



# 使用**Cloud Volumes ONTAP**

## Cloud Volumes ONTAP

NetApp  
June 15, 2022

# 目錄

使用Cloud Volumes ONTAP .....	1
授權管理 .....	1
Volume與LUN管理 .....	10
Aggregate管理 .....	31
儲存VM管理 .....	33
安全性與資料加密 .....	64
系統管理 .....	71
系統健全狀況與事件 .....	93

# 使用Cloud Volumes ONTAP

## 授權管理

### 管理容量型授權

從Digital Wallet管理容量型授權、確保您的NetApp帳戶擁有足夠的容量來容納Cloud Volumes ONTAP 您的系統。

\_容量型授權\_可讓您針對Cloud Volumes ONTAP 每個TiB的容量付費。

「數位錢包」可讓您從Cloud Volumes ONTAP 單一位置管理用於支援的授權。您可以新增授權並更新現有授權。

["深入瞭解Cloud Volumes ONTAP 解不知如何取得授權"](#)。

### 如何將授權新增至Digital Wallet

向NetApp銷售代表購買授權後、NetApp會寄送一封電子郵件給您、附上序號和其他授權詳細資料。

在此期間、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。

如果Cloud Manager無法新增授權、您必須自行手動將其新增至Digital Wallet。例如、如果Connector安裝在無法存取網際網路的位置、您就必須自行新增授權。 [瞭解如何將購買的授權新增至您的帳戶](#)。

### 檢視您帳戶的容量

依套件檢視授權容量和已配置容量、確保您有足夠空間容納資料磁碟區。

#### 步驟

1. 按一下\*「所有服務」>「數位錢包」>Cloud Volumes ONTAP「參考」\*。
2. 選取\*容量型授權\*後、即可檢視每個套件的授權容量和已配置容量。



3. 如有需要、請購買額外的授權容量、然後將授權新增至您的帳戶。

## 將購買的授權新增至您的帳戶

如果您在Digital Wallet中沒有看到您購買的授權、您需要將授權新增至Cloud Manager、以便能夠Cloud Volumes ONTAP 使用該容量來進行支援。

您需要的是 **#8217** ；需要的是什麼

- 您需要向Cloud Manager提供授權或授權檔案的序號。
- 如果您要輸入序號、請先輸入 "[將您的NetApp支援網站帳戶新增至Cloud Manager](#)"。這是獲授權存取序號的NetApp支援網站帳戶。

### 步驟

1. 按一下\*「所有服務」>「數位錢包」> Cloud Volumes ONTAP 「參考」\*。
2. 按一下「\* 新增授權 \*」。
3. 輸入容量型授權的序號、或上傳授權檔案。

如果您輸入序號、您也需要選擇獲授權存取序號的NetApp Support Site帳戶。

4. 按一下「\* 新增授權 \*」。

## 更新容量型授權

如果您購買額外容量或延長授權期限、Cloud Manager會自動更新Digital Wallet中的授權。您無需做任何事。

不過、如果您在無法存取網際網路的位置部署Cloud Manager、則必須在Cloud Manager中手動更新授權。

授權檔案（如果您有HA配對、則為\_file\_）。

### 步驟

1. 按一下\*「所有服務」>「數位錢包」> Cloud Volumes ONTAP 「參考」\*。
2. 按一下授權旁邊的動作功能表、然後選取\*更新授權\*。
3. 上傳授權檔案。
4. 按一下\*上傳授權\*。

## 移除容量型授權

如果容量型授權過期且不再使用、您可以隨時將其移除。

### 步驟

1. 按一下\*「所有服務」>「數位錢包」> Cloud Volumes ONTAP 「參考」\*。
2. 按一下授權旁邊的動作功能表、然後選取\*移除授權\*。
3. 按一下「\* 移除 \*」以確認。

## 管理 **Keystone Flex** 訂閱

啟用訂閱功能以搭配Cloud Volumes ONTAP 使用、從Digital Wallet管理Keystone Flex訂閱。您也可以要求變更已提交的容量、也可以取消訂閱連結。

\_Keystone Flex訂購\_是NetApp提供的隨需付費儲存服務。

「數位錢包」可讓您從Cloud Volumes ONTAP 單一位置管理用於支援的授權。您可以新增授權並更新現有授權。

["深入瞭解Cloud Volumes ONTAP 解不知如何取得授權"](#)。

## 授權您的帳戶

在Cloud Manager中使用及管理Keystone Flex訂閱之前、您必須先聯絡NetApp、以利用Keystone Flex訂閱來授權Cloud Manager使用者帳戶。

### 步驟

1. 按一下「所有服務>數位錢包」。
2. 按一下\* Keystone Flex訂閱\*。
3. 如果您看到\*歡迎使用NetApp Keystone S不到\*頁面、請傳送電子郵件至頁面上所列的地址。

NetApp代表將授權您的使用者帳戶存取訂閱、以處理您的申請。

4. 請返回\* Keystone Flex訂購\*以檢視您的訂閱內容。



連結您要搭配Cloud Volumes ONTAP 使用的訂閱內容。

## 連結訂閱

在NetApp授權您的帳戶之後、您必須連結Keystone Flex訂閱Cloud Volumes ONTAP 以供搭配使用。此動作可讓使用者選擇訂閱做為新Cloud Volumes ONTAP 版的功能表系統的充電方法。

### 步驟

1. 按一下「所有服務>數位錢包」。
2. 按一下\* Keystone Flex訂閱\*。

3. 如需您要連結的訂閱、請按一下 **...** 然後選取\*連結\*。

Subscription Number	Committed	Consumed	# of Instances	Expiration Date	
A-S00014001	6.64 TiB	 4.35 TiB	0	July 29th, 2022	<b>...</b>
A-S00014002	6.64 TiB	 4.35 TiB	0	July 29th, 2022	View detail and edit
A-S00014003	6.64 TiB	 4.35 TiB	0	July 29th, 2022	Link 

訂閱內容現已連結至您的Cloud Manager帳戶、可在建立Cloud Volumes ONTAP 運作環境時選擇。

申請更多或更少的已認可容量

如果您需要調整訂閱的已提交容量、可以直接從Cloud Manager介面傳送要求。

步驟

1. 按一下「所有服務>數位錢包」。
2. 按一下\* Keystone Flex訂閱\*。
3. 如需調整容量的訂閱、請按一下 **...** 然後選取\*檢視詳細資料並編輯\*。
4. 輸入一或多個訂閱所需的已提交容量。

### Subscription Modification for A-S00014001

Service Level	Current Committed Capacity	Current Consumed Capacity	Requested Committed Capacity
Extreme	0.977 TiB	0.293 TiB	<input type="text" value="Enter amount"/> TiB
Premium	0.977 TiB	0.488 TiB	<input type="text" value="Enter amount"/> TiB
Performance	0 TiB	0 TiB	<input type="text" value="Enter amount"/> TiB
Standard	0.732 TiB	0.439 TiB	<input type="text" value="Enter amount"/> TiB
Value	0.977 TiB	 0.879 TiB	<input type="text" value="Enter amount"/> TiB
Data Tiering	0 TiB	0 TiB	<input type="text" value="Enter amount"/> TiB
CVO Primary	1.96 TiB	 1.76 TiB	<input type="text" value="3"/> TiB
CVO Secondary	1.02 TiB	0.488 TiB	<input type="text" value="Enter amount"/> TiB

#### Additional Information

Is there anything else we should know about your request?  
Please be as descriptive as possible.

Enter your notes here

5. 向下捲動、輸入申請的任何其他詳細資料、然後按一下\*提交\*。

您的申請會在NetApp系統中建立Ticket以供處理。

## 取消訂閱連結

如果您不想再將Keystone Flex訂閱搭配新Cloud Volumes ONTAP 的功能使用、可以取消訂閱連結。請注意、您只能取消連結未附加至現有Cloud Volumes ONTAP 的訂閱內容的訂閱。

## 步驟

- 按一下「所有服務>數位錢包」。
- 按一下\* Keystone Flex訂閱\*。
- 若要取消連結訂閱、請按一下  然後選取\*取消連結\*。

訂閱會從Cloud Manager帳戶中取消連結、因此在建立Cloud Volumes ONTAP 運作中的環境時、不再可供選擇。

## 管理節點型授權

在Digital Wallet中管理節點型授權、以確保每Cloud Volumes ONTAP 個版本均具有有效的授權、並具有所需的容量。

\_Node型授權\_是前一代授權模式（不適用於新客戶）：

- 向NetApp購買BYOL授權
- 從雲端供應商的市場訂閱每小時隨付（PAYGO）

「數位錢包」可讓您從Cloud Volumes ONTAP 單一位置管理用於支援的授權。您可以新增授權並更新現有授權。

"深入瞭解Cloud Volumes ONTAP 解不知如何取得授權"。

## 管理PAYGO授權

「Digital Wallet」頁面可讓您檢視每Cloud Volumes ONTAP 個PAYGO更新系統的詳細資料、包括序號和PAYGO授權類型。

### 步驟

1. 按一下\*「所有服務」>「數位錢包」> Cloud Volumes ONTAP 「參考」\*。
2. 從下拉式清單中選取\*節點型授權\*。
3. 按一下\* PAYGO\*。
4. 請在表格中檢視每個PAYGO授權的詳細資料。



5. 如有需要、請按一下\*管理PAYGO授權\*以變更PAYGO授權或變更執行個體類型。

## 管理 BYOL 授權

透過新增及移除系統授權與額外容量授權、來管理您直接向NetApp購買的授權。

### 新增未指派的授權

將節點型授權新增至Digital Wallet、以便在建立新Cloud Volumes ONTAP 的作業系統時選取授權。數位錢包會將這些授權識別為\_未指派\_。



## 步驟

1. 按一下\*「所有服務」>「數位錢包」> Cloud Volumes ONTAP 「參考」\*。
2. 從下拉式清單中選取\*節點型授權\*。
3. 按一下\*未指派\*。
4. 按一下「新增未指派的授權」。
5. 輸入授權的序號或上傳授權檔案。

如果您還沒有授權檔案、請參閱下列章節。

6. 按一下「\* 新增授權 \*」。

Cloud Manager會將授權新增至Digital Wallet。授權將被識別為未指派、直到您將其與新Cloud Volumes ONTAP的一套系統關聯為止。之後、授權會移至「數位錢包」中的「\* BYOL\*」索引標籤。

## Exchange未指派的節點型授權

如果Cloud Volumes ONTAP 您擁有尚未使用的未指派節點型支援功能、您可以將授權轉換為Cloud Backup授權、Cloud Data Sense授權或Cloud Tiering授權、以交換授權。

交換授權會撤銷Cloud Volumes ONTAP 該服務的不含美元的授權、並為該服務建立相當於美元的授權：

- 針對某個不符合需求的HA配對授權Cloud Volumes ONTAP 會轉換為51 TiB資料服務授權
- 針對單一節點的授權Cloud Volumes ONTAP 會轉換為32 TiB資料服務授權

轉換後的授權到期日與Cloud Volumes ONTAP 不含更新授權的到期日相同。

## 步驟

1. 按一下\*「所有服務」>「數位錢包」> Cloud Volumes ONTAP 「參考」\*。
2. 從下拉式清單中選取\*節點型授權\*。
3. 按一下\*未指派\*。
4. 按一下「\* Exchange授權\*」。

BYOL (14)	Eval (2)	Unassigned (3)	PAYGO (6)		Q	Add Unassigned Licenses
Serial Number	Type	Cloud Provider	License Expiry	Status		
012345678901234567890	Single Node	All Providers	April 20, 2022	Unassigned	Exchange License	...
012345678901234567891	Single Node	Azure	April 20, 2022	Unassigned	Exchange License	...
012345678901234567892	Single Node	AWS	January 1, 2022	Exchanged to Cloud Tiering on August 1, 2021		...

5. 選取您要與其交換授權的服務。
6. 如果出現提示、請為HA配對選取額外的授權。
7. 閱讀法律同意書、然後按一下\*同意\*。

Cloud Manager會將未指派的授權轉換成您所選的服務。您可以在「資料服務授權」標籤中檢視新授權。

#### 取得系統授權檔案

在大多數情況下、Cloud Manager 會使用您的 NetApp 支援網站帳戶自動取得授權檔案。但如果無法、則需要手動上傳授權檔案。如果您沒有授權檔案、可以從 netapp.com 取得。

#### 步驟

1. 前往 "[NetApp 授權檔案產生器](#)" 並使用您的 NetApp 支援網站認證登入。
2. 輸入您的密碼、選擇產品、輸入序號、確認您已閱讀並接受隱私權政策、然後按一下 \* 提交 \*。

◦ 範例 \*



Form fields and content:

- Password\*: [Masked]
- Product Line\*: NetApp ONTAP Cloud BYOL for AWS
- Product Serial #: 90120130000000000555
- Text: Not only is protecting your data required by law, but your privacy is also very important to us. Please read and agree to the NetApp [Data Privacy Policy](#) before you continue. For information related to NetApp's privacy policy please click here [Privacy Policy](#) or contact [privacy@netapp.com](mailto:privacy@netapp.com).
- Checkbox: ☒ I have read NetApp's new [Global Data Privacy Policy](#) and understand how NetApp and its selected partners may use my personal data.
- Submit button

3. 選擇您要透過電子郵件或直接下載來接收 serialNumber.NLF Json 檔案。

#### 更新系統授權

當您透過聯絡 NetApp 代表續約 BYOL 訂閱時、Cloud Manager 會自動從 NetApp 取得新授權、並將其安裝在 Cloud Volumes ONTAP 該系統上。

如果 Cloud Manager 無法透過安全的網際網路連線存取授權檔案、您可以自行取得檔案、然後手動將檔案上傳至 Cloud Manager。

#### 步驟

1. 按一下\*「所有服務」>「數位錢包」> Cloud Volumes ONTAP 「參考」\*。
2. 從下拉式清單中選取\*節點型授權\*。
3. 在「\* BYOL\*」標籤中、展開Cloud Volumes ONTAP 關於某個系統的詳細資料。
4. 按一下系統授權旁的動作功能表、然後選取\*更新授權\*。
5. 上傳授權檔案（若您有HA配對、則為檔案）。
6. 按一下 \* 更新授權 \*。

Cloud Manager 會更新 Cloud Volumes ONTAP 整個作業系統的授權。

## 管理額外容量授權

您可以購買Cloud Volumes ONTAP 額外容量授權給某個不含BYOL的系統、以配置超過368TiB的BYOL系統授權容量。例如、您可以購買一個額外的授權容量、以配置多達736 TiB的容量來Cloud Volumes ONTAP 供使用。或者、您也可以購買三份額外容量授權、最多可取得1.4 PIB。

單一節點系統或 HA 配對可購買的授權數量不受限制。

## 新增容量授權

透過Cloud Manager右下角的聊天圖示聯絡我們、購買額外的容量授權。購買授權後、您可以將其套用Cloud Volumes ONTAP 至一套系統。

### 步驟

1. 按一下\*「所有服務」>「數位錢包」> Cloud Volumes ONTAP 「參考」\*。
2. 從下拉式清單中選取\*節點型授權\*。
3. 在「\* BYOL\*」標籤中、展開Cloud Volumes ONTAP 關於某個系統的詳細資料。
4. 按一下「新增容量授權」。
5. 輸入序號或上傳授權檔案（如果您有HA配對、也可以輸入檔案）。
6. 按一下「新增容量授權」。

## 更新容量授權

如果您延長額外容量授權的期限、則必須在Cloud Manager中更新授權。

### 步驟

1. 按一下\*「所有服務」>「數位錢包」> Cloud Volumes ONTAP 「參考」\*。
2. 從下拉式清單中選取\*節點型授權\*。
3. 在「\* BYOL\*」標籤中、展開Cloud Volumes ONTAP 關於某個系統的詳細資料。
4. 按一下容量授權旁邊的動作功能表、然後選取\*更新授權\*。
5. 上傳授權檔案（若您有HA配對、則為檔案）。
6. 按一下 \* 更新授權 \*。

## 移除容量授權

如果額外的容量授權過期且不再使用、您可以隨時將其移除。

### 步驟

1. 按一下\*「所有服務」>「數位錢包」> Cloud Volumes ONTAP 「參考」\*。
2. 從下拉式清單中選取\*節點型授權\*。
3. 在「\* BYOL\*」標籤中、展開Cloud Volumes ONTAP 關於某個系統的詳細資料。
4. 按一下容量授權旁的動作功能表、然後選取\*移除授權\*。
5. 按一下「移除」。

將試用版授權轉換為**BYOL**

試用版授權可提供30天的使用時間。您可以在就地升級的評估授權上套用新的BYOL授權。

當您將試用版授權轉換為BYOL時、Cloud Manager會重新啟動Cloud Volumes ONTAP 該系統。

- 對於單節點系統、重新啟動會在重新開機程序期間導致I/O中斷。
- 對於HA配對、重新啟動會啟動接管和恢復、以繼續為用戶端提供I/O服務。

#### 步驟

1. 按一下\*「所有服務」>「數位錢包」> Cloud Volumes ONTAP 「參考」\*。
2. 從下拉式清單中選取\*節點型授權\*。
3. 按一下\* Eval\*。
4. 在表格中、按一下\*「轉換成BYOL授權\*」以取得Cloud Volumes ONTAP 一套系統。
5. 輸入序號或上傳授權檔案。
6. 按一下\*「轉換授權\*」。

Cloud Manager會開始轉換程序。此程序會自動重新啟動。Cloud Volumes ONTAP備份時、授權資訊會反映出新的授權。

#### 在**PAYGO**和**BYOL**之間切換

不支援將系統從PAYGO的節點授權轉換成BYOL的節點授權（反之亦然）。如果您想要在隨用隨付訂閱和BYOL訂閱之間切換、則必須部署新系統、並將資料從現有系統複製到新系統。

#### 步驟

1. 打造全新 Cloud Volumes ONTAP 的運作環境。
2. 針對您需要複製的每個磁碟區、在系統之間設定一次性資料複製。

["瞭解如何在系統之間複製資料"](#)

3. 刪除原始工作環境、終止Cloud Volumes ONTAP 不再需要的功能。

["瞭解如何刪除Cloud Volumes ONTAP 功能不正常的工作環境"](#)。

## Volume與LUN管理

### 建立FlexVol 功能區

如果您在啟動初始Cloud Volumes ONTAP 的支援功能後需要更多儲存設備、可以FlexVol從Cloud Manager建立新的適用於NFS、CIFS或iSCSI的支援功能。

Cloud Manager提供多種建立新磁碟區的方法：

- 指定新磁碟區的詳細資料、讓Cloud Manager為您處理基礎資料集合體。 [深入瞭解](#)。
- 在您選擇的資料集合體上建立磁碟區。 [深入瞭解](#)。

- 從範本建立磁碟區、以針對特定應用程式（例如資料庫或串流服務）的工作負載需求、最佳化磁碟區。[深入瞭解](#)。
- 在HA組態的第二個節點上建立磁碟區。[深入瞭解](#)。

## 開始之前

關於Volume資源配置的幾點注意事項：

- 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、[使用 IQN 從主機連線至 LUN](#)。
- 您可以從 System Manager 或 CLI 建立其他 LUN 。
- 如果您想在 AWS 中使用 CIFS 、則必須設定 DNS 和 Active Directory 。如需詳細資訊、請參閱 "[AWS 的 Cloud Volumes ONTAP 網路需求](#)"。
- 如果Cloud Volumes ONTAP 您的支援Amazon EBS彈性Volume功能的組態、您可能會想要 "[深入瞭解建立Volume時會發生什麼事](#)"。

## 建立Volume

建立磁碟區最常見的方法是指定所需的磁碟區類型、然後Cloud Manager會為您處理磁碟配置。但您也可以選擇要在其上建立磁碟區的特定Aggregate。

### 步驟

1. 在「畫版」頁面上、按兩下Cloud Volumes ONTAP 您要在其中配置FlexVol 一份「功能區」的「功能區」系統名稱。
2. 透過Cloud Manager為您處理磁碟配置、或為磁碟區選擇特定的集合體、來建立新的磁碟區。

只有在您對Cloud Volumes ONTAP 自己的系統上的資料集合體有充分的瞭解時、才建議您選擇特定的集合體。

#### 任何Aggregate

在Volumes（磁碟區）索引標籤中、按一下\* Add Volume\*（新增磁碟區）>\* New Volume\*。

#### 特定Aggregate

- a. 按一下功能表圖示、然後按一下 \* 進階 > 進階分配 \*。
- b. 按一下功能表以取得 Aggregate 。
- c. 按一下「\* 建立 Volume \*」。

3. 依照精靈中的步驟建立磁碟區。

- a. 詳細資料、保護及標記：輸入有關磁碟區的基本詳細資料、然後選取Snapshot原則。

此頁面上的部分欄位是不知自明的。下列清單說明您可能需要指引的欄位：

欄位	說明
Volume大小	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。
標記	您新增至Volume的標記會與相關聯 <a href="#">"應用程式範本服務"</a> 可協助您組織及簡化資源管理。
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。

- b. 傳輸協定：為磁碟區（NFS、CIFS或iSCSI）選擇傳輸協定、然後提供所需的資訊。

如果您選取CIFS但未設定伺服器、Cloud Manager會在您按一下\*「下一步」\*之後提示您設定CIFS連線。

["瞭解支援的用戶端傳輸協定和版本"](#)。

以下各節將說明您可能需要指引的欄位。說明會依傳輸協定加以組織。

## NFS

### 存取控制

選擇自訂匯出原則、讓用戶端可以使用磁碟區。

### 匯出原則

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。

## CIFS

### 權限與使用者/群組

可讓您控制使用者和群組存取SMB共用區的層級（也稱為存取控制清單或ACL）。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。

### 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AWS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\* OID=computers,O=corp\*。
- 若要將Azure AD網域服務設定為Cloud Volumes ONTAP AD伺服器以供使用、請在此欄位中輸入\* OID=AADDC computers\*或\* OID=AADDC使用者\*。 <https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou>["Azure 說明文件：在 Azure AD 網域服務託管網域中建立組織單位（OU）"]
- 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 \*。 [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)["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 ["Cloud Manager 自動化文件"](#) 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。

## iSCSI

### LUN

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。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、["使用 IQN 從主機連線至 LUN"](#)。

### 啟動器群組

啟動器群組（igroup）指定哪些主機可以存取儲存系統上的指定 LUN

### 主機啟動器（IQN）

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。

a. 磁碟類型：根據您的效能需求和成本需求、為磁碟區選擇基礎磁碟類型。

- ["在 AWS 中調整系統規模"](#)
- ["在 Azure 中調整系統規模"](#)
- ["在 Google Cloud 中調整系統規模"](#)

4. 使用率設定檔與分層原則：選擇是否啟用或停用磁碟區上的儲存效率功能、然後選取 ["Volume 分層原則"](#)。

包含多項儲存效率功能、可減少您所需的總儲存容量。ONTAP 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。

5. 審查：檢閱磁碟區的詳細資料、然後按一下\*新增\*。

Cloud Manager 會在 Cloud Volumes ONTAP 整個系統上建立磁碟區。



## 從範本建立Volume

如果貴組織已建立Cloud Volumes ONTAP 了適用於特定應用程式工作負載需求最佳化的功能、以便部署這些磁碟區、請依照本節中的步驟進行。

此範本應能讓您的工作更輕鬆、因為範本中已定義了某些Volume參數、例如磁碟類型、大小、傳輸協定、快照原則、雲端供應商、以及更多資訊。當參數已預先定義時、您只需跳至下一個Volume參數即可。



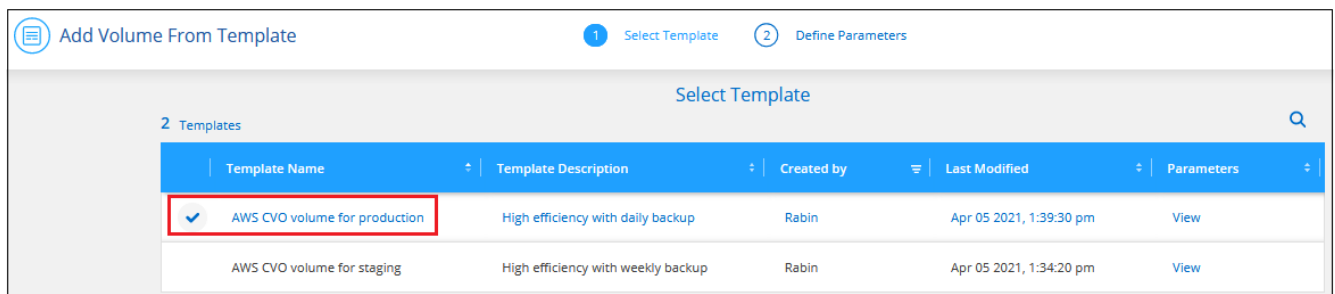
使用範本時、您只能建立NFS或CIFS磁碟區。

### 步驟

1. 在「畫版」頁面上、按一下Cloud Volumes ONTAP 您要配置Volume的功能區系統名稱。
2. 按一下  >\*從範本新增Volume\*。



3. 在「選取範本」頁面中、選取您要用來建立磁碟區的範本、然後按一下「下一步」。



此時會顯示「定義參數」頁面。

### Define Parameters

Enter your values for the actions. Parameters that are locked by the template are not editable.

#### Actions

```

graph TD
    A[Create Volume in Cloud Volumes ONTAP (1)] --> B[Enable Cloud Backup (1)]
    B --> A
  
```

☐ Show read-only parameters

#### Details

Volume Name ?

Volume Size (GB) ?

#### Protection

Snapshot Policy

#### Usage Profile

☒ Storage Efficiency
 ☐ No Storage Efficiency

#### Disk Type

Disk Type



如果您想查看這些參數的值、可以按一下「Show read-only parameters\*（顯示唯讀參數\*）」核取方塊、以顯示範本已鎖定的所有欄位。根據預設、這些預先定義的欄位會隱藏、只會顯示您需要填寫的欄位。

- 在 `_context_` 區域中、工作環境會填入您剛開始使用的工作環境名稱。您需要選擇要在其中建立磁碟區的\*儲存VM\*。
- 新增所有非模板硬編碼的參數值。請參閱 [建立Volume](#) 如需部署Cloud Volumes ONTAP 一套解決方案的所有必要參數詳細資訊、請參閱。
- 如果您不需要定義其他動作（例如、設定Cloud Backup）、請按一下\*執行範本\*。

如果還有其他動作、請按一下左窗格中的動作、以顯示您需要完成的參數。



例如、如果「啟用雲端備份」動作需要您選取備份原則、您現在就可以這麼做了。

- 按一下\*執行範本\*。

此功能會配置磁碟區並顯示頁面、以便您查看進度。Cloud Volumes ONTAP



此外、如果範本中實作任何次要動作、例如在磁碟區上啟用Cloud Backup、也會執行該動作。

在HA組態的第二個節點上建立磁碟區

根據預設、Cloud Manager 會在 HA 組態的第一個節點上建立磁碟區。如果您需要雙節點向用戶端提供資料的雙主動式組態、則必須在第二個節點上建立集合體和磁碟區。

步驟

1. 在「畫版」頁面上、按兩下 Cloud Volumes ONTAP 您要管理集合體的運作環境名稱。
2. 按一下功能表圖示、然後按一下 \* 進階 > 進階分配 \*。
3. 按一下「\* 新增 Aggregate \*」、然後建立 Aggregate。
4. 對於主節點、請在 HA 配對中選擇第二個節點。
5. Cloud Manager 建立 Aggregate 之後、選取該集合體、然後按一下「\* 建立 Volume \*」。
6. 輸入新磁碟區的詳細資料、然後按一下「\* 建立 \*」。

Cloud Manager會在HA配對的第二個節點上建立磁碟區。



對於部署在多個 AWS 可用性區域中的 HA 配對、您必須使用磁碟區所在節點的浮動 IP 位址、將磁碟區掛載到用戶端。

建立Volume之後

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。

如果要將配額套用至磁碟區、則必須使用 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。

管理現有磁碟區

Cloud Manager可讓您管理磁碟區和CIFS伺服器。它也會提示您移動磁碟區、以避免發生

## 容量問題。

### 管理磁碟區

您可以在儲存需求變更時管理磁碟區。您可以檢視、編輯、複製、還原及刪除磁碟區。

#### 步驟

1. 在「畫版」頁面上、按兩下 Cloud Volumes ONTAP 您要管理磁碟區的「功能區」工作環境。
2. 管理您的磁碟區：

工作	行動
檢視磁碟區的相關資訊	選取磁碟區、然後按一下「* 資訊 *」。
編輯磁碟區（僅限讀寫磁碟區）	<div><div><div>a. 選取磁碟區、然後按一下 * 編輯 *。</div><div>b. 修改磁碟區的Snapshot原則、NFS傳輸協定版本、NFS存取控制清單（匯出原則）或共用權限、然後按一下*更新*。</div></div><div><div></div><div>如果您需要自訂 Snapshot 原則、可以使用 System Manager 來建立。</div></div></div>
複製磁碟區	<div><div><div>a. 選取磁碟區、然後按一下 * Clone （複製） *。</div><div>b. 視需要修改複本名稱、然後按一下 * Clone （複製） *。</div></div><div>此程序會建立 FlexClone Volume。FlexClone Volume 是可寫入的時間點複本、空間效率極高、因為它會使用少量的空間作為中繼資料、然後只會在資料變更或新增時耗用額外空間。</div><div>若要深入瞭解 FlexClone Volume、請參閱 "<a href="#">《 9 邏輯儲存管理指南》ONTAP</a>"。</div></div>
將資料從 Snapshot 複本還原至新的 Volume	<div><div><div>a. 選取磁碟區、然後按一下 * 從 Snapshot 複本還原 *。</div><div>b. 選取 Snapshot 複本、輸入新磁碟區的名稱、然後按一下 * 還原 *。</div></div></div>
隨需建立 Snapshot 複本	<div><div><div>a. 選取一個磁碟區、然後按一下 * 「Create a Snapshot Copy*（建立 Snapshot 複本 *）」。</div><div>b. 視需要變更名稱、然後按一下「* 建立 *」。</div></div></div>
取得 NFS 掛載命令	<div><div><div>a. 選取磁碟區、然後按一下 * 掛載 Command*。</div><div>b. 按一下 * 複本 *。</div></div></div>
檢視 iSCSI 磁碟區的目標 IQN	<div><div><div>a. 選取磁碟區、然後按一下「* 目標 IQN*」。</div><div>b. 按一下 * 複本 *。</div><div>c. "<a href="#">使用 IQN 從主機連線至 LUN</a>"。</div></div></div>

工作	行動
變更基礎磁碟類型	a. 選取磁碟區、然後按一下 * 變更磁碟類型與分層原則 * 。 b. 選取磁碟類型、然後按一下 * 變更 * 。 <div>            Cloud Manager 會將磁碟區移至使用所選磁碟類型的現有 Aggregate 、或為磁碟區建立新的 Aggregate 。         </div>
變更分層原則	a. 選取磁碟區、然後按一下 * 變更磁碟類型與分層原則 * 。 b. 按一下 * 編輯原則 * 。 c. 選取不同的原則、然後按一下 * 變更 * 。 <div>            Cloud Manager 會將磁碟區移至現有的 Aggregate 、該集合體使用所選的磁碟類型進行分層、或是為磁碟區建立新的 Aggregate 。         </div>
刪除 Volume	a. 選取磁碟區、然後按一下 * 刪除 * 。 b. 再按一下 * 刪除 * 以確認。

## 調整磁碟區大小

根據預設、當磁碟區空間不足時、它會自動增加至最大大小。預設值為1、000、表示磁碟區的大小可增加至11倍。此值可在連接器的設定中設定。

如果您需要調整磁碟區大小、您可以透過調整磁碟區大小 "[系統管理程式ONTAP](#)"。調整磁碟區大小時、請務必將系統的容量限制列入考量。前往 "[發行說明 Cloud Volumes ONTAP](#)" 以取得更多詳細資料。

## 修改CIFS伺服器

如果您變更 DNS 伺服器或 Active Directory 網域、您需要在 Cloud Volumes ONTAP 更新版中修改 CIFS 伺服器、以便繼續將儲存設備提供給用戶端。

### 步驟

1. 在工作環境中、按一下功能表圖示、然後按一下 \* 進階 > CIFS 設定 \* 。
2. 指定 CIFS 伺服器的設定：

工作	行動
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。ifdef : : GCP[如果您正在設定Google Managed Active Directory、則AD預設可透過169.254.169.254 IP位址存取。endif::GCP]
要加入的 Active Directory 網域	您要 CIFS 伺服器加入之 Active Directory ( AD ) 網域的 FQDN 。

工作	行動
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	<p>AD 網域中與 CIFS 伺服器相關聯的組織單位。預設值為「CN= 電腦」。</p> <ul style="list-style-type: none"> <li>• 若要將AWS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* OID=computers,O=corp*。</li> <li>• 若要將Azure AD網域服務設定為Cloud Volumes ONTAP AD伺服器以供使用、請在此欄位中輸入* OID=AADDC computers*或* OID=AADDC使用者*。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure 說明文件：在 Azure AD 網域服務託管網域中建立組織單位（OU）"^]</li> <li>• 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 *。https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud文件：Google託管Microsoft AD的組織單位"^]</li> </ul>
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。

3. 按一下「\* 儲存 \*」。

利用變更更新 CIFS 伺服器。Cloud Volumes ONTAP

## 移動Volume

移動磁碟區以提高容量使用率、改善效能、並達成服務層級協議。

您可以在 System Manager 中移動磁碟區、方法是選取磁碟區和目的地 Aggregate、啟動磁碟區移動作業、以及選擇性地監控磁碟區移動工作。使用 System Manager 時、磁碟區移動作業會自動完成。

### 步驟

1. 使用 System Manager 或 CLI 將磁碟區移至 Aggregate。

在大多數情況下、您可以使用 System Manager 來移動磁碟區。

如需相關指示、請參閱 "《《 9 Volume Move Express Guide 》（英文） ONTAP"。

## 當Cloud Manager顯示「需要採取行動」訊息時、請移動Volume

Cloud Manager可能會顯示「必要行動」訊息、指出移動磁碟區是避免容量問題的必要措施、但您必須自行修正問題。如果發生這種情況、您需要找出如何修正問題、然後移動一或多個磁碟區。



當Aggregate已達到90%使用容量時、Cloud Manager會顯示這些必要行動訊息。如果啟用資料分層、則當Aggregate達到80%已使用容量時、訊息會顯示。根據預設、10%的可用空間會保留給資料分層。"深入瞭解資料分層的可用空間比率"。

## 步驟

1. [找出如何修正問題](#)。
2. 根據您的分析、移動磁碟區以避免容量問題：
  - [將磁碟區移至其他系統](#)。
  - [將磁碟區移至同一系統上的其他 Aggregate](#)。

## 找出如何修正容量問題

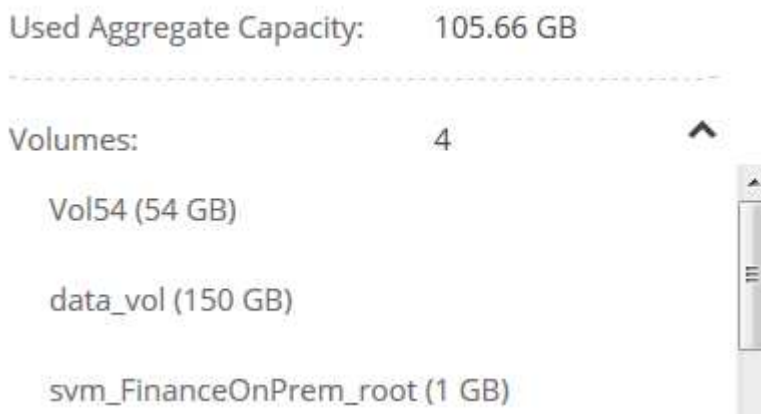
如果Cloud Manager無法提供移動磁碟區以避免容量問題的建議、您必須識別需要移動的磁碟區、以及是否應該將它們移到同一個系統上的其他Aggregate或其他系統上。

## 步驟

1. 檢視必要行動訊息中的進階資訊、以識別已達到容量上限的集合體。

例如、進階資訊應該說類似以下的內容： Agggr1 已達到其容量上限。

2. 識別一個或多個要從集合體移出的磁碟區：
  - a. 在工作環境中、按一下功能表圖示、然後按一下 \* 進階 > 進階配置 \* 。
  - b. 選取 Aggregate 、然後按一下「 \* 資訊 \* 」。
  - c. 展開 Volume 清單。



- d. 檢閱每個磁碟區的大小、然後選擇一或多個磁碟區從集合區移出。
- 您應該選擇足夠大的磁碟區來釋放集合體中的空間、以避免未來發生額外的容量問題。
3. 如果系統尚未達到磁碟限制、您應該將磁碟區移至同一個系統上的現有集合體或新集合體。
- 如需詳細資訊、請參閱 ["將磁碟區移至另一個 Aggregate 、以避免容量問題"](#)。
4. 如果系統已達到磁碟限制、請執行下列任何一項：
    - a. 刪除所有未使用的磁碟區。
    - b. 重新排列磁碟區、以釋放集合體上的空間。

如需詳細資訊、請參閱 ["將磁碟區移至另一個 Aggregate 、以避免容量問題"](#)。



- c. 將兩個或多個磁碟區移至另一個有空間的系統。

如需詳細資訊、請參閱 ["將磁碟區移至其他系統、以避免發生容量問題"](#)。

將磁碟區移至其他系統、以避免發生容量問題

您可以將一個或多個 Volume 移至另 Cloud Volumes ONTAP 一個作業系統、以避免容量問題。如果系統達到磁碟限制、您可能需要這麼做。

您可以依照此工作中的步驟來修正下列必要行動訊息：

Moving a volume is necessary to avoid capacity issues; however, Cloud Manager cannot perform this action for you because the system has reached the disk limit.

. 步驟

- . 找出 Cloud Volumes ONTAP 具備可用容量的系統、或是部署新系統。
- . 將來源工作環境拖放到目標工作環境、以執行磁碟區的一次性資料複寫。

+  
如需詳細資訊、請參閱 ["在系統之間複寫資料"](#)。

1. 移至「複寫狀態」頁面、然後中斷 SnapMirror 關係、將複寫的磁碟區從資料保護磁碟區轉換為讀寫磁碟區。

如需詳細資訊、請參閱 ["管理資料複寫排程和關係"](#)。

2. 設定磁碟區以進行資料存取。

如需設定目的地 Volume 以進行資料存取的相關資訊、請參閱 "[《 9 Volume Disaster Recovery Express 指南》 ONTAP](#)"。

3. 刪除原始 Volume 。

如需詳細資訊、請參閱 ["管理磁碟區"](#)。

將磁碟區移至其他Aggregate、以避免容量問題

您可以將一個或多個磁碟區移至另一個 Aggregate 、以避免發生容量問題。

您可以依照此工作中的步驟來修正下列必要行動訊息：

Moving two or more volumes is necessary to avoid capacity issues; however, Cloud Manager cannot perform this action for you.

. 步驟

- . 驗證現有的 Aggregate 是否具有您需要移動的磁碟區可用容量：

+  
.. 在工作環境中、按一下功能表圖示、然後按一下 \* 進階 > 進階配置 \* 。



.. 選取每個 Aggregate、按一下「\* 資訊 \*」、然後檢視可用容量（Aggregate capacity 容納量減去已使用的 Aggregate capacity）。

+

aggr1

Aggregate Capacity: 442.94 GB

Used Aggregate Capacity: 105.66 GB

1. 如有需要、請將磁碟新增至現有的 Aggregate：
  - a. 選取 Aggregate、然後按一下「Add disks\*（新增磁碟\*）」。
  - b. 選取要新增的磁碟數目、然後按一下「Add\*（新增\*）」。
2. 如果沒有集合體具有可用容量、請建立新的集合體。

如需詳細資訊、請參閱 ["建立 Aggregate"](#)。

3. 使用 System Manager 或 CLI 將磁碟區移至 Aggregate。
4. 在大多數情況下、您可以使用 System Manager 來移動磁碟區。

如需相關指示、請參閱 ["《 9 Volume Move Express Guide 》（英文） ONTAP"](#)。

#### 磁碟區移動可能會緩慢執行的原因

如果 Cloud Volumes ONTAP 下列任一情況屬實、則移動 Volume 所需時間可能比預期更長：

- 磁碟區是複製的。
- Volume 是實體複本的父實體。
- 來源或目的地 Aggregate 具有單一資料處理量最佳化 HDD（ST1）磁碟。
- 其中一個集合體使用舊的物件命名配置。兩個 Aggregate 都必須使用相同的名稱格式。

如果在 9.4 版或更早版本的 Aggregate 上啟用資料分層、則會使用較舊的命名配置。

- 來源與目的地集合體上的加密設定不相符、或是正在進行重新金鑰。
- 在移動磁碟區時指定了 `_分層原則_` 選項、以變更分層原則。
- 磁碟區移動時指定了 `-generation-destination-key_` 選項。

#### 將非作用中資料分層至低成本物件儲存設備

您可以將熱資料的 SSD 或 HDD 效能層與非作用中資料的物件儲存容量層合併、藉此降低 Cloud Volumes ONTAP VMware 的儲存成本。資料分層是 FabricPool 以不同步技術為後盾。如需詳細概述、請參閱 ["資料分層總覽"](#)。

若要設定資料分層、您需要執行下列動作：

支援大部分的組態。如果Cloud Volumes ONTAP 您的系統執行的是最新版本、那麼您應該會很滿意。"深入瞭解"。

- 對於 AWS、您需要 VPC 端點對 S3。深入瞭解。
- 對於 Azure 而言、只要 Cloud Manager 具備必要的權限、您就不需要執行任何操作。深入瞭解。
- 若為Google Cloud、您需要設定私有Google Access的子網路、並設定服務帳戶。深入瞭解。

必須在集合體上啟用資料分層、才能在磁碟區上啟用資料分層。您應該瞭解新磁碟區和現有磁碟區的需求。深入瞭解。

Cloud Manager 會在您建立、修改或複寫磁碟區時、提示您選擇分層原則。

- "在讀寫磁碟區上分層資料"
- "在資料保護磁碟區上分層資料"



什麼是資料分層不需要的？ #8217 ？

- 您不需要安裝功能授權、就能進行資料分層。
- 您不需要為容量層建立物件存放區。Cloud Manager 能幫您達成這項目標。
- 您不需要在系統層級啟用資料分層。

Cloud Manager 會在系統建立時、為 Cold 資料建立物件存放區、只要沒有連線或權限問題。之後、您只需要在磁碟區上啟用資料分層功能（在某些情況下、在 Aggregate 上）。

支援資料分層的組態

您可以在使用特定組態和功能時啟用資料分層。

#### AWS支援

- AWS支援資料分層功能、從Cloud Volumes ONTAP 功能表9.2開始。
- 效能層可以是通用SSD（GP3或gp2）或已配置的IOPS SSD（IO1）。



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。

#### 支援Azure

- Azure支援下列資料分層：
  - 9.4版、搭配單一節點系統
  - 9.6版、搭配HA配對
- 效能層可以是優質SSD託管磁碟、標準SSD託管磁碟或標準HDD託管磁碟。

## 支援Google Cloud

- Google Cloud支援資料分層功能、從Cloud Volumes ONTAP 推出的功能僅支援32個9.6個。
- 效能層可以是SSD持續磁碟、平衡持續磁碟或標準持續磁碟。

### 功能互通性

- 加密技術支援資料分層。
- 必須在磁碟區上啟用精簡配置。

### 需求

視您的雲端供應商而定、必須設定特定的連線和權限、Cloud Volumes ONTAP 以便讓效益管理系統將冷資料分層處理至物件儲存設備。

#### 將冷資料分層至 AWS S3 的需求

確保 Cloud Volumes ONTAP 與 S3 建立連線。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？"](#)。

#### 將冷資料分層至 Azure Blob 儲存設備的需求

只要 Cloud Manager 具備所需的權限、您就不需要在效能層與容量層之間建立連線。如果 Cloud Manager 原則具有下列權限、Cloud Manager 可為您啟用 vnet 服務端點：

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

權限包含在最新版本中 ["Cloud Manager 原則"](#)。

#### 將冷資料分層至 Google Cloud Storage 儲存庫的需求

- 駐留的子網路 Cloud Volumes ONTAP 必須設定為私有 Google Access。如需相關指示、請參閱 ["Google Cloud 文件：設定私有 Google Access"](#)。
- 服務帳戶必須附加Cloud Volumes ONTAP 至

["瞭解如何設定此服務帳戶"](#)。

當您建立Cloud Volumes ONTAP 一個運作環境時、系統會提示您選擇此服務帳戶。

如果您在部署期間未選擇服務帳戶、則必須關閉Cloud Volumes ONTAP 該服務帳戶、前往Google Cloud主控台、然後將該服務帳戶附加至Cloud Volumes ONTAP 該故障。然後、您可以依照下一節所述、啟用資料分層。

- 若要使用客戶管理的加密金鑰來加密儲存區、請啟用Google Cloud儲存區使用金鑰。

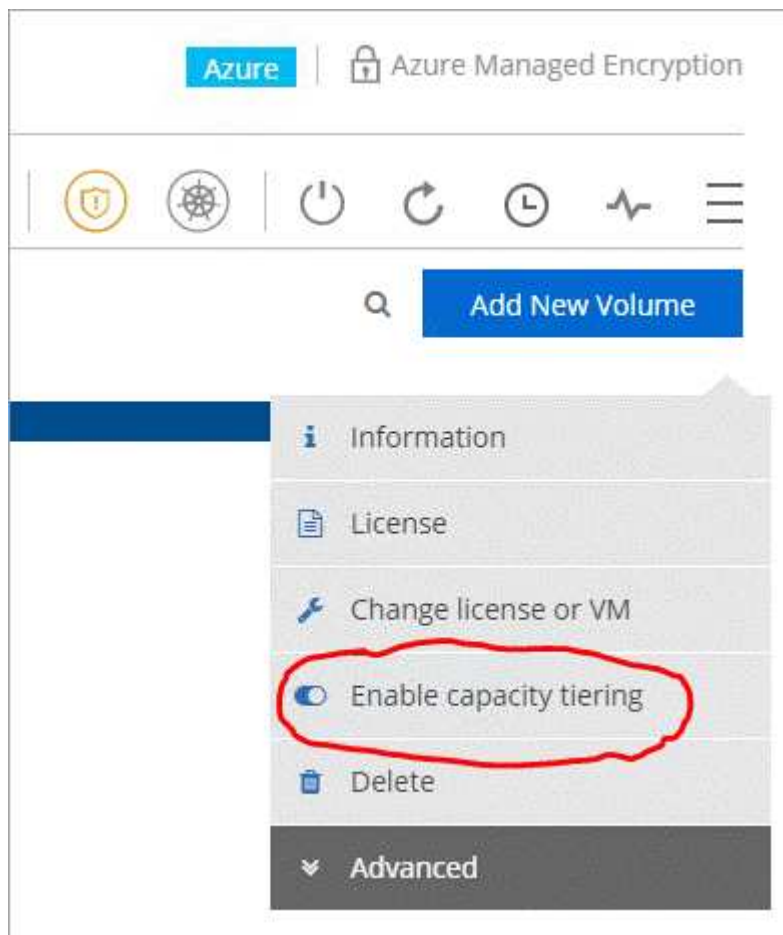
"瞭解如何搭配Cloud Volumes ONTAP 使用客戶管理的加密金鑰"。

在實作需求之後啟用資料分層

只要沒有連線或權限問題、Cloud Manager 就會在系統建立時、為 Cold 資料建立物件存放區。如果您在建立系統之前未實作上述要求、則必須手動啟用分層、以建立物件存放區。

步驟

1. 確保您已符合所有要求。
2. 在「畫版」頁面上、按兩下 Cloud Volumes ONTAP 「實例」的名稱。
3. 按一下功能表圖示、然後選取 \* 啟用容量分層 \* 。



只有在 Cloud Manager 建立系統時無法啟用資料分層功能時、才會看到此選項。

在Google Cloud中、必須先將服務帳戶附加至Cloud Volumes ONTAP 無法顯示此選項的功能。確保您已符合所有要求。

4. 按一下「\* 啟用 \*」、Cloud Manager 就能建立物件存放區、供此 Cloud Volumes ONTAP 支援系統用於階層式資料。

## 確保在 **Aggregate** 上啟用分層

必須在集合體上啟用資料分層、才能在磁碟區上啟用資料分層。您應該瞭解新磁碟區和現有磁碟區的需求。

### • \* 新磁碟區 \*

如果您要在新磁碟區上啟用資料分層功能、就不需要擔心在集合體上啟用資料分層功能。Cloud Manager 會在已啟用分層功能的現有 Aggregate 上建立磁碟區、如果啟用資料分層的 Aggregate 不存在、則會為磁碟區建立新的 Aggregate。

### • \* 現有磁碟區 \*

如果您想要在現有磁碟區上啟用資料分層、則必須確保已在基礎 Aggregate 上啟用資料分層。如果在現有的 Aggregate 上未啟用資料分層、則需要使用 System Manager 將現有的 Aggregate 附加至物件存放區。

## 確認是否在 **Aggregate** 上啟用分層的步驟

1. 在 Cloud Manager 中開啟工作環境。
2. 按一下功能表圖示、按一下 \* 進階 \*、然後按一下 \* 進階分配 \*。
3. 驗證是否在 Aggregate 上啟用或停用分層。



## 在集合體上啟用分層的步驟

1. 在 System Manager 中、按一下 \* Storage > Tiers\*。
2. 按一下 Aggregate 的動作功能表、然後選取 \* 附加 Cloud Tiers\*。
3. 選取要附加的雲端層、然後按一下「\* 儲存 \*」。

您現在可以在新的和現有的磁碟區上啟用資料分層、如下一節所述。

## 從讀寫磁碟區分層資料

可將讀寫磁碟區上的非作用中資料分層保存至具成本效益的物件儲存設備、以釋出效能層以供熱資料使用。  
Cloud Volumes ONTAP

## 步驟

1. 在工作環境中、建立新磁碟區或變更現有磁碟區的層級：

工作	行動
建立新的 Volume	按一下「* 新增 Volume *」。
修改現有的 Volume	選取磁碟區、然後按一下 * 變更磁碟類型與分層原則 *。

2. 選取分層原則。

如需這些原則的說明、請參閱 ["資料分層總覽"](#)。

◦ 範例 \*



如果啟用資料分層的 Aggregate 不存在、Cloud Manager 會為磁碟區建立新的 Aggregate。

從資料保護磁碟區分層資料

可將資料從資料保護磁碟區分層至容量層。Cloud Volumes ONTAP 如果您啟動目的地 Volume、資料會隨著讀取而逐漸移至效能層。

步驟

1. 在「畫版」頁面上、選取包含來源磁碟區的工作環境、然後將其拖曳至您要複寫磁碟區的工作環境。
2. 依照提示操作、直到您到達分層頁面、並啟用資料分層以供物件儲存使用。

◦ 範例 \*



如需複寫資料的說明、請參閱 ["在雲端之間複寫資料"](#)。



## 變更階層式資料的儲存類別

部署 Cloud Volumes ONTAP 完功能後、您可以變更 30 天內未存取的非使用中資料儲存類別、藉此降低儲存成本。如果您確實存取資料、存取成本就會較高、因此在變更儲存類別之前、您必須先將此納入考量。

階層式資料的儲存類別是全系統的、並非每個 Volume 都有。

如需支援的儲存類別資訊、請參閱 ["資料分層總覽"](#)。

### 步驟

1. 在工作環境中、按一下功能表圖示、然後按一下「\* 儲存類別 \*」或「\* Blob 儲存分層 \*」。
2. 選擇一個儲存類別、然後按一下「Save」（儲存）。

## 變更資料分層的可用空間比率

資料分層的可用空間比率定義Cloud Volumes ONTAP 將資料分層儲存至物件儲存時、需要多少空間才能在物件SSD/HDD上使用。預設設定為10%可用空間、但您可以根據需求調整設定。

例如、您可以選擇少於10%的可用空間、以確保您使用購買的容量。之後、Cloud Manager可以在需要額外容量時（直到達到Aggregate的磁碟限制）、為您購買額外的磁碟。



如果空間不足、Cloud Volumes ONTAP 則無法移動資料、可能會導致效能降低。任何變更都應謹慎進行。如果您不確定、請聯絡NetApp支援部門以取得指引。

此比率對災難恢復案例非常重要、因為Cloud Volumes ONTAP 當資料從物件儲存區讀取時、將資料移至SSD/HDD以提供更好的效能。如果空間不足、Cloud Volumes ONTAP 則無法移動資料。在變更比率時、請將此納入考量、以便符合您的業務需求。

### 步驟

1. 在Cloud Manager主控台右上角、按一下\*設定\*圖示、然後選取\*連接器設定\*。



2. 在\* Capacity 下、按一下 Aggregate Capacity臨界值- Free Space Ratio for Data Tiering \*。
3. 根據您的需求變更可用空間比率、然後按一下「儲存」。

## 變更自動分層原則的冷卻週期

如果Cloud Volumes ONTAP 您使用\_auto\_分層原則在某個SURFVolume上啟用資料分層、您可以根據業務需求調整預設的冷卻時間。此動作僅支援使用API。

冷卻期間是指磁碟區中的使用者資料在被視為「冷」並移至物件儲存設備之前、必須保持非作用中狀態的天數。

自動分層原則的預設冷卻期間為31天。您可以變更冷卻期間、如下所示：

- 9.8或更新版本：2天至183天
- 9.7或更早：2天至63天

## 步驟

1. 建立磁碟區或修改現有磁碟區時、請將 `_mirumCoolingDays` 參數與 API 要求搭配使用。

## 將 LUN 連接至主機

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、請使用 IQN 從主機連線至 LUN。

請注意下列事項：

- Cloud Manager 的自動容量管理不適用於 LUN。Cloud Manager 建立 LUN 時、會停用自動擴充功能。
- 您可以從 System Manager 或 CLI 建立其他 LUN。

## 步驟

1. 在「畫版」頁面上、按兩下 Cloud Volumes ONTAP 您要管理磁碟區的「功能區」工作環境。
2. 選取磁碟區、然後按一下「\* 目標 IQN\*」。
3. 按一下「\* 複製 \*」以複製 IQN 名稱。
4. 設定從主機到 LUN 的 iSCSI 連線。
  - ["適用於 Red Hat Enterprise Linux 的支援 9 iSCSI Express 組態：啟動目標的 iSCSI 工作階段 ONTAP"](#)
  - ["適用於 Windows 的 S89 iSCSI Express 組態：以目標啟動 iSCSI 工作階段 ONTAP"](#)

## 利用 NetApp 功能加速資料存取 FlexCache

流通量是儲存磁碟區、可快取來源（或來源）磁碟區的 NFS 讀取資料。FlexCache 後續讀取快取資料會加快該資料的存取速度。

您可以使用 FlexCache 功能區來加速資料存取、或卸載大量存取磁碟區的流量。由於資料無需存取來源磁碟區、因此能夠直接提供服務、因此在用戶端需要重複存取相同資料時、支援使用者更能提升效能。FlexCache 適用於讀取密集的系統工作負載的資料量。FlexCache

Cloud Manager FlexCache 目前並未提供對各個版本的管理、但您可以使用 ONTAP CLI 或 ONTAP 功能完善的系統管理程式來建立及管理 FlexCache 各個版本：

- ["《資料存取能力快速指南》的《支援資料量》（英文） FlexCache"](#)
- ["在 FlexCache System Manager 中建立功能區"](#)

從 3.7.2 版開始、Cloud Manager 會為 FlexCache 所有的 Cloud Volumes ONTAP 全新推出的功能介紹系統產生一套功能不全的使用許可證。授權包含 500 GiB 使用限制。





## Aggregate管理

### 建立Aggregate

您可以自行建立集合體、或是讓 Cloud Manager 在建立磁碟區時為您執行集合體。自行建立集合體的好處在於、您可以選擇基礎磁碟大小、以便根據所需的容量或效能來調整集合體大小。



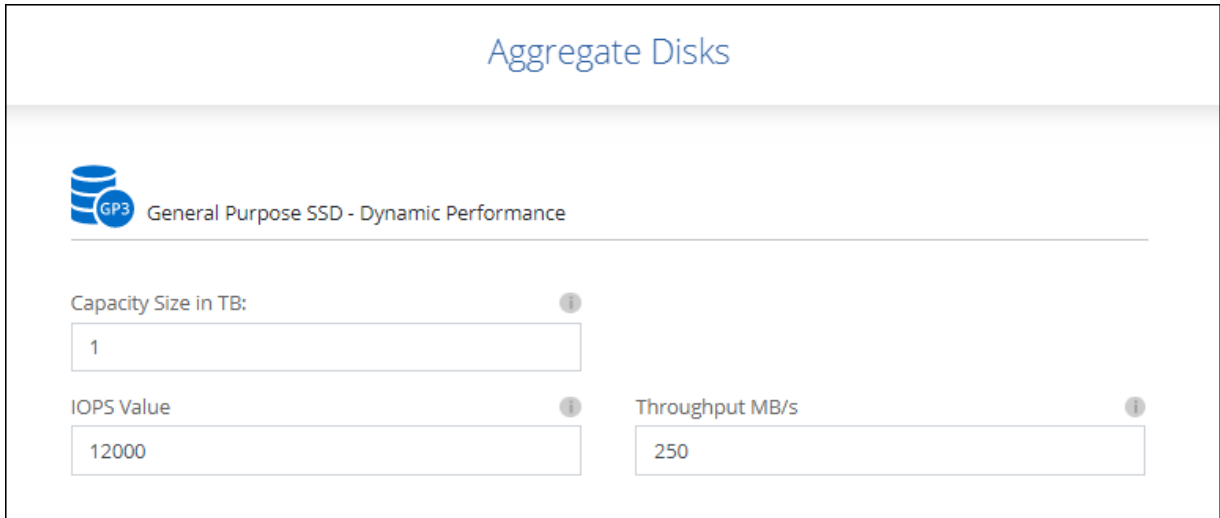
所有磁碟和集合體都必須直接從 Cloud Manager 建立和刪除。您不應從其他管理工具執行這些動作。這樣做可能會影響系統穩定性、阻礙未來新增磁碟的能力、並可能產生備援雲端供應商費用。

#### 步驟

1. 在「畫版」頁面上、按兩下 Cloud Volumes ONTAP 您要管理集合體的實例名稱。
2. 按一下功能表圖示、然後按一下 \* 進階 > 進階分配 \*。
3. 按一下「\* 新增 Aggregate \*」、然後指定 Aggregate 的詳細資料。

## AWS

- 如果系統提示您選擇磁碟類型和磁碟大小、請參閱 ["在Cloud Volumes ONTAP AWS中規劃您的不一樣組態"](#)。
- 如果系統提示您輸入Aggregate的容量大小、則表示您要在支援Amazon EBS彈性磁碟區功能的組態上建立Aggregate。下列螢幕快照顯示由GP3磁碟組成的新Aggregate範例。



["深入瞭解彈性磁碟區的支援"](#)。

## Azure

如需磁碟類型與磁碟大小的說明、請參閱 ["在Cloud Volumes ONTAP Azure中規劃您的不一樣組態"](#)。

## Google Cloud

如需磁碟類型與磁碟大小的說明、請參閱 ["在Cloud Volumes ONTAP Google Cloud規劃您的不一樣組態"](#)。

4. 按一下「\* 執行 \*」、然後按一下「\* 核准並購買 \*」。

## 管理集合體

新增磁碟、檢視有關集合體的資訊、以及刪除這些磁碟來管理集合體。



所有磁碟和集合體都必須直接從 Cloud Manager 建立和刪除。您不應從其他管理工具執行這些動作。這樣做可能會影響系統穩定性、阻礙未來新增磁碟的能力、並可能產生備援雲端供應商費用。

如果您要刪除 Aggregate、則必須先刪除 Aggregate 中的磁碟區。

如果Aggregate空間不足、您可以使用System Manager將磁碟區移至其他Aggregate。

### 步驟

1. 在「畫版」頁面上、按兩下 Cloud Volumes ONTAP 您要管理集合體的功能性工作環境。
2. 按一下功能表圖示、然後按一下 \* 進階 > 進階分配 \*。

### 3. 管理您的 Aggregate：

工作	行動
檢視有關 Aggregate 的資訊	選取一個 Aggregate、然後按一下「* 資訊 *」。
在特定 Aggregate 上建立磁碟區	選取一個 Aggregate、然後按一下「* 建立 Volume *」。
將磁碟新增至 Aggregate	<div><div>a. 選取一個Aggregate、然後按一下*「Add disks*」。</div><div>b. 選取您要新增的磁碟數目、然後按一下「* 新增 *」。</div></div> <div> 集合體中的所有磁碟大小必須相同。</div>
增加支援Amazon EBS彈性Volume的Aggregate容量	<div><div>a. 選取一個Aggregate、然後按一下*增加容量*。</div><div>b. 輸入您要新增的額外容量、然後按一下「新增」。</div></div> <p>請注意、您必須將Aggregate的容量增加至少256 GiB或集合體大小的10%。</p> <p>例如、如果您有1.77 TiB Aggregate、則10%為181 GiB。此值低於256 GiB、因此集合體的大小必須至少增加256 GiB。</p>
刪除 Aggregate	<div><div>a. 選取不包含任何磁碟區的 Aggregate、然後按一下 * 刪除 *。</div><div>b. 再按一下 * 刪除 * 以確認。</div></div>

## 儲存VM管理

### 在Cloud Manager中管理儲存VM

儲存虛擬機器是 ONTAP 執行於支援內部的虛擬機器、可為您的用戶端提供儲存與資料服務。您可能知道這是 *SVM* 或 *vserver*。根據預設、系統會設定一個儲存 VM、但部分組態會支援額外的儲存 VM。Cloud Volumes ONTAP

#### 支援的儲存 VM 數量

某些組態支援多個儲存VM。前往 "[發行說明 Cloud Volumes ONTAP](#)" 驗證Cloud Volumes ONTAP 支援的儲存VM數量是否適用於您的版本的支援。

#### 使用多個儲存VM

Cloud Manager 支援您從 System Manager 或 CLI 建立的任何其他儲存 VM。

例如、下圖顯示如何在建立 Volume 時選擇儲存 VM。

### Details & Protection

Storage VM Name

svm\_name1

Volume Name

Size (GiB)

Volume size

Snapshot Policy

default

Default Policy

下圖顯示如何在將磁碟區複製至其他系統時、選擇儲存 VM 。

Destination Volume Name

volume\_copy

Destination Storage VM Name

svm\_name1

Destination Aggregate

Automatically select the best aggregate

#### 修改預設儲存**VM**的名稱

Cloud Manager 會自動為其所建立的 Cloud Volumes ONTAP 單一儲存 VM 命名、以供其使用。如果您有嚴格的命名標準、可以修改儲存 VM 的名稱。例如、您可能希望名稱與您為 ONTAP 自己的叢集命名儲存虛擬機器的方式相符。

如果您建立 Cloud Volumes ONTAP 任何其他的儲存 VM 以供使用、則無法從 Cloud Manager 重新命名儲存 VM 。您必須 Cloud Volumes ONTAP 使用 System Manager 或 CLI 直接從支援功能進行此作業。

## 步驟

1. 在工作環境中、按一下功能表圖示、然後按一下 \* 資訊 \* 。
2. 按一下儲存 VM 名稱右側的編輯圖示。

 **Working Environment Information**

**ONTAP**

Serial Number:

System ID:

system-id-capacitytest

Cluster Name:

capacitytest

ONTAP Version:

9.7RC1

Date Created:

Jul 6, 2020 07:42:02 am

Storage VM Name:

svm\_capacitytest 

3. 在「修改 SVM 名稱」對話方塊中、變更名稱、然後按一下「\* 儲存 \*」。

## 管理儲存VM以進行災難恢復

Cloud Manager 不提供任何儲存 VM 災難恢復的設定或協調支援。您必須使用 System Manager 或 CLI 。

- ["SVM 災難恢復準備快速指南"](#)
- ["SVM Disaster Recovery Express 指南"](#)

## 在Cloud Volumes ONTAP AWS中建立資料服務儲存VM以供其使用

儲存虛擬機器是 ONTAP 執行於支援內部的虛擬機器、可為您的用戶端提供儲存與資料服務。您可能知道這是 SVM 或 vservers。根據預設、系統會設定一個儲存 VM、但部分組態會支援額外的儲存 VM。Cloud Volumes ONTAP

若要建立額外的資料服務儲存VM、您需要在AWS中分配IP位址、然後根據ONTAP 您的靜態組態執行支援功能指令。Cloud Volumes ONTAP

## 支援的儲存 VM 數量

從9.7版開始、特定Cloud Volumes ONTAP 的支援功能可支援多個儲存VM。前往 ["發行說明 Cloud Volumes ONTAP"](#) 驗證Cloud Volumes ONTAP 支援的儲存VM數量是否適用於您的版本的支援。

所有其他 Cloud Volumes ONTAP 的支援功能均支援單一資料服務儲存 VM 、以及一部用於災難恢復的目的地儲存 VM 。如果來源儲存VM發生中斷、您可以啟動目的地儲存VM進行資料存取。

### 驗證組態的限制

每個EC2執行個體都支援每個網路介面的私有IPv4位址數目上限。在AWS中為新的儲存VM分配IP位址之前、您必須先確認限制。

### 步驟

1. 請選擇 "《不知》中的「儲存限制」區段Cloud Volumes ONTAP"。
2. 識別執行個體類型的每個介面IP位址數目上限。
3. 請記下這個數字、因為您在AWS中分配IP位址時、會在下一節中需要這個數字。

### 在AWS中分配IP位址

在為新的儲存VM建立生命期之前、必須先將私有的IPv4位址指派給AWS中的連接埠e0a。

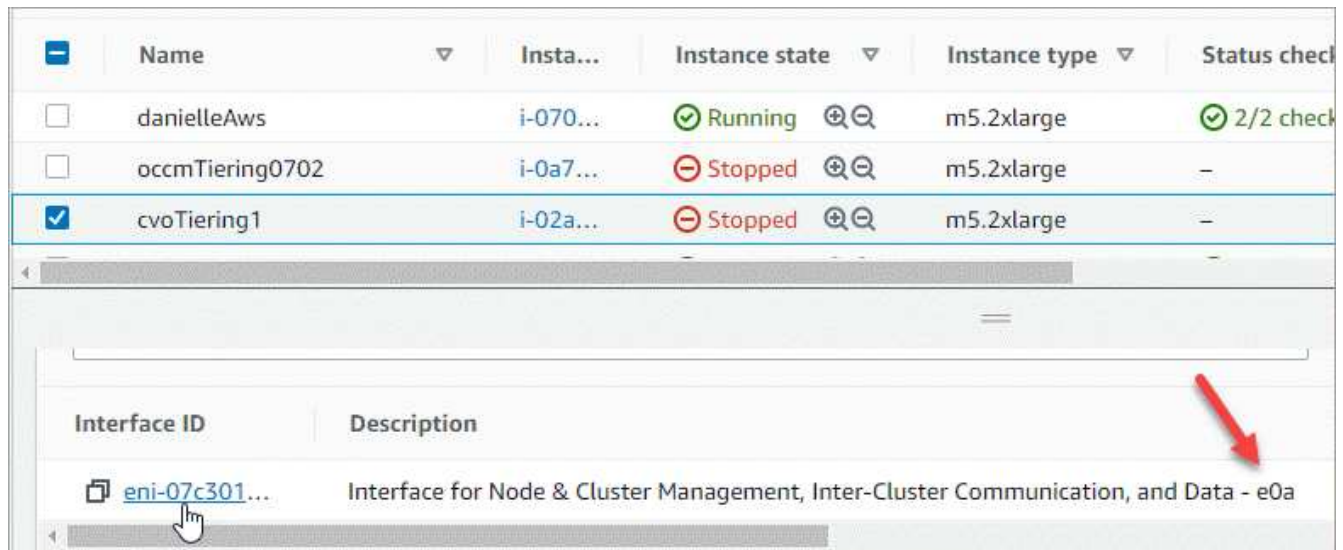
請注意、儲存VM的選用管理LIF需要在單一節點系統和單一AZ的HA配對上使用私有IP位址。此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

### 步驟

1. 登入AWS並開啟EC2服務。
2. 選取Cloud Volumes ONTAP 「這個實例」、然後按一下「網路」。

如果您要在HA配對上建立儲存VM、請選取節點1。

3. 向下捲動至\*網路介面\*、然後按一下\*介面ID\*以取得連接埠e0a。



4. 選取網路介面、然後按一下\*「動作」>「管理IP位址」\*。
5. 展開e0a的IP位址清單。
6. 驗證IP位址：
  - a. 計算已分配IP位址的數量、以確認連接埠是否有空間可用於其他IP。

您應該已經在本頁上一節中找出每個介面支援的IP位址上限。

- b. 選用：前往CLI Cloud Volumes ONTAP 執行\*網路介面show\*以確認每個IP位址都在使用中。

如果IP位址未在使用中、您可以將其與新的儲存VM搭配使用。

7. 回到AWS主控台、按一下\*指派新的IP位址\*、根據新儲存VM所需的容量來指派額外的IP位址。

- 單節點系統：需要一個未使用的次要私有IP。

若要在儲存VM上建立管理LIF、則需要選用的次要私有IP。

- 單一AZ中的HA配對：節點1上需要一個未使用的次要私有IP。

若要在儲存VM上建立管理LIF、則需要選用的次要私有IP。

- 多個AZs中的HA配對：每個節點需要一個未使用的次要私有IP。

8. 如果您要在單一AZ中分配HA配對的IP位址、請啟用\*允許重新指派次要私有IPv4位址\*。

9. 按一下「\* 儲存 \*」。

10. 如果您在多個AZs中有HA配對、則必須針對節點2重複這些步驟。

### 在單一節點系統上建立儲存VM

這些步驟可在單一節點系統上建立新的儲存VM。建立NAS LIF需要一個私有IP位址、如果您想要建立管理LIF、則需要另一個選用的私有IP位址。

#### 步驟

1. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2  
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway  
subnet_gateway
```

2. 建立NAS LIF。

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-data-files -home-port e0a -address private_ip_x -netmask  
node1Mask -lif ip_nas_2 -home-node cvo-node
```

其中\_Private IP x是e0a上未使用的次要私有IP。

3. 選用：建立儲存VM管理LIF。

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node
```

其中\_Private IP是e0a上另一個未使用的次要私有IP。

4. 將一個或多個集合體指派給儲存VM。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

這是必要步驟、因為新的儲存VM需要存取至少一個Aggregate、才能在儲存VM上建立磁碟區。

### 在單一AZ的HA配對上建立儲存VM

這些步驟可在單一AZ的HA配對上建立新的儲存VM。建立NAS LIF需要一個私有IP位址、如果您想要建立管理LIF、則需要另一個選用的私有IP位址。

這兩個生命點都會分配到節點1上。如果發生故障、私有IP位址可以在節點之間移動。

#### 步驟

1. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. 在節點1上建立NAS LIF。

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node1
```

其中\_Private IP x是CVO節點1 e0a上未使用的次要私有IP。在接管時、此IP位址可重新定位至CVO-node2的e0a、因為服務原則的預設資料檔表示IP可移轉至合作夥伴節點。

3. 選用：在節點1上建立儲存VM管理LIF。



```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-management -home-port e0a -address private_ip_y -netmask  
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

其中\_Private IP是e0a上另一個未使用的次要私有IP。

4. 將一個或多個集合體指派給儲存VM。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

這是必要步驟、因為新的儲存VM需要存取至少一個Aggregate、才能在儲存VM上建立磁碟區。

5. 如果您執行Cloud Volumes ONTAP 的是版本不含更新版本的版本、請修改儲存VM的網路服務原則。

需要修改服務、因為Cloud Volumes ONTAP 這樣可確保支援功能可將iSCSI LIF用於傳出管理連線。

```

network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client

```

## 在多個AZs的HA配對上建立儲存VM

這些步驟可在多個AZs的HA配對上建立新的儲存VM。

NAS LIF需要浮動 IP位址、管理LIF則為選用。這些浮動IP位址不需要您在AWS中分配私有IP。而是會在AWS路由表中自動設定浮動IP、以指向同一個VPC中的特定節點ENI。

為了讓浮動IP能夠搭配ONTAP 使用、必須在每個節點上的每個儲存VM上設定私有IP位址。這反映在以下步驟中、其中iSCSI LIF是在節點1和節點2上建立。

### 步驟

1. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2  
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway  
subnet_gateway
```

## 2. 在節點1上建立NAS LIF。

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-data-files -home-port e0a -address floating_ip -netmask  
node1Mask -lif ip_nas_floating_2 -home-node cvo-node1
```

- 在部署HA組態的AWS區域中、所有VPC的浮動IP位址必須位於CIDR區塊之外。192 · 168 · 0 · 27是一個浮動IP地址的例子。"[深入瞭解如何選擇浮動IP位址](#)"。
- 「服務原則預設資料檔案」表示IP可以移轉至合作夥伴節點。

## 3. 選用：在節點1上建立儲存VM管理LIF。

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-management -home-port e0a -address floating_ip -netmask  
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

## 4. 在節點1上建立iSCSI LIF。

```
network interface create -vserver svm_2 -service-policy default-data-  
blocks -home-port e0a -address private_ip -netmask node1Mask -lif  
ip_node1_iscsi_2 -home-node cvo-node1
```

- 此iSCSI LIF是支援儲存VM中浮動IP的LIF移轉所必需的。它不一定是iSCSI LIF、但無法設定在節點之間移轉。
- 「服務原則預設資料區塊」表示IP位址不會在節點之間移轉。
- \_Private IP是CVO節點1的eth0 (e0a) 上未使用的次要私有IP位址。

## 5. 在節點2上建立iSCSI LIF。

```
network interface create -vserver svm_2 -service-policy default-data-  
blocks -home-port e0a -address private_ip -netmaskNode2Mask -lif  
ip_node2_iscsi_2 -home-node cvo-node2
```

- 此iSCSI LIF是支援儲存VM中浮動IP的LIF移轉所必需的。它不一定是iSCSI LIF、但無法設定在節點之間

移轉。

- 「服務原則預設資料區塊」表示IP位址不會在節點之間移轉。
- \_Private IP是CVO節點2的eth0 (e0a) 上未使用的次要私有IP位址。

6. 將一個或多個集合體指派給儲存VM。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

這是必要步驟、因為新的儲存VM需要存取至少一個Aggregate、才能在儲存VM上建立磁碟區。

7. 如果您執行Cloud Volumes ONTAP 的是版本不含更新版本的版本、請修改儲存VM的網路服務原則。

需要修改服務、因為Cloud Volumes ONTAP 這樣可確保支援功能可將iSCSI LIF用於傳出管理連線。

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client
```

## 在Cloud Volumes ONTAP Azure中建立資料服務儲存VM以供其使用

儲存虛擬機器是 ONTAP 執行於支援內部的虛擬機器、可為您的用戶端提供儲存與資料服務。您可能知道這是 SVM 或 vservers。根據預設、系統會設定一個儲存VM、但在Azure上執行時、則支援其他儲存VM。Cloud Volumes ONTAP Cloud Volumes ONTAP

若要建立額外的資料服務儲存VM、您必須在Azure中配置IP位址、然後執行ONTAP 支援功能指令、以建立儲存VM和資料LIF。

### 支援的儲存 VM 數量

從9.9.0版本開始、特定Cloud Volumes ONTAP 的支援功能可支援多個儲存VM。前往 ["發行說明 Cloud Volumes ONTAP"](#) 驗證Cloud Volumes ONTAP 支援的儲存VM數量是否適用於您的版本的支援。

所有其他 Cloud Volumes ONTAP 的支援功能均支援單一資料服務儲存 VM 、以及一部用於災難恢復的目的地儲存 VM 。如果來源儲存VM發生中斷、您可以啟動目的地儲存VM進行資料存取。

### 在Azure中配置IP位址

您必須先在Azure中配置IP位址、才能建立儲存VM並分配LIF。

#### 單一節點系統

在您建立儲存VM並分配LIF之前、必須先將IP位址指派給Azure中的nic0。

您需要為資料LIF存取建立IP位址、並為儲存VM (SVM) 管理LIF建立另一個選用的IP位址。此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

#### 步驟

1. 登入Azure入口網站、然後開啟\*虛擬機器\*服務。
2. 按一下Cloud Volumes ONTAP 「不完整虛擬機器」的名稱。
3. 按一下\*網路\*。
4. 按一下nic0的網路介面名稱。
5. 在\*設定\*下、按一下\* IP組態\*。
6. 按一下「\* 新增 \*」。
7. 輸入IP組態的名稱、選取\*動態\*、然後按一下\*確定\*。
8. 按一下您剛才建立的IP組態名稱、將\*指派\*變更為\*靜態\*、然後按一下\*儲存\*。

最好使用靜態IP位址、因為靜態IP可確保IP位址不會變更、有助於避免不必要的應用程式中斷運作。

如果您要建立SVM管理LIF、請重複這些步驟以建立其他IP位址。

複製您剛建立的私有IP位址。當您為新的儲存VM建立生命期時、必須指定這些IP位址。

#### HA配對

如何為HA配對分配IP位址、取決於您使用的儲存傳輸協定。

## iSCSI

在您建立儲存VM並分配LIF之前、必須先將iSCSI IP位址指派給Azure中的nic0。iSCSI的IPS會指派給nic0而非負載平衡器、因為iSCSI會使用ALUA進行容錯移轉。

您需要建立下列IP位址：

- 從節點1存取iSCSI資料LIF的IP位址
- 從節點2存取iSCSI資料LIF的IP位址
- 儲存VM（SVM）管理LIF的選用IP位址

此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

### 步驟

1. 登入Azure入口網站、然後開啟\*虛擬機器\*服務。
2. 按一下Cloud Volumes ONTAP 節點1的「支援不支援虛擬機器」名稱。
3. 按一下\*網路\*。
4. 按一下nic0的網路介面名稱。
5. 在\*設定\*下、按一下\* IP組態\*。
6. 按一下「\* 新增 \*」。
7. 輸入IP組態的名稱、選取\*動態\*、然後按一下\*確定\*。
8. 按一下您剛才建立的IP組態名稱、將\*指派\*變更為\*靜態\*、然後按一下\*儲存\*。

最好使用靜態IP位址、因為靜態IP可確保IP位址不會變更、有助於避免不必要的應用程式中斷運作。

9. 在節點2上重複這些步驟。
10. 如果您要建立SVM管理LIF、請在節點1上重複這些步驟。

## NFS

您用於NFS的IP位址會配置在負載平衡器中、以便在發生容錯移轉事件時、IP位址可以移轉到其他節點。

您需要建立下列IP位址：

- 單一IP位址、可從節點1存取NAS資料LIF
- 單一IP位址、可從節點2存取NAS資料LIF
- 儲存VM（SVM）管理LIF的選用IP位址

此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

### 步驟

1. 在Azure入口網站中、開啟\*負載平衡器\*服務。
2. 按一下HA配對的負載平衡器名稱。
3. 從節點1建立資料LIF存取的前端IP組態、從節點2存取資料LIF的前端IP組態、以及儲存VM（SVM）管

理LIF的另一個選用前端IP。

- a. 在\*設定\*下、按一下\*前端IP組態\*。
- b. 按一下「\*新增\*」。
- c. 輸入前端IP的名稱、選取Cloud Volumes ONTAP 該子網路做為「靜態HA配對」、保留「動態」選項、並在「可用區域」中保留「區域-備援」選項、以確保區域故障時IP位址仍可繼續使用。

The screenshot shows the Microsoft Azure portal interface for configuring a load balancer. The breadcrumb navigation is 'Home > Load balancing > azureha1011s3-rg-lb >'. The main heading is 'Add frontend IP configuration'. Below the heading, the resource name 'azureha1011s3-rg-lb' is displayed. The configuration form includes the following fields:

- Name \***: A text input field containing 'ip-for-svm2' with a checkmark icon on the right.
- Virtual network**: A dropdown menu showing 'Default-Networking-vnet'.
- Subnet \***: A dropdown menu showing 'default (172.19.2.0/24)' with a downward arrow icon.
- Assignment**: Two radio buttons, 'Dynamic' (which is selected) and 'Static'.
- Availability zone \***: A dropdown menu showing 'Zone-redundant' with a downward arrow icon.

- d. 按一下您剛才建立的前端IP組態名稱、將\*指派\*變更為\*靜態\*、然後按一下\*儲存\*。

最好使用靜態IP位址、因為靜態IP可確保IP位址不會變更、有助於避免不必要的應用程式中斷運作。

4. 為您剛建立的每個前端IP新增健全狀況探查。

- a. 在負載平衡器的\*設定\*下、按一下\*健全狀況探查\*。
- b. 按一下「\*新增\*」。
- c. 輸入健全狀況探針的名稱、然後輸入介於63005和65000之間的連接埠號碼。保留其他欄位的預設值。

連接埠號碼必須介於63005和65000之間。例如、如果您要建立三個健全狀況探針、可以輸入使用連接埠編號63005、63006和63007的探針。

Microsoft Azure

Search resources, services, and

[Home](#) > [Load balancers](#) > [azureha1011s3-rg-lb](#) >

## Add health probe ...

azureha1011s3-rg-lb

Name *	svm2-health-probe1	✓
Protocol *	TCP	▼
Port * ⓘ	63005	✓
Interval * ⓘ	5	seconds
Unhealthy threshold * ⓘ	2	consecutive failures
Used by ⓘ	Not used	

5. 為每個前端IP建立新的負載平衡規則。
  - a. 在負載平衡器的\*設定\*下、按一下\*負載平衡規則\*。
  - b. 按一下\*「Add\*（新增\*）」、然後輸入所需資訊：
    - 名稱：輸入規則的名稱。
    - \* IP Version ：選取 IPV\*。
    - 前端IP位址：選取您剛建立的前端IP位址之一。
    - \* HA連接埠\*：啟用此選項。
    - 後端集區：保留已選取的預設後端集區。
    - 健全狀況探查：選取您為所選前端IP所建立的健全狀況探查。
    - 工作階段持續性：選取\*無\*。
    - 浮動IP：選擇\*已啟用\*。



## Add load balancing rule

chandanaTcpRst3-rg-lb

**i** A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

**Name \***

jimmy\_new\_rule ✓

**IP Version \***

☒ IPv4 ☐ IPv6

**Frontend IP address \*** ⓘ

10.1.0.156 (dataAFIP) ▼

☒ HA Ports ⓘ

**Backend pool** ⓘ

backendPool (2 virtual machines) ▼

**Health probe** ⓘ

dataAProbe (TCP:63002) ▼

**Session persistence** ⓘ

None ▼

**Floating IP** ⓘ

☐ Disabled ☒ Enabled

6. 確認Cloud Volumes ONTAP 適用於此功能的網路安全群組規則可讓負載平衡器針對上述步驟4所建立的健全狀況探查傳送TCP探查。請注意、這是預設允許的。

### 中小企業

用於SMB資料的IP位址會配置在負載平衡器中、以便在發生容錯移轉事件時、IP位址可以移轉到其他節點。

您需要建立下列IP位址：

- 單一IP位址、可從節點1存取NAS資料LIF
- 單一IP位址、可從節點2存取NAS資料LIF
- 節點1上iSCSI LIF的一個IP位址
- 節點2上iSCSI LIF的一個IP位址

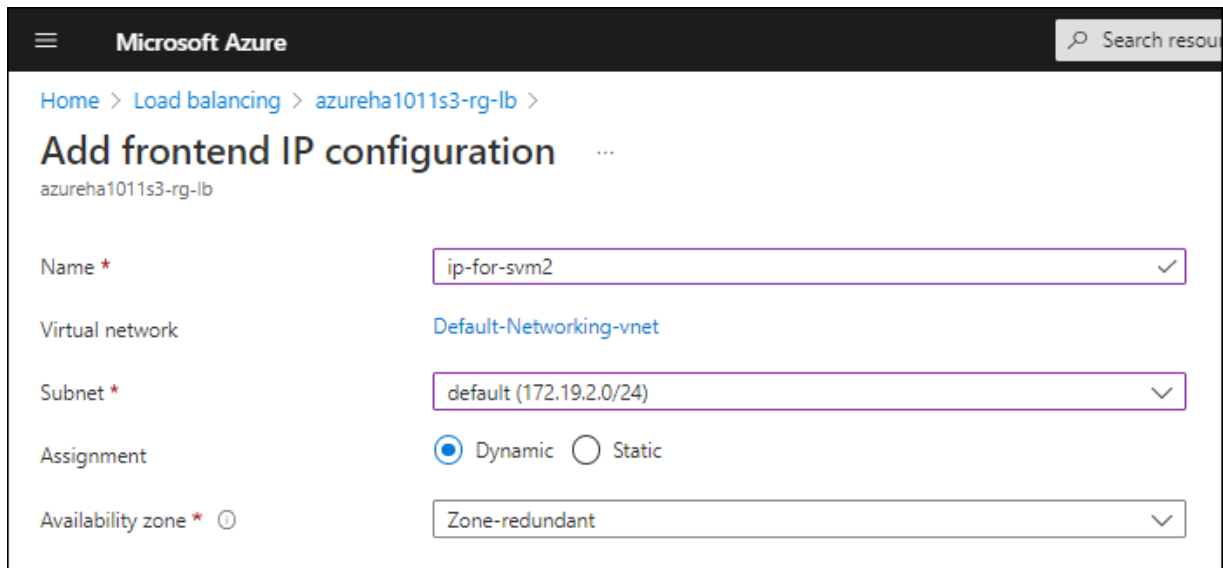
DNS和SMB通訊需要iSCSI LIF。iSCSI LIF用於此用途、因為它不會在容錯移轉時移轉。

- 儲存VM（SVM）管理LIF的選用IP位址

此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

## 步驟

1. 在Azure入口網站中、開啟\*負載平衡器\*服務。
2. 按一下HA配對的負載平衡器名稱。
3. 建立所需的前端IP組態數目：
  - a. 在\*設定\*下、按一下\*前端IP組態\*。
  - b. 按一下「\*新增\*」。
  - c. 輸入前端IP的名稱、選取Cloud Volumes ONTAP 該子網路做為「靜態HA配對」、保留「動態」選項、並在「可用區域」中保留「區域-備援」選項、以確保區域故障時IP位址仍可繼續使用。



The screenshot shows the 'Add frontend IP configuration' page in the Microsoft Azure portal. The breadcrumb navigation is 'Home > Load balancing > azureha1011s3-rg-lb >'. The title is 'Add frontend IP configuration' with a three-dot menu icon. Below the title is the resource name 'azureha1011s3-rg-lb'. The form contains the following fields:

- Name \***: A text box containing 'ip-for-svm2' with a checkmark icon on the right.
- Virtual network**: A text box containing 'Default-Networking-vnet'.
- Subnet \***: A dropdown menu showing 'default (172.19.2.0/24)' with a downward arrow.
- Assignment**: Two radio buttons, 'Dynamic' (selected) and 'Static'.
- Availability zone \* ⓘ**: A dropdown menu showing 'Zone-redundant' with a downward arrow.

- d. 按一下您剛才建立的前端IP組態名稱、將\*指派\*變更為\*靜態\*、然後按一下\*儲存\*。
- 最好使用靜態IP位址、因為靜態IP可確保IP位址不會變更、有助於避免不必要的應用程式中斷運作。
4. 為您剛建立的每個前端IP新增健全狀況探查。
    - a. 在負載平衡器的\*設定\*下、按一下\*健全狀況探查\*。
    - b. 按一下「\*新增\*」。
    - c. 輸入健全狀況探針的名稱、然後輸入介於63005和65000之間的連接埠號碼。保留其他欄位的預設值。

連接埠號碼必須介於63005和65000之間。例如、如果您要建立三個健全狀況探針、可以輸入使用連接埠編號63005、63006和63007的探針。

Microsoft Azure

Search resources, services, and

[Home](#) > [Load balancers](#) > [azureha1011s3-rg-lb](#) >

## Add health probe

azureha1011s3-rg-lb

Name *	svm2-health-probe1	✓
Protocol *	TCP	▼
Port * ⓘ	63005	✓
Interval * ⓘ	5	seconds
Unhealthy threshold * ⓘ	2	consecutive failures
Used by ⓘ	Not used	

5. 為每個前端IP建立新的負載平衡規則。
- 在負載平衡器的\*設定\*下、按一下\*負載平衡規則\*。
  - 按一下\*「Add\*（新增\*）」、然後輸入所需資訊：
    - 名稱：輸入規則的名稱。
    - \* IP Version ：選取 IPV\*。
    - 前端IP位址：選取您剛建立的前端IP位址之一。
    - \* HA連接埠\*：啟用此選項。
    - 後端集區：保留已選取的預設後端集區。
    - 健全狀況探查：選取您為所選前端IP所建立的健全狀況探查。
    - 工作階段持續性：選取\*無\*。
    - 浮動IP：選擇\*已啟用\*。

## Add load balancing rule

chandanaTcpRst3-rg-lb

**i** A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name \*

jimmy\_new\_rule

IP Version \*



IPv4



IPv6

Frontend IP address \* ⓘ

10.1.0.156 (dataAFIP)

☒ HA Ports ⓘ

Backend pool ⓘ

backendPool (2 virtual machines)

Health probe ⓘ

dataProbe (TCP:63002)

Session persistence ⓘ

None

Floating IP ⓘ

Disabled

Enabled

6. 確認Cloud Volumes ONTAP 適用於此功能的網路安全群組規則可讓負載平衡器針對上述步驟4所建立的健全狀況探查傳送TCP探查。請注意、這是預設允許的。

複製您剛建立的私有IP位址。當您為新的儲存VM建立生命期時、必須指定這些IP位址。

### 建立儲存VM和LIF

在Azure中配置IP位址之後、您可以在單一節點系統或HA配對上建立新的儲存VM。

#### 單一節點系統

如何在單一節點系統上建立儲存VM和LIF、取決於您使用的儲存傳輸協定。

## iSCSI

請依照下列步驟建立新的儲存VM、以及所需的LIF。

### 步驟

1. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. 建立資料LIF：

```
network interface create -vserver <svm-name> -home-port e0a -address  
<iscsi-ip-address> -lif <lif-name> -home-node <name-of-node1> -data  
-protocol iscsi
```

3. 選用：建立儲存VM管理LIF。

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node node1 -status-admin up -failover-policy  
system-defined -firewall-policy mgmt -home-port e0a -auto-revert  
false -failover-group Default
```

4. 將一個或多個集合體指派給儲存VM。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

這是必要步驟、因為新的儲存VM需要存取至少一個Aggregate、才能在儲存VM上建立磁碟區。

## NFS

請依照下列步驟建立新的儲存VM、以及所需的LIF。

### 步驟

1. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

## 2. 建立資料LIF：

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol cifs,nfs -address <nfs-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy disabled -firewall-policy data -home-port e0a -auto  
-revert true -failover-group Default
```

## 3. 選用：建立儲存VM管理LIF。

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node node1 -status-admin up -failover-policy  
system-defined -firewall-policy mgmt -home-port e0a -auto-revert  
false -failover-group Default
```

## 4. 將一個或多個集合體指派給儲存VM。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

這是必要步驟、因為新的儲存VM需要存取至少一個Aggregate、才能在儲存VM上建立磁碟區。

### 中小企業

請依照下列步驟建立新的儲存VM、以及所需的LIF。

#### 步驟

### 1. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>
```

## 2. 建立資料LIF：

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol cifs,nfs -address <nfs-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy disabled -firewall-policy data -home-port e0a -auto
-revert true -failover-group Default
```

## 3. 選用：建立儲存VM管理LIF。

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node node1 -status-admin up -failover-policy
system-defined -firewall-policy mgmt -home-port e0a -auto-revert
false -failover-group Default
```

## 4. 將一個或多個集合體指派給儲存VM。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

這是必要步驟、因為新的儲存VM需要存取至少一個Aggregate、才能在儲存VM上建立磁碟區。

## HA配對

如何在HA配對上建立儲存VM和LIF、取決於您使用的儲存傳輸協定。

## iSCSI

請依照下列步驟建立新的儲存VM、以及所需的LIF。

### 步驟

1. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. 建立資料生命量：

- a. 使用下列命令在節點1上建立iSCSI LIF。

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-  
node1> -data-protocol iscsi
```

- b. 使用下列命令在節點2上建立iSCSI LIF。

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-  
node2> -data-protocol iscsi
```

3. 選用：在節點1上建立儲存VM管理LIF。

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node node1 -status-admin up -failover-policy  
system-defined -firewall-policy mgmt -home-port e0a -auto-revert  
false -failover-group Default
```

此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

4. 將一個或多個集合體指派給儲存VM。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```



這是必要步驟、因為新的儲存VM需要存取至少一個Aggregate、才能在儲存VM上建立磁碟區。

5. 如果您執行Cloud Volumes ONTAP 的是版本不含更新版本的版本、請修改儲存VM的網路服務原則。

需要修改服務、因為Cloud Volumes ONTAP 這樣可確保支援功能可將iSCSI LIF用於傳出管理連線。

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client
```

## NFS

請依照下列步驟建立新的儲存VM、以及所需的LIF。

### 步驟

1. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

## 2. 建立資料生命量：

### a. 使用下列命令在節點1上建立NAS LIF。

```
network interface create -vserver <svm-name> -lif <lif-name>  
-role data -data-protocol cifs,nfs -address <nfs--ip-address>  
-netmask-length <length> -home-node <name-of-nodel> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe1>
```

### b. 使用下列命令在節點2上建立NAS LIF。

```
network interface create -vserver <svm-name> -lif <lif-name>  
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>  
-netmask-length <length> -home-node <name-of-node2> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe2>
```

## 3. 選用：在節點1上建立儲存VM管理LIF。

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node node1 -status-admin up -failover-policy  
system-defined -firewall-policy mgmt -home-port e0a -auto-revert  
false -failover-group Default -probe-port <port-number-for-azure-  
health-probe3>
```

此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

## 4. 將一個或多個集合體指派給儲存VM。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

這是必要步驟、因為新的儲存VM需要存取至少一個Aggregate、才能在儲存VM上建立磁碟區。

5. 如果您執行Cloud Volumes ONTAP 的是版本不含更新版本的版本、請修改儲存VM的網路服務原則。

需要修改服務、因為Cloud Volumes ONTAP 這樣可確保支援功能可將iSCSI LIF用於傳出管理連線。

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client
```

#### 中小企業

請依照下列步驟建立新的儲存VM、以及所需的LIF。

#### 步驟

1. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

## 2. 建立NAS資料生命量：

### a. 使用下列命令在節點1上建立NAS LIF。

```
network interface create -vserver <svm-name> -lif <lif-name>  
-role data -data-protocol cifs,nfs -address <nfs-ip-address>  
-netmask-length <length> -home-node <name-of-node1> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe1>
```

### b. 使用下列命令在節點2上建立NAS LIF。

```
network interface create -vserver <svm-name> -lif <lif-name>  
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>  
-netmask-length <length> -home-node <name-of-node2> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe2>
```

## 3. 建立iSCSI LIF以提供DNS與SMB通訊：

### a. 使用下列命令在節點1上建立iSCSI LIF。

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-  
node1> -data-protocol iscsi
```

### b. 使用下列命令在節點2上建立iSCSI LIF。

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-  
node2> -data-protocol iscsi
```

## 4. 選用：在節點1上建立儲存VM管理LIF。

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node node1 -status-admin up -failover-policy
system-defined -firewall-policy mgmt -home-port e0a -auto-revert
false -failover-group Default -probe-port <port-number-for-azure-
health-probe3>
```

此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

5. 將一個或多個集合體指派給儲存VM。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

這是必要步驟、因為新的儲存VM需要存取至少一個Aggregate、才能在儲存VM上建立磁碟區。

6. 如果您執行Cloud Volumes ONTAP 的是版本不含更新版本的版本、請修改儲存VM的網路服務原則。  
需要修改服務、因為Cloud Volumes ONTAP 這樣可確保支援功能可將iSCSI LIF用於傳出管理連線。

```

network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client

```

在HA配對上建立儲存VM之後、最好先等待12小時、再在該SVM上配置儲存設備。Cloud Manager從Cloud Volumes ONTAP 發行版的《截至目前為止》開始、會在12小時的時間間隔內掃描HA配對負載平衡器的設定。如果有新的SVM、Cloud Manager會啟用可縮短非計畫性容錯移轉的設定。

## 在Cloud Volumes ONTAP Google Cloud中建立資料服務儲存VM以供其使用

儲存虛擬機器是 ONTAP 執行於支援內部的虛擬機器、可為您的用戶端提供儲存與資料服務。您可能知道這是 SVM 或 vservers。根據預設、系統會設定一個儲存 VM、但部分組態會支援額外的儲存 VM。Cloud Volumes ONTAP

### 支援的儲存 VM 數量

從9.11.1版開始、Cloud Volumes ONTAP Google Cloud中的特定支援功能可支援多個儲存VM。前往 ["發行說明"](#)

Cloud Volumes ONTAP" 驗證Cloud Volumes ONTAP 支援的儲存VM數量是否適用於您的版本的支援。

所有其他 Cloud Volumes ONTAP 的支援功能均支援單一資料服務儲存 VM 、以及一部用於災難恢復的目的地儲存 VM 。如果來源儲存VM發生中斷、您可以啟動目的地儲存VM進行資料存取。

## 建立儲存VM

如果授權支援、您可以在單一節點系統或HA配對上建立多個儲存VM。請注意、您必須使用Cloud Manager API 在HA配對上建立儲存VM、而您可以使用CLI或System Manager在單一節點系統上建立儲存VM。

### 單一節點系統

這些步驟使用CLI在單一節點系統上建立新的儲存VM。建立資料LIF需要一個私有IP位址、如果您想要建立管理LIF、則需要另一個選用的私有IP位址。

### 步驟

1. 在Google Cloud中、移至Cloud Volumes ONTAP 「實例」、並為每個LIF新增一個IP位址至nic0。

**Edit network interface**

Network \*  
default

Subnetwork \*  
default IPv4 (10.138.0.0/20)

**i** To use IPv6, you need an IPv6 subnet range. [LEARN MORE](#)

**IP stack type**

☒ IPv4 (single-stack)

☐ IPv4 and IPv6 (dual-stack)

Primary internal IP  
gcpvco-vm-ip-nic0-nodemgmt (10.138.0.46)

**Alias IP ranges**

Subnet range	Alias IP range *
Subnet range 1 Primary (10.138.0.0/20)	Alias IP range 1 * 10.138.0.25/32
Subnet range 2 Primary (10.138.0.0/20)	Alias IP range 2 * 10.138.0.23/32
Subnet range 3 Primary (10.138.0.0/20)	Alias IP range 3 * 10.138.0.21/32
Subnet range 4 Primary (10.138.0.0/20)	Alias IP range 4 * 10.138.0.31/32

**+ ADD IP RANGE**

External IPv4 address  
None

如果您想在儲存VM上建立管理LIF、則需要一個IP位址用於資料LIF、另一個選用IP位址。

"Google Cloud文件：新增別名IP範圍至現有執行個體"

2. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

```
vserver create -vserver <svm-name> -subtype default -rootvolume <root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name> -gateway <ip-of-gateway-server>
```

3. 指定您在Google Cloud中新增的IP位址、以建立資料LIF。



## iSCSI

```
network interface create -vserver <svm-name> -home-port e0a -address  
<iscsi-ip-address> -lif <lif-name> -home-node <name-of-node1> -data  
-protocol iscsi
```

## NFS或SMB

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol cifs,nfs -address <nfs-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy disabled -firewall-policy data -home-port e0a -auto  
-revert true -failover-group Default
```

4. 選用：指定您在Google Cloud中新增的IP位址、以建立儲存VM管理LIF。

```
network interface create -vserver <svm-name> -lif <lif-name> -role data  
-data-protocol none -address <svm-mgmt-ip-address> -netmask-length  
<length> -home-node node1 -status-admin up -failover-policy system-  
defined -firewall-policy mgmt -home-port e0a -auto-revert false  
-failover-group Default
```

5. 將一個或多個集合體指派給儲存VM。

```
vserver add-aggregates -vserver <svm-name> -aggregates <aggr1,aggr2>
```

這是必要步驟、因為新的儲存VM需要存取至少一個Aggregate、才能在儲存VM上建立磁碟區。

## HA配對

您必須使用Cloud Manager API在Cloud Volumes ONTAP Google Cloud的一套系統上建立儲存VM。因為Cloud Manager會使用所需的LIF服務、以及傳出SMB/CIFS通訊所需的iSCSI LIF來設定儲存VM、因此需要使用API（而非System Manager或CLI）。

請注意、Cloud Manager會在Google Cloud中配置所需的IP位址、並使用資料LIF來建立儲存VM、以進行SMB/NFS存取、並使用iSCSI LIF來進行傳出SMB通訊。

從3.9.19版本開始、Connector需要下列權限、才能建立及管理Cloud Volumes ONTAP 適用於各個HA配對的儲存VM：

- `compute.instanceGroups.get`
- `compute.addresses.get`

這些權限包含在中 ["NetApp 提供的原則"](#)

#### 步驟

1. 使用下列API呼叫建立儲存VM：

「POST /occm/api/gcp/ha/辦公 環境/ {we\_ID} /svm/」

申請機構應包括下列項目：

```
{ "svmName": "myNewSvm1" }
```

### 管理HA配對上的儲存VM

Cloud Manager API也支援重新命名及刪除HA配對上的儲存VM。

#### 重新命名儲存VM

如有需要、您可以隨時變更儲存VM的名稱。

#### 步驟

1. 使用下列API呼叫重新命名儲存VM：

「PPUT /occm/API/GCP / ha /工作環境/ {we ID} /SVM」

申請機構應包括下列項目：

```
{  
  "svmNewName": "newSvmName",  
  "svmName": "oldSvmName"  
}
```

#### 刪除儲存VM

如果您不再需要儲存VM、可以從Cloud Volumes ONTAP 停止功能中刪除。

#### 步驟

1. 使用下列API呼叫來刪除儲存VM：

「刪除/occm/api/gcp/ha/工作 環境/ {we\_ID} /Svm/ {Svm\_name} 」

## 安全性與資料加密

使用 **NetApp** 加密解決方案加密磁碟區

支援NetApp Volume Encryption (NVE) 和NetApp Aggregate Encryption (NAE) Cloud

Volumes ONTAP。NVE和NAE是軟體型解決方案、可啟用FIPS 140-2標準的磁碟區閒置資料加密功能。"深入瞭解這些加密解決方案"。

外部金鑰管理程式支援NVE和NAE。

新的Aggregate在您設定外部金鑰管理程式之後、預設會啟用NAE。非 NAE Aggregate 一部分的新磁碟區預設會啟用 NVE（例如、如果在設定外部金鑰管理程式之前已建立現有的 Aggregate）。

不支援內建金鑰管理。Cloud Volumes ONTAP

您的支援系統應該已向 NetApp 註冊。Cloud Volumes ONTAP NetApp Volume Encryption授權會自動安裝在Cloud Volumes ONTAP 每個註冊NetApp支援的支援系統上。

- "新增 NetApp 支援網站帳戶至 Cloud Manager"
- "註冊隨用隨付系統"



Cloud Manager 不會在中國地區的系統上安裝 NVE 授權。

#### 步驟

1. 檢閱中支援的關鍵管理程式清單 "NetApp 互通性對照表工具"。



搜尋 \* 關鍵經理 \* 解決方案。

2. "連線 Cloud Volumes ONTAP 至 CLI"。
3. 設定外部金鑰管理。
  - AWS："如ONTAP 需相關指示、請參閱《產品資訊》文件"
  - Azure："Azure Key Vault (AKV) "
  - Google Cloud："Google Cloud金鑰管理服務"

## 使用Azure Key Vault管理金鑰

您可以使用 "Azure Key Vault (AKV) " 在ONTAP Azure部署的應用程式中保護您的不加密金鑰。

AKV可用於保護 "NetApp Volume Encryption (NVE) 金鑰" 僅適用於資料SVM。

使用AKV的金鑰管理可透過CLI或ONTAP REST API來啟用。

使用AKV時、請注意、預設會使用資料SVM LIF與雲端金鑰管理端點進行通訊。節點管理網路用於與雲端供應商的驗證服務 (login.microsoftonline.com) 進行通訊。如果叢集網路設定不正確、叢集將無法正確使用金鑰管理服務。

#### 先決條件

- 必須執行9.10.1版或更新版本Cloud Volumes ONTAP
- 已安裝Volume Encryption (VE) 授權 (NetApp Volume Encryption授權會自動安裝在Cloud Volumes ONTAP 向NetApp支援註冊的每個支援系統上)
- 已安裝多租戶加密金鑰管理 (MTEKM) 授權

- 您必須是叢集或SVM管理員
- 現用Azure訂閱

#### 限制

- AKV只能在資料SVM上設定

#### 組態程序

概述的步驟將說明如何向Cloud Volumes ONTAP Azure註冊您的「還原組態」、以及如何建立Azure Key Vault和金鑰。如果您已經完成這些步驟、請確定您擁有正確的組態設定、尤其是在中 [建立Azure Key Vault](#)，然後繼續 [組態Cloud Volumes ONTAP](#)。

- [Azure應用程式註冊](#)
- [建立Azure用戶端機密](#)
- [建立Azure Key Vault](#)
- [建立加密金鑰](#)
- [建立Azure Active Directory端點（僅限HA）](#)
- [組態Cloud Volumes ONTAP](#)

#### Azure應用程式註冊

1. 您必須先在Azure訂閱中註冊您的應用程式Cloud Volumes ONTAP、才能使用此功能來存取Azure Key Vault。在Azure入口網站中、選取「應用程式註冊」。
2. 選擇「\*\*新登錄」。
3. 提供應用程式名稱、並選取支援的應用程式類型。Azure Key Vault使用預設的單一租戶即可滿足需求。選擇「註冊」。
4. 在Azure Overview（Azure總覽）視窗中、選取您已註冊的應用程式。將應用程式（用戶端）ID \*和\*目錄（租戶）ID \*複製到安全位置。在稍後的註冊程序中、將會需要這些工具。

#### 建立Azure用戶端機密

1. 在Azure入口網站Cloud Volumes ONTAP 中、選取「認證與機密」窗格。
2. 選取「\*\*新用戶端機密」\*輸入有意義的用戶端機密名稱。NetApp建議使用24個月的到期日、不過您的特定雲端治理原則可能需要不同的設定。
3. 選取「\*新增」以儲存用戶端機密。立即複製機密的\*值\*、並將其儲存在安全的地方、以供未來設定使用。在您離開頁面後、不會顯示機密值。

#### 建立Azure Key Vault

1. 如果您有現有的Azure Key Vault、您可以將其連線Cloud Volumes ONTAP 至您的功能表組態、不過您必須將存取原則調整為此程序中的設定。
2. 在Azure入口網站中、瀏覽至「\*\*關鍵故障」區段。
3. 選擇「建立」。輸入所需資訊、包括資源群組、地區和價格層、並選擇保留刪除的保存資料室的天數、以及是否啟用清除保護。就本組態而言、預設值已足夠、不過您的特定雲端治理原則可能需要不同的設定。
4. 選擇「\*下一步」以選擇存取原則。
5. 選擇「\* Azure Disk Encryption\*（\* Azure磁碟加密）」作為磁碟區加密選項、選擇「\* Vault存取原則\*」作

為權限模式。

6. 選取「\*\*新增存取原則」。
7. 選取「自範本設定」（選用）字段旁邊的插入號。然後選擇「\*\*金鑰、機密與認證管理」
8. 選擇每個下拉式權限功能表（金鑰、秘密、憑證）、然後在功能表清單頂端選擇所有\*、以選取所有可用的權限。您應該擁有：
  - 關鍵權限：19個已選取
  - \*\*機密權限：選擇8項
  - 認證權限：16項已選取
9. 選取「\*新增」以建立存取原則。
10. 選擇「下一步」進入「\*網路」\*選項。
11. 選擇適當的網路存取方法、或選擇「所有網路」和「審查+建立」來建立金鑰保存庫。（網路存取方法可能由治理原則或您的企業雲端安全團隊規定。）
12. 記錄金鑰庫URI：在您建立的金鑰庫中、瀏覽至「總覽」功能表、然後從右側欄複製「\*\* Vault URI」。您稍後將需要此功能。

#### 建立加密金鑰

1. 在您為Cloud Volumes ONTAP 之建立的Key Vault功能表中、瀏覽至「\*\* Keys」選項。
2. 選取「產生/匯入」以建立新的金鑰。
3. 將預設選項設為「\*\*產生」。
4. 提供下列資訊：
  - 加密金鑰名稱
  - 金鑰類型：RSA
  - RSA金鑰大小：2048
  - 已啟用：是
5. 選取「建立」以建立加密金鑰。
6. 返回「\*\*按鍵」功能表、然後選取您剛建立的按鍵。
7. 在「目前版本」下方選取金鑰ID、即可檢視金鑰內容。
8. 找到「\*\*金鑰識別碼」欄位。將URI複製到但不包括十六進位字串。

#### 建立Azure Active Directory端點（僅限HA）

1. 只有在您將Azure Key Vault設定為HA Cloud Volumes ONTAP 功能環境時、才需要執行此程序。
2. 在Azure入口網站中、瀏覽至「\*\*虛擬網路」。
3. 選取部署Cloud Volumes ONTAP 了整個功能區的虛擬網路、然後選取頁面左側的「\*\*Subnets」（子網路）功能表。
4. 從Cloud Volumes ONTAP 清單中選取要部署的子網路名稱。
5. 瀏覽至「服務端點\*」標題。在下拉式功能表中、從清單中選取「Microsoft.AzureActiveDirectory」。
6. 選取「\*\*儲存」以擷取您的設定。

## 組態Cloud Volumes ONTAP

1. 使用您偏好的SSH用戶端連線至叢集管理LIF。
2. 進入進階權限模式ONTAP：「et advanc進 階-con Off」（設定進階-con Off）
3. 識別所需的資料SVM、並驗證其DNS組態：「vserver services name-service DNS show」
  - a. 如果所需資料SVM的DNS項目存在、且其中包含Azure DNS項目、則不需要採取任何行動。如果沒有、請為資料SVM新增DNS伺服器項目、以指向Azure DNS、私有DNS或內部部署伺服器。這應該符合叢集管理SVM的項目：「vserver services name-service DNS create -vserver *svm\_name*-domain *\_name* -servers *ip\_address*」
  - b. 確認已為資料SVM建立DNS服務：「vserver services name-service DNS show」
4. 使用應用程式登錄後儲存的用戶端ID和租戶ID來啟用Azure Key Vault：「安全金鑰管理程式外部azure enable -vserver *Svm\_name*-client-id *Azure*用戶端\_*ID*-租 戶ID *Azure*租戶\_*ID*-name *Azure*金鑰名稱-key-id *Azure*金鑰\_*ID*」
5. 驗證金鑰管理程式組態：「安全金鑰管理程式外部azure show」
6. 檢查金鑰管理程式的狀態：「安全金鑰管理程式外部azure檢查」輸出內容如下：

```
::*> security key-manager external azure check

Vserver: data_svm_name
Node: akvlab01-01

Category: service_reachability
Status: OK

Category: ekvip_server
Status: OK

Category: kms_wrapped_key_status
Status: UNKNOWN
Details: No volumes created yet for the vserver. Wrapped KEK status
will be available after creating encrypted volumes.

3 entries were displayed.
```

如果「連線能力」狀態不是「正常」、SVM將無法以所有必要的連線和權限來連線至Azure Key Vault服務。初始組態時、「kms」迴應鍵狀態會報告「unkNOWNKNOWNKY」。第一個磁碟區加密後、其狀態會變更為「OK（正常）」。

7. 選用：建立測試Volume以驗證NVE的功能。

```
「vol create -vserver Svm_name-volume vol/Volume_name-Aggregate aggr _-size _size-state online
-policy default」
```

如果設定正確、Cloud Volumes ONTAP 則會自動建立Volume並啟用Volume加密。

8. 確認磁碟區已正確建立並加密。如果是的話、「-is-Encrypted」參數會顯示為「true」。「vol show

-vserver *svm\_name*-Fields is加密」

## 利用Google的雲端金鑰管理服務來管理金鑰

您可以使用 "[Google Cloud Platform的金鑰管理服務（雲端KMS）](#)" 在ONTAP Google Cloud Platform部署的應用程式中保護您的不加密金鑰。

雲端KMS的金鑰管理可透過CLI或ONTAP REST API啟用。

使用Cloud KMS時、請注意、預設會使用資料SVM LIF與雲端金鑰管理端點進行通訊。節點管理網路用於與雲端供應商的驗證服務（[oauth2.googleapis.com](#)）進行通訊。如果叢集網路設定不正確、叢集將無法正確使用金鑰管理服務。

### 先決條件

- 必須執行9.10.1版或更新版本Cloud Volumes ONTAP
- 已安裝Volume Encryption（VE）授權
- 已安裝多租戶加密金鑰管理（MTEKM）授權
- 您必須是叢集或SVM管理員
- 現用Google Cloud Platform訂閱

### 限制

- 雲端KMS只能在資料SVM上設定

### 組態

#### Google Cloud

1. 在您的Google Cloud環境中、"[建立對稱的GCP金鑰環和金鑰](#)"。
2. 為Cloud Volumes ONTAP 您的服務帳戶建立自訂角色。

```
gcloud iam roles create kmsCustomRole
  --project=<project_id>
  --title=<kms_custom_role_name>
  --description=<custom_role_description>

  --permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersions.
list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.
useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.loca
tions.get,cloudkms.locations.list,resourceManager.projects.get
  --stage=GA
```

3. 將自訂角色指派給Cloud KMS金鑰與Cloud Volumes ONTAP 更新服務帳戶：「gCloud kms金鑰add-iam-policy-binding *key\_name*-keyring *key\_ring\_name*-location -member *ServiceAccount* : *\_service\_Account\_Name*-role專案/*customer\_project\_id*/ros/ros/kmsCustomrole」
4. 下載服務帳戶Json金鑰：「gCloud iam服務帳戶金鑰可建立金鑰檔案-iam-account=*sa-name*@*project-id*.iam.gserviceaccount.com」

## Cloud Volumes ONTAP

1. 使用您偏好的SSH用戶端連線至叢集管理LIF。
2. 切換至進階權限等級：「et -priv榮幸 進階」
3. 為資料SVM建立DNS。「建立網域C\_<project >\_internal -name-servers server\_address-vserver Svm\_name」
4. 建立CMEK項目：「安全金鑰管理程式外部GCP啟用-vserver Svm\_name-project -id project \_-key-ring\_name \_key\_ring\_name-key-ring\_location key\_ring\_stip-key-name key\_name」
5. 出現提示時、請從GCP帳戶輸入服務帳戶Json金鑰。
6. 確認啟用的程序成功：「安全金鑰管理程式外部GCP檢查-vserver svm\_name」
7. 選用：建立磁碟區以測試加密「volvol create volvolvole\_name-Aggregate Aggregate \_-vserver \_vserver\_name-size 10G」

### 疑難排解

如果您需要疑難排解、可以跳接上述最後兩個步驟中的原始REST API記錄：

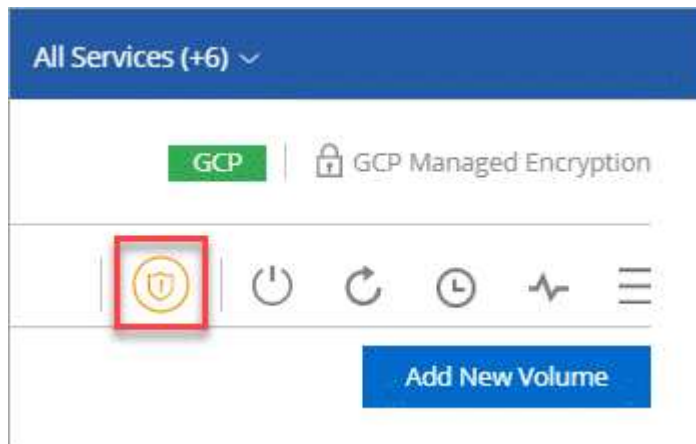
1. "以d為準"
2. "ystemShell -node\_node\_-command tail -f /mroot/etc/log/mlog/kmip2\_client.log"

## 改善防範勒索軟體的能力

勒索軟體攻擊可能會耗費一定的時間、資源和商譽。Cloud Manager 可讓您針對勒索軟體實作 NetApp 解決方案、提供有效的可見度、偵測及補救工具。

### 步驟

1. 在工作環境中、按一下 \* 勒索軟體 \* 圖示。



2. 實作 NetApp 勒索軟體解決方案：
  - a. 如果您的磁碟區未啟用 Snapshot 原則、請按一下「\* 啟動 Snapshot Policy\*」。

NetApp Snapshot 技術提供業界最佳的勒索軟體補救解決方案。成功還原的關鍵在於從未受感染的備份還原。Snapshot 複本為唯讀、可防止勒索軟體毀損。他們也能提供精細度、以建立單一檔案複本或完整災難恢復解決方案的映像。



- b. 按一下「\* 啟動 FPolicy\*」以啟用 ONTAP 的 FPolicy 解決方案、此解決方案可根據檔案副檔名來封鎖檔案作業。

這項預防解決方案可封鎖常見的勒索軟體檔案類型、藉此改善保護、避免勒索軟體攻擊。

預設 FPolicy 範圍會封鎖下列副檔名的檔案：

微、加密、鎖定、加密、加密、crinf、r5a、XRNT、XDBL、R16M01D05、Pzdc、好、好！、天哪！、RDM、RRK、加密RS、crjoker、EnCipErEd、LeChiffre



Cloud Manager 會在 Cloud Volumes ONTAP 啟用 FPolicy on 功能時建立此範圍。此清單是根據常見的勒索軟體檔案類型。您可以使用 Cloud Volumes ONTAP 來自於整個 CLI 的 `_vserver fpolicy scoon__` 命令來自訂封鎖的副檔名。

### Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

#### 1 Enable Snapshot Copy Protection

50 %  
Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes

Activate Snapshot Policy

#### 2 Block Ransomware File Extensions

ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

[View Denied File Names](#)

Activate FPolicy

## 系統管理

### 升級 Cloud Volumes ONTAP 版軟體

從 Cloud Volumes ONTAP Cloud Manager 升級功能、即可存取最新的功能與增強功能。升級軟體之前、您應該先準備 Cloud Volumes ONTAP 好用的不一樣系統。

#### 升級總覽

在開始 Cloud Volumes ONTAP 進行還原升級程序之前、您應該注意下列事項。

#### 僅從 Cloud Manager 升級

必須從 Cloud Manager 完成升級。Cloud Volumes ONTAP 您不應 Cloud Volumes ONTAP 使用 System Manager 或 CLI 來升級功能。這樣做可能會影響系統穩定性。

#### 如何升級

Cloud Manager 提供兩種升級 Cloud Volumes ONTAP 方法：

- 在工作環境中顯示升級通知之後
- 將升級映像放在HTTPS位置、然後提供Cloud Manager URL

#### 支援的升級途徑

您可以升級的版本取決於您目前執行的版本。Cloud Volumes ONTAP Cloud Volumes ONTAP

目前版本	您可以直接升級至的版本
9.11.0	9.11.1.
9.10.1	9.11.1.
	9.11.0
9.10.0%	9.10.1
9.9.1	9.10.1
	9.10.0%
9.9.0	9.9.1
9.8	9.9.1
9.7	9.8
9.6	9.7
9.5.	9.6
9.4	9.5.
9.3	9.4
9.2	9.3
9.1	9.2
9.0	9.1
8.3	9.0

請注意下列事項：

- 支援的升級途徑Cloud Volumes ONTAP 與內部部署ONTAP 的內部部署的更新途徑不同。
- 如果您依照工作環境中顯示的升級通知進行升級、Cloud Manager會提示您升級至遵循這些支援升級途徑的版本。
- 如果您將升級映像放在HTTPS位置進行升級、請務必遵循這些支援的升級途徑。
- 在某些情況下、您可能需要升級數次才能達到目標版本。

例如、如果您執行的是9.8版、而且想要升級至9.10.1版、則必須先升級至9.9.1版、然後再升級至9.10.1版。

#### 還原或降級

不Cloud Volumes ONTAP 支援還原或降級至先前版本的功能。

## 支援註冊

必須向 NetApp 支援部門註冊、才能使用本頁所述的任何方法來升級軟體。Cloud Volumes ONTAP 這適用於 PAYGO 和 BYOL。您需要 ["手動登錄 PAYGO 系統"](#)、但 BYOL 系統預設為註冊。



尚未註冊支援的系統仍會在有新版本可用時收到 Cloud Manager 中顯示的軟體更新通知。但您必須先註冊系統、才能升級軟體。

## HA 中介程序的升級

Cloud Manager 也會在 Cloud Volumes ONTAP 升級過程中視需要更新中介執行個體。

## 準備升級

執行升級之前、您必須先確認系統已就緒、並進行任何必要的組態變更。

- [\[Plan for downtime\]](#)
- [\[Verify that automatic giveback is still enabled\]](#)
- [\[Suspend SnapMirror transfers\]](#)
- [\[Verify that aggregates are online\]](#)

## 計畫停機時間

當您升級單節點系統時、升級程序會使系統離線長達 25 分鐘、在此期間 I/O 會中斷。

升級 HA 配對不中斷營運、而且 I/O 不中斷。在此不中斷營運的升級程序中、會同時升級每個節點、以繼續為用戶端提供 I/O 服務。

## 確認自動恢復功能仍啟用

自動恢復必須在 Cloud Volumes ONTAP 一個「無法恢復的 HA 配對」上啟用（這是預設設定）。如果沒有、則作業將會失敗。

["供應說明文件：設定自動恢復的命令 ONTAP"](#)

## 暫停 SnapMirror 傳輸

如果 Cloud Volumes ONTAP 某個不活躍的 SnapMirror 關係、最好在更新 Cloud Volumes ONTAP 該軟件之前暫停傳輸。暫停傳輸可防止 SnapMirror 故障。您必須暫停來自目的地系統的傳輸。



即使 Cloud Backup 使用 SnapMirror 實作來建立備份檔案（稱為 SnapMirror Cloud）、升級系統時也不需要暫停備份。

這些步驟說明如何使用系統管理程式來執行 9.3 版及更新版本。

## 步驟

1. 從目的地系統登入 System Manager。

您可以將網頁瀏覽器指向叢集管理 LIF 的 IP 位址、以登入 System Manager。您可以在 Cloud Volumes ONTAP 不工作環境中找到 IP 位址。



您要從其中存取 Cloud Manager 的電腦、必須有連至 Cloud Volumes ONTAP NetApp 的網路連線。例如、您可能需要從雲端供應商網路中的跨接主機登入 Cloud Manager。

2. 按一下 \* 保護 > 關係 \*。
3. 選取關係、然後按一下 \* 作業 > 靜止 \*。

驗證Aggregate是否在線上

更新軟體之前、必須先在線上安裝適用於 Cloud Volumes ONTAP 此功能的 Aggregate。在大多數的組態中、Aggregate 都應該處於線上狀態、但如果沒有、則應該將其上線。

這些步驟說明如何使用系統管理程式來執行 9.3 版及更新版本。

步驟

1. 在工作環境中、按一下功能表圖示、然後按一下 \* 進階 > 進階配置 \*。
2. 選取 Aggregate、按一下 \* Info\*、然後確認狀態為線上。

aggr1		
Aggregate Capacity:	88.57 GB	
-----		
Used Aggregate Capacity:	1.07 GB	
-----		
Volumes:	2	▼
-----		
AWS Disks:	1	▼
-----		
State:	online	

3. 如果 Aggregate 離線、請使用 System Manager 將 Aggregate 上線：
  - a. 按一下「\* 儲存設備 > 集合體與磁碟 > Aggregate \*」。
  - b. 選取 Aggregate、然後按一下 \* 更多動作 > 狀態 > 線上 \*。

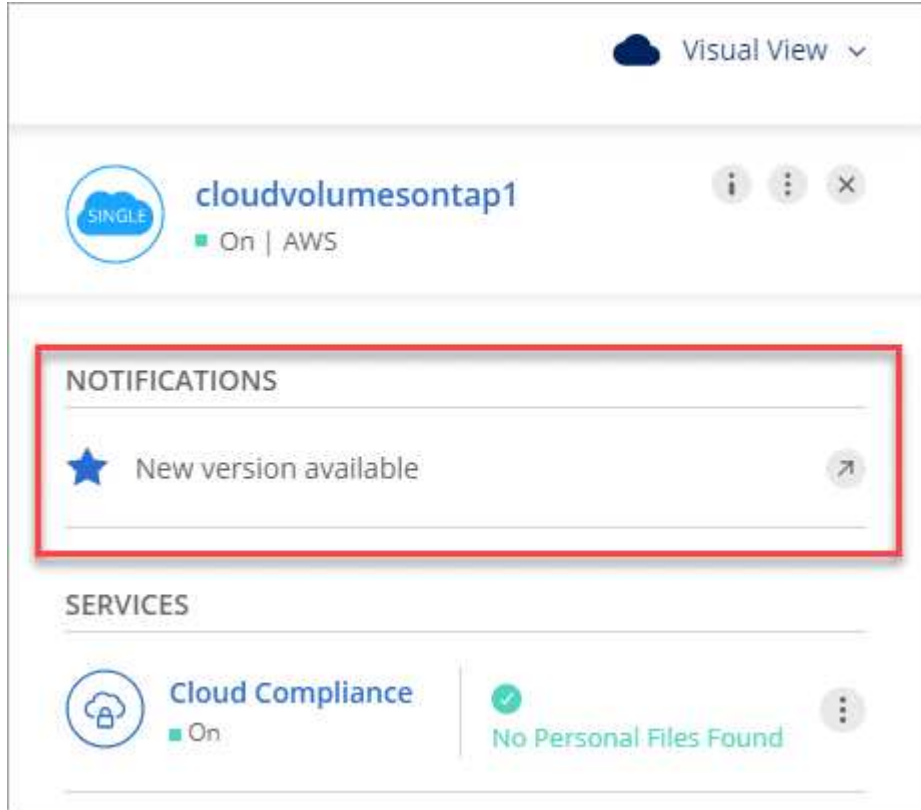
## 升級Cloud Volumes ONTAP

Cloud Manager會在有新版本可供升級時通知您。您可以從此通知開始升級程序。如需詳細資訊、請參閱 [\[Upgrade from Cloud Manager notifications\]](#)。

使用外部URL上的映像執行軟體升級的另一種方法。如果 Cloud Manager 無法存取 S3 儲存區來升級軟體、或是您已獲得修補程式、此選項將會很有幫助。如需詳細資訊、請參閱 [\[Upgrade from an image available at a URL\]](#)。

## 從Cloud Manager通知升級

Cloud Manager Cloud Volumes ONTAP 會在出現新版 Cloud Volumes ONTAP 的功能時、於不支援功能的環境中顯示通知：



您可以從此通知開始升級程序、從 S3 儲存區取得軟體映像、安裝映像、然後重新啟動系統、藉此自動化程序。

Cloud Manager作業（例如Volume或Aggregate建立）不得在Cloud Volumes ONTAP 作業系統上進行。

### 步驟

1. 按一下 \* Canvas\* 。
2. 選取工作環境。

如果有新版本可用、則右窗格中會出現通知：



3. 如果有可用的新版本、請按一下 \* 升級 \* 。
4. 在「版本資訊」頁面中、按一下連結以閱讀指定版本的「版本說明」、然後選取「\* 我讀過 ... \*」核取方塊。
5. 在「終端使用者授權合約（EULA）」頁面中、閱讀 EULA、然後選取「\* 我閱讀並核准 EULA\*」。
6. 在「檢閱與核准」頁面中、閱讀重要附註、選取 \* 我瞭解 ... \*、然後按一下 \* 執行 \* 。

Cloud Manager 會啟動軟體升級。軟體更新完成後、即可在工作環境中執行動作。

如果您暫停 SnapMirror 傳輸、請使用 System Manager 繼續傳輸。

從URL提供的映像升級

您可以將Cloud Volumes ONTAP ImageSoft映像放在Connector或HTTP伺服器上、然後從Cloud Manager開始軟體升級。如果 Cloud Manager 無法存取 S3 儲存區來升級軟體、您可以使用此選項。

Cloud Manager作業（例如Volume或Aggregate建立）不得在Cloud Volumes ONTAP 作業系統上進行。

步驟

1. 選用：設定HTTP伺服器、以裝載Cloud Volumes ONTAP 支援此功能的軟體映像。

如果您有虛擬網路的VPN連線、您可以將Cloud Volumes ONTAP 該Imagesoftware映像放在您自己網路中的HTTP伺服器上。否則、您必須將檔案放在雲端的HTTP伺服器上。

2. 如果您使用自己的安全群組Cloud Volumes ONTAP 來執行功能、請確定傳出規則允許HTTP連線Cloud Volumes ONTAP 、以便讓畫面能夠存取軟體映像。



預設情況下、預先定義Cloud Volumes ONTAP 的「支援HTTP連線」安全群組會允許傳出HTTP連線。

3. 從取得軟體映像 ["NetApp 支援網站"](#)。
4. 將軟體映像複製到Connector上的目錄、或是將從其中提供檔案的HTTP伺服器上。

例如、您可以將軟體映像複製到Connector上的下列路徑：

`/opt/application/netapp/cloudmanager/dock_occm/data/ontap / imes/`

5. 在 Cloud Manager 的工作環境中、按一下功能表圖示、然後按一下 \* 進階 > 更新 Cloud Volumes ONTAP \*。
6. 在「更新軟體」頁面上輸入URL、然後按一下「變更映像」。

如果您將軟體映像複製到上述路徑中的Connector、請輸入下列URL：

`http://<Connector-private-IP-address>/ontap/images/<image-file-name>`

7. 按 \* Proceed\* 確認。

Cloud Manager 會啟動軟體更新。軟體更新完成後、即可在工作環境中執行動作。

如果您暫停 SnapMirror 傳輸、請使用 System Manager 繼續傳輸。

### 修正使用Google Cloud NAT閘道時的下載失敗

Connector會自動下載Cloud Volumes ONTAP 適用於更新的軟體。如果您的組態使用Google Cloud NAT閘道、下載可能會失敗。您可以限制軟體映像分成的零件數量來修正此問題。此步驟必須使用Cloud Manager API完成。

#### 步驟

1. 將PUT要求提交至/occm/config、並以下列Json做為本文：

```
{
  "maxDownloadSessions": 32
}
```

`_MaxDownloadSseds_` 的值可以是1或任何大於1的整數。如果值為1、則下載的映像不會分割。

請注意、32為範例值。您應該使用的值取決於NAT組態和可同時使用的工作階段數目。

["深入瞭解/occm/config API呼叫"](#)。

### 註冊隨用隨付系統

NetApp提供的支援包含Cloud Volumes ONTAP 在整個過程中、但您必須先向NetApp註冊系統、才能啟動支援。

向 NetApp 註冊 PAYGO 系統時、必須 ONTAP 使用任何方法來升級 \_\_LW\_NETAPP 軟體 ["本頁說明"](#)。



尚未註冊支援的系統仍會在有新版本可用時收到 Cloud Manager 中顯示的軟體更新通知。但您必須先註冊系統、才能升級軟體。

#### 步驟

1. 如果您尚未將 NetApp 支援網站帳戶新增至 Cloud Manager 、請前往 \* 帳戶設定 \* 、立即新增帳戶。

["瞭解如何新增 NetApp 支援網站帳戶"](#)。

2. 在「畫版」頁面上、按兩下您要註冊的系統名稱。
3. 按一下功能表圖示、然後按一下 \* 支援註冊 \* ：



4. 選擇 NetApp 支援網站帳戶、然後按一下 \* 註冊 \* 。

Cloud Manager 會向 NetApp 註冊系統。

## 管理 **Cloud Volumes ONTAP** 功能不全

您可以從 Cloud Volumes ONTAP Cloud Manager 停止並開始執行功能、以管理雲端運算成本。

### 排程 **Cloud Volumes ONTAP** 自動關閉功能

您可能想要在 Cloud Volumes ONTAP 特定時間間隔內關閉此功能、以降低運算成本。您可以將 Cloud Manager 設定為在特定時間自動關機、然後重新啟動系統、而非手動執行此動作。

#### 關於這項工作

- 排定 Cloud Volumes ONTAP 自動關機功能時、如果執行中的資料傳輸正在進行、Cloud Manager 會將關機時間延後。

Cloud Manager 會在傳輸完成後關閉系統。

- 此工作會排程 HA 配對中兩個節點的自動關機。
- 透過 Cloud Volumes ONTAP 排定的關機功能關閉功能時、不會建立開機和根磁碟的快照。



只有在執行手動關機時、才會自動建立快照、如下一節所述。

#### 步驟

1. 在工作環境中、按一下時鐘圖示：



2. 指定關機排程：

- a. 選擇您要每天、每個工作日、每個週末或三種選項的任意組合來關閉系統。
- b. 指定您要關閉系統的時間、以及關閉系統的時間長度。

#### ▪ 範例 \*

下圖顯示每週六上午 12 : 00 指示 Cloud Manager 關閉系統的排程48 小時。Cloud Manager 每週一上午 12 : 00 重新啟動系統

<input type="checkbox"/>	Turn off every weekday Mon, Tue, Wed, Thu, Fri	turn off at	08 : 00 PM	for	12	Hours (1-24)
<input checked="" type="checkbox"/>	Turn off every weekend Sat	turn off at	12 : 00 AM	for	48	Hours (1-48)

3. 按一下「\* 儲存 \*」。

Cloud Manager 會儲存排程。時鐘圖示會變更、表示已設定排程：



## 停止 Cloud Volumes ONTAP

停止 Cloud Volumes ONTAP 使用功能可節省運算成本、並建立根磁碟和開機磁碟的快照、有助於疑難排解。



為了降低成本、Cloud Manager會定期刪除較舊的根磁碟和開機磁碟快照。根磁碟和開機磁碟只會保留兩個最新的快照。

當您停止 HA 配對時、Cloud Manager 會關閉兩個節點。

#### 步驟

1. 在工作環境中、按一下 \* 關閉 \* 圖示。



2. 保留建立快照的選項、因為快照可以啟用系統還原。

3. 按一下 \* 關閉 \* 。

停止系統可能需要幾分鐘的時間。您可以稍後從工作環境頁面重新啟動系統。

## 使用 NTP 同步系統時間

指定 NTP 伺服器可同步處理網路中系統之間的時間、有助於避免時間差異所造成的問題。

使用指定NTP伺服器 ["Cloud Manager API"](#) 或從使用者介面進行 ["建立CIFS伺服器"](#)。

## 修改系統寫入速度

Cloud Manager 可讓您選擇 Cloud Volumes ONTAP 一般或高速寫入速度來執行功能。預設寫入速度為正常。如果工作負載需要快速寫入效能、您可以改為高速寫入。

所有類型的單一節點系統和部分HA配對組態均支援高速寫入。檢視中支援的組態 ["發行說明 Cloud Volumes ONTAP"](#)

在變更寫入速度之前、您應該先進行 ["瞭解一般與高設定之間的差異"](#)。

關於這項工作

- 確保磁碟區或集合體建立等作業未在進行中。
- 請注意、這項變更會重新啟動Cloud Volumes ONTAP 整個系統。這是一項中斷營運的程序、需要整個系統停機。

步驟

1. 在工作環境中、按一下功能表圖示、然後按一下 \* 進階 > 寫入速度 \* 。
2. 選擇 \* 正常 \* 或 \* 高 \* 。

如果您選擇「高」、則必須閱讀「我瞭解 ...」聲明、並勾選方塊以確認。

3. 按一下「\* 儲存 \*」、檢閱確認訊息、然後按一下「\* 繼續 \*」。

## 變更Cloud Volumes ONTAP 密碼以供使用

包含叢集管理帳戶。Cloud Volumes ONTAP如有需要、您可以從 Cloud Manager 變更此帳戶的密碼。



您不應透過 System Manager 或 CLI 變更管理帳戶的密碼。密碼不會反映在 Cloud Manager 中。因此 Cloud Manager 無法正確監控執行個體。

步驟

1. 在工作環境中、按一下功能表圖示、然後按一下 \* 進階 > 設定密碼 \* 。
2. 輸入新密碼兩次、然後按一下「\* 儲存 \*」。

新密碼必須與您最近使用的六個密碼之一不同。

## 新增、移除或刪除系統

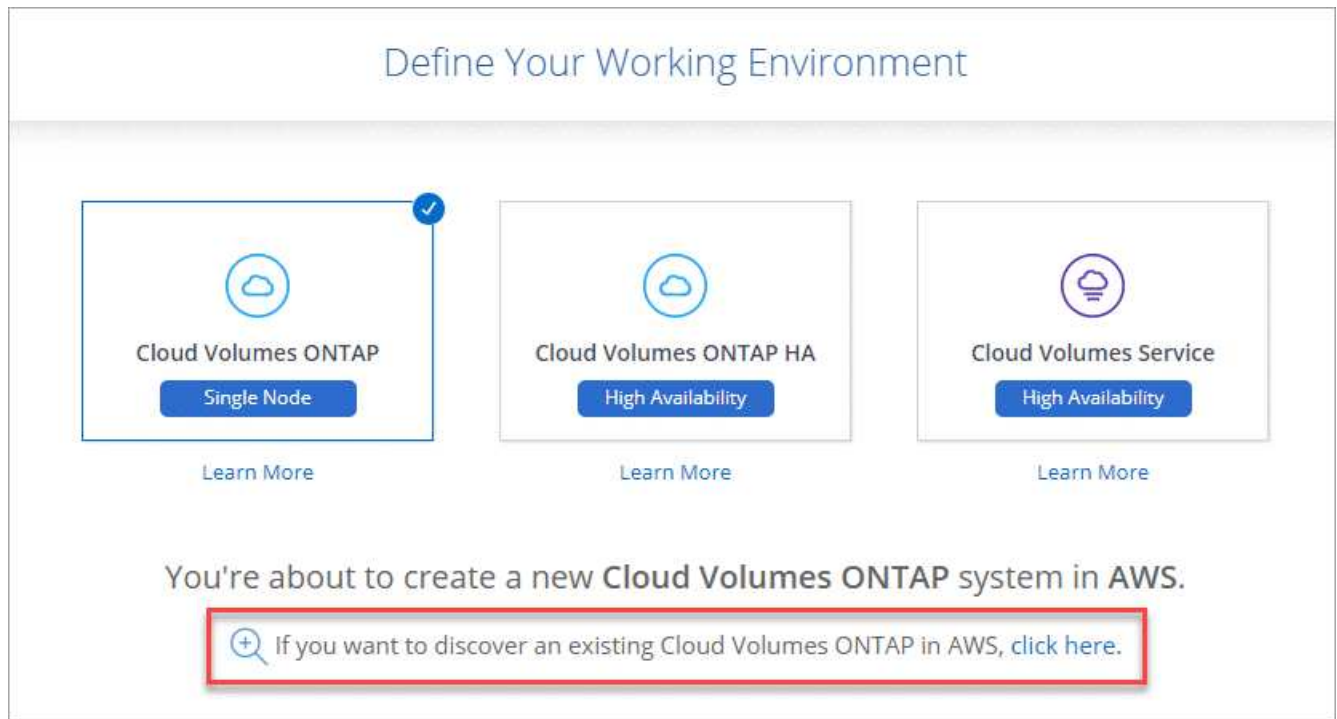
將現有 **Cloud Volumes ONTAP** 的功能系統新增至 **Cloud Manager**

您可以探索並新增 Cloud Volumes ONTAP 現有的 NetApp 系統至 Cloud Manager。如果您部署了新的 Cloud Manager 系統、您可以這麼做。

您必須知道 Cloud Volumes ONTAP 該密碼才能使用此功能。

### 步驟

1. 在「畫版」頁面上、按一下「\* 新增工作環境 \*」。
2. 選取系統所在的雲端供應商。
3. 選擇 Cloud Volumes ONTAP 哪種類型的系統。
4. 按一下連結以探索現有系統。



5. 在「區域」頁面上、選擇執行個體所在的區域、然後選取執行個體。
6. 在「認證資料」頁面上、輸入 Cloud Volumes ONTAP for the fu位 管理員使用者的密碼、然後按一下「\* 執行 \*」。

Cloud Manager 會將 Cloud Volumes ONTAP 這些不全的執行個體新增至工作區。

### 移除 **Cloud Volumes ONTAP** 運作環境

帳戶管理員可移除 Cloud Volumes ONTAP 運作中的環境、將其移至其他系統、或疑難排解探索問題。

移除 Cloud Volumes ONTAP 功能不全的工作環境、將其從 Cloud Manager 中移除。它不會刪除 Cloud Volumes ONTAP 此作業系統。您稍後可以重新探索工作環境。

從 Cloud Manager 移除工作環境可讓您執行下列動作：

- 在另一個工作區重新探索
- 從另一個 Cloud Manager 系統重新探索
- 如果在初始探索期間發生問題、請重新探索

#### 步驟

1. 在 Cloud Manager 主控台右上角、按一下「設定」圖示、然後選取 \* 「工具」 \* 。



2. 在「工具」頁面中、按一下 \* 「啟動 \*」 。
3. 選取 Cloud Volumes ONTAP 您要移除的「不工作環境」。
4. 在「Review and Approve」（檢閱並核准）頁面上、按一下「 \* Go \* 」 。

Cloud Manager 會移除工作環境。使用者可隨時從「畫版」頁面重新探索此工作環境。

#### 刪除Cloud Volumes ONTAP 一個系統

您應該一律從Cloud Volumes ONTAP Cloud Manager刪除不適用的系統、而不要從雲端供應商的主控制台刪除。例如、如果您從Cloud Volumes ONTAP 雲端供應商處終止授權的樣例、則無法將授權金鑰用於其他執行個體。您必須從 Cloud Manager 刪除工作環境、才能釋出授權。

刪除工作環境時、Cloud Manager會終止Cloud Volumes ONTAP 執行個體、並刪除磁碟和快照。

刪除工作環境時、不會刪除由其他服務（例如雲端備份與雲端資料感測與監控執行個體）管理的資源。您必須自行手動刪除。如果您沒有、您將繼續收取這些資源的費用。



Cloud Manager在Cloud Volumes ONTAP 雲端供應商部署時、可在執行個體上提供終止保護。此選項有助於防止意外終止。

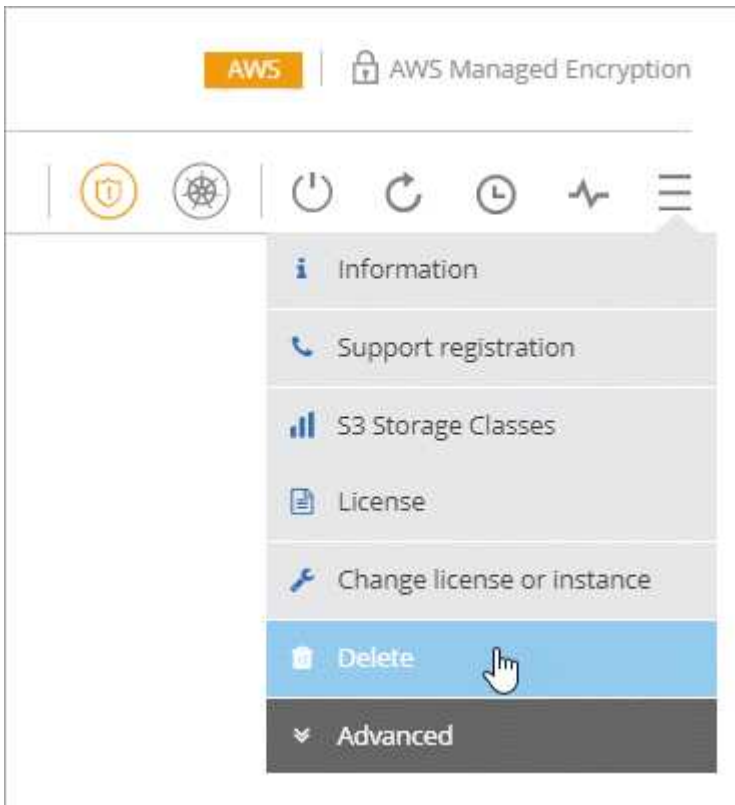
#### 步驟

1. 如果您在工作環境中啟用Cloud Backup、請先判斷是否仍需要備份資料、然後再決定 ["如有必要、請刪除備份"](#) 。

Cloud Backup Cloud Volumes ONTAP 的設計與不受依賴。當您刪除Cloud Volumes ONTAP 一個還原系統時、Cloud Backup不會自動刪除備份、而且UI目前不支援刪除系統後的備份。

2. 如果您在此工作環境中啟用「雲端資料感應」或「監控」功能、而其他工作環境並未使用這些服務、則您必須刪除這些服務的執行個體。
  - ["深入瞭解Cloud Data Sense執行個體"](#) 。
  - ["深入瞭解監控擷取設備"](#) 。
3. 刪除Cloud Volumes ONTAP 這個作業環境。

- a. 在「畫版」頁面上、按兩下Cloud Volumes ONTAP 您要刪除的「紙張工作環境」名稱。
- b. 按一下功能表圖示、然後按一下\*刪除\*。



- c. 輸入工作環境的名稱、然後按一下 \* 刪除 \*。

刪除工作環境最多可能需要 5 分鐘。

## AWS管理

變更**EC2**執行個體類型**Cloud Volumes ONTAP** 以供使用

在Cloud Volumes ONTAP AWS中啟動時、您可以從多個執行個體或類型中進行選擇。如果判斷執行個體的大小過小或過大、您可以隨時變更執行個體類型。

關於這項工作

- 自動恢復必須在 Cloud Volumes ONTAP 一個「無法恢復的 HA 配對」上啟用（這是預設設定）。如果沒有、則作業將會失敗。

["供應說明文件：設定自動恢復的命令 ONTAP"](#)

- 變更執行個體類型可能會影響AWS服務費用。
- 此作業會重新啟動 Cloud Volumes ONTAP 。

對於單一節點系統、I/O 會中斷。

對於 HA 配對、變更不中斷營運。HA 配對可繼續提供資料。



Cloud Manager 會啟動接管作業並等待回饋、一次只能正常變更一個節點。NetApp 的 QA 團隊在這段過程中測試了寫入和讀取檔案的能力、並未發現客戶端有任何問題。隨著連線變更、我們確實看到 I/O 層級的重試次數、但應用程式層卻取代了 NFS/CIFS 連線的這些短「重新連線」。

#### 步驟

1. 在工作環境中、按一下功能表圖示、然後選取\*變更執行個體\*。
2. 如果您使用的是節點型PAYGO授權、您可以選擇不同的授權。
3. 選擇執行個體類型、選取核取方塊以確認您瞭解變更的影響、然後按一下\*確定\*。

以新組態重新開機。Cloud Volumes ONTAP

#### 在多個AZs中變更HA配對的路由表

您可以修改AWS路由表、其中包含部署在多個AWS可用性區域 (AZs) 中之HA配對的浮動IP位址路由。如果新的 NFS 或 CIFS 用戶端需要存取 AWS 中的 HA 配對、您可以這麼做。

#### 步驟

1. 在工作環境中、按一下功能表圖示、然後按一下 \* 資訊 \*。
2. 按一下 \* 路由表 \*。
3. 修改所選路由表的清單、然後按一下「\* 儲存 \*」。

Cloud Manager 會傳送 AWS 要求來修改路由表。

#### 監控 AWS 資源成本

Cloud Manager 可讓您檢視在 Cloud Volumes ONTAP AWS 中執行功能的相關資源成本。您也可以瞭解使用 NetApp 功能來降低儲存成本、省下多少成本。

當您重新整理頁面時、Cloud Manager 會更新成本。如需最終成本詳細資料、請參閱 AWS。

#### 步驟

1. 確認 Cloud Manager 可從 AWS 取得成本資訊：
  - a. 確保提供 Cloud Manager 權限的 IAM 原則包括下列動作：

```
"ce:GetReservationUtilization",  
"ce:GetDimensionValues",  
"ce:GetCostAndUsage",  
"ce:GetTags"
```

這些行動包含在最新的中 "[Cloud Manager 原則](#)"。從 NetApp Cloud Central 部署的新系統會自動包含這些權限。

- b. "[啟動 \\* 工作環境 Id\\* 標籤](#)"。



為了追蹤 AWS 成本、Cloud Manager 會指派成本分配標籤給 Cloud Volumes ONTAP 各個執行個體。建立第一個工作環境之後、請啟動 \* 工作環境 Id\* 標籤。使用者定義的標記不會出現在 AWS 帳單報告上、除非您在帳單和成本管理主控台中啟動它們。

2. 在「畫版」頁面上、選取 Cloud Volumes ONTAP 一個運作環境、然後按一下「\* 成本 \*」。

「成本」頁面會顯示目前和過去幾個月的成本、並顯示您每年的 NetApp 節約效益（如果您已啟用 NetApp 的 Volume 節約功能）。

下圖顯示成本頁範例：



## Azure管理

變更Azure VM類型Cloud Volumes ONTAP 以供使用

在Cloud Volumes ONTAP Microsoft Azure中啟動時、您可以從多種VM類型中進行選擇。您可以隨時變更VM類型、只要判斷其規模過小或過大、就能滿足您的需求。

關於這項工作

- 自動恢復必須在 Cloud Volumes ONTAP 一個「無法恢復的 HA 配對」上啟用（這是預設設定）。如果沒有、則作業將會失敗。

"供應說明文件：設定自動恢復的命令 ONTAP"

- 變更VM類型可能會影響Microsoft Azure服務費用。
- 此作業會重新啟動 Cloud Volumes ONTAP 。

對於單一節點系統、I/O 會中斷。

對於 HA 配對、變更不中斷營運。HA 配對可繼續提供資料。



Cloud Manager 會啟動接管作業並等待回饋、一次只能正常變更一個節點。NetApp 的 QA 團隊在這段過程中測試了寫入和讀取檔案的能力、並未發現客戶端有任何問題。隨著連線變更、我們確實看到 I/O 層級的重試次數、但應用程式層卻取代了 NFS/CIFS 連線的這些短「重新連線」。

#### 步驟

1. 在工作環境中、按一下功能表圖示、然後選取\*變更VM\*。
2. 如果您使用的是節點型PAYGO授權、您可以選擇不同的授權。
3. 選取VM類型、選取核取方塊以確認您瞭解變更的影響、然後按一下\*確定\*。

以新組態重新開機。Cloud Volumes ONTAP

在**Cloud Volumes ONTAP Azure**中覆寫**CIFS**鎖、以利執行不需使用的功能

帳戶管理員可在Cloud Manager中啟用一項設定、以避免Cloud Volumes ONTAP 在Azure 維護活動期間發生有關還原儲存設備的問題。啟用此設定時 Cloud Volumes ONTAP 、不支援 CIFS 會鎖定並重設作用中的 CIFS 工作階段。

Microsoft Azure 會排程在其虛擬機器上定期進行維護活動。當某個維護事件發生在Cloud Volumes ONTAP 一個不支援的HA配對上時、HA配對會啟動儲存設備接管。如果在此維護事件期間有作用中的CIFS工作階段、則CIFS檔案上的鎖定功能可能會妨礙儲存設備恢復。

如果啟用此設定、Cloud Volumes ONTAP 則會取消鎖定並重設作用中的 CIFS 工作階段。因此、HA配對可在這些維護事件期間完成儲存恢復。



此程序可能會對 CIFS 用戶端造成破壞。未從 CIFS 用戶端提交的資料可能會遺失。

您必須先建立連接器、才能變更 Cloud Manager 設定。"瞭解方法"。

#### 步驟

1. 在Cloud Manager主控台右上角、按一下「設定」圖示、然後選取「連接器設定」。



2. 在\* Azure 下、按一下 Azure CIFS Locks for Azure HA工作環境\*。
3. 按一下核取方塊以啟用此功能、然後按一下「儲存」。

使用**Azure**私有連結或服務端點

使用Azure Private Link連線至相關儲存帳戶。Cloud Volumes ONTAP如有需要、您可以停用Azure私有連結、改用服務端點。



## 總覽

根據預設、Cloud Manager會啟用Azure Private Link、以便Cloud Volumes ONTAP 在支援的各個層面及其相關儲存帳戶之間建立連線。Azure Private Link可保護Azure中端點之間的連線安全、並提供效能優勢。

如有需要、您可以設定Cloud Volumes ONTAP 使用服務端點、而非Azure Private Link。

無論是哪一種組態、Cloud Manager都會限制Cloud Volumes ONTAP 存取網路、以利連接到既供連接到儲存帳戶。網路存取僅限於Cloud Volumes ONTAP 部署了下列項目的vnet和部署Connector的vnet。

停用**Azure**私有連結、改用服務端點

如果貴企業需要、您可以在Cloud Manager中變更設定、讓Cloud Volumes ONTAP 其設定使用服務端點、而非Azure Private Link。變更此設定會套用Cloud Volumes ONTAP 至您所建立的新版資訊系統。

## 步驟

1. 在Cloud Manager主控台右上角、按一下「設定」圖示、然後選取「連接器設定」。
2. 在\* Azure 下、按一下\*使用**Azure Private Link**。
3. 取消選擇\* Cloud Volumes ONTAP 在不同時使用\*私有連結的情況下、連接到儲存帳戶\*。
4. 按一下「\* 儲存 \*」。

使用**Azure**私有連結

在大多數情況下、您不需要做任何事、就能使用Cloud Volumes ONTAP 下列功能來設定Azure私有連結：Cloud Manager可為您管理Azure私有連結。但是如果您使用 Azure 私有 DNS 、則需要編輯組態檔。您也應該瞭解Azure中的Connector位置需求。

## 私有連結連線的運作方式

Cloud Manager在Cloud Volumes ONTAP Azure中部署時、會在資源群組中建立私有端點。私有端點與Cloud Volumes ONTAP 用於實現功能不均的儲存帳戶相關聯。因此Cloud Volumes ONTAP 、存取資料可透過Microsoft主幹網路存取。

當用戶端與Cloud Volumes ONTAP S時 位於相同的vnet內、在連接VNets的對等網路內、或在使用私有VPN或ExpressRoute連線至vnet的內部部署網路中、用戶端存取會透過私有連結進行。

以下範例顯示用戶端透過私有連結從同一個Vnet存取、以及從內部網路存取具有私有VPN或ExpressRoute連線的權限。



### 連接器位於Azure中

連接器應部署在Cloud Volumes ONTAP 其所管理的或所管理的各個系統所在的Azure區域 "[Azure區域配對](#)" 適用於整個系統。Cloud Volumes ONTAP這項需求可確保Cloud Volumes ONTAP Azure Private Link連線可用於連接至相關的儲存帳戶。

### 向Cloud Manager提供Azure私有DNS的詳細資料

如果您使用 "[Azure 私有 DNS](#)"然後您需要修改每個 Connector 上的組態檔。否則、Cloud Manager 無法在Cloud Volumes ONTAP 支援 Azure 及其相關儲存帳戶的情況下、啟用 Azure Private Link 連線。

請注意、DNS 名稱必須符合 Azure DNS 命名需求 "[如 Azure 文件所示](#)"。

### 步驟

1. SSH 連接至 Connector 主機並登入。
2. 瀏覽至下列目錄：`/opp/application/netapp/cloudmanager/docker_occm/data`
3. 修改下列參數以編輯app.conf、如下所示：

```
"user-private-dns-zone-settings": {
  "use-existing": true,
  "resource-group": "<resource group name of the DNS zone>",
  "subscription": "<subscription ID>"
}
```

只有當私有DNS區域存在於與Connector不同的訂閱中時、才需要訂購參數。

#### 4. 儲存檔案並登出 Connector 。

不需要重新開機。

#### 在故障時啟用復原功能

如果Cloud Manager無法建立Azure私有連結做為特定行動的一部分、則在不使用Azure私有連結連線的情況下完成此行動。當建立新的工作環境（單一節點或HA配對）、或是HA配對上發生下列動作時、就會發生這種情況：建立新的Aggregate、新增磁碟至現有的Aggregate、或是在超過32 TiB時建立新的儲存帳戶。

如果Cloud Manager無法建立Azure私有連結、您可以啟用復原功能來變更此預設行為。這有助於確保您完全符合貴公司的安全法規。

如果您啟用復原、Cloud Manager會停止動作、並回復作為行動一部分所建立的所有資源。

只有API支援啟用復原功能。

#### 步驟

1. 請使用「PUT /occm/config（放入/occm/config）API呼叫與下列要求內容：

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

## Google Cloud管理

變更Google Cloud機器類型Cloud Volumes ONTAP 以供使用

在Cloud Volumes ONTAP Google Cloud上啟動時、您可以從多種機器類型中進行選擇。如果判斷執行個體的大小過小或過大、您可以隨時變更執行個體或機器類型。

#### 關於這項工作

- 自動恢復必須在 Cloud Volumes ONTAP 一個「無法恢復的 HA 配對」上啟用（這是預設設定）。如果沒有、則作業將會失敗。

["供應說明文件：設定自動恢復的命令 ONTAP"](#)

- 變更機器類型可能會影響Google Cloud服務費用。
- 此作業會重新啟動 Cloud Volumes ONTAP 。

對於單一節點系統、I/O 會中斷。

對於 HA 配對、變更不中斷營運。HA 配對可繼續提供資料。



Cloud Manager 會啟動接管作業並等待回饋、一次只能正常變更一個節點。NetApp 的 QA 團隊在這段過程中測試了寫入和讀取檔案的能力、並未發現客戶端有任何問題。隨著連線變更、我們確實看到 I/O 層級的重試次數、但應用程式層卻取代了 NFS/CIFS 連線的這些短「重新連線」。

## 步驟

1. 在工作環境中、按一下功能表圖示、然後選取\*變更機器\*。
2. 如果您使用的是節點型PAYGO授權、您可以選擇不同的授權。
3. 選取機器類型、選取核取方塊以確認您瞭解變更的影響、然後按一下\*確定\*。

以新組態重新開機。Cloud Volumes ONTAP

## 使用進階檢視來管理Cloud Volumes ONTAP

如果您需要執行Cloud Volumes ONTAP 進階的支援管理功能、可以使用ONTAP 支援ONTAP 此功能的支援功能、這個功能是隨附於一個系統的管理介面。我們直接在Cloud Manager中加入System Manager介面、因此您不需要離開Cloud Manager進行進階管理。

此「進階檢視」可作為預覽使用。我們計畫改善這項體驗、並在即將推出的版本中加入增強功能。請使用產品內建聊天功能、向我們傳送意見反應。

## 功能

Cloud Manager的進階檢視可讓您存取其他管理功能：

- 進階儲存管理

管理一致性群組、共用區、qtree、配額和儲存VM。

- 網路管理

管理IPspace、網路介面、連接埠集和乙太網路連接埠。

- 活動與工作

檢視事件記錄、系統警示、工作和稽核記錄。

- 進階資料保護

保護儲存VM、LUN及一致性群組。

- 主機管理

設定SAN啟動器群組和NFS用戶端。

## 支援的組態

透過System Manager進階管理功能、Cloud Volumes ONTAP 可在標準雲端區域中以支援使用支援的版本為0、10.0及更新版本。

不支援在GovCloud區域或沒有外傳網際網路存取的區域整合System Manager。

## 限制

下列功能不支援出現在System Manager介面中Cloud Volumes ONTAP 的部分功能：

- 雲端分層

不支援Cloud Volumes ONTAP 使用Cloud Tiering服務。建立磁碟區時、必須直接從Cloud Manager的標準檢視設定將資料分層至物件儲存設備。

- 階層

System Manager不支援集合管理（包括本機層級和雲端層）。您必須直接從Cloud Manager的「標準檢視」管理集合體。

- 韌體升級

不支援Cloud Volumes ONTAP 從\*叢集>設定\*頁面自動更新韌體。

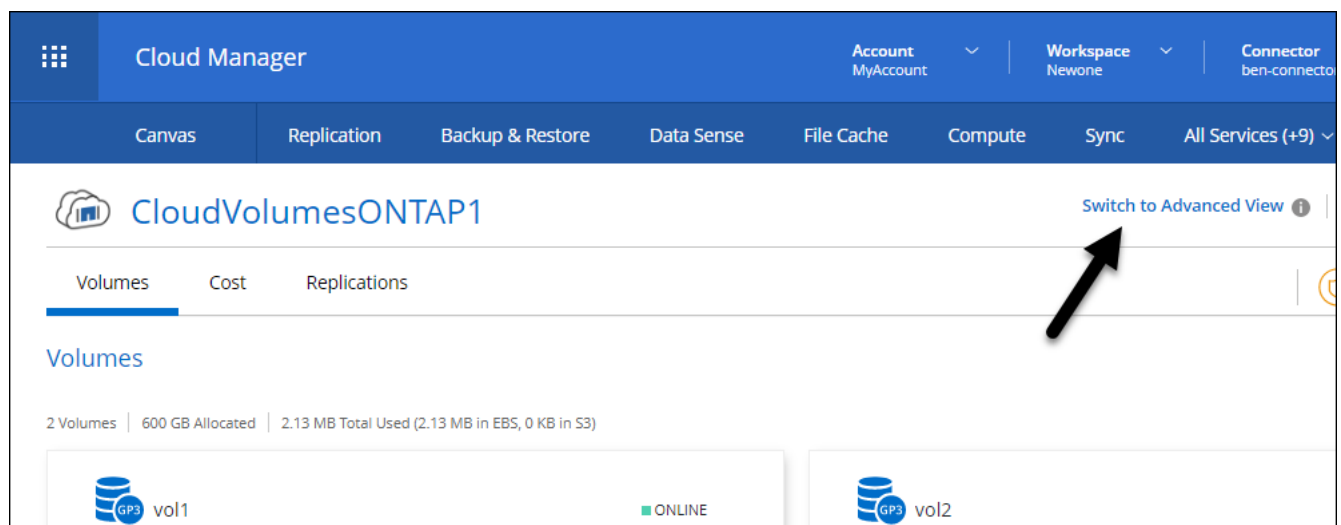
此外、不支援System Manager的角色型存取控制。

## 如何開始使用

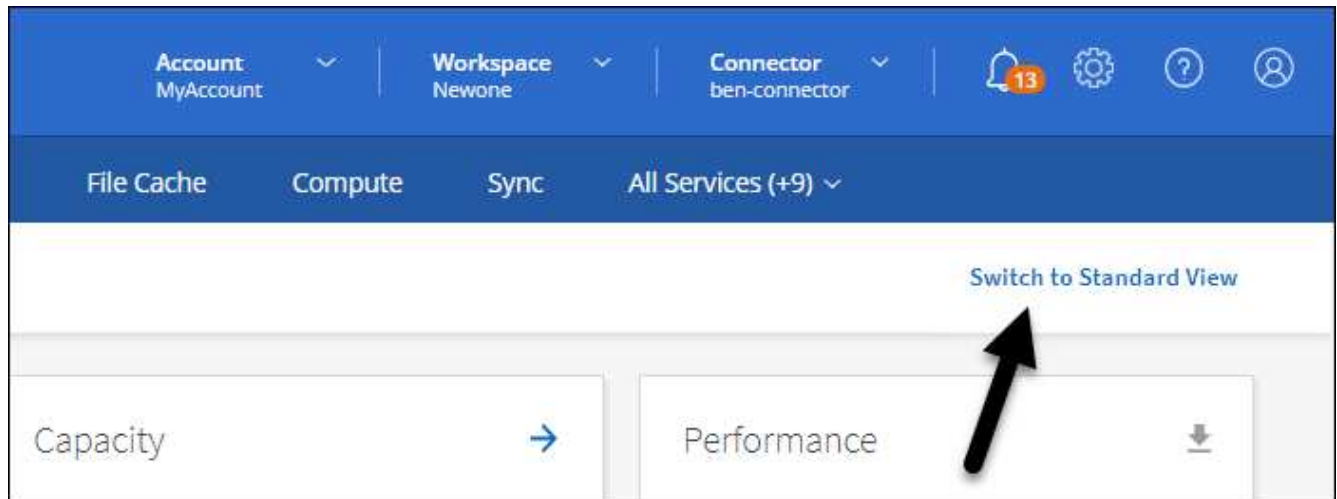
開啟Cloud Volumes ONTAP 一個運作環境、然後按一下「進階檢視」選項。

## 步驟

1. 在「畫版」頁面上、按兩下Cloud Volumes ONTAP 某個系統的名稱。
2. 在右上角、按一下\*切換至進階檢視\*。



3. 如果出現確認訊息、請仔細閱讀、然後按一下\*關閉\*。
4. 使用System Manager來管理Cloud Volumes ONTAP 功能。
5. 如有需要、請按一下\*切換至標準檢視\*、透過Cloud Manager返回標準管理。



### 協助使用System Manager

如果您需要協助、請Cloud Volumes ONTAP 參閱《System Manager with》（搭配使用系統管理程式）["本文檔 ONTAP"](#) 以取得逐步指示。以下是幾個可能有幫助的連結：

- ["Volume與LUN管理"](#)
- ["網路管理"](#)
- ["資料保護"](#)

### 從Cloud Volumes ONTAP CLI管理

利用此功能、您可以執行所有的管理命令、這是進階工作或使用CLI時的最佳選擇。Cloud Volumes ONTAP您可以使用 Secure Shell （SSH）連線至 CLI 。

您使用 SSH 連線 Cloud Volumes ONTAP 到 Suse 的主機必須有連至 Cloud Volumes ONTAP Suse 的網路連線。例如、您可能需要從雲端供應商網路中的跨接主機執行SSH。



當部署於多個 AZs 時 Cloud Volumes ONTAP、使用浮動 IP 位址進行叢集管理介面、這表示外部路由無法使用。您必須從屬於同一個路由網域的主機連線。

#### 步驟

1. 在 Cloud Manager 中、識別叢集管理介面的 IP 位址：
  - a. 在「畫版」頁面上、選取 Cloud Volumes ONTAP 「系統」。
  - b. 複製右窗格中顯示的叢集管理 IP 位址。
2. 使用 SSH 連線至使用管理帳戶的叢集管理介面 IP 位址。
  - 範例 \*

下圖顯示使用 Putty 的範例：



Specify the destination you want to connect to

Host Name (or IP address)  Port

Connection type:

☐ Raw ☐ Iinet ☐ Rlogin ☒ SSH ☐ Serial

3. 在登入提示下、輸入 admin 帳戶的密碼。

◦ 範例 \*

```
Password: *****  
COT2::>
```

## 系統健全狀況與事件

### 驗AutoSupport 證此設定

可主動監控系統健全狀況、並傳送訊息給NetApp技術支援部門。AutoSupport根據預設、AutoSupport 每個節點上都會啟用支援功能、以便使用HTTPS傳輸傳輸協定將訊息傳送給技術支援。最好驗證AutoSupport 此資訊是否能傳送。

如果Cloud Manager帳戶管理員在您啟動執行個體之前、已將Proxy伺服器新增至Cloud Manager、Cloud Volumes ONTAP 則會將此代理伺服器設定為使用AutoSupport 該代理伺服器來接收消息。

唯一必要的組態步驟是確保Cloud Volumes ONTAP 透過NAT執行個體或環境的Proxy服務、實現出站網際網路連線。如需詳細資料、請參閱雲端供應商的網路需求。

- ["AWS網路需求"](#)
- ["Azure網路需求"](#)
- ["Google Cloud網路需求"](#)

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

### 設定EMS

事件管理系統（EMS）會收集ONTAP 並顯示有關發生在故障系統上的事件資訊。若要接收事件通知、您可以針對特定事件嚴重性設定事件目的地（電子郵件地址、SNMP 設陷主機或 syslog 伺服器）和事件路由。

您可以使用 CLI 設定 EMS 。如需相關指示、請參閱 ["文件：EMS組態總覽ONTAP"](#)。

## 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。