ae603          | Floating IP   | static     | active      |
| <input type="checkbox"/> | 172.23.0.4/32 | tgw-attach-00eba3eac3250d7db   vpc-673ae603          | Floating IP   | static     | active      |

#### 4. 修改需要存取浮動 IP 位址的 VPC 路由表。

- 新增路由項目至浮動 IP 位址。
- 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     | lgw-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

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。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   | lgw-b2182dd7          | 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

6. 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)



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

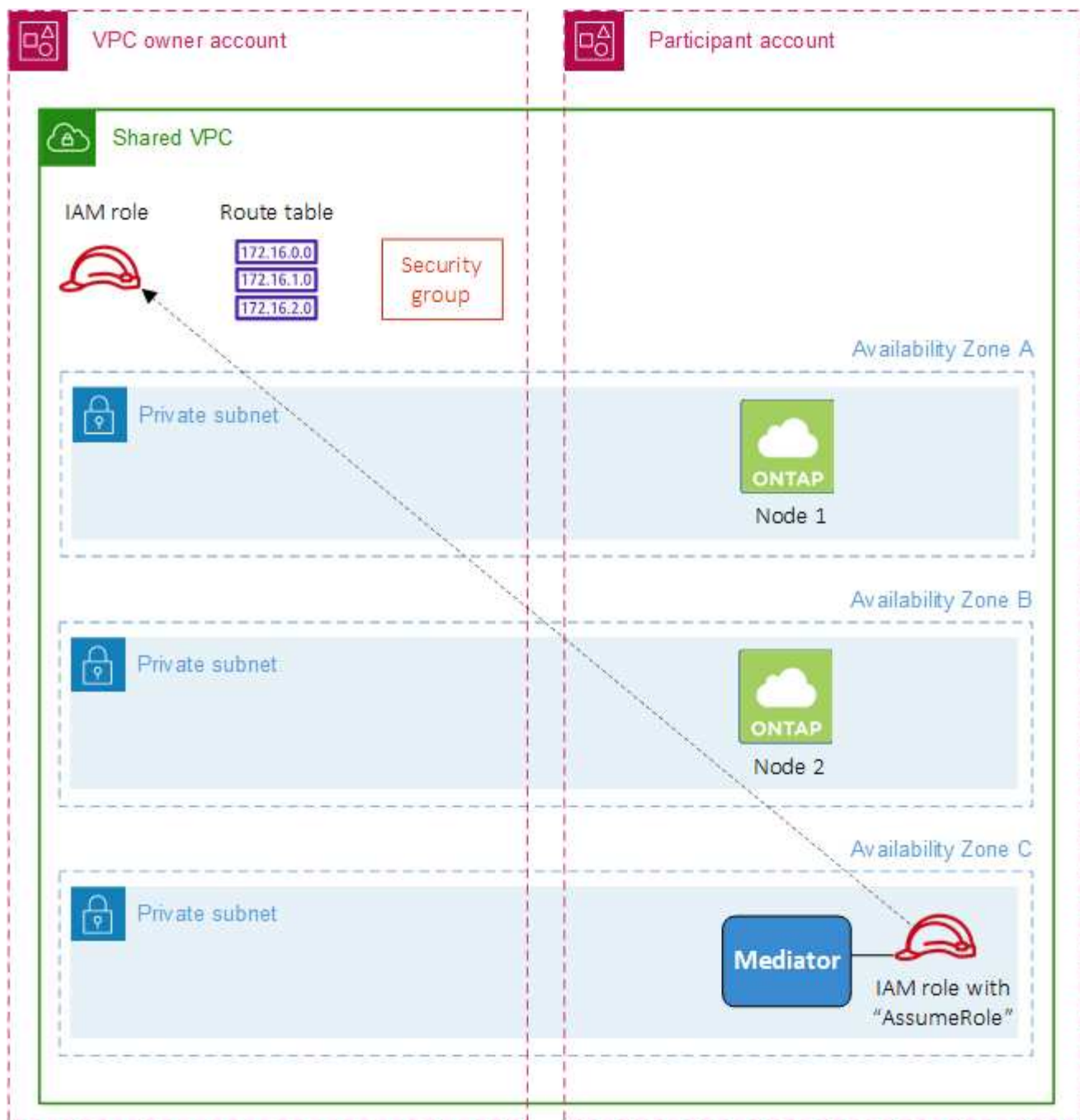
從9.11.1版開始、Cloud Volumes ONTAP AWS支援搭配VPC共享功能的更新版、VPC共用功能可讓您的組織與其他AWS帳戶共用子網路。若要使用此組態、您必須設定AWS環境、然後使用API部署HA配對。

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 運作環境時、Cloud Manager會自動建立IAM角色、並將其附加至中介者。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。Cloud Manager 能幫您達成這項目標。

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Cloud Manager API建立全新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「assumeRoleArn」

「assumeRoleArn」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"
}
```

+

"深入瞭解Cloud Volumes ONTAP 解NetApp API"

## AWS 的安全群組規則

Cloud Manager 會建立 AWS 安全性群組、其中包含 Connector 和 Cloud Volumes ONTAP NetApp 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

預先定義之安全性群組中的傳入規則來源為 0.00.0.0/0 。

| 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、以 HTTPS 存取 System Manager 網路主控台  |
| 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 | 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

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  |
| 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  |
|------------|------|---------------|----------------------------|---------------|---|
| 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） |
| 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                                  |

#### 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

傳入規則的來源為 0.00.0.0/0。

| 傳輸協定 | 連接埠  | 目的                            |
|------|------|-------------------------------|
| SSH  | 22   | SSH 連線至 HA 中介器                |
| TCP  | 3000 | 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    | 連接器 IP 位址  | 下載中介程式升級   |
| HTTPS | 443.. | AWS API 服務 | 協助進行儲存容錯移轉 |
| UDP   | 53.   | AWS API 服務 | 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。

Cloud Manager 一律會建立這個安全群組。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

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   |
|------------------------|-------|-------|------------------------|--|
| API 呼叫與 AutoSupport 功能 | HTTPS | 443.. | 傳出網際網路和 ONTAP 叢集管理 LIF | API會呼叫AWS和ONTAP VMware、Cloud Data Sense、勒索軟體服務、並將AutoSupport 這些訊息傳送給NetApp |
| API 呼叫                 | TCP   | 3000  | 充當HA中介者ONTAP           | 與ONTAP NetApp HA中介人通訊  |
|                        | 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  |

| 服務     | 傳輸協定 | 連接埠 | 目的地                   | 目的  |
|--------|------|-----|-----------------------|---|
| 雲端資料感測 | HTTP | 80  | Cloud Data Sense 執行個體 | Cloud Data Sense for Cloud Volumes ONTAP 功能 |

## 設定 AWS KMS

如果您想搭配 Cloud Volumes ONTAP 使用 Amazon 加密搭配使用、則需要設定 AWS 金鑰管理服務（KMS）。

### 步驟

1. 確認存在作用中的客戶主金鑰（CMK）。

CMK 可以是 AWS 託管的 CMK、也可以是客戶託管的 CMK。它可以與 Cloud Manager 及 Cloud Volumes ONTAP 其他 AWS 帳戶位於相同的 AWS 帳戶中、也可以位於不同的 AWS 帳戶中。

"AWS 文件：客戶主要金鑰（CMK）"

2. 將 IAM 角色新增為 Cloud Manager 提供權限、做為 \_key 使用者\_、以修改每個 CMK 的金鑰原則。

將 IAM 角色新增為主要使用者、可讓 Cloud Manager 有權搭配 Cloud Volumes ONTAP 使用 CMK。

"AWS 文件：編輯金鑰"

3. 如果 CMK 位於不同的 AWS 帳戶、請完成下列步驟：

- a. 從 CMK 所在的帳戶移至 KMS 主控台。
- b. 選取金鑰。
- c. 在「\* 一般組態 \*」窗格中、複製金鑰的 ARN。

建立 Cloud Volumes ONTAP 一套系統時、您必須提供 ARN 給 Cloud Manager。

- d. 在 \* 其他 AWS 帳戶 \* 窗格中、新增提供 Cloud Manager 權限的 AWS 帳戶。

在大多數情況下、這是 Cloud Manager 所在的帳戶。如果 AWS 中未安裝 Cloud Manager、則您會將 AWS 存取金鑰提供給 Cloud Manager。



### Other AWS accounts

×

Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. [Learn more](#)

arn:aws:iam::

:root

Remove

Add another AWS account

Cancel

Save changes

- e. 現在請切換至 AWS 帳戶、該帳戶可為 Cloud Manager 提供權限、並開啟 IAM 主控台。
- f. 建立包含下列權限的 IAM 原則。
- g. 將原則附加至提供 Cloud Manager 權限的 IAM 角色或 IAM 使用者。

下列原則提供 Cloud Manager 從外部 AWS 帳戶使用 CMK 所需的權限。請務必修改「資源」區段中的區域和帳戶 ID。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowUseOfTheKey",
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:externalaccountid:key/externalkeyid"
      ]
    },
    {
      "Sid": "AllowAttachmentOfPersistentResources",
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:externalaccountid:key/externalaccountid"
      ],
      "Condition": {
        "Bool": {
          "kms:GrantIsForAWSResource": true
        }
      }
    }
  ]
}

```

+

如需此程序的其他詳細資料、請參閱 ["AWS文件：允許其他帳戶的使用者使用KMS金鑰"](#)。

- 如果您使用由客戶管理的CMK、請將Cloud Volumes ONTAP「IAM角色」新增為「\_key使用者」、以修改CMK的金鑰原則。

如果您在Cloud Volumes ONTAP 支援資料分層的情況下、想要加密儲存在S3儲存區中的資料、就必須執行

此步驟。

您需要在部署Cloud Volumes ONTAP 完時執行此步驟 after、因為IAM角色是在您建立工作環境時建立的。  
(當然、您可以選擇使用現有Cloud Volumes ONTAP 的IAM角色、因此可以在之前執行此步驟。)

["AWS 文件：編輯金鑰"](#)

## 在Cloud Volumes ONTAP AWS中設定適用於此功能的授權

決定Cloud Volumes ONTAP 要搭配使用哪種授權選項之後、您必須先執行幾個步驟、才能在建立新的工作環境時選擇授權選項。

### Freemium

選擇Freemium產品、即可免費使用Cloud Volumes ONTAP 多達500 GiB的配置容量。 ["深入瞭解Freemium產品"](#)。

#### 步驟

1. 在「畫版」頁面上、按一下「新增工作環境」、然後依照Cloud Manager中的步驟進行。
  - a. 在\*詳細資料與認證\*頁面上、按一下\*編輯認證>新增訂閱\*、然後依照提示訂閱AWS Marketplace中的隨用隨付方案。

除非您超過500 GiB的已配置容量、系統會自動轉換為、否則不會透過市場訂閱付費 ["Essentials套件"](#)。



## Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

☐ **Pay-Per-TiB - Annual Contract**  
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

☒ **Pay-as-you-go**  
Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

- 1 AWS Marketplace**  
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 Cloud Manager**  
Save your subscription and associate the Marketplace subscription with your AWS credentials.

**Continue** **Cancel**

- a. 返回Cloud Manager之後、當您進入「充電方法」頁面時、請選取\* Freemium \*。

### Select Charging Method

|   |             |   |
|---|-------------|---|
| <input type="radio"/> Professional                        | By capacity | ▼ |
| <input type="radio"/> Essential                           | By capacity | ▼ |
| <input checked="" type="radio"/> Freemium (Up to 500 GiB) | By capacity | ▼ |
| <input type="radio"/> Per Node                            | By node     | ▼ |

"請參閱逐步指示、以在Cloud Volumes ONTAP AWS中啟動功能"。

#### 容量型授權

容量型授權可讓您針對Cloud Volumes ONTAP 容量的每個TiB付費。容量型授權的形式為\_package\_

： Essentials套件或Professional套件。

Essentials和Professional套件可搭配下列消費模式使用：

- 向NetApp購買的授權（BYOL）
- 從AWS Marketplace訂閱時數小時隨付（PAYGO）
- AWS Marketplace的年度合約

["深入瞭解容量型授權"](#)。

下列各節將說明如何開始使用這些消費模式。

## BYOL

事先向NetApp購買授權（BYOL）、即可在Cloud Volumes ONTAP 任何雲端供應商部署支援系統。

步驟

1. ["請聯絡NetApp銷售人員以取得授權"](#)
2. ["將您的NetApp支援網站帳戶新增至Cloud Manager"](#)

Cloud Manager會自動查詢NetApp的授權服務、以取得與您NetApp支援網站帳戶相關之授權的詳細資料。如果沒有錯誤、Cloud Manager會自動將授權新增至Digital Wallet。

您的授權必須先從Digital Wallet取得、才能搭配Cloud Volumes ONTAP 使用。如有需要、您可以 ["手動將授權新增至Digital Wallet"](#)。

3. 在「畫版」頁面上、按一下「新增工作環境」、然後依照Cloud Manager中的步驟進行。
  - a. 在\*詳細資料與認證\*頁面上、按一下\*編輯認證>新增訂閱\*、然後依照提示訂閱AWS Marketplace中的隨用隨付方案。

您向NetApp購買的授權一律會先收取費用、但如果您超過授權容量或授權到期、則會從市場的每小時費率中收取費用。

## Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

☐ Pay-Per-TiB - Annual Contract

Pay for Cloud Volumes ONTAP with an annual, upfront payment.

☒ Pay-as-you-go

Pay for Cloud Volumes ONTAP at an hourly rate.

### The next steps:

1 **AWS Marketplace**

Subscribe and then click **Set Up Your Account** to configure your account.

2 **Cloud Manager**

Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue

Cancel

- a. 返回Cloud Manager之後、請在前往「充電方法」頁面時、選取容量型套件。

### Select Charging Method



Professional

By capacity



Essential

By capacity



Freemium (Up to 500 GiB)

By capacity



Per Node

By node



"請參閱逐步指示、以在Cloud Volumes ONTAP AWS中啟動功能"。

### PAYGO訂閱

從雲端供應商的市場訂閱優惠、每小時支付一次。

當您建立Cloud Volumes ONTAP 一個可運作的環境時、Cloud Manager會提示您訂閱AWS Marketplace提供的合約。該訂閱之後會與工作環境建立關聯、以便進行充電。您可以在其他工作環境中使用相同的訂閱。

#### 步驟

1. 在「畫版」頁面上、按一下「新增工作環境」、然後依照Cloud Manager中的步驟進行。
  - a. 在\*詳細資料與認證\*頁面上、按一下\*編輯認證>新增訂閱\*、然後依照提示訂閱AWS Marketplace中的隨用隨付方案。

The screenshot shows a dialog box titled "Edit Credentials & Add Subscription". Below the title, there is a horizontal line and a paragraph of text: "Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe." Below this text are two selectable options, each in a light gray box. The first option is "Pay-Per-TiB - Annual Contract" with a radio button, and its description is "Pay for Cloud Volumes ONTAP with an annual, upfront payment." The second option is "Pay-as-you-go" with a selected radio button (indicated by a blue dot), and its description is "Pay for Cloud Volumes ONTAP at an hourly rate." Below these options is another horizontal line and the text "The next steps:". This is followed by a numbered list of two steps. Step 1 is "AWS Marketplace" with a blue circle containing the number 1, and the instruction "Subscribe and then click **Set Up Your Account** to configure your account." Step 2 is "Cloud Manager" with a blue circle containing the number 2, and the instruction "Save your subscription and associate the Marketplace subscription with your AWS credentials." At the bottom right of the dialog box are two buttons: a blue "Continue" button and a gray "Cancel" button.

**Edit Credentials & Add Subscription**

---

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

☐ **Pay-Per-TiB - Annual Contract**  
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

☒ **Pay-as-you-go**  
Pay for Cloud Volumes ONTAP at an hourly rate.

---

**The next steps:**

- 1 AWS Marketplace**  
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 Cloud Manager**  
Save your subscription and associate the Marketplace subscription with your AWS credentials.

---

**Continue** **Cancel**

- b. 返回Cloud Manager之後、請在前往「充電方法」頁面時、選取容量型套件。

Select Charging Method

☒ Professional

By capacity

▼

☐ Essential

By capacity

▼

☐ Freemium (Up to 500 GiB)

By capacity

▼

☐ Per Node

By node

▼

"請參閱逐步指示、以在Cloud Volumes ONTAP AWS中啟動功能"。



您可以從「設定」>「認證」頁面管理與AWS帳戶相關的AWS Marketplace訂閱。"瞭解如何管理AWS帳戶和訂閱"

#### 年度合約

每年向雲端供應商的市場購買一年一度的合約即可付款。

Cloud Manager類似於每小時訂閱、會提示您訂閱AWS Marketplace提供的年度合約。

#### 步驟

1. 在「畫版」頁面上、按一下「新增工作環境」、然後依照Cloud Manager中的步驟進行。
  - a. 在\*詳細資料與認證\*頁面上、按一下\*編輯認證>新增訂閱\*、然後依照提示在AWS Marketplace訂閱年度合約。

## Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

☒ **Pay-Per-TiB - Annual Contract**  
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

☐ **Pay-as-you-go**  
Pay for Cloud Volumes ONTAP at an hourly rate.

**The next steps:**

- 1 AWS Marketplace**  
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 Cloud Manager**  
Save your subscription and associate the Marketplace subscription with your AWS credentials.

**Continue** **Cancel**

b. 返回Cloud Manager之後、請在前往「充電方法」頁面時、選取容量型套件。

### Select Charging Method

|  |             |   |
|--|-------------|---|
| <input checked="" type="radio"/> Professional  | By capacity | ▼ |
| <input type="radio"/> Essential                | By capacity | ▼ |
| <input type="radio"/> Freemium (Up to 500 GiB) | By capacity | ▼ |
| <input type="radio"/> Per Node                 | By node     | ▼ |

"請參閱逐步指示、以在Cloud Volumes ONTAP AWS中啟動功能"。

### Keystone Flex 訂閱

Keystone Flex訂閱是一種隨需付費的訂閱型服務。"深入瞭解Keystone Flex訂閱"。

## 步驟

1. 如果您尚未訂閱、"請聯絡NetApp"
2. <mailto:ng-keystone-success@netapp.com> [聯絡NetApp]、以一或多個Keystone Flex訂閱授權您的Cloud Manager使用者帳戶。
3. NetApp授權您的帳戶之後、"連結您的訂閱內容以供Cloud Volumes ONTAP 搭配使用"。
4. 在「畫版」頁面上、按一下「新增工作環境」、然後依照Cloud Manager中的步驟進行。
  - a. 當系統提示您選擇充電方法時、請選取Keystone Flex訂閱充電方法。

Select Charging Method

☒ **Keystone** By capacity ^

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1 v

☐ Professional By capacity v

☐ Essential By capacity v

☐ Freemium (Up to 500 GiB) By capacity v

☐ Per Node By node v

"請參閱逐步指示、以在Cloud Volumes ONTAP AWS中啟動功能"。

## 在 Cloud Volumes ONTAP AWS 中啟動

您可以 Cloud Volumes ONTAP 在單一系統組態中或 AWS 中以 HA 配對的形式啟動功能。

### 開始之前

您需要下列項目才能建立工作環境。

- 已啟動並執行的連接器。
  - 您應該擁有 "與工作區相關的連接器"。
  - "您應該隨時準備好讓 Connector 保持運作"。

- 瞭解您要使用的組態。

您應該已做好準備、選擇組態、並從系統管理員取得 AWS 網路資訊。如需詳細資訊、請參閱 ["規劃 Cloud Volumes ONTAP 您的需求組態"](#)。

- 瞭解設定 Cloud Volumes ONTAP 驗證功能所需的條件。

["瞭解如何設定授權"](#)。

- 適用於 CIFS 組態的 DNS 與 Active Directory。

如需詳細資訊、請參閱 ["AWS 的網路需求 Cloud Volumes ONTAP"](#)。

## 在 Cloud Volumes ONTAP AWS 中啟動單一節點的效能不整系統

如果您想 Cloud Volumes ONTAP 要在 AWS 中啟動功能、您需要在 Cloud Manager 中建立新的工作環境。

建立工作環境之後、Cloud Manager 會立即在指定的 VPC 中啟動測試執行個體、以驗證連線能力。如果成功、Cloud Manager 會立即終止執行個體、然後開始部署 Cloud Volumes ONTAP 該系統。如果 Cloud Manager 無法驗證連線能力、則無法建立工作環境。測試執行個體為 T2.奈 米（預設 VPC 租賃）或 m3.medium（專屬 VPC 租賃）。

### 步驟

1. [[訂閱]在「畫版」頁面上、按一下「新增工作環境」、然後依照提示進行。
2. \* 選擇位置 \*：選擇 \* Amazon Web Services\* 和 \* Cloud Volumes ONTAP 《單一節點 \*》。
3. 如果出現提示、["建立連接器"](#)。
4. \* 詳細資料與認證 \*：選擇性地變更 AWS 認證資料與訂閱、輸入工作環境名稱、視需要新增標記、然後輸入密碼。

本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

| 欄位       | 說明   |
|----------|--|
| 工作環境名稱   | Cloud Manager 會使用工作環境名稱來命名 Cloud Volumes ONTAP 支援系統和 Amazon EC2 執行個體。如果您選取該選項、它也會使用名稱做為預先定義安全性群組的前置詞。  |
| 新增標記     | AWS 標籤是 AWS 資源的中繼資料。Cloud Manager 會將標記新增至 Cloud Volumes ONTAP 該執行個體、以及與該執行個體相關聯的每個 AWS 資源。建立工作環境時、您最多可以從使用者介面新增四個標記、然後在建立之後新增更多標記。請注意、在建立工作環境時、API 不會限制您使用四個標記。如需標記的相關資訊、請參閱 <a href="#">"AWS 文件：標記 Amazon EC2 資源"</a> 。 |
| 使用者名稱和密碼 | 這些是 Cloud Volumes ONTAP 適用於整個叢集管理員帳戶的認證資料。您可以使用這些認證資料、Cloud Volumes ONTAP 透過 System Manager 或其 CLI 連線至功能驗證。保留預設的 _admin_ 使用者名稱、或將其變更為自訂使用者名稱。  |



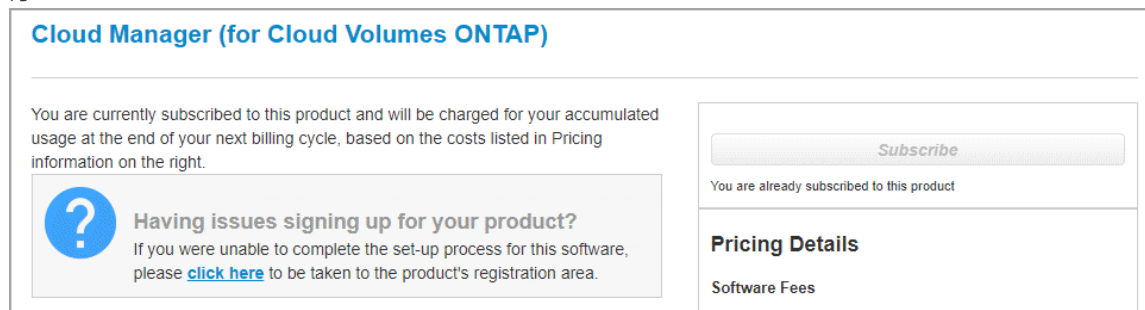
| 欄位     | 說明   |
|--------|--|
| 編輯認證資料 | 選擇與您要部署此系統之帳戶相關的AWS認證資料。您也可以將AWS Marketplace訂閱與此Cloud Volumes ONTAP 款作業系統建立關聯。按一下*新增訂閱*、將所選認證資料與新的AWS Marketplace訂閱建立關聯。訂閱可以是一年一度的合約、或Cloud Volumes ONTAP 是以每小時的費率支付。https://docs.netapp.com/us-en/cloud-manager-setup-admin/task-adding-aws-accounts.html["瞭解如何將額外的 AWS 認證資料新增至 Cloud Manager"^]。 |

下列影片說明如何將隨用隨付服務市場訂閱與 AWS 認證資料建立關聯：

► [https://docs.netapp.com/zh-tw/cloud-manager-cloud-volumes-ontap//media/video\\_subscribing\\_aws.mp4](https://docs.netapp.com/zh-tw/cloud-manager-cloud-volumes-ontap//media/video_subscribing_aws.mp4)

(video)

如果多位 IAM 使用者使用相同的 AWS 帳戶、則每位使用者都需要訂閱。第一位使用者訂閱之後、AWS Marketplace 會通知後續使用者他們已經訂閱、如下圖所示。雖然 AWS account 已有訂閱、但每個 IAM 使用者都需要將自己與該訂閱建立關聯。如果您看到以下訊息、請按一下 \* 按一下此處 \* 連結、前往 Cloud Central 並完成程序。



5. \* 服務 \* : 啟用或停用 Cloud Volumes ONTAP 您不想搭配使用的個別服務。

- "深入瞭解Cloud Data Sense"。
- "深入瞭解Cloud Backup"。
- "深入瞭解監控"。

6. 位置與連線：輸入您在中記錄的網路資訊 "AWS工作表"。

如果您有 AWS Outpost、Cloud Volumes ONTAP 您可以選擇 Outpost VPC、在該 Outpost 中部署單一節點的一套系統。體驗與 AWS 中的任何其他 VPC 相同。

下圖顯示已填寫的頁面：

| Location   | Connectivity   |
|--|--|
| <div>AWS Region</div> <div>US West   Oregon</div>        | <div>Security Group</div> <div><input checked="" type="radio"/> Generated security group <input type="radio"/> Use existing security group</div> |
| <div>VPC</div> <div>vpc-3a01e05f - 172.31.0.0/16</div>   | <div>SSH Authentication Method</div> <div><input checked="" type="radio"/> Password <input type="radio"/> Key Pair</div>                         |
| <div>Subnet</div> <div>172.31.5.0/24 (OCCM subnet)</div> |  |

7. \* 資料加密 \* : 不選擇資料加密或 AWS 管理的加密。

對於 AWS 管理的加密、您可以從帳戶或其他 AWS 帳戶中選擇不同的客戶主金鑰（CMK）。



建立 Cloud Volumes ONTAP 一套系統後、您無法變更 AWS 資料加密方法。

"瞭解如何設定 AWS KMS for Cloud Volumes ONTAP the 功能"。

"深入瞭解支援的加密技術"。

8. 充電方法與**NSS**帳戶：指定您要搭配此系統使用的收費選項、然後指定NetApp支援網站帳戶。
  - ["深入瞭解Cloud Volumes ONTAP 解適用於此功能的授權選項"](#)。
  - ["瞭解如何設定授權"](#)。
9. 《》（僅限AWS Marketplace年度合約）：請檢閱預設組態、然後按一下\*「Continue」（繼續）或按一下「Change Configuration」（變更組態）\*以選取您自己的組態。Cloud Volumes ONTAP

如果您保留預設組態、則只需指定一個Volume、然後檢閱並核准組態。

10. 預先設定的套件：選取其中一個套件以快速啟動Cloud Volumes ONTAP 功能、或按一下\*變更組態\*以選取您自己的組態。

如果您選擇其中一個套件、則只需指定一個Volume、然後檢閱並核准組態。

11. \* IAM角色\*：最好保留預設選項、讓Cloud Manager為您建立角色。

如果您偏好使用自己的原則、就必須符合 ["有關節點的原則要求 Cloud Volumes ONTAP"](#)。

12. 授權：視Cloud Volumes ONTAP 需要變更此版本、並選取執行個體類型和執行個體租賃。



如果所選版本有較新的發行候選版本、一般可用度或修補程式版本、Cloud Manager 會在建立工作環境時、將系統更新至該版本。例如、如果您選擇Cloud Volumes ONTAP 了「更新」功能、就會進行更新。更新不會從一個版本發生到另一個版本、例如從 9.6 到 9.7。

13. \* 基礎儲存資源\*：選擇初始 Aggregate 的設定：磁碟類型、每個磁碟的大小、以及是否應啟用資料分層。

請注意下列事項：

- 磁碟類型適用於初始磁碟區。您可以為後續磁碟區選擇不同的磁碟類型。
- 磁碟大小適用於初始 Aggregate 中的所有磁碟、以及 Cloud Manager 在使用簡易資源配置選項時所建立的任何其他集合體。您可以使用進階配置選項、建立使用不同磁碟大小的集合體。

如需選擇磁碟類型和大小的說明、請參閱 ["在 AWS 中調整系統規模"](#)。

- 您可以在建立或編輯磁碟區時、選擇特定的磁碟區分層原則。
- 如果停用資料分層、您可以在後續的 Aggregate 上啟用。

["瞭解資料分層的運作方式"](#)。

14. \* 寫入速度與 WORM\*：選擇 \* 正常 \* 或 \* 高速 \* 寫入速度、並視需要啟動一次寫入、多次讀取（WORM）儲存設備。

["深入瞭解寫入速度"](#)。

如果啟用雲端備份或啟用資料分層、則無法啟用WORM。

["深入瞭解 WORM 儲存設備"](#)。

15. \* 建立 Volume\*：輸入新磁碟區的詳細資料、或按一下 \* 跳過 \*。

["瞭解支援的用戶端傳輸協定和版本"](#)。

本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

| 欄位                     | 說明  |
|------------------------|---|
| 尺寸                     | 您可以輸入的最大大小、主要取決於您是否啟用精簡配置、這可讓您建立比目前可用實體儲存容量更大的磁碟區。  |
| 存取控制（僅適用於 NFS）         | 匯出原則會定義子網路中可存取磁碟區的用戶端。根據預設、Cloud Manager 會輸入一個值、讓您存取子網路中的所有執行個體。  |
| 權限與使用者 / 群組（僅限 CIFS）   | 這些欄位可讓您控制使用者和群組（也稱為存取控制清單或 ACL）的共用存取層級。您可以指定本機或網域 Windows 使用者或群組、或 UNIX 使用者或群組。如果您指定網域 Windows 使用者名稱、則必須使用網域\使用者名稱格式來包含使用者的網域。  |
| Snapshot 原則            | Snapshot 複製原則會指定自動建立的 NetApp Snapshot 複本的頻率和數量。NetApp Snapshot 複本是一種不影響效能的時間點檔案系統映像、需要最少的儲存容量。您可以選擇預設原則或無。您可以針對暫時性資料選擇「無」：例如、Microsoft SQL Server 的 Tempdb。   |
| 進階選項（僅適用於 NFS）         | 為磁碟區選取 NFS 版本：NFSv3 或 NFSv3。  |
| 啟動器群組和 IQN（僅適用於 iSCSI） | iSCSI 儲存目標稱為 LUN（邏輯單元）、以標準區塊裝置的形式呈現給主機。啟動器群組是 iSCSI 主機節點名稱的表格、可控制哪些啟動器可存取哪些 LUN。iSCSI 目標可透過標準乙太網路介面卡（NIC）、TCP 卸載引擎（TOE）卡（含軟體啟動器）、整合式網路介面卡（CNA）或專用主機匯流排介面卡（HBA）連線至網路、並由 iSCSI 合格名稱（IQN）識別。建立 iSCSI Volume 時、Cloud Manager 會自動為您建立 LUN。我們只要在每個磁碟區建立一個 LUN、就能輕鬆完成工作、因此不需要管理。建立磁碟區之後、 <a href="#">"使用 IQN 從主機連線至 LUN"</a> 。 |

下圖顯示 CIFS 傳輸協定的「Volume」（磁碟區）頁面：

### Volume Details, Protection & Protocol

#### Details & Protection

Volume Name:

Size (GB):

Snapshot Policy:

Default Policy

#### Protocol

NFS **CIFS** iSCSI

Share name:

Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

16. \* CIFS 設定 \*：如果您選擇 CIFS 傳輸協定、請設定 CIFS 伺服器。

| 欄位                       | 說明   |
|--------------------------|--|
| DNS 主要和次要 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」。如果您將 AWS 託管 Microsoft AD 設定為 AD 伺服器 Cloud Volumes ONTAP 以供使用、您應該在此欄位中輸入 * OID=computers,O=corp*。   |
| DNS 網域                   | 適用於整個儲存虛擬 Cloud Volumes ONTAP 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                  | 選擇 * 使用 Active Directory 網域 * 來使用 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。請注意、您只能在建立 CIFS 伺服器時設定 NTP 伺服器。您建立 CIFS 伺服器之後、就無法進行設定。 |

17. \* 使用率設定檔、磁碟類型及分層原則 \*：視需要選擇是否要啟用儲存效率功能、並編輯磁碟區分層原則。

如需詳細資訊、請參閱 ["瞭解 Volume 使用量設定檔"](#) 和 ["資料分層總覽"](#)。

18. \* 審查與核准 \*：檢閱並確認您的選擇。

- 檢閱組態的詳細資料。
- 按一下 \* 更多資訊 \* 以檢閱 Cloud Manager 將購買的支援與 AWS 資源詳細資料。
- 選取「\* 我瞭解 ... \*」核取方塊。
- 按一下「\* 執行 \*」。

Cloud Manager 會啟動 Cloud Volumes ONTAP 此功能。您可以追蹤時間表的進度。

如果您在啟動 Cloud Volumes ONTAP 該實例時遇到任何問題、請檢閱故障訊息。您也可以選取工作環境、然後按一下重新建立環境。

如需其他協助、請前往 ["NetApp Cloud Volumes ONTAP 支援"](#)。

完成後

- 如果您已配置 CIFS 共用區、請授予使用者或群組檔案和資料夾的權限、並確認這些使用者可以存取共用區並建立檔案。
- 如果您要將配額套用至磁碟區、請使用 System Manager 或 CLI。

配額可讓您限制或追蹤使用者、群組或 qtree 所使用的磁碟空間和檔案數量。

## 在 Cloud Volumes ONTAP AWS 中啟動一個「叢集 HA 配對」

如果您想要在 Cloud Volumes ONTAP AWS 中啟動一個「叢集 HA 配對」、就必須在 Cloud Manager 中建立 HA 工作環境。

目前 AWS out貼 文不支援 HA 配對。

建立工作環境之後、Cloud Manager 會立即在指定的 VPC 中啟動測試執行個體、以驗證連線能力。如果成功、Cloud Manager 會立即終止執行個體、然後開始部署 Cloud Volumes ONTAP 該系統。如果 Cloud Manager 無法驗證連線能力、則無法建立工作環境。測試執行個體為 T2.奈 米（預設 VPC 租賃）或 m3.medium（專屬 VPC 租賃）。

### 步驟

1. 在「畫版」頁面上、按一下「\* 新增工作環境 \*」、然後依照提示進行。
2. \* 選擇位置 \*：選擇 \* Amazon Web Services\* 和 \* Cloud Volumes ONTAP 《單一節點 \*》。
3. \* 詳細資料與認證 \*：選擇性地變更 AWS 認證資料與訂閱、輸入工作環境名稱、視需要新增標記、然後輸入密碼。

本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

| 欄位       | 說明   |
|----------|--|
| 工作環境名稱   | Cloud Manager 會使用工作環境名稱來命名 Cloud Volumes ONTAP 支援系統和 Amazon EC2 執行個體。如果您選取該選項、它也會使用名稱做為預先定義安全性群組的前置詞。  |
| 新增標記     | AWS 標籤是 AWS 資源的中繼資料。Cloud Manager 會將標記新增至 Cloud Volumes ONTAP 該執行個體、以及與該執行個體相關聯的每個 AWS 資源。建立工作環境時、您最多可以從使用者介面新增四個標記、然後在建立之後新增更多標記。請注意、在建立工作環境時、API 不會限制您使用四個標記。如需標記的相關資訊、請參閱 " <a href="#">AWS 文件：標記 Amazon EC2 資源</a> "。  |
| 使用者名稱和密碼 | 這些是 Cloud Volumes ONTAP 適用於整個叢集管理員帳戶的認證資料。您可以使用這些認證資料、Cloud Volumes ONTAP 透過 System Manager 或其 CLI 連線至功能驗證。保留預設的 _admin_ 使用者名稱、或將其變更為自訂使用者名稱。  |
| 編輯認證資料   | 選擇 AWS 認證資料和市場訂閱、以搭配此 Cloud Volumes ONTAP 款功能系統使用。按一下*新增訂閱*、將所選認證資料與新的 AWS Marketplace 訂閱建立關聯。訂閱可以是一年一度的合約、或 Cloud Volumes ONTAP 是以每小時的費率支付。如果直接向 NetApp（BYOL）購買授權、則無需訂閱 AWS。<br>◦ <a href="https://docs.netapp.com/us-en/cloud-manager-setup-admin/task-adding-aws-accounts.html">https://docs.netapp.com/us-en/cloud-manager-setup-admin/task-adding-aws-accounts.html</a> ["瞭解如何將額外的 AWS 認證資料新增至 Cloud Manager"]。 |

下列影片說明如何將隨用隨付服務市場訂閱與 AWS 認證資料建立關聯：

► [https://docs.netapp.com/zh-tw/cloud-manager-cloud-volumes-ontap/media/video\\_subscribing\\_aws.mp4](https://docs.netapp.com/zh-tw/cloud-manager-cloud-volumes-ontap/media/video_subscribing_aws.mp4)



(video)

如果多位 IAM 使用者使用相同的 AWS 帳戶、則每位使用者都需要訂閱。第一位使用者訂閱之後、AWS Marketplace 會通知後續使用者他們已經訂閱、如下圖所示。雖然 AWS account 已有訂閱、但每個 IAM 使用者都需要將自己與該訂閱建立關聯。如果您看到以下訊息、請按一下 \* 按一下此處 \* 連結、前往 Cloud Central 並完成程序。



### Cloud Manager (for Cloud Volumes ONTAP)

You are currently subscribed to this product and will be charged for your accumulated usage at the end of your next billing cycle, based on the costs listed in Pricing information on the right.



#### Having issues signing up for your product?

If you were unable to complete the set-up process for this software, please [click here](#) to be taken to the product's registration area.

Subscribe

You are already subscribed to this product

#### Pricing Details

Software Fees

4. \* 服務 \* : 讓服務保持啟用或停用您不想搭配 Cloud Volumes ONTAP 此作業系統使用的個別服務。

- "深入瞭解Cloud Data Sense"。
- "深入瞭解Cloud Backup"。
- "深入瞭解監控"。

5. \* HA 部署模式 \* : 選擇 HA 組態。

如需部署模型的總覽、請參閱 "適用於 AWS 的 HA Cloud Volumes ONTAP"。

6. \* 地區與 VPC\* : 輸入您在 AWS 工作表中記錄的網路資訊。

下圖顯示為多個 AZ 組態填寫的頁面：

### Region & VPC

AWS Region

US East | N. Virginia

VPC

vpc-a76d91c2 - 172.31.0.0/16

Security group

Use a generated security group

Node 1:

Availability Zone

us-east-1a

Subnet

172.31.8.0/24

Node 2:

Availability Zone

us-east-1b

Subnet

172.31.9.0/24

Mediator:

Availability Zone

us-east-1c

Subnet

172.31.2.0/24

7. \* 連線能力與 SSH 驗證 \* : 選擇 HA 配對與中介器的連線方法。

8. \* 浮動 IP \* : 如果您選擇多個 AZs 、請指定浮動 IP 位址。

該地區所有 VPC 的 IP 位址必須位於 CIDR 區塊之外。如需其他詳細資料、請參閱 ["AWS 在 Cloud Volumes ONTAP 多個 AZs 中的功能需求"](#)。

9. \* 路由表 \* : 如果您選擇多個 AZs 、請選取應包含浮動 IP 位址路由的路由表。

如果您有多個路由表、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 此功能配對。如需路由表的詳細資訊、請參閱 ["AWS 文件：路由表"](#)。

10. \* 資料加密 \* : 不選擇資料加密或 AWS 管理的加密。

對於 AWS 管理的加密、您可以從帳戶或其他 AWS 帳戶中選擇不同的客戶主金鑰（CMK）。



建立 Cloud Volumes ONTAP 一套系統後、您無法變更 AWS 資料加密方法。

["瞭解如何設定 AWS KMS for Cloud Volumes ONTAP the 功能"](#)。

["深入瞭解支援的加密技術"](#)。

11. 充電方法與NSS帳戶：指定您要搭配此系統使用的收費選項、然後指定NetApp支援網站帳戶。

- ["深入瞭解Cloud Volumes ONTAP 解適用於此功能的授權選項"](#)。

- ["瞭解如何設定授權"](#)。

12. 《》（僅限AWS Marketplace年度合約）：請檢閱預設組態、然後按一下\*「Continue」（繼續）或按一下「Change Configuration」（變更組態）\*以選取您自己的組態。Cloud Volumes ONTAP

如果您保留預設組態、則只需指定一個Volume、然後檢閱並核准組態。

13. 預先設定的套件（僅限每小時或BYOL）：選取其中一個套件以快速啟動Cloud Volumes ONTAP 功能、或按一下\*變更組態\*以選取您自己的組態。

如果您選擇其中一個套件、則只需指定一個Volume、然後檢閱並核准組態。

14. \* IAM角色\*：最好保留預設選項、讓Cloud Manager為您建立角色。

如果您偏好使用自己的原則、就必須符合 ["有關節點和 HA 中介器的原則要求 Cloud Volumes ONTAP"](#)。

15. 授權：視Cloud Volumes ONTAP 需要變更此版本、並選取執行個體類型和執行個體租賃。



如果所選版本有較新的發行候選版本、一般可用度或修補程式版本、Cloud Manager 會在建立工作環境時、將系統更新至該版本。例如、如果您選擇Cloud Volumes ONTAP 了「更新」功能、就會進行更新。更新不會從一個版本發生到另一個版本、例如從 9.6 到 9.7。

16. \* 基礎儲存資源 \* : 選擇初始 Aggregate 的設定：磁碟類型、每個磁碟的大小、以及是否應啟用資料分層。

請注意下列事項：

- 磁碟類型適用於初始磁碟區。您可以為後續磁碟區選擇不同的磁碟類型。



- 磁碟大小適用於初始 Aggregate 中的所有磁碟、以及 Cloud Manager 在使用簡易資源配置選項時所建立的任何其他集合體。您可以使用進階配置選項、建立使用不同磁碟大小的集合體。

如需選擇磁碟類型和大小的說明、請參閱 ["在 AWS 中調整系統規模"](#)。

- 您可以在建立或編輯磁碟區時、選擇特定的磁碟區分層原則。
- 如果停用資料分層、您可以在後續的 Aggregate 上啟用。

["瞭解資料分層的運作方式"](#)。

17. \* 寫入速度與 WORM \* : 選擇 \* 正常 \* 或 \* 高速 \* 寫入速度、並視需要啟動一次寫入、多次讀取 (WORM) 儲存設備。

["深入瞭解寫入速度"](#)。

如果啟用雲端備份或啟用資料分層、則無法啟用 WORM。

["深入瞭解 WORM 儲存設備"](#)。

18. \* 建立 Volume \* : 輸入新磁碟區的詳細資料、或按一下 \* 跳過 \* 。

["瞭解支援的用戶端傳輸協定和版本"](#)。

本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

| 欄位                      | 說明   |
|-------------------------|--|
| 尺寸                      | 您可以輸入的最大大小、主要取決於您是否啟用精簡配置、這可讓您建立比目前可用實體儲存容量更大的磁碟區。   |
| 存取控制 (僅適用於 NFS)         | 匯出原則會定義子網路中可存取磁碟區的用戶端。根據預設、Cloud Manager 會輸入一個值、讓您存取子網路中的所有執行個體。   |
| 權限與使用者 / 群組 (僅限 CIFS)   | 這些欄位可讓您控制使用者和群組 (也稱為存取控制清單或 ACL) 的共用存取層級。您可以指定本機或網域 Windows 使用者或群組、或 UNIX 使用者或群組。如果您指定網域 Windows 使用者名稱、則必須使用網域 \ 使用者名稱格式來包含使用者的網域。   |
| Snapshot 原則             | Snapshot 複製原則會指定自動建立的 NetApp Snapshot 複本的頻率和數量。NetApp Snapshot 複本是一種不影響效能的時間點檔案系統映像、需要最少的儲存容量。您可以選擇預設原則或無。您可以針對暫時性資料選擇「無」：例如、Microsoft SQL Server 的 Tempdb。  |
| 進階選項 (僅適用於 NFS)         | 為磁碟區選取 NFS 版本：NFSv3 或 NFSv3。   |
| 啟動器群組和 IQN (僅適用於 iSCSI) | iSCSI 儲存目標稱為 LUN (邏輯單元)、以標準區塊裝置的形式呈現給主機。啟動器群組是 iSCSI 主機節點名稱的表格、可控制哪些啟動器可存取哪些 LUN。iSCSI 目標可透過標準以太網路介面卡 (NIC)、TCP 卸載引擎 (TOE) 卡 (含軟體啟動器)、整合式網路介面卡 (CNA) 或專用主機匯流排介面卡 (HBA) 連線至網路、並由 iSCSI 合格名稱 (IQN) 識別。建立 iSCSI Volume 時、Cloud Manager 會自動為您建立 LUN。我們只要在每個磁碟區建立一個 LUN、就能輕鬆完成工作、因此不需要管理。建立磁碟區之後、 <a href="#">"使用 IQN 從主機連線至 LUN"</a> 。 |

下圖顯示 CIFS 傳輸協定的「Volume」（磁碟區）頁面：

Volume Details, Protection & Protocol

Details & Protection

Volume Name:

vol

Size (GB):

250

Snapshot Policy:

default

Default Policy

Protocol

NFS

CIFS

ISCSI

Share name:

vol\_share

Permissions:

Full Control

Users / Groups:

engineering

Valid users and groups separated by a semicolon

19. \* CIFS 設定 \*：如果您選取 CIFS 傳輸協定、請設定 CIFS 伺服器。

| 欄位                       | 說明   |
|--------------------------|--|
| DNS 主要和次要 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」。如果您將 AWS 託管 Microsoft AD 設定為 AD 伺服器 Cloud Volumes ONTAP 以供使用、您應該在此欄位中輸入 * OID=computers,O=corp*。   |
| DNS 網域                   | 適用於整個儲存虛擬 Cloud Volumes ONTAP 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                  | 選擇 * 使用 Active Directory 網域 * 來使用 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。請注意、您只能在建立 CIFS 伺服器時設定 NTP 伺服器。您建立 CIFS 伺服器之後、就無法進行設定。 |

20. \* 使用率設定檔、磁碟類型及分層原則 \*：視需要選擇是否要啟用儲存效率功能、並編輯磁碟區分層原則。

如需詳細資訊、請參閱 ["瞭解 Volume 使用量設定檔"](#) 和 ["資料分層總覽"](#)。

21. \* 審查與核准 \*：檢閱並確認您的選擇。

- 檢閱組態的詳細資料。
- 按一下 \* 更多資訊 \* 以檢閱 Cloud Manager 將購買的支援與 AWS 資源詳細資料。

c. 選取「\* 我瞭解 ... \*」核取方塊。

d. 按一下「\* 執行 \*」。

Cloud Manager 會啟動 Cloud Volumes ONTAP「叢集式 HA 配對」。您可以追蹤時間表的進度。

如果您在啟動 HA 配對時遇到任何問題、請檢閱故障訊息。您也可以選取工作環境、然後按一下重新建立環境。

如需其他協助、請前往 "[NetApp Cloud Volumes ONTAP 支援](#)"。

完成後

- 如果您已配置 CIFS 共用區、請授予使用者或群組檔案和資料夾的權限、並確認這些使用者可以存取共用區並建立檔案。
- 如果您要將配額套用至磁碟區、請使用 System Manager 或 CLI。

配額可讓您限制或追蹤使用者、群組或 qtree 所使用的磁碟空間和檔案數量。

## 開始使用Cloud Volumes ONTAP AWS C2S環境中的功能

與標準AWS區域類似、您可以在中使用Cloud Manager "[AWS商業雲端服務 \(C2S\)](#)" 部署Cloud Volumes ONTAP 的環境、為您的雲端儲存設備提供企業級功能。AWS C2S是美國專屬的封閉區域智慧社群；本頁的說明僅適用於AWS C2S區域使用者。

### C2S支援的功能

Cloud Manager在C2S環境中提供下列功能：

- Cloud Volumes ONTAP
- 資料複寫
- 稽核時間表

對於這個功能、您可以建立單一節點系統或HA配對。Cloud Volumes ONTAP這兩種授權選項皆可使用：隨用隨付及自帶授權（BYOL）。

在C2S中、也支援Cloud Volumes ONTAP 將資料分層至S3的功能。

限制

- Cloud Manager不提供任何NetApp的雲端服務。
- 由於在C2S環境中無法存取網際網路、因此下列功能也無法使用：
  - 與NetApp Cloud Central整合
  - 從Cloud Manager自動升級軟體
  - NetApp AutoSupport
  - AWS Cloud Volumes ONTAP 有關資源的成本資訊
- C2S環境不支援Freemium授權。

## 部署總覽

在C2S中開始使用功能包括幾個步驟。Cloud Volumes ONTAP

### 1. 準備AWS環境。

這包括設定網路、訂閱Cloud Volumes ONTAP 功能、設定權限、以及選擇性設定AWS KMS。

### 2. 安裝Connector並設定Cloud Manager。

在開始使用Cloud Manager部署Cloud Volumes ONTAP 功能時、您必須先建立\_Connector\_。Connector可讓Cloud Manager管理公有雲環境中的資源和程序（包括Cloud Volumes ONTAP

您將從安裝在Connector執行個體上的軟體登入Cloud Manager。

### 3. 從Cloud Volumes ONTAP Cloud Manager啟動

以下說明每個步驟。

## 準備AWS環境

您的AWS環境必須滿足幾項需求。

設定您的網路

設定AWS網路、Cloud Volumes ONTAP 使其能夠正常運作。

## 步驟

1. 選擇要在其中啟動Connector執行個體和Cloud Volumes ONTAP 例項的VPC和子網路。
2. 確保您的 VPC 和子網路支援連接器與 Cloud Volumes ONTAP 支援之間的連線。
3. 設定 S3 服務的 VPC 端點。

如果您想要將冷資料從 Cloud Volumes ONTAP 不願儲存到低成本物件儲存設備、則需要 VPC 端點。

訂閱**Cloud Volumes ONTAP** 此功能

需要訂閱Marketplace才能從Cloud Volumes ONTAP Cloud Manager部署功能。

## 步驟

1. 前往AWS Intelligence Community Marketplace搜尋Cloud Volumes ONTAP 功能。
2. 選取您要部署的產品項目。
3. 檢閱條款、然後按一下\*接受\*。
4. 如果您打算部署其他產品、請針對這些產品重複上述步驟。

您必須使用Cloud Manager來啟動Cloud Volumes ONTAP 執行個體。您不得Cloud Volumes ONTAP 從EC2 主控台啟動支援的執行個體。

## 設定權限

設定IAM原則和角色、為Cloud Manager和Cloud Volumes ONTAP 功能提供他們在AWS商業雲端服務環境中執行行動所需的權限。

您需要IAM原則和IAM角色來執行下列各項：

- Connector執行個體
- 執行個體Cloud Volumes ONTAP
- 不只是執行個體（如果您想部署HA配對）Cloud Volumes ONTAP

## 步驟

1. 移至AWS IAM主控台、然後按一下\* Policies \*。
2. 建立Connector執行個體的原則。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceStatus",
      "ec2:RunInstances",
      "ec2:ModifyInstanceAttribute",
      "ec2:DescribeRouteTables",
      "ec2:DescribeImages",
      "ec2:CreateTags",
      "ec2:CreateVolume",
      "ec2:DescribeVolumes",
      "ec2:ModifyVolumeAttribute",
      "ec2>DeleteVolume",
      "ec2:CreateSecurityGroup",
      "ec2>DeleteSecurityGroup",
      "ec2:DescribeSecurityGroups",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:CreateNetworkInterface",
      "ec2:DescribeNetworkInterfaces",
      "ec2>DeleteNetworkInterface",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeDhcpOptions",
      "ec2:CreateSnapshot",
```

```

        "ec2:DeleteSnapshot",
        "ec2:DescribeSnapshots",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "iam:PassRole",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:ListInstanceProfiles",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "kms:List*",
        "kms:Describe*",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2>DeletePlacementGroup"
    ],
    "Resource": "*"
},
{
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",

```

```

        "s3:ListBucketVersions"
    ],
    "Resource": [
        "arn:aws-iso:s3:::fabric-pool*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/WorkingEnvironment": "*"
        }
    },
    "Resource": [
        "arn:aws-iso:ec2:*:*:instance/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Resource": [
        "arn:aws-iso:ec2:*:*:volume/*"
    ]
}
]
}

```

3. 建立Cloud Volumes ONTAP 一套適用於此功能的原則。

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws-iso:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws-iso:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3>DeleteObject"
    ],
    "Resource": "arn:aws-iso:s3:::fabric-pool-*",
    "Effect": "Allow"
  }]
}

```

4. 如果您計畫部署Cloud Volumes ONTAP 一個「叢集HA配對」、請為HA中介者建立原則。

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:AssignPrivateIpAddresses",
      "ec2:CreateRoute",
      "ec2>DeleteRoute",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeRouteTables",
      "ec2:DescribeVpcs",
      "ec2:ReplaceRoute",
      "ec2:UnassignPrivateIpAddresses"
    ],
    "Resource": "*"
  }]
}

```



## 5. 使用角色類型Amazon EC2建立IAM角色、並附加您在先前步驟中建立的原則。

與原則類似、您應該有一個IAM角色用於連接器、一個用於Cloud Volumes ONTAP 鏈結節點、另一個用於HA中介器（如果您要部署HA配對）。

啟動Connector執行個體時、您必須選取Connector IAM角色。

從Cloud Manager建立一套可運作的環境時、您可以選擇IAM角色做Cloud Volumes ONTAP 為功能性的部分、以及HA中介器Cloud Volumes ONTAP 。

### 設定 AWS KMS

如果您想搭配Cloud Volumes ONTAP 使用Amazon加密搭配使用、請確保AWS金鑰管理服務符合要求。

#### 步驟

1. 請確定您的帳戶或其他AWS帳戶中存在使用中的客戶主金鑰（CMK）。

CMK 可以是 AWS 託管的 CMK 、也可以是客戶託管的 CMK 。

2. 如果CMK位於AWS帳戶中、而該帳戶與您打算部署Cloud Volumes ONTAP 的帳戶不同、則您需要取得該金鑰的ARN。

建立Cloud Volumes ONTAP 一套系統時、您必須提供ARN給Cloud Manager 。

3. 將Cloud Manager執行個體的IAM角色新增至CMK的主要使用者清單。

這讓Cloud Manager有權將CMK搭配Cloud Volumes ONTAP 使用。

### 安裝及設定Cloud Manager

您Cloud Volumes ONTAP 必須先從AWS Marketplace啟動Connector執行個體、然後登入並設定Cloud Manager、才能在AWS中啟動此類系統。

#### 步驟

1. 取得由憑證授權單位（CA）簽署的根憑證（採用隱私權增強型郵件（PEF）Base - 64編碼的X . 509格式）。請參閱貴組織的原則與程序、以取得該憑證。

您必須在設定程序期間上傳憑證。Cloud Manager透過HTTPS將要求傳送至AWS時、會使用信任的憑證。

2. 啟動Connector執行個體：

- a. 前往適用於Cloud Manager的AWS Intelligence Community Marketplace頁面。
- b. 在「自訂啟動」索引標籤上、選擇從EC2主控台啟動執行個體的選項。
- c. 依照提示設定執行個體。

設定執行個體時請注意下列事項：

- 建議使用T3.xLarge。
- 您必須選擇在準備AWS環境時所建立的IAM角色。

- 您應該保留預設的儲存選項。
  - Connector所需的連線方法如下：SSH、HTTP和HTTPS。
3. 從連線至Connector執行個體的主機設定Cloud Manager：
- a. 開啟網頁瀏覽器並輸入下列 URL：<http://ipaddress:80>
  - b. 指定用於連線至AWS服務的Proxy伺服器。
  - c. 上傳您在步驟1中取得的憑證。
  - d. 完成設定精靈中的步驟以設定Cloud Manager。
    - 系統詳細資料：輸入此Cloud Manager執行個體的名稱、並提供貴公司名稱。
    - 建立使用者：建立您將用來管理Cloud Manager的管理使用者。
    - 審查：檢閱詳細資料並核准終端使用者授權合約。
  - e. 若要完成CA簽署憑證的安裝、請從EC2主控台重新啟動Connector執行個體。
4. 重新啟動Connector之後、請使用您在設定精靈中建立的系統管理員使用者帳戶登入。

## 產品Cloud Volumes ONTAP 發表

您可以Cloud Volumes ONTAP 在Cloud Manager中建立新的工作環境、在AWS商業雲端服務環境中啟動執行個體。

您需要的是 **#8217**；需要的是什麼

- 如果您購買授權、則必須擁有從NetApp收到的授權檔案。授權檔案是Json格式的.NLF檔案。
- 需要金鑰配對、才能對HA中介器啟用金鑰型SSH驗證。

## 步驟

1. 在「工作環境」頁面上、按一下「新增工作環境」。
2. 在「Create（建立）」下、選取Cloud Volumes ONTAP 「HseHA」或Cloud Volumes ONTAP 「
3. 完成精靈中的步驟以啟動Cloud Volumes ONTAP 整套系統。

完成精靈時請注意下列事項：

- 如果您想要在Cloud Volumes ONTAP 多個可用度區域中部署SeseHA、請依照下列方式部署組態、因為在發佈時AWS商業雲端服務環境中只有兩個AZs可用：
    - 節點1：可用度區域A
    - 節點2：可用度區域B
    - 中介：可用度區域A或B
  - 您應該保留預設選項、以使用產生的安全性群組。
- 預先定義的安全性群組包含Cloud Volumes ONTAP 一些規則、這些規則是讓整個公司順利運作所需的。如果您需要使用自己的安全性、請參閱下方的安全性群組一節。
- 您必須選擇在準備AWS環境時所建立的IAM角色。
  - 基礎AWS磁碟類型適用於初始Cloud Volumes ONTAP 的流通量。

您可以為後續磁碟區選擇不同的磁碟類型。

- AWS磁碟的效能與磁碟大小有關。

您應該選擇能提供所需持續效能的磁碟大小。如需EBS效能的詳細資訊、請參閱AWS文件。

- 磁碟大小是系統上所有磁碟的預設大小。



如果您稍後需要不同的大小、可以使用「進階配置」選項來建立使用特定大小磁碟的集合體。

- 儲存效率功能可改善儲存使用率、並減少所需的儲存總容量。

Cloud Manager 會啟動 Cloud Volumes ONTAP 此功能。您可以追蹤時間表的進度。

### 安全性群組規則

Cloud Manager會建立安全群組、其中包括Cloud Manager和Cloud Volumes ONTAP NetApp在雲端成功運作所需的傳入和傳出規則。您可能想要參照連接埠進行測試、或是想要使用自己的安全性群組。

#### Connector的安全性群組

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 Web 瀏覽器到本機使用者介面的 HTTP 存取 |
| 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  |

#### 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 |

#### 安全性群組Cloud Volumes ONTAP

適用於不支援節點的安全群組Cloud Volumes ONTAP 需要傳入和傳出規則。

#### 傳入規則

預先定義之安全性群組中的傳入規則來源為 0.00.0.0/0 。

| 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、以 HTTPS 存取 System Manager 網路主控台  |
| 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 | 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

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 |

## HA中介器的外部安全群組

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

傳入規則的來源是來自連接器所在VPC的流量。

| 傳輸協定 | 連接埠  | 目的                            |
|------|------|-------------------------------|
| SSH  | 22   | SSH 連線至 HA 中介器                |
| TCP  | 3000 | 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 |

## HA中介器的內部安全群組

針對此功能、預先定義 Cloud Volumes ONTAP 的內部安全群組包含下列規則：Cloud Manager 一律會建立這個安全群組。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 |

## 開始使用Microsoft Azure

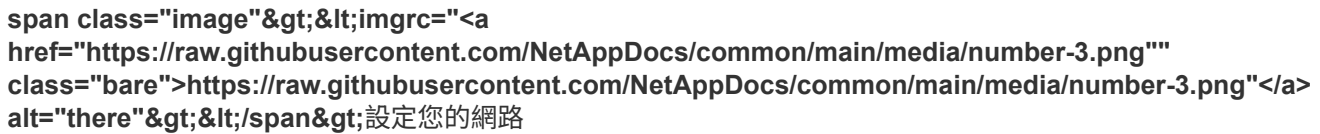
### Azure中的功能快速入門Cloud Volumes ONTAP

只要幾個步驟、Cloud Volumes ONTAP 就能開始使用適用於 Azure 的功能。

如果您沒有 ["連接器"](#) 然而、帳戶管理員需要建立一個帳戶。 ["瞭解如何在 Azure 中建立 Connector"](#)。

當您建立第一個 Cloud Volumes ONTAP 運作環境時、如果您還沒有連接器、Cloud Manager 會提示您部署連接器。

Cloud Manager 提供符合工作負載需求的預先設定套件、您也可以建立自己的組態。如果您選擇自己的組態、應該瞭解可用的選項。"深入瞭解"。

設定您的網路

1. 確保您的 Vnet 和子網路可支援連接器與 Cloud Volumes ONTAP 支援的連接功能。
2. 啟用從目標 vnet 的傳出網際網路存取、讓 Connector 和 Cloud Volumes ONTAP 支援中心能夠連絡多個端點。

這個步驟很重要、因為連接器 Cloud Volumes ONTAP 無法在沒有外傳網際網路存取的情況下管理不穩定。如果您需要限制傳出連線、請參閱的端點清單 "[Connector 與 Cloud Volumes ONTAP the](#)"。

"深入瞭解網路需求"。

按一下「\* 新增工作環境 \*」、選取您要部署的系統類型、然後完成精靈中的步驟。"閱讀逐步指示"。

相關連結

- "[從 Cloud Manager 建立 Connector](#)"
- "[從 Azure Marketplace 建立 Connector](#)"
- "[在 Linux 主機上安裝 Connector 軟體](#)"
- "[Cloud Manager 具備權限的功能](#)"

## 在Cloud Volumes ONTAP Azure中規劃您的不一樣組態

在 Cloud Volumes ONTAP Azure 中部署時、您可以選擇符合工作負載需求的預先設定系統、也可以自行建立組態。如果您選擇自己的組態、應該瞭解可用的選項。

選擇**Cloud Volumes ONTAP** 一個不含功能的授權

有多種授權選項可供Cloud Volumes ONTAP 選擇。每個選項都能讓您選擇符合需求的消費模式。

- "[深入瞭解Cloud Volumes ONTAP 解適用於此功能的授權選項](#)"
- "[瞭解如何設定授權](#)"

選擇支援的地區

大多數Microsoft Azure地區均支援此功能。Cloud Volumes ONTAP "[檢視支援區域的完整清單](#)"。

選擇支援的**VM**類型

根據您選擇的授權類型、支援多種 VM 類型。Cloud Volumes ONTAP

"[Azure支援Cloud Volumes ONTAP 的支援功能組態](#)"

## 瞭解儲存限制

一個不含資源的系統的原始容量上限 Cloud Volumes ONTAP 與授權有關。其他限制會影響集合體和磁碟區的大小。在規劃組態時、您應該注意這些限制。

### "Azure的Cloud Volumes ONTAP 儲存限制"

#### 在Azure中調整系統規模

調整 Cloud Volumes ONTAP 您的支援規模、有助於滿足效能與容量的需求。在選擇 VM 類型、磁碟類型和磁碟大小時、您應該注意幾個關鍵點：

#### 虛擬機器類型

請查看中支援的虛擬機器類型 ["發行說明 Cloud Volumes ONTAP"](#) 然後檢閱每種受支援 VM 類型的詳細資料。請注意、每種 VM 類型都支援特定數量的資料磁碟。

- ["Azure 文件：通用虛擬機器大小"](#)
- ["Azure 文件：記憶體最佳化的虛擬機器大小"](#)

#### Azure 磁碟類型

當您建立 Cloud Volumes ONTAP 用於實現效能不均的磁碟區時、您需要選擇 Cloud Volumes ONTAP 底層的雲端儲存設備、以利將其用作磁碟。

HA 系統使用優質網頁。同時、單一節點系統可使用兩種 Azure 託管磁碟：

- [\\_ Premium SSD 託管磁碟 \\_](#) 以更高的成本、為 I/O 密集的工作負載提供高效能。
- [\\_ 標準 SSD 託管磁碟 \\_](#) 為需要低 IOPS 的工作負載提供一致的效能。
- 如果您不需要高 IOPS、而且想要降低成本、那麼 [\\_ 標準 HDD 託管磁碟 \\_](#) 是個不錯的選擇。

如需這些磁碟使用案例的其他詳細資料、請參閱 ["Microsoft Azure 文件：Azure 提供哪些磁碟類型？"](#)。

#### Azure 磁碟大小

啟動 Cloud Volumes ONTAP 時、您必須選擇集合體的預設磁碟大小。Cloud Manager 會將此磁碟大小用於初始 Aggregate、以及使用簡易資源配置選項時所建立的任何其他 Aggregate。您可以建立使用不同於預設磁碟大小的 Aggregate ["使用進階配置選項"](#)。



集合體中的所有磁碟大小必須相同。

在選擇磁碟大小時、您應該考量幾個因素。磁碟大小會影響您支付的儲存成本、您可以在集合體中建立的磁碟區大小、Cloud Volumes ONTAP 可供使用的總容量、以及儲存效能。

Azure Premium Storage 的效能與磁碟大小有關。較大的磁碟可提供較高的 IOPS 和處理量。例如、選擇1個TiB磁碟可提供比500 GiB磁碟更好的效能、而且成本更高。

標準儲存設備的磁碟大小沒有效能差異。您應該根據所需的容量來選擇磁碟大小。

請參閱 Azure、瞭解每個磁碟大小的 IOPS 與處理量：

- ["Microsoft Azure：託管磁碟定價"](#)

- ["Microsoft Azure：網頁 Blobs 定價"](#)

## 檢視預設系統磁碟

Cloud Manager除了儲存使用者資料之外、也購買雲端儲存設備來儲存Cloud Volumes ONTAP 作業系統資料（開機資料、根資料、核心資料和NVRAM）。為了規劃目的、在部署Cloud Volumes ONTAP 完更新之前、您可能需要先檢閱這些詳細資料。

["在Cloud Volumes ONTAP Azure中檢視系統資料的預設磁碟"](#)。



連接器也需要系統磁碟。 ["檢視Connector預設組態的詳細資料"](#)。

## 收集網路資訊

在 Cloud Volumes ONTAP Azure 中部署時、您需要指定虛擬網路的詳細資料。您可以使用工作表向系統管理員收集資訊。

| Azure 資訊         | 您的價值 |
|------------------|------|
| 區域               |      |
| 虛擬網路（vnet）       |      |
| 子網路              |      |
| 網路安全群組（如果使用您自己的） |      |

## 選擇寫入速度

Cloud Manager 可讓您選擇 Cloud Volumes ONTAP 適合的寫入速度設定。在您選擇寫入速度之前、您應該先瞭解一般與高設定之間的差異、以及使用高速寫入速度時的風險與建議。 ["深入瞭解寫入速度"](#)。

## 選擇Volume使用設定檔

包含多項儲存效率功能、可減少您所需的總儲存容量。ONTAP在 Cloud Manager 中建立 Volume 時、您可以選擇啟用這些功能的設定檔、或是停用這些功能的設定檔。您應該深入瞭解這些功能、以協助您決定要使用的設定檔。

NetApp 儲存效率功能提供下列效益：

### 資源隨需配置

為主機或使用者提供比實體儲存資源池實際擁有更多的邏輯儲存設備。儲存空間不會預先配置儲存空間、而是會在寫入資料時動態分配給每個磁碟區。

### 重複資料刪除

找出相同的資料區塊、並以單一共用區塊的參考資料取代這些區塊、藉此提升效率。這項技術可消除位於同一個磁碟區的備援資料區塊、進而降低儲存容量需求。

### 壓縮

藉由壓縮主儲存設備、次儲存設備和歸檔儲存設備上磁碟區內的資料、來減少儲存資料所需的實體容量。



## Azure 的網路需求 Cloud Volumes ONTAP

設定您的 Azure 網路、Cloud Volumes ONTAP 使其能夠正常運作。這包括連接器和 Cloud Volumes ONTAP 整個過程的網路功能。

### 需求 Cloud Volumes ONTAP

Azure 必須符合下列網路需求。

#### 傳出網際網路存取

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>

["瞭解如何驗AutoSupport 證功能"](#)。

#### IP位址

Cloud Manager 會將下列 IP 位址分配給 Cloud Volumes ONTAP Azure 中的功能：

- 單一節點：5 個 IP 位址
- HA 配對：16 個 IP 位址

請注意、Cloud Manager 會在 HA 配對上建立 SVM 管理 LIF、但不會在 Azure 中的單一節點系統上建立。



LIF 是與實體連接埠相關聯的 IP 位址。諸如 VMware 的管理工具需要 SVM 管理 LIF SnapCenter。

#### 安全連線至Azure服務

根據預設、Cloud Manager會啟用Azure Private Link、以便Cloud Volumes ONTAP 在支援的過程中連接到各個層面和Azure儲存帳戶。

在大多數情況下、您完全不需要做任何事——由NetApp Cloud Manager為您管理Azure Private Link。但如果您使用Azure私有DNS、則必須編輯組態檔。您也應該瞭解Azure中的Connector位置需求。

您也可以視業務需求而停用「私有連結」連線。如果您停用連結、Cloud Manager會設定Cloud Volumes ONTAP 使用服務端點的功能。

["深入瞭解如何搭配Cloud Volumes ONTAP 使用Azure私有連結或服務端點搭配使用"](#)。

#### 連線至其他ONTAP 的系統

若要在Cloud Volumes ONTAP Azure中的某個系統與ONTAP 其他網路中的某些系統之間複寫資料、您必須在Azure vnet與其他網路（例如您的公司網路）之間建立VPN連線。

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

**HA互連的连接埠**

一個包含HA互連的「支援功能」配對、可讓每個節點持續檢查其合作夥伴是否正常運作、並鏡射另一個非揮發性記憶體記錄資料。Cloud Volumes ONTAP HA互連使用TCP連接埠10006進行通訊。

依預設、HA互連生命體之間的通訊會開啟、而且此連接埠沒有安全性群組規則。但是、如果您在HA互連生命期之間建立防火牆、則必須確保TCP流量已開啟連接埠10006、如此HA配對才能正常運作。

**Azure資源群組中只有一組HA配對**

您必須使用\_Dedicated資源群組來處理Cloud Volumes ONTAP 您在Azure中部署的每一組EHA。資源群組僅支援一個HA配對。

如果您嘗試在Cloud Volumes ONTAP Azure資源群組中部署第二個「功能組」配對、Cloud Manager會發生連線問題。

**安全性群組**

您不需要建立安全性群組、因為Cloud Manager能幫您建立安全性群組。如果您需要使用自己的安全性群組規則、請參閱下列安全性群組規則。

**安全性群組規則**

Cloud Manager 會建立 Azure 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。

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

**單一節點系統的傳入規則**

下列規則會允許流量、除非說明中註明會封鎖特定的傳入流量。

| 優先順序和名稱                      | 連接埠與傳輸協定    | 來源與目的地 | 說明  |
|------------------------------|-------------|--------|---|
| 1000 inbound SSH             | 22 TCP      | 任意     | SSH 存取叢集管理 LIF 的 IP 位址或節點管理 LIF                     |
| 1001 inbound http            | 80 TCP      | 任意     | 使用叢集管理 LIF 的 IP 位址、以 HTTP 存取 System Manager Web 主控台 |
| 1002inbound （入站）_111_TCP     | 111 TCP     | 任意     | 遠端程序需要 NFS  |
| 1003 inbound _111_udp        | 111 udp     | 任意     | 遠端程序需要 NFS  |
| 1004 inbound （傳入）_139        | 139 TCP     | 任意     | CIFS 的 NetBios 服務工作階段                               |
| 1005inbound （傳入）_161-162_tcp | 161-162 TCP | 任意     | 簡單的網路管理傳輸協定   |

| 優先順序和名稱                             | 連接埠與傳輸協定        | 來源與目的地                   | 說明   |
|-------------------------------------|-----------------|--------------------------|--|
| 1006 inbound (傳入)<br>_161-162_udp   | 161-162 udp     | 任意                       | 簡單的網路管理傳輸協定  |
| 1007 inbound _443                   | 443 TCP         | 任意                       | 使用叢集管理 LIF 的 IP 位址、以 HTTPS 存取 System Manager 網路主控台 |
| 1008 inbound _445                   | 445 TCP         | 任意                       | Microsoft SMB/CIFS over TCP 搭配 NetBios 架構          |
| 1009 inbound _6335_tcp              | 635 TCP         | 任意                       | NFS 掛載   |
| 1010 inbound _6335_udp              | 635 udp         | 任意                       | NFS 掛載   |
| 1011 inbound (傳入)<br>_749           | 749 TCP         | 任意                       | Kerberos   |
| 1012 inbound _2049_tcp              | 2049 TCP        | 任意                       | NFS 伺服器精靈  |
| 1013 inbound _2049_udp              | 2049 udp        | 任意                       | NFS 伺服器精靈  |
| 1014 inbound (傳入)<br>_3260          | 3260 TCP        | 任意                       | 透過 iSCSI 資料 LIF 存取 iSCSI                           |
| 1015 inbound _4045-4046_tcp         | 4045-4046 TCP   | 任意                       | NFS 鎖定精靈和網路狀態監控                                    |
| 1016 inbound _4045-4046_udp         | 4045-4046 udp   | 任意                       | NFS 鎖定精靈和網路狀態監控                                    |
| 1017 inbound _10000                 | 10000 TCP       | 任意                       | 使用 NDMP 備份   |
| 1018 inbound (傳入)<br>_11104-11105   | 11104-11105 TCP | 任意                       | SnapMirror 資料傳輸                                    |
| 3000 inbound 拒絕<br>_all_tcp         | 任何連接埠 TCP       | 任意                       | 封鎖所有其他 TCP 傳入流量                                    |
| 3001 inbound 拒絕<br>_all_udp         | 任何連接埠 udp       | 任意                       | 封鎖所有其他的 UDP 傳入流量                                   |
| 65000 AllowVnetInBound              | 任何連接埠任何傳輸協定     | 虛擬網路至虛擬網路                | 來自 vnet 的傳入流量                                      |
| 65001 AllowAzureLoadBalancerInBound | 任何連接埠任何傳輸協定     | 將 AzureLoadBalancer 移至任何 | Azure Standard 負載平衡器的資料流量                          |
| 65500 DenyAllInBound                | 任何連接埠任何傳輸協定     | 任意                       | 封鎖所有其他傳入流量   |

## HA 系統的傳入規則

下列規則會允許流量、除非說明中註明會封鎖特定的傳入流量。



HA 系統的傳入規則少於單一節點系統、因為傳入資料流量會流經 Azure Standard Load Balancer。因此、來自負載平衡器的流量應開啟、如「AllowAzureLoadBalancerInBound」規則所示。

| 優先順序和名稱                              | 連接埠與傳輸協定    | 來源與目的地                   | 說明   |
|--------------------------------------|-------------|--------------------------|--|
| 100 inbound (傳入) _443                | 443 任何傳輸協定  | 任意                       | 使用叢集管理 LIF 的 IP 位址、以 HTTPS 存取 System Manager 網路主控台 |
| 101 inbound (傳入) _111_TCP            | 111 任何傳輸協定  | 任意                       | 遠端程序需要 NFS   |
| 102 inbound _2049_tcp                | 2049 任何傳輸協定 | 任意                       | NFS 伺服器精靈  |
| 111 inbound (傳入) _ssh                | 22 任何傳輸協定   | 任意                       | SSH 存取叢集管理 LIF 的 IP 位址或節點管理 LIF                    |
| 121inbound (傳入) _53                  | 53 任何傳輸協定   | 任意                       | DNS 與 CIFS   |
| 65000 AllowVnetInBound               | 任何連接埠任何傳輸協定 | 虛擬網路至虛擬網路                | 來自 vnet 的傳入流量                                      |
| 65001 AllowAzureLoad BalancerInBound | 任何連接埠任何傳輸協定 | 將 AzureLoadBalancer 移至任何 | Azure Standard 負載平衡器的資料流量                          |
| 65500 DenyAllInBound                 | 任何連接埠任何傳輸協定 | 任意                       | 封鎖所有其他傳入流量   |

## 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。

| 連接埠 | 傳輸協定    | 目的     |
|-----|---------|--------|
| 全部  | 所有 TCP  | 所有傳出流量 |
| 全部  | 所有的 udp | 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               | 連接埠    | 傳輸協定      | 來源                            | 目的地                 | 目的  |
|------------------|--------|-----------|-------------------------------|---------------------|---|
| Active Directory | 88     | TCP       | 節點管理 LIF                      | Active Directory 樹系 | Kerberos V 驗證                             |
|                  | 137.   | UDP       | 節點管理 LIF                      | Active Directory 樹系 | NetBios 名稱服務                              |
|                  | 138    | UDP       | 節點管理 LIF                      | Active Directory 樹系 | NetBios 資料報服務                             |
|                  | 139.   | TCP       | 節點管理 LIF                      | Active Directory 樹系 | NetBios 服務工作階段                            |
|                  | 389    | TCP 與 UDP | 節點管理 LIF                      | Active Directory 樹系 | LDAP                                      |
|                  | 445    | TCP       | 節點管理 LIF                      | Active Directory 樹系 | Microsoft SMB/CIFS over TCP 搭配 NetBios 架構 |
|                  | 464.64 | TCP       | 節點管理 LIF                      | Active Directory 樹系 | Kerberos V 變更及設定密碼 ( Set_change )         |
|                  | 464.64 | UDP       | 節點管理 LIF                      | Active Directory 樹系 | Kerberos 金鑰管理                             |
|                  | 749    | TCP       | 節點管理 LIF                      | Active Directory 樹系 | Kerberos V 變更與設定密碼 ( RPCSEC_GSS )         |
|                  | 88     | TCP       | 資料 LIF ( NFS 、 CIFS 、 iSCSI ) | Active Directory 樹系 | Kerberos V 驗證                             |
|                  | 137.   | UDP       | 資料 LIF ( NFS 、 CIFS )         | Active Directory 樹系 | NetBios 名稱服務                              |
|                  | 138    | UDP       | 資料 LIF ( NFS 、 CIFS )         | Active Directory 樹系 | NetBios 資料報服務                             |
|                  | 139.   | TCP       | 資料 LIF ( NFS 、 CIFS )         | Active Directory 樹系 | NetBios 服務工作階段                            |
|                  | 389    | TCP 與 UDP | 資料 LIF ( NFS 、 CIFS )         | Active Directory 樹系 | LDAP                                      |
|                  | 445    | TCP       | 資料 LIF ( NFS 、 CIFS )         | Active Directory 樹系 | Microsoft SMB/CIFS over TCP 搭配 NetBios 架構 |
|                  | 464.64 | TCP       | 資料 LIF ( NFS 、 CIFS )         | Active Directory 樹系 | Kerberos V 變更及設定密碼 ( Set_change )         |
|                  | 464.64 | UDP       | 資料 LIF ( NFS 、 CIFS )         | Active Directory 樹系 | Kerberos 金鑰管理                             |
|                  | 749    | TCP       | 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  |
| DHCP             | 68     | UDP       | 節點管理 LIF                      | DHCP                | 第一次設定的 DHCP 用戶端                           |
| DHCPS            | 67     | UDP       | 節點管理 LIF                      | DHCP                | DHCP 伺服器                                  |

| 服務         | 連接埠           | 傳輸協定 | 來源                              | 目的地           | 目的                             |
|------------|---------------|------|---------------------------------|---------------|--------------------------------|
| DNS        | 53.           | UDP  | 節點管理 LIF 與資料 LIF ( NFS 、 CIFS ) | DNS           | DNS                            |
| NDMP       | 18600 – 18699 | TCP  | 節點管理 LIF                        | 目的地伺服器        | NDMP 複本                        |
| SMTP       | 25            | TCP  | 節點管理 LIF                        | 郵件伺服器         | 可以使用 SMTP 警示 AutoSupport 來執行功能 |
| SNMP       | 161.          | TCP  | 節點管理 LIF                        | 監控伺服器         | 透過 SNMP 設陷進行監控                 |
|            | 161.          | UDP  | 節點管理 LIF                        | 監控伺服器         | 透過 SNMP 設陷進行監控                 |
|            | 162%          | TCP  | 節點管理 LIF                        | 監控伺服器         | 透過 SNMP 設陷進行監控                 |
|            | 162%          | UDP  | 節點管理 LIF                        | 監控伺服器         | 透過 SNMP 設陷進行監控                 |
| SnapMirror | 11104.        | TCP  | 叢集間 LIF                         | 叢集間 LIF ONTAP | 管理 SnapMirror 的叢集間通訊工作階段       |
|            | 11105.        | TCP  | 叢集間 LIF                         | 叢集間 LIF ONTAP | SnapMirror 資料傳輸                |
| 系統記錄       | 514           | UDP  | 節點管理 LIF                        | 系統記錄伺服器       | 系統記錄轉送訊息                       |

## 連接器需求

設定您的網路、讓 Connector 能夠管理公有雲環境中的資源和程序。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、您可以從「設定」頁面指定 Proxy 伺服器。請參閱 ["將 Connector 設定為使用 Proxy 伺服器"](#)。

## 連線至目標網路

連接器需要網路連線至您要部署 Cloud Volumes ONTAP 的 VPC 和 VNets 。

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

## 傳出網際網路存取

連接器需要存取傳出網際網路、才能管理公有雲環境中的資源和程序。

| 端點   | 目的                                     |
|--|--|
| <a href="https://support.netapp.com">https://support.netapp.com</a>  | 以取得授權資訊、並將AutoSupport 資訊傳送給NetApp支援部門。 |
| <a href="https://*.cloudmanager.cloud.netapp.com">https://*.cloudmanager.cloud.netapp.com</a>  | 在Cloud Manager中提供SaaS功能與服務。            |
| <a href="https://cloudmanagerinfraproduct.azurecr.io">https://cloudmanagerinfraproduct.azurecr.io</a><br><a href="https://*.blob.core.windows.net">https://*.blob.core.windows.net</a> | 升級Connector及其Docker元件。                 |

## 安全性群組規則

Connector 的安全性群組需要傳入和傳出規則。

### 傳入規則

| 連接埠   | 傳輸協定  | 目的                              |
|-------|-------|---------------------------------|
| 22    | SSH   | 提供對 Connector 主機的 SSH 存取權       |
| 80    | HTTP  | 提供從用戶端 Web 瀏覽器到本機使用者介面的 HTTP 存取 |
| 443.. | HTTPS | 提供 HTTPS 存取、從用戶端網頁瀏覽器存取本機使用者介面  |

### 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。

| 連接埠 | 傳輸協定    | 目的     |
|-----|---------|--------|
| 全部  | 所有 TCP  | 所有傳出流量 |
| 全部  | 所有的 udp | 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                     | 連接埠   | 傳輸協定  | 目的地                    | 目的   |
|------------------------|-------|-------|------------------------|--|
| API 呼叫與 AutoSupport 功能 | 443.. | HTTPS | 傳出網際網路和 ONTAP 叢集管理 LIF | API將Azure和ONTAP VMware呼叫、Cloud Data Sense、勒索軟體服務、並將AutoSupport VMware訊息傳送給NetApp |
| DNS                    | 53.   | UDP   | DNS                    | 用於 Cloud Manager 的 DNS 解析  |

## 設定Cloud Volumes ONTAP 支援使用Azure中客戶管理的金鑰

資料會使用在Cloud Volumes ONTAP Azure中的功能自動加密 "[Azure 儲存服務加密](#)" 使用Microsoft管理的金鑰。但您可以改用自己的加密金鑰、只要執行本頁的步驟即可。

### 資料加密總覽

Azure中的資料會使用自動加密Cloud Volumes ONTAP "[Azure 儲存服務加密](#)"。預設實作使用Microsoft管理的金鑰。無需設定。

如果您想要使用客戶管理的支援服務金鑰Cloud Volumes ONTAP 搭配使用、則必須完成下列步驟：

1. 從Azure建立金鑰保存庫、然後在該保存庫中產生金鑰
2. 在Cloud Manager中、使用API建立Cloud Volumes ONTAP 一個使用金鑰的功能不全的環境

### 金鑰旋轉

如果您建立新版的金鑰、Cloud Volumes ONTAP 則更新版本會自動使用最新的金鑰版本。

### 資料加密方式

建立Cloud Volumes ONTAP 一個設定為使用客戶管理金鑰的功能完善的支援環境之後Cloud Volumes ONTAP、即可將下列資料加密。

#### HA 配對

- 所有的Azure儲存帳戶Cloud Volumes ONTAP 均使用客戶管理的金鑰進行加密。
- 任何新的儲存帳戶（例如新增磁碟或集合體時）也會使用相同的金鑰。

#### 單一節點

- 所有的Azure儲存帳戶Cloud Volumes ONTAP 均使用客戶管理的金鑰進行加密。
- 對於根磁碟、開機磁碟和資料磁碟、Cloud Manager使用 "[磁碟加密集](#)"，可透過託管磁碟管理加密金鑰。
- 任何新的資料磁碟也會使用相同的磁碟加密集。
- NVRAM和核心磁碟是使用Microsoft管理的金鑰來加密、而非使用客戶管理的金鑰。

### 建立金鑰保存庫並產生金鑰

金鑰庫必須位於您計畫建立Cloud Volumes ONTAP 此系統的同一個Azure訂閱和地區。

#### 步驟

1. "[在您的Azure訂閱中建立金鑰庫](#)"。

請注意金鑰庫的下列需求：

- 金鑰保存庫必須與Cloud Volumes ONTAP 該系統位於相同的區域。
- 應啟用下列選項：
  - 軟刪除（此選項預設為啟用、但不可停用）
  - 清除保護



- \* Azure磁碟加密、適用於Volume加密\* (Cloud Volumes ONTAP 僅適用於單一節點的整套系統)

## 2. "在金鑰保存庫中產生金鑰"。

請注意金鑰的下列需求：

- 金鑰類型必須為\* RSA\*。
- 建議的RSA金鑰大小為\* 2048\*、但支援其他大小。

### 建立使用加密金鑰的工作環境

建立金鑰庫並產生加密金鑰之後、您可以建立Cloud Volumes ONTAP 新的、設定為使用金鑰的整套系統。使用Cloud Manager API可支援這些步驟。

如果您想要將客戶管理的金鑰與單一節點Cloud Volumes ONTAP 的作業系統搭配使用、請確定Cloud Manager Connector具有下列權限：

```
"Microsoft.Compute/diskEncryptionSets/read"  
"Microsoft.Compute/diskEncryptionSets/write",  
"Microsoft.Compute/diskEncryptionSets/delete"  
"Microsoft.KeyVault/vaults/deploy/action",  
"Microsoft.KeyVault/vaults/read",  
"Microsoft.KeyVault/vaults/accessPolicies/write"
```

您可以在上找到最新的權限清單 "[Cloud Manager 原則頁面](#)"。



HA配對不需要前三個權限。

### 步驟

1. 請使用下列Cloud Manager API呼叫、取得Azure訂閱中的金鑰保存清單。

對於HA配對：「Get /azure/ha/mata/Vault」

對於單一節點：「Get /azure/VSA/中繼資料/資料保存」

請記下\*名稱\*和\*資源群組\*。您需要在下一步中指定這些值。

["深入瞭解此API呼叫"](#)。

2. 使用下列Cloud Manager API呼叫、取得資料保險箱內的金鑰清單。

對於HA配對：「Get /azure/ha/matmata/keys/Vault」

對於單一節點：「Get /azure/VSA/中繼資料/金鑰庫」

請記下\*金鑰名稱\*。您需要在下一步中指定該值（連同資料保險箱名稱）。

["深入瞭解此API呼叫"](#)。

3. 使用Cloud Volumes ONTAP 下列Cloud Manager API呼叫建立一套系統。

a. 對於HA配對：

「POST /azure/ha/辦公 環境」

申請本文必須包含下列欄位：

```
"azureEncryptionParameters": {  
  "key": "keyName",  
  "vaultName": "vaultName"  
}
```

["深入瞭解此API呼叫"](#)。

b. 對於單一節點系統：

「POST /azure/VSA/工作環境」

申請本文必須包含下列欄位：

```
"azureEncryptionParameters": {  
  "key": "keyName",  
  "vaultName": "vaultName"  
}
```

+

["深入瞭解此API呼叫"](#)。

您有一個Cloud Volumes ONTAP 全新的支援系統、可設定使用客戶管理的金鑰進行資料加密。

## 在Cloud Volumes ONTAP Azure中設定for NetApp的授權

決定Cloud Volumes ONTAP 要搭配使用哪種授權選項之後、您必須先執行幾個步驟、才能在建立新的工作環境時選擇授權選項。

### Freemium

選擇Freemium產品、即可免費使用Cloud Volumes ONTAP 多達500 GiB的配置容量。 ["深入瞭解Freemium產品"](#)。

### 步驟

1. 在「畫版」頁面上、按一下「新增工作環境」、然後依照Cloud Manager中的步驟進行。

a. 在\*詳細資料與認證\*頁面上、按一下\*編輯認證>新增訂閱\*、然後依照提示訂閱Azure Marketplace中的隨用隨付方案。

除非您超過500 GiB的已配置容量、系統會自動轉換為、否則不會透過市場訂閱付費 "Essentials套件"。

**Edit Credentials & Add Subscription**

Associate Subscription to Credentials ⓘ

Credentials  
Managed Service Identity

Azure Subscription  
OCCM Dev (Default)

Marketplace Subscription  
ⓘ A marketplace subscription isn't associated with the selected Azure subscription.

+ Add Subscription

Apply Cancel

- a. 返回Cloud Manager之後、當您進入「充電方法」頁面時、請選取\* Freemium \*。

**Select Charging Method**

|                                  |                          |             |   |
|----------------------------------|--------------------------|-------------|---|
| <input type="radio"/>            | Professional             | By capacity | ▼ |
| <input type="radio"/>            | Essential                | By capacity | ▼ |
| <input checked="" type="radio"/> | Freemium (Up to 500 GiB) | By capacity | ▼ |
| <input type="radio"/>            | Per Node                 | By node     | ▼ |

"請參閱Cloud Volumes ONTAP 逐步指示、以在Azure中推出《功能不全》"。

### 容量型授權

容量型授權可讓您針對Cloud Volumes ONTAP 容量的每個TiB付費。容量型授權的形式為\_package\_：Essentials套件或Professional套件。

Essentials和Professional套件可搭配下列消費模式使用：

- 向NetApp購買的授權（BYOL）
- Azure Marketplace的每小時隨付隨付（PAYGO）訂閱
- 年度合約

["深入瞭解容量型授權"](#)。

下列各節將說明如何開始使用這些消費模式。

## BYOL

事先向NetApp購買授權（BYOL）、即可在Cloud Volumes ONTAP 任何雲端供應商部署支援系統。

### 步驟

1. ["請聯絡NetApp銷售人員以取得授權"](#)
2. ["將您的NetApp支援網站帳戶新增至Cloud Manager"](#)

Cloud Manager會自動查詢NetApp的授權服務、以取得與您NetApp支援網站帳戶相關之授權的詳細資料。如果沒有錯誤、Cloud Manager會自動將授權新增至Digital Wallet。

您的授權必須先從Digital Wallet取得、才能搭配Cloud Volumes ONTAP 使用。如有需要、您可以 ["手動將授權新增至Digital Wallet"](#)。

3. 在「畫版」頁面上、按一下「新增工作環境」、然後依照Cloud Manager中的步驟進行。
  - a. 在\*詳細資料與認證\*頁面上、按一下\*編輯認證>新增訂閱\*、然後依照提示訂閱Azure Marketplace中的隨用隨付方案。

您向NetApp購買的授權一律會先收取費用、但如果您超過授權容量或授權到期、則會從市場的每小時費率中收取費用。

### Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev (Default)

Marketplace Subscription

ⓘ A marketplace subscription isn't associated with the selected Azure subscription.

+ Add Subscription

Apply Cancel

- a. 返回Cloud Manager之後、請在前往「充電方法」頁面時、選取容量型套件。

### Select Charging Method

|  |             |   |
|--|-------------|---|
| <input checked="" type="radio"/> Professional  | By capacity | ▼ |
| <input type="radio"/> Essential                | By capacity | ▼ |
| <input type="radio"/> Freemium (Up to 500 GiB) | By capacity | ▼ |
| <input type="radio"/> Per Node                 | By node     | ▼ |

"請參閱Cloud Volumes ONTAP 逐步指示、以在Azure中推出《功能不全》"。

#### PAYGO訂閱

從雲端供應商的市場訂閱優惠、每小時支付一次。

當您建立Cloud Volumes ONTAP 一個可運作的環境時、Cloud Manager會提示您訂閱Azure Marketplace提供的合約。該訂閱之後會與工作環境建立關聯、以便進行充電。您可以在其他工作環境中使用相同的訂閱。

## 步驟

1. 在「畫版」頁面上、按一下「新增工作環境」、然後依照Cloud Manager中的步驟進行。
  - a. 在\*詳細資料與認證\*頁面上、按一下\*編輯認證>新增訂閱\*、然後依照提示訂閱Azure Marketplace中的隨付方案。

The screenshot shows a dialog box titled "Edit Credentials & Add Subscription". It has a section "Associate Subscription to Credentials" with a help icon. Below this are two dropdown menus: "Credentials" set to "Managed Service Identity" and "Azure Subscription" set to "OCCM Dev (Default)". A message box states: "A marketplace subscription isn't associated with the selected Azure subscription." Below the message is a blue button with a plus icon and the text "Add Subscription". At the bottom are two buttons: "Apply" (blue) and "Cancel" (grey).

- b. 返回Cloud Manager之後、請在前往「充電方法」頁面時、選取容量型套件。

The screenshot shows a dialog box titled "Select Charging Method". It contains four radio button options: "Professional" (selected), "Essential", "Freemium (Up to 500 GiB)", and "Per Node". To the right of each option is a button labeled "By capacity" (for the first three) or "By node" (for the last one), followed by a downward arrow icon.

"請參閱Cloud Volumes ONTAP 逐步指示、以在Azure中推出《功能不全》"。



您可以從「設定」>「認證」頁面管理Azure Marketplace與Azure帳戶相關的訂閱。"[瞭解如何管理您的Azure帳戶和訂閱](#)"

#### 年度合約

購買年度合約、每年支付Cloud Volumes ONTAP 一份銷售費。

#### 步驟

1. 請聯絡您的NetApp銷售代表以購買年度合約。

該合約可在Azure Marketplace以\_Private\_優惠形式提供。

NetApp與您分享私人優惠之後、您可以在工作環境建立期間、從Azure Marketplace訂閱年度方案。

2. 在「畫版」頁面上、按一下「新增工作環境」、然後依照Cloud Manager中的步驟進行。
  - a. 在\*詳細資料與認證\*頁面上、按一下\*編輯認證>新增訂閱>繼續\*。
  - b. 在Azure入口網站中、選取與Azure帳戶共享的年度計畫、然後按一下\*訂閱\*。
  - c. 返回Cloud Manager之後、請在前往「充電方法」頁面時、選取容量型套件。

Select Charging Method

|  |             |   |
|--|-------------|---|
| <input checked="" type="radio"/> Professional  | By capacity | ▼ |
| <input type="radio"/> Essential                | By capacity | ▼ |
| <input type="radio"/> Freemium (Up to 500 GiB) | By capacity | ▼ |
| <input type="radio"/> Per Node                 | By node     | ▼ |

"[請參閱Cloud Volumes ONTAP 逐步指示](#)、以在Azure中推出《功能不全》"。

#### Keystone Flex 訂閱

Keystone Flex訂閱是一種隨需付費的訂閱型服務。"[深入瞭解Keystone Flex訂閱](#)"。

#### 步驟

1. 如果您尚未訂閱、"[請聯絡NetApp](#)"
2. <mailto:ng-keystone-success@netapp.com> [聯絡NetApp]、以一或多個Keystone Flex訂閱授權您的Cloud Manager使用者帳戶。
3. NetApp授權您的帳戶之後、"[連結您的訂閱內容以供Cloud Volumes ONTAP 搭配使用](#)"。
4. 在「畫版」頁面上、按一下「新增工作環境」、然後依照Cloud Manager中的步驟進行。

- a. 當系統提示您選擇充電方法時、請選取Keystone Flex訂閱充電方法。

Select Charging Method

☒ **Keystone** By capacity ^

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1 v

☐ Professional By capacity v

☐ Essential By capacity v

☐ Freemium (Up to 500 GiB) By capacity v

☐ Per Node By node v

"請參閱[Cloud Volumes ONTAP 逐步指示](#)、以在Azure中推出《功能不全》"。

## 在 Cloud Volumes ONTAP Azure 中啟動

您可以 Cloud Volumes ONTAP 在 Cloud Manager 中建立運作不正常的環境、在 Azure 中啟動單一節點系統或 HA 配對。

您需要下列項目才能建立工作環境。

- 已啟動並執行的連接器。
  - 您應該擁有 "[與工作區相關的連接器](#)"。
  - "[您應該隨時準備好讓 Connector 保持運作](#)"。
- 瞭解您要使用的組態。

您應該已經選擇組態、並從系統管理員取得 Azure 網路資訊。如需詳細資訊、請參閱 "[規劃 Cloud Volumes ONTAP 您的需求組態](#)"。

- 瞭解設定Cloud Volumes ONTAP 驗證功能所需的條件。

"[瞭解如何設定授權](#)"。



Cloud Manager Cloud Volumes ONTAP 在 Azure 中建立一套功能完善的系統時、會建立多個 Azure 物件、例如資源群組、網路介面和儲存帳戶。您可以在精靈結束時檢閱資源摘要。



資料遺失的可能性

最佳實務做法是針對每 Cloud Volumes ONTAP 個系統使用新的專屬資源群組。

由於資料遺失的風險、不建議在 Cloud Volumes ONTAP 現有的共享資源群組中部署此功能。雖然 Cloud Manager 可在 Cloud Volumes ONTAP 部署失敗或刪除時、從共用資源群組移除資源的功能、但 Azure 使用者可能會不小心從 Cloud Volumes ONTAP 共用資源群組中刪除這些資源。

#### 步驟

1. [[訂閱]在「畫版」頁面上、按一下「新增工作環境」、然後依照提示進行。
2. \* 選擇位置 \* : 選擇 \* Microsoft Azure \* 與 \* Cloud Volumes ONTAP 《單一節點 \* 》或 \* Cloud Volumes ONTAP 《高可用度 \* 》。
3. 如果出現提示、"建立連接器"。
4. 詳細資料與認證：選擇性變更 Azure 認證與訂閱、指定叢集名稱、視需要新增標籤、然後指定認證資料。

下表說明您可能需要指導的欄位：


| 欄位                 | 說明  |
|--------------------|---|
| 工作環境名稱             | Cloud Manager 會使用工作環境名稱來命名 Cloud Volumes ONTAP 整個系統、以及 Azure 虛擬機器。如果您選取該選項、它也會使用名稱做為預先定義安全性群組的前置詞。  |
| 資源群組標記             | 標記是 Azure 資源的中繼資料。當您在此欄位中輸入標記時、Cloud Manager 會將標記新增至與 Cloud Volumes ONTAP 該系統相關聯的資源群組。建立工作環境時、您最多可以從使用者介面新增四個標記、然後在建立之後新增更多標記。請注意、在建立工作環境時、API 不會限制您使用四個標記。如需標記的相關資訊、請參閱 " <a href="#">Microsoft Azure 說明文件：使用標籤來組織 Azure 資源</a> "。 |
| 使用者名稱和密碼           | 這些是 Cloud Volumes ONTAP 適用於整個叢集管理員帳戶的認證資料。您可以使用這些認證資料、Cloud Volumes ONTAP 透過 System Manager 或其 CLI 連線至功能驗證。保留預設的 _admin_ 使用者名稱、或將其變更為自訂使用者名稱。   |
| [[video ) ] 編輯認證資料 | 您可以選擇不同的 Azure 認證資料和其他 Azure 訂閱、以搭配此 Cloud Volumes ONTAP 款作業系統使用。您必須將 Azure Marketplace 訂閱與所選 Azure 訂閱建立關聯、才能部署隨用隨付 Cloud Volumes ONTAP 的功能。" <a href="#">瞭解如何新增認證</a> "。   |

下列影片說明如何將 Marketplace 訂閱與 Azure 訂閱建立關聯：

► <https://docs.netapp.com/zh-tw/cloud-manager-cloud-volumes->

5. \* 服務 \*：啟用或停用 Cloud Volumes ONTAP 您不想搭配使用的個別服務。
  - ["深入瞭解Cloud Data Sense"](#)。
  - ["深入瞭解Cloud Backup"](#)。
  - ["深入瞭解監控服務"](#)。
6. 位置與連線：選取位置、資源群組、安全性群組、然後選取核取方塊以確認連接器與目標位置之間的網路連線。

下表說明您可能需要指導的欄位：

| 欄位    | 說明  |
|-------|---|
| 位置    | 對於單一節點系統、您可以選擇要部署 Cloud Volumes ONTAP 的可用度區域。如果您未選擇 AZ、Cloud Manager 會為您選擇一個。   |
| 資源群組  | <p>建立Cloud Volumes ONTAP 新的資源群組以供使用、或使用現有的資源群組。最佳實務做法是使用全新的資源群組 Cloud Volumes ONTAP 來進行支援。雖然可以在Cloud Volumes ONTAP 現有的共享資源群組中部署功能、但由於資料遺失的風險、不建議這麼做。如需詳細資料、請參閱上述警告。</p> <p>您必須使用專屬的資源群組來處理Cloud Volumes ONTAP 您在Azure中部署的每個「EHA配對」。資源群組僅支援一個HA配對。如果您嘗試在Cloud Volumes ONTAP Azure資源群組中部署第二個「功能組」配對、Cloud Manager會發生連線問題。</p> <div><p>如果您使用的Azure帳戶具有 <a href="#">"必要權限"</a>Cloud Manager可在Cloud Volumes ONTAP 部署失敗或刪除時、從資源群組移除不必要的資源。</p></div> |
| 安全性群組 | 如果您選擇現有的安全群組、則必須符合Cloud Volumes ONTAP 下列需求： <a href="#">"檢視預設的安全性群組"</a> 。  |

7. 充電方法與**NSS**帳戶：指定您要搭配此系統使用的收費選項、然後指定NetApp支援網站帳戶。
  - ["深入瞭解Cloud Volumes ONTAP 解適用於此功能的授權選項"](#)。
  - ["瞭解如何設定授權"](#)。
8. \* 預先設定的套件 \*：選取其中一個套件以快速部署 Cloud Volumes ONTAP 某個作業系統、或按一下 \* 建立我自己的組態 \*。

如果您選擇其中一個套件、則只需指定一個 Volume、然後檢閱並核准組態。

9. 授權：視Cloud Volumes ONTAP 需要變更此版本、然後選取虛擬機器類型。



如果所選版本有較新的發行候選版本、一般可用度或修補程式版本、Cloud Manager 會在建立工作環境時、將系統更新至該版本。例如、如果您選擇Cloud Volumes ONTAP 了「更新」功能、就會進行更新。更新不會從一個版本發生到另一個版本、例如從 9.6 到 9.7。

10. \* 從 Azure Marketplace 訂閱 \*：如果 Cloud Manager 無法以程式設計方式部署 Cloud Volumes ONTAP 功能、請依照下列步驟進行。

11. \* 基礎儲存資源 \*：選擇初始 Aggregate 的設定：磁碟類型、每個磁碟的大小、以及是否應啟用資料分層至 Blob 儲存設備。

請注意下列事項：

- 磁碟類型適用於初始磁碟區。您可以為後續磁碟區選擇不同的磁碟類型。
- 磁碟大小適用於初始 Aggregate 中的所有磁碟、以及 Cloud Manager 在使用簡易資源配置選項時所建立的任何其他集合體。您可以使用進階配置選項、建立使用不同磁碟大小的集合體。

如需選擇磁碟類型和大小的說明、請參閱 "[在 Azure 中調整系統規模](#)"。

- 您可以在建立或編輯磁碟區時、選擇特定的磁碟區分層原則。
- 如果停用資料分層、您可以在後續的 Aggregate 上啟用。

["深入瞭解資料分層"](#)。

12. \* 寫入速度與 WORM \*（僅限單節點系統）：選擇 \* 正常 \* 或 \* 高速 \* 寫入速度、並視需要啟動一次寫入、多次讀取（WORM）儲存設備。

["深入瞭解寫入速度"](#)。

如果啟用雲端備份或啟用資料分層、則無法啟用 WORM。

["深入瞭解 WORM 儲存設備"](#)。

13. \* 安全通訊至儲存設備與 WORM \*（僅限 HA）：選擇是否啟用 HTTPS 連線至 Azure 儲存帳戶、並視需要啟動一次寫入、多次讀取（WORM）儲存設備。

HTTPS 連線是 Cloud Volumes ONTAP 從一個名為「支援速度」的鏈接至 Azure 儲存帳戶。請注意、啟用此選項可能會影響寫入效能。您無法在建立工作環境之後變更設定。

["深入瞭解 WORM 儲存設備"](#)。

14. \* 建立 Volume \*：輸入新磁碟區的詳細資料、或按一下 \* 跳過 \*。

["瞭解支援的用戶端傳輸協定和版本"](#)。

本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

| 欄位                   | 說明   |
|----------------------|--|
| 尺寸                   | 您可以輸入的最大大小、主要取決於您是否啟用精簡配置、這可讓您建立比目前可用實體儲存容量更大的磁碟區。   |
| 存取控制（僅適用於 NFS）       | 匯出原則會定義子網路中可存取磁碟區的用戶端。根據預設、Cloud Manager 會輸入一個值、讓您存取子網路中的所有執行個體。   |
| 權限與使用者 / 群組（僅限 CIFS） | 這些欄位可讓您控制使用者和群組（也稱為存取控制清單或 ACL）的共用存取層級。您可以指定本機或網域 Windows 使用者或群組、或 UNIX 使用者或群組。如果您指定網域 Windows 使用者名稱、則必須使用網域\使用者名稱格式來包含使用者的網域。 |

| 欄位                     | 說明  |
|------------------------|---|
| Snapshot 原則            | Snapshot 複製原則會指定自動建立的 NetApp Snapshot 複本的頻率和數量。NetApp Snapshot 複本是一種不影響效能的時間點檔案系統映像、需要最少的儲存容量。您可以選擇預設原則或無。您可以針對暫時性資料選擇「無」：例如、Microsoft SQL Server 的 Tempdb。   |
| 進階選項（僅適用於 NFS）         | 為磁碟區選取 NFS 版本：NFSv3 或 NFSv3。  |
| 啟動器群組和 IQN（僅適用於 iSCSI） | iSCSI 儲存目標稱為 LUN（邏輯單元）、以標準區塊裝置的形式呈現給主機。啟動器群組是 iSCSI 主機節點名稱的表格、可控制哪些啟動器可存取哪些 LUN。iSCSI 目標可透過標準乙太網路介面卡（NIC）、TCP 卸載引擎（TOE）卡（含軟體啟動器）、整合式網路介面卡（CNA）或專用主機匯流排介面卡（HBA）連線至網路、並由 iSCSI 合格名稱（IQN）識別。建立 iSCSI Volume 時、Cloud Manager 會自動為您建立 LUN。我們只要在每個磁碟區建立一個 LUN、就能輕鬆完成工作、因此不需要管理。建立磁碟區之後、 <a href="#">"使用 IQN 從主機連線至 LUN"</a> 。 |

下圖顯示 CIFS 傳輸協定的「Volume」（磁碟區）頁面：

### Volume Details, Protection & Protocol

#### Details & Protection

Volume Name:  Size (GB):

Snapshot Policy: default

Default Policy

#### Protocol

NFS
CIFS
iSCSI

Share name:  Permissions: Full Control

Users / Groups:

Valid users and groups separated by a semicolon

15. \* CIFS 設定 \*：如果您選擇 CIFS 傳輸協定、請設定 CIFS 伺服器。

| 欄位                       | 說明   |
|--------------------------|--|
| DNS 主要和次要 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。  |

| 欄位      | 說明  |
|---------|---|
| 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」。若要將 Azure AD 網域服務設定為 Cloud Volumes ONTAP AD 伺服器以供使用、您應在此欄位中輸入 *OID=AADDC computers* 或 *OID=AADDC 使用者*。<br>◦ <a href="https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou">https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou</a> ["Azure 說明文件：在 Azure AD 網域服務託管網域中建立組織單位（OU）"] |
| DNS 網域  | 適用於整個儲存虛擬 Cloud Volumes ONTAP 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 | 選擇 * 使用 Active Directory 網域 * 來使用 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。請注意、您只能在建立 CIFS 伺服器時設定 NTP 伺服器。您建立 CIFS 伺服器之後、就無法進行設定。  |

16. \* 使用率設定檔、磁碟類型及分層原則 \*：視需要選擇是否要啟用儲存效率功能、並變更磁碟區分層原則。

如需詳細資訊、請參閱 ["瞭解 Volume 使用量設定檔"](#) 和 ["資料分層總覽"](#)。

17. \* 審查與核准 \*：檢閱並確認您的選擇。

- 檢閱組態的詳細資料。
- 按一下 \* 更多資訊 \* 以檢閱 Cloud Manager 將購買的支援與 Azure 資源詳細資料。
- 選取「\* 我瞭解 ... \*」核取方塊。
- 按一下「\* 執行 \*」。

Cloud Manager 部署 Cloud Volumes ONTAP 了這個功能。您可以追蹤時間表的進度。

如果您在部署 Cloud Volumes ONTAP 此系統時遇到任何問題、請檢閱故障訊息。您也可以選取工作環境、然後按一下 \* 重新建立環境 \*。

如需其他協助、請前往 ["NetApp Cloud Volumes ONTAP 支援"](#)。

完成後

- 如果您已配置 CIFS 共用區、請授予使用者或群組檔案和資料夾的權限、並確認這些使用者可以存取共用區並建立檔案。
- 如果您要將配額套用至磁碟區、請使用 System Manager 或 CLI。

配額可讓您限制或追蹤使用者、群組或 qtree 所使用的磁碟空間和檔案數量。

## 開始使用 Google Cloud

### 在 Google Cloud 中快速入門 Cloud Volumes ONTAP

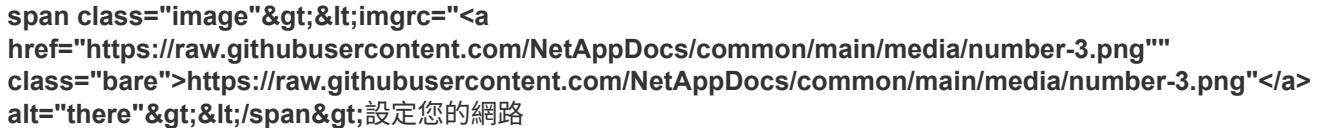
只要幾個步驟、就能開始使用 Cloud Volumes ONTAP 適用於 GCP 的功能。

如果您沒有 ["連接器"](#) 然而、帳戶管理員需要建立一個帳戶。 ["瞭解如何在 GCP 中建立連接器"](#)。

當您建立第一個 Cloud Volumes ONTAP 運作環境時、如果您還沒有連接器、Cloud Manager 會提示您部署連接器。

Cloud Manager 提供符合工作負載需求的預先設定套件、您也可以建立自己的組態。如果您選擇自己的組態、應該瞭解可用的選項。

["深入瞭解規劃組態"](#)。

The diagram illustrates a network setup for Cloud Volumes ONTAP. It shows a VPC (Virtual Private Cloud) containing several subnets. A connector is shown connecting to the VPC. The text indicates that the connector needs to be configured with the appropriate network settings, including VPC and subnet information.

1. 確保您的 VPC 和子網路支援連接器與 Cloud Volumes ONTAP 支援之間的連線。
2. 如果您打算啟用資料分層、["設定Cloud Volumes ONTAP 私有Google Access的子網路"](#)。
3. 如果您要部署 HA 配對、請確定您有四個 VPC 、每個 VPC 都有自己的子網路。
4. 如果您使用的是共享VPC、請將\_Compute Network User\_角色提供給Connector服務帳戶。
5. 啟用從目標 VPC 的傳出網際網路存取、讓 Connector 和 Cloud Volumes ONTAP 支援中心能夠連絡多個端點。

這個步驟很重要、因為連接器 Cloud Volumes ONTAP 無法在沒有外傳網際網路存取的情況下管理不穩定。如果您需要限制傳出連線、請參閱的端點清單 ["Connector 與 Cloud Volumes ONTAP the"](#)。

["深入瞭解網路需求"](#)。

下列兩種用途需要Google Cloud服務帳戶：Cloud Volumes ONTAP第一個是啟用時 ["資料分層"](#) 將冷資料分層至Google Cloud中的低成本物件儲存設備。第二個是啟用時 ["Cloud Backup Service"](#) 將磁碟區備份至低成本的物件儲存設備。

您可以設定一個服務帳戶、並將其用於這兩種用途。服務帳戶必須具有\*儲存設備管理\*角色。

["閱讀逐步指示"](#)。

["在專案中啟用下列 Google Cloud API"](#)。這些 API 是部署連接器和 Cloud Volumes ONTAP 功能不全的必備條件。

- Cloud Deployment Manager V2 API
- 雲端記錄 API
- Cloud Resource Manager API
- 運算引擎 API
- 身分識別與存取管理（IAM）API

按一下「\* 新增工作環境 \*」、選取您要部署的系統類型、然後完成精靈中的步驟。["閱讀逐步指示"](#)。

相關連結

- ["從 Cloud Manager 建立 Connector"](#)
- ["在 Linux 主機上安裝 Connector 軟體"](#)
- ["Cloud Manager 具備 GCP 權限的功能"](#)



## 在Cloud Volumes ONTAP Google Cloud規劃您的不一樣組態

在 Cloud Volumes ONTAP Google Cloud 中部署時、您可以選擇符合工作負載需求的預先設定系統、或是建立自己的組態。如果您選擇自己的組態、應該瞭解可用的選項。

選擇**Cloud Volumes ONTAP** 一個不含功能的授權

有多種授權選項可供Cloud Volumes ONTAP 選擇。每個選項都能讓您選擇符合需求的消費模式。

- ["深入瞭解Cloud Volumes ONTAP 解適用於此功能的授權選項"](#)
- ["瞭解如何設定授權"](#)

選擇支援的地區

支援大部分Google Cloud地區的支援。Cloud Volumes ONTAP ["檢視支援區域的完整清單"](#)。

選擇支援的機器類型

根據您選擇的授權類型、支援多種機器類型。Cloud Volumes ONTAP

["支援的GCP組態Cloud Volumes ONTAP"](#)

瞭解儲存限制

一個不含資源的系統的原始容量上限 Cloud Volumes ONTAP 與授權有關。其他限制會影響集合體和磁碟區的大小。在規劃組態時、您應該注意這些限制。

["適用於GCP的儲存限制Cloud Volumes ONTAP"](#)

在**GCP**中調整系統規模

調整 Cloud Volumes ONTAP 您的支援規模、有助於滿足效能與容量的需求。在選擇機器類型、磁碟類型和磁碟大小時、您應該注意幾個關鍵點：

機器類型

請查看中支援的機器類型 ["發行說明 Cloud Volumes ONTAP"](#) 然後檢視 Google 提供的每種受支援機器類型的詳細資料。將工作負載需求與機器類型的 vCPU 和記憶體數量配對。請注意、每個 CPU 核心都能提升網路效能。

如需詳細資料、請參閱下列內容：

- ["Google Cloud 文件：N1 標準機器類型"](#)
- ["Google Cloud 文件：效能"](#)

**GCP** 磁碟類型

當您建立 Cloud Volumes ONTAP 用於資料的 Volume 時、您需要選擇 Cloud Volumes ONTAP 基礎雲端儲存設備、以便將其用於磁碟。磁碟類型可以是下列任一種：

- *Zonal SSD*持續式磁碟：SSD持續式磁碟最適合需要高隨機IOPS速率的工作負載。

- 分區平衡的持續磁碟：這些SSD可提供較低的每GB IOPS、以平衡效能與成本。
- *Zonal Standard*持續式磁碟：標準持續式磁碟經濟實惠、可處理連續讀寫作業。

如需詳細資料、請參閱 ["Google Cloud 文件：分區持續磁碟（標準和 SSD）"](#)。

## GCP 磁碟大小

部署 Cloud Volumes ONTAP 一套系統時、您需要選擇初始磁碟大小。之後、您可以讓 Cloud Manager 為您管理系統容量、但如果您想自行建置集合體、請注意下列事項：

- 集合體中的所有磁碟大小必須相同。
- 判斷您需要的空間、同時考量效能。
- 持續性磁碟的效能會隨著磁碟大小和系統可用的 vCPU 數目而自動擴充。

如需詳細資料、請參閱下列內容：

- ["Google Cloud 文件：分區持續磁碟（標準和 SSD）"](#)
- ["Google Cloud 文件：最佳化持續磁碟和本機 SSD 效能"](#)

## 檢視預設系統磁碟

Cloud Manager除了儲存使用者資料之外、也購買雲端儲存設備來儲存Cloud Volumes ONTAP 作業系統資料（開機資料、根資料、核心資料和NVRAM）。為了規劃目的、在部署Cloud Volumes ONTAP 完更新之前、您可能需要先檢閱這些詳細資料。

- ["在Cloud Volumes ONTAP Google Cloud中檢視系統資料的預設磁碟"](#)。
- ["Google Cloud文件：資源配額"](#)

Google Cloud Compute Engine會強制執行資源使用量配額、因此您應該在部署Cloud Volumes ONTAP 時確保未達到上限。



連接器也需要系統磁碟。 ["檢視Connector預設組態的詳細資料"](#)。

## 收集網路資訊

在 Cloud Volumes ONTAP GCP 中部署時、您需要指定虛擬網路的詳細資料。您可以使用工作表向系統管理員收集資訊。

- 單節點系統的網路資訊 \*

| GCP 資訊 | 您的價值 |
|--------|------|
| 區域     |      |
| 區域     |      |
| VPC 網路 |      |
| 子網路    |      |



| GCP 資訊          | 您的價值 |
|-----------------|------|
| 防火牆原則（如果使用您自己的） |      |

- 多個區域中 HA 配對的網路資訊 \*

| GCP 資訊          | 您的價值 |
|-----------------|------|
| 區域              |      |
| 節點 1 的區域        |      |
| 節點 2 的區域        |      |
| 中介人區域           |      |
| VPC-0 和子網路      |      |
| VPC-1 和子網路      |      |
| VPC-2 和子網路      |      |
| VPC-3 和子網路      |      |
| 防火牆原則（如果使用您自己的） |      |

- 單一區域中 HA 配對的網路資訊 \*

| GCP 資訊          | 您的價值 |
|-----------------|------|
| 區域              |      |
| 區域              |      |
| VPC-0 和子網路      |      |
| VPC-1 和子網路      |      |
| VPC-2 和子網路      |      |
| VPC-3 和子網路      |      |
| 防火牆原則（如果使用您自己的） |      |

## 選擇寫入速度

Cloud Manager 可讓您選擇 Cloud Volumes ONTAP 適合的寫入速度設定、但 Google Cloud 中的高可用度（HA）配對除外。在您選擇寫入速度之前、您應該先瞭解一般與高設定之間的差異、以及使用高速寫入速度時的風險與建議。"[深入瞭解寫入速度](#)"。

## 選擇Volume使用設定檔

包含多項儲存效率功能、可減少您所需的總儲存容量。ONTAP在 Cloud Manager 中建立 Volume 時、您可以選擇啟用這些功能的設定檔、或是停用這些功能的設定檔。您應該深入瞭解這些功能、以協助您決定要使用的設定檔。

NetApp 儲存效率功能提供下列效益：

## 資源隨需配置

為主機或使用者提供比實體儲存資源池實際擁有更多的邏輯儲存設備。儲存空間不會預先配置儲存空間、而是會在寫入資料時動態分配給每個磁碟區。

## 重複資料刪除

找出相同的資料區塊、並以單一共用區塊的參考資料取代這些區塊、藉此提升效率。這項技術可消除位於同一個磁碟區的備援資料區塊、進而降低儲存容量需求。

## 壓縮

藉由壓縮主儲存設備、次儲存設備和歸檔儲存設備上磁碟區內的資料、來減少儲存資料所需的實體容量。

## GCP 中的功能需求 Cloud Volumes ONTAP

設定您的 Google Cloud Platform 網路功能、Cloud Volumes ONTAP 讓支援的系統能夠正常運作。這包括連接器和 Cloud Volumes ONTAP 整個過程的網路功能。

如果您想要部署 HA 配對、應該這樣做 ["瞭解 HA 配對如何在 GCP 中運作"](#)。

### 需求 Cloud Volumes ONTAP

GCP 必須符合下列要求。

#### 內部負載平衡器

Cloud Manager會自動建立四個Google Cloud內部負載平衡器（TCP/IP）、以管理Cloud Volumes ONTAP 傳入至該HA配對的流量。您不需要在結束時進行任何設定我們將此列為一項要求、只是告知您網路流量、並減輕任何安全顧慮。

其中一個負載平衡器用於叢集管理、一個用於儲存VM（SVM）管理、一個用於連接節點1的NAS流量、最後一個用於連接節點2的NAS流量。

每個負載平衡器的設定如下：

- 一個共享的私有IP位址
- 一次全域健全狀況檢查

根據預設、狀況檢查所使用的連接埠為63001、63002和63003。

- 一個區域TCP後端服務
- 一個區域性的udp後端服務
- 一個TCP轉送規則
- 一個udp轉送規則
- 全域存取已停用

即使預設停用全域存取、仍支援在部署後啟用IT。我們停用此功能、因為跨區域流量的延遲時間會大幅增加。我們希望確保您不會因為意外的跨區域裝載而有負面體驗。啟用此選項是專為您的業務需求所打造。

## 一個或多個區域用於HA配對

您可以跨多個區域或單一區域部署HA組態、確保資料的高可用度。建立HA配對時、Cloud Manager會提示您選擇多個區域或單一區域。

- 多個區域（建議）

跨三個區域部署 HA 組態、可確保在區域內發生故障時、仍能持續提供資料。請注意、與使用單一區域相比、寫入效能略低、但卻是最低的。

- 單一區域

當部署在單一區域時、Cloud Volumes ONTAP 使用分散配置原則的即可實現不受限制的 HA 組態。此原則可確保 HA 組態不會在區域內發生單點故障、而無需使用個別區域來實現故障隔離。

此部署模式可降低成本、因為各區域之間不需支付任何資料出口費用。

## 四個虛擬私有雲端、適用於HA配對

HA組態需要四個虛擬私有雲端（VPC）。由於 GCP 要求每個網路介面位於獨立的 VPC 網路、因此需要四台 VPC。

建立 HA 配對時、Cloud Manager 會提示您選擇四個 VPC：

- VPC-0 用於資料和節點的傳入連線
- VPC-1、VPC-2 和 VPC-3 用於節點與 HA 中介器之間的內部通訊



## HA配對的子網路

每個VPC都需要私有子網路。

如果您將Connector放在VPC-0中、則必須在子網路上啟用私有Google Access、才能存取API並啟用資料分層。

這些VPC中的子網路必須具有不同的CIDR範圍。它們不能有重疊的CIDR範圍。

## 單一節點系統適用的單一虛擬私有雲

單一節點系統需要一個 VPC 。

## 共享VPC

支援的對象包括 Google Cloud 共享 VPC 和獨立 VPC 。 Cloud Volumes ONTAP

對於單一節點系統、VPC可以是共享VPC或獨立VPC。

HA配對需要四個VPC。每個VPC都可以是共享的或獨立的。例如、VPC-0可以是共享VPC、VPC-1、VPC-2和VPC-3則可以是獨立式VPC。

共享 VPC 可讓您設定及集中管理多個專案中的虛擬網路。您可以在 主機專案 中設定共享 VPC 網路、並在 Cloud Volumes ONTAP 服務專案 中部署連接器與支援虛擬機器執行個體。 ["Google Cloud 文件：共](#)

享 VPC 總覽"。

"檢閱Connector部署所涵蓋的必要共享VPC權限"。

## VPC中的封包鏡射

"封包鏡射" 必須在部署Cloud Volumes ONTAP 了下列項目的Google Cloud VPC中停用。啟用封包鏡射時、無法正常運作。Cloud Volumes ONTAP

## 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>

"瞭解如何驗AutoSupport 證功能"。



如果您使用 HA 配對、HA 中介器不需要傳出網際網路存取。

## 私有IP位址

Cloud Manager會在Cloud Volumes ONTAP GCP中分配下列數量的私有IP位址給各個方面：

- 單一節點：3或4個私有IP位址

如果Cloud Volumes ONTAP 您使用API部署了Sf2並指定下列旗標、則可以跳過儲存VM (SVM) 管理LIF的建立：

「kipSvmManagementLif: true」

LIF 是與實體連接埠相關聯的 IP 位址。諸如VMware等管理工具需要儲存VM (SVM) 管理LIF SnapCenter。

- \* HA配對\*：14或15個私有IP位址

- VPC-0的7或8個私有IP位址

如果Cloud Volumes ONTAP 您使用API部署了Sf2並指定下列旗標、則可以跳過儲存VM (SVM) 管理LIF的建立：

「kipSvmManagementLif: true」

- VPC-1的兩個私有IP位址
- VPC-2的兩個私有IP位址
- VPC-3的三個私有IP位址

## 防火牆規則

您不需要建立防火牆規則、因為 Cloud Manager 能為您做到這一點。如果您需要使用自己的防火牆、請參閱下列防火牆規則。

請注意、HA 組態需要兩組防火牆規則：

- VPC-0 中 HA 元件的一組規則。這些規則可讓您存取 Cloud Volumes ONTAP 資料以存取資料。 [深入瞭解](#)。
- VPC-1 、 VPC-2 和 VPC-3 中的另一組 HA 元件規則。這些規則可用於 HA 元件之間的傳入和傳出通訊。 [深入瞭解](#)。

## 從 Cloud Volumes ONTAP 功能區連接到 Google Cloud Storage、以利資料分層

如果您想要將冷資料分層至 Google Cloud Storage 資源桶、Cloud Volumes ONTAP 則必須將駐留的子網路設定為私有 Google Access （如果您使用 HA 配對、則此子網路位於 VPC-0 ）。如需相關指示、請參閱 ["Google Cloud 文件：設定私有 Google Access"](#) 。

如需在 Cloud Manager 中設定資料分層所需的其他步驟、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 GCP 中的某個系統與 ONTAP 其他網路中的某個系統之間複寫資料、您必須在 VPC 與另一個網路（例如您的公司網路）之間建立 VPN 連線。

如需相關指示、請參閱 ["Google Cloud 文件：雲端 VPN 概述"](#) 。

## 連接器需求

設定您的網路、讓 Connector 能夠管理公有雲環境中的資源和程序。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、您可以從「設定」頁面指定 Proxy 伺服器。請參閱 ["將 Connector 設定為使用 Proxy 伺服器"](#) 。

## 連線至目標網路

連接器需要網路連線至您要部署 Cloud Volumes ONTAP 的 VPC 。如果您要部署 HA 配對、則 Connector 只需要連線至 VPC-0 。

如果您計畫在 Cloud Volumes ONTAP 獨立於 Connector 的 VPC 上部署物件、則需要設定 VPC 網路對等。 ["深入瞭解 VPC 網路對等關係"](#)

## 傳出網際網路存取

連接器需要存取傳出網際網路、才能管理公有雲環境中的資源和程序。

| 端點  | 目的  |
|---|---|
| <a href="https://support.netapp.com">https://support.netapp.com</a>                           | 以取得授權資訊、並將 AutoSupport 資訊傳送給 NetApp 支援部門。 |
| <a href="https://*.cloudmanager.cloud.netapp.com">https://*.cloudmanager.cloud.netapp.com</a> | 在 Cloud Manager 中提供 SaaS 功能與服務。           |

| 端點  | 目的                     |
|---|------------------------|
| https://cloudmanagerinfraprod.azurecr.io<br>https://*.blob.core.windows.net | 升級Connector及其Docker元件。 |

## 防火牆規則 Cloud Volumes ONTAP

Cloud Manager 會建立 GCP 防火牆規則、其中包含 Cloud Volumes ONTAP 運作成功所需的傳入和傳出規則。您可能需要參照連接埠進行測試、或是偏好使用自己的防火牆規則。

適用於此功能的防火牆規則 Cloud Volumes ONTAP 需要傳入和傳出規則。

如果您要部署 HA 組態、Cloud Volumes ONTAP 以下是 VPC-0 中的防火牆規則。

### 傳入規則

對於HA配對、預先定義的防火牆原則中傳入流量的來源篩選器為0.00.0.0/0。

對於單一節點系統、您可以在部署期間、為預先定義的防火牆原則選擇來源篩選器：

- **\*限定VPC\***：傳入流量的來源篩選器為VPC的子網路範圍、Cloud Volumes ONTAP 適用於該系統、以及連接器所在VPC的子網路範圍。這是建議的選項。
- **所有VPC**：傳入流量的來源篩選器為0.00.0.0/0 IP範圍。

如果您使用自己的防火牆原則、請確定您新增了所有需要與Cloud Volumes ONTAP 之通訊的網路、但同時也請務必新增這兩個位址範圍、以讓內部Google負載平衡器正常運作。這些位址分別為130.211.0.0/22和35.191.0/16。如需詳細資訊、請參閱 "[Google Cloud文件：負載平衡器防火牆規則](#)"。

| 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、以 HTTPS 存取 System Manager 網路主控台  |
| 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 | 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   |

| 傳輸協定 | 連接埠         | 目的                            |
|------|-------------|-------------------------------|
| 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    |
| TCP  | 63001-63050 | 負載平衡探針連接埠、判斷哪個節點正常（僅 HA 配對需要） |
| 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

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  |
| 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 )     |
| DHCP             | UDP       | 68     | 節點管理 LIF                      | DHCP                | 第一次設定的 DHCP 用戶端                           |

| 服務         | 傳輸協定 | 連接埠           | 來源                              | 目的地           | 目的                             |
|------------|------|---------------|---------------------------------|---------------|--------------------------------|
| 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                       |

### VPC-1 、 VPC-2 和 VPC-3 的防火牆規則

在 GCP 中、HA 組態會部署在四個 VPC 上。VPC-0 中 HA 組態所需的防火牆規則為 [以上所列 Cloud Volumes ONTAP 的 for 列舉](#)。

同時、Cloud Manager針對VPC-1、VPC-2和VPC-3中的執行個體所建立的預先定義防火牆規則、可透過\_all\_傳輸協定和連接埠進行入侵通訊。這些規則可在HA節點之間進行通訊。

HA節點與HA中介器之間的通訊會透過連接埠3260 (iSCSI) 進行。

### Connector 的防火牆規則

連接器的防火牆規則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 Web 瀏覽器到本機使用者介面的 HTTP 存取 |
| 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  |

## 傳出規則

連接器的預先定義防火牆規則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 的預先定義防火牆規則包括下列傳出規則。

| 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  |
|------------------------|-------|-------|------------------------|---|
| API 呼叫與 AutoSupport 功能 | HTTPS | 443.. | 傳出網際網路和 ONTAP 叢集管理 LIF | API會呼叫GCP和ONTAP VMware、Cloud Data Sense、勒索軟體服務、並將AutoSupport 此訊息傳送給NetApp |
| DNS                    | UDP   | 53.   | DNS                    | 用於 Cloud Manager 的 DNS 解析   |

## 在GCP中規劃VPC服務控制

選擇使用VPC服務控制來鎖定Google Cloud環境時、您應該瞭解Cloud Manager和Cloud Volumes ONTAP 效益分析如何與Google Cloud API互動、以及如何設定服務邊界以部署Cloud Manager和Cloud Volumes ONTAP 效益分析。

VPC服務控管可讓您控制在信任邊界之外存取Google管理的服務、封鎖來自不信任位置的資料存取、並降低未獲授權的資料傳輸風險。 ["深入瞭解Google Cloud VPC服務控制"](#)。

### NetApp服務如何與VPC服務控制通訊

諸如Cloud Central和Cloud Manager等NetApp服務可直接與Google Cloud API通訊。這可能是從Google Cloud 外部的IP位址觸發（例如從api.services.cloud.netapp.com）、或從指派給Cloud Manager Connector的內部位址觸發。

視連接器的部署風格而定、您可能需要針對服務邊界進行某些例外。

## 映像

利用NetApp管理的GCP專案中的影像、即可同時Cloud Volumes ONTAP 使用此功能。如果Cloud Volumes ONTAP 貴組織的原則禁止使用組織內部未裝載的映像、則這可能會影響Cloud Manager Connector和功能的部署。

您可以使用手動安裝方法手動部署Connector、Cloud Volumes ONTAP 但也需要從NetApp專案中擷取影像。您必須提供允許的清單、才能部署連接器和Cloud Volumes ONTAP 功能表。

### 部署Connector

部署Connector的使用者必須能夠參考專案ID *NetApp-cloudmanag\_\_* 中裝載的映像、以及專案編號 *\_14190056516*。

### 部署Cloud Volumes ONTAP 功能

- Cloud Manager服務帳戶必須參考專案ID *NetApp-cloudmanag\_\_* 中所託管的映像、以及服務專案中的專案編號 *\_14190056516*。
- 預設Google API服務代理程式的服務帳戶必須參考專案ID *NetApp-cloudmanag\_\_* 中所裝載的映像、以及服務專案中的專案編號 *\_14190056516*。

以下是使用VPC服務控制擷取這些影像所需的規則範例。

### VPC服務控制周邊原則

原則允許VPC服務控制規則集例外。如需原則的詳細資訊、請參閱 "[GCP VPC服務控制原則文件](#)"。

若要設定Cloud Manager所需的原則、請瀏覽至組織內部的VPC服務控制周邊、然後新增下列原則。這些欄位應符合VPC服務控制原則頁面中提供的選項。另請注意、\* all \*規則是必要的、且\*或\*參數應用於規則集中。

### 入口規則

```
From:
  Identities:
    [User Email Address]
  Source > All sources allowed
To:
  Projects =
    [Service Project]
  Services =
    Service name: iam.googleapis.com
      Service methods: All actions
    Service name: compute.googleapis.com
      Service methods: All actions
```

或

```
From:
  Identities:
    [User Email Address]
  Source > All sources allowed
To:
  Projects =
    [Host Project]
  Services =
    Service name: compute.googleapis.com
    Service methods: All actions
```

或

```
From:
  Identities:
    [Service Project Number]@cloudservices.gserviceaccount.com
  Source > All sources allowed
To:
  Projects =
    [Service Project]
    [Host Project]
  Services =
    Service name: compute.googleapis.com
    Service methods: All actions
```

出口規則

```
From:
  Identities:
    [Service Project Number]@cloudservices.gserviceaccount.com
To:
  Projects =
    14190056516
  Service =
    Service name: compute.googleapis.com
    Service methods: All actions
```



上述專案編號是NetApp用來儲存Connector和Cloud Volumes ONTAP for the SURO影像的專案\_NetApp-cloudmanag\_\_。

## 建立資料分層與備份的服務帳戶

下列兩種用途需要Google Cloud服務帳戶：Cloud Volumes ONTAP第一個是啟用時 "[資料分層](#)" 將冷資料分層至Google Cloud中的低成本物件儲存設備。第二個是啟用時 "[Cloud Backup Service](#)" 將磁碟區備份至低成本的物件儲存設備。

使用服務帳戶存取及管理階層資料的儲存庫、以及另一個儲存庫進行備份。Cloud Volumes ONTAP

您可以設定一個服務帳戶、並將其用於這兩種用途。服務帳戶必須具有\*儲存設備管理\*角色。

### 步驟

1. 在Google Cloud主控台中、"[前往「服務帳戶」頁面](#)"。
2. 選取您的專案。
3. 按一下「建立服務帳戶」、並提供必要資訊。
  - a. 服務帳戶詳細資料：輸入名稱和說明。
  - b. 授予此服務帳戶專案存取權：選取\*儲存管理員\*角色。



- c. 授予使用者此服務帳戶的存取權：將Connector服務帳戶新增為\_Service Account User\_至此新的服務帳戶。

此步驟僅適用於資料分層。不需要Cloud Backup Service 使用此功能。

Create service account

✓ Service account details

✓ Grant this service account access to project (optional)

3 Grant users access to this service account (optional)

Grant access to users or groups that need to perform actions as this service account. [Learn more](#)

Service account users role

netapp-cloud-manager@iam.gserviceaccount.com

?

Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role

?

Grant users the permission to administer this service account

DONE

CANCEL

建立Cloud Volumes ONTAP 一套運作環境時、您稍後需要選擇服務帳戶。



Details and Credentials

default-project

Google Cloud Project

gcp-sub2

Marketplace Subscription

Edit Project

Details

Working Environment Name (Cluster Name)

cloudvolumesontap

Service Account

Service Account Name

account1

Add Labels

Optional Field | Up to four labels

Credentials

User Name

admin

Password

Confirm Password

## 搭配 Cloud Volumes ONTAP 使用客戶管理的加密金鑰

雖然Google Cloud Storage會在資料寫入磁碟之前先加密資料、但您可以使用Cloud Manager API來建立Cloud Volumes ONTAP 使用\_客戶管理的加密金鑰\_的支援系統。這些是您使用 Cloud Key Management Service 在 GCP 中產生及管理的金鑰。

### 步驟

1. 確保Cloud Manager Connector服務帳戶在專案層級（儲存金鑰的專案）擁有正確的權限。

權限由提供 "[Cloud Manager Yaml檔案](#)" 根據預設、但如果您使用雲端金鑰管理服務的替代專案、則可能無法套用。

權限如下：

```
- cloudkms.cryptoKeyVersions.list
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
```

2. 確認的服務帳戶 "[Google Compute Engine服務代理程式](#)" 具有金鑰的Cloud KMS Encrypter/Dec供 解密權限。

服務帳戶名稱使用下列格式：「service-[service\_project\_number]@ compute-system.iam.gserviceaccount.com」。

## "Google Cloud文件：使用IAM搭配Cloud KMS使用-授予資源角色"

3. 若要取得金鑰的「ID」、請叫用「/GCP / VSA /中繼資料/ GCP加密金鑰」API呼叫的「Get」命令、或在GCP主控台的金鑰上選擇「Copy Resource Name」（複製資源名稱）。
4. 如果使用客戶管理的加密金鑰和分層資料來物件儲存設備、Cloud Manager會嘗試使用相同的金鑰來加密持續磁碟。但您必須先啟用Google Cloud Storage儲存桶、才能使用這些金鑰：
  - a. 請依照下列步驟尋找Google Cloud Storage服務代理程式 "[Google Cloud文件：取得Cloud Storage服務代理程式](#)"。
  - b. 瀏覽至加密金鑰、並指派具有Cloud KMS Encrypter/Decrypter權限的Google Cloud Storage服務代理程式。

如需詳細資訊、請參閱 "[Google Cloud文件：使用客戶管理的加密金鑰](#)"

5. 建立工作環境時、請將「GcpEncryption」參數搭配API要求使用。

。範例 \*

```
"gcpEncryptionParameters": {  
  "key": "projects/project-1/locations/us-east4/keyRings/keyring-  
1/cryptoKeys/generatedkey1"  
}
```

請參閱 "[Cloud Manager自動化文件](#)" 如需使用「GcpEncryption」參數的詳細資訊、

## 在Cloud Volumes ONTAP Google Cloud中設定適用於此技術的授權

決定Cloud Volumes ONTAP 要搭配使用哪種授權選項之後、您必須先執行幾個步驟、才能在建立新的工作環境時選擇授權選項。

### Freemium

選擇Freemium產品、即可免費使用Cloud Volumes ONTAP 多達500 GiB的配置容量。 "[深入瞭解Freemium產品](#)"。

#### 步驟

1. 在「畫版」頁面上、按一下「新增工作環境」、然後依照Cloud Manager中的步驟進行。
  - a. 在\*詳細資料與認證\*頁面上、按一下\*編輯認證>新增訂閱\*、然後依照提示訂閱Google Cloud Marketplace中的隨用隨付方案。

除非您超過500 GiB的已配置容量、系統會自動轉換為、否則不會透過市場訂閱付費 "[Essentials套件](#)"。

- b. 返回Cloud Manager之後、當您進入「充電方法」頁面時、請選取\* Freemium \*。

Select Charging Method

|   |             |   |
|---|-------------|---|
| <input type="radio"/> Professional                        | By capacity | ▼ |
| <input type="radio"/> Essential                           | By capacity | ▼ |
| <input checked="" type="radio"/> Freemium (Up to 500 GiB) | By capacity | ▼ |
| <input type="radio"/> Per Node                            | By node     | ▼ |

"請參閱逐步指示Cloud Volumes ONTAP 、在Google Cloud中啟動「功能不全」"。

### 容量型授權

容量型授權可讓您針對Cloud Volumes ONTAP 容量的每個TiB付費。容量型授權的形式為\_package\_：Essentials套件或Professional套件。

Essentials和Professional套件可搭配下列消費模式使用：

- 向NetApp購買的授權（BYOL）
- 從Google Cloud Marketplace訂閱時數小時隨付（PAYGO）
- 年度合約

"深入瞭解容量型授權"。

下列各節將說明如何開始使用這些消費模式。

### BYOL

事先向NetApp購買授權（BYOL）、即可在Cloud Volumes ONTAP 任何雲端供應商部署支援系統。

#### 步驟

1. "請聯絡NetApp銷售人員以取得授權"
2. "將您的NetApp支援網站帳戶新增至Cloud Manager"

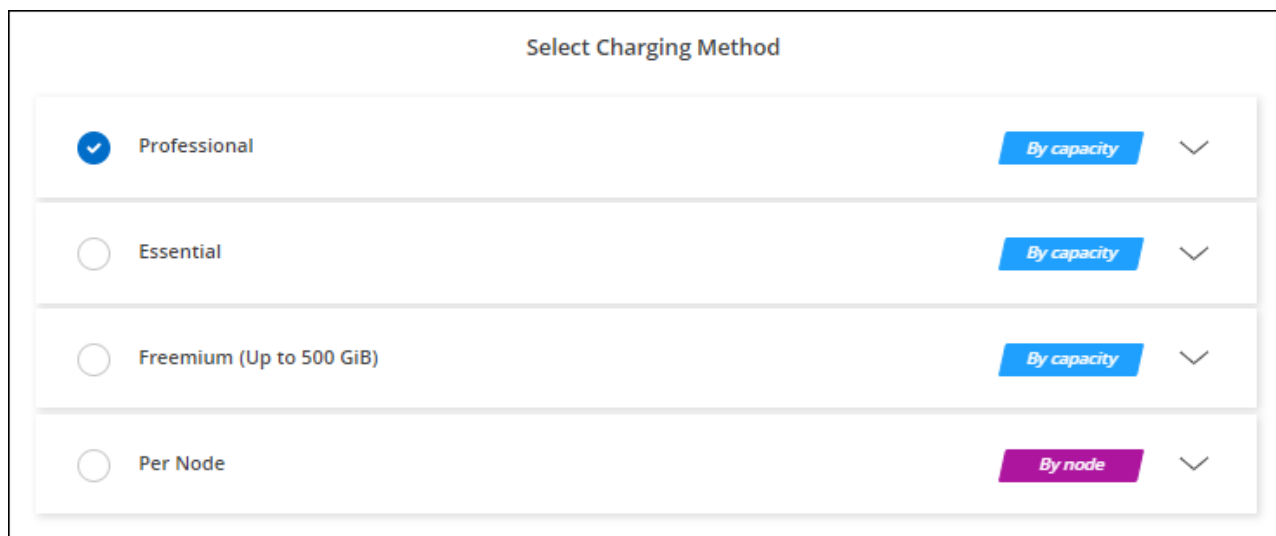
Cloud Manager會自動查詢NetApp的授權服務、以取得與您NetApp支援網站帳戶相關之授權的詳細資料。如果沒有錯誤、Cloud Manager會自動將授權新增至Digital Wallet。

您的授權必須先從Digital Wallet取得、才能搭配Cloud Volumes ONTAP 使用。如有需要、您可以 "手動將授權新增至Digital Wallet"。

3. 在「畫版」頁面上、按一下「新增工作環境」、然後依照Cloud Manager中的步驟進行。
  - a. 在\*詳細資料與認證\*頁面上、按一下\*編輯認證>新增訂閱\*、然後依照提示訂閱Google Cloud Marketplace中的隨用隨付方案。

您向NetApp購買的授權一律會先收取費用、但如果您超過授權容量或授權到期、則會從市場的每小時費率中收取費用。

- b. 返回Cloud Manager之後、請在前往「充電方法」頁面時、選取容量型套件。



| Select Charging Method                         |             |
|--|-------------|
| <input checked="" type="radio"/> Professional  | By capacity |
| <input type="radio"/> Essential                | By capacity |
| <input type="radio"/> Freemium (Up to 500 GiB) | By capacity |
| <input type="radio"/> Per Node                 | By node     |

"請參閱逐步指示Cloud Volumes ONTAP、在Google Cloud中啟動「功能不全」"。

#### PAYGO訂閱

從雲端供應商的市場訂閱優惠、每小時支付一次。

當您建立Cloud Volumes ONTAP 一個可運作的環境時、Cloud Manager會提示您訂閱Google Cloud Marketplace提供的合約。該訂閱之後會與工作環境建立關聯、以便進行充電。您可以在其他工作環境中使用相同的訂閱。

#### 步驟

1. 在「畫版」頁面上、按一下「新增工作環境」、然後依照Cloud Manager中的步驟進行。
  - a. 在\*詳細資料與認證\*頁面上、按一下\*編輯認證>新增訂閱\*、然後依照提示訂閱Google Cloud Marketplace中的隨用隨付方案。
  - b. 返回Cloud Manager之後、請在前往「充電方法」頁面時、選取容量型套件。

Select Charging Method

☒ Professional

By capacity

▼

☐ Essential

By capacity

▼

☐ Freemium (Up to 500 GiB)

By capacity

▼

☐ Per Node

By node

▼

"請參閱逐步指示Cloud Volumes ONTAP 、在Google Cloud中啟動「功能不全」"。



您可以從「設定」>「認證」頁面管理與您帳戶相關的Google Cloud Marketplace訂閱。 "[瞭解如何管理您的Google Cloud認證與訂閱](#)"

#### 年度合約

購買年度合約、每年支付Cloud Volumes ONTAP 一份銷售費。

#### 步驟

1. 請聯絡您的NetApp銷售代表以購買年度合約。

合約可在Google Cloud Marketplace以\_Private\_優惠形式提供。

在NetApp與您分享私人優惠之後、您可以在工作環境建立期間、從Google Cloud Marketplace訂閱年度方案。

2. 在「畫版」頁面上、按一下「新增工作環境」、然後依照Cloud Manager中的步驟進行。
  - a. 在\*詳細資料與認證\*頁面上、按一下\*編輯認證>新增訂閱\*、然後依照提示在Google Cloud Marketplace訂閱年度計畫。
  - b. 在Google Cloud中、選取與您的帳戶共享的年度計畫、然後按一下\*訂閱\*。
  - c. 返回Cloud Manager之後、請在前往「充電方法」頁面時、選取容量型套件。

Select Charging Method

|  |             |   |
|--|-------------|---|
| <input checked="" type="radio"/> Professional  | By capacity | ▼ |
| <input type="radio"/> Essential                | By capacity | ▼ |
| <input type="radio"/> Freemium (Up to 500 GiB) | By capacity | ▼ |
| <input type="radio"/> Per Node                 | By node     | ▼ |

"請參閱逐步指示Cloud Volumes ONTAP 、在Google Cloud中啟動「功能不全」"。

### Keystone Flex 訂閱

Keystone Flex訂閱是一種隨需付費的訂閱型服務。 "深入瞭解Keystone Flex訂閱"。

#### 步驟

1. 如果您尚未訂閱、 "請聯絡NetApp"
2. <mailto:ng-keystone-success@netapp.com> [聯絡NetApp]、以一或多個Keystone Flex訂閱授權您的Cloud Manager使用者帳戶。
3. NetApp授權您的帳戶之後、 "連結您的訂閱內容以供Cloud Volumes ONTAP 搭配使用"。
4. 在「畫版」頁面上、按一下「新增工作環境」、然後依照Cloud Manager中的步驟進行。
  - a. 當系統提示您選擇充電方法時、請選取Keystone Flex訂閱充電方法。

Select Charging Method

☒ **Keystone** By capacity ^

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1 v

☐ **Professional** By capacity v

☐ **Essential** By capacity v

☐ **Freemium (Up to 500 GiB)** By capacity v

☐ **Per Node** By node v

"請參閱逐步指示[Cloud Volumes ONTAP](#)、在Google Cloud中啟動「功能不全」"。

## 在 **Cloud Volumes ONTAP GCP** 中啟動

您可以 **Cloud Volumes ONTAP** 在單一節點組態中或在 Google Cloud Platform 中以 HA 配對的形式啟動功能。

開始之前

您需要下列項目才能建立工作環境。

- 已啟動並執行的連接器。
  - 您應該擁有 "[與工作區相關的連接器](#)"。
  - "[您應該隨時準備好讓 Connector 保持運作](#)"。
  - 與 Connector 相關的服務帳戶 "[應具備最新權限](#)"。
- 瞭解您要使用的組態。

您應該先選擇組態、然後從系統管理員取得GCP網路資訊、以做好準備。如需詳細資訊、請參閱 "[規劃 Cloud Volumes ONTAP 您的需求組態](#)"。

- 瞭解設定Cloud Volumes ONTAP 驗證功能所需的條件。

"瞭解如何設定授權"。

- Google Cloud API應該是 ["在您的專案中啟用"](#)：
  - Cloud Deployment Manager V2 API
  - 雲端記錄 API
  - Cloud Resource Manager API
  - 運算引擎 API
  - 身分識別與存取管理（IAM）API

在 **GCP** 中啟動單一節點系統

在 Cloud Manager 中建立工作環境、以在 Cloud Volumes ONTAP GCP 中推出功能

步驟

1. [\[\[訂閱\]](#)在「畫版」頁面上、按一下「新增工作環境」、然後依照提示進行。
2. \* 選擇位置 \*：選擇 \* Google Cloud \* 和 \* Cloud Volumes ONTAP
3. 如果出現提示、["建立連接器"](#)。
4. 詳細資料與認證：選取專案、指定叢集名稱、選擇性地選取服務帳戶、選擇性地新增標籤、然後指定認證資料。

下表說明您可能需要指導的欄位：

| 欄位       | 說明   |
|----------|--|
| 工作環境名稱   | Cloud Manager 會使用工作環境名稱來命名 Cloud Volumes ONTAP 支援系統和 GCP VM 執行個體。如果您選取該選項、它也會使用名稱做為預先定義安全性群組的前置詞。  |
| 服務帳戶名稱   | 如果您打算使用 <a href="#">"資料分層"</a> 或 <a href="#">"雲端備份"</a> 有了這個功能、您就需要啟用*服務帳戶*、並選取具有預先定義儲存管理員角色的服務帳戶。Cloud Volumes ONTAP <a href="#">"瞭解如何建立服務帳戶"</a> 。   |
| 新增標籤     | 標籤是 GCP 資源的中繼資料。Cloud Manager 會將標籤新增 Cloud Volumes ONTAP 至與系統相關的支援系統和 GCP 資源。建立工作環境時、您最多可以從使用者介面新增四個標籤、然後在建立之後新增更多標籤。請注意、在建立工作環境時、API 不會限制您使用四個標籤。如需標籤的相關資訊、請參閱 <a href="#">"Google Cloud 文件：標示資源"</a> 。 |
| 使用者名稱和密碼 | 這些是Cloud Volumes ONTAP 適用於整個叢集管理員帳戶的認證資料。您可以使用這些認證資料、Cloud Volumes ONTAP 透過 System Manager 或其 CLI 連線至功能驗證。保留預設的_admin_使用者名稱、或將其變更為自訂使用者名稱。   |



| 欄位   | 說明  |
|------|---|
| 編輯專案 | <p>選取 Cloud Volumes ONTAP 您要駐留的專案。預設專案是 Cloud Manager 所在的專案。</p> <p>如果您在下拉式清單中沒有看到任何其他專案、則表示您尚未將 Cloud Manager 服務帳戶與其他專案建立關聯。前往 Google Cloud 主控台、開啟 IAM 服務、然後選取專案。將具有 Cloud Manager 角色的服務帳戶新增至該專案。您必須針對每個專案重複此步驟。</p> <div style="display: flex; align-items: center; margin-top: 10px;">  <div> <p>這是您為 Cloud Manager 設定的服務帳戶、<a href="#">"如本頁所述"</a>。</p> </div> </div> <p>按一下 * 「新增訂閱」 * 、將選取的認證資料與訂閱建立關聯。</p> <p>若要建立隨用隨付 Cloud Volumes ONTAP 的功能性系統、您需要從 Cloud Volumes ONTAP GCP Marketplace 選擇與訂閱功能相關的 GCP 專案。</p> |

下列影片說明如何將隨用隨付服務市場訂閱關聯至GCP專案。或者、請依照中的步驟訂閱 ["將 Marketplace 訂閱與 GCP 認證建立關聯"](#) 區段。

► [https://docs.netapp.com/zh-tw/cloud-manager-cloud-volumes-ontap//media/video\\_subscribing\\_gcp.mp4](https://docs.netapp.com/zh-tw/cloud-manager-cloud-volumes-ontap//media/video_subscribing_gcp.mp4)

(video)

5. \* 服務 \*：選取您要在此系統上使用的服務。若要選取「雲端備份」或使用分層、您必須在步驟3中指定「服務帳戶」。
6. 位置與連線：選擇位置、選擇防火牆原則、並確認與Google Cloud儲存設備的網路連線、以進行資料分層。

下表說明您可能需要指導的欄位：

| 欄位         | 說明   |
|------------|--|
| 連線驗證       | 若要將冷資料分層至Google Cloud Storage儲存庫、Cloud Volumes ONTAP 必須將駐留的子網路設定為私有Google Access。如需相關指示、請參閱 <a href="#">"Google Cloud 文件：設定私有 Google Access"</a> 。   |
| 產生的防火牆原則   | 如果讓Cloud Manager為您產生防火牆原則、您必須選擇允許流量的方式： <ul style="list-style-type: none"><li>• 如果您選擇*選取的VPC only（僅VPC）*、則傳入流量的來源篩選器為所選VPC的子網路範圍、以及連接器所在VPC的子網路範圍。這是建議的選項。</li><li>• 如果您選擇*所有VPC*、傳入流量的來源篩選器為0.0.0.0/0 IP範圍。</li></ul> |
| 使用現有的防火牆原則 | 如果您使用現有的防火牆原則、請確定其中包含必要的規則。 <a href="#">"深入瞭解Cloud Volumes ONTAP 解適用於此功能的防火牆規則"</a> 。  |

7. 充電方法與NSS帳戶：指定您要搭配此系統使用的收費選項、然後指定NetApp支援網站帳戶。
  - ["深入瞭解Cloud Volumes ONTAP 解適用於此功能的授權選項"](#)。
  - ["瞭解如何設定授權"](#)。
8. \* 預先設定的套件 \*：選取其中一個套件以快速部署 Cloud Volumes ONTAP 某個作業系統、或按一下 \* 建立我自己的組態 \*。

如果您選擇其中一個套件、則只需指定一個 Volume、然後檢閱並核准組態。

9. 授權：視Cloud Volumes ONTAP 需要變更此版本、然後選取機器類型。



如果所選版本有較新的發行候選版本、一般可用度或修補程式版本、Cloud Manager 會在建立工作環境時、將系統更新至該版本。例如、如果您選擇Cloud Volumes ONTAP 了「更新」功能、就會進行更新。更新不會從一個版本發生到另一個版本、例如從 9.6 到 9.7。

10. \* 基礎儲存資源 \*：選擇初始 Aggregate 的設定：每個磁碟的磁碟類型和大小。

磁碟類型適用於初始磁碟區。您可以為後續磁碟區選擇不同的磁碟類型。

磁碟大小適用於初始 Aggregate 中的所有磁碟、以及 Cloud Manager 在使用簡易資源配置選項時所建立的任何其他集合體。您可以使用進階配置選項、建立使用不同磁碟大小的集合體。

如需選擇磁碟類型和大小的說明、請參閱 ["在 GCP 中調整系統規模"](#)。

11. \* 寫入速度與 WORM \*：選擇 \* 正常 \* 或 \* 高速 \* 寫入速度、並視需要啟動一次寫入、多次讀取（WORM）儲存設備。

只有單一節點系統才支援選擇寫入速度。

["深入瞭解寫入速度"](#)。

如果啟用雲端備份或啟用資料分層、則無法啟用WORM。

["深入瞭解 WORM 儲存設備"](#)。

12. \* Google Cloud Platform 中的資料分層 \*：選擇是否要在初始 Aggregate 上啟用資料分層、選擇階層式資料的儲存類別、然後選擇具有預先定義儲存管理角色的服務帳戶（Cloud Volumes ONTAP 適用於更新版本的更新版本）、或是選擇 GCP 帳戶（Cloud Volumes ONTAP 不適用於功能表 9.6）。

請注意下列事項：

- Cloud Manager 會在 Cloud Volumes ONTAP 整個過程中設定服務帳戶。此服務帳戶提供資料分層至 Google Cloud Storage 儲存庫的權限。請務必將 Connector 服務帳戶新增為分層服務帳戶的使用者、否則您將無法從 Cloud Manager 選取該帳戶。
- 如需新增 GCP 帳戶的說明、請參閱 ["設定和新增 GCP 帳戶、以便使用 9.6 進行資料分層"](#)。
- 您可以在建立或編輯磁碟區時、選擇特定的磁碟區分層原則。
- 如果停用資料分層、您可以在後續的 Aggregate 上啟用、但您需要關閉系統、並從 GCP 主控台新增服務帳戶。

["深入瞭解資料分層"](#)。

13. \* 建立 Volume \*：輸入新磁碟區的詳細資料、或按一下 \* 跳過 \*。

["瞭解支援的用戶端傳輸協定和版本"](#)。

本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

| 欄位                   | 說明  |
|----------------------|---|
| 尺寸                   | 您可以輸入的最大大小、主要取決於您是否啟用精簡配置、這可讓您建立比目前可用實體儲存容量更大的磁碟區。  |
| 存取控制（僅適用於 NFS）       | 匯出原則會定義子網路中可存取磁碟區的用戶端。根據預設、Cloud Manager 會輸入一個值、讓您存取子網路中的所有執行個體。  |
| 權限與使用者 / 群組（僅限 CIFS） | 這些欄位可讓您控制使用者和群組（也稱為存取控制清單或 ACL）的共用存取層級。您可以指定本機或網域 Windows 使用者或群組、或 UNIX 使用者或群組。如果您指定網域 Windows 使用者名稱、則必須使用網域\使用者名稱格式來包含使用者的網域。                              |
| Snapshot 原則          | Snapshot 複製原則會指定自動建立的 NetApp Snapshot 複本的頻率和數量。NetApp Snapshot 複本是一種不影響效能的時間點檔案系統映像、需要最少的儲存容量。您可以選擇預設原則或無。您可以針對暫時性資料選擇「無」：例如、Microsoft SQL Server 的 Tempdb。 |
| 進階選項（僅適用於 NFS）       | 為磁碟區選取 NFS 版本：NFSv3 或 NFSv3。  |

| 欄位                     | 說明  |
|------------------------|---|
| 啟動器群組和 IQN（僅適用於 iSCSI） | iSCSI 儲存目標稱為 LUN（邏輯單元）、以標準區塊裝置的形式呈現給主機。啟動器群組是 iSCSI 主機節點名稱的表格、可控制哪些啟動器可存取哪些 LUN。iSCSI 目標可透過標準乙太網路介面卡（NIC）、TCP 卸載引擎（TOE）卡（含軟體啟動器）、整合式網路介面卡（CNA）或專用主機匯流排介面卡（HBA）連線至網路、並由 iSCSI 合格名稱（IQN）識別。建立 iSCSI Volume 時、Cloud Manager 會自動為您建立 LUN。我們只要在每個磁碟區建立一個 LUN、就能輕鬆完成工作、因此不需要管理。建立磁碟區之後、 <a href="#">"使用 IQN 從主機連線至 LUN"</a> 。 |

下圖顯示 CIFS 傳輸協定的「Volume」（磁碟區）頁面：

### Volume Details, Protection & Protocol

#### Details & Protection

Volume Name:

Size (GB):

Snapshot Policy: default

Default Policy

#### Protocol

NFS
CIFS
iSCSI

Share name:

Permissions: Full Control

Users / Groups:

Valid users and groups separated by a semicolon

14. \* CIFS 設定 \*：如果您選擇 CIFS 傳輸協定、請設定 CIFS 伺服器。

| 欄位                       | 說明  |
|--------------------------|---|
| DNS 主要和次要 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。如果您要設定 Google Managed Active Directory、AD 預設可透過 169.254.169.254 IP 位址存取。  |
| 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」。若要將 Google 託管 Microsoft AD 設定為 Cloud Volumes ONTAP AD 伺服器以供使用、請在此欄位中輸入 * OU=computers,OU=Cloud *<br><a href="https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units">https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units</a> ["Google Cloud 文件：Google 託管 Microsoft AD 的組織單位"] |

| 欄位      | 說明   |
|---------|--|
| DNS 網域  | 適用於整個儲存虛擬 Cloud Volumes ONTAP 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 | 選擇 * 使用 Active Directory 網域 * 來使用 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。請注意、您只能在建立 CIFS 伺服器時設定 NTP 伺服器。您建立 CIFS 伺服器之後、就無法進行設定。 |

15. \* 使用率設定檔、磁碟類型及分層原則 \*：視需要選擇是否要啟用儲存效率功能、並變更磁碟區分層原則。

如需詳細資訊、請參閱 ["瞭解 Volume 使用量設定檔"](#) 和 ["資料分層總覽"](#)。

16. \* 審查與核准 \*：檢閱並確認您的選擇。

- 檢閱組態的詳細資料。
- 按一下 \* 更多資訊 \* 以檢閱 Cloud Manager 將購買的支援與 GCP 資源詳細資料。
- 選取「\* 我瞭解 ... \*」核取方塊。
- 按一下「\* 執行 \*」。

Cloud Manager 部署 Cloud Volumes ONTAP 了這個功能。您可以追蹤時間表的進度。

如果您在部署 Cloud Volumes ONTAP 此系統時遇到任何問題、請檢閱故障訊息。您也可以選取工作環境、然後按一下 \* 重新建立環境 \*。

如需其他協助、請前往 ["NetApp Cloud Volumes ONTAP 支援"](#)。

完成後

- 如果您已配置 CIFS 共用區、請授予使用者或群組檔案和資料夾的權限、並確認這些使用者可以存取共用區並建立檔案。
- 如果您要將配額套用至磁碟區、請使用 System Manager 或 CLI。

配額可讓您限制或追蹤使用者、群組或 qtree 所使用的磁碟空間和檔案數量。

在 **GCP** 中啟動 **HA** 配對

在 Cloud Manager 中建立工作環境、以在 Cloud Volumes ONTAP GCP 中推出功能

步驟

- 在「畫版」頁面上、按一下「\* 新增工作環境 \*」、然後依照提示進行。
- \* 選擇位置 \*：選擇 \* Google Cloud \* 和 \* Cloud Volumes ONTAP 《\*》 HA \*。
- \* 詳細資料與認證 \*：選取專案、指定叢集名稱、選擇性地選取服務帳戶、選擇性地新增標籤、然後指定認證資料。

下表說明您可能需要指導的欄位：

| 欄位       | 說明   |
|----------|--|
| 工作環境名稱   | Cloud Manager 會使用工作環境名稱來命名 Cloud Volumes ONTAP 支援系統和 GCP VM 執行個體。如果您選取該選項、它也會使用名稱做為預先定義安全性群組的前置詞。  |
| 服務帳戶名稱   | 如果您打算使用 "分層" 或 "雲端備份" 服務、您必須啟用 * 服務帳戶 * 交換器、然後選取具有預先定義儲存管理角色的服務帳戶。   |
| 新增標籤     | 標籤是 GCP 資源的中繼資料。Cloud Manager 會將標籤新增 Cloud Volumes ONTAP 至與系統相關的支援系統和 GCP 資源。建立工作環境時、您最多可以從使用者介面新增四個標籤、然後在建立之後新增更多標籤。請注意、在建立工作環境時、API 不會限制您使用四個標籤。如需標籤的相關資訊、請參閱 <a href="#">"Google Cloud 文件：標示資源"</a> 。   |
| 使用者名稱和密碼 | 這些是 Cloud Volumes ONTAP 適用於整個叢集管理員帳戶的認證資料。您可以使用這些認證資料、Cloud Volumes ONTAP 透過 System Manager 或其 CLI 連線至功能驗證。保留預設的 _admin_ 使用者名稱、或將其變更為自訂使用者名稱。  |
| 編輯專案     | <p>選取 Cloud Volumes ONTAP 您要駐留的專案。預設專案是 Cloud Manager 所在的專案。</p> <p>如果您在下拉式清單中沒有看到任何其他專案、則表示您尚未將 Cloud Manager 服務帳戶與其他專案建立關聯。前往 Google Cloud 主控台、開啟 IAM 服務、然後選取專案。將具有 Cloud Manager 角色的服務帳戶新增至該專案。您必須針對每個專案重複此步驟。</p> <div style="display: flex; align-items: center; margin-top: 10px;">  <div> <p>這是您為 Cloud Manager 設定的服務帳戶、<a href="#">"如本頁所述"</a>。</p> <p>按一下 * 「新增訂閱」 * 、將選取的認證資料與訂閱建立關聯。</p> <p>若要建立隨用隨付 Cloud Volumes ONTAP 的功能性系統、您需要從 Cloud Volumes ONTAP GCP Marketplace 選擇與訂閱功能相關的 GCP 專案。</p> </div> </div> |

下列影片說明如何將隨用隨付服務市場訂閱關聯至 GCP 專案。或者、請依照中的步驟訂閱 ["將 Marketplace 訂閱與 GCP 認證建立關聯"](#) 區段。

► [https://docs.netapp.com/zh-tw/cloud-manager-cloud-volumes-ontap//media/video\\_subscribing\\_gcp.mp4](https://docs.netapp.com/zh-tw/cloud-manager-cloud-volumes-ontap//media/video_subscribing_gcp.mp4)



(video)

4. \* 服務 \* : 選取您要在此系統上使用的服務。若要選取「雲端備份」或使用分層、您必須在步驟3中指定「服務帳戶」。
5. \* HA 部署模式 \* : 選擇多個區域（建議）或單一區域進行 HA 組態。然後選取區域和區域。

["深入瞭解 HA 部署模式"](#)。

6. \* 連線能力 \* : 為 HA 組態選取四個不同的 VPC、在每個 VPC 中選取一個子網路、然後選擇防火牆原則。

["深入瞭解網路需求"](#)。

7. 充電方法與**NSS**帳戶: 指定您要搭配此系統使用的收費選項、然後指定NetApp支援網站帳戶。

- ["深入瞭解Cloud Volumes ONTAP 解適用於此功能的授權選項"](#)。

- ["瞭解如何設定授權"](#)。

8. \* 預先設定的套件 \* : 選取其中一個套件以快速部署 Cloud Volumes ONTAP 某個作業系統、或按一下 \* 建立我自己的組態 \* 。

如果您選擇其中一個套件、則只需指定一個 Volume、然後檢閱並核准組態。

9. 授權: 視Cloud Volumes ONTAP 需要變更此版本、然後選取機器類型。



如果所選版本有較新的發行候選版本、一般可用度或修補程式版本、Cloud Manager 會在建立工作環境時、將系統更新至該版本。例如、如果您選擇Cloud Volumes ONTAP 了「更新」功能、就會進行更新。更新不會從一個版本發生到另一個版本、例如從 9.6 到 9.7。

10. \* 基礎儲存資源 \* : 選擇初始 Aggregate 的設定: 每個磁碟的磁碟類型和大小。

磁碟類型適用於初始磁碟區。您可以為後續磁碟區選擇不同的磁碟類型。

磁碟大小適用於初始 Aggregate 中的所有磁碟、以及 Cloud Manager 在使用簡易資源配置選項時所建立的任何其他集合體。您可以使用進階配置選項、建立使用不同磁碟大小的集合體。

如需選擇磁碟類型和大小的說明、請參閱 ["在 GCP 中調整系統規模"](#)。

11. \* WORM \* : 視需要啟動一次寫入、多次讀取（WORM）儲存設備。

如果資料分層已啟用、則無法啟用 WORM。 ["深入瞭解 WORM 儲存設備"](#)。

12. \* Google Cloud Platform 中的資料分層 \* : 選擇是否要在初始 Aggregate 上啟用資料分層、選擇階層式資料的儲存類別、然後選取具有預先定義儲存管理角色的服務帳戶。

請注意下列事項:

- Cloud Manager 會在 Cloud Volumes ONTAP 整個過程中設定服務帳戶。此服務帳戶提供資料分層至 Google Cloud Storage 儲存庫的權限。請務必將 Connector 服務帳戶新增為分層服務帳戶的使用者、否則您將無法從 Cloud Manager 選取該帳戶。
- 您可以在建立或編輯磁碟區時、選擇特定的磁碟區分層原則。
- 如果停用資料分層、您可以在後續的 Aggregate 上啟用、但您需要關閉系統、並從 GCP 主控台新增服務帳戶。

"深入瞭解資料分層"。

13. \* 建立 Volume \* : 輸入新磁碟區的詳細資料、或按一下 \* 跳過 \* 。

"瞭解支援的用戶端傳輸協定和版本"。

本頁中的部分欄位是不知自明的。下表說明您可能需要指導的欄位：

| 欄位                     | 說明  |
|------------------------|---|
| 尺寸                     | 您可以輸入的最大大小、主要取決於您是否啟用精簡配置、這可讓您建立比目前可用實體儲存容量更大的磁碟區。  |
| 存取控制（僅適用於 NFS）         | 匯出原則會定義子網路中可存取磁碟區的用戶端。根據預設、Cloud Manager 會輸入一個值、讓您存取子網路中的所有執行個體。  |
| 權限與使用者 / 群組（僅限 CIFS）   | 這些欄位可讓您控制使用者和群組（也稱為存取控制清單或 ACL）的共用存取層級。您可以指定本機或網域 Windows 使用者或群組、或 UNIX 使用者或群組。如果您指定網域 Windows 使用者名稱、則必須使用網域\使用者名稱格式來包含使用者的網域。  |
| Snapshot 原則            | Snapshot 複製原則會指定自動建立的 NetApp Snapshot 複本的頻率和數量。NetApp Snapshot 複本是一種不影響效能的時間點檔案系統映像、需要最少的儲存容量。您可以選擇預設原則或無。您可以針對暫時性資料選擇「無」：例如、Microsoft SQL Server 的 Tempdb。   |
| 進階選項（僅適用於 NFS）         | 為磁碟區選取 NFS 版本：NFSv3 或 NFSv3。  |
| 啟動器群組和 IQN（僅適用於 iSCSI） | iSCSI 儲存目標稱為 LUN（邏輯單元）、以標準區塊裝置的形式呈現給主機。啟動器群組是 iSCSI 主機節點名稱的表格、可控制哪些啟動器可存取哪些 LUN。iSCSI 目標可透過標準乙太網路介面卡（NIC）、TCP 卸載引擎（TOE）卡（含軟體啟動器）、整合式網路介面卡（CNA）或專用主機匯流排介面卡（HBA）連線至網路、並由 iSCSI 合格名稱（IQN）識別。建立 iSCSI Volume 時、Cloud Manager 會自動為您建立 LUN。我們只要在每個磁碟區建立一個 LUN、就能輕鬆完成工作、因此不需要管理。建立磁碟區之後、 <a href="#">"使用 IQN 從主機連線至 LUN"</a> 。 |

下圖顯示 CIFS 傳輸協定的「Volume」（磁碟區）頁面：

### Volume Details, Protection & Protocol

#### Details & Protection

Volume Name:  Size (GB):

Snapshot Policy:

*i* Default Policy

#### Protocol

NFS **CIFS** iSCSI

Share name:  Permissions:

Users / Groups:

Valid users and groups separated by a semicolon



14. \* CIFS 設定 \* : 如果您選擇 CIFS 傳輸協定、請設定 CIFS 伺服器。

| 欄位                       | 說明  |
|--------------------------|---|
| DNS 主要和次要 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。如果您要設定 Google Managed Active Directory、AD 預設可透過 169.254.169.254 IP 位址存取。  |
| 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」。若要將 Google 託管 Microsoft AD 設定為 Cloud Volumes ONTAP AD 伺服器以供使用、請在此欄位中輸入 * OU=computers, OU=Cloud *<br>◦ <a href="https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units">https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units</a> ["Google Cloud 文件：Google 託管 Microsoft AD 的組織單位"] |
| DNS 網域                   | 適用於整個儲存虛擬 Cloud Volumes ONTAP 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                  | 選擇 * 使用 Active Directory 網域 * 來使用 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。請注意、您只能在建立 CIFS 伺服器時設定 NTP 伺服器。您建立 CIFS 伺服器之後、就無法進行設定。  |

15. \* 使用率設定檔、磁碟類型及分層原則 \* : 視需要選擇是否要啟用儲存效率功能、並變更磁碟區分層原則。

如需詳細資訊、請參閱 ["瞭解 Volume 使用量設定檔"](#) 和 ["資料分層總覽"](#)。

16. \* 審查與核准 \* : 檢閱並確認您的選擇。

- 檢閱組態的詳細資料。
- 按一下 \* 更多資訊 \* 以檢閱 Cloud Manager 將購買的支援與 GCP 資源詳細資料。
- 選取「\* 我瞭解 ... \*」核取方塊。
- 按一下「\* 執行 \*」。

Cloud Manager 部署 Cloud Volumes ONTAP 了這個功能。您可以追蹤時間表的進度。

如果您在部署 Cloud Volumes ONTAP 此系統時遇到任何問題、請檢閱故障訊息。您也可以選取工作環境、然後按一下 \* 重新建立環境 \*。

如需其他協助、請前往 ["NetApp Cloud Volumes ONTAP 支援"](#)。

完成後

- 如果您已配置 CIFS 共用區、請授予使用者或群組檔案和資料夾的權限、並確認這些使用者可以存取共用區並建立檔案。

- 如果您要將配額套用至磁碟區、請使用 System Manager 或 CLI 。

配額可讓您限制或追蹤使用者、群組或 qtree 所使用的磁碟空間和檔案數量。

## 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。