使用Cloud Volumes ONTAP

Cloud Volumes ONTAP

NetApp
February 19, 2026

目錄

使用Cloud Volumes ONTAP

許可證管理

管理Cloud Volumes ONTAP基於容量的許可

從NetApp Console管理基於容量的許可證，以確保您的NetApp帳戶具有足夠的容量用於您的Cloud Volumes ONTAP系統。

_基於容量的許可證_使您能夠按 TiB 容量支付Cloud Volumes ONTAP 的費用。

您可以從NetApp Console管理基於容量的Cloud Volumes ONTAP許可證。

> 雖然控制台中管理的產品和服務的實際使用情況和計量始終以 GiB 和 TiB 計算，但 GB/GiB 和 TB/TiB 這兩個術語可互換使用。這反映在雲端市場清單、報價、清單描述和其他支援文件中

"了解有關Cloud Volumes ONTAP許可證的更多信息" 。

如何將許可證新增至NetApp Console

從NetApp銷售代表處購買許可證後， NetApp將向您發送一封電子郵件，其中包含序號和其他許可詳細資訊。

同時，控制台會自動查詢 NetApp 的授權服務，以取得與您的NetApp支援網站帳戶相關的授權的詳細資訊。如果沒有錯誤，它會添加許可證。

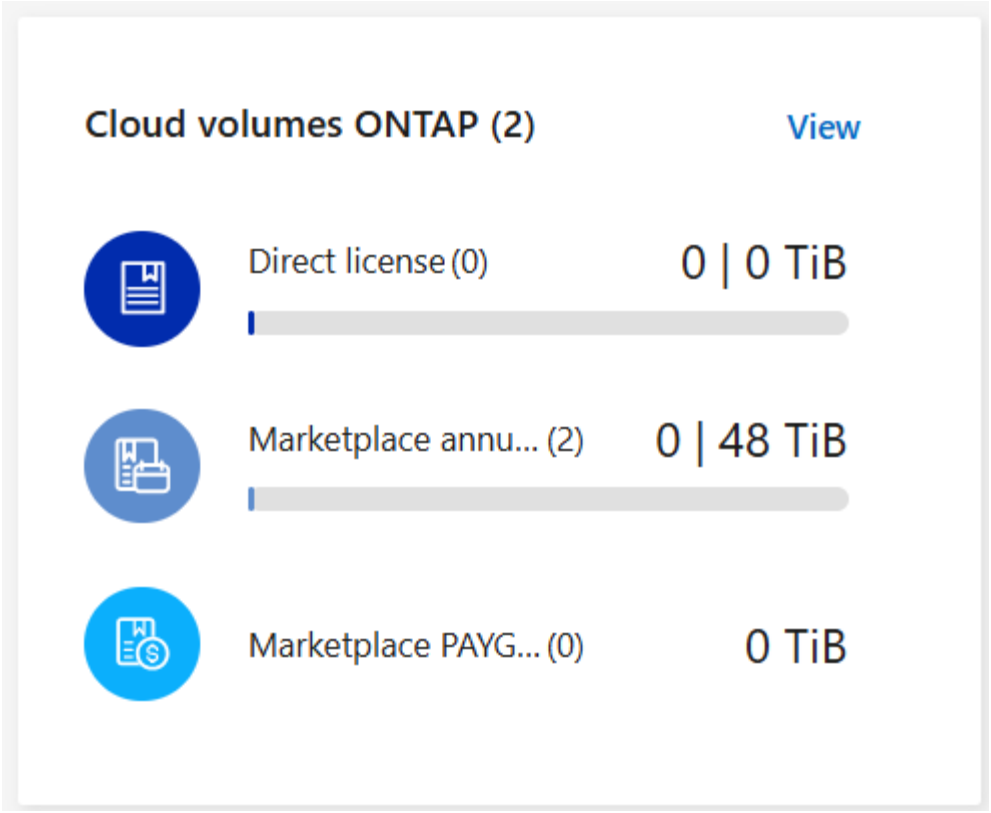
如果控制台無法新增許可證，則需要手動新增它們。例如，如果控制台代理安裝在沒有網路存取的位置，則您需要自行新增許可證。 "了解如何將購買的許可證新增至您的帳戶" 。

查看您帳戶中已消耗的容量

控制台顯示您帳戶中消耗的總容量以及按許可包消耗的容量。這可以幫助您了解收費方式以及是否需要購買額外的容量。

步驟

1. 從左側導覽窗格中，選擇「管理」> 「Licenses and subscriptions」 。
2. 在「概覽」標籤上， Cloud Volumes ONTAP圖塊顯示為您的帳戶配置的目前容量。



- _直接許可證_是您的NetApp帳戶中所有Cloud Volumes ONTAP系統的總配置容量。收費基於每個磁碟區的配置大小，而不考慮磁碟區內的本機、已使用、儲存或有效空間。
- _年度合約_是您從NetApp購買的總授權容量（自帶授權 (BYOL) 或市場合約）。
- *PAYGO* 是使用雲端市場訂閱的總配置容量。只有當消耗的容量高於授權容量或控制台中沒有可用的 BYOL 授權時，才使用 PAYGO 收費。

3. 選擇「檢視」以查看每個許可證包所消耗的容量。
4. 選擇「許可證」標籤查看您購買的每個包許可證的詳細資訊。

   為了更了解 Essentials 套件所顯示的容量，您應該熟悉充電的工作原理。 "了解 Essentials 套餐的收費" 。

5. 選擇「訂閱」標籤來查看按許可證消費模式消耗的容量。此選項卡包括 PAYGO 和年度合約許可證。

   您只會看到與您目前正在查看的組織相關的訂閱。

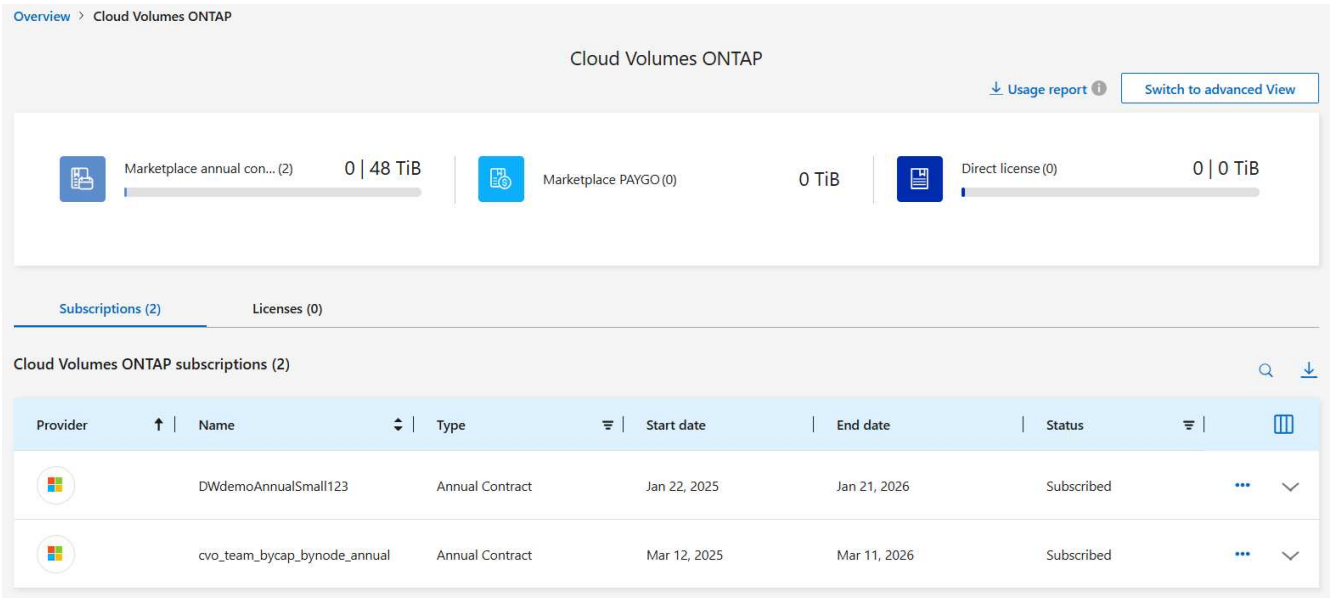
6. 當您查看有關訂閱的資訊時，您可以與表中的詳細資訊進行互動。展開一行可以查看更多詳細資訊。
   - 選擇 選擇表中顯示的列。請注意，「期限」和「自動續訂」欄預設不會出現。自動續約列僅顯示 Azure 合約的續約資訊。

查看包裹詳情

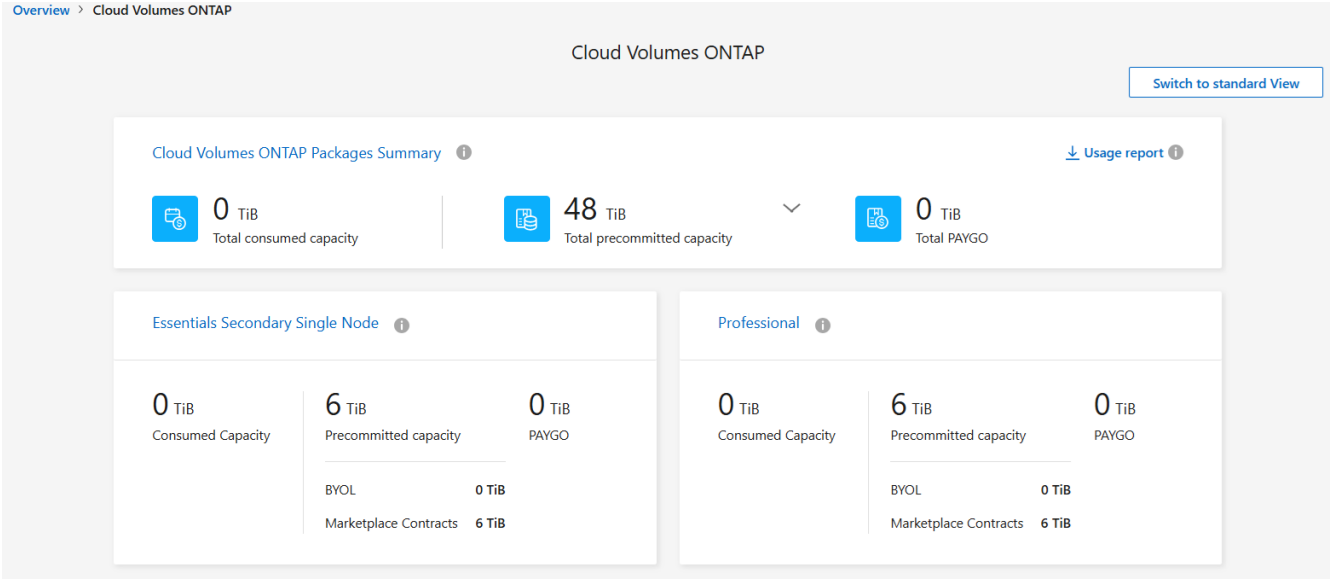
您可以透過在Cloud Volumes ONTAP頁面上切換到傳統模式來查看每個套件使用的容量的詳細資訊。

1. 從左側導覽窗格中，選擇「管理」> 「Licenses and subscriptions」 。
2. 在「概覽」標籤上， Cloud Volumes ONTAP圖塊顯示為您的帳戶配置的目前容量。
3. 選擇「檢視」以查看每個授權包的配置容量。

4. 選擇*切換到進階視圖*。



5. 查看您想要查看的包裹的詳細資訊。



改變充電方式

基於容量的許可以_包_的形式提供。建立Cloud Volumes ONTAP系統時，您可以根據業務需求從多個授權包中進行選擇。如果您在建立系統後需求發生變化，您可以隨時更改套餐。例如，您可以從 Essentials 套件變更為 Professional 套件。

"了解有關基於容量的許可包的更多信息" 。

關於此任務

- 更改收費方式不會影響您是透過從NetApp (BYOL) 購買的授權或透過雲端提供者的市場即用即付 (PAYGO) 訂閱進行收費。

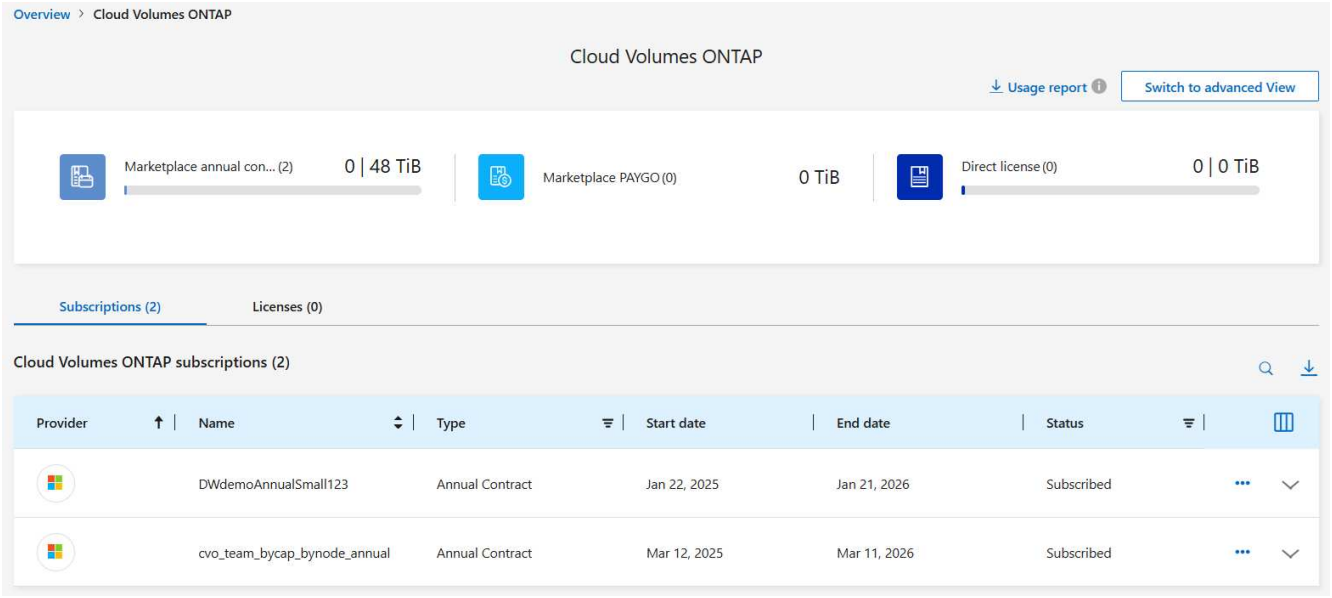
  控制台總是會先嘗試根據許可證收費。如果沒有許可證，則會根據市場訂閱收費。您不必將 BYOL 訂閱轉換

為市場訂閱，反之亦然。

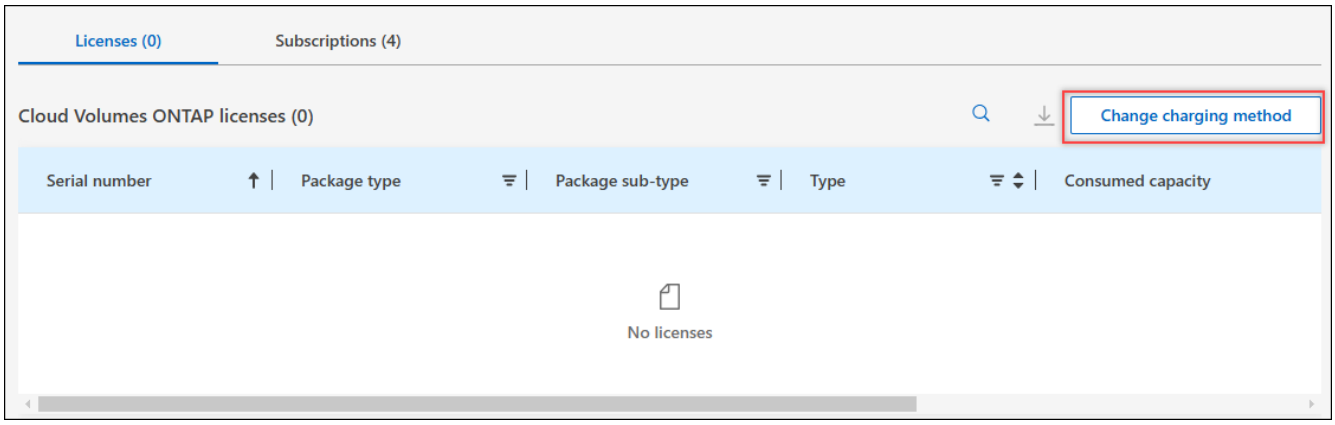
- 如果您擁有來自雲端提供者市場的私人優惠或合同，則更改為合同中未包含的收費方式將導致對 BYOL（如果您從NetApp購買了許可證）或 PAYGO 收費。

步驟

1. 從左側導覽窗格中，選擇「管理」> 「Licenses and subscriptions」 。
2. 選擇“概覽”標籤。
3. 在Cloud Volumes ONTAP圖塊上，選擇 檢視。
4. 選擇*切換到進階視圖*。



5. 向下捲動到*基於容量的許可證*表並選擇*更改收費方式*。



6. 在*變更收費方式*彈出視窗中，選擇Cloud Volumes ONTAP系統，選擇新的收費方式，然後確認您了解變更套餐類型將影響服務費用。
7. 選擇*更改充電方式*。

下載使用情況報告

您可以從控制台下載四份使用量報告。這些使用情況報告提供您的訂閱的容量詳細信息，並告訴您如何為Cloud Volumes ONTAP訂閱中的資源付費。可下載的報告會擷取某個時間點的數據，並且可以輕鬆地與他人分享。

以下報告可供下載。顯示的容量值以 TiB 為單位。

- 進階用法：此報告包含以下資訊：
  - 總消耗容量
  - 預先承諾的總容量
  - 總 BYOL 容量
  - 市場合約總容量
  - PAYGO 總容量
- * Cloud Volumes ONTAP軟體包使用情況*：此報告包含每個軟體包的以下資訊：
  - 總消耗容量
  - 預先承諾的總容量
  - 總 BYOL 容量
  - 市場合約總容量
  - PAYGO 總容量
- 儲存虛擬機器使用情況：此報告顯示收費容量在Cloud Volumes ONTAP系統和儲存虛擬機器 (SVM) 之間的分配。此資訊僅在報告中提供。它包含以下資訊：
  - 系統 ID 和名稱（顯示為 UUID）
  - 雲端
  - NetApp帳號 ID
  - 系統配置
  - SVM 名稱
  - 預配置容量
  - 充電容量匯總
  - 市集計費條款
  - Cloud Volumes ONTAP軟體套件或功能
  - 收費 SaaS 市集訂閱名稱
  - 收費 SaaS 市集訂閱 ID

- 工作負載類型

- 磁碟區使用情況：此報表顯示Cloud Volumes ONTAP系統中如何依磁碟區細分收費容量。控制台中的任何螢幕上均不顯示此資訊。它包括以下資訊：
  - 系統 ID 和名稱（顯示為 UUID）
  - SVN 名稱
  - 卷 ID
  - 卷類型
  - 卷配置容量

    FlexClone磁碟區不包含在此報表中，因為這些類型的磁碟區不會產生費用。

步驟

1. 從左側導覽窗格中，選擇「管理」> 「Licenses and subscriptions」。
2. 在*概覽*標籤上，從Cloud Volumes ONTAP圖塊中選擇*檢視*。
3. 選擇*使用情況報告*。

   使用情況報告下載。

4. 開啟下載的檔案以存取報告。

透過NetApp Console管理Cloud Volumes ONTAP 的Keystone訂閱

透過啟用與Cloud Volumes ONTAP一起使用的訂閱並要求變更訂閱服務等級的承諾容量，在NetApp Console中管理您的Keystone訂閱。請求服務等級的額外容量可為Cloud Volumes ONTAP系統提供更多儲存空間。

NetApp Keystone是一種靈活的隨選付費訂閱服務，可為喜歡 OpEx 而非 CapEx 或租賃的客戶提供混合雲體驗。

"了解有關Keystone的更多信息"

授權您的帳戶

您需要先聯絡NetApp授權您的控制台帳號使用Keystone訂閱，然後才能在控制台中使用和管理Keystone訂閱。

步驟

1. 從NetApp Console選單中，選擇「管理 >Licenses and subscriptions」。
2. 選擇* Keystone訂閱*。
3. 如果您看到「歡迎使用NetApp Keystone」頁面，請向頁面上列出的地址發送電子郵件。

   NetApp代表將透過授權您的帳戶存取訂閱來處理您的要求。

4. 返回“Keystone訂閱”選項卡查看您的訂閱。

連結訂閱

在NetApp授權您的帳戶後，您可以連結Keystone訂閱以用於Cloud Volumes ONTAP。此操作使用戶能夠選擇訂閱作為新Cloud Volumes ONTAP系統的收費方式。

步驟

1. 從NetApp Console選單中，選擇「管理 >Licenses and subscriptions」。
2. 選擇* Keystone訂閱*。
3. 對於您想要連結的訂閱，請點擊 ••• 並選擇*連結*。

結果

訂閱現已連結至您的控制台組織或帳戶，並可在建立Cloud Volumes ONTAP工作環境時進行選擇。

請求更多或更少的承諾容量

如果您想要變更訂閱服務等級的承諾容量，您可以直接從控制台向NetApp傳送請求。請求服務等級的額外容量可為Cloud Volumes ONTAP系統提供更多儲存空間。

步驟

1. 從NetApp Console選單中，選擇「管理 >Licenses and subscriptions」。
2. 選擇* Keystone訂閱*。
3. 對於要調整容量的訂閱，請按一下 ••• 並選擇*查看詳細資訊和編輯*。
4. 輸入一個或多個訂閱所請求的承諾容量。
5. 向下滾動，輸入請求的任何其他詳細信息，然後點擊“提交”。

結果

您的請求將在 NetApp 系統中建立一張票以供處理。

監控使用情況

Digital Advisor儀表板可讓您監控Keystone訂閱使用情況並產生報告。

"了解有關監控訂閱使用情況的更多信息"

取消訂閱鏈接

如果您不再想將Keystone訂閱與控制台一起使用，您可以取消訂閱連結。請注意，您只能取消連結未附加至現有Cloud Volumes ONTAP訂閱的訂閱。

步驟

1. 從NetApp Console選單中，選擇「管理 >Licenses and subscriptions」。
2. 選擇* Keystone*。
3. 對於要取消連結的訂閱，點擊 ••• 並選擇*取消連結*。

結果

該訂閱已與您的控制台組織或帳戶取消鏈接，並且在創建Cloud Volumes ONTAP工作環境時不再可供選擇。

管理Cloud Volumes ONTAP 的基於節點的許可

在NetApp Console中管理基於節點的許可證，以確保每個Cloud Volumes ONTAP系統都具有所需容量的有效許可證。

_基於節點的許可證_是上一代許可證模型（不適用於新客戶）：

- 從NetApp購買自帶授權 (BYOL)
- 從雲端供應商的市場購買按小時付費 (PAYGO) 訂閱

您可以從NetApp Console管理基於節點的Cloud Volumes ONTAP許可證。

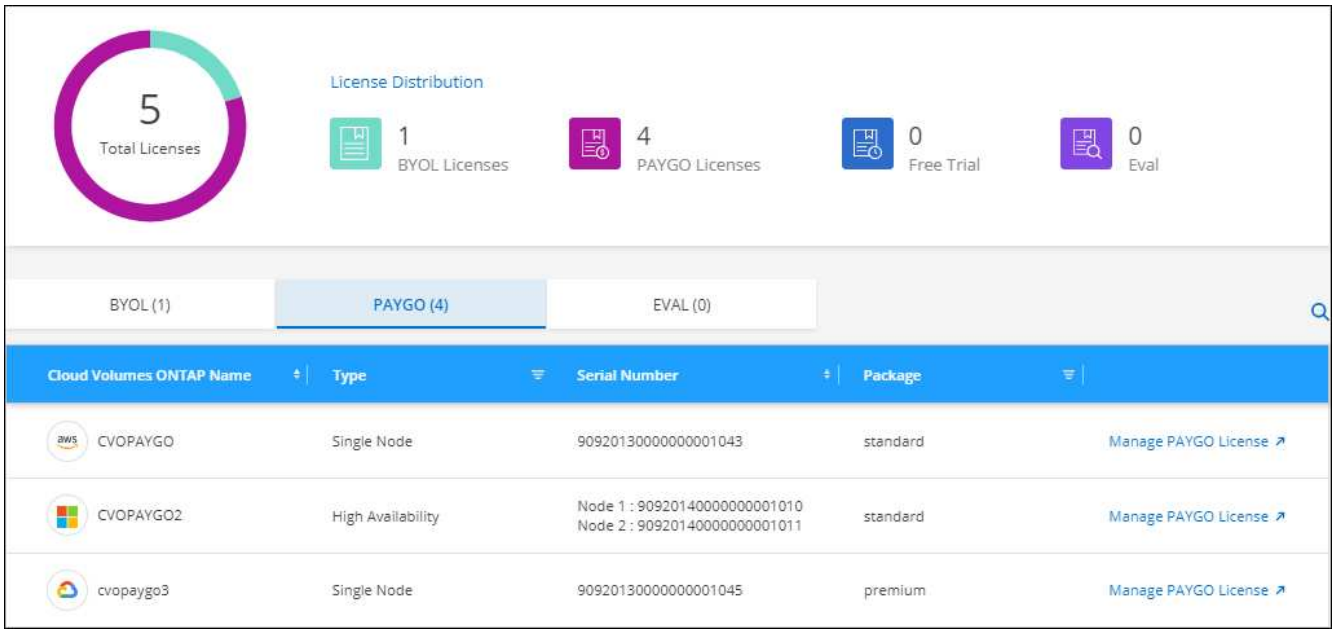
"了解有關Cloud Volumes ONTAP許可證的更多信息" 。

管理 PAYGO 許可證

Licenses and subscriptions選單，您可以查看有關每個 PAYGO Cloud Volumes ONTAP系統的詳細信息，包括序號和 PAYGO 許可證類型。

步驟

1. 從左側導覽窗格中，選擇「管理」> 「Licenses and subscriptions」 。
2. 選擇“概覽”標籤。
3. 在Cloud Volumes ONTAP圖塊上，選擇 檢視。
4. 從下拉式選單中選擇*基於節點的授權*。
5. 點擊*PAYGO*。
6. 在表格中查看有關每個 PAYGO 許可證的詳細資訊。



7. 如果需要，請按一下*管理 PAYGO 授權*來變更 PAYGO 授權或變更執行個體類型。

管理 **BYOL** 許可證

透過新增和刪除系統許可證和額外容量許可證來管理您直接從NetApp購買的許可證。

已限制 BYOL 授權的購買、延期和續約。有關更多信息，請參閱 "Cloud Volumes ONTAP的 BYOL 授權可用性受限" 。

新增未分配的許可證

將基於節點的許可證新增至控制台，以便您在建立新的Cloud Volumes ONTAP系統時可以選擇該許可證。控制台將這些許可證標識為_未分配_。

步驟

1. 從左側導覽窗格中，選擇「管理」> 「Licenses and subscriptions」 。
2. 選擇“概覽”標籤。
3. 在Cloud Volumes ONTAP圖塊上，選擇 檢視。
4. 從下拉式選單中選擇*基於節點的授權*。
5. 按一下“未分配”。
6. 按一下「新增未指派的許可證」 。
7. 輸入許可證的序號或上傳許可證文件。

   如果您還沒有許可證文件，請參閱下面的部分。

8. 按一下「新增許可證」 。

結果

控制台新增許可證。在您將許可證與新的Cloud Volumes ONTAP系統關聯之前，該許可證將被標識為未指派。此後，許可證將移至「Licenses and subscriptions」中的「BYOL」標籤。

交換未分配的基於節點的許可證

如果您有未指派的基於節點的Cloud Volumes ONTAP許可證且尚未使用，則可以將其轉換為NetApp Backup and Recovery許可證、 NetApp Data Classification許可證或NetApp Cloud Tiering許可證來交換該許可證。

交換許可證將撤銷Cloud Volumes ONTAP許可證並為該服務建立等值美元的許可證：

- Cloud Volumes ONTAP HA 對的授權轉換為 51 TiB 直接許可證
- Cloud Volumes ONTAP單節點授權轉換為 32 TiB 直接許可證

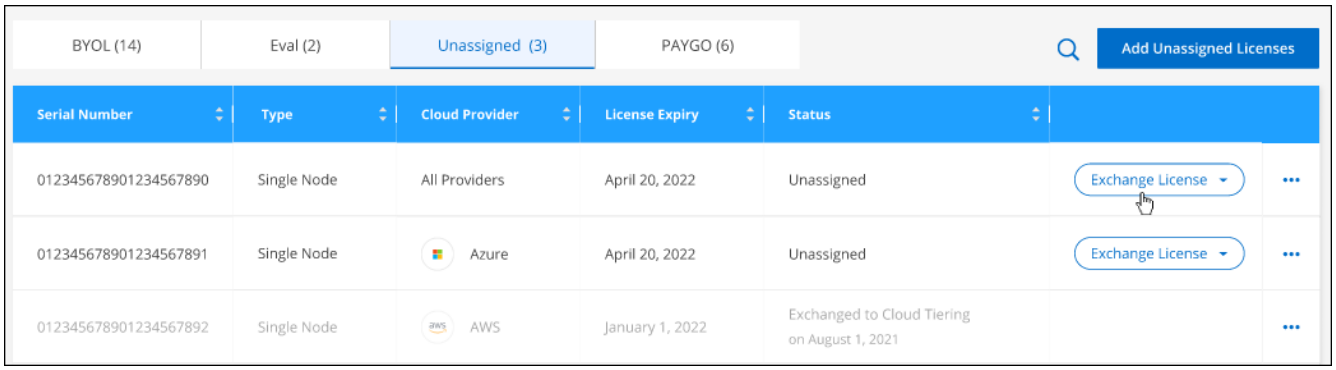
轉換後的許可證的到期日與Cloud Volumes ONTAP許可證相同。

"查看如何交換基於節點的許可證的演練。"

步驟

1. 從左側導覽窗格中，選擇「管理」> 「Licenses and subscriptions」 。
2. 選擇“概覽”標籤。

3. 在Cloud Volumes ONTAP圖塊上，選擇 檢視。
4. 從下拉式選單中選擇*基於節點的授權*。
5. 按一下“未分配”。
6. 按一下「交換許可證」。



7. 選擇您想要交換許可證的服務。
8. 如果出現提示，請為 HA 對選擇一個額外的許可證。
9. 閱讀法律同意並點擊*同意*。

結果

控制台將未指派的許可證轉換為您選擇的服務。您可以在「資料服務許可證」標籤中查看新的許可證。

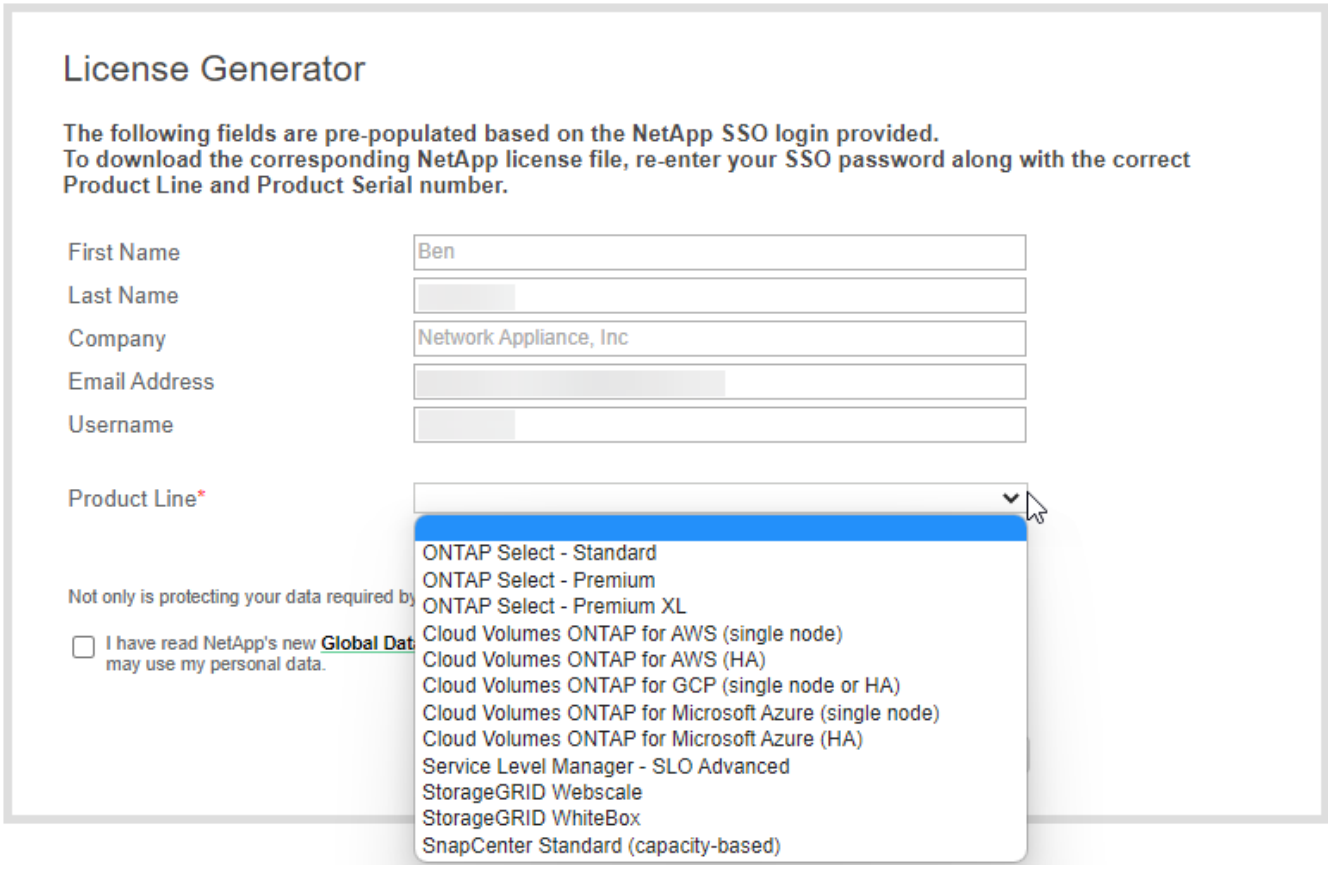
取得系統許可證文件

在大多數情況下，控制台可以使用您的NetApp支援網站帳戶自動取得您的授權文件。但如果不能，那麼您將需要手動上傳許可證文件。如果您沒有許可證文件，您可以從 netapp.com 取得。

步驟

1. 前往 "NetApp許可證文件產生器"並使用您的NetApp支援網站憑證登入。
2. 輸入您的密碼，選擇您的產品，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*。

   例子



3. 選擇您是否希望透過電子郵件或直接下載接收 serialnumber.NLF JSON 檔案。

更新系統許可證

當您透過聯絡NetApp代表續訂 BYOL 訂閱時，控制台會自動從NetApp取得新授權並將其安裝在Cloud Volumes ONTAP系統上。如果控制台無法透過安全的網路連線存取許可證文件，您可以自行取得該文件，然後手動上傳該文件。

步驟

1. 從左側導覽窗格中，選擇「管理」> 「Licenses and subscriptions」。
2. 選擇“概覽”標籤。
3. 在Cloud Volumes ONTAP圖塊上，選擇 檢視。
4. 從下拉式選單中選擇*基於節點的授權*。
5. 在 **BYOL** 標籤中，展開Cloud Volumes ONTAP系統的詳細資訊。
6. 點擊系統許可證旁邊的操作選單，然後選擇*更新許可證*。
7. 上傳許可證文件（如果您有 HA 對，則上傳多個文件）。
8. 按一下「更新許可證」。

結果

控制台更新Cloud Volumes ONTAP系統上的許可證。

您可以為Cloud Volumes ONTAP BYOL 系統購買額外的容量許可證，以分配超過 BYOL 系統許可證提供的 368 TiB 的容量。例如，您可以購買一個額外的許可證容量，為Cloud Volumes ONTAP分配最多 736 TiB 的容量。或者您可以購買三個額外的容量許可證以獲得高達 1.4 PiB。

您可以為單節點系統或 HA 配對購買的授權數量沒有限制。

新增容量許可證

透過控制台右下角的聊天圖示聯絡我們，購買額外容量許可證。購買許可證後，您可以將其套用至Cloud Volumes ONTAP系統。

步驟

1. 從左側導覽窗格中，選擇「管理」> 「Licenses and subscriptions」。
2. 選擇“概覽”標籤。
3. 在Cloud Volumes ONTAP圖塊上，選擇 檢視。
4. 從下拉式選單中選擇*基於節點的授權*。
5. 在 **BYOL** 標籤中，展開Cloud Volumes ONTAP系統的詳細資訊。
6. 按一下「新增容量許可證」。
7. 輸入序號或上傳許可證文件（如果您有 HA 對，則上傳文件）。
8. 按一下「新增容量許可證」。

更新容量許可證

如果您延長了額外容量許可證的期限，則需要在控制台中更新許可證。

步驟

1. 從左側導覽窗格中，選擇「管理」> 「Licenses and subscriptions」。
2. 選擇“概覽”標籤。
3. 在Cloud Volumes ONTAP圖塊上，選擇 檢視。
4. 從下拉式選單中選擇*基於節點的授權*。
5. 在 **BYOL** 標籤中，展開Cloud Volumes ONTAP系統的詳細資訊。
6. 按一下容量許可證旁的操作選單，然後選擇*更新許可證*。
7. 上傳許可證文件（如果您有 HA 對，則上傳多個文件）。
8. 按一下「更新許可證」。

刪除容量許可證

如果額外容量許可證已過期且不再使用，那麼您可以隨時將其刪除。

步驟

1. 從左側導覽窗格中，選擇「管理」> 「Licenses and subscriptions」。

2. 選擇“概覽”標籤。
3. 在Cloud Volumes ONTAP圖塊上，選擇 檢視。
4. 從下拉式選單中選擇*基於節點的授權*。
5. 在 **BYOL** 標籤中，展開Cloud Volumes ONTAP系統的詳細資訊。
6. 點擊容量許可證旁邊的操作選單，然後選擇*刪除許可證*。
7. 按一下“刪除”。

PAYGO 與 **BYOL** 之間的變化

不支援將系統從 PAYGO 按節點授權轉換為 BYOL 按節點授權（反之亦然）。如果您想在按使用量付費訂閱和 BYOL 訂閱之間切換，那麼您需要部署一個新系統並將資料從現有系統複製到新系統。

步驟

1. 建立一個新的Cloud Volumes ONTAP系統。
2. 對於需要複製的每個卷，在系統之間設定一次性資料複製。

   "了解如何在系統之間複製數據"

3. 透過刪除原始系統來終止不再需要的Cloud Volumes ONTAP系統。

   "了解如何刪除Cloud Volumes ONTAP系統" 。

相關連結

關聯："基於節點的許可證的可用性終止" "將基於節點的許可證轉換為基於容量的許可證"

捲和 LUN 管理

在Cloud Volumes ONTAP系統上建立FlexVol volume

如果在啟動初始Cloud Volumes ONTAP系統後需要更多存儲，您可以從NetApp Console為 NFS、CIFS 或 iSCSI 建立新的FlexVol磁碟區。

您可以透過多種方式建立新磁碟區：

- 指定新磁碟區的詳細信息，並讓控制台為您處理底層資料聚合。了解更多
- 在您選擇的資料聚合上建立磁碟區。了解更多
- 在 HA 配置中的第二個節點上建立磁碟區。了解更多

開始之前

關於卷配置的一些注意事項：

- 當您建立 iSCSI 磁碟區時，控制台會自動為您建立 LUN。我們透過為每個磁碟區建立一個 LUN 來簡化操作，因此無需進行任何管理。建立磁碟區後，"使用 IQN 從主機連線到 LUN" 。
- 您可以從ONTAP系統管理員或ONTAP 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。有關詳細信息，請參閱"Cloud Volumes ONTAP for AWS 的網路需求"。
- 如果您的Cloud Volumes ONTAP配置支援 Amazon EBS 彈性磁碟區功能，您可能需要"詳細了解建立磁碟區時發生的情況"。

創建卷

建立磁碟區最常見的方法是指定所需的磁碟區類型，然後讓控制台為您處理磁碟指派。但您也可以選擇要在其上建立磁碟區的特定聚合。

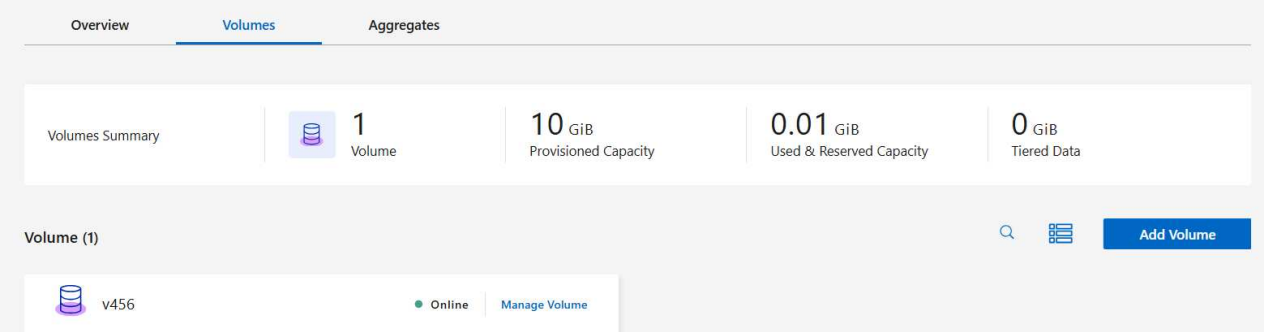
步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在 **Systems** 頁面上，雙擊要在其上設定FlexVol volume的Cloud Volumes ONTAP系統的名稱。

   您可以透過讓控制台為您處理磁碟分配來建立捲，或為磁碟區選擇特定的聚合。只有當您對Cloud Volumes ONTAP系統上的資料聚合有充分了解時，才建議選擇特定的聚合。

任何聚合

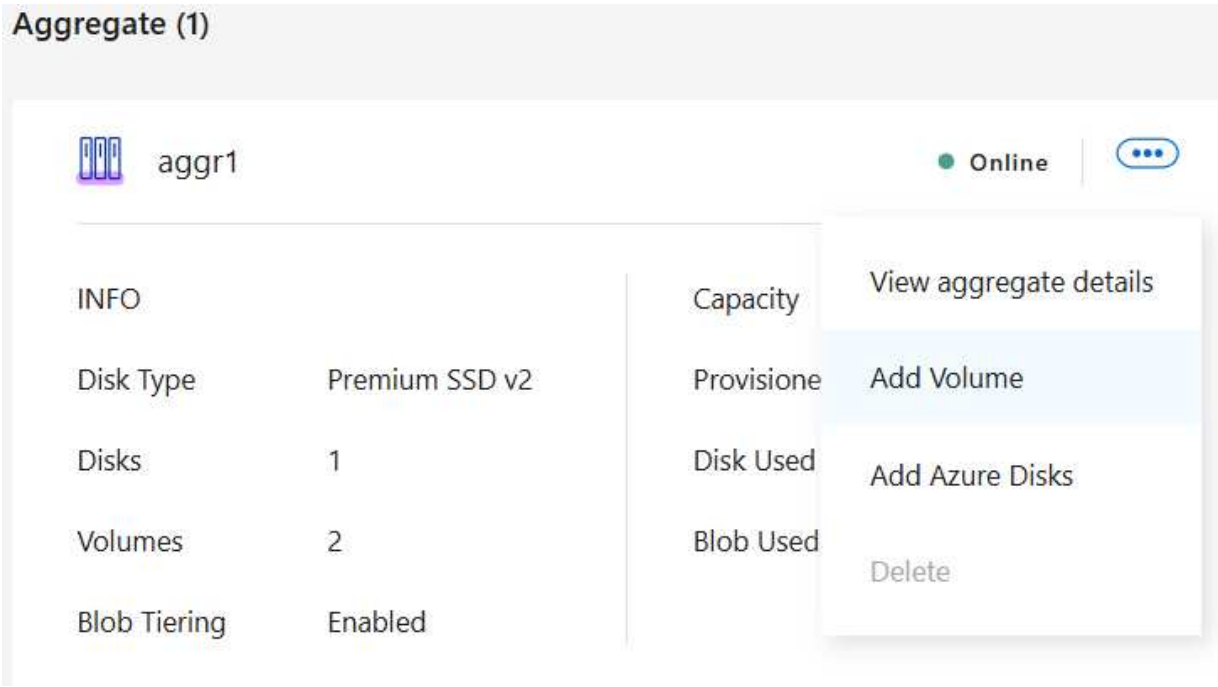
選擇“卷”選項卡，然後按一下“新增卷”



特定骨材

a. 在*聚合*選項卡上，轉到所需的聚合並點擊 ••• 圖示.

b. 選擇*新增卷*



3. 請依照精靈中的步驟建立磁碟區。

a. 詳細資訊、保護和標籤：輸入有關磁碟區的基本詳細資訊並選擇快照策略。

此頁面上的某些欄位是不言自明的。以下列表描述了您可能需要指導的欄位：

場地	描述
卷名	您可以為新磁碟區輸入的可識別名稱。
卷大小	您可以輸入的最大大小很大程度上取決於您是否啟用精簡配置，這使您能夠建立比目前可用的實體儲存更大的磁碟區。

場地	描述
儲存虛擬機器 (SVM)	儲存虛擬機是在ONTAP內運作的虛擬機，可為您的用戶端提供儲存和資料服務。您可能知道這是 SVM 或 vserver。 Cloud Volumes ONTAP預設配置一個儲存虛擬機，但某些配置支援額外的儲存虛擬機。您可以為新磁碟區指定儲存虛擬機器。
快照策略	Snapshot 副本策略指定自動建立的NetApp Snapshot 副本的頻率和數量。NetApp Snapshot 副本是時間點檔案系統映像，它不會影響效能並且只需要最少的儲存空間。您可以選擇預設策略或無策略。對於瞬態數據，您可能會選擇無：例如，對於 Microsoft SQL Server，請選擇 tempdb。

b. 協定：為磁碟區選擇一個協定（NFS、CIFS 或 iSCSI），然後提供所需的資訊。

   如果您選擇 CIFS 但尚未設定伺服器，則按一下「下一步」後控制台會提示您設定 CIFS 連線。

   "了解支援的客戶端協定和版本" 。

   以下部分描述了您可能需要指導的欄位。這些描述是按照協議組織的。

NFS

存取控制

選擇自訂匯出策略以使磁碟區可供客戶端使用。

出口政策

定義子網路中可以存取磁碟區的客戶端。預設情況下，控制台輸入一個提供對子網路中所有實例的存取權限的值。

CIFS

權限和使用者/群組

使您能夠控制使用者和群組對 SMB 共用的存取等級（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。如果指定網域 Windows 使用者名，則必須使用網域\使用者名稱格式包含使用者的網域。

DNS 主 **IP** 位址和輔助 **IP** 位址

為 CIFS 伺服器提供名稱解析的 DNS 伺服器的 IP 位址。所列的 DNS 伺服器必須包含定位 CIFS 伺服器將加入的網域的 Active Directory LDAP 伺服器和網域控制站所需的服務位置記錄 (SRV)。

如果您正在設定 Google 管理的 Active Directory，則預設可以使用 169.254.169.254 IP 位址存取 AD。

要加入的 **Active Directory** 網域

您希望 CIFS 伺服器加入的 Active Directory (AD) 網域的 FQDN。

授權加入網域的憑證

具有足夠權限將電腦新增至 AD 網域內指定組織單位 (OU) 的 Windows 帳戶的名稱和密碼。

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 網域內與 CIFS 伺服器關聯的組織單位。預設值為 CN=Computers。

- 若要將 AWS Managed Microsoft AD 設定為Cloud Volumes ONTAP 的AD 伺服器，請在此欄位中輸入 **OU=Computers,OU=corp**。
- 若要將 Azure AD 網域服務設定為Cloud Volumes ONTAP 的AD 伺服器，請在此欄位中輸入 **OU=AADDC Computers** 或 **OU=AADDC Users**。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure 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 Managed Microsoft AD 設定為Cloud Volumes ONTAP的 AD 伺服器，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 Managed Microsoft AD 中的組織單位"^]

DNS 網域

Cloud Volumes ONTAP儲存虛擬機器 (SVM) 的 DNS 網域。大多數情況下，該域與 AD 域相同。

NTP 伺服器

選擇「使用 Active Directory 網域」以使用 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，那麼您應該使用 API。欲了解更多信息，請參閱 "NetApp Console自動化文檔"。

請注意，只有在建立 CIFS 伺服器時才能設定 NTP 伺服器。建立 CIFS 伺服器後，它不可配置。

iSCSI

邏輯單元號

iSCSI 儲存目標稱為 LUN（邏輯單元），並以標準區塊裝置呈現給主機。當您建立 iSCSI 磁碟區時，控制台會自動為您建立 LUN。我們透過為每個磁碟區建立一個 LUN 來簡化操作，因此無需進行任何管理。建立磁碟區後，"使用 IQN 從主機連線到 LUN" 。

發起者群組

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 目標透過標準乙太網路網路適配器 (NIC)、具有軟體啟動器的 TCP 卸載引擎 (TOE) 卡、融合網路適配器 (CNA) 或專用主機匯流排適配器 (HBA) 連接到網絡，並透過 iSCSI 限定名稱 (IQN) 進行識別。

a. 磁碟類型：根據您的效能需求和成本要求為磁碟區選擇底層磁碟類型。

   - "在 AWS 中調整系統規模"
     - "在 Azure 中調整系統大小"
     - "在 Google Cloud 中調整系統規模"

4. 使用設定檔和分層策略：選擇是否啟用或停用磁碟區上的儲存效率功能，然後選擇"卷分層策略"。

   ONTAP包含多種儲存效率功能，可減少您所需的總儲存量。 NetApp儲存效率功能有以下優勢：

   精簡配置

   向主機或使用者提供比實體儲存池中實際擁有的更多的邏輯儲存。不是預先分配儲存空間，而是在寫入資料時動態地將儲存空間分配給每個磁碟區。

   重複資料刪除

   透過定位相同的資料塊並將其替換為對單一共享區塊的引用來提高效率。該技術透過消除駐留在同一磁碟區中的冗餘資料區塊來減少儲存容量需求。

   壓縮

   透過壓縮主儲存、輔助儲存和歸檔儲存磁碟區內的資料來減少儲存資料所需的實體容量。

5. 審核：審核有關卷的詳細信息，然後按一下*新增*。

結果

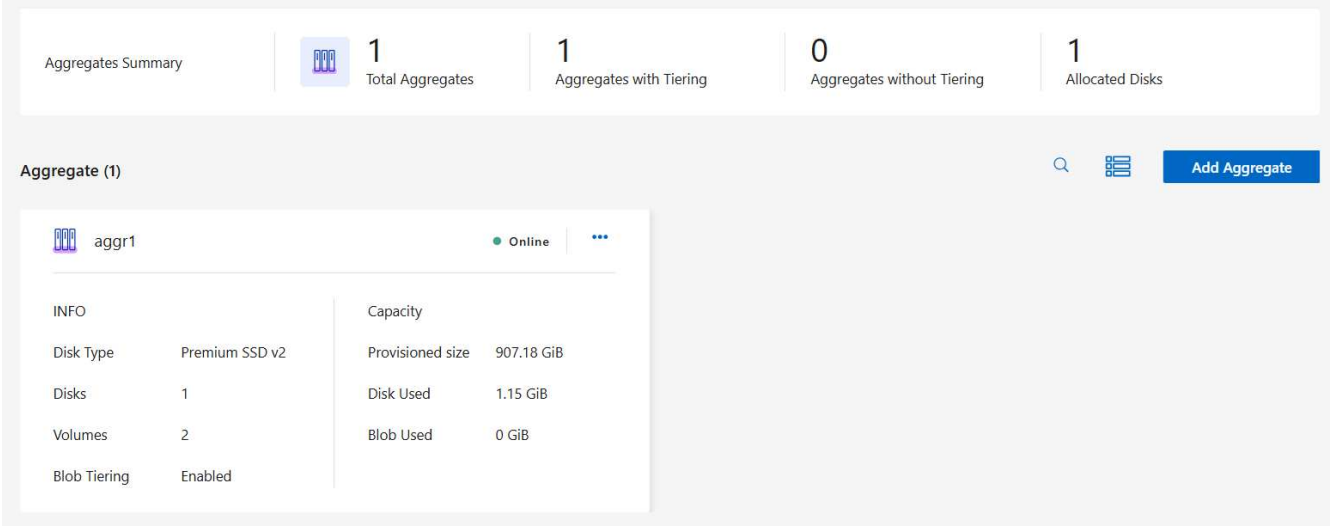
控制台在Cloud Volumes ONTAP系統上建立磁碟區。

在 HA 配置中的第二個節點上建立卷

預設情況下，控制台在 HA 配置中的第一個節點上建立磁碟區。如果您需要主動-主動配置，其中兩個節點都向客戶端提供數據，則必須在第二個節點上建立聚合和磁碟區。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在「系統」頁面上，雙擊要管理聚合的Cloud Volumes ONTAP系統的名稱。
3. 在“聚合”標籤上，按一下“新增聚合”，然後建立聚合。



4. 對於主節點，選擇 HA 對中的第二個節點。
5. 控制台建立聚合後，選擇它，然後按一下*建立磁碟區*。
6. 輸入新卷的詳細信息，然後按一下“建立”。

結果

控制台在 HA 對中的第二個節點上建立磁碟區。

對於在多個 AWS 可用區中部署的 HA 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。

建立磁碟區後

如果您配置了 CIFS 共享，請授予使用者或群組對檔案和資料夾的權限，並驗證這些使用者是否可以存取共用並建立檔案。

如果要將配額應用於卷，則必須使用ONTAP系統管理員或ONTAP CLI。配額可讓您限製或追蹤使用者、群組或 qtree 使用的磁碟空間和檔案數量。

管理Cloud Volumes ONTAP系統上的捲

您可以在NetApp Console中管理磁碟區和 CIFS 伺服器。您也可以移動磁碟區以避免容量問題。

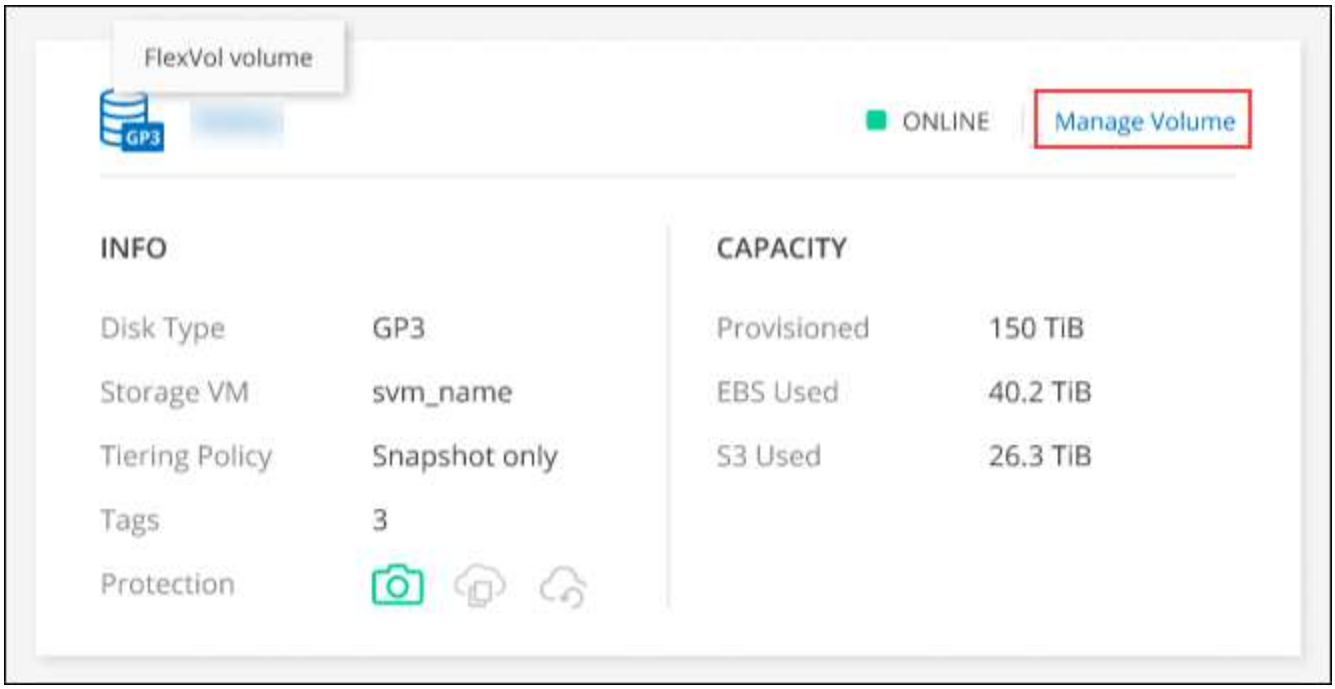
您可以在NetApp Console標準視圖中管理卷，也可以透過控制台中包含的ONTAP系統管理器來管理卷，以進行高級捲管理。標準視圖提供了一組有限的選項來修改您的捲。系統管理器提供高階管理，例如複製、調整大小、更改反勒索軟體、分析、保護和活動追蹤的設定以及跨層移動磁碟區。有關信息，請參閱"使用系統管理員管理Cloud Volumes ONTAP"。

管理磁碟區

透過使用控制台的標準視圖，您可以根據儲存需求管理磁碟區。您可以檢視、編輯、複製、還原和刪除磁碟區。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在*系統*頁面上，雙擊要管理磁碟區的Cloud Volumes ONTAP系統。
3. 選擇“卷”選項卡。



4. 在所需的捲圖塊上，按一下*管理磁碟區*。

任務	行動
查看有關卷的信息	在「管理磁碟區」面板的「磁碟區操作」下，按一下「檢視磁碟區詳細資料」。
取得NFS掛載命令	a. 在「管理磁碟區」面板的「磁碟區操作」下，按一下「安裝指令」。 b. 按一下“複製”。

任務	行動
複製卷	a. 在「管理磁碟區」面板的「磁碟區操作」下，按一下「複製磁碟區」。 b. 根據需要修改克隆名稱，然後按一下“克隆”。 此過程會建立一個FlexClone磁碟區。 FlexClone磁碟區是可寫入的、時間點副本，它節省空間，因為它只使用少量空間來儲存元數據，並且僅在更改或新增資料時才消耗額外的空間。 要了解有關FlexClone卷的更多信息，請參閱 "ONTAP 9 邏輯儲存管理指南"。
編輯卷（限讀寫卷）	a. 在“管理磁碟區”面板的“磁碟區操作”下，按一下“編輯磁碟區設定” b. 修改磁碟區的快照策略、NFS 協定版本、NFS 存取控制清單（匯出策略）或共用權限，然後按一下*套用*。 如果您需要自訂 Snapshot 策略，則可以使用ONTAP System Manager 建立它們。
刪除卷	a. 在「管理磁碟區」面板的「磁碟區操作」下，按一下「刪除磁碟區」。 b. 在「刪除磁碟區」視窗下，輸入要刪除的磁碟區的名稱。 c. 再次點選“刪除”進行確認。
按需建立 Snapshot 副本	a. 在「管理磁碟區」面板的「保護操作」下，按一下「建立 Snapshot 副本」。 b. 如果需要，請變更名稱，然後按一下“建立”。
將資料從 Snapshot 副本還原到新卷	a. 在「管理磁碟區」面板的「保護操作」下，按一下「從 Snapshot 副本還原」。 b. 選擇一個 Snapshot 副本，輸入新磁碟區的名稱，然後按一下「復原」。
更改底層磁碟類型	a. 在「管理磁碟區」面板的「進階操作」下，按一下「變更磁碟類型」。 b. 選擇磁碟類型，然後按一下“變更”。 控制台將磁碟區移至使用所選磁碟類型的現有聚合，或為該磁碟區建立新的聚合。

任務	行動
更改分層策略	a. 在「管理磁碟區」面板的「進階操作」下，按一下「變更分層策略」。 b. 選擇不同的策略並點擊*更改*。 控制台將磁碟區移至使用具有分層功能的所選磁碟類型的現有聚合，或為該磁碟區建立新的聚合。
刪除卷	a. 選擇一個卷，然後按一下“刪除”。 b. 在對話方塊中輸入磁碟區的名稱。 c. 再次點選“刪除”進行確認。

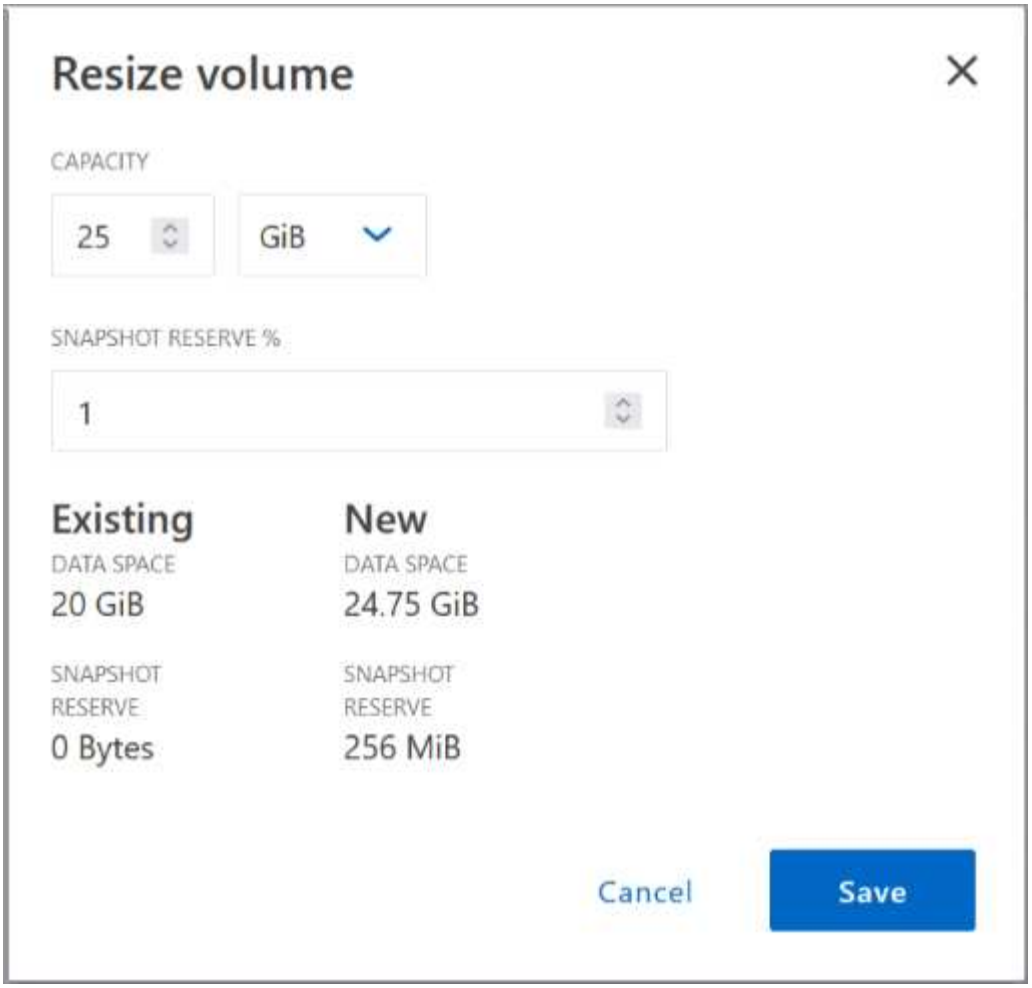
調整磁碟區大小

預設情況下，當磁碟區空間不足時，它會自動增長到最大大小。預設值為 1,000，這表示磁碟區可以增長到其大小的 11 倍。該值可以在控制台代理的設定中配置。

如果您需要調整磁碟區大小，您可以從控制台中的ONTAP系統管理員進行操作。

步驟

1. 按一下系統管理員視圖以透過ONTAP系統管理員調整磁碟區大小。請參閱"如何開始" 。
2. 從左側導覽選單中，選擇“儲存”>“磁碟區”。
3. 從磁碟區清單中，確定應調整大小的磁碟區。
4. 點選選項圖標 。
5. 選擇*調整大小*。
6. 在*調整磁碟區大小*畫面上，根據需要編輯容量和快照預留百分比。您可以將現有的可用空間與修改後的容量進行比較。
7. 點選“儲存”。



調整磁碟區大小時，請務必考慮系統的容量限制。前往 "Cloud Volumes ONTAP發行說明"了解更多。

修改 **CIFS** 伺服器

如果您變更 DNS 伺服器或 Active Directory 網域，則需要修改Cloud Volumes ONTAP中的 CIFS 伺服器，以便它可以繼續為用戶端提供儲存服務。

步驟

1. 從Cloud Volumes ONTAP系統的 **Overview** 標籤中，按一下右側面板下的 **Feature** 標籤。
2. 在 CIFS 設定欄位下，按一下 鉛筆圖示 以顯示 CIFS 設定視窗。
3. 指定 CIFS 伺服器的設定：

任務	行動
選擇儲存虛擬機器 (SVM)	選擇 Cloud Volume ONTAP儲存虛擬機器 (SVM) 顯示其配置的 CIFS 資訊。
要加入的 Active Directory 網域	您希望 CIFS 伺服器加入的 Active Directory (AD) 網域的 FQDN。
授權加入網域的憑證	具有足夠權限將電腦新增至 AD 網域內指定組織單位 (OU) 的 Windows 帳戶的名稱和密碼。

任務	行動
DNS 主 IP 位址和輔助 IP 位址	為 CIFS 伺服器提供名稱解析的 DNS 伺服器的 IP 位址。所列的 DNS 伺服器必須包含定位 Active Directory LDAP 伺服器和 CIFS 伺服器將加入的網域的網域控制站所需的服務位置記錄 (SRV)。 ifdef::gcp[] 如果您正在設定 Google Managed Active Directory，則預設可以使用 169.254.169.254 IP 位址存取 AD。 endif::gcp[]
DNS 網域	Cloud Volumes ONTAP儲存虛擬機器 (SVM) 的 DNS 網域。大多數情況下，該域與 AD 域相同。
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 網域內與 CIFS 伺服器關聯的組織單位。預設值為 CN=Computers。 • 若要將 AWS Managed Microsoft AD 設定為Cloud Volumes ONTAP 的AD 伺服器，請在此欄位中輸入 **OU=Computers,OU=corp**。 • 若要將 Azure AD 網域服務設定為Cloud Volumes ONTAP 的AD 伺服器，請在此欄位中輸入 **OU=AADDC Computers** 或 **OU=AADDC Users**。"Azure 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 Managed Microsoft AD 設定為Cloud Volumes ONTAP 的 AD 伺服器，請在此欄位中輸入 **OU=Computers,OU=Cloud** 。"Google Cloud 文件：Google Managed Microsoft AD 中的組織單位"

4. 點選“設定”。

結果

Cloud Volumes ONTAP使用變更來更新 CIFS 伺服器。

移動磁碟區

移動磁碟區以提高容量利用率、提高效能並滿足服務等級協定。

您可以在ONTAP系統管理員中移動卷，方法是選擇磁碟區和目標聚合、啟動卷移動操作以及選擇性地監控卷移動作業。使用系統管理員時，磁碟區移動操作會自動完成。

步驟

1. 使用ONTAP系統管理員或ONTAP CLI 將磁碟區移至聚合。

   在大多數情況下，您可以使用系統管理員來移動磁碟區。

   有關說明，請參閱"ONTAP 9 捲移動快速指南"。

當控制台顯示「需要操作」訊息時移動卷

控制台可能會顯示「需要採取行動」訊息，表示需要移動磁碟區以避免容量問題，但您需要自行解決問題。如果發生這種情況，您需要確定如何修正問題，然後移動一個或多個磁碟區。

當聚合已達到 90% 的使用容量時，控制台會顯示這些「需要操作」訊息。如果啟用了資料分層，則當聚合已達到 80% 的已使用容量時會顯示訊息。預設情況下，保留 10% 的可用空間用於資料分層。"了解有關數據分層的可用空間比率的更多信息" 。

步驟

1. [確定如何修正容量問題] 。
2. 根據您的分析，移動卷以避免容量問題：
   - [將磁碟區移至另一個系統以避免容量問題] 。
   - [將磁碟區移至另一個聚合以避免容量問題] 。

確定如何修正容量問題

如果控制台無法提供移動磁碟區以避免容量問題的建議，則必須確定需要移動的磁碟區以及是否應將它們移至同一系統上的另一個聚合或另一個系統。

步驟

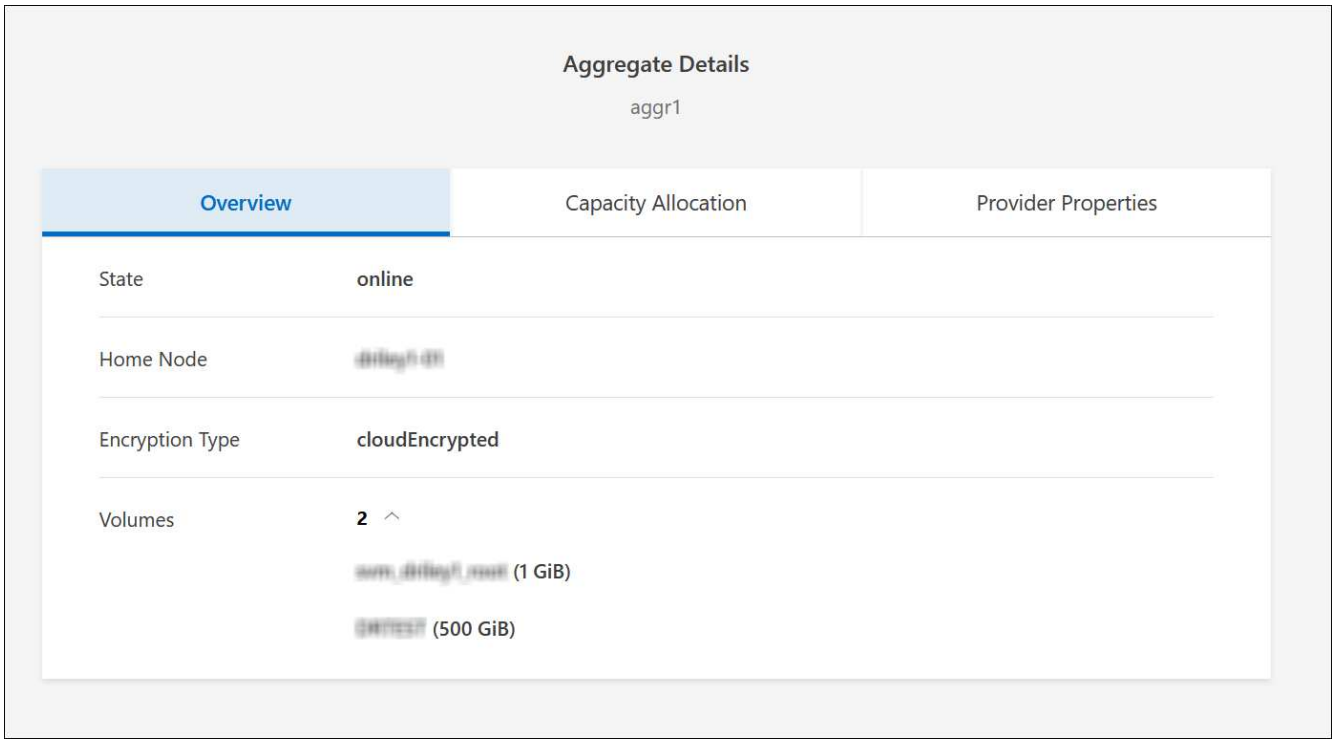
1. 查看“需要操作”訊息中的高級信息，以確定已達到其容量限制的聚合。

   例如，進階資訊應該顯示類似以下內容：聚合 aggr1 已達到其容量限制。

2. 確定要移出聚合的一個或多個磁碟區：

   a. 在Cloud Volumes ONTAP系統中，按一下 **Aggregates tab**。
   b. 在聚合圖塊上，按一下 圖標，然後點擊*查看匯總詳情*。
   c. 在「聚合詳細資料」畫面的「概述」標籤下，檢視每個磁碟區的大小並選擇要移出聚合的一個或多個磁碟區。

      您應該選擇足夠大的磁碟區來釋放聚合中的空間，以避免將來出現額外的容量問題。



3. 如果系統尚未達到磁碟限制，則應將磁碟區移至現有聚合或同一系統上的新聚合。

   有關信息，請參閱將磁碟區移至另一個聚合以避免容量問題。

4. 如果系統已達到磁碟限制，請執行下列操作之一：
   a. 刪除所有未使用的磁碟區。
   b. 重新排列磁碟區以釋放聚合上的空間。

      有關信息，請參閱將磁碟區移至另一個聚合以避免容量問題。

   c. 將兩個或多個磁碟區移動到另一個有空間的系統。

      有關信息，請參閱將磁碟區移至另一個聚合以避免容量問題。

將磁碟區移至另一個系統以避免容量問題

您可以將一個或多個磁碟區移至另一個Cloud Volumes ONTAP系統以避免容量問題。如果系統達到其磁碟限制，您可能需要執行此操作。

關於此任務

您可以按照此任務中的步驟來修正以下「需要操作」訊息：

> 移動磁碟區對於避免容量問題是必要的；但是，控制台無法為您執行此操作，因為系統已達到磁碟限制。

步驟

1. 確定具有可用容量的Cloud Volumes ONTAP系統，或部署新系統。

2. 將來源系統拖曳到目標系統以執行磁碟區的一次性資料複製。

   有關信息，請參閱"在系統之間複製數據"。

3. 前往「複製狀態」頁面，然後中斷SnapMirror關係，將複製的磁碟區從資料保護磁碟區轉換為讀取/寫入磁碟區。

   有關信息，請參閱"管理資料複製計劃和關係"。

4. 配置資料存取的磁碟區。

   有關配置資料存取目標磁碟區的信息，請參閱"ONTAP 9 卷災難復原快速指南"。

5. 刪除原始磁碟區。

   有關信息，請參閱"管理磁碟區"。

將磁碟區移至另一個聚合以避免容量問題

您可以將一個或多個磁碟區移至另一個聚合以避免容量問題。

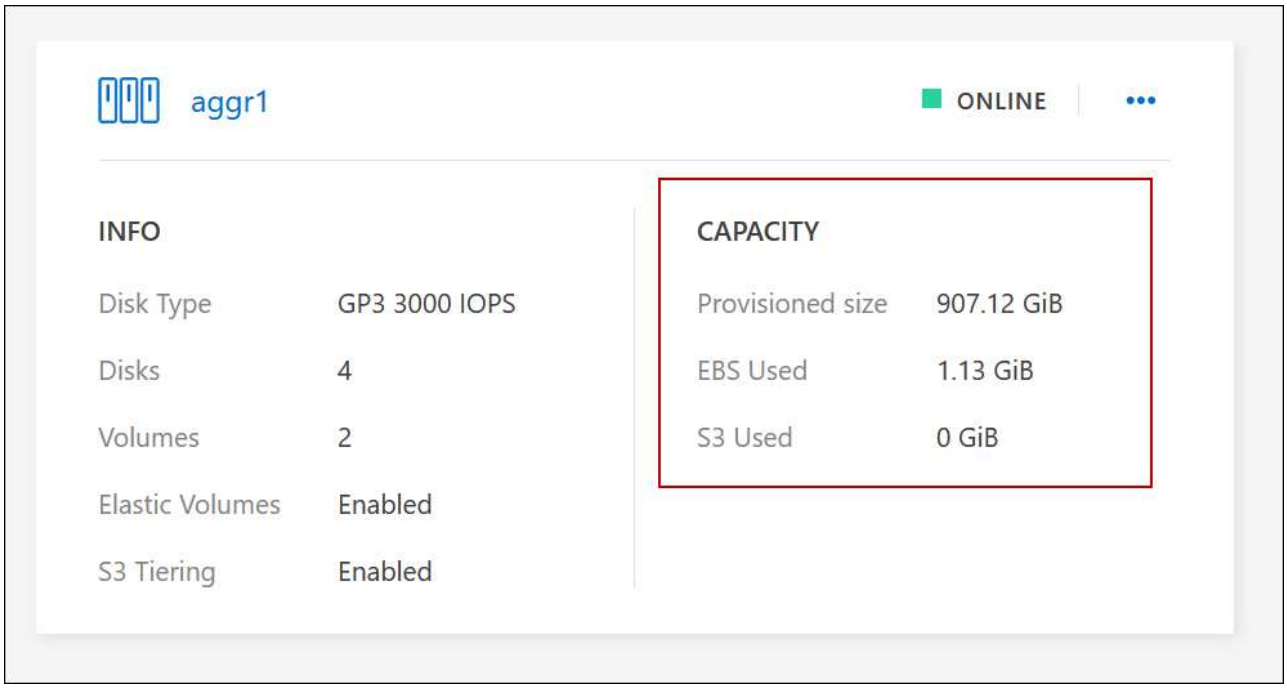
關於此任務

您可以按照此任務中的步驟來修正以下「需要操作」訊息：

> 需要移動兩個或更多磁碟區以避免容量問題；但是，控制台無法為您執行此操作。

步驟

1. 驗證現有聚合是否具有可供您需要移動的磁碟區所使用的容量：
   a. 在Cloud Volumes ONTAP系統上，按一下 **Aggregates tab**。
   b. 在所需的聚合圖塊上，按一下 ••• 圖標，然後*查看聚合詳細資訊*以查看可用容量（預先配置大小減去已使用聚合容量）。



2. 如果需要，將磁碟新增至現有聚合：
   a. 選擇聚合，然後按一下 ••• 圖示 > 新增磁碟。
   b. 選擇要新增的磁碟數量，然後按一下「新增」。
3. 如果沒有可用容量的聚合，則建立一個新的聚合。

   有關信息，請參閱"建立聚合"。
4. 使用ONTAP系統管理員或ONTAP CLI 將磁碟區移至聚合。
5. 在大多數情況下，您可以使用系統管理員來移動磁碟區。

   有關說明，請參閱"ONTAP 9 捲移動快速指南"。

交易量變動執行緩慢的原因

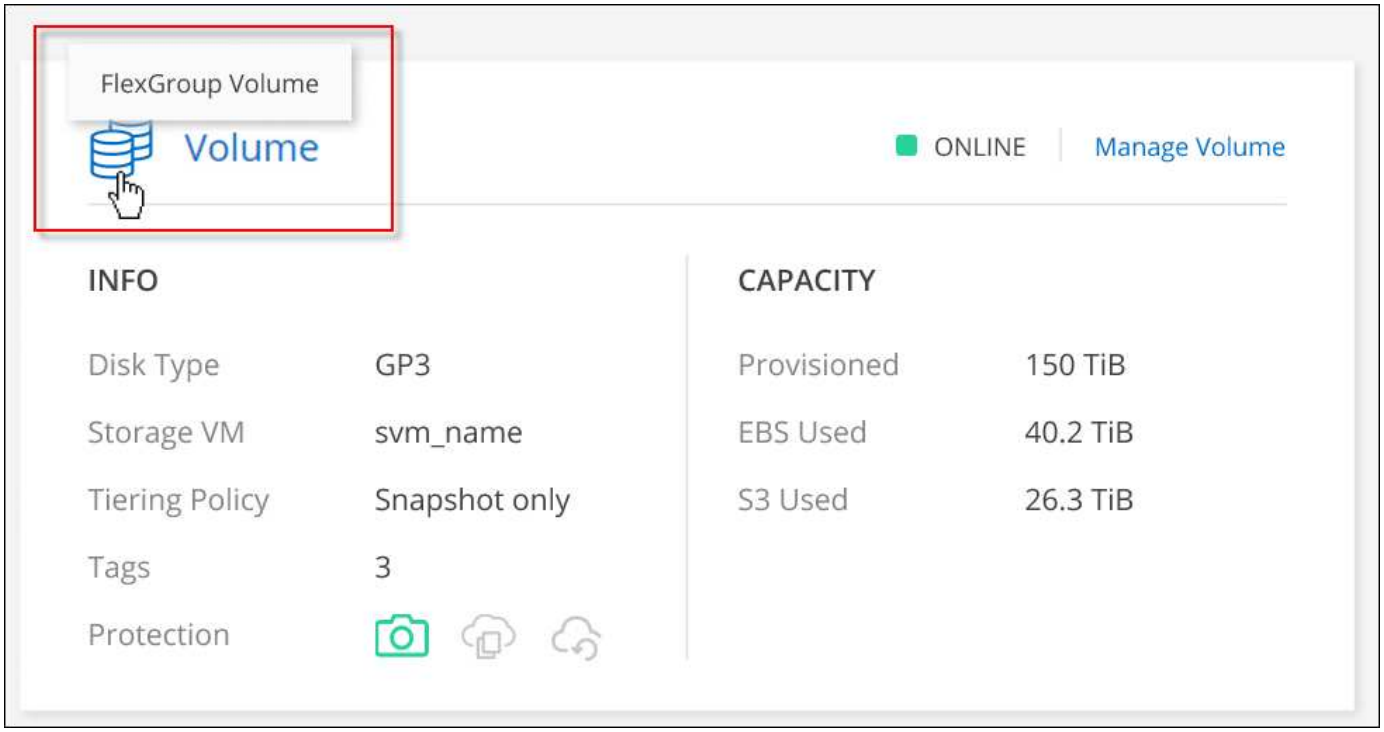
如果Cloud Volumes ONTAP符合以下任何條件，則行動磁碟區所需的時間可能會比您預期的要長：

- 該卷是一個克隆。
- 該卷是克隆的父親卷。
- 來源聚合或目標聚合具有單一吞吐量最佳化 HDD (st1) 磁碟。
- 其中一個聚合使用了較舊的物件命名方案。兩個聚合必須使用相同的名稱格式。

  如果在 9.4 或更早版本中的聚合上啟用了資料分層，則使用較舊的命名方案。
- 來源聚合和目標聚合上的加密設定不匹配，或正在進行重新金鑰。
- 在磁碟區移動時指定了 *-tiering-policy* 選項來變更分層原則。
- 在磁碟區移動時指定了 *-generate-destination-key* 選項。

查看FlexGroup卷

您可以直接透過控制台中的「磁碟區」標籤檢視透過ONTAP System Manager 或ONTAP CLI 建立的FlexGroup區。您可以透過專用的 **Volumes** 圖塊查看 FleGroup 卷的詳細信息，並透過圖示的懸停文字識別每個FlexGroup卷組。此外，您可以透過磁碟區樣式列識別和排序磁碟區清單視圖下的FlexGroup磁碟區。



目前，您只能在控制台下方查看現有的FlexGroup磁碟區。您無法在控制台中建立FlexGroup磁碟區。

將非活動Cloud Volumes ONTAP資料分層到低成本物件存儲

您可以透過將用於熱資料的 SSD 或 HDD 效能層與用於非活動資料的物件儲存容量層結合來降低Cloud Volumes ONTAP的儲存成本。資料分層由FabricPool技術提供支援。有關進階概述，請參閱"資料分層概述"。

要設定資料分層，您需要執行以下操作：

1 選擇支援的配置

大多數配置都受支援。如果您擁有執行最新版本的Cloud Volumes ONTAP系統，那麼您就可以開始了。"了解更多" 。

2 確保**Cloud Volumes ONTAP**與物件儲存之間的連接

- 對於 AWS，您需要一個指向 Amazon Simple Storage Service （Amazon S3）的 VPC 終端節點。了解更多.
- 對於 Azure，只要NetApp Console具有所需的權限，您就不需要執行任何操作。了解更多 。

- 對於 Google Cloud，您需要設定私人 Google Access 子網路並設定服務帳戶。了解更多 。

3 確保您已啟用分層聚合

應在聚合上啟用資料分層，以便在磁碟區上啟用它。您應該了解新捲和現有捲的要求。了解更多 。

4 建立、修改或複製磁碟區時選擇分層策略

當您建立、修改或複製磁碟區時， NetApp Console會提示您選擇分層策略。

- "來自讀寫卷的層次數據"
- "來自資料保護卷的分層數據"

> 資料分層不需要什麼？
>
> - 您不需要安裝功能授權來啟用資料分層。
> - 您不需要為容量層建立物件儲存。控制台會為您完成該操作。
> - 您不需要在系統層級啟用資料分層。
>
> 控制台在創建系統時為冷數據創建對象存儲，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（在某些情況下，在聚合體上 ）。

支援資料分層的配置

您可以在使用特定配置和功能時啟用資料分層。

AWS 支援

- 從Cloud Volumes ONTAP 9.2 開始，AWS 支援資料分層。
- 性能層可以是通用 SSD（gp3 或 gp2）或預先配置 IOPS SSD（io1）。

> 使用吞吐量最佳化 HDD (st1) 時，我們不建議將資料分層到物件儲存。

- 非活動資料分層儲存到 Amazon S3 儲存桶。不支援分層到其他提供者。

Azure 中的支持

- Azure 支援資料分層，如下所示：
  - 版本 9.4 適用於單節點系統
  - 9.6 版，配備 HA 對
- 效能層可以是高級 SSD 託管磁碟、標準 SSD 託管磁碟或標準 HDD 託管磁碟。
- 非活動資料分層到 Microsoft Azure Blob。不支援分層到其他提供者。

Google Cloud 支援

- 從Cloud Volumes ONTAP 9.6 開始，Google Cloud 支援資料分層。
- 效能層可以是 SSD 持久性磁碟、平衡持久性磁碟或標準持久性磁碟。
- 非活動資料分層儲存到 Google Cloud Storage。不支援分層到其他提供者。

功能互通性

- 資料分層由加密技術支援。
- 必須在磁碟區上啟用精簡配置。

要求

根據您的雲端供應商，必須設定某些連線和權限，以便Cloud Volumes ONTAP可以將冷資料分層到物件儲存。

將冷資料分層至 Amazon S3 的要求

確保 Cloud Volumes ONTAP 已連線至 Amazon S3。提供此連線的最佳方法是建立指向 S3 服務的 VPC 端點。有關說明，請參閱 "AWS 文件：建立網關終端節點"。

建立 VPC 端點時，請確保選擇與Cloud Volumes ONTAP實例相對應的區域、VPC 和路由表。您還必須修改安全群組以新增允許流量到 S3 端點的出站 HTTPS 規則。否則， Cloud Volumes ONTAP無法連線到 S3 服務。

如果您遇到任何問題，請參閱 "AWS Support 知識中心：為什麼我無法使用閘道 VPC 終端節點連接到 S3 儲存桶？"。

將冷資料分層到 Azure Blob 儲存體的需求

只要控制台具有所需的權限，您就不需要在效能層和容量層之間建立連線。如果控制台代理程式的自訂角色具有下列權限，則控制台將為您啟用 VNet 服務終端：

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

自訂角色預設包含權限。 "查看控制台代理程式的 Azure 權限"

將冷資料分層到 Google Cloud Storage 儲存桶的要求

- 必須為Cloud Volumes ONTAP所在的子網路設定私有 Google Access。有關說明，請參閱 "Google Cloud 文件：配置私有 Google 存取權限"。
- 必須將服務帳戶附加到Cloud Volumes ONTAP。

  "了解如何設定此服務帳號" 。

  建立Cloud Volumes ONTAP系統時，系統會提示您選擇此服務帳戶。

  如果在部署過程中未選擇服務帳號，則需要關閉 Cloud Volumes ONTAP，前往 Google Cloud Console，然後將服務帳號附加到 Cloud Volumes ONTAP 執行個體。之後，您可以按照下一節中的說明啟用資料分層。

- 若要使用客戶管理的加密金鑰加密儲存桶，請啟用 Google Cloud 儲存桶以使用該金鑰。

  "了解如何將客戶管理的加密金鑰與Cloud Volumes ONTAP結合使用" 。

實現要求後啟用資料分層

只要沒有連線或權限問題，控制台就會在建立系統時為冷資料建立物件儲存。如果您在建立系統之後才實現上面列出的要求，那麼您將需要透過 API 或ONTAP系統管理員手動啟用分層，從而建立物件儲存。

透過控制台啟用分層的功能將在未來的Cloud Volumes ONTAP版本中提供。

確保在聚合上啟用分層

必須在聚合上啟用資料分層才能在磁碟區上啟用資料分層。您應該了解新捲和現有捲的要求。

- 新卷

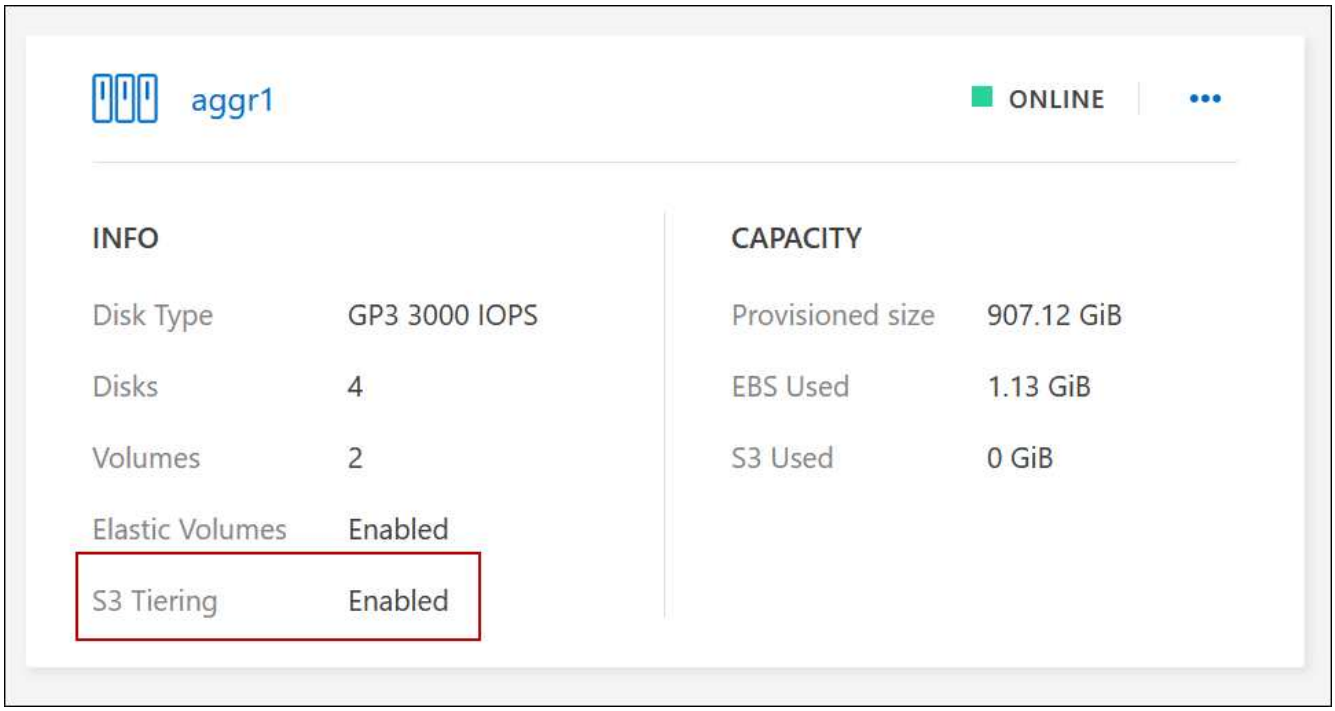
  如果您在新磁碟區上啟用資料分層，則無需擔心在聚合上啟用資料分層。控制台在已啟用分層的現有聚合上建立卷，或者如果尚不存在啟用資料分層的聚合，則為該磁碟區建立新的聚合。

- 現有捲

  若要在現有磁碟區上啟用資料分層，請確保在底層聚合上啟用它。如果現有聚合上未啟用資料分層，則需要使用ONTAP系統管理器將現有聚合附加到物件儲存。

確認聚合上是否啟用了分層的步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 開啟Cloud Volumes ONTAP系統。
3. 選擇“聚合”標籤並檢查聚合上是否啟用或停用分層。



在聚合上啟用分層的步驟

1. 在ONTAP系統管理員中，按一下「儲存」>「層級」。
2. 點擊聚合的操作選單並選擇*附加雲層*。
3. 選擇要附加的雲層，然後按一下「儲存」。

下一步是什麼？

現在您可以在新磁碟區和現有磁碟區上啟用資料分層，如下一節所述。

來自讀寫卷的層次數據

Cloud Volumes ONTAP可以將讀寫磁碟區上的非活動資料分層到經濟高效的物件儲存中，從而釋放效能層以儲存熱資料。

步驟

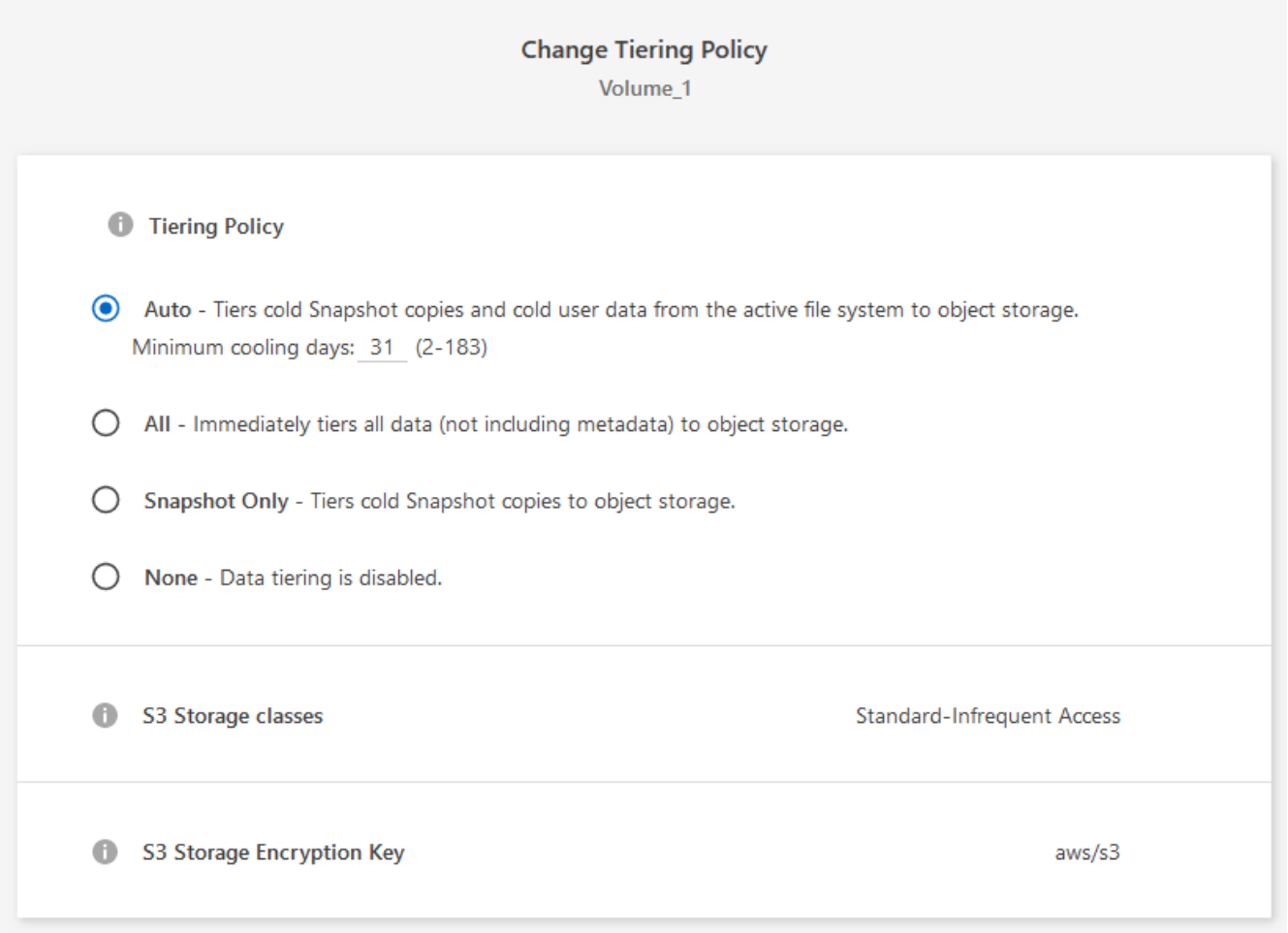
1. 在系統下的*Volumes*標籤中，建立一個新磁碟區或變更現有磁碟區的圖層：

任務	行動
建立新磁碟區	按一下“新增磁碟區”。
修改現有捲	選擇所需的磁碟區圖區塊，按一下「管理磁碟區」以存取「管理磁碟區」右側面板，然後按一下右側面板下的「進階操作」和「變更分層原則」。

2. 選擇分層策略。

   有關這些政策的描述，請參閱"資料分層概述"。

   例子



如果尚不存在啟用資料分層的聚合，則控制台將為磁碟區建立一個新的聚合。

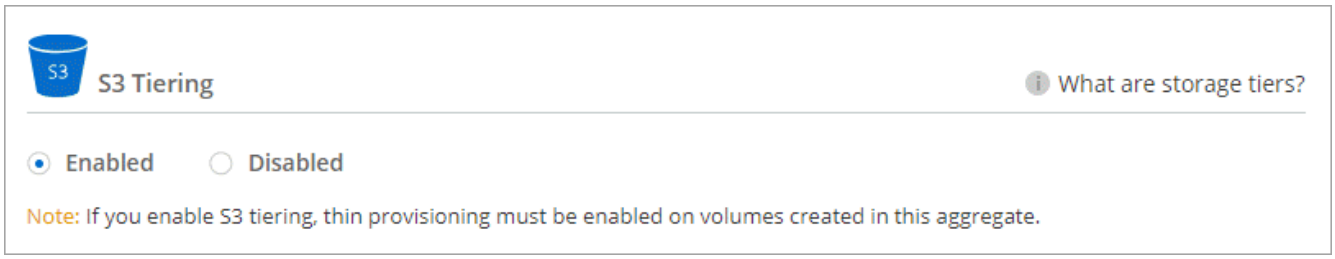
來自資料保護卷的分層數據

Cloud Volumes ONTAP可以將資料從資料保護磁碟區分層到容量層。如果啟動目標卷，資料在讀取時會逐漸移動到效能層。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在 系統 頁面上，選擇包含來源磁碟區的Cloud Volumes ONTAP系統，然後將其拖曳到要將磁碟區複製到的系統。
3. 依照提示操作，直到到達分層頁面並啟用資料分層到物件儲存。

   例子



有關複製資料的協助，請參閱 "將數據複製到雲端或從雲端複製數據"。

變更分層資料的儲存類別

部署Cloud Volumes ONTAP後，您可以透過變更 30 天未存取的非活動資料的儲存類別來降低儲存成本。如果您確實存取數據，則存取成本會更高，因此在更改儲存類別之前必須考慮到這一點。

分層資料的儲存類別是系統範圍的，而不是每個磁碟區的。

有關受支援的儲存類別的信息，請參閱"資料分層概述"。

步驟

1. 在Cloud Volumes ONTAP系統上，按一下選單圖標，然後按一下 儲存類別 或 **Blob** 儲存分層。
2. 選擇一個儲存類，然後按一下*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了將資料分層到物件儲存時Cloud Volumes ONTAP SSD/HDD 上需要多少可用空間。預設設定是 10% 的可用空間，但您可以根據需要調整設定。

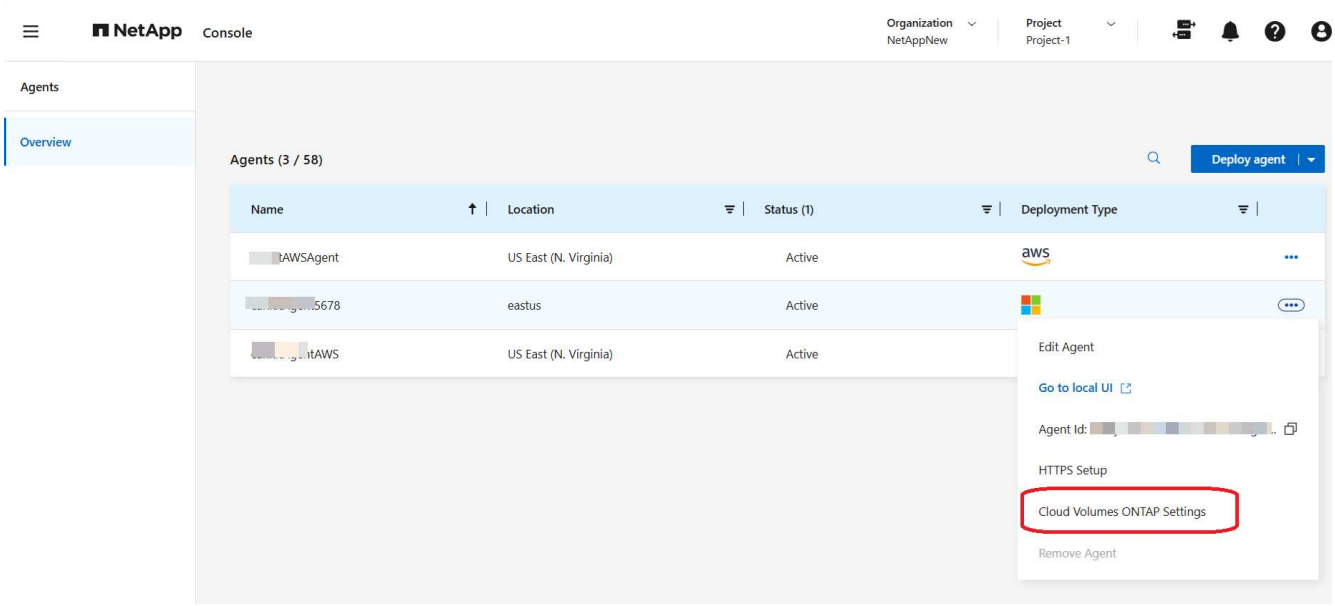
例如，您可以選擇少於 10% 的可用空間，以確保您利用所購買的容量。當需要額外容量時，控制台可以為您購買額外的磁碟（直到達到聚合的磁碟限制）。

如果沒有足夠的空間，那麼Cloud Volumes ONTAP就無法移動數據，而且您可能會遇到效能下降的情況。任何改變都應謹慎進行。如果您不確定，請聯絡NetApp支援尋求指導。

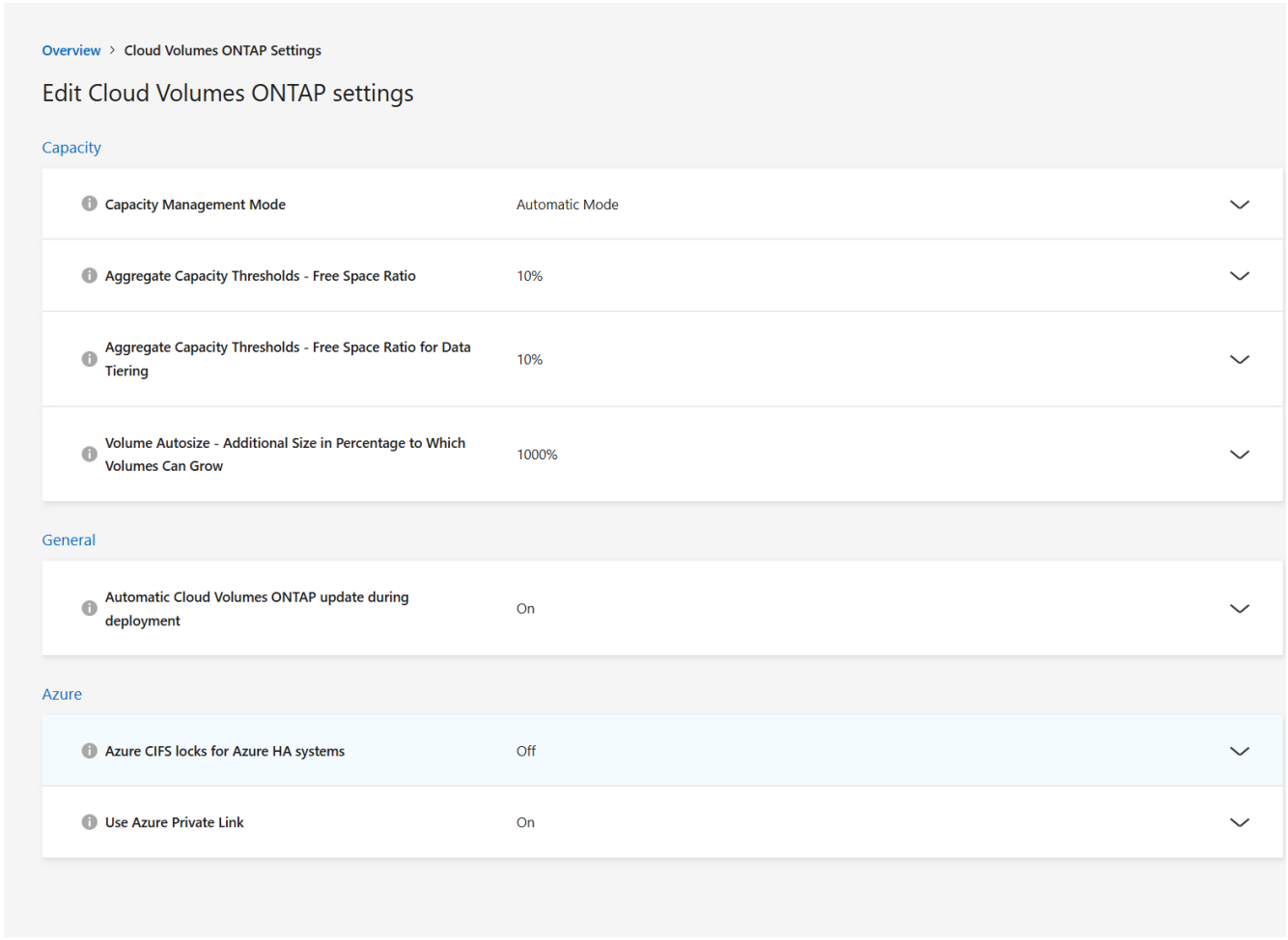
此比率對於災難復原場景很重要，因為當從物件儲存讀取資料時， Cloud Volumes ONTAP會將資料移至 SSD/HDD 以提供更好的效能。如果沒有足夠的空間，那麼Cloud Volumes ONTAP就無法移動資料。在更改比例時請考慮到這一點，以便滿足您的業務需求。

步驟

1. 從左側導覽窗格前往*管理>代理*。
2. 點選 ••• 管理Cloud Volumes ONTAP系統的控制台代理的圖示。
3. 選擇* Cloud Volumes ONTAP設定*。



4. 在「容量」下，按一下「聚合容量閾值 - 資料分層的可用空間比率」。



5. 根據您的要求更改可用空間比例，然後按一下「儲存」。

更改自動分層策略的冷卻期

如果您使用自動分層策略在Cloud Volumes ONTAP磁碟區上啟用了資料分層，則可以根據業務需求調整預設冷卻期。僅使用ONTAP CLI 和 API 支援此操作。

冷卻期是指磁碟區中的使用者資料在被視為「冷」並移動到物件儲存之前必須保持不活動的天數。

自動分層策略的預設冷卻期為 31 天。您可以如下變更冷卻時間：

- 9.8 或更高版本：2 天至 183 天
- 9.7 或更早版本：2 天至 63 天

步

1. 建立磁碟區或修改現有磁碟區時，請在 API 請求中使用 *minimumCoolingDays* 參數。

在系統退役時刪除 **S3** 儲存桶

當您退役環境時，您可以刪除包含來自Cloud Volumes ONTAP系統的分層資料的 S3 儲存桶。

只有在滿足以下條件時，您才可以刪除 S3 儲存桶：

- Cloud Volume ONTAP系統已從控制台中刪除。
- 所有物件都從儲存桶中刪除，並且 S3 儲存桶為空。

當您退役Cloud Volumes ONTAP系統時，為該環境建立的 S3 儲存桶不會自動刪除。相反，它保持孤立狀態以防止任何意外的資料遺失。您可以刪除儲存桶中的對象，然後移除 S3 儲存桶本身，或保留它以供日後使用。參考 "ONTAP CLI：vserver object-store-server bucket 刪除"。

從主機系統連接到**Cloud Volumes ONTAP**上的 **LUN**

當您建立 iSCSI 磁碟區時， NetApp Console會自動為您建立 LUN。我們透過為每個磁碟區建立一個 LUN 來簡化操作，因此無需進行任何管理。建立磁碟區後，使用 IQN 從主機連線到 LUN。

請注意以下事項：

- 控制台的自動容量管理不適用於 LUN。當它建立 LUN 時，它會停用自動增長功能。
- 您可以從ONTAP系統管理員或ONTAP CLI 建立其他 LUN。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在*系統*頁面上，雙擊要管理磁碟區的Cloud Volumes ONTAP系統。
3. 在系統中，選擇*Volumes*選項卡。
4. 前往所需的磁碟區圖區塊，然後選擇*管理磁碟區*以存取右側的管理磁碟區面板。
5. 按一下*目標 iQN*。
6. 按一下*複製*以複製 iQN 名稱。

7. 建立從主機到 LUN 的 iSCSI 連線。
    - "適用於 Red Hat Enterprise Linux 的ONTAP 9 iSCSI 快速設定：啟動與目標的 iSCSI 會話"
    - "適用於 Windows 的ONTAP 9 iSCSI 快速設定：啟動與目標的 iSCSI 會話"
    - "ONTAP SAN 主機配置"

使用**Cloud Volumes ONTAP**系統上的**FlexCache**磁碟區加速資料存取

FlexCache卷是一種儲存卷，用於快取從原始（或來源）卷讀取的 SMB 和 NFS 資料。隨後讀取快取資料可以加快對該資料的存取速度。

您可以使用FlexCache磁碟區來加快資料存取速度或卸載存取量大的磁碟區的流量。 FlexCache磁碟區有助於提高效能，特別是當用戶端需要重複存取相同資料時，因為可以直接提供資料而無需存取原始磁碟區。 FlexCache卷非常適合讀取密集的系統工作負載。

NetApp Console提供FlexCache磁碟區的管理"NetApp Volume Caching"。

您也可以使用ONTAP CLI 或ONTAP系統管理器來建立和管理FlexCache磁碟區：

- "FlexCache卷實現更快資料存取電源指南"
- "在 System Manager 中建立FlexCache卷"

當來源加密時使用**FlexCache**

在原始磁碟區已加密的Cloud Volumes ONTAP系統上設定FlexCache時，需要執行額外的步驟，以確保FlexCache磁碟區可以正確存取和快取加密資料。

開始之前

1. 加密設定：確保來源磁碟區完全加密且可操作。對於Cloud Volumes ONTAP系統，這涉及與特定於雲端的金鑰管理服務整合。

對於 AWS，這通常表示使用 AWS 金鑰管理服務 (KMS)。有關信息，請參閱"使用 AWS Key Management Service 管理金鑰"。

對於 Azure，您需要為NetApp磁碟區加密 (NVE) 設定 Azure Key Vault。有關信息，請參閱"使用 Azure Key Vault 管理金鑰"。

對於 Google Cloud，它是 Google Cloud Key Management Service。有關信息，請參閱"使用 Google 的雲端金鑰管理服務管理金鑰"。

1. 金鑰管理服務：在建立FlexCache區之前，請先確認金鑰管理服務是否在Cloud Volumes ONTAP系統上正確設定。此配置對於FlexCache磁碟區解密來自原始磁碟區的資料至關重要。
2. 許可：確認有效的FlexCache許可證可用並在Cloud Volumes ONTAP系統上啟動。
3. * ONTAP版本*：確保您的Cloud Volumes ONTAP系統的ONTAP版本支援帶有加密磁碟區的FlexCache 。參考最新 "ONTAP發行說明"或相容性矩陣以獲取更多資訊。
4. 網路配置：確保網路配置允許原始磁碟區和FlexCache磁碟區之間的無縫通訊。這包括雲端環境中的正確路由和 DNS 解析。

步驟

使用加密來源磁碟區在Cloud Volumes ONTAP系統上建立FlexCache磁碟區。有關詳細步驟和其他注意事項，請參閱以下部分：

- "FlexCache卷實現更快資料存取電源指南"
- "在 System Manager 中建立FlexCache卷"

聚合管理

為Cloud Volumes ONTAP系統建立聚合

您可以自行建立聚合，也可以讓NetApp Console在建立磁碟區時為您建立聚合。自行建立聚合的好處是您可以選擇底層磁碟大小，從而可以根據所需的容量或效能調整聚合的大小。

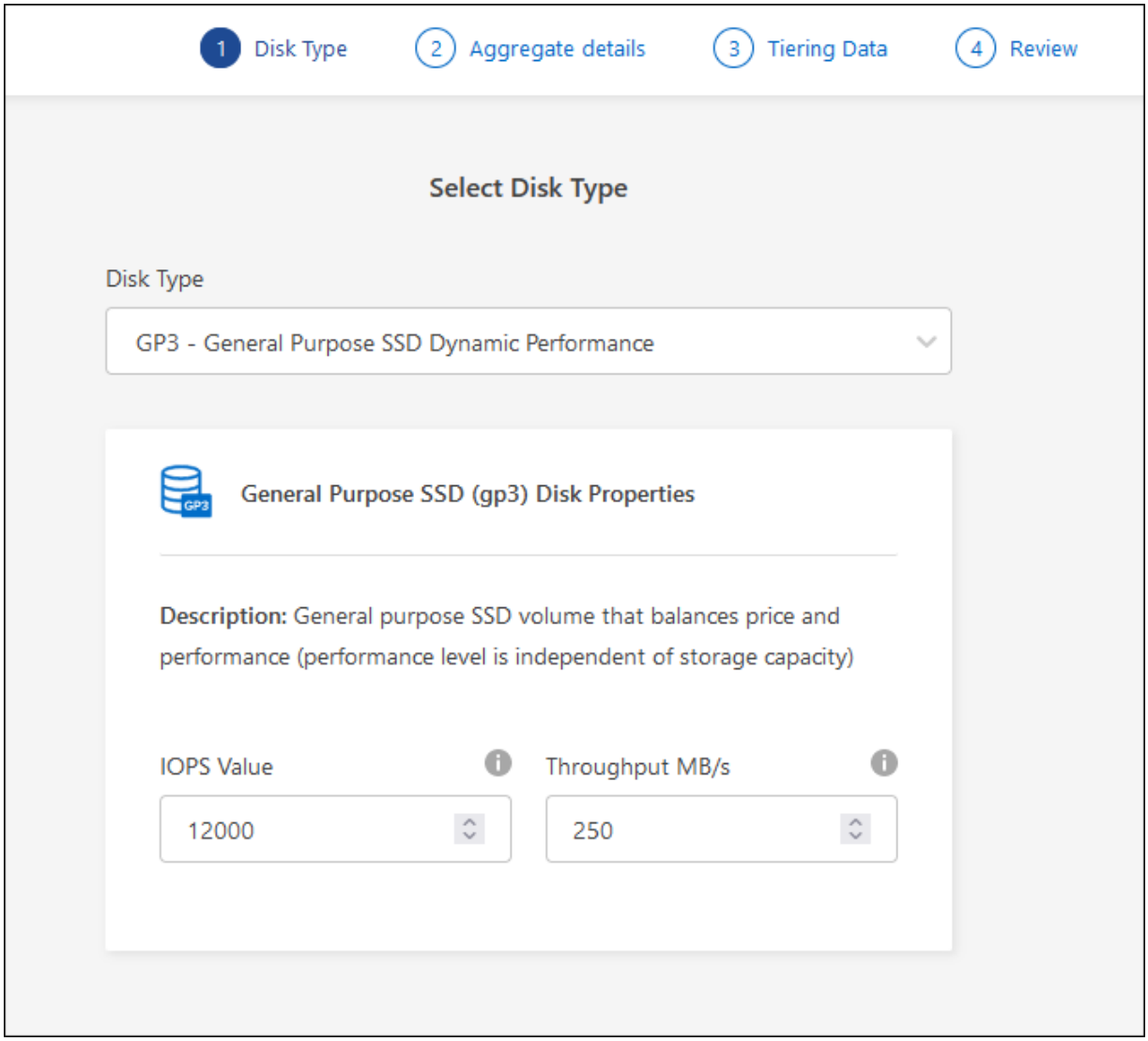
必須直接從控制台建立和刪除所有磁碟和聚合。您不應從其他管理工具執行這些操作。這樣做會影響系統穩定性，妨礙將來添加磁碟的能力，並可能產生冗餘的雲端供應商費用。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在「系統」頁面上，雙擊要管理聚合的Cloud Volumes ONTAP系統的名稱。
3. 在“聚合”標籤上，按一下“新增聚合”，然後指定聚合的詳細資訊。

AWS

- 如果系統提示您選擇磁碟類型和磁碟大小，請參閱"在 AWS 中規劃您的Cloud Volumes ONTAP配置"。
- 如果提示您輸入聚合的容量大小，表示您正在支援 Amazon EBS 彈性磁碟區功能的配置上建立聚合。以下螢幕截圖顯示了由 gp3 磁碟組成的新聚合的範例。



"了解有關彈性卷支持的更多信息"。

Azure

有關磁碟類型和磁碟大小的協助，請參閱"在 Azure 中規劃您的Cloud Volumes ONTAP配置"。

Google雲

有關磁碟類型和磁碟大小的協助，請參閱"在 Google Cloud 中規劃您的Cloud Volumes ONTAP配置"。

4. 按一下“新增”，然後按一下“核准並購買”。

管理Cloud Volumes ONTAP叢集的聚合

透過新增磁碟、查看有關聚合的資訊以及刪除聚合來自行管理聚合。

必須直接從NetApp Console建立和刪除所有磁碟和聚合。您不應從其他管理工具執行這些操作。這樣做會影響系統穩定性，妨礙將來添加磁碟的能力，並可能產生冗餘的雲端供應商費用。

開始之前

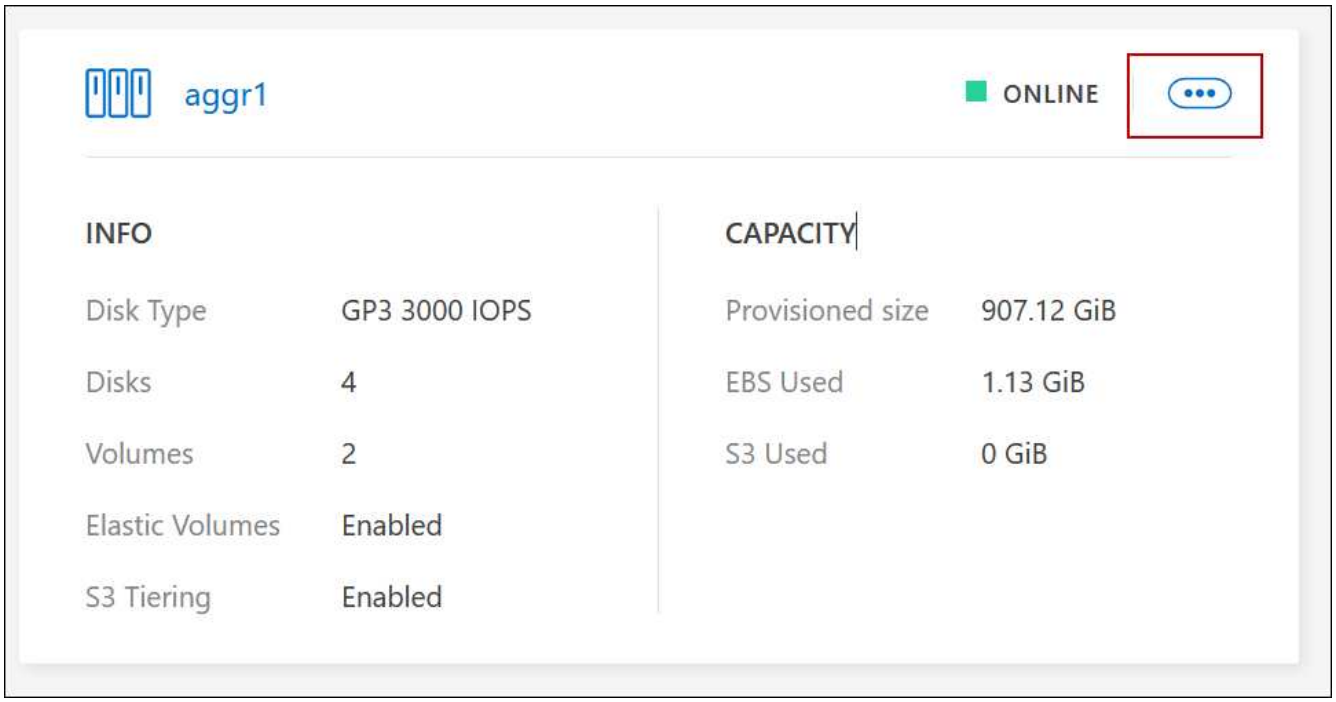
如果要刪除聚合，則必須先刪除聚合中的磁碟區。

關於此任務

如果聚合空間不足，您可以使用ONTAP系統管理員將磁碟區移至另一個聚合。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在「系統」頁面上，雙擊要管理聚合的Cloud Volumes ONTAP系統。
3. 從系統詳細資料中，按一下「聚合」標籤。
4. 對於所需的聚合，按一下 ••• 管理操作的圖示。



5. 透過可用選項管理您的聚合 ••• 菜單。

若要將磁碟新增至聚合，聚合中的所有磁碟必須具有相同的大小。

對於 AWS，您可以增加支援 Amazon EBS 彈性磁碟區的聚合的容量。

1. 根據 ••• 在選單上，點選*增加容量*。
2. 輸入您想要新增的額外容量，然後按一下*增加*。

請注意，您必須將聚合的容量增加至少 256 GiB 或聚合大小的 10%。例如，如果您有 1.77 TiB 聚合，則 10% 就是 181 GiB。這低於 256 GiB，因此聚合的大小必須增加 256 GiB 的最小值。

在控制台代理上管理Cloud Volumes ONTAP聚合容量

每個控制台代理程式都有設定來決定如何管理Cloud Volumes ONTAP的聚合容量。

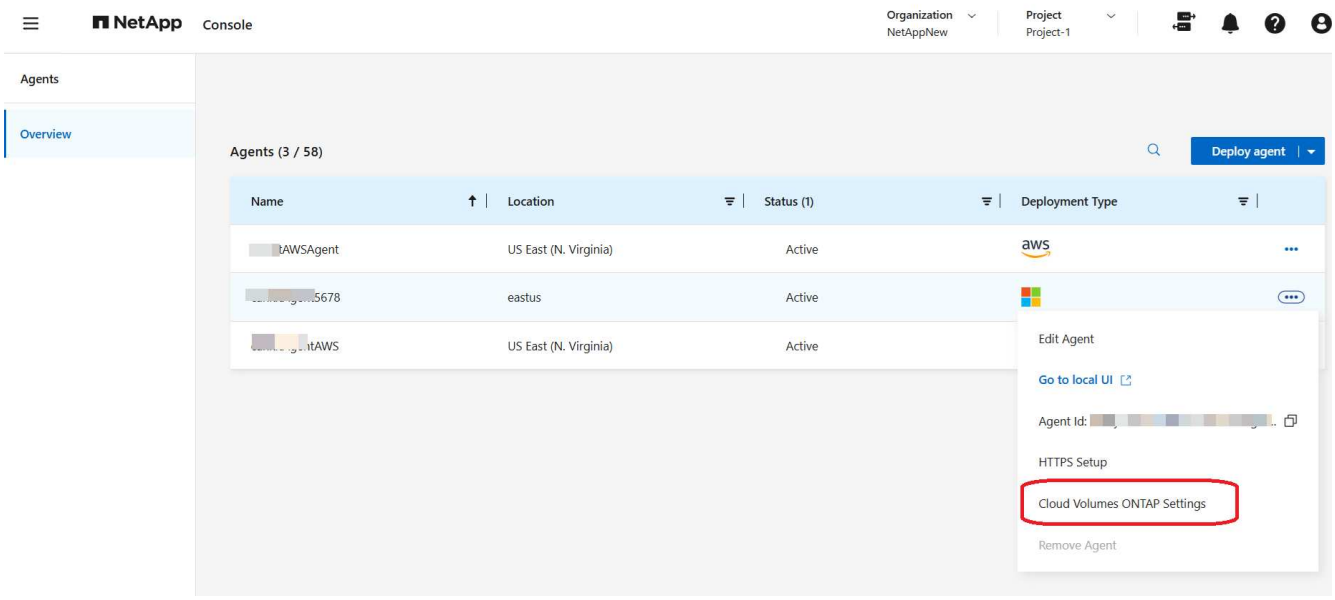
這些設定會影響控制台代理程式管理的所有Cloud Volumes ONTAP系統。如果您有另一個控制台代理，則可以進行不同的配置。

所需權限

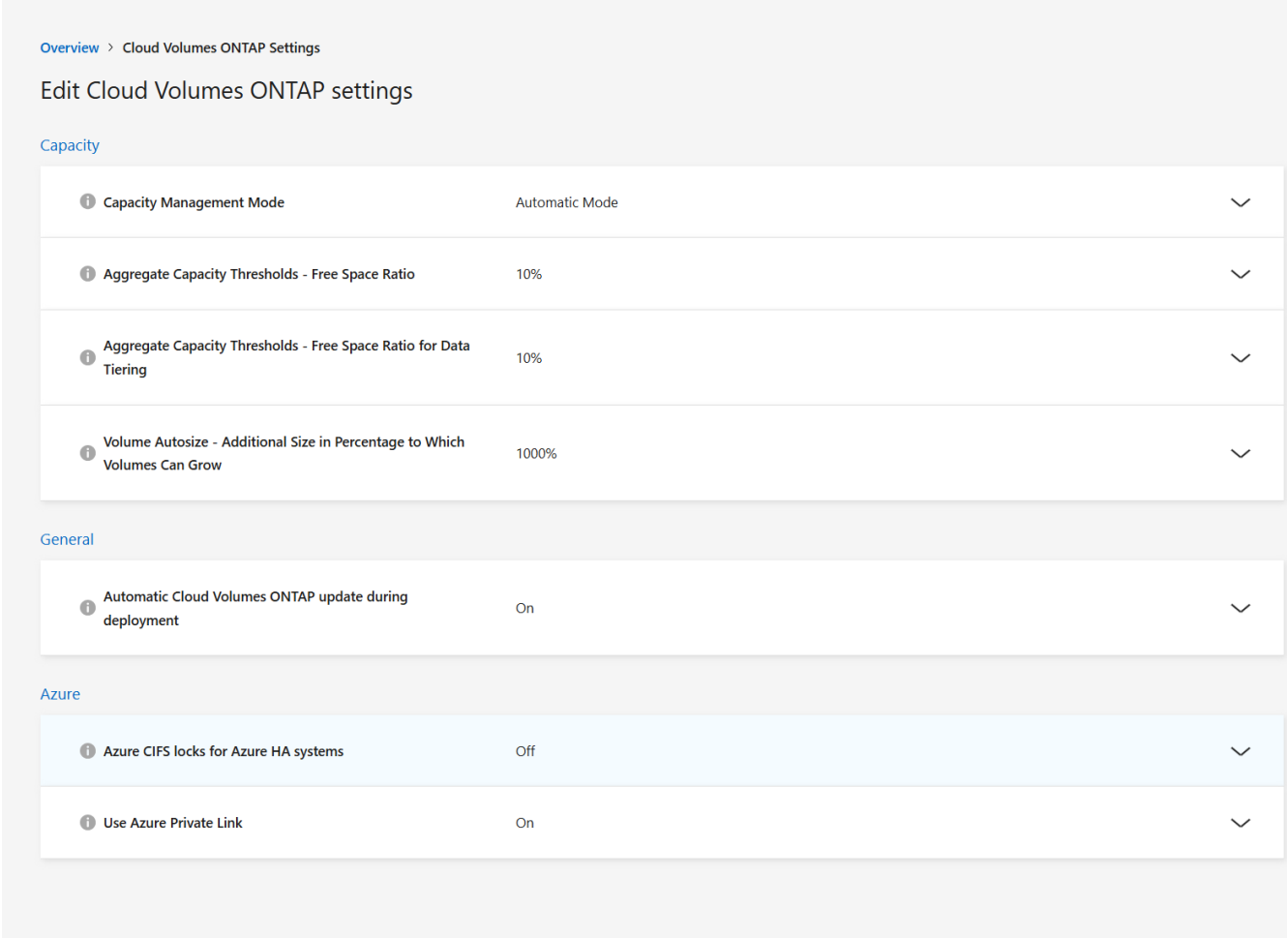
您需要NetApp Console的組織或帳號管理員權限才能修改Cloud Volumes ONTAP設定。

步驟

1. 從左側導覽窗格前往*管理>代理*。
2. 點選 ••• 管理Cloud Volumes ONTAP系統的控制台代理的圖示。
3. 選擇* Cloud Volumes ONTAP設定*。



4. 在「容量」下，修改以下任意設定：



容量管理模式

選擇控制台是否應通知您儲存容量決策，或是否應自動為您管理容量需求。

"了解容量管理模式的工作原理" 。

總容量門檻 - 可用空間比率

此比率是容量管理決策中的關鍵參數，無論您處於自動或手動容量管理模式，了解其影響都至關重要。建議根據您的特定儲存需求和預期成長來設定此閾值，以維持資源利用率和成本之間的平衡。

在手動模式下，如果聚合上的可用空間比率低於指定的閾值，則會觸發通知，提醒您應採取措施解決低可用空間比率問題。監控這些通知並手動管理總容量以避免服務中斷並確保最佳效能非常重要。

可用空間比率計算如下：（聚合容量 - 聚合上的總使用容量）/聚合容量

參考"自動容量管理"現在了解容量在Cloud Volumes ONTAP中自動管理。

聚合容量閾值 - 資料分層的可用空間比率

定義將資料分層到容量層（物件儲存）時效能層（磁碟）上需要多少可用空間。

此比率對於災難復原場景很重要。當從容量層讀取資料時， Cloud Volumes ONTAP會將資料移至效能層以提供更好的效能。如果沒有足夠的空間，那麼Cloud Volumes ONTAP就無法移動資料。

5. 點選“儲存”。

在 Azure 中管理磁碟效能

在 Azure 中管理Cloud Volumes ONTAP的 Premium SSD v2 磁碟效能

您可以透過設定 Premium SSD v2 磁碟的 IOPS 和吞吐量參數來最佳化 Azure 中的Cloud Volumes ONTAP效能。此功能僅在Cloud Volumes ONTAP已部署 Azure Premium SSD v2 磁碟類型時可用，在初始部署期間無法使用。透過提升效能，您可以充分利用 Azure Premium SSD v2 磁碟的靈活性和高效能功能。

Premium SSD v2 磁碟支援需要快速、可靠性能、低延遲、高 IOPS 和高吞吐量的工作負載。透過調整 IOPS 和吞吐量設置，您可以自訂部署中聚合的效能。有關 Premium SSD v2 磁碟的更多信息，請參閱 "部署進階 SSD v2 磁碟"。

使用 API 實作修改 Premium SSD v2 磁碟設定的自動化流程。有關執行Cloud Volumes ONTAP API 呼叫的信息，請參閱 "您的第一次 API 呼叫"。

關於此任務

- 此功能適用於 Azure 單一可用性區域中的Cloud Volumes ONTAP部署。
- 更改磁碟設定會統一改變 RAID 群組或聚合的效能。為了確保整個叢集效能的一致性，叢集中所有磁碟的效能都調整到同一水平。
- 這些變更僅影響單一聚合體，不會影響群組內的其他聚合體。
- 在NetApp Console中部署Cloud Volumes ONTAP或進行容量最佳化時自動配置的高級 SSD v2 磁碟，或透過 API 新增的高級 SSD v2 磁碟，均可進行修改。
- 不支援磁碟調整大小（更改磁碟容量）。

開始之前

在配置 Premium SSD v2 磁碟的 IOPS 和吞吐量參數之前，請注意以下幾點：

- 請確保您僅選擇了進階 SSD v2 資料磁碟。 Premium SSD v1 磁碟或根磁碟和啟動磁碟不符合此變更條件。
- 使用Cloud Volumes ONTAP在部署期間建立的預先配置基線設定作為對應磁碟大小的最小 IOPS 和吞吐量值。這些基準設定與 Premium SSD v1 的效能特點相符。
- 將 IOPS 和吞吐量值設定為等於或高於磁碟大小的最低基準值。例如，對於 1TB 的磁碟大小，將最小 IOPS 值設為 5,000，將最小吞吐量值設為 200 MBps。您可以設定高於這些最小值的值，但不能低於這些最小值。
- 在支援的 Premium SSD v2 範圍內配置值：IOPS 在 3000 到 80000 之間，吞吐量在 125 到 1200 MBps 之間。
- 請確保您的 Premium SSD v2 磁碟大小在 Azure Cloud Volumes ONTAP支援的 500GB 到 32TB 範圍內。請注意，這些大小限制與 Azure 為進階 SSD v2 磁碟提供的最小值和最大值不同。

步驟

- 使用下列 API 呼叫來變更 IOPS 和吞吐量的屬性值：

  在 24 小時內，您最多可以呼叫此 API 四次。

```
PUT /azure/vsa/aggregates/{workingEnvironmentId}/{aggregateName}
```

在請求主體中包含以下參數：

```
{
  "aggregateName": "aggr_name",
  "iops": "modified_iops_value",
  "throughput": "modified_throughput_value",
  "workingEnvironmentId": "we_id"
}
```

完成後

API 回傳回應表示操作成功後，請在 Azure 入口網站中檢查Cloud Volumes ONTAP系統的磁碟詳細信息，以驗證修改後的參數。

相關資訊

- "準備使用 API"
- "Cloud Volumes ONTAP工作流程"
- "取得所需的標識符"
- "使用 REST API 存取Cloud Volumes ONTAP"
- "在可用性集中將 Premium SSD v2 與虛擬機器一起使用"

在 **Azure Cloud Volumes ONTAP**中變更進階 **SSD** 磁碟的效能層級

您可以使用 Azure 入口網站升級 Azure Cloud Volumes ONTAP高階 SSD 託管磁碟的效能層級。這是一個手動過程，涉及將每個高級 SSD 磁碟的磁碟層級變更為更高效能的層級。更改NVRAM磁碟的效能層級可以透過提供更高的 IOPS 和吞吐量能力來幫助緩解效能瓶頸並提高Cloud Volumes ONTAP系統的效率。

請務必與NetApp支援團隊合作，確定您環境中遇到的瓶頸是由於NVRAM磁碟引起的，升級該層級可以解決該問題。

關於此任務

- 預設情況下，Azure 中的Cloud Volumes ONTAP在 P20 層部署高階 SSD 磁碟作為NVRAM 。P20 層級提供平衡的效能，適合大多數工作負載。但是，如果您的工作負載需要更高的效能，您可以將NVRAM磁碟升級到更高的級別，例如 P30。

  目前，您只能透過 Azure 入口網站將NVRAM磁碟從 P20 層升級至 P30 層。

- 您無需更改磁碟大小。容量仍然是 512 GB。此操作只會改變磁碟的效能等級。

開始之前

- 仔細評估是否有必要進行此項更改，因為將NVRAM磁碟升級到更高效能等級會產生額外的成本。
- 您的Cloud Volumes ONTAP版本必須為 9.11.1 或更高版本。對於較低版本，您可以升級到 9.11.1 或更高版本，或向NetApp支援部門提出功能策略變更請求 (FPVR)。

步驟

此場景假設有兩個節點 node01 和 node02 在Cloud Volumes ONTAP高可用性 (HA) 部署中。使用 Azure 入口網站升級層級。

1. 運行此命令以進行 node1 活動節點。手動故障轉移 node02。

   ```
   storage failover takeover -ofnode <Node02>
   ```

2. Sign inAzure 入口網站。
3. 接管完成後，請前往虛擬機器實例。 `node02`然後點擊“停止”按鈕將其關閉。
4. 導航至資源組 node02 從磁碟清單中選擇NVRAM磁碟以變更層級。
5. 選擇*尺寸+性能*。
6. 在「效能等級」下拉式選單中，選擇 P30 - 5000 IOPS, 200MB/s。
7. 選擇*調整大小*。
8. 打開 node02 實例。
9. 檢查 Azure 序列控制台，直到看到以下訊息： waiting for giveback。
10. 執行此命令即可回饋 node02：

    ```
    storage failover giveback -ofnode <Node02>
    ```

11. 重複這些步驟 node01 製作 node02 接管 node01`這樣您就可以升級NVRAM磁碟層。 `node01。

完成後

當您啟動兩個節點後，請在 Azure 入口網站中檢查Cloud Volumes ONTAP系統的磁碟詳細信息，以驗證修改後的參數。

相關資訊

- Azure 文件： "無需停機即可更改性能等級"
- 支援團隊知識庫： "如何在 Azure CVO 升級NVRAM磁碟的效能層"
- "升級Cloud Volumes ONTAP軟體版本"

儲存虛擬機器管理

管理Cloud Volumes ONTAP 的儲存虛擬機

儲存虛擬機是在ONTAP內運作的虛擬機，可為您的用戶端提供儲存和資料服務。您可能知道這是一個_SVM_或_vserver_。 Cloud Volumes ONTAP預設配置一個儲存虛擬機，但某些配置支援額外的儲存虛擬機。

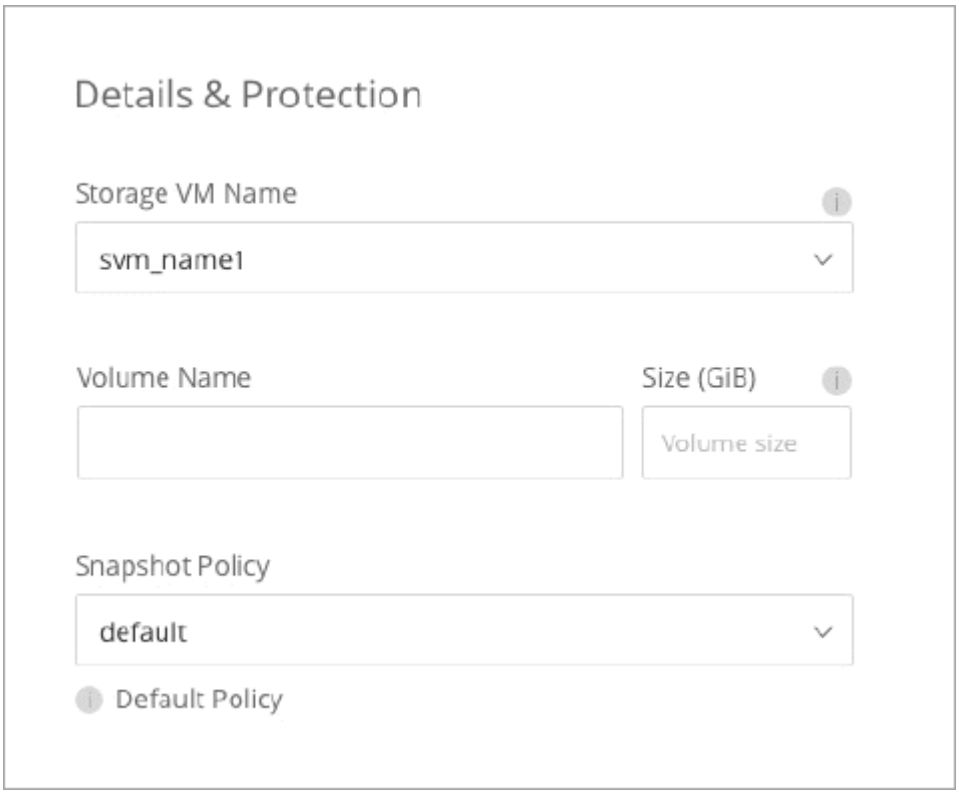
支援的儲存虛擬機器數量

特定配置支援多個儲存虛擬機器。前往 "Cloud Volumes ONTAP發行說明"驗證您的Cloud Volumes ONTAP版本支援的儲存虛擬機器數量。

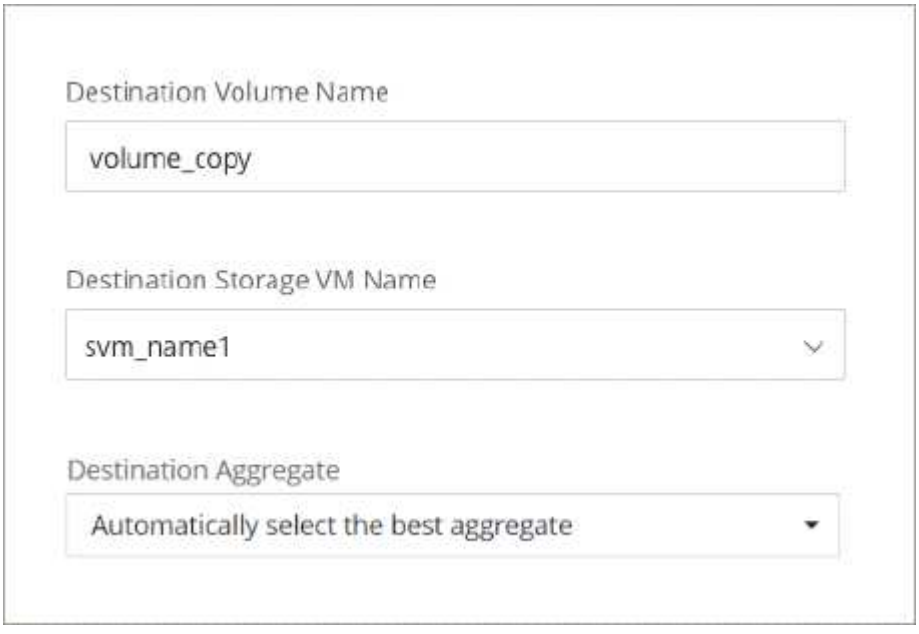
使用多個儲存虛擬機

NetApp Console支援您從ONTAP系統管理員或ONTAP CLI 建立的任何其他儲存虛擬機器。

例如，下圖顯示如何在建立磁碟區時選擇儲存虛擬機器。



下圖顯示了將磁碟區複製到另一個系統時如何選擇儲存虛擬機器。



修改預設儲存虛擬機器的名稱

控制台會自動命名其為Cloud Volumes ONTAP所建立的單一儲存虛擬機器。如果您有嚴格的命名標準，則可以

從ONTAP系統管理員、 ONTAP CLI 或 API 修改儲存虛擬機器的名稱。例如，您可能希望該名稱與ONTAP叢集的儲存虛擬機器的命名方式相符。

管理 **AWS** 中**Cloud Volumes ONTAP**的資料服務儲存虛擬機

儲存虛擬機是在ONTAP內運作的虛擬機，可為您的用戶端提供儲存和資料服務。您可能知道這是一個_SVM_或_vserver_。 Cloud Volumes ONTAP預設配置一個儲存虛擬機，但某些配置支援額外的儲存虛擬機。

若要建立額外的資料服務儲存虛擬機，您需要在 AWS 中指派 IP 位址，然後根據您的Cloud Volumes ONTAP設定執行ONTAP命令。

支援的儲存虛擬機器數量

從 9.7 版本開始，特定的Cloud Volumes ONTAP配置支援多個儲存虛擬機器。前往 "Cloud Volumes ONTAP發行說明"驗證您的Cloud Volumes ONTAP版本支援的儲存虛擬機器數量。

所有其他Cloud Volumes ONTAP配置都支援一個資料服務儲存虛擬機器和一個用於災難復原的目標儲存虛擬機器。如果來源儲存虛擬機器發生中斷，您可以啟動目標儲存虛擬機器進行資料存取。

驗證配置的限制

每個 EC2 執行個體支援每個網路介面的最大私有 IPv4 位址數量。在 AWS 中為新的儲存虛擬機器指派 IP 位址之前，您需要驗證限制。

步驟

1. 去 "Cloud Volumes ONTAP發行說明中的儲存限制部分"。
2. 確定您的執行個體類型每個介面的最大 IP 位址數。
3. 記下這個號碼，因為在下一節中分配 AWS 中的 IP 位址時需要它。

在 **AWS** 中分配 **IP** 位址

在為新的儲存虛擬機器建立 LIF 之前，必須將私人 IPv4 位址指派給 AWS 中的連接埠 e0a。

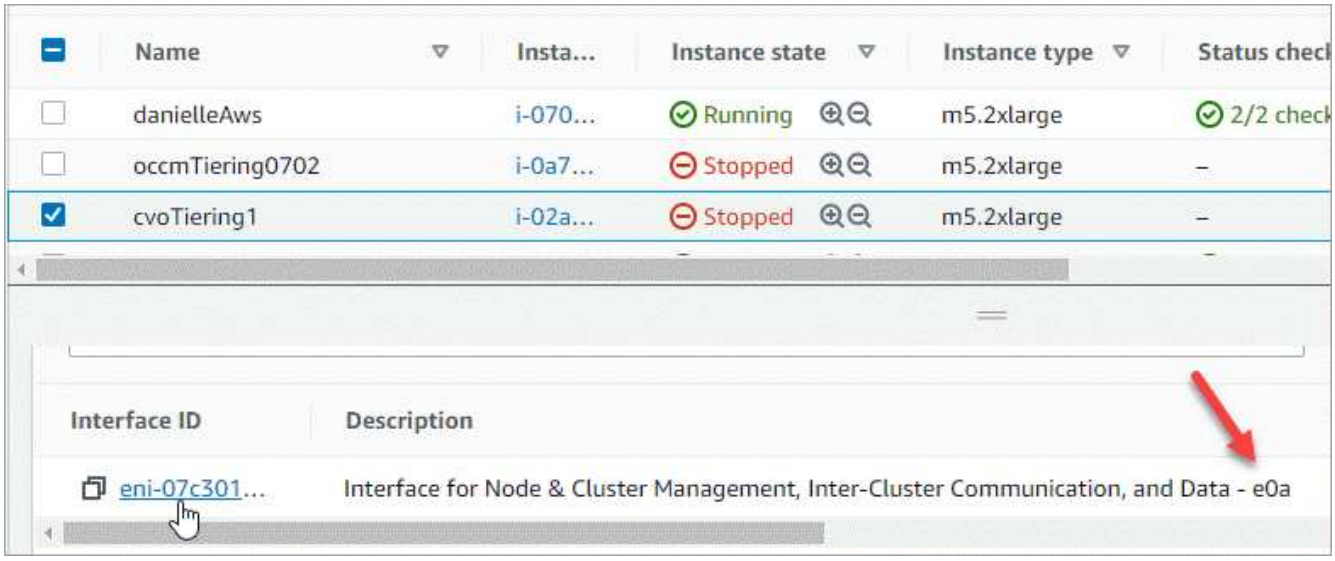
請注意，儲存虛擬機器的選用管理 LIF 需要在單節點系統和單一可用區（AZ）中的高可用性（HA）對上指派私人 IP 位址。此管理 LIF 提供與管理工具（例如 SnapCenter）的連結。

步驟

1. 登入AWS並開啟EC2服務。
2. 選擇Cloud Volumes ONTAP實例並點選 網路。

   如果您要在 HA 對上建立儲存虛擬機，請選擇節點 1。

3. 向下捲動至*網路介面*並點選連接埠 e0a 的*介面 ID*。



4. 選擇網路介面並點選*操作>管理 IP 位址*。
5. 展開 e0a 的 IP 位址清單。
6. 驗證 IP 位址：
   a. 計算已指派的 IP 位址數量，以確認連接埠是否有空間容納額外的 IP。

      您應該已經在本頁的上一節中確定了每個介面支援的最大 IP 位址數量。

   b. 可選：前往Cloud Volumes ONTAP的ONTAP CLI 並執行 **network interface show** 以確認每個 IP 位址都在使用中。

      如果 IP 位址未使用，那麼您可以將其與新的儲存 VM 一起使用。

7. 返回 AWS 控制台，按一下「指派新 IP 位址」以根據新儲存 VM 所需的數量指派其他 IP 位址。
   - 單節點系統：需要一個未使用的次要私有 IP。

     如果您想在儲存虛擬機器上建立管理 LIF，則需要選購的輔助私人 IP。

   - 單一 AZ 中的 HA 對：節點 1 上需要一個未使用的輔助私有 IP。

     如果您想在儲存虛擬機器上建立管理 LIF，則需要選購的輔助私人 IP。

   - 多個可用區中的 HA 對：每個節點都需要一個未使用的輔助私有 IP。
8. 如果您要在單一 AZ 中的 HA 對上指派 IP 位址，請啟用*允許重新指派輔助私有 IPv4 位址*。
9. 點選“儲存”。
10. 如果您在多個可用區中有一個 HA 對，則需要對節點 2 重複這些步驟。

在單節點系統上建立儲存 **VM**

這些步驟會在單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到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 上未使用的輔助私有 IP。

3. 可選：建立儲存虛擬機器管理 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_y* 是 e0a 上另一個未使用的輔助私有 IP。

4. 將一個或多個聚合分配給儲存虛擬機器。

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

此步驟是必需的，因為新的儲存虛擬機器需要存取至少一個聚合，然後您才能在儲存虛擬機器上建立磁碟區。

在單一可用區內的 **HA** 對上建立儲存虛擬機

這些步驟在單一 AZ 中的 HA 對上建立一個新的儲存虛擬機器。建立 NAS LIF 需要一個私人 IP 位址，如果要建立管理 LIF，則需要另一個可選的私人 IP 位址。

這兩個 LIF 都分配在節點 1 上。如果發生故障，私人 IP 位址可以在節點之間移動。

步驟

1. 建立儲存虛擬機器和到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-node1 的 e0a 上未使用的輔助私有 IP。在接管的情況下，該 IP 位址可以重新定位到 cvo-node2 的 e0a，因為服務策略 default-data-files 表示 IP 可以遷移到合作夥伴節點。

3. 選用：在節點 1 上建立儲存虛擬機器管理 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_y* 是 e0a 上另一個未使用的輔助私有 IP。

4. 將一個或多個聚合分配給儲存虛擬機器。

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

此步驟是必需的，因為新的儲存虛擬機器需要存取至少一個聚合，然後您才能在儲存虛擬機器上建立磁碟區。

5. 如果您使用的是Cloud Volumes ONTAP 9.11.1 或更高版本，請修改儲存虛擬機器的網路服務策略。

需要修改服務，因為它可以確保Cloud Volumes ONTAP可以使用 iSCSI LIF 進行出站管理連線。

```
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
```

在多個可用區的 **HA** 對上建立儲存虛擬機

這些步驟在多個 AZ 中的 HA 對上建立一個新的儲存虛擬機器。

對於 NAS LIF 來說，浮動 IP 位址是必需的，而對於管理 LIF 來說，浮動 IP 位址是可選的。這些浮動 IP 位址不需要您在 AWS 中指派私有 IP。相反，浮動 IP 會在 AWS 路由表中自動配置為指向相同 VPC 中特定節點的 ENI。

為了使浮動 IP 與ONTAP一起運作，必須在每個節點上的每個儲存虛擬機器上配置一個私人 IP 位址。這反映在以下步驟中，其中在節點 1 和節點 2 上建立 iSCSI LIF。

步驟

1. 建立儲存虛擬機器和到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
```

   - 浮動 IP 位址必須位於您部署 HA 配置的 AWS 區域中的所有 VPC 的 CIDR 區塊之外。 192.168.209.27 是一個範例浮動 IP 位址。"了解有關選擇浮動 IP 位址的更多信息" 。
   - `-service-policy default-data-files`表示 IP 可以遷移到夥伴節點。

3. 選用：在節點 1 上建立儲存虛擬機器管理 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 nodei1Mask -lif
ip_node1_iscsi_2 -home-node cvo-node1
```

   - 此 iSCSI LIF 需要支援儲存虛擬機器中浮動 IP 的 LIF 遷移。它不必是 iSCSI LIF，但不能配置為在節點之間遷移。
   - `-service-policy default-data-block`表示IP位址不會在節點之間遷移。
   - *private_ip* 是 cvo_node1 的 eth0 (e0a) 上未使用的輔助私有 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 需要支援儲存虛擬機器中浮動 IP 的 LIF 遷移。它不必是 iSCSI LIF，但不能配置為在節點

之間遷移。

- `-service-policy default-data-block`表示IP位址不會在節點之間遷移。
- *private_ip* 是 cvo_node2 的 eth0 (e0a) 上未使用的輔助私有 IP 位址。

6. 將一個或多個聚合分配給儲存虛擬機器。

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

此步驟是必需的，因為新的儲存虛擬機器需要存取至少一個聚合，然後您才能在儲存虛擬機器上建立磁碟區。

7. 如果您使用的是Cloud Volumes ONTAP 9.11.1 或更高版本，請修改儲存虛擬機器的網路服務策略。

需要修改服務，因為它可以確保Cloud Volumes ONTAP可以使用 iSCSI LIF 進行出站管理連線。

```
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 Azure 中管理Cloud Volumes ONTAP的資料服務儲存虛擬機

儲存虛擬機是在ONTAP內運作的虛擬機，可為您的用戶端提供儲存和資料服務。您可能知道這是一個_SVM_或_vserver_。 Cloud Volumes ONTAP預設為儲存虛擬機，但您可以在 Azure 中執行Cloud Volumes ONTAP時建立其他儲存虛擬機器。

若要在 Azure 中建立和管理其他資料服務儲存虛擬機，您應該使用 API。這是因為 API 自動化了建立儲存虛擬機器和配置所需網路介面的過程。建立儲存虛擬機器時， NetApp Console會配置所需的 LIF 服務，以及儲存虛擬機器出站 SMB/CIFS 通訊所需的 iSCSI LIF。

有關執行Cloud Volumes ONTAP API 呼叫的信息，請參閱 "您的第一次 API 呼叫"。

支援的儲存虛擬機器數量

從Cloud Volumes ONTAP 9.9.0 開始，根據您的許可證，支援具有特定配置的多個儲存虛擬機器。請參閱 "Cloud Volumes ONTAP發行說明"驗證您的Cloud Volumes ONTAP版本支援的儲存虛擬機器數量。

9.9.0 之前的所有Cloud Volumes ONTAP版本都支援一個資料服務儲存虛擬機器和一個用於災難復原的目標儲存虛擬機器。如果來源儲存虛擬機器發生中斷，您可以啟動目標儲存虛擬機器進行資料存取。

建立儲存虛擬機

根據您的設定和授權類型，您可以透過 NetApp Console 的 API，在單一節點系統或高可用性（HA）組態中建立多個儲存 VM。

關於此任務

當您使用 API 建立儲存虛擬機器並配置所需的網路介面時，控制台也會修改 `default-data-files`透過從 NAS 資料 LIF 中刪除以下服務並將其新增至用於出站管理連線的 iSCSI 資料 LIF，可以在資料儲存虛擬機器上實施策略：

- `data-fpolicy-client`
- `management-ad-client`
- `management-dns-client`
- `management-ldap-client`
- `management-nis-client`

開始之前

控制台代理程式需要特定權限才能為Cloud Volumes ONTAP建立儲存虛擬機器。所需權限包含在 "NetApp提供的政策"。

單節點系統

使用下列 API 呼叫在單節點系統上建立儲存 VM。

```
POST /azure/vsa/working-environments/{workingEnvironmentId}/svm
```

在請求主體中包含以下參數：

```
{ "svmName": "myNewSvm1"
   "svmPassword": "optional, the API takes the cluster password if not
provided"
   "mgmtLif": "optional, to create an additional management LIF, if you
want to use the storage VM for management purposes"}
```

HA 對

使用以下 API 呼叫在 HA 對上建立儲存虛擬機器：

```
POST /azure/ha/working-environments/{workingEnvironmentId}/svm
```

在請求主體中包含以下參數：

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
   "mgmtLif": "optional value, to create an additional management LIF, if
you want to use the storage VM for management purposes"}
```

管理單節點系統和 HA 配對上的儲存 VM

使用 API，您可以重新命名和刪除單節點和 HA 配置中的儲存虛擬機器。

開始之前

控制台代理程式需要特定權限來管理Cloud Volumes ONTAP 的儲存虛擬機器。所需權限包含在 "NetApp提供的政策"。

重新命名儲存虛擬機

若要重新命名儲存虛擬機，您應該提供現有儲存虛擬機和新儲存虛擬機的名稱作為參數。

步驟

- 使用下列 API 呼叫重新命名單節點系統上的儲存 VM：

  ```
  PUT /azure/vsa/working-environments/{workingEnvironmentId}/svm
  ```

  在請求主體中包含以下參數：

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

- 使用以下 API 呼叫重命名 HA 對上的儲存虛擬機器：

```
PUT /azure/ha/working-environments/{workingEnvironmentId}/svm
```

在請求主體中包含以下參數：

```
{
  "svmNewName": "NewSvmName",
  "svmName": "OldSvmName"
}
```

刪除儲存虛擬機

在單一節點或 HA 配置中，如果儲存虛擬機器沒有任何活動卷，則可以將其刪除。

步驟

- 使用以下 API 呼叫刪除單節點系統上的儲存 VM ：

  ```
  DELETE /azure/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}
  ```

- 使用以下 API 呼叫刪除 HA 對上的儲存虛擬機器：

  ```
  DELETE /azure/ha/working-environments/{workingEnvironmentId}/svm/{svmName}
  ```

相關資訊

- "準備使用 API"
- "Cloud Volumes ONTAP工作流程"
- "取得所需的標識符"
- "使用NetApp Console的 REST API"

在 Google Cloud 中管理Cloud Volumes ONTAP的資料服務儲存虛擬機

儲存虛擬機是在ONTAP內運作的虛擬機，可為您的用戶端提供儲存和資料服務。您可能知道這是一個_SVM_或_vserver_。 Cloud Volumes ONTAP預設配置一個儲存虛擬機，但某些配置支援額外的儲存虛擬機。

要在 Google Cloud 中建立和管理其他資料服務儲存虛擬機，您應該使用 API。這是因為 API 自動化了建立儲存虛擬機器和配置所需網路介面的過程。建立儲存虛擬機器時， NetApp Console會配置所需的 LIF 服務，以及儲存虛擬機器出站 SMB/CIFS 通訊所需的 iSCSI LIF。

有關執行Cloud Volumes ONTAP API 呼叫的信息，請參閱 "您的第一次 API 呼叫"。

支援的儲存虛擬機器數量

從Cloud Volumes ONTAP 9.11.1 開始，根據您的許可證，支援具有特定配置的多個儲存虛擬機器。請參閱 "Cloud Volumes ONTAP發行說明"驗證您的Cloud Volumes ONTAP版本支援的儲存虛擬機器數量。

9.11.1 之前的所有Cloud Volumes ONTAP版本都支援一個資料服務儲存虛擬機器和一個用於災難復原的目標儲

存虛擬機器。如果來源儲存虛擬機器發生中斷，您可以啟動目標儲存虛擬機器進行資料存取。

建立儲存虛擬機

根據您的組態和授權類型，您可以使用 API 在單節點系統或高可用性 （HA） 組態中建立多個儲存 VM。

關於此任務

當您使用 API 建立儲存虛擬機器並配置所需的網路介面時，控制台也會修改 `default-data-files`透過從 NAS 資料 LIF 中刪除以下服務並將其新增至用於出站管理連線的 iSCSI 資料 LIF，可以在資料儲存虛擬機器上實施策略：

- `data-fpolicy-client`
- `management-ad-client`
- `management-dns-client`
- `management-ldap-client`
- `management-nis-client`

開始之前

控制台代理程式需要特定權限才能為Cloud Volumes ONTAP HA 對建立儲存虛擬機器。所需的權限包含在... "NetApp提供的政策" 。

單節點系統

使用下列 API 呼叫在單節點系統上建立儲存 VM。

```
POST /gcp/vsa/working-environments/{workingEnvironmentId}/svm
```

在請求主體中包含以下參數：

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
   "mgmtLif": "optional value, to create an additional management LIF, if
you want to use the storage VM for management purposes"}
```

HA 對

使用以下 API 呼叫在 HA 對上建立儲存虛擬機器：

```
POST /gcp/ha/working-environments/{workingEnvironmentId}/svm/
```

在請求主體中包含以下參數：

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
}
```

管理儲存虛擬機

使用 API，您可以重新命名和刪除單節點和 HA 配置中的儲存虛擬機器。

開始之前

控制台代理程式需要特定權限來管理Cloud Volumes ONTAP HA 對的儲存虛擬機器。所需的權限包含在... "NetApp提供的政策" 。

重新命名儲存虛擬機

若要重新命名儲存虛擬機，您應該提供現有儲存虛擬機和新儲存虛擬機的名稱作為參數。

步驟

- 使用下列 API 呼叫重新命名單節點系統上的儲存 VM：

  `PUT /gcp/vsa/working-environments/{workingEnvironmentId}/svm`

  在請求主體中包含以下參數：

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

- 使用以下 API 呼叫重命名 HA 對上的儲存虛擬機器：

  `PUT /gcp/ha/working-environments/{workingEnvironmentId}/svm`

  在請求主體中包含以下參數：

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

刪除儲存虛擬機

在單一節點或 HA 配置中，如果儲存虛擬機器沒有任何活動卷，則可以將其刪除。

步驟

- 使用以下 API 呼叫刪除單節點系統上的儲存 VM ：

```
DELETE /gcp/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}
```

- 使用以下 API 呼叫刪除 HA 對上的儲存虛擬機器：

```
DELETE /gcp/ha/working-environments/{workingEnvironmentId}/svm/{svmName}
```

相關資訊

- "準備使用 API"
- "Cloud Volumes ONTAP工作流程"
- "取得所需的標識符"
- "使用NetApp Console的 REST API"

為Cloud Volumes ONTAP設定儲存虛擬機器災難復原

NetApp Console不提供儲存虛擬機器 (SVM) 災難復原的設定或編排支援。若要執行這些任務，請使用ONTAP System Manager 或ONTAP CLI。

如果要在兩個 Cloud Volumes ONTAP 系統之間設定 SnapMirror SVM 複製，則複製必須在兩個 HA 配對系統或兩個單節點系統之間進行。您無法在 HA 配對系統和單節點系統之間設定 SnapMirror SVM 複製。

有關ONTAP CLI 說明，請參閱以下文件。

- "SVM 災難復原準備快速指南"
- "SVM 災難復原快速指南"

安全性和資料加密

使用NetApp加密解決方案加密Cloud Volumes ONTAP上的捲

Cloud Volumes ONTAP支援NetApp磁碟區加密 (NVE) 和NetApp聚合加密 (NAE)。 NVE 和 NAE 是基於軟體的解決方案，可實現符合 FIPS 140-2 標準的捲靜態資料加密。"了解有關這些加密解決方案的更多信息" 。

NVE 和 NAE 均由外部金鑰管理器支援。

如果def::aws[] endif::aws[] 如果def::azure[] endif::azure[] 如果def::gcp[] endif::gcp[] 如果def::aws[] endif::aws[] 如果def::azure[] endif::azure[] 如果你::gcp[] defendiffcp[]

使用 AWS 金鑰管理服務管理Cloud Volumes ONTAP加密金鑰

您可以使用"AWS 的金鑰管理服務 (KMS)"在 AWS 部署的應用程式中保護您的ONTAP加密金鑰。

可以使用 CLI 或ONTAP REST API 啟用 AWS KMS 的金鑰管理。

使用 KMS 時，請注意預設使用資料 SVM 的 LIF 與雲端金鑰管理端點進行通訊。節點管理網路用於與 AWS 的身份驗證服務進行通訊。如果叢集網路配置不正確，叢集將無法正確利用金鑰管理服務。

開始之前

- Cloud Volumes ONTAP必須運作 9.12.0 或更高版本
- 您必須已安裝磁碟區加密 (VE) 許可證，並且
- 您必須已安裝多租用戶加密金鑰管理 (MTEKM) 授權。
- 您必須是叢集或 SVM 管理員
- 您必須擁有有效的 AWS 訂閱

您只能為資料 SVM 配置金鑰。

配置

AWS

1. 您必須創建一個"授予"用於管理加密的 IAM 角色將使用的 AWS KMS 金鑰。 IAM 角色必須包含允許以下操作的策略：
   - `DescribeKey`
   - `Encrypt`
   - `Decrypt`若要建立贈款，請參閱"AWS 文件"。
2. "為適當的 IAM 角色新增策略。"政策應該支持 `DescribeKey`， `Encrypt` ，和 `Decrypt`營運.

Cloud Volumes ONTAP

1. 切換到您的Cloud Volumes ONTAP環境。
2. 切換到進階權限等級：
   `set -privilege advanced`
3. 啟用 AWS 金鑰管理員：
   `security key-manager external aws enable -vserver` *`data_svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. 出現提示時，輸入金鑰。
5. 確認 AWS KMS 已正確配置：
   `security key-manager external aws show -vserver` *`svm_name`*

使用 **Azure Key Vault** 管理**Cloud Volumes ONTAP**加密金鑰

您可以使用 Azure Key Vault (AKV) 來保護 Azure 部署的應用程式中ONTAP加密金鑰。請參閱"Microsoft 文件"。

AKV 僅可用於保護資料 SVM 的NetApp磁碟區加密 (NVE) 金鑰。欲了解更多信息，請參閱"ONTAP文檔" 。

可以使用 CLI 或ONTAP REST API 啟用 AKV 金鑰管理。

使用 AKV 時，請注意預設使用資料 SVM LIF 與雲端金鑰管理端點通訊。節點管理網路用於與雲端提供者的身份驗證服務（login.microsoftonline.com）進行通訊。如果叢集網路配置不正確，叢集將無法正確利用金鑰管理服

務。

開始之前

- Cloud Volumes ONTAP必須運作 9.10.1 或更高版本
- 已安裝磁碟區加密 (VE) 授權（NetApp磁碟區加密許可證會自動安裝在每個在NetApp支援中註冊的Cloud Volumes ONTAP系統上）
- 您必須擁有多租戶加密金鑰管理 (MT_EK_MGMT) 許可證
- 您必須是叢集或 SVM 管理員
- 有效的 Azure 訂閱

限制

- AKV 只能在資料 SVM 上配置
- NAE 不能與 AKV 一起使用。 NAE 需要外部支援的 KMIP 伺服器。
- Cloud Volumes ONTAP節點每 15 分鐘輪詢一次 AKV，以確認可存取性和金鑰可用性。此輪詢週期是不可設定的，並且在輪詢嘗試連續四次失敗後（總共 1 小時），磁碟區將處於離線狀態。

配置過程

概述的步驟擷取如何向 Azure 註冊您的Cloud Volumes ONTAP配置以及如何建立 Azure Key Vault 和金鑰。如果您已經完成這些步驟，請確保您具有正確的配置設置，特別是在建立 Azure Key Vault，然後繼續Cloud Volumes ONTAP配置。

- 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）
- Cloud Volumes ONTAP配置

Azure 應用程式註冊

1. 您必須先在 Azure 訂閱中註冊您希望Cloud Volumes ONTAP用於存取 Azure Key Vault 的應用程式。在 Azure 入口網站中，選擇套用註冊。
2. 選擇新註冊。
3. 為您的應用程式提供名稱並選擇支援的應用程式類型。預設的單一租戶足以滿足 Azure Key Vault 的使用。選擇註冊。
4. 在 Azure 概覽視窗中，選擇已註冊的應用程式。將應用程式（客戶端）**ID**和目錄（租用戶）**ID**複製到安全位置。在稍後的註冊過程中將需要它們。

建立 **Azure** 用戶端機密

1. 在 Azure Key Vault 應用程式註冊的 Azure 入口網站中，選擇「憑證和機密」窗格。
2. 選擇新客戶端密鑰。為您的客戶端密鑰輸入一個有意義的名稱。 NetApp建議的有效期限為 24 個月；但是，您的特定雲端治理策略可能需要不同的設定。
3. 按一下新增以建立客戶端金鑰。複製值列中列出的秘密字串，並將其儲存在安全的位置，以便稍後使

用Cloud Volumes ONTAP配置。當您離開該頁面後，秘密值將不再顯示。

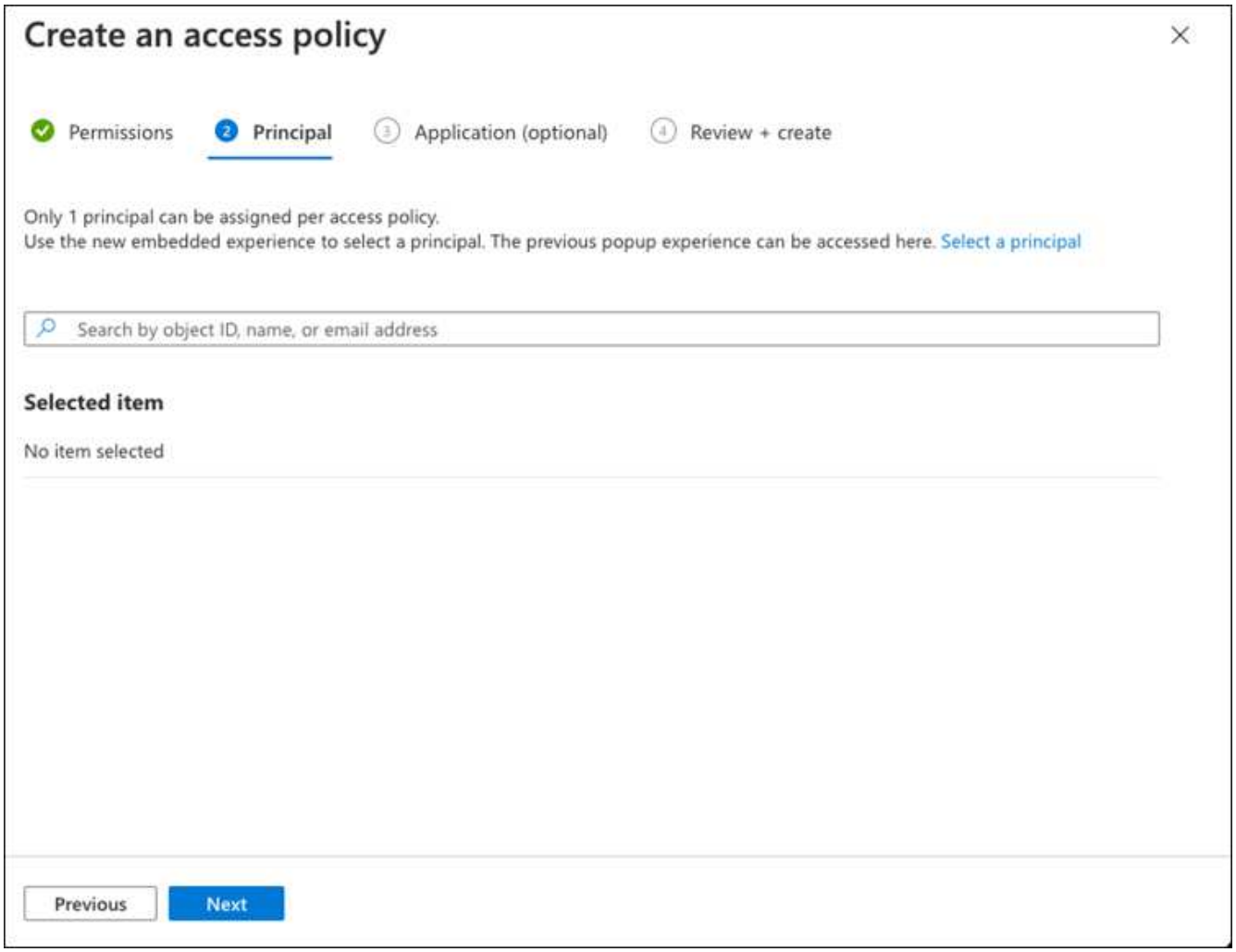
建立 **Azure Key Vault**

1. 如果您有現有的 Azure Key Vault，則可以將其連接到Cloud Volumes ONTAP配置；但是，您必須根據此過程中的設定調整存取原則。
2. 在 Azure 入口網站中，導覽至 **Key Vaults** 部分。
3. 點擊「+建立」並輸入所需信息，包括資源組、區域和定價層。此外，輸入保留已刪除保管庫的天數，並在金鑰保管庫上選擇啟用清除保護。
4. 選擇下一步來選擇存取策略。
5. 選擇以下選項：
   a. 在存取配置下，選擇**Vault** 訪問策略。
   b. 在資源存取下，選擇**Azure** 磁碟加密進行磁碟區加密。
6. 選擇“+建立”以新增存取策略。
7. 在從範本配置下，按一下下拉式選單，然後選擇金鑰、機密和憑證管理範本。
8. 選擇每個下拉權限選單（金鑰、秘密、憑證），然後在選單清單頂部選擇全選以選擇所有可用的權限。您應該：
   - 關鍵權限：已選擇 20 個
   - 秘密權限：已選擇 8 個
   - 憑證權限：已選擇 16 個


Create an access policy
1 Permissions
2 Principal
3 Application (optional)
4 Review + create
Configure from a template
Key, Secret, & Certificate Management
Key permissions
Key Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Cryptographic Operations
Select all
Decrypt
Encrypt
Unwrap Key
Wrap Key
Verify
Sign
Privileged Key Operations
Select all
Purge
Release
Rotation Policy Operations
Select all
Rotate
Get Rotation Policy
Set Rotation Policy
Secret permissions
Secret Management Operations
Select all
Get
List
Set
Delete
Recover
Backup
Restore
Privileged Secret Operations
Select all
Purge
Certificate permissions
Certificate Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Manage Contacts
Manage Certificate Authorities
Get Certificate Authorities
List Certificate Authorities
Set Certificate Authorities
Delete Certificate Authorities
Privileged Certificate Operations
Select all
Purge
Previous
Next

9. 按一下下一步，選擇您在 Azure 中建立的主體註冊應用程式Azure 應用程式註冊。選擇下一步。

   每個策略只能分配一個主體。



10. 按一下下一步兩次，直到到達審核並建立。然後，按一下建立。
11. 選擇下一步進入網路選項。
12. 選擇適當的網路存取方法或選擇所有網路和檢視 **+** 建立來建立金鑰保管庫。 （網路存取方法可能由治理策略或您的企業雲端安全團隊規定。）
13. 記錄金鑰保管庫 URI：在您建立的金鑰保管庫中，導覽至概覽功能表並從右側列複製**Vault URI**。您需要它來完成後面的步驟。

建立加密金鑰

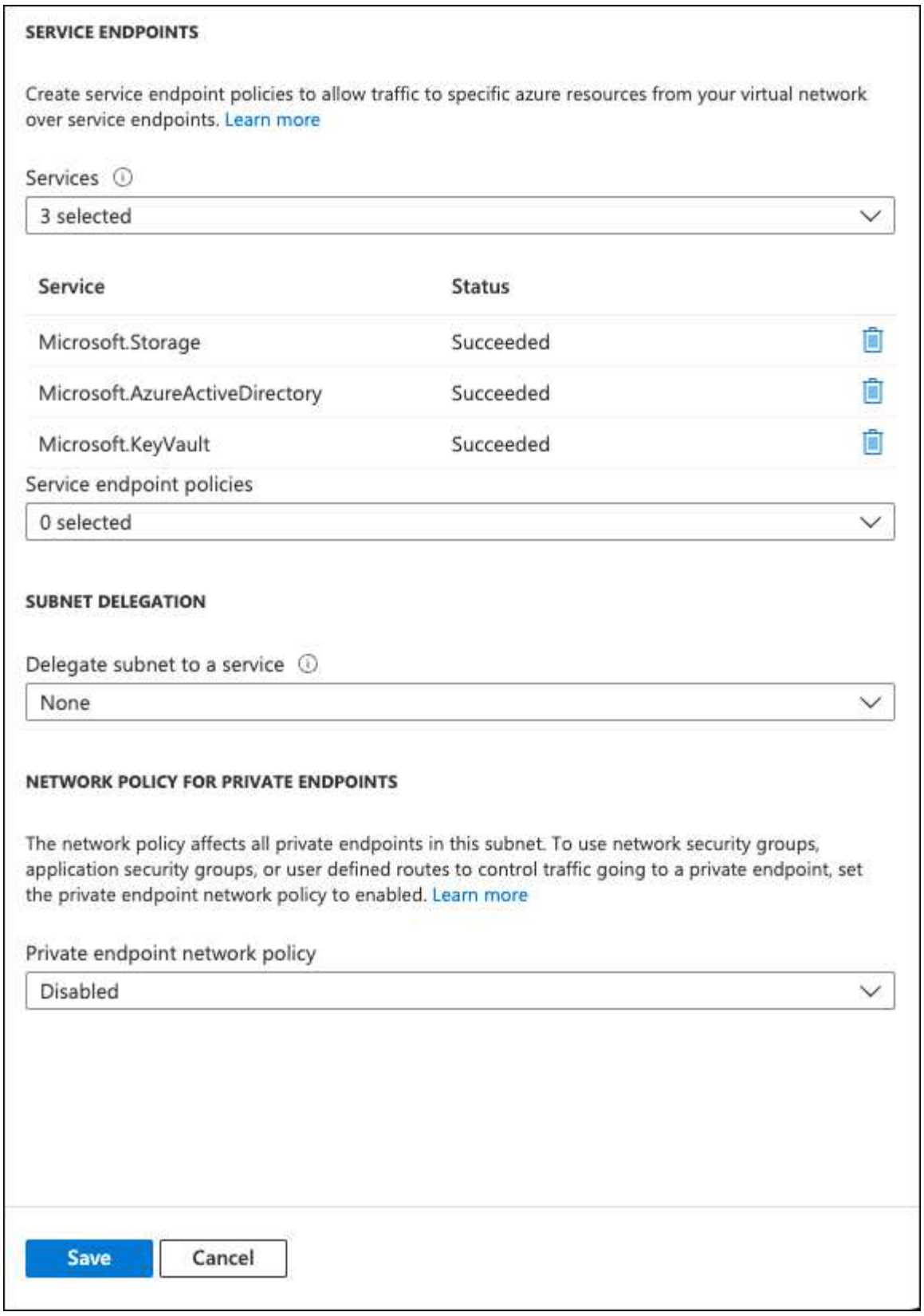
1. 在您為Cloud Volumes ONTAP建立的 Key Vault 選單中，導覽至 **Keys** 選項。
2. 選擇產生/導入來建立新金鑰。
3. 將預設選項設定為生成。
4. 提供以下資訊：
   - 加密金鑰名稱

- 金鑰類型：RSA
- RSA金鑰大小：2048
- 已啟用：是

5. 選擇建立來建立加密金鑰。
6. 返回**Keys**選單並選擇您剛剛建立的密鑰。
7. 選擇目前版本下的金鑰ID，查看金鑰屬性。
8. 找到密鑰標識符欄位。複製 URI，直到但不包括十六進位字串。

建立 **Azure Active Directory** 端點（僅限 **HA**）

1. 僅當您為 HA Cloud Volumes ONTAP系統設定 Azure Key Vault 時才需要此程序。
2. 在 Azure 入口網站中導覽至虛擬網路。
3. 選擇部署Cloud Volumes ONTAP系統的虛擬網絡，然後選擇頁面左側的子網選單。
4. 從清單中選擇Cloud Volumes ONTAP部署的子網路名稱。
5. 導航至服務端點標題。在下拉式選單中，選擇以下內容：
   - **Microsoft.AzureActiveDirectory**
   - **Microsoft.KeyVault**
   - **Microsoft.Storage**（可選）



6. 選擇儲存來捕獲您的設定。

Cloud Volumes ONTAP配置

1. 使用您首選的 SSH 用戶端連線到叢集管理 LIF。
2. 在ONTAP中進入進階權限模式：

```
set advanced -con off
```

3. 確定所需的資料 SVM 並驗證其 DNS 配置：
`vserver services name-service dns show`

   a. 如果所需資料 SVM 的 DNS 項目存在且包含 Azure DNS 項目，則無需執行任何操作。如果沒有，請為資料 SVM 新增指向 Azure DNS、私人 DNS 或本機伺服器的 DNS 伺服器項目。這應該與叢集管理員 SVM 的條目相符：
   `vserver services name-service dns create -vserver SVM_name -domains domain -name-servers IP_address`

   b. 驗證已為資料 SVM 建立 DNS 服務：
   `vserver services name-service dns show`

4. 使用應用程式註冊後儲存的用戶端 ID 和租用戶 ID 啟用 Azure Key Vault：
`security key-manager external azure enable -vserver SVM_name -client-id Azure_client_ID -tenant-id Azure_tenant_ID -name key_vault_URI -key-id full_key_URI`

   這 `_full_key_URI`價值必須利用 `<https:// <key vault host name>/keys/<key label>`格式。

5. 成功啟用 Azure Key Vault 後，輸入 `client secret value`當出現提示時。

6. 檢查密鑰管理器的狀態：
`security key-manager external azure check`輸出將如下所示：

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

Vserver: data_svm_name
Node: akvlab01-01

Category: service_reachability
    Status: OK

Category: ekmip_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 `service_reachability`狀態不是 `OK`，SVM 無法透過所有必要的連線和權限存取 Azure Key Vault 服務。確保您的 Azure 網路策略和路由不會阻止您的私人 vNet 到達 Azure Key Vault 公共終端點。如果確實如此，請考慮使用 Azure Private 端點從 vNet 內部存取 Key Vault。您可能還需要在 SVM 上新增靜態主機條目來解析端點的私人 IP 位址。

這 `kms_wrapped_key_status`將會報告 `UNKNOWN`在初始配置時。其狀態將變為 `OK`第一卷加密後。

7. 可選：建立測試卷以驗證 NVE 的功能。

   ```
   vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size
   -state online -policy default
   ```

   如果配置正確， Cloud Volumes ONTAP將自動建立磁碟區並啟用磁碟區加密。

8. 確認卷已正確建立並加密。如果是的話， `-is-encrypted`參數將顯示為 `true`。
   ```
   vol show -vserver SVM_name -fields is-encrypted
   ```
9. 可選：如果要更新 Azure Key Vault 驗證憑證上的憑證，請使用下列命令：
   ```
   security key-manager external azure update-credentials -vserver v1
   -authentication-method certificate
   ```

相關連結

- "設定Cloud Volumes ONTAP以在 Azure 中使用客戶管理的金鑰"
- "Microsoft Azure 文件：關於 Azure Key Vault"
- "ONTAP指令參考指南"

使用 Google Cloud KMS 管理Cloud Volumes ONTAP加密金鑰

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

可以使用ONTAP CLI 或ONTAP REST API 啟用 Cloud KMS 的金鑰管理。

使用 Cloud KMS 時，請注意預設使用資料 SVM 的 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提供者的身份驗證服務（oauth2.googleapis.com）進行通訊。如果叢集網路配置不正確，叢集將無法正確利用金鑰管理服務。

開始之前

- 您的系統應該執行Cloud Volumes ONTAP 9.10.1 或更高版本
- 您必須使用資料 SVM。 Cloud KMS 只能在資料 SVM 上配置。
- 您必須是叢集或 SVM 管理員
- 應在 SVM 上安裝磁碟區加密 (VE) 許可證
- 從Cloud Volumes ONTAP 9.12.1 GA 開始，也應安裝多租用戶加密金鑰管理 (MTEKM) 許可證
- 需要有效的 Google Cloud Platform 訂閱

配置

Google雲

1. 在您的 Google Cloud 環境中，"建立對稱 GCP 金鑰環和金鑰" 。
2. 為 Cloud KMS 金鑰和Cloud Volumes ONTAP服務帳戶指派自訂角色。
   a. 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.cryptoKeyVersio
ns.list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVer
sions.useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,clou
dkms.locations.get,cloudkms.locations.list,resourcemanager.projects.g
et
    --stage=GA
```

b. 指派您建立的自訂角色：
`gcloud kms keys add-iam-policy-binding *key_name* --keyring *key_ring_name* --location *key_location* --member serviceAccount:_service_account_Name_ --role projects/*customer_project_id*/roles/kmsCustomRole`

> 如果您使用的是Cloud Volumes ONTAP 9.13.0 或更高版本，則無需建立自訂角色。您可以指派預定義的[cloudkms.cryptoKeyEncrypterDecrypter^] 角色。

3. 下載服務帳戶 JSON 金鑰：
`gcloud iam service-accounts keys create key-file --iam-account=*sa-name*@*project-id*.iam.gserviceaccount.com`

Cloud Volumes ONTAP

1. 使用您首選的 SSH 用戶端連線到叢集管理 LIF。
2. 切換到進階權限等級：
`set -privilege advanced`
3. 為資料 SVM 建立 DNS。
`dns create -domains c.<*project*>.internal -name-servers *server_address* -vserver *SVM_name*`
4. 建立 CMEK 條目：
`security key-manager external gcp enable -vserver *SVM_name* -project-id *project* -key-ring-name *key_ring_name* -key-ring-location *key_ring_location* -key-name *key_name*`
5. 出現提示時，請輸入您的 GCP 帳戶中的服務帳戶 JSON 金鑰。
6. 確認啟用流程成功：
`security key-manager external gcp check -vserver *svm_name*`
7. 可選：建立磁碟區來測試加密 `vol create *volume_name* -aggregate *aggregate* -vserver *vserver_name* -size 10G`

故障排除

如果需要進行故障排除，您可以在上面的最後兩個步驟中追蹤原始 REST API 日誌：

1. `set d`
2. `systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2_client.log`

為Cloud Volumes ONTAP啟用NetApp勒索軟體防護解決方案

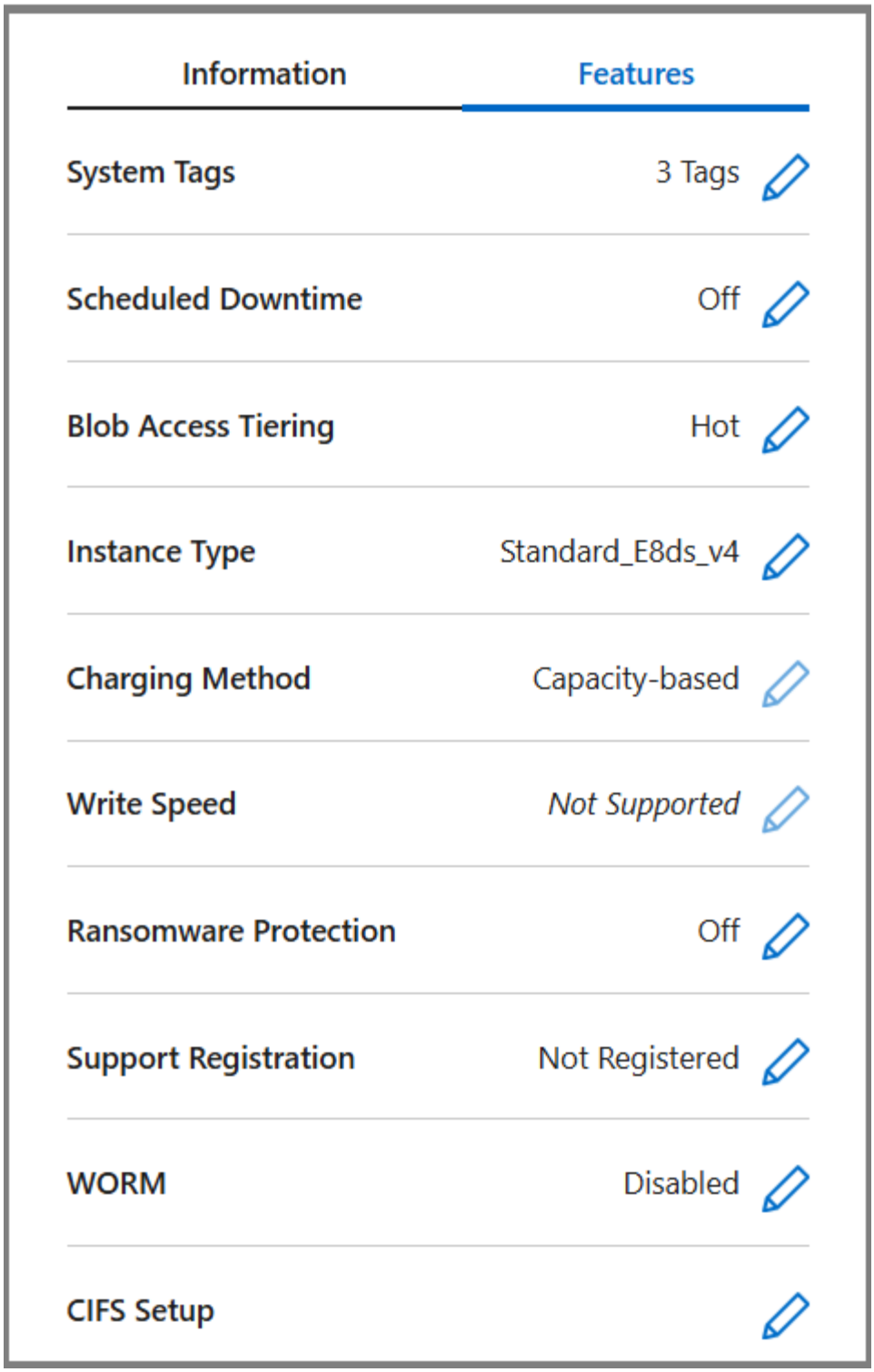
勒索軟體攻擊會浪費企業的時間、資源和聲譽。 NetApp Console可讓您實施兩種NetApp勒索軟體解決方案：針對共同勒索軟體檔案副檔名的防護和自主勒索軟體防護 (ARP)。這些解決方案為可見性、檢測和補救提供了有效的工具。

防禦常見勒索軟體檔案副檔名

控制台上的勒索軟體防護設定可讓您利用ONTAP FPolicy 功能來防禦常見的勒索軟體檔案擴充類型。

步驟

1. 在 **Systems** 頁面上，雙擊您配置為使用勒索軟體保護的Cloud Volumes ONTAP系統的名稱。
2. 在「概述」標籤上，按一下「功能」面板，然後按一下「勒索軟體防護」旁的鉛筆圖示。



3. 實施NetApp勒索軟體解決方案：

   a. 如果您的磁碟區未啟用快照策略，請按一下「啟動快照策略」。

      NetApp Snapshot 技術提供了業界最佳的勒索軟體補救解決方案。成功復原的關鍵是從未受感染的備份中復原。快照副本是唯讀的，可防止勒索軟體破壞。他們還可以提供創建單一文件副本或完整災難復原解決方案的圖像的粒度。

   b. 按一下「啟動 **FPolicy**」以啟用 ONTAP 的 FPolicy 解決方案，該解決方案可以根據檔案的副檔名阻止檔

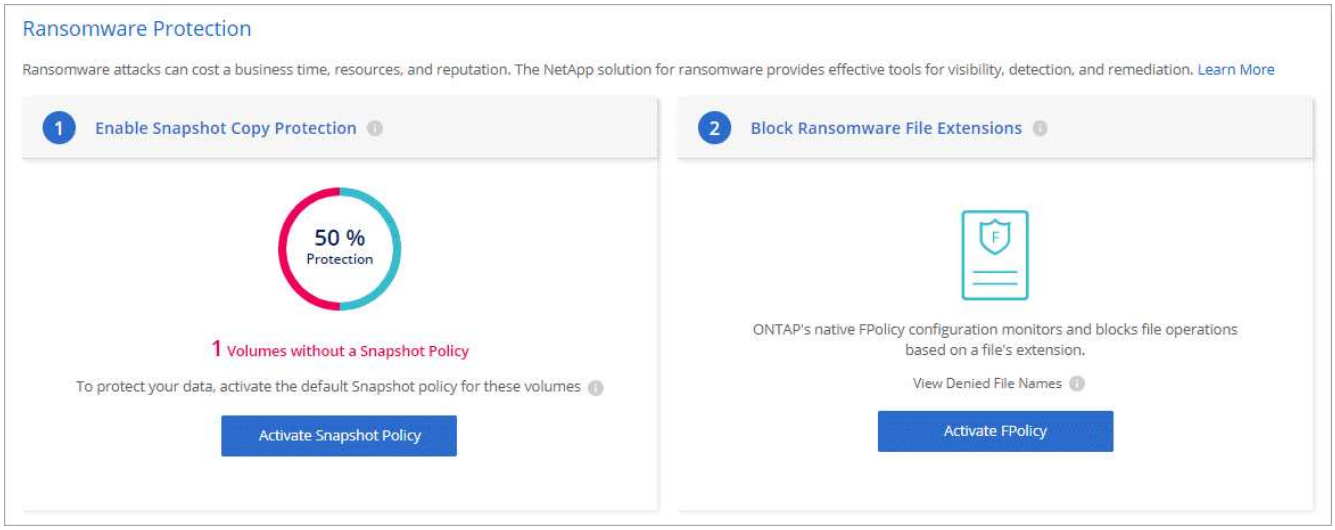
案操作。

此預防解決方案透過阻止常見的勒索軟體檔案類型來提高對勒索軟體攻擊的防護。

預設 FPolicy 範圍會封鎖具有下列副檔名的檔案：

micro、加密、鎖定、加密、crypt、crinf、r5a、XRNT、XTBL、R16M01D05、pzdc、好、哈哈！、OMG！ 、RDM、RRK、encryptedRS、crjoker、EnCiPhErEd、LeChiffre

當您在Cloud Volumes ONTAP上啟動 FPolicy 時，將會建立此範圍。此列表基於常見的勒索軟體檔案類型。您可以使用Cloud Volumes ONTAP CLI 中的 *vserver fpolicy policy scope* 指令自訂被封鎖的檔案副檔名。



自主勒索軟體防護

Cloud Volumes ONTAP支援自主勒索軟體防護 (ARP) 功能，可對工作負載進行分析，以主動偵測並警告可能表明勒索軟體攻擊的異常活動。

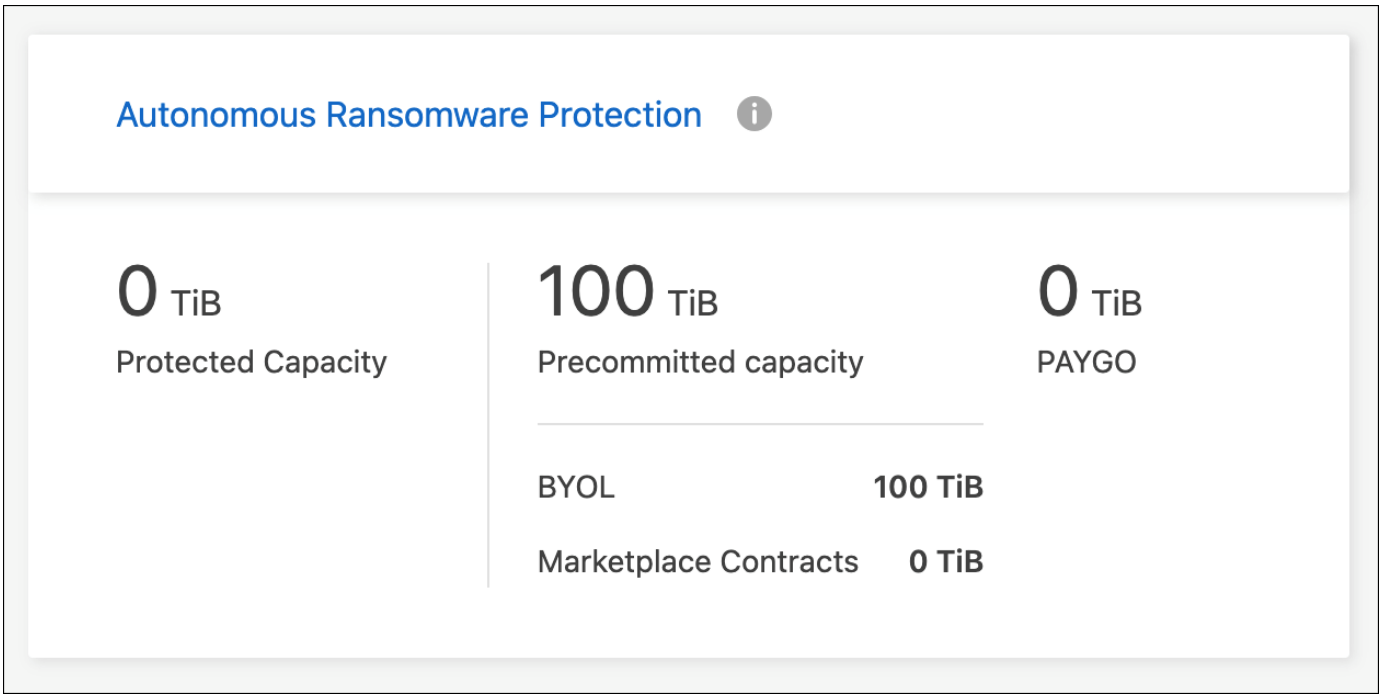
與透過以下方式提供的檔案副檔名保護分開 "勒索軟體防護設置"，ARP 功能使用工作負載分析根據偵測到的「異常活動」向使用者發出潛在攻擊警報。勒索軟體防護設定和 ARP 功能可以結合使用，以實現全面的勒索軟體防護。

ARP 功能可與自帶授權 (BYOL) 一起使用，且無需額外付費即可在市場訂閱您的授權。

啟用 ARP 的磁碟區具有指定狀態「學習模式」或「活動」 。

卷的 ARP 配置是透過ONTAP系統管理器和ONTAP CLI 執行的。

有關如何使用ONTAP System Manager 和ONTAP CLI 啟用 ARP 的更多信息，請參閱 "ONTAP文件：啟用自主勒索軟體防護"。



在Cloud Volumes ONTAP上建立 WORM 檔案的防篡改 Snapshot 副本

您可以在Cloud Volumes ONTAP系統上建立一次寫入、多次讀取 (WORM) 檔案的防篡改 Snapshot 副本，並在特定保留期內以未修改的形式保留快照。此功能由SnapLock技術提供支持，並提供了額外的資料保護和合規性層。

開始之前

確保用於建立 Snapshot 副本的磁碟區是SnapLock磁碟區。有關在卷上啟用SnapLock保護的信息，請參閱 "ONTAP文件：設定SnapLock"。

步驟

1. 從SnapLock磁碟區建立 Snapshot 副本。有關使用 CLI 或系統管理員建立 Snapshot 副本的信息，請參閱 "ONTAP文件：管理本機 Snapshot 副本概述"。

   Snapshot 副本繼承了磁碟區的 WORM 屬性，使其具有防篡改功能。底層的SnapLock技術可確保快照在指定的保留期結束之前受到保護，不會被編輯和刪除。

2. 如果需要編輯這些快照，您可以修改保留期。欲了解更多信息，請參閱 "ONTAP文檔：設定保留時間"。

> ⓘ 即使 Snapshot 副本在特定保留期內受到保護，叢集管理員也可以刪除來源磁碟區，因為Cloud Volumes ONTAP中的 WORM 儲存在「可信任儲存管理員」模型下執行。此外，受信任的雲端管理員可以透過操作雲端儲存資源來刪除WORM資料。

相關連結

- 有關 WORM 的更多信息，請參閱"了解Cloud Volumes ONTAP上的 WORM 存儲"。
- 有關SnapLock卷的充電信息，請參閱"Cloud Volumes ONTAP中的授權和計費"。

系統管理

升級Cloud Volumes ONTAP

從NetApp Console升級Cloud Volumes ONTAP以取得最新的功能和增強功能。在升級軟體之前，您應該準備好Cloud Volumes ONTAP系統。

升級概述

在開始Cloud Volumes ONTAP升級程序之前，您應該注意以下事項。

僅從控制台升級

您不應使用ONTAP系統管理員或ONTAP CLI 升級Cloud Volumes ONTAP ，而應僅使用控制台升級。否則可能會影響系統穩定性。

控制台提供了兩種升級Cloud Volumes ONTAP 的方法：

- 透過關注系統上出現的升級通知
- 透過將升級映像放置在 HTTPS 位置，然後向控制台提供 URL

支援的升級路徑

您可以升級到的 Cloud Volumes ONTAP 版本取決於您目前正在執行的版本。下表中每個發行版本的通用版本或修補程式版本代表可供升級的基本版本。有關可用修補程式的詳細資訊，請參閱每個發行版本的 "版本化發行說明"。

AWS 支援的升級路徑

目前版本	可直接升級到的版本
9.17.1 P1	9.18.1
9.16.1	9.17.1 P1
9.15.1	9.16.1
9.15.0	9.15.1
9.14.1	9.15.1
	9.15.0
9.14.0	9.14.1
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1
9.12.1	9.13.1
	9.13.0
9.12.0	9.12.1

目前版本	可直接升級到的版本
9.11.1	9.12.1
	9.12.0
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

Azure 支援的升級路徑

目前版本	可直接升級到的版本
9.17.1 P1	9.18.1
9.16.1 P3	9.17.1 P1
9.15.1 P10	9.16.1 P3
9.14.1 P13	9.15.1 P10
9.13.1 P16	9.14.1 P13
9.12.1 P18	9.13.1 P16
9.11.1 P20	9.12.1 P18

如果您在 Azure 中擁有較低版本的Cloud Volumes ONTAP ，則必須先升級到下一個版本，然後按照支援的升級路徑達到目標版本。例如，如果您有Cloud Volumes ONTAP 9.7 P7，請遵循下列升級路徑：

- 9.7 P7 → 9.8 P18
- 9.8 P18 → 9.9.1 P15

- 9.9.1 P15 → 9.10.1 P12
- 9.10.1 P12 → 9.11.1 P20

Google Cloud 支援的升級路徑

目前版本	可直接升級到的版本
9.17.1 P1	9.18.1
9.16.1	9.17.1 P1
9.15.1	9.16.1
9.15.0	9.15.1
9.14.1	9.15.1
	9.15.0
9.14.0	9.14.1
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1
9.12.1	9.13.1
	9.13.0
9.12.0	9.12.1
9.11.1	9.12.1
	9.12.0
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

目前版本	可直接升級到的版本
9.0	9.1
8.3	9.0

請注意以下事項：

- Cloud Volumes ONTAP支援的升級路徑與本機ONTAP叢集支援的升級路徑不同。
- 如果您按照系統中出現的通知進行升級，控制台將提示您升級到遵循這些支援的升級路徑的版本。
- 如果透過將升級映像放置在 HTTPS 位置來進行升級，請務必遵循這些支援的升級路徑。
- 在某些情況下，您可能需要升級幾次才能達到目標版本。

  例如，如果您正在執行版本 9.8 並且想要升級到 9.10.1，則首先需要升級到版本 9.9.1，然後再升級到 9.10.1。

補丁版本

從 2024 年 1 月開始，僅當Cloud Volumes ONTAP的三個最新版本發布補丁時才可進行補丁升級。當 RC 或 GA 版本無法部署時，偶爾會有修補程式版本可供部署。

我們使用最新的 GA 版本來確定要在控制台中顯示的最新版本。例如，如果目前 GA 版本是 9.13.1，則控制台中會出現 9.11.1-9.13.1 的補丁。

對於補丁版本 9.11.1 或更低版本，您需要使用手動升級程序下載ONTAP映像。

作為補丁版本的一般規則，您可以從較低的補丁版本升級到相同或下一個Cloud Volumes ONTAP版本中的任何較高補丁版本。

以下是幾個例子：

- 9.13.0 → 9.13.1 P15
- 9.12.1 → 9.13.1 P2

恢復或降級

不支援將Cloud Volumes ONTAP還原或降級到先前的版本。

支援註冊

必須在NetApp支援處註冊Cloud Volumes ONTAP才能使用本頁所述的任何方法升級軟體。這適用於現收現付（PAYGO）和自備授權（BYOL）。你需要"手動註冊PAYGO系統"，而 BYOL 系統是預設註冊的。

未註冊支援的系統仍會在有新版本可用時收到控制台中出現的軟體更新通知。但您需要先註冊系統才能升級軟體。

HA 調解器的升級

控制台也會在Cloud Volumes ONTAP升級過程中根據需求更新中介實例。

使用 **c4**、**m4** 和 **r4 EC2** 執行個體類型在 **AWS** 中進行升級

Cloud Volumes ONTAP不再支援 c4、m4 和 r4 EC2 執行個體類型。您可以使用這些實例類型將現有部署升級到Cloud Volumes ONTAP版本 9.8-9.12.1。在升級之前，我們建議您更改實例類型。如果您無法變更實例類型，則需要啟用增強連網升級之前。閱讀以下部分以了解有關變更實例類型和啟用增強連網的詳細資訊。

在執行 9.13.0 及更高版本的Cloud Volumes ONTAP中，您無法使用 c4、m4 和 r4 EC2 執行個體類型進行升級。在這種情況下，您需要減少磁碟數量，然後更改實例類型或部署具有 c5、m5 和 r5 EC2 執行個體類型的新 HA 對配置並遷移資料。

更改實例類型

c4、m4 和 r4 EC2 執行個體類型允許每個節點擁有比 c5、m5 和 r5 EC2 執行個體類型更多的磁碟。如果您正在執行的 c4、m4 或 r4 EC2 執行個體每個節點的磁碟數低於 c5、m5 和 r5 執行個體每個節點的最大磁碟限額，則可以將 EC2 執行個體類型變更為 c5、m5 或 r5。

"檢查 EC2 執行個體的磁碟和分層限制" "變更Cloud Volumes ONTAP的 EC2 執行個體類型"

如果您無法變更實例類型，請依照[啟用增強連網]。

啟用增強連網

若要升級至Cloud Volumes ONTAP 9.8 及更高版本，您必須在執行 c4、m4 或 r4 實例類型的叢集上啟用_增強網路_。若要啟用 ENA，請參閱知識庫文章"如何在 AWS Cloud Volumes ONTAP執行個體上啟用 SR-IOV 或 ENA 等增強網絡"。

準備升級

在執行升級之前，您必須驗證系統已準備就緒並進行任何必要的配置變更。

- [規劃停機時間]
- [驗證自動交還是否仍然啟用]
- 暫停SnapMirror傳輸
- [驗證聚合是否在線]
- 驗證所有 LIF 是否位於主端口

規劃停機時間

升級單節點系統時，升級過程會使系統離線最多 25 分鐘，在此期間 I/O 會中斷。

在許多情況下，升級 HA 對不會造成中斷，且 I/O 也不會中斷。在此無中斷升級過程中，每個節點都會同步升級，以繼續為客戶端提供 I/O 服務。

面向會話的協定在升級過程中可能會對某些區域的用戶端和應用程式造成不利影響。有關詳細信息，請參閱"ONTAP文檔"

驗證自動交還是否仍然啟用

必須在Cloud Volumes ONTAP HA 對上啟用自動交還（這是預設）。如果不是，則操作將會失敗。

"ONTAP文件：用於設定自動交還的命令"

暫停SnapMirror傳輸

如果Cloud Volumes ONTAP系統具有活動的SnapMirror關係，最好在更新Cloud Volumes ONTAP軟體之前暫停傳輸。暫停傳輸可防止SnapMirror故障。您必須暫停從目標系統的傳輸。

儘管NetApp Backup and Recovery使用SnapMirror的實作來建立備份檔案（稱為SnapMirror Cloud），但在系統升級時無需暫停備份。

關於此任務

以下步驟介紹如何使用ONTAP System Manager 9.3 及更高版本。

步驟

1. 從目標系統登入系統管理員。

   您可以透過將 Web 瀏覽器指向叢集管理 LIF 的 IP 位址來登入系統管理員。您可以在Cloud Volumes ONTAP系統中找到 IP 位址。

   您從中存取控制台的電腦必須具有與Cloud Volumes ONTAP 的網路連線。例如，您可能需要從雲端供應商網路中的跳轉主機登入控制台。

2. 點選*保護>關係*。
3. 選擇關係並點選*操作>靜默*。

驗證聚合是否在線

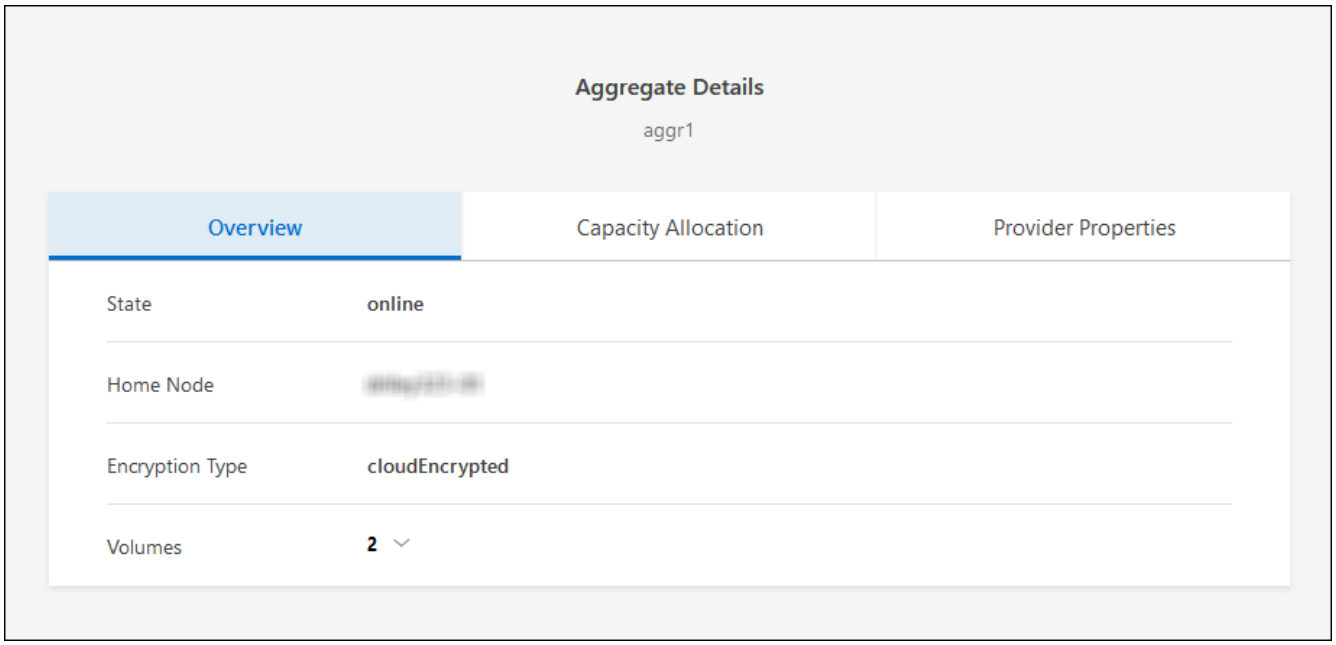
在更新軟體之前， Cloud Volumes ONTAP的聚合必須處於線上狀態。在大多數配置中，聚合應該處於線上狀態，但如果沒有，則應將其置於線上狀態。

關於此任務

以下步驟介紹如何使用ONTAP System Manager 9.3 及更高版本。

步驟

1. 在Cloud Volumes ONTAP系統上，按一下 **Aggregates** 標籤。
2. 在所需的聚合圖塊上，按一下 圖標，然後選擇*查看匯總詳情*。



3. 如果聚合處於離線狀態，請使用ONTAP系統管理員使聚合處於連線狀態：
   a. 按一下“儲存”>“聚合和磁碟”>“聚合”。
   b. 選擇聚合，然後按一下*更多操作>狀態>線上*。

驗證所有 **LIF** 是否位於主端口

升級前，所有 LIF 必須位於主連接埠上。請參閱ONTAP文檔"驗證所有 LIF 是否位於主端口"。

若發生升級失敗錯誤，請查閱知識庫 (KB) 文章"Cloud Volumes ONTAP升級失敗"。

升級Cloud Volumes ONTAP

當有新版本可供升級時，控制台會通知您。您可以從此通知開始升級程序。有關更多信息，請參閱[從控制台通知升級] 。

執行軟體升級的另一種方法是使用外部 URL 上的映像。如果控制台無法存取 S3 儲存桶來升級軟體或您獲得了補丁，則此選項很有用。有關更多信息，請參閱透過 URL 上的可用影像進行升級 。

從控制台通知升級

當有新版本的Cloud Volumes ONTAP Cloud Volumes ONTAP工作環境中顯示通知：

您必須擁有NetApp支援網站帳戶，然後才能透過通知升級Cloud Volumes ONTAP 。

您可以從此通知開始升級過程，該通知透過從 S3 儲存桶取得軟體映像、安裝映像，然後重新啟動系統來自動執行該過程。

開始之前

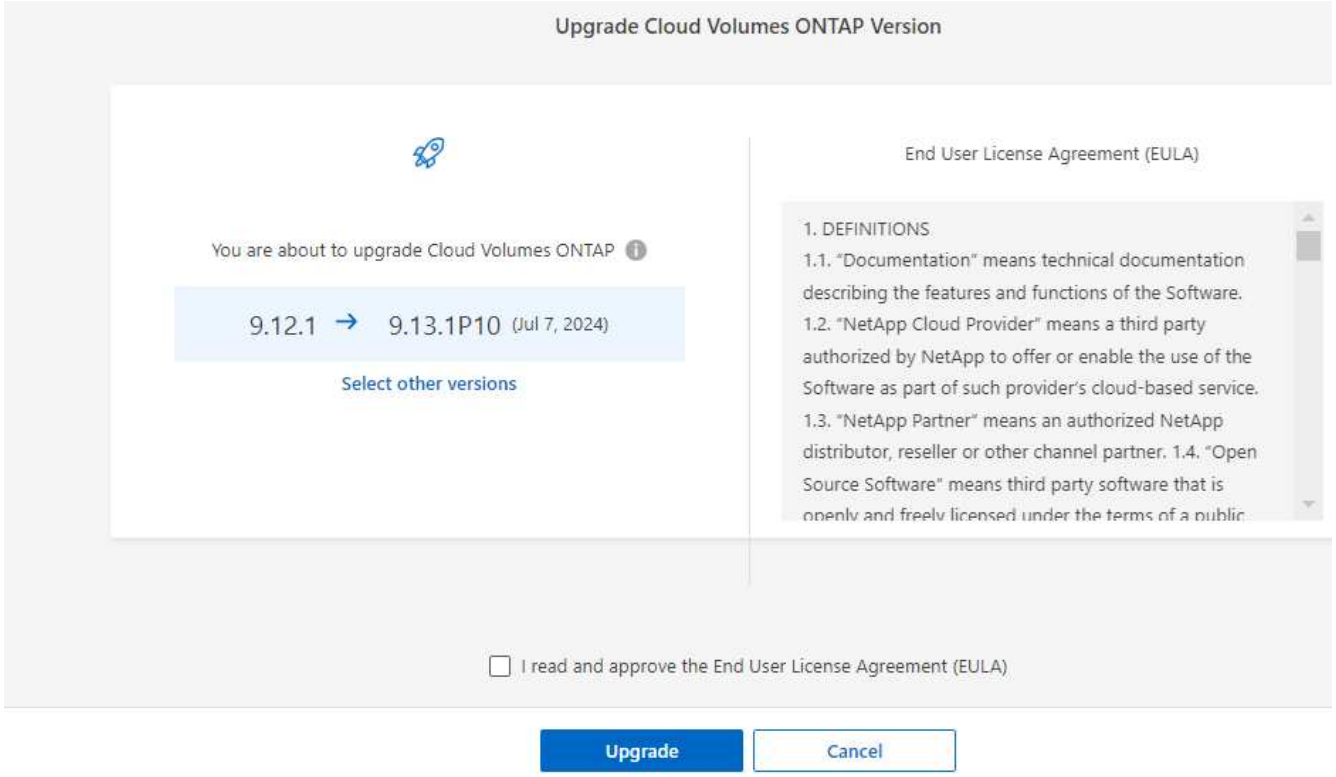
Cloud Volumes ONTAP系統上不得進行磁碟區或聚合建立等操作。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 選擇一個Cloud Volumes ONTAP系統。

   如果有新版本可用，概覽標籤中會出現通知：

3. 如果要升級已安裝的Cloud Volumes ONTAP版本，請按一下“立即升級！”預設情況下，您會看到最新的、相容的升級版本。

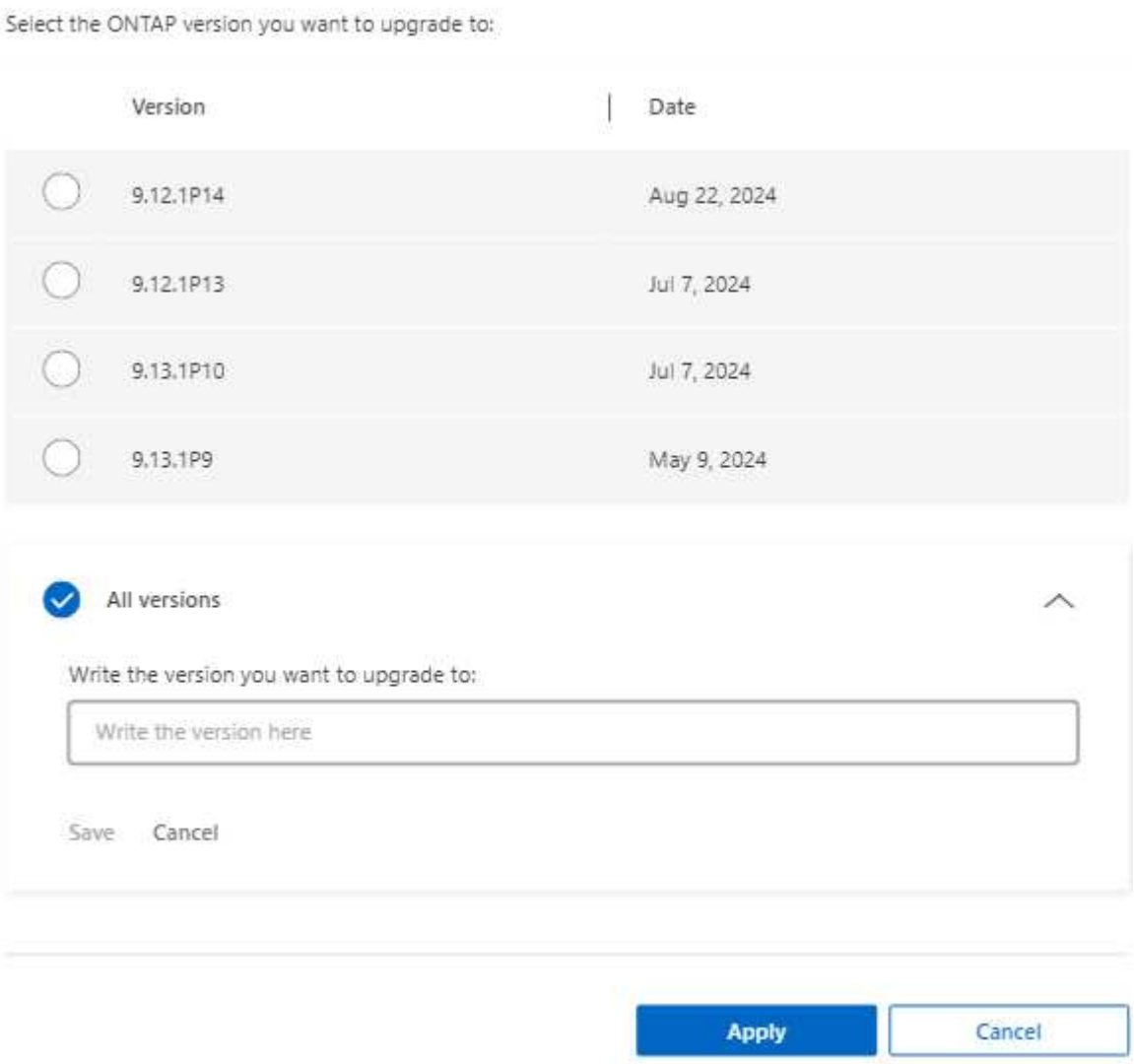


   若要升級到其他版本，請點選*選擇其他版本*。您會看到所列的最新Cloud Volumes ONTAP版本也與您系統上安裝的版本相容。例如，您的系統上安裝的版本是9.12.1P3，並且有以下相容版本可用：

   - 9.12.1P4 至 9.12.1P14
   - 9.13.1 和 9.13.1P1 您會看到 9.13.1P1 是升級的預設版本，而 9.12.1P13、9.13.1P14、9.13.1 和 9.13.1P1 是其他可用版本。

4. 或者，您可以按一下「所有版本」來輸入要升級到的另一個版本（例如，已安裝版本的下一個修補程式）。有關目前Cloud Volumes ONTAP版本的相容升級路徑，請參閱"支援的升級路徑"。

5. 按一下“儲存”，然後按一下“應用”



。

6. 在升級Cloud Volumes ONTAP頁面中，請閱讀 EULA，然後選擇 我已閱讀並同意 **EULA**。
7. 選擇*升級*。
8. 若要查看進度，請在Cloud Volumes ONTAP系統上選擇 **Audit**。

結果

控制台開始軟體升級。軟體更新完成後，您可以在系統上執行操作。

完成後

如果您暫停了SnapMirror傳輸，請使用系統管理員恢復傳輸。

透過 **URL** 上的可用影像進行升級

您可以將Cloud Volumes ONTAP軟體映像放在控制台代理程式或 HTTP 伺服器上，然後從控制台啟動軟體升級。如果控制台無法存取 S3 儲存桶來升級軟體，您可以使用此選項。

開始之前

- Cloud Volumes ONTAP系統上不得進行磁碟區或聚合建立等操作。

- 如果您使用 HTTPS 託管ONTAP映像，則升級可能會因缺少憑證而導致的 SSL 驗證問題而失敗。解決方法是產生並安裝 CA 簽署的證書，用於ONTAP和控制台之間的身份驗證。

  前往NetApp知識庫查看逐步說明：

  "NetApp KB：如何將控制台設定為 HTTPS 伺服器來託管升級映像"

步驟

1. 選用：設定可以託管Cloud Volumes ONTAP軟體映像的 HTTP 伺服器。

   如果您有與虛擬網路的 VPN 連接，則可以將Cloud Volumes ONTAP軟體映像放置在您自己網路中的 HTTP 伺服器上。否則，您必須將檔案放在雲端中的 HTTP 伺服器上。

2. 如果您對Cloud Volumes ONTAP使用自己的安全群組，請確保出站規則允許 HTTP 連接，以便Cloud Volumes ONTAP可以存取軟體映像。

   預先定義的Cloud Volumes ONTAP安全群組預設允許出站 HTTP 連線。

3. 從以下位置取得軟體映像 "NetApp支援站點"。
4. 將軟體映像複製到控制台代理或將提供該檔案的 HTTP 伺服器上的目錄中。

   有兩條路徑可用。正確的路徑取決於您的控制台代理版本。

   - `/opt/application/netapp/cloudmanager/docker_occm/data/ontap/images/`
   - `/opt/application/netapp/cloudmanager/ontap/images/`
5. 在系統上，按一下 ••• 圖標，然後點擊*更新Cloud Volumes ONTAP*。
6. 在更新Cloud Volumes ONTAP版本頁面上，輸入 URL，然後按一下 變更圖片。

   如果您將軟體映像複製到上面顯示的路徑中的控制台代理，則需要輸入以下 URL：

   http://<Console_agent_private-IP-address>/ontap/images/<映像檔名>

   在 URL 中，**image-file-name** 必須遵循「cot.image.9.13.1P2.tgz」格式。

7. 按一下“繼續”進行確認。

結果

控制台開始軟體更新。軟體更新完成後，您就可以在系統上執行操作。

完成後

如果您暫停了SnapMirror傳輸，請使用系統管理員恢復傳輸。

修復使用 **Google Cloud NAT** 閘道時下載失敗的問題

控制台代理程式會自動下載Cloud Volumes ONTAP 的軟體更新。如果您的設定使用 Google Cloud NAT 網關，下載可能會失敗。您可以透過限制軟體映像劃分的部分數來解決此問題。您必須使用 API 來完成此步驟。

步

1. 向 `/occm/`config 提交 PUT 請求，並將以下 JSON 作為正文：

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

maxDownloadSessions 的值可以是 1 或任何大於 1 的整數。如果值為1，則下載的影像不會被分割。

請注意，32 是一個範例值。您應該使用的值取決於您的 NAT 配置和您可以同時擁有的會話數。

"了解有關 /occm/config API 呼叫的更多信息" 。

註冊Cloud Volumes ONTAP即用即付系統

Cloud Volumes ONTAP即用即付 (PAYGO) 系統包含NetApp的支持，但您必須先透過向NetApp註冊系統來啟動支援。

需要向NetApp註冊 PAYGO 系統才能使用任何方法升級ONTAP軟體"本頁描述"。

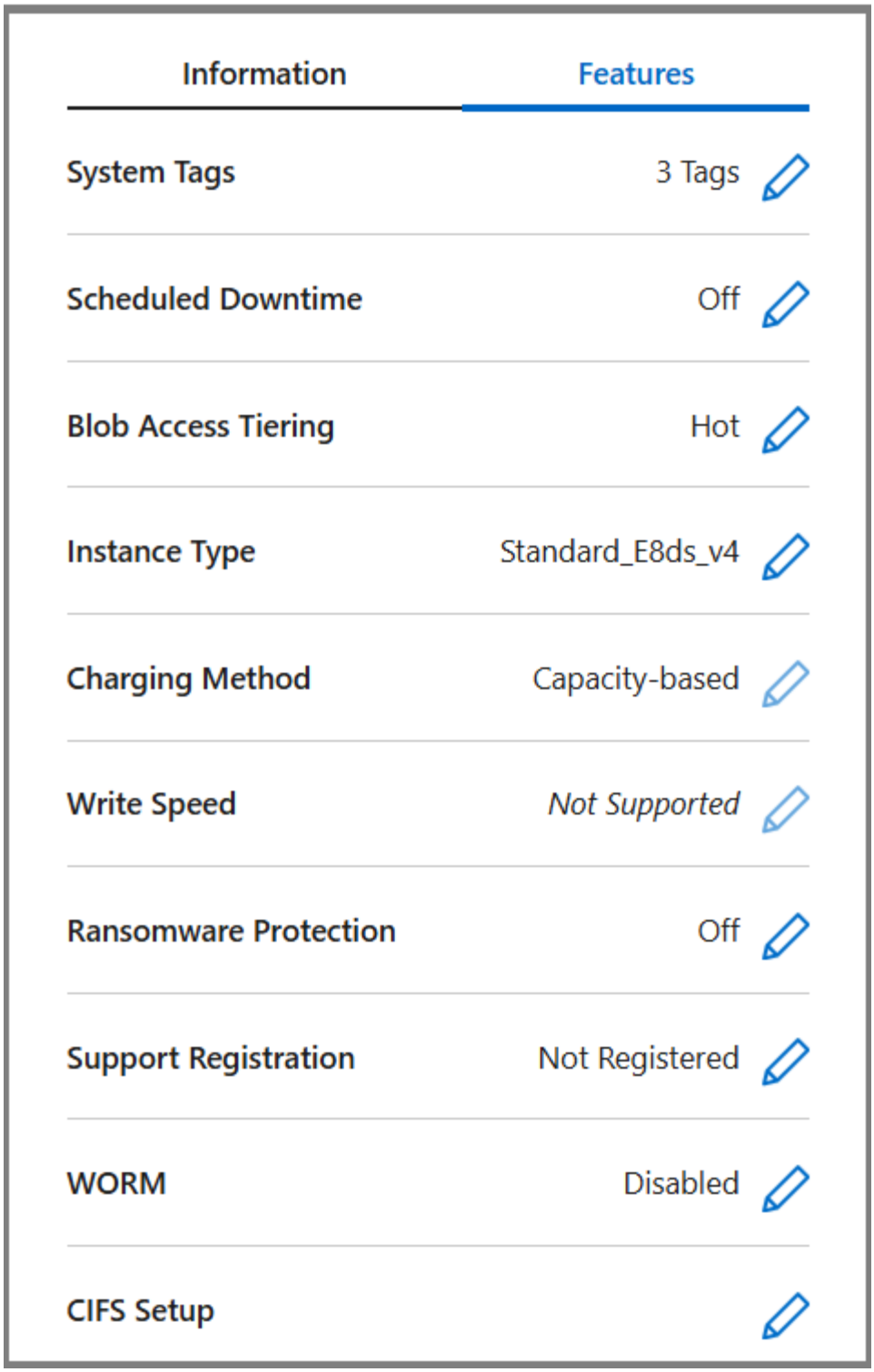
未註冊支援的系統仍會在有新版本可用時收到NetApp Console中顯示的軟體更新通知。但您需要先註冊系統才能升級軟體。

步驟

1. 如果您尚未將NetApp支援網站帳戶新增至控制台，請前往 帳戶設定 並立即新增。

   "了解如何新增NetApp支援網站帳戶" 。

2. 在「系統」頁面上，雙擊要註冊的系統的名稱。
3. 在「概述」標籤上，按一下「功能」面板，然後按一下「支援註冊」旁邊的鉛筆圖示。



4. 選擇NetApp支援網站帳號並點選「註冊」。

結果

該系統已在NetApp註冊。

將Cloud Volumes ONTAP基於節點的許可證轉換為基於容量的許可證

在基於節點的許可證的可用性終止 (EOA) 之後，您應該使用NetApp Console中的許可證轉

換工具過渡到基於容量的許可證。

對於年度或長期承諾， NetApp建議您在 EOA 日期（2024 年 11 月 11 日）或許可證到期日之前聯繫您的NetApp代表，以確保過渡的先決條件到位。如果您沒有Cloud Volumes ONTAP節點的長期合同，並且根據按需付費 (PAYGO) 訂閱運行您的系統，那麼在 2024 年 12 月 31 日支援終止 (EOS) 之前規劃您的轉換非常重要。在這兩種情況下，您都應確保您的系統符合要求，然後再使用NetApp Console中的許可證轉換工具實現無縫過渡。

有關 EOA 和 EOS 的信息，請參閱"基於節點的許可證的可用性終止"。

關於此任務

- 當您使用許可證轉換工具時，從基於節點到基於容量的許可模型的轉換是在現場線上進行的，從而無需進行任何資料遷移或配置額外的雲端資源。
- 它是一種無中斷操作，不會發生服務中斷或應用程式停機。
- Cloud Volumes ONTAP系統中的帳戶和應用程式資料保持不變。
- 轉換後，底層雲端資源不受影響。
- 許可證轉換工具支援所有部署類型，例如單節點、單可用區 (AZ) 中的高可用性 (HA)、多 AZ 中的 HA、自帶許可證 (BYOL) 和 PAYGO。
- 該工具支援所有基於節點的許可證作為來源，以及所有基於容量的許可證作為目標。例如，如果您擁有基於節點的 PAYGO 標準許可證，則可以將其轉換為透過市場購買的任何基於容量的許可證。 NetApp已限制 BYOL 授權的購買、延期和續約。有關更多信息，請參閱 "Cloud Volumes ONTAP的 BYOL 授權可用性受限" 。
- 所有雲端供應商、AWS、Azure 和 Google Cloud 都支援轉換。
- 轉換後，基於節點的許可證的序號將被基於容量的格式取代。這是轉換的一部分，並反映在您的NetApp支援網站 (NSS) 帳戶中。
- 當您過渡到基於容量的模型時，您的資料將繼續保留在與基於節點的許可相同的位置。這種方法保證了資料放置不會中斷，並在整個過渡過程中堅持資料主權原則。

開始之前

- 您應該擁有一個具有客戶存取權限或管理員存取權限的 NSS 帳戶。
- 您的 NSS 帳戶應使用您用於存取控制台的使用者憑證進行註冊。
- Cloud Volumes ONTAP系統應連結至具有客戶存取權限或管理員存取權限的 NSS 帳戶。
- 您應該擁有有效的基於容量的許可證，可以是 BYOL 許可證或市場訂閱。
- 您的帳戶中應該有基於容量的許可證。此授權可以是市場訂閱，也可以是控制台中 **Licenses and subscriptions** 下提供的 BYOL/私人優惠包。
- 在選擇目的地套餐之前，請先了解以下標準：
  - 如果帳戶具有基於容量的 BYOL 許可證，則所選目標包應與帳戶的 BYOL 基於容量的許可證保持一致：
    - 什麼時候 `Professional`被選為目標包，該帳戶應具有帶有專業包的 BYOL 許可證：
    - 什麼時候 `Essentials`被選為目標包，該帳戶應具有 Essentials 包的 BYOL 授權。
  - 如果目標套件與帳戶的 BYOL 授權可用性不一致，則表示基於容量的授權可能不包含所選套件。在這種情況下，我們將透過您的市場訂閱向您收費。
  - 如果沒有基於容量的 BYOL 授權而只有市場訂閱，則應確保所選包包含在基於容量的市場訂閱中。

- 如果您現有的基於容量的許可證中沒有足夠的容量，並且您有市場訂閱來對額外的容量使用收費，那麼您將透過市場訂閱為額外的容量付費。
- 如果您現有的基於容量的許可證中沒有足夠的容量，並且您沒有市場訂閱來收取額外容量使用的費用，則無法進行轉換。您應該添加市場訂閱來收取額外容量或將可用容量擴展到您目前的授權。
- 如果目標套件與帳戶的 BYOL 授權可用性不一致，且您現有的基於容量的授權中沒有足夠的容量，那麼您將透過市場訂閱付費。

如果任何一項要求未滿足，則許可證轉換不會發生。在特定情況下，許可證可能會轉換，但不能使用。點擊資訊圖示以識別問題並採取糾正措施。

步驟

1. 在「系統」頁面上，雙擊要修改許可證類型的系統的名稱。
2. 在「概述」標籤上，按一下「功能」面板。
3. 檢查*充電方式*旁邊的鉛筆圖示。如果您的系統的充電方式是 `Node Based`，可轉換為按容量充電。

   如果您的Cloud Volumes ONTAP系統已按容量收費，或任何要求未滿足，則該圖示將被停用。

4. 在*將基於節點的許可證轉換為基於容量的許可證*螢幕上，驗證系統名稱和來源許可證詳細資訊。
5. 選擇轉換現有許可證的目標包：
   - 必需品。預設值為 `Essentials`。
   - 專業的
6. 如果您擁有 BYOL 許可證，則可以在轉換完成後選取核取方塊以從控制台中刪除基於節點的許可證。如果轉換仍在進行中，選取此核取方塊將不會從控制台中刪除授權。此選項不適用於市場訂閱。
7. 選取核取方塊以確認您了解變更的含義，然後按一下「繼續」。

完成後

查看新的許可證序號並在控制台的*Licenses and subscriptions*選單中驗證變更。

不同超標量中的定價

有關定價的詳細信息，請訪問 "NetApp Console網站"。

有關特定超標量中的私人優惠的信息，請寫信至：

- AWS - awspo@netapp.com
- Azure - azurepo@netapp.com
- Google Cloud - gcppo@netapp.com

啟動並停止Cloud Volumes ONTAP系統

您可以從NetApp Console停止並啟動Cloud Volumes ONTAP來管理您的雲端運算成本。

安排**Cloud Volumes ONTAP**自動關閉

您可能想要在特定時間間隔內關閉Cloud Volumes ONTAP以降低運算成本。您無需手動執行此操作，而是可以將控制台配置為在特定時間自動關閉然後重新啟動系統。

關於此任務

- 當您計劃自動關閉Cloud Volumes ONTAP系統時，如果正在進行活動資料傳輸，控制台會延遲關閉。

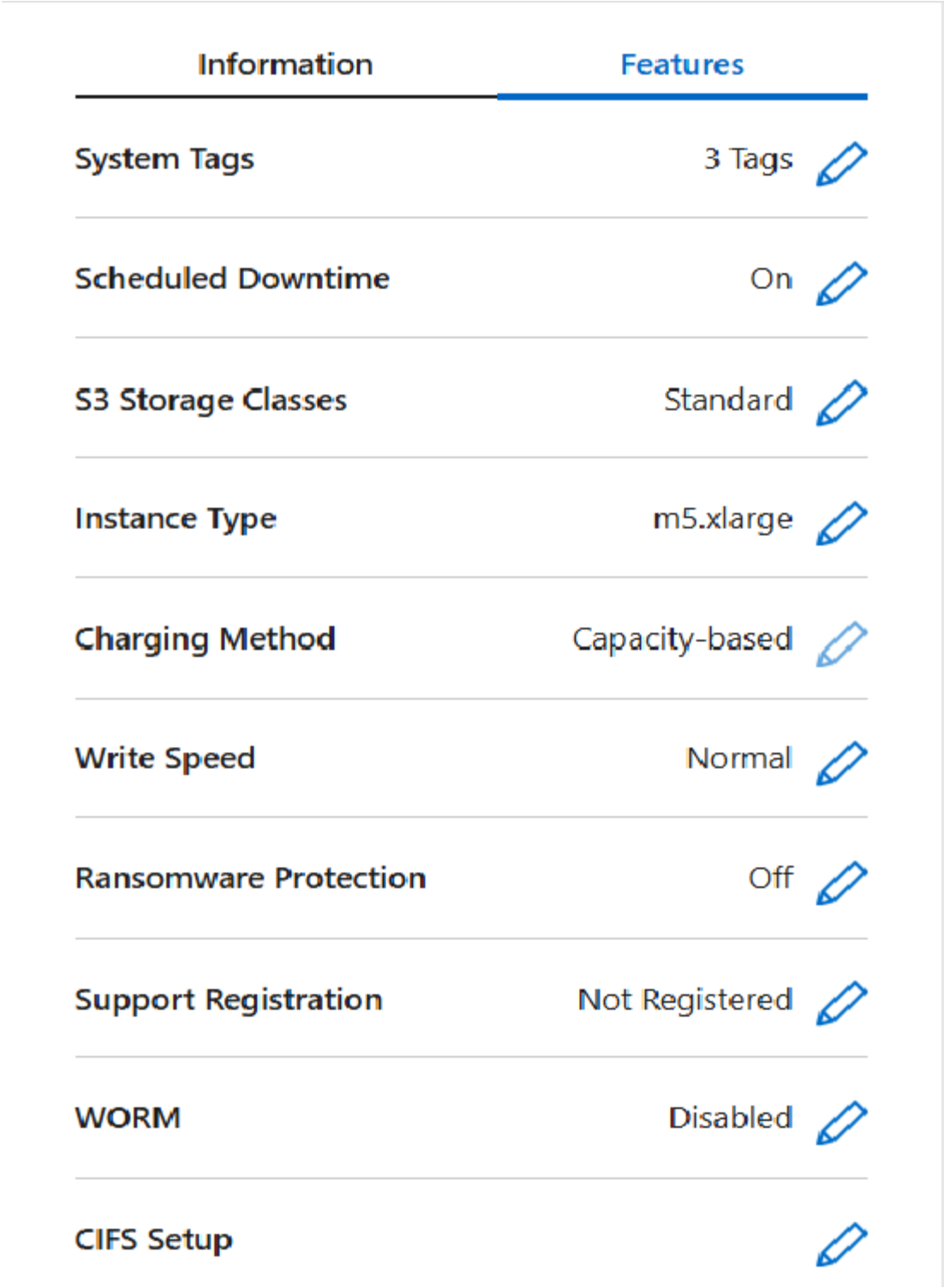
  傳輸完成後，系統將關閉。

- 此任務計劃會自動關閉 HA 對中的兩個節點。
- 透過排程關閉來關閉Cloud Volumes ONTAP時，不會建立啟動磁碟和根磁碟的快照。

  如下一節所述，只有在執行手動關機時才會自動建立快照。

步驟

1. 在*系統*頁面上，雙擊Cloud Volumes ONTAP系統。
2. 在「概覽」標籤上，按一下「功能」面板，然後按一下「規劃停機時間」旁的鉛筆圖示。



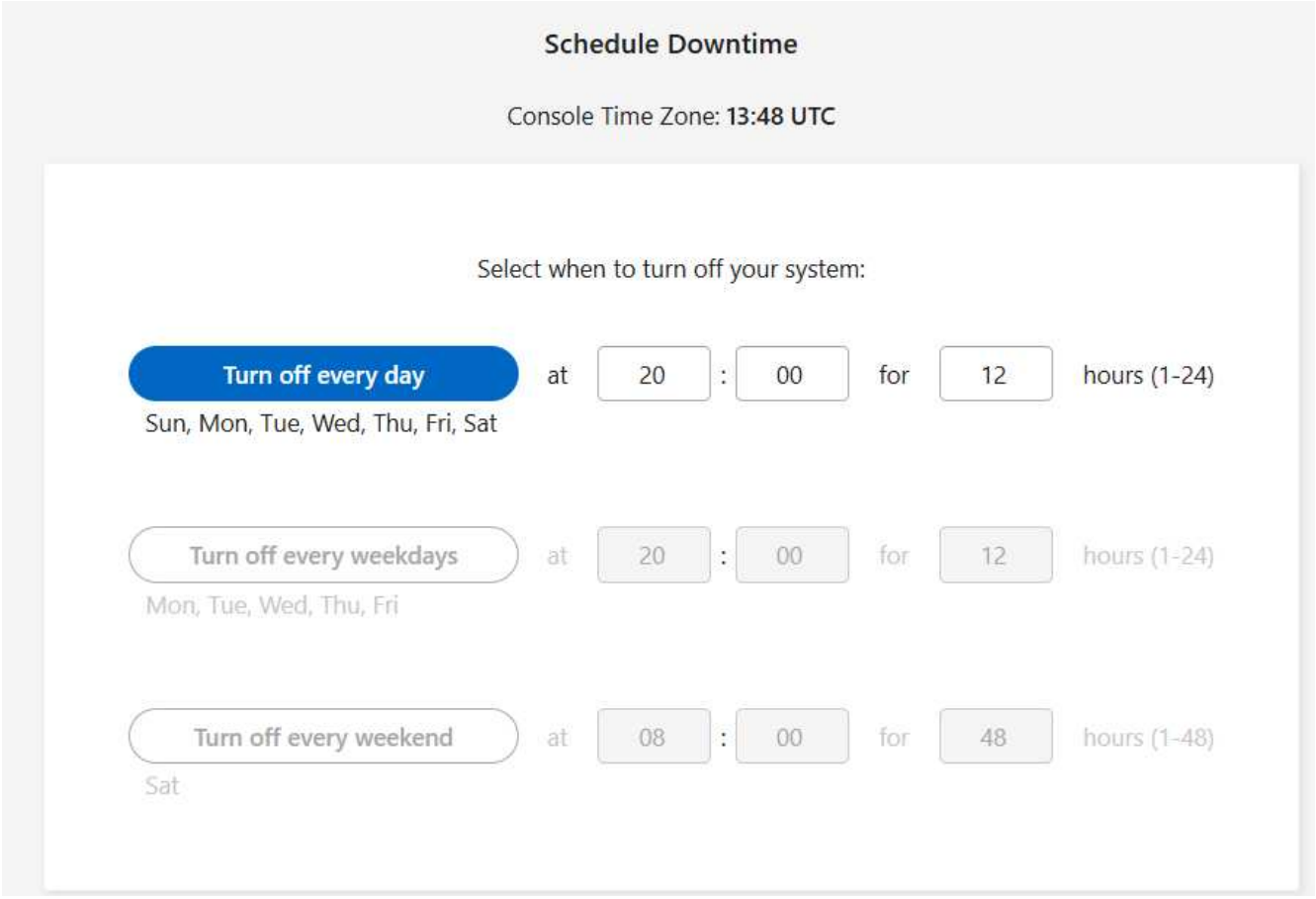
3. 指定關機計劃：

   a. 選擇是否每天、每個工作日、每個週末或這三個選項的任意組合關閉系統。

   b. 指定您想要關閉系統的時間以及關閉系統的時間長度。

      例子

      下圖顯示了一個時間表，指示控制台每週六晚上 20:00（晚上 8:00）關閉系統 12 小時。控制台每週一凌晨 12:00 重新啟動系統



4. 點選“儲存”。

結果

時間表已儲存。功能面板下對應的計劃停機時間行項目顯示「開啟」。

停止Cloud Volumes ONTAP

停止Cloud Volumes ONTAP可節省計算成本並建立根磁碟和啟動磁碟的快照，這有助於排除故障。

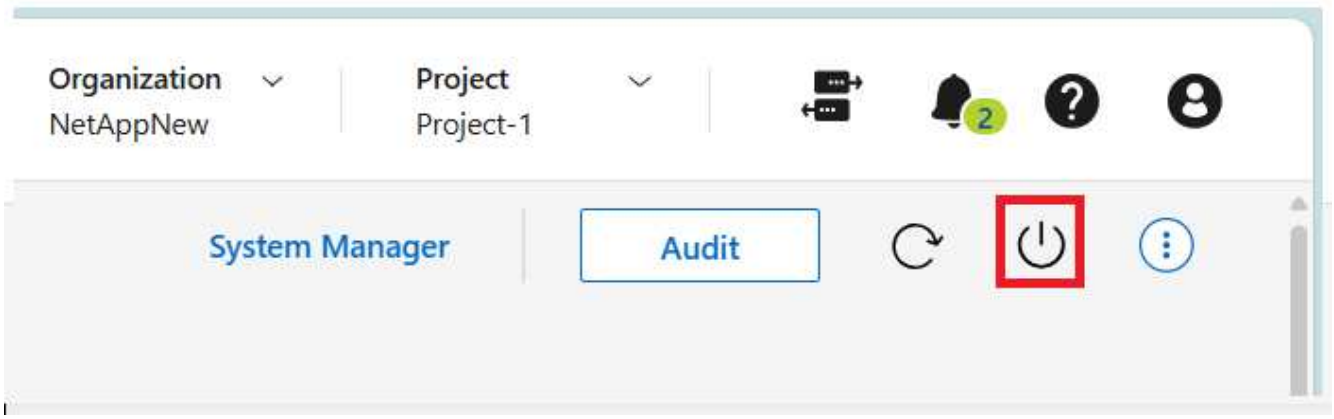
> 為了降低成本，控制台會定期刪除根和啟動磁碟的舊快照。根磁碟和啟動磁碟僅保留最近的兩個快照。

關於此任務

當您停止 HA 對時，控制台將關閉兩個節點。

步驟

1. 在系統中，按一下「關閉」圖示。



2. 保持建立快照的選項處於啟用狀態，因為快照可以啟用系統復原。
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*系統*頁面重新啟動系統。

   重新啟動時會自動建立快照。

使用 NTP 伺服器同步Cloud Volumes ONTAP系統時間

為確保準確的時間同步，您必須為Cloud Volumes ONTAP系統設定網路時間協定 (NTP) 伺服器。請確保在所有雲端供應商上為Cloud Volumes ONTAP系統設定 NTP 伺服器，以保持網路內時間同步的一致性。

如果您未設定 NTP 伺服器，可能會遇到服務中斷和時間同步不準確的情況。

您可以使用以下命令指定 NTP 伺服器：

- "NetApp ConsoleAPI"。
- ONTAP CLI 指令 "建立叢集時間服務 NTP 伺服器"。

相關連結

- 知識庫（KB）文章： "CVO叢集如何使用NTP？"
- "準備使用 API"
- "Cloud Volumes ONTAP工作流程"
- "取得所需的標識符"
- "使用NetApp Console的 REST API"

修改系統寫入速度

您可以在NetApp Console中為Cloud Volumes ONTAP選擇正常或高寫入速度。預設寫入速度正常。如果您的工作負載需要快速寫入效能，您可以變更為高寫入速度。

所有類型的單節點系統和部分 HA 配對配置均支援高寫入速度。在 "Cloud Volumes ONTAP發行說明"中查看支

援的配置

在更改寫入速度之前，您應該"了解正常設定和高設定之間的差異"。

關於此任務

- 確保磁碟區或聚合建立等操作尚未進行。
- 請注意，此變更將重新啟動Cloud Volumes ONTAP系統。這是一個破壞性的過程，需要整個系統停機。

步驟

1. 在*系統*頁面上，雙擊您配置寫入速度的系統的名稱。
2. 在「概述」標籤上，按一下「功能」面板，然後按一下「寫入速度」旁邊的鉛筆圖示。
3. 選擇*正常*或*高*。

   如果您選擇“高”，那麼您需要閱讀“我明白...”聲明並透過勾選方塊進行確認。

   從 9.13.0 版本開始，Google Cloud 中的Cloud Volumes ONTAP HA 對支援 高 寫入速度選項。

4. 按一下“儲存”，查看確認訊息，然後按一下“核准”。

變更Cloud Volumes ONTAP叢集管理員密碼

Cloud Volumes ONTAP包含一個叢集管理員帳戶。如果需要，您可以從NetApp Console變更此帳戶的密碼。

您不應透過ONTAP系統管理員或ONTAP CLI 變更管理員帳戶的密碼。密碼不會反映在控制台中。因此，控制台無法正確監控實例。

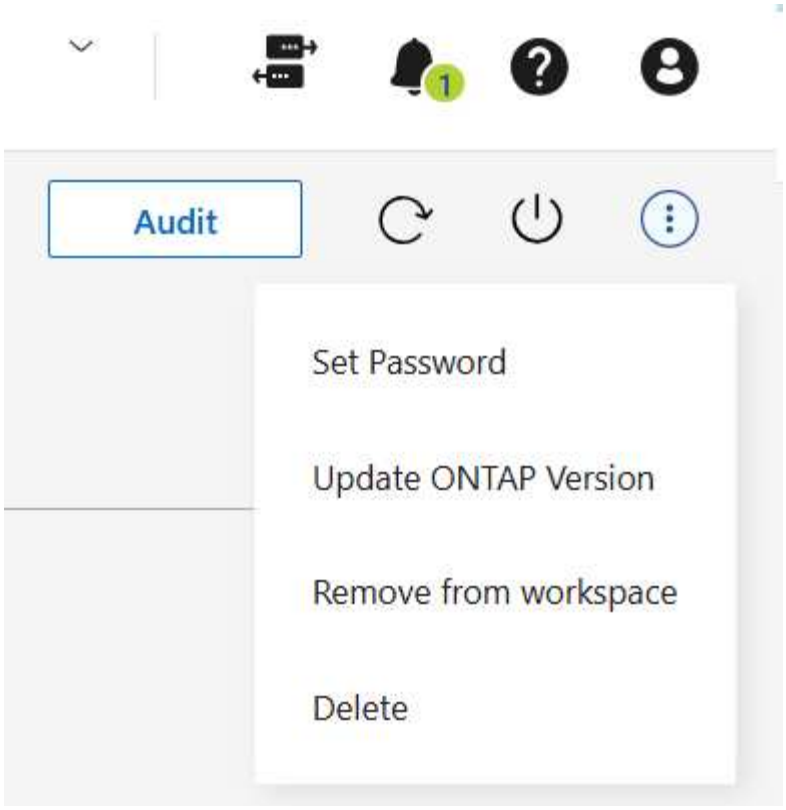
關於此任務

密碼必須遵守一些規則。新密碼：

- 不應包含該詞 `admin`
- 長度必須介於 8 到 50 個字元之間
- 必須至少包含一個英文字母和一個數字
- 不應包含以下特殊字元： `/ ( ) { } [ ] # : % " ? \`

步驟

1. 在*系統*頁面上，雙擊Cloud Volumes ONTAP系統的名稱。
2. 在控制台的右上角，按一下...圖標，然後選擇*設定密碼*。



新增、移除或刪除系統

將現有的**Cloud Volumes ONTAP**系統新增至**NetApp Console**

您可以探索現有的 Cloud Volumes ONTAP 系統並將其新增至 NetApp Console 以進行集中管理。當您使用帳戶上線系統時，該系統會註冊到該帳戶。在具有多個帳戶或組織的環境中，您只能探索和管理已註冊到您的 Console 登入帳戶的系統。

在進行系統註冊時，請確保所有操作均在系統最初註冊的同一組織和帳戶內執行。例如，您可以將 Cloud Volumes ONTAP 系統遷移到新的 Console 代理，但遷移過程必須在同一組織內進行。

您無法探索、檢視或管理已註冊到其他帳戶或組織的系統。

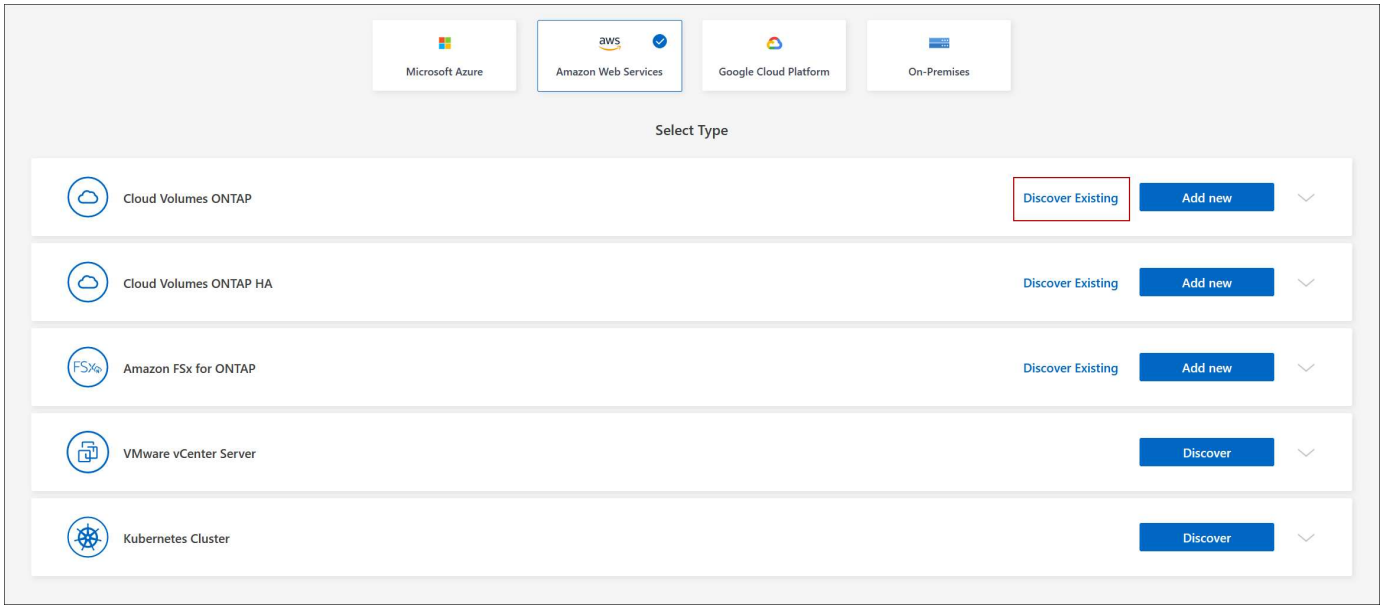
開始之前

您必須知道Cloud Volumes ONTAP管理員使用者帳號的密碼。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在*系統*頁面上，按一下*新增系統*。
3. 選擇系統所在的雲端提供者。
4. 選擇要新增的Cloud Volumes ONTAP系統的類型。
5. 點擊連結即可發現現有系統。

+



1. 在「區域」頁面上，選擇一個區域。您可以看到在所選區域中運作的系統。

   Cloud Volumes ONTAP系統在此頁面中以實例形式表示。從清單中，您可以只選擇使用目前帳戶註冊的那些執行個體。

2. 在「憑證」頁面上，輸入Cloud Volumes ONTAP管理員使用者的密碼，然後選擇「**Go**」。

結果

控制台將Cloud Volumes ONTAP系統新增至 系統 頁面。

從**NetApp Console**移除**Cloud Volumes ONTAP**系統

您可以刪除Cloud Volumes ONTAP系統以將其移至另一個系統或解決發現問題。

關於此任務

刪除Cloud Volumes ONTAP系統會將其從NetApp Console中移除。它不會刪除Cloud Volumes ONTAP系統。如果需要，您可以稍後重新發現該系統。

步驟

1. 在「系統」頁面上，雙擊要刪除的系統。
2. 在控制台的右上角，按一下 ••• 圖標，然後選擇*從工作區中刪除*。
3. 在*從工作區中刪除*視窗中，按一下*刪除*。

結果

控制台刪除系統。使用者可以隨時從*系統*頁面重新發現已刪除的系統。

從**NetApp Console**移除**Cloud Volumes ONTAP**系統

您應該始終從NetApp Console中刪除Cloud Volumes ONTAP系統，而不是從雲端提供者的應用程式中刪除。例如，如果您終止了雲端提供者授權的Cloud Volumes ONTAP實例，則您不能將該授權金鑰用於另一個實例。您必須從控制台中刪除Cloud Volumes ONTAP系統

才能釋放許可證。

當您刪除系統時，控制台會終止Cloud Volumes ONTAP實例並刪除磁碟和快照。

> 刪除系統時，不會刪除其他資源，例如NetApp Backup and Recovery管理的備份以及NetApp Data Classification的實例。您需要手動刪除它們。如果您不這樣做，那麼您將繼續為這些資源支付費用。

當控制台在您的雲端提供者中部署Cloud Volumes ONTAP時，它會對執行個體啟用終止保護。此選項有助於防止意外終止。

步驟

1. 如果您在系統上啟用了備份和還原功能，請確定是否仍然需要備份的數據，然後… "如有必要，刪除備份" 。

   備份和還原在設計上獨立於Cloud Volumes ONTAP 。當您刪除Cloud Volumes ONTAP系統時，備份和復原不會自動刪除備份，且 UI 中目前不支援在系統被刪除後刪除備份。

2. 如果您在此系統上啟用了資料分類，並且沒有其他系統使用此服務，那麼您需要刪除該服務的實例。

   "了解有關資料分類實例的更多信息" 。

3. 刪除Cloud Volumes ONTAP系統。
   a. 在「系統」頁面上，雙擊要刪除的Cloud Volumes ONTAP系統的名稱。
   b. 在控制台的右上角，按一下•••圖標，然後選擇*刪除*。
   c. 輸入要刪除的系統的名稱，然後按一下「刪除」。刪除系統可能需要最多五分鐘。

> 僅適用於Cloud Volumes ONTAP Professional 許可證，備份和復原是免費的。此免費福利不適用於已刪除的環境。如果Cloud Volumes ONTAP環境的備份副本保留在備份和復原實例中，則您將需要為備份副本付費，直到它們被刪除為止。

AWS 管理

修改 **AWS** 中**Cloud Volumes ONTAP**系統的 **EC2** 執行個體類型

在 AWS 中啟動Cloud Volumes ONTAP時，您可以從多個執行個體或類型中進行選擇。如果您確定實例類型太小或太大，無法滿足您的需求，您可以隨時變更實例類型。

關於此任務

- 必須在Cloud Volumes ONTAP HA 對上啟用自動交還（這是預設）。如果不是，則操作將會失敗。

  "ONTAP 9 文件：用於設定自動交還的命令"

- 變更執行個體類型可能會影響 AWS 服務費用。
- 此操作重新啟動Cloud Volumes ONTAP。

  對於單節點系統， I/O 會中斷。

  對於 HA 對來說，這種變化是無中斷的。 HA 對繼續提供數據。

NetApp Console透過啟動接管並等待返回來一次更改一個節點。 NetApp 的品質保證團隊在過程中對檔案的寫入和讀取進行了測試，並且沒有發現客戶端的任何問題。隨著連接的變化，在 I/O 層級觀察到一些重試，但應用層克服了 NFS/CIFS 連接的重新連接。

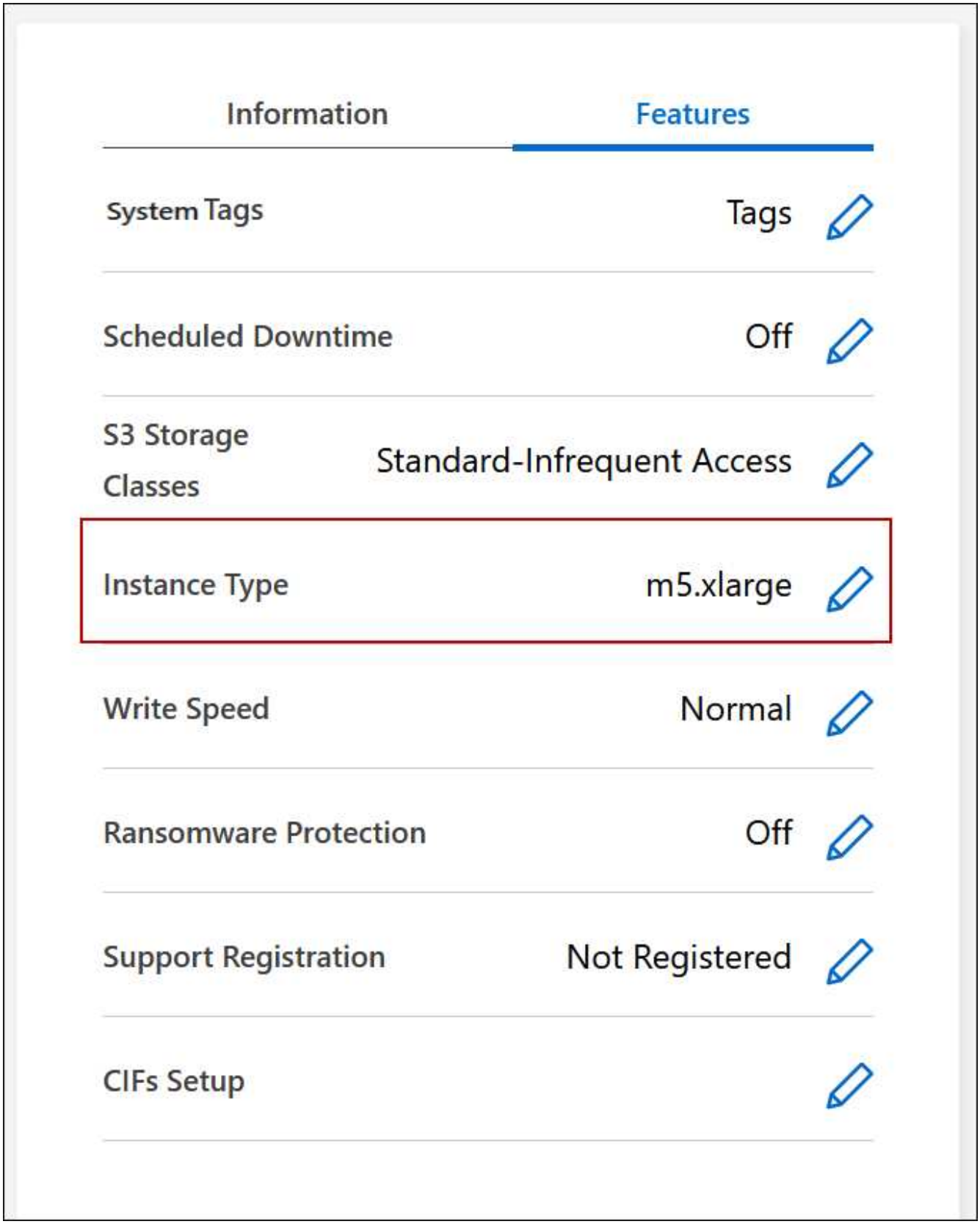
參考

有關 AWS 支援的實例類型列表，請參閱"支援的 EC2 實例"。

如果您無法將實例類型從 c4、m4 或 r4 實例變更為其他類型，請參閱知識庫文章"將 AWS Xen CVO 執行個體轉換為 Nitro (KVM)"。

步驟

1. 在*系統*頁面上，選擇系統。
2. 在概覽標籤上，按一下功能面板，然後按一下*實例類型*旁邊的鉛筆圖示。



如果您使用的是基於節點的即用即付 (PAYGO) 許可證，則可以透過點擊「許可證類型」旁邊的鉛筆圖示來選擇不同的許可證和實例類型。

3. 選擇實例類型，選取核取方塊以確認您了解變更的含義，然後按一下*變更*。

結果

Cloud Volumes ONTAP使用新設定重新啟動。

修改多個 **AWS AZ** 中的**Cloud Volumes ONTAP HA** 對的路由表

您可以修改 AWS 路由表，其中包含部署在多個 AWS 可用區 (AZ) 中的 HA 對的浮動 IP 位址的路由。如果新的 NFS 或 CIFS 用戶端需要存取 AWS 中的 HA 對，您可以這樣做。

步驟

1. 在*系統*頁面上，選擇系統。
2. 在概覽標籤上，按一下功能面板，然後按一下*路由表*旁的鉛筆圖示。
3. 修改所選路由表列表，然後按一下「儲存」。

結果

NetApp Console傳送 AWS 請求來修改路由表。

Azure 管理

變更**Cloud Volumes ONTAP**的 **Azure VM** 類型

在 Microsoft Azure 中啟動Cloud Volumes ONTAP時，您可以從多種 VM 類型中進行選擇。如果您確定虛擬機器類型太小或太大，無法滿足您的需求，您可以隨時變更虛擬機器類型。

關於此任務

- 必須在Cloud Volumes ONTAP HA 對上啟用自動交還（這是預設）。如果不是，則操作將會失敗。

  "ONTAP 9 文件：用於設定自動交還的命令"

- 變更 VM 類型可能會影響 Microsoft Azure 服務費用。
- 此操作重新啟動Cloud Volumes ONTAP。

  對於單節點系統， I/O 會中斷。

  對於 HA 對來說，這種變化是無中斷的。 HA 對繼續提供數據。

NetApp Console透過啟動接管並等待返回來一次更改一個節點。 NetApp 的品質保證團隊在過程中對檔案的寫入和讀取進行了測試，並且沒有發現客戶端的任何問題。隨著連接的變化，在 I/O 層級觀察到一些重試，但應用層克服了 NFS/CIFS 連接的重新連接。

步驟

1. 在*系統*頁面上，選擇系統。
2. 在「概述」標籤上，按一下「功能」面板，然後按一下「**VM** 類型」旁邊的鉛筆圖示。

   如果您使用的是基於節點的即用即付 (PAYGO) 許可證，則可以透過點擊「許可證類型」旁邊的鉛筆圖示來選擇不同的許可證和 VM 類型。

3. 選擇 VM 類型，選取核取方塊以確認您了解變更的含義，然後按一下「變更」。

結果

Cloud Volumes ONTAP使用新設定重新啟動。

覆寫 **Azure** 中**Cloud Volumes ONTAP HA** 對的 **CIFS** 鎖

組織或帳戶管理員可以在NetApp Console中啟用一項設置，以防止在 Azure 維護事件期間出現Cloud Volumes ONTAP儲存復原問題。啟用此設定後， Cloud Volumes ONTAP將否決 CIFS 鎖定並重設活動的 CIFS 會話。

關於此任務

Microsoft Azure 會安排其虛擬機器的定期維護事件。當Cloud Volumes ONTAP HA 對上發生維護事件時，HA 對會啟動儲存接管。如果在此維護事件期間有活動的 CIFS 會話，則 CIFS 檔案上的鎖定可能會阻止儲存復原。

如果啟用此設置， Cloud Volumes ONTAP將否決鎖定並重置活動的 CIFS 會話。因此，HA 對可以在這些維護事件期間完成儲存恢復。

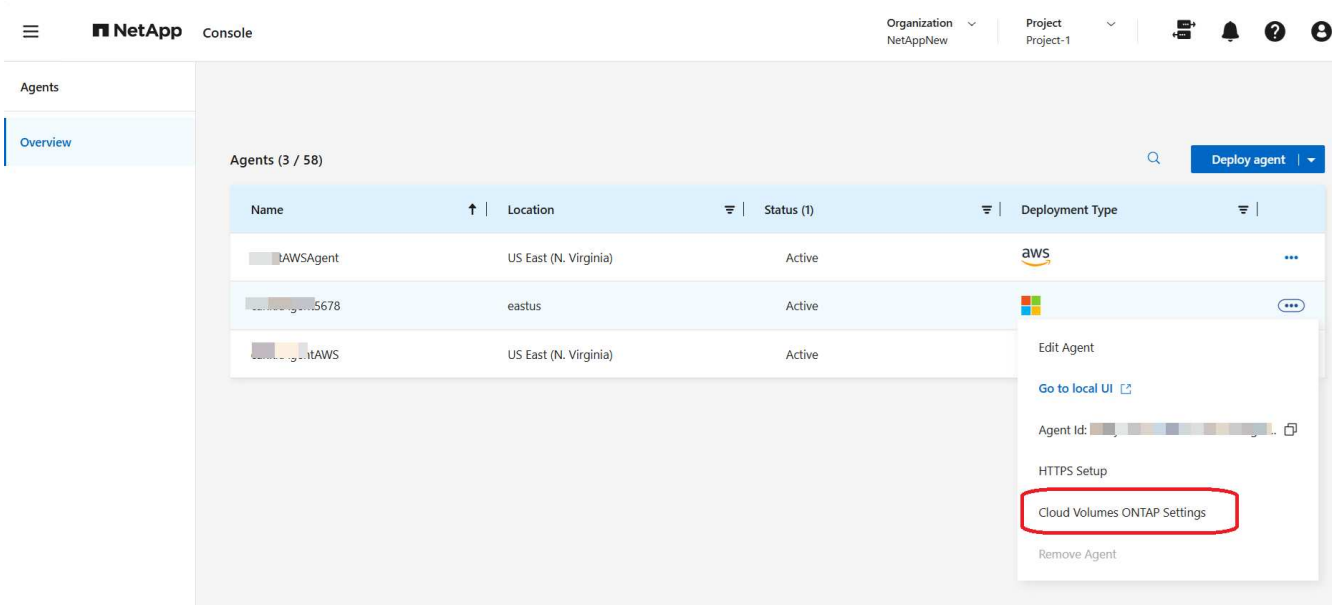
此過程可能會對 CIFS 用戶端造成破壞。 CIFS 用戶端未提交的資料可能會遺失。

開始之前

您需要先建立控制台代理，然後才能變更控制台設定。 "學習使用" 。

步驟

1. 從左側導覽窗格前往*管理>代理*。
2. 點選 ••• 管理Cloud Volumes ONTAP系統的控制台代理的圖示。
3. 選擇* Cloud Volumes ONTAP設定*。



4. 在「Azure」下，按一下「Azure HA 系統的 Azure CIFS 鎖定」。
5. 按一下複選框以啟用該功能，然後按一下“儲存”。

為Cloud Volumes ONTAP系統使用 Azure Private Link 或服務端點

Cloud Volumes ONTAP使用 Azure Private Link 連接到其關聯的儲存帳戶。如果需要，您可以停用 Azure Private Links 並改用服務端點。

概況

預設情況下， NetApp Console啟用 Azure Private Link 來建立Cloud Volumes ONTAP與其關聯儲存帳戶之間的連線。 Azure 專用連結可保護 Azure 中端點之間的連線並提供效能優勢。

如果需要，您可以將Cloud Volumes ONTAP設定為使用服務端點而不是 Azure Private Link。

無論採用哪種配置，控制台始終限制Cloud Volumes ONTAP和儲存帳戶之間的連接的網路存取。網路存取僅限於部署Cloud Volumes ONTAP 的VNet 和部署控制台代理程式的 VNet。

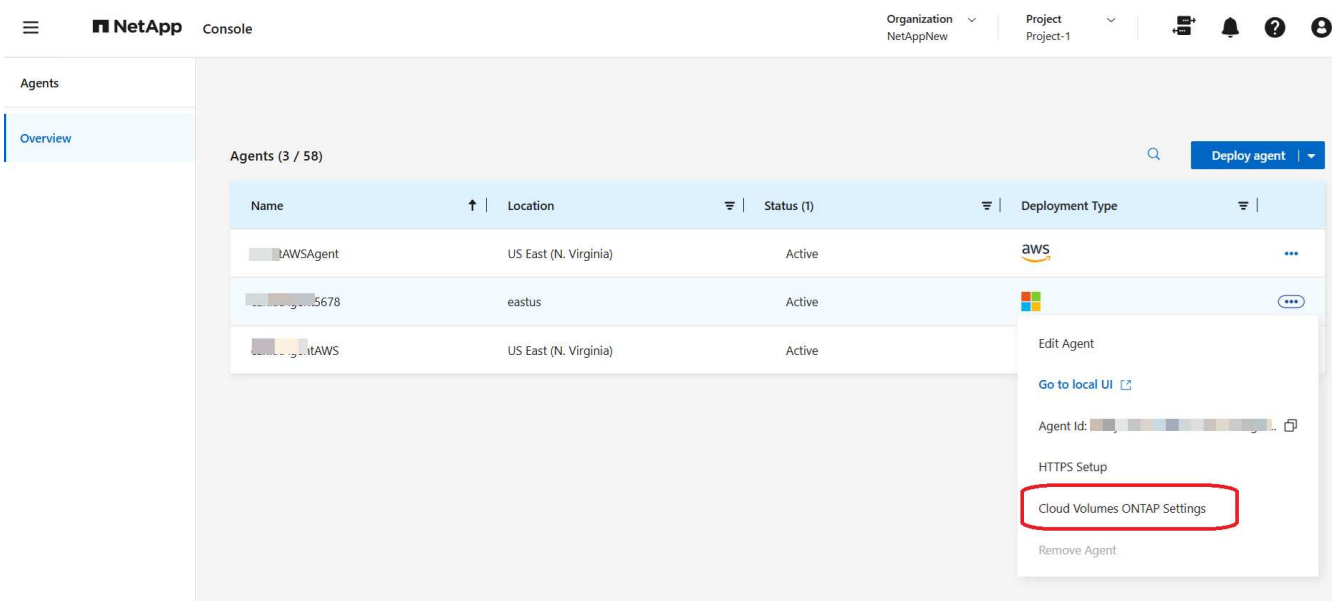
停用 Azure Private Links 並改用服務終點

如果您的業務需要，您可以在控制台中變更設置，以便將Cloud Volumes ONTAP配置為使用服務端點而不是 Azure Private Link。變更此設定適用於您建立的新Cloud Volumes ONTAP系統。服務端點僅支援"Azure 區域對"控制台代理程式和Cloud Volumes ONTAP VNet 之間。

控制台代理應部署在與其管理的Cloud Volumes ONTAP系統相同的 Azure 區域中，或部署在 "Azure 區域對"適用於Cloud Volumes ONTAP系統。

步驟

1. 從左側導覽窗格前往*管理>代理*。
2. 點選 ••• 管理Cloud Volumes ONTAP系統的控制台代理的圖示。
3. 選擇* Cloud Volumes ONTAP設定*。



4. 在「**Azure**」下，按一下「使用 **Azure** 專用連結」。
5. 取消選擇* Cloud Volumes ONTAP和儲存帳戶之間的專用連結連線*。
6. 點選“儲存”。

完成後

如果您停用了 Azure Private Links 且控制台代理程式使用代理伺服器，則必須啟用直接 API 流量。

"了解如何在控制台代理上啟用直接 API 流量"

使用 **Azure Private Links**

在大多數情況下，您無需執行任何操作即可設定與Cloud Volumes ONTAP 的Azure Private 連結。控制台為您管理 Azure 專用連結。但是如果您使用現有的 Azure 私人 DNS 區域，則需要編輯設定檔。

自訂 **DNS** 的要求

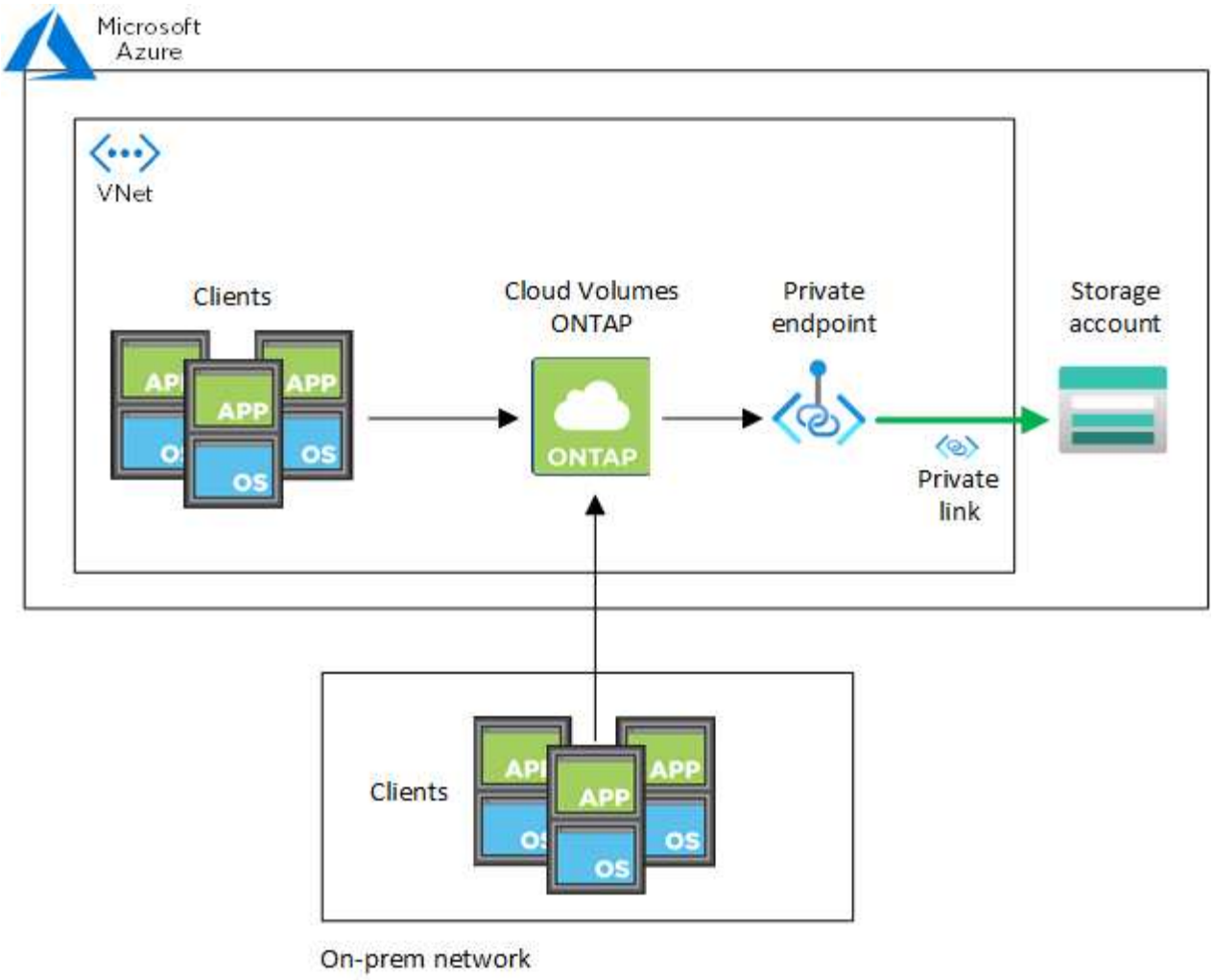
或者，如果您使用自訂 DNS，則需要從自訂 DNS 伺服器建立至 Azure 私人 DNS 區域的條件轉送器。要了解更多信息，請參閱"Azure 關於使用 DNS 轉送器的文檔"。

專用連結連接的工作原理

當控制台在 Azure 中部署Cloud Volumes ONTAP時，它會在資源組中建立一個私有端點。私有端點與Cloud Volumes ONTAP 的儲存帳戶相關聯。因此，對Cloud Volumes ONTAP儲存的存取需要透過 Microsoft 主幹網路。

當客戶端與Cloud Volumes ONTAP位於同一 VNet 內、位於對等 VNet 內或位於本機網路中時，用戶端存取將透過專用連結進行。

以下範例展示了用戶端如何透過專用連結從同一 VNet 內部以及從具有專用 VPN 或 ExpressRoute 連接的本機網路存取。



如果控制台代理程式和Cloud Volumes ONTAP系統部署在不同的 VNet 中，則必須在部署控制台代理程式的 VNet 和部署Cloud Volumes ONTAP系統的 VNet 之間設定 VNet 對等連線。

提供有關 **Azure** 專用 **DNS** 的詳細信息

如果你使用 "Azure 專用 DNS"，那麼就需要在每個Console代理上修改一個設定檔。否則，控制台無法設定Cloud Volumes ONTAP與其關聯儲存帳戶之間的 Azure Private Link 連線。

請注意，DNS 名稱必須符合 Azure DNS 命名要求 "如 Azure 文件所示"。

步驟

1. 透過 SSH 連接到控制台代理主機並登入。
2. 導航至 `/opt/application/netapp/cloudmanager/docker_occm/data`目錄。
3. 編輯 `app.conf`透過添加 `user-private-dns-zone-settings`具有以下關鍵字-值對的參數：

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

這 `subscription`僅當私有 DNS 區域與控制台代理的訂閱不同時才需要關鍵字。

4. 儲存檔案並登出控制台代理程式。

   不需要重新啟動。

啟用故障回滾

如果控制台無法在特定操作中建立 Azure 專用鏈接，它將在沒有 Azure 專用連結連接的情況下完成此操作。建立新系統（單一節點或 HA 對）時，或在 HA 對上執行以下操作時，可能會發生這種情況：建立新聚合、向現有聚合新增磁碟或在超過 32 TiB 時建立新的儲存帳戶。

如果控制台無法建立 Azure 專用鏈接，您可以透過啟用回溯來變更此預設行為。這有助於確保您完全遵守公司的安全規定。

如果啟用回滾，控制台將停止該操作並回滾作為該操作的一部分所建立的所有資源。

您可以透過 API 或更新 app.conf 檔案來啟用回滾。

透過 **API** 啟用回滾

步

1. 使用 `PUT /occm/config`具有以下請求主體的 API 呼叫：

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

透過更新 **app.conf** 啟用回滾

步驟

1. 透過 SSH 連接到控制台代理的主機並登入。
2. 導覽至以下目錄：/opt/application/netapp/cloudmanager/docker_occm/data
3. 編輯 app.conf，新增以下參數和值：

```
 "rollback-on-private-link-failure": true
```

. 儲存檔案並登出控制台代理程式。

不需要重新啟動。

在 **Azure** 控制台中移動**Cloud Volumes ONTAP**的 **Azure** 資源組

Cloud Volumes ONTAP支援 Azure 資源組移動，但工作流程僅在 Azure 控制台中進行。

您可以將Cloud Volumes ONTAP系統從同一 Azure 訂閱內的一個資源群組移至 Azure 中的另一個資源群組。不支援在不同的 Azure 訂閱之間行動資源群組。

步驟

1. 刪除Cloud Volumes ONTAP系統。請參閱"刪除Cloud Volumes ONTAP系統" 。
2. 在 Azure 控制台中執行資源組移動。

   若要完成移動，請參閱"Microsoft Azure 文件中的“將資源移至新的資源群組或訂閱”"。
3. 在*系統*頁面上，發現系統。
4. 在系統資訊中尋找新的資源組。

結果

系統及其資源（虛擬機器、磁碟、儲存帳戶、網路介面、快照）位於新的資源群組中。

在 **Azure** 中隔離**SnapMirror**流量

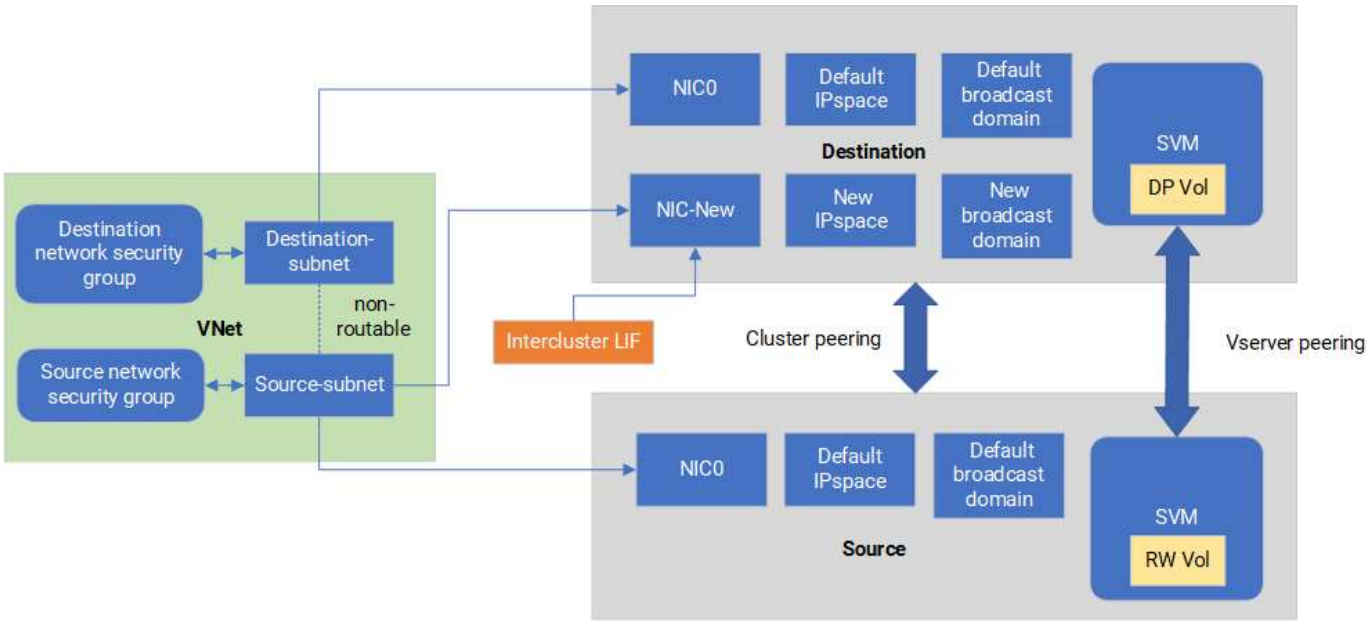
使用 Azure 中的Cloud Volumes ONTAP ，您可以將SnapMirror複製流量與資料和管理流量分開。為了將SnapMirror複製流量與資料流量隔離，您需要新增一個新的網路介面卡 (NIC)、一個相關的群集間 LIF 和一個不可路由的子網路。

關於 **Azure** 中的**SnapMirror**流量隔離

預設情況下， NetApp Console會在相同子網路上設定Cloud Volumes ONTAP部署中的所有 NIC 和 LIF。在這樣的設定中， SnapMirror複製流量和資料和管理流量使用相同的子網路。隔離SnapMirror流量利用了無法路由到用於資料和管理流量的現有子網路的額外子網路。

圖 **1**

下圖顯示了在單一節點部署中，使用附加 NIC、關聯的群集間 LIF 和不可路由子網路對SnapMirror複製流量進行隔離。 HA 對部署略有不同。



開始之前

回顧以下注意事項：

- 您只能向Cloud Volumes ONTAP單節點或 HA 對部署（VM 實例）新增單一 NIC 以實現SnapMirror流量隔離。
- 若要新增新的 NIC，您部署的 VM 實例類型必須具有未使用的 NIC。
- 來源叢集和目標叢集應該可以存取同一個虛擬網路 (VNet)。目標叢集是 Azure 中的Cloud Volumes ONTAP系統。來源叢集可以是 Azure 中的Cloud Volumes ONTAP系統或ONTAP系統。

步驟 1：建立額外的 NIC 並連接到目標 VM

本節提供有關如何建立附加 NIC 並將其附加到目標 VM 的說明。目標 VM 是 Azure 中Cloud Volumes ONTAP中的單節點或 HA 對系統，您要設定額外的 NIC。

步驟

1. 在ONTAP CLI 中，停止節點。

```
dest::> halt -node <dest_node-vm>
```

2. 在 Azure 入口網站中，檢查 VM（節點）狀態是否已停止。

```
az vm get-instance-view --resource-group <dest-rg> --name <dest-vm>
--query instanceView.statuses[1].displayStatus
```

3. 使用 Azure Cloud Shell 中的 Bash 環境停止節點。
   a. 停止節點。

```
az vm stop --resource-group <dest_node-rg> --name <dest_node-vm>
```

b. 解除分配節點。

```
az vm deallocate --resource-group <dest_node-rg> --name <dest_node-vm>
```

4. 設定網路安全群組規則，讓兩個子網路（來源叢集子網路和目標叢集子網路）互不可達。
   a. 在目標虛擬機器上建立新的 NIC。
   b. 尋找來源叢集子網路的子網路 ID。

```
az network vnet subnet show -g <src_vnet-rg> -n <src_subnet> --vnet-name <vnet> --query id
```

   c. 使用來源叢集子網路的子網路 ID 在目標虛擬機器上建立新的 NIC。在這裡輸入新 NIC 的名稱。

```
az network nic create -g <dest_node-rg> -n <dest_node-vm-nic-new> --subnet <id_from_prev_command> --accelerated-networking true
```

   d. 保存私有IP位址。此 IP 位址 <new_added_nic_primary_addr> 用於在廣播域，新 NIC 的群集間 LIF。
5. 將新的 NIC 附加到 VM。

```
az vm nic add -g <dest_node-rg> --vm-name <dest_node-vm> --nics <dest_node-vm-nic-new>
```

6. 啟動虛擬機器（節點）。

```
az vm start --resource-group <dest_node-rg>  --name <dest_node-vm>
```

7. 在 Azure 入口網站中，前往 網路 並確認新的 NIC（例如 nic-new）存在並且加速網路已啟用。

```
az network nic list --resource-group azure-59806175-60147103-azure-rg --query "[].{NIC: name, VM: virtualMachine.id}"
```

對於 HA 對部署，請對合作夥伴節點重複這些步驟。

步驟 2：為新 NIC 建立新的 IP 空間、廣播域和群集間 LIF

群集間 LIF 的單獨 IP 空間為群集間複製的網路功能提供了邏輯分離。

使用ONTAP CLI 執行以下步驟。

步驟

1. 建立新的 IP 空間（new_ipspace）。

```
dest::> network ipspace create -ipspace <new_ipspace>
```

2. 在新的 IP 空間（new_ipspace）上建立廣播網域並新增 nic-new 連接埠。

```
dest::> network port show
```

3. 對於單節點系統，新增連接埠為 *e0b*。對於使用託管磁碟的 HA 配對部署，新增連接埠為 *e0d*。對於使用分頁 Blob 的 HA 配對部署，新增連接埠為 *e0e*。請使用節點名稱，而非 VM 名稱。執行 `node show`以尋找節點名稱。

```
dest::> broadcast-domain create -broadcast-domain <new_bd> -mtu 1500
-ipspace <new_ipspace> -ports <dest_node-cot-vm:e0b>
```

4. 在新的廣播域 (new_bd) 和新的 NIC (nic-new) 上建立叢集間 LIF。

```
dest::> net int create -vserver <new_ipspace> -lif <new_dest_node-ic-
lif> -service-policy default-intercluster -address
<new_added_nic_primary_addr> -home-port <e0b> -home-node <node> -netmask
<new_netmask_ip> -broadcast-domain <new_bd>
```

5. 驗證新的集群間 LIF 的建立。

```
dest::> net int show
```

對於 HA 對部署，請對合作夥伴節點重複這些步驟。

步驟 3：驗證來源系統和目標系統之間的叢集對等連接

本節提供有關如何驗證來源系統和目標系統之間的對等關係的說明。

使用ONTAP CLI 執行以下步驟。

步驟

1. 驗證目標群集的群集間 LIF 是否可以對來源群集的群集間 LIF 執行 ping 操作。由於目標群集執行此命令，

因此目標 IP 位址是來源上的群集間 LIF IP 位址。

```
dest::> ping -lif <new_dest_node-ic-lif> -vserver <new_ipspace>
-destination <10.161.189.6>
```

2. 驗證來源集群的集群間 LIF 是否可以 ping 通目標集群的集群間 LIF。目標是在目標上建立的新 NIC 的 IP 位址。

```
src::> ping -lif <src_node-ic-lif> -vserver <src_svm> -destination
<10.161.189.18>
```

對於 HA 對部署，請對合作夥伴節點重複這些步驟。

步驟 4：在來源系統和目標系統之間建立 SVM 對等連接

本節提供如何在來源系統和目標系統之間建立 SVM 對等的說明。

使用ONTAP CLI 執行以下步驟。

步驟

1. 使用來源集群間 LIF IP 位址作為目標在目標上建立集群對等 `-peer-addrs`。對於 HA 對，列出兩個節點的來源群集間 LIF IP 位址作為 `-peer-addrs`。

```
dest::> cluster peer create -peer-addrs <10.161.189.6> -ipspace
<new_ipspace>
```

2. 輸入並確認密碼。
3. 使用目標群集 LIF IP 位址作為來源群集的 IP 位址，在來源上建立群集對等連接 `peer-addrs`。對於 HA 對，列出兩個節點的目標群集間 LIF IP 位址作為 `-peer-addrs`。

```
src::> cluster peer create -peer-addrs <10.161.189.18>
```

4. 輸入並確認密碼。
5. 檢查集群是否對等。

```
src::> cluster peer show
```

成功的對等連線在可用性欄位中顯示 可用。

6. 在目標上建立 SVM 對等連線。來源 SVM 和目標 SVM 都應該是資料 SVM。

```
dest::> vserver peer create -vserver <dest_svm> -peer-vserver <src_svm>
-peer-cluster <src_cluster> -applications snapmirror``
```

7. 接受 SVM 對等連線。

```
src::> vserver peer accept -vserver <src_svm> -peer-vserver <dest_svm>
```

8. 檢查 SVM 是否已對等。

```
dest::> vserver peer show
```

同行國家顯示*peered* 和對等應用程式顯示*snapmirror*.

步驟 5：在來源系統和目標系統之間建立SnapMirror複製關係

本節提供如何在來源系統和目標系統之間建立SnapMirror複製關係的說明。

要移動現有的SnapMirror複製關係，必須先中斷現有的SnapMirror複製關係，然後再建立新的SnapMirror複製關係。

使用ONTAP CLI 執行以下步驟。

步驟

1. 在目標 SVM 上建立資料保護磁碟區。

```
dest::> vol create -volume <new_dest_vol> -vserver <dest_svm> -type DP
-size <10GB> -aggregate <aggr1>
```

2. 在目標上建立SnapMirror複製關係，其中包括複製的SnapMirror策略和計劃。

```
dest::> snapmirror create -source-path src_svm:src_vol  -destination
-path  dest_svm:new_dest_vol -vserver dest_svm -policy
MirrorAllSnapshots -schedule 5min
```

3. 在目標上初始化SnapMirror複製關係。

```
dest::> snapmirror initialize -destination-path  <dest_svm:new_dest_vol>
```

4. 在ONTAP CLI 中，透過執行以下命令驗證SnapMirror關係狀態：

```
dest::> snapmirror show
```

關係狀態是 `Snapmirrored`關係的健康是 `true`。

5. 可選：在ONTAP CLI 中，執行以下命令查看SnapMirror關係的操作記錄。

```
dest::> snapmirror show-history
```

或者，您可以掛載來源磁碟區和目標卷，將檔案寫入來源卷，並驗證磁碟區是否複製到目標磁碟區。

Google Cloud 管理

變更Cloud Volumes ONTAP的 Google Cloud 機器類型

在 Google Cloud 中啟動Cloud Volumes ONTAP時，您可以從多種機器類型中進行選擇。如果您確定實例或機器類型太小或太大，無法滿足您的需求，您可以隨時變更執行個體或機器類型。

關於此任務

- 必須在Cloud Volumes ONTAP HA 對上啟用自動交還（這是預設）。如果不是，則操作將會失敗。

  "ONTAP 9 文件：用於設定自動交還的命令"

- 更改機器類型可能會影響 Google Cloud 服務費用。
- 此操作重新啟動Cloud Volumes ONTAP。

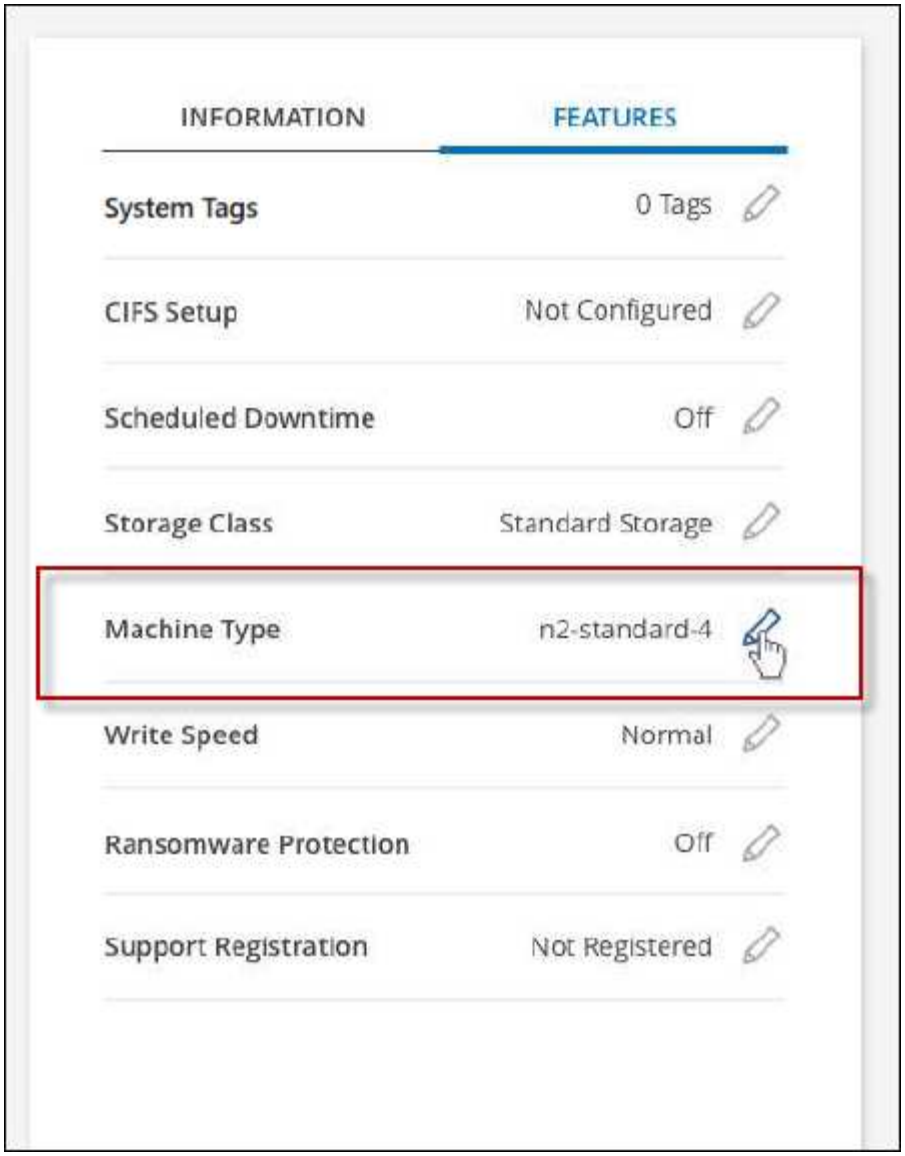
  對於單節點系統， I/O 會中斷。

  對於 HA 對來說，這種變化是無中斷的。 HA 對繼續提供數據。

NetApp Console透過啟動接管並等待返回來一次更改一個節點。 NetApp 的品質保證團隊在過程中對檔案的寫入和讀取進行了測試，並且沒有發現客戶端的任何問題。隨著連接的變化，在 I/O 層級觀察到一些重試，但應用層克服了 NFS/CIFS 連接的重新連接。

步驟

1. 在*系統*頁面上，選擇系統。
2. 在概覽標籤上，按一下功能面板，然後按一下*機器類型*旁邊的鉛筆圖示。



如果您使用的是基於節點的即用即付 (PAYGO) 許可證，則可以透過點擊「許可證類型」旁邊的鉛筆圖示來選擇不同的許可證和機器類型。

1. 選擇機器類型，選取核取方塊以確認您了解變更的含義，然後按一下*變更*。

結果

Cloud Volumes ONTAP使用新設定重新啟動。

將現有的 **Cloud Volumes ONTAP** 部署轉換為 **Infrastructure Manager**

自 2026 年 1 月 12 日起，Google Cloud 中新的 Cloud Volumes ONTAP 部署可以使用 Google Cloud Infrastructure Manager。Google 即將棄用 Google Cloud Deployment Manager，改用 Infrastructure Manager。因此，您需要手動執行遷移工具，將現有的 Cloud Volumes ONTAP 部署從 Deployment Manager 遷移到 Infrastructure Manager。此程序只需執行一次，之後您的系統將自動開始使用 Infrastructure Manager。

關於此任務

過渡工具可在 "NetApp 支援網站"中使用，並建立下列工件：

- Terraform 工件，儲存於 `conversion_output/deployment_name`。
- 轉換結果摘要已儲存在 `conversion_output/batch_summary_<deployment_name>_<timestamp>.json`中。
- 偵錯記錄儲存在 `<gcp project number>-<region>-blueprint-config/<cvo name>` 目錄中。您需要這些記錄進行疑難排解。 `<gcp project number>-<region>-blueprint-config` 儲存貯體儲存 Terraform 記錄。

使用 Infrastructure Manager 的 Cloud Volumes ONTAP 系統會將資料和記錄儲存在 Google Cloud Storage 儲存桶中。這些儲存桶可能會產生額外費用，但請勿編輯或刪除儲存桶及其內容：

- `gs://netapp-cvo-infrastructure-manager-<project id>/dm-to-im-convert`：用於儲存 Cloud Volumes ONTAP Terraform 文件
- `<gcp project number>-<region>-blueprint-config`：用於儲存 Google Cloud Terraform 工件

開始之前

- 請確保您的 Cloud Volumes ONTAP 系統版本為 9.16.1 或更高版本。
- 確保沒有透過 Google Cloud Console 手動編輯過任何 Cloud Volumes ONTAP 資源或其屬性。
- 請確保已啟用 Google Cloud API。請參閱 "啟用 Google Cloud API"。請確保除了其他 API 之外，還啟用了 Google Cloud Quotas API。
- 請確認 NetApp Console agent 的服務帳戶擁有所有必要的權限。請參閱 "控制台代理的 Google Cloud 權限"。
- 轉換工具使用以下網域。在您的網路中於連接埠 443 上啟用它們：

網域	港口	協定	方向	目的
cloudresourcemanager.googleapis.com	443	TCP	外傳	專案驗證
deploymentmanager.googleapis.com	443	TCP	外傳	部署探索
config.googleapis.com	443	TCP	外傳	Infrastructure Manager API
storage.googleapis.com	443	TCP	外傳	GCS 儲存貯體作業
iam.googleapis.com	443	TCP	外傳	服務帳戶驗證
compute.googleapis.com	443	TCP	外傳	Google Cloud 和 Terraform Import 與 Plan 使用的運算 API 呼叫
openidconnect.googleapis.com	443	TCP	外傳	驗證

網域	港口	協定	方向	目的
oauth2.googleapis.com	443	TCP	外傳	OAuth2 權杖交換
registry.terraform.io	443	TCP	外傳	Terraform 提供者登錄
releases.hashicorp.com	443	TCP	外傳	Terraform 二進位下載
apt.releases.hashicorp.com	443	TCP	外傳	HashiCorp APT 存儲庫
us-central1-docker.pkg.dev	443	TCP	外傳	GCP Artifact Registry
metadata.google.internal	80	HTTP	內部	VM 元資料和驗證權杖

步驟

請依照下列步驟從 Deployment Manager 過渡到 Infrastructure Manager，並為現有的 Cloud Volumes ONTAP 部署執行該工具。

1. 建立角色並將其附加到服務帳戶：
   a. 建立具有下列權限的 YAML 檔案：

```
title: NetApp Dm TO IM Convert Solution
description: Permissions for the service account associated with the
VM where the tool will run.
stage: GA
includedPermissions:
- compute.addresses.get
- compute.disks.get
- compute.forwardingRules.get
- compute.healthChecks.get
- compute.instanceGroups.get
- compute.instances.get
- compute.regionBackendServices.get
- config.deployments.create
- config.deployments.get
- config.deployments.getLock
- config.deployments.lock
- config.deployments.unlock
- config.deployments.update
- config.deployments.delete
- config.deployments.updateState
- config.operations.get
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- iam.serviceAccounts.get
- storage.buckets.create
- storage.objects.create
- storage.objects.delete
- storage.objects.get
- storage.objects.list
```

b. 在 Google Cloud 中建立自訂角色，並賦予其 YAML 檔案中定義的權限。
`gcloud iam roles create dmtoim_convert_tool_role --project=PROJECT_ID \
--file=YAML_FILE_PATH`如需詳細資訊，請參閱 "建立和管理自訂角色"。

c. 將自訂角色附加到您將用於建立 VM 的服務帳戶。

d. 將 `roles/iam.serviceAccountUser`角色新增至此服務帳戶。請參閱 "服務帳戶概覽"。

2. 建立一個具有以下組態的 VM 。您可以在此 VM 上執行此工具。
   - 機器類型：Google Compute Engine 機器類型 e2-medium
   - 作業系統：Ubuntu 25.10 AMD64 Minimal （映像：ubuntu-minimal-2510-amd64）
   - 網路：防火牆允許 HTTP 和 HTTPs
   - 磁碟大小：20GB
   - 安全性：服務帳戶：您建立的服務帳戶

- 安全性：存取範圍 - 為每個 API 設定存取權限：
  - 雲端平台：已啟用
  - Compute Engine ：唯讀
  - 儲存：唯讀 （預設）
  - Google Cloud Logging（以前稱為 Stackdriver Logging）API：僅寫入（預設）
  - Stackdriver Monitoring（現為 Google Cloud Operations 的一部分）API：僅寫入（預設）
  - 服務管理：唯讀 （預設）
  - 服務控制：已啟用 （預設）
  - Google Cloud Trace（以前稱為 Stackdriver Trace）：僅寫入（預設）

3. 使用 SSH 連線至新建立的 VM： `gcloud compute ssh dmtoim-convert-executor-vm --zone <region where VM is deployed>`
4. 使用您的 NSS 憑證從 "NetApp 支援網站"下載轉換工具： `wget <download link from NetApp Support site>`
5. 解壓縮下載的 TAR 檔： `tar -xvf <downloaded file name>`
6. 下載並安裝以下必備套件：
   - Docker：28.2.2 build 28.2.2-0ubuntu1 或更新版本
   - Terraform：1.14.1 或更高版本
   - Python：3.13.7、python3-pip、python3 venv

   ```
   sudo apt-get update
   sudo apt-get install python3-pip python3-venv -y
   wget -O - https://apt.releases.hashicorp.com/gpg | sudo gpg --dearmor
   -o /usr/share/keyrings/hashicorp-archive-keyring.gpg
   echo "deb [arch=$(dpkg --print-architecture) signed-
   by=/usr/share/keyrings/hashicorp-archive-keyring.gpg]
   https://apt.releases.hashicorp.com noble main" | sudo tee
   /etc/apt/sources.list.d/hashicorp.list
   sudo apt update && sudo apt install terraform
   sudo apt-get install -y docker.io
   sudo systemctl start docker
   ```

   Google Cloud CLI `gcloud` 已預先安裝在虛擬機器上。

7. 將目前使用者新增至 Docker 群組，以便工具無需 `sudo` 權限即可使用 Docker。

   ```
   sudo usermod -aG docker $USER
   newgrp docker
   ```

8. 安裝轉換工具：

```
cd <folder where you extracted the tool>
 ./install.sh
```

這會將工具安裝在隔離的環境中 `dmconvert-venv`，並驗證是否已安裝所有必要的軟體套件。

9. 輸入工具的安裝環境： `source dmconvert-venv/bin/activate`
10. 以 `non-sudo`使用者身分執行轉換工具。確保使用與 Console 代理的服務帳戶相同的服務帳戶，並且該服務帳戶擁有所有 "Google Cloud Infrastructure Manager 所需的權限"。

```
dmconvert \
--project-id=<the Google Cloud project ID for the Cloud Volumes ONTAP
deployment> \
--cvo-name=<Cloud Volumes ONTAP system name> \
--service-account=<the service account attached to the Console agent>
```

完成後

此工具會顯示所有 Cloud Volumes ONTAP 系統及其 SVM 詳細資訊的清單。運行完成後，您可以查看所有已轉換系統的狀態。每個已轉換的系統都會以 *<converted system name-imdeploy>* 格式顯示在 Google Console 的 Infrastructure Manager 下，表示 Console 現在使用 Infrastructure Manager API 來管理該 Cloud Volumes ONTAP 系統。

轉換完成後，請勿在 Google Cloud Console 中刪除 Deployment Manager 的部署物件。此部署物件包含 Infrastructure Manager 用於管理 Cloud Volumes ONTAP 系統的元資料。

如果需要回滾轉換，則必須使用同一台虛擬機器。如果已轉換所有系統且無需回滾到 Deployment Manager，則可以刪除該虛擬機器。

復原轉換

如果您不想繼續轉換，可以按照以下步驟回溯到 Deployment Manager：

步驟

1. 在同一個 您為執行該工具而建立的 VM 上，執行以下命令：

```
dmconvert \
--project-id=<the Google Cloud project ID for the Cloud Volumes ONTAP
deployment> \
--cvo-name=<Cloud Volumes ONTAP system name> \
--service-account=<the service account attached to the Console agent> \
--rollback
```

2. 請等待復原完成。

相關連結

- "NetApp Console Agent 4.2.0 發行說明"
- "Google Cloud Infrastructure Manager 所需的權限"

使用系統管理員管理Cloud Volumes ONTAP

Cloud Volumes ONTAP中的高階儲存管理功能可透過ONTAP系統管理器 (ONTAP System Manager) 使用，它是ONTAP系統提供的管理介面。您可以直接從NetApp Console存取系統管理員。

特徵

您可以使用控制台中的ONTAP系統管理員執行各種儲存管理功能。以下列表包含其中一些功能，但並不詳盡：

- 進階儲存管理：管理一致性群組、共用、qtree、配額和儲存虛擬機器。
- 成交量變動： "將磁碟區移動到不同的聚合。"
- 網路管理：管理 IP 空間、網路介面、連接埠集和乙太網路連接埠。
- 管理FlexGroup磁碟區：您只能透過系統管理員建立和管理FlexGroup磁碟區。 BlueXP控制台不支援FlexGroup磁碟區建立。
- 事件和作業：查看事件日誌、系統警報、作業和稽核日誌。
- 進階資料保護：保護儲存虛擬機器、LUN 和一致性群組。
- 主機管理：設定 SAN 啟動器群組和 NFS 用戶端。
- ONTAP S3 物件儲存管理：Cloud Volumes ONTAP 中的 ONTAP S3 儲存管理功能僅在 System Manager 中可用，而不在 Console 中可用。

支援的配置

- 標準雲端區域中的Cloud Volumes ONTAP 9.10.0 及更高版本可透過ONTAP System Manager 進行進階儲存管理。
- GovCloud 區域或沒有出站網路存取的區域不支援系統管理員整合。

限制

Cloud Volumes ONTAP不支援系統管理器介面中顯示的一些功能：

- NetApp Cloud Tiering： Cloud Volumes ONTAP不支援 Cloud Tiering。建立磁碟區時，您應該直接從標準視圖設定資料分層到物件儲存。
- 層級：系統管理員不支援聚合管理（包括本機層級和雲端層級）。您必須直接從標準視圖管理聚合。
- 韌體升級： Cloud Volumes ONTAP不支援從系統管理員的 叢集 **>** 設定 頁面進行自動韌體更新。
- 基於角色的存取控制：系統管理員不支援基於角色的存取控制。
- SMB 持續可用性 (CA)： Cloud Volumes ONTAP不支援 "持續可用的 SMB 共享"實現無中斷運作。

配置存取系統管理員的身份驗證

身為管理員，您可以為從控制台存取ONTAP系統管理員的使用者啟動身份驗證。您可以根據ONTAP使用者角色

確定正確的存取權限級別，並根據需要啟用或停用身份驗證。如果啟用身份驗證，則使用者每次從控制台存取系統管理員或重新載入頁面時都需要輸入其ONTAP使用者憑證，因為控制台不會在內部儲存憑證。如果您停用身份驗證，使用者可以使用管理員憑證存取系統管理員。

此設定適用於您組織或帳戶中的ONTAP使用者的每個控制台代理，無論Cloud Volumes ONTAP系統為何。

所需權限

您需要指派組織或帳戶管理員權限才能修改Cloud Volumes ONTAP使用者驗證的控制台代理設定。

步驟

1. 從左側導覽窗格前往*管理>代理*。
2. 點選 ••• 所需控制台代理的圖示並選擇*編輯控制台代理*。
3. 在*強制使用者憑證*下，選取*啟用/停用*複選框。預設情況下，身份驗證是禁用的。

   如果將此值設為*啟用*，則身份驗證將會重置，並且您必須修改任何現有工作流程以適應此變更。

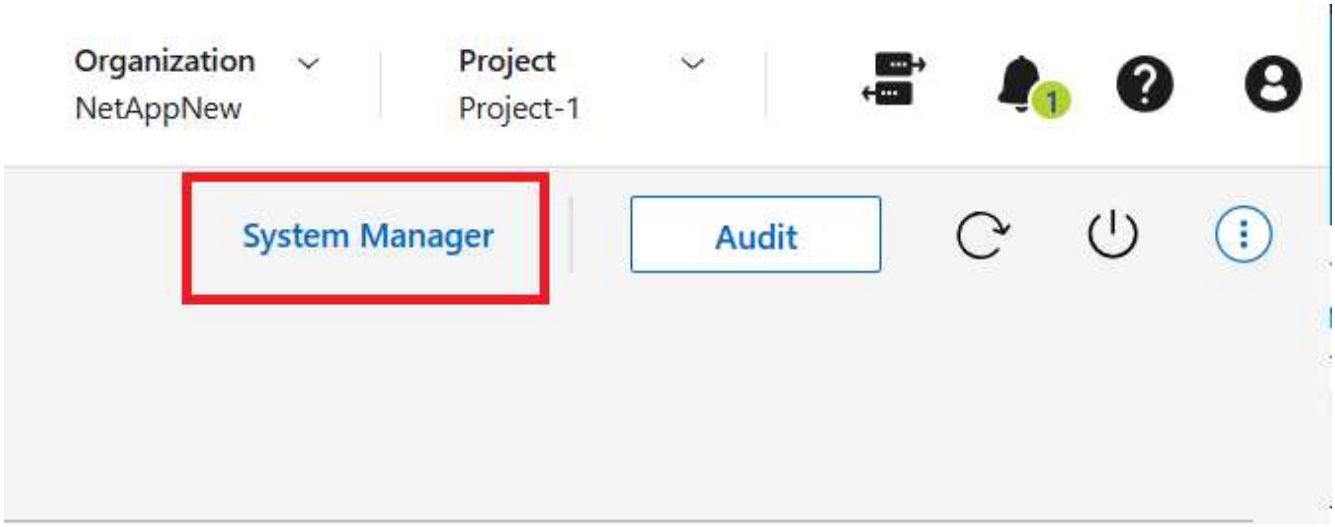
4. 點選“儲存”。

開始使用系統管理員

您可以從Cloud Volumes ONTAP系統存取ONTAP System Manager。

步驟

1. 從左側導覽功能表中，選擇“儲存”>“管理”。
2. 在*系統*頁面上，雙擊所需的Cloud Volumes ONTAP系統。
3. 按一下“系統管理員”。



4. 如果出現提示，請輸入您的ONTAP使用者憑證並點擊 登入。
5. 如果出現確認訊息，請仔細閱讀並按一下「關閉」。

使用系統管理員來管理您的Cloud Volumes ONTAP系統。您可以按一下「返回」返回控制台。

有關使用系統管理員的協助

如果您需要使用 System Manager 和Cloud Volumes ONTAP 的協助，您可以參考 "ONTAP文檔"以獲得逐步說明。以下是一些可能有幫助的ONTAP文件連結：

- "ONTAP角色、應用程式和身份驗證"
- "使用 System Manager 存取叢集" 。
- "捲和 LUN 管理"
- "網管"
- "資料保護"
- "建立持續可用的 SMB 共享"

從 CLI 管理Cloud Volumes ONTAP

Cloud Volumes ONTAP CLI 讓您能夠執行所有管理命令，對於高階任務或您喜歡使用 CLI 來說，它是一個不錯的選擇。您可以使用安全外殼 (SSH) 連接到 CLI。

開始之前

使用 SSH 連線到Cloud Volumes ONTAP 的主機必須具有與Cloud Volumes ONTAP 的網路連線。例如，您可能需要從雲端供應商網路中的跳轉主機進行 SSH。

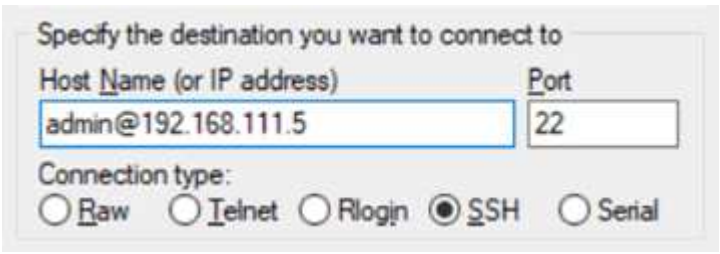
當部署在多個 AZ 中時， Cloud Volumes ONTAP HA 配置使用浮動 IP 位址作為叢集管理接口，這表示外部路由不可用。您必須從屬於相同路由域的主機進行連線。

步驟

1. 在NetApp Console中，確定叢集管理介面的 IP 位址：
   a. 從左側導覽功能表中，選擇“儲存”>“管理”。
   b. 在*系統*頁面上，選擇Cloud Volumes ONTAP系統。
   c. 複製右側窗格中顯示的叢集管理 IP 位址。
2. 使用 SSH 使用管理員帳戶連線到叢集管理介面 IP 位址。

   例子

   下圖顯示了使用 PuTTY 的範例：



3. 在登入提示字元下，輸入管理員帳戶的密碼。

例子

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

系統健康和事件

驗證Cloud Volumes ONTAP 的AutoSupport設置

AutoSupport主動監控系統的健康狀況並向NetApp技術支援發送訊息。預設情況下，每個節點上都啟用AutoSupport ，以使用 HTTPS 傳輸協定向技術支援發送訊息。最好驗證AutoSupport是否可以發送這些訊息。

唯一需要的設定步驟是確保Cloud Volumes ONTAP具有外部網路連線。有關詳細信息，請參閱您的雲端提供者的網路要求。

AutoSupport要求

Cloud Volumes ONTAP節點需要NetApp AutoSupport的出站互聯網存取權限，它可以主動監控系統的健康狀況並向NetApp技術支援發送訊息。

路由和防火牆策略必須允許 HTTPS 流量到達下列端點，以便Cloud Volumes ONTAP可以傳送AutoSupport訊息：

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

如果沒有可用的出站網路連線來傳送AutoSupport訊息， NetApp Console會自動設定您的Cloud Volumes ONTAP系統以使用控制台代理程式作為代理伺服器。唯一的要求是確保控制台代理的安全群組允許透過連接埠 3128 進行入站連線。部署控制台代理程式後，您需要開啟此連接埠。

如果您為Cloud Volumes ONTAP定義了嚴格的出站規則，那麼您還需要確保Cloud Volumes ONTAP安全群組允許透過連接埠 3128 進行出站連線。

如果您使用 HA 對，則 HA 中介不需要外部網路存取。

驗證出站網路存取可用後，您可以測試AutoSupport以確保它可以發送訊息。有關說明，請參閱 "ONTAP文檔：設定AutoSupport"。

排除AutoSupport配置故障

如果出站連線不可用，且控制台無法設定您的Cloud Volumes ONTAP系統以使用控制台代理程式作為代理伺服器，您將收到來自控制台的通知，提示您的系統無法傳送AutoSupport訊息。請依照以下步驟解決此問題。

步驟

1. 使用 SSH 安全地連接到Cloud Volumes ONTAP系統，以使用ONTAP CLI。

"了解如何透過 SSH 連線到Cloud Volumes ONTAP" 。

2. 查看AutoSupport子系統的詳細狀態：

```
autosupport check show-details
```

回覆內容如下：

```
    Category: smtp
          Component: mail-server
             Status: failed
             Detail: SMTP connectivity check failed for destination:
                     mailhost. Error: Could not resolve host -
'mailhost'
            Corrective Action: Check the hostname of the SMTP server

    Category: http-https
        Component: http-put-destination
            Status: ok
            Detail: Successfully connected to:
                    <https://support.netapp.com/put/AsupPut/>.

          Component: http-post-destination
             Status: ok
             Detail: Successfully connected to:

https://support.netapp.com/asupprod/post/1.0/postAsup.

    Category: on-demand
          Component: ondemand-server
             Status: ok
             Detail: Successfully connected to:
                     https://support.netapp.com/aods/asupmessage.

    Category: configuration
            Component: configuration
                Status: ok
                Detail: No configuration issues found.
    5 entries were displayed.
```

如果 http-https 類別的狀態是 OK 這表示AutoSupport已正確配置，可以發送訊息。

3. 否則，請驗證每個Cloud Volumes ONTAP節點的代理 URL：

```
autosupport show -fields proxy-url
```

4. 如果代理 URL 參數為空，請設定Cloud Volumes ONTAP以使用控制台代理作為代理：

```
autosupport modify -proxy-url http://<console agent private ip>:3128
```

5. 再次確認AutoSupport狀態：

   ```
   autosupport check show-details
   ```

6. 如果狀態仍然失敗，請驗證Cloud Volumes ONTAP和控制台代理之間是否透過連接埠建立連線。 `3128`。
7. 如果驗證後狀態仍然失敗，請透過 SSH 連線至控制台代理程式。

   "了解有關控制台代理連接到 Linux VM 的更多信息"

8. 前往 `/opt/application/netapp/cloudmanager/docker_occm/data/`。
9. 開啟代理設定檔 `squid.conf`。這是文件的結構：

   ```
   http_port 3128
   acl netapp_support dst support.netapp.com
   http_access allow netapp_support
   request_header_max_size 21 KB
   reply_header_max_size 21 KB
   http_access deny all
   httpd_suppress_version_string on
   ```

10. 如果您的檔案中沒有Cloud Volumes ONTAP系統的 CIDR 區塊條目，請新增條目並允許存取：

    ```
    acl cvonet src <cidr>

    http_access allow cvonet
    ```

    以下是一個例子：

    ```
    http_port 3128
    acl netapp_support dst support.netapp.com
    acl cvonet src <cidr>
    http_access allow netapp_support
    http_access allow cvonet
    request_header_max_size 21 KB
    reply_header_max_size 21 KB
    http_access deny all
    httpd_suppress_version_string on
    ```

11. 編輯設定檔後，重啟代理容器。 `sudo`。然後，根據您使用的是 Docker 還是 Podman，執行以下命令：

    對於 Docker，請運行 `docker restart squid`。

    如果您使用的是 Podman，請執行 `podman restart squid`。

12. 傳回ONTAP CLI 並驗證Cloud Volumes ONTAP是否可以傳送AutoSupport訊息：

```
autosupport check show-details
```

相關連結

- "AWS 中Cloud Volumes ONTAP的網路需求"
- "Azure 中Cloud Volumes ONTAP的網路需求"
- "Google Cloud 中Cloud Volumes ONTAP的網路需求"

為Cloud Volumes ONTAP系統設定 EMS

事件管理系統 (EMS) 收集並顯示有關ONTAP系統上發生的事件的資訊。若要接收事件通知，您可以為特定事件嚴重性設定事件目的地（電子郵件地址、SNMP 陷阱主機或系統日誌伺服器）和事件路由。

您可以使用 CLI 設定 EMS。有關說明，請參閱 "ONTAP文件：EMS 配置概述"。