使用Cloud Volumes ONTAP

Cloud Volumes ONTAP

NetApp
April 23, 2024

目錄

使用Cloud Volumes ONTAP

授權管理

管理容量型授權

從 BlueXP 數位錢包管理容量型授權、以確保您的 NetApp 帳戶擁有足夠的容量供 Cloud Volumes ONTAP 系統使用。

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

_BlueXP 數位錢包 _ 可讓您從單一位置管理 Cloud Volumes ONTAP 的授權。您可以新增授權並更新現有授權。

> 雖然 BlueXP 管理的產品和服務的實際使用量和計量都是以 GiB 和 TiB 計算、但是會交替使用「 GB/GiB 」和「 TB/TiB 」這兩個詞彙。這會反映在 Cloud Marketplace 清單、價格報價、上市說明及其他支援文件中

"深入瞭Cloud Volumes ONTAP 解不知如何取得授權"。

如何將授權新增至 **BlueXP** 數位錢包

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

在此期間、BlueXP會自動查詢NetApp的授權服務、以取得NetApp 支援網站 與您的帳戶相關之授權的詳細資料。如果沒有錯誤、 BlueXP 會自動將授權新增至數位錢包。

如果 BlueXP 無法新增授權、您必須自行手動將授權新增至數位錢包。例如、如果Connector安裝在無法存取網際網路的位置、您就必須自行新增授權。 瞭解如何將購買的授權新增至您的帳戶。

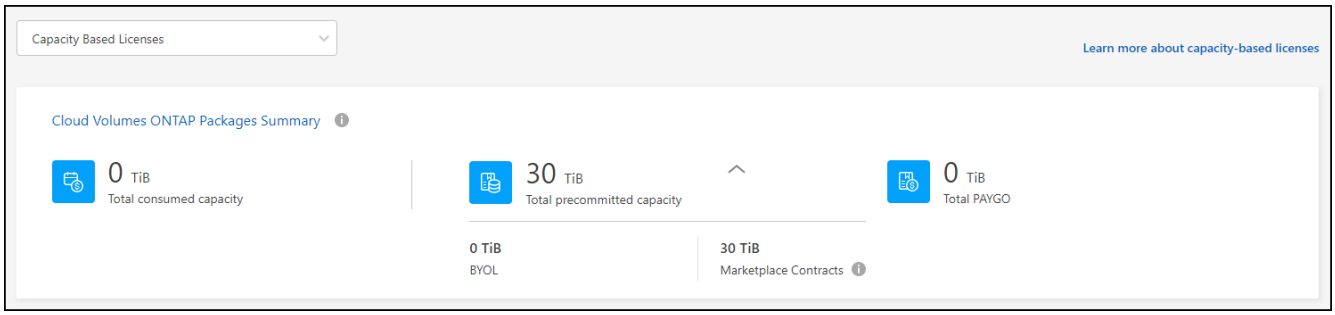
檢視您帳戶中的已用容量

BlueXP 數位錢包可顯示您帳戶的總使用容量、以及授權套件所耗用的容量。這有助於瞭解您的收費方式、以及您是否需要購買額外容量。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在 * Cloud Volumes ONTAP * 標籤上、選取 * 容量型授權 * 。
3. 檢視套件摘要、其中會顯示您已耗用的容量、預先認可的總容量和 PAYGO 總容量。
   - _總使用容量_是Cloud Volumes ONTAP NetApp帳戶中所有供應系統的總容量。無論磁碟區內的本機、已用、已儲存或有效空間為何、充電都是根據每個磁碟區的已配置大小而計算。
   - *Total preconted capacity* 是您從 NetApp 購買的總授權容量（ BYOL 或 Marketplace Contract ）。
   - _Total PAYGO_是使用雲端市場訂閱的已配置總容量。只有當使用容量高於授權容量、或 BlueXP 數位錢包中沒有 BYOL 授權時、才會使用 PAYGO 進行收費。

     以下是 BlueXP 數位錢包中 Cloud Volumes ONTAP 套件摘要的範例：



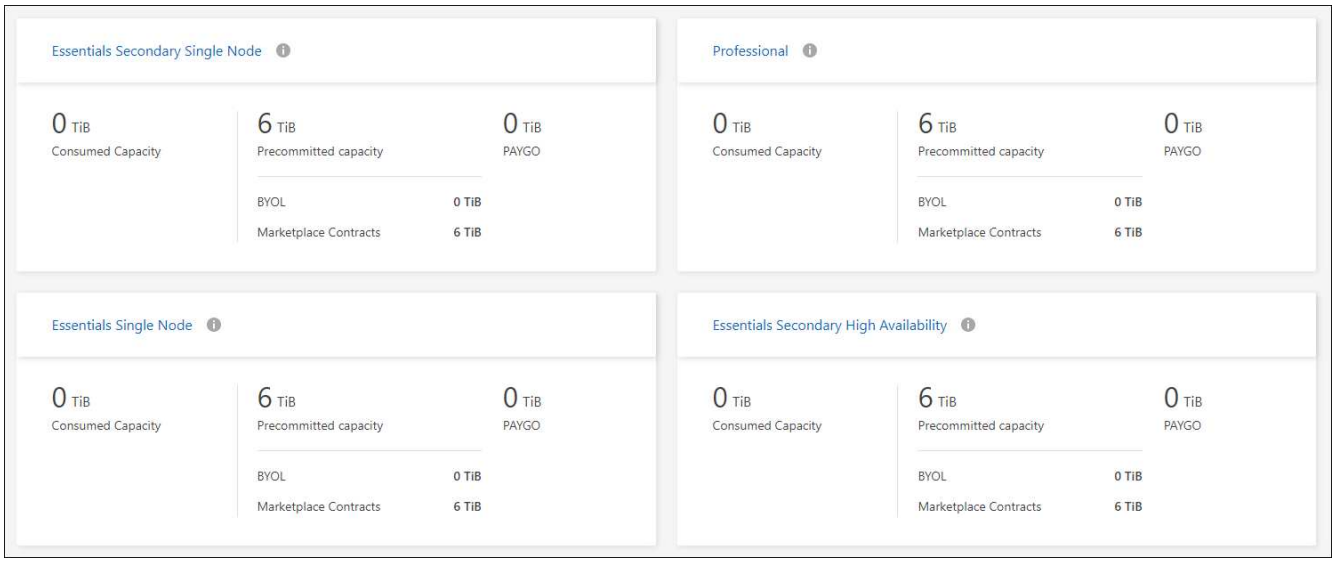
4. 在摘要下、檢視每個授權套件的耗用容量。

   - 耗用容量 _ 顯示該套件的磁碟區容量。如需特定套件的詳細資料、請將滑鼠游標移到工具提示上。

     若要更深入瞭解Essentials套件的顯示容量、您應該熟悉充電的運作方式。 "瞭解如何為Essentials套裝方案充電"。

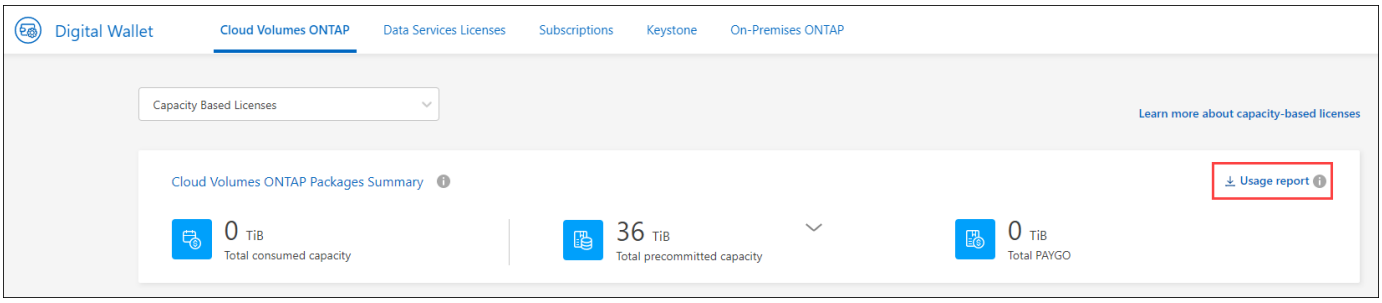
   - _ 預先承諾容量 _ 是您從 NetApp 購買的授權容量（BYOL 或 Marketplace 合約）。
     - *BYOL* 顯示您從 NetApp 購買的此套件類型的授權容量。
     - *Marketplace Contracts* 顯示您購買的此套件類型的市場合約授權容量。
   - *PAYGO* 會依授權使用模式顯示使用容量。

     以下是一個擁有多個授權套件的帳戶範例：



下載使用報告

帳戶管理員可以從 BlueXP 的數位錢包下載四份使用報告。這些使用報告會提供您訂閱的容量詳細資料、並告訴您如何為 Cloud Volumes ONTAP 訂閱中的資源收取費用。可下載的報告會在某個時間點擷取資料、並可輕鬆與他人共用。



以下報告可供下載。顯示的容量值以 TiB 為單位。

- * 高階使用率 * ：此報告會清楚顯示數位錢包中「 Cloud Volumes ONTAP 套件摘要」卡的內容。其中包括下列資訊：
  - 總使用容量
  - 預認可容量總計
  - BYOL 總容量
  - 市場總合約容量
  - PAYGO 總容量
- * Cloud Volumes ONTAP 套件使用 * ：此報告會清楚顯示數位錢包內的套裝卡片內容。除了最佳化的 I/O 套件外、其中包括每個套件的下列資訊：
  - 總使用容量
  - 預認可容量總計
  - BYOL 總容量
  - 市場總合約容量
  - PAYGO 總容量
- * 儲存虛擬機器使用率 * ：此報告顯示如何在 Cloud Volumes ONTAP 系統和儲存虛擬機器（ SVM ）之間分解已計費的容量。此資訊無法在數位錢包的任何畫面上取得。其中包括下列資訊：
  - 工作環境 ID 和名稱（顯示為 UUID ）
  - 雲端
  - NetApp 帳戶 ID
  - 工作環境組態
  - SVM名稱
  - 已配置的容量
  - 充電容量綜合報告
  - 市場帳單期限
  - Cloud Volumes ONTAP 套件或功能
  - 向 SaaS Marketplace 訂閱名稱收費
  - 向 SaaS Marketplace 訂閱 ID 收費
  - 工作負載類型

- * Volume 使用量 * ：此報告顯示如何在工作環境中、依磁碟區來分解收費容量。此資訊無法在數位錢包的任何畫面上取得。其中包括下列資訊：
  - 工作環境 ID 和名稱（顯示為 UUID ）
  - SVN 名稱
  - Volume ID
  - Volume類型
  - Volume 資源配置容量

> 此報告不包含 FlexClone Volume 、因為這些類型的磁碟區不會產生費用。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在 * Cloud Volumes ONTAP * 標籤上、選取 * 容量型授權 * 、然後按一下 * 使用報告 * 。

   使用報告會下載。

3. 開啟下載的檔案以存取報告。

將購買的授權新增至您的帳戶

如果您在 BlueXP 數位錢包中沒有看到購買的授權、則需要將授權新增至 BlueXP 、以便 Cloud Volumes ONTAP 可以使用該容量。

您需要的產品

- 您需要提供BlueXP授權或授權檔案的序號。
- 如果您要輸入序號、請先輸入 "將NetApp 支援網站 您的不更新帳戶新增至藍圖XP"。這是獲授權可以存取序號的 NetApp 支援網站帳戶。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在* Cloud Volumes ONTAP 《》索引標籤上、保留*容量型授權、然後按一下*新增授權*。
3. 輸入容量型授權的序號、或上傳授權檔案。

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

4. 按一下「 * 新增授權 * 」。

更新容量型授權

如果您購買額外容量或延長授權期限、 BlueXP 會自動更新數位錢包中的授權。您無需做任何事。

不過、如果您在無法存取網際網路的位置部署了BlueXP、則需要手動更新BlueXP中的授權。

您需要的產品

授權檔案（如果您有HA配對、則為_file_）。

如需如何取得授權檔案的詳細資訊、請參閱 "取得系統授權檔案"。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在* Cloud Volumes ONTAP 《》索引標籤上、按一下授權旁的動作功能表、然後選取*更新授權。
3. 上傳授權檔案。
4. 按一下*上傳授權*。

變更充電方法

容量型授權的形式為_package_。建立 Cloud Volumes ONTAP 工作環境時、您可以根據業務需求、從多個授權套件中選擇。如果您在建立工作環境之後需要變更、您可以隨時變更套件。例如、您可以將 Essentials 套件變更為專業版套件。

"深入瞭解容量型授權套件"。

關於這項工作

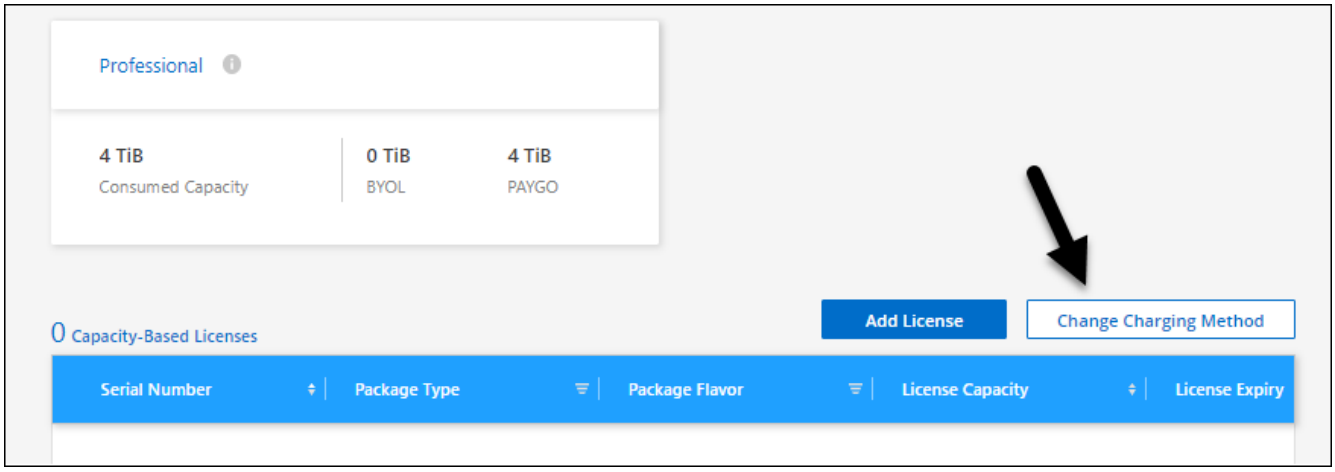
- 變更收費方式並不會影響您是透過從 NetApp （ BYOL ）購買的授權或雲端供應商的市場（隨用付費）收取費用。

  BlueXP 一律會先嘗試根據授權收費。如果沒有可用的授權、就會根據市場訂閱收費。BYOL 不需要「轉換」即可訂閱市場、反之亦然。

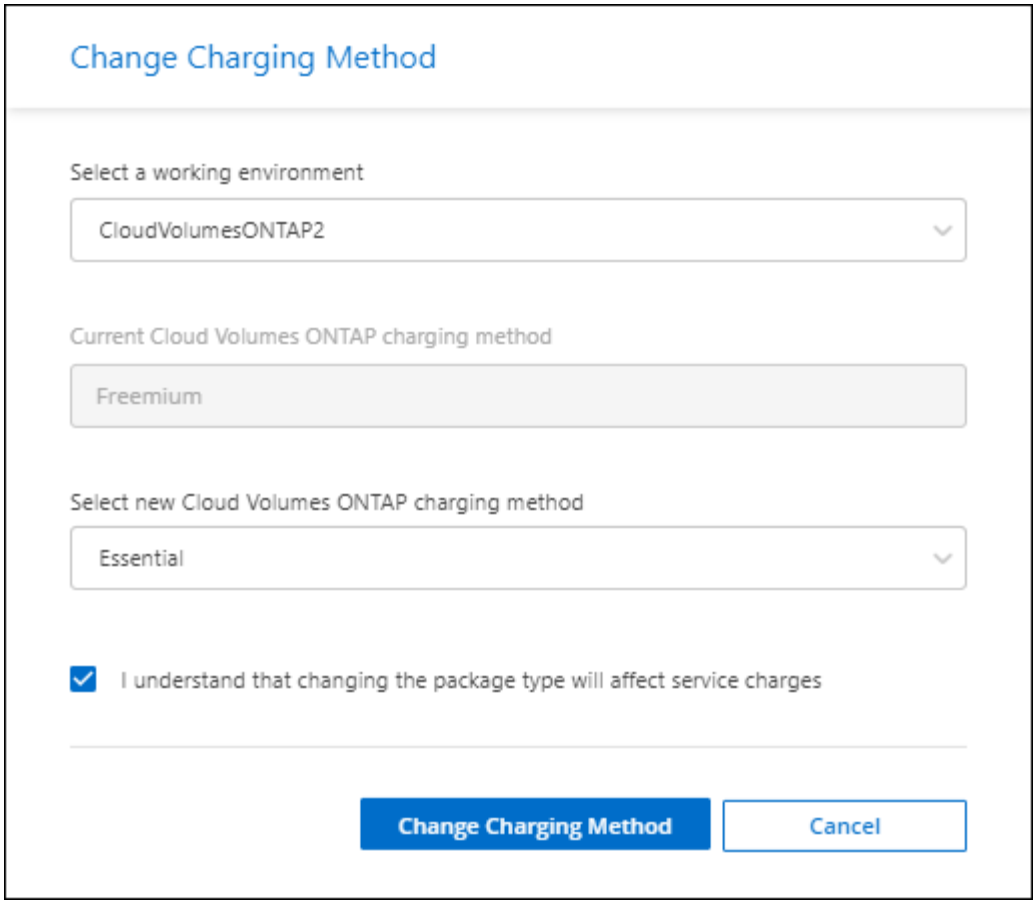
- 如果您有來自雲端供應商市場的私人優惠或合約、改用未包含在合約中的收費方法、將會導致依BYOL（如果您向NetApp購買授權）或PAYGO收取費用。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在* Cloud Volumes ONTAP 《》索引標籤上、按一下「*變更充電方法」。



3. 選取工作環境、選擇新的充電方法、然後確認您瞭解變更套件類型將會影響服務費用。



4. 按一下*變更收費方法*。

結果

BlueXP改變Cloud Volumes ONTAP 了這個系統的充電方法。

您可能也會注意到 BlueXP 數位錢包會重新整理每個套件類型的已用容量、以因應您剛做的變更。

移除容量型授權

如果容量型授權過期且不再使用、您可以隨時將其移除。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在* Cloud Volumes ONTAP 《》索引標籤上、按一下授權旁的動作功能表、然後選取*移除授權。
3. 按一下「 * 移除 * 」以確認。

管理 **Keystone** 訂閱

從 BlueXP 數位電子錢包管理 Keystone 訂閱、只要啟用 Cloud Volumes ONTAP 訂閱、並要求變更訂閱服務層級的承諾容量即可。為服務層級要求額外容量、可為內部部署 ONTAP 叢集或 Cloud Volumes ONTAP 系統提供更多儲存空間。

NetApp Keystone 是彈性的隨成長付費訂閱型服務、可為偏好營運成本而非資本支出或租賃的客戶、提供混合雲體驗。

"深入瞭解 Keystone"

授權您的帳戶

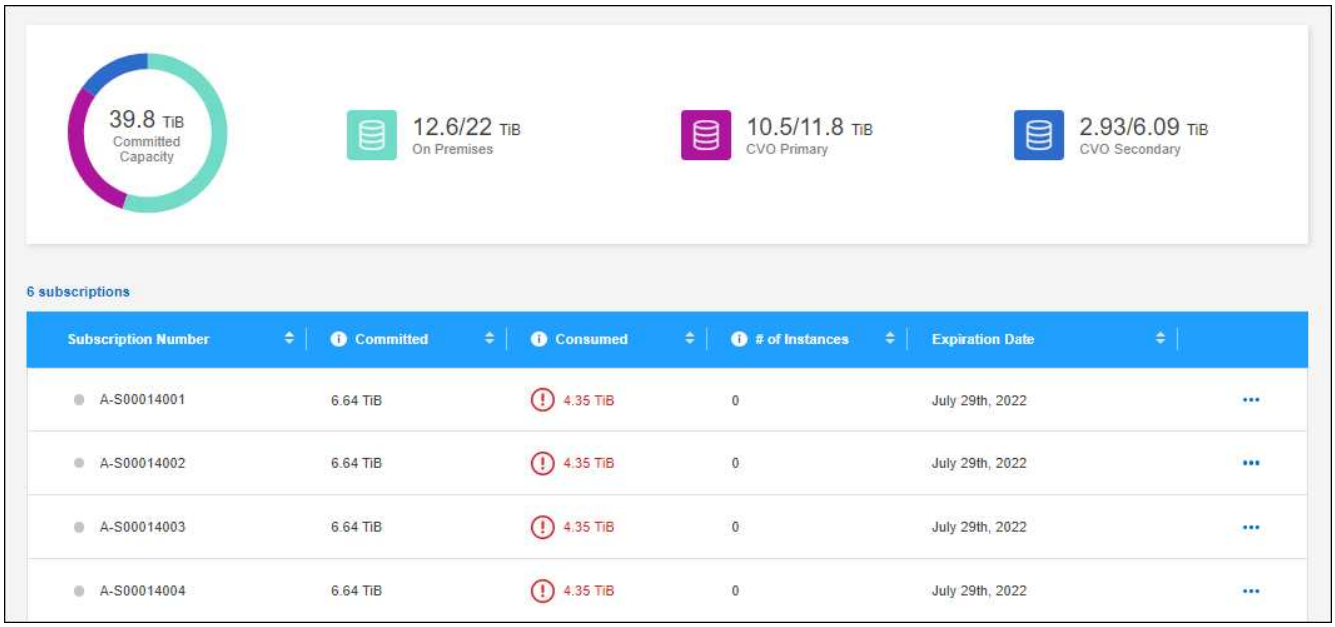
在 BlueXP 中使用和管理 Keystone 訂閱之前、您必須先聯絡 NetApp 、以授權您的 BlueXP 使用者帳戶使用 Keystone 訂閱。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 選取 * Keystone * 。
3. 如果您看到*歡迎使用NetApp Keystone S不到*頁面、請傳送電子郵件至頁面上所列的地址。

   NetApp代表將授權您的使用者帳戶存取訂閱、以處理您的申請。

4. 返回 * Keystone Subscription* 檢視您的訂閱。

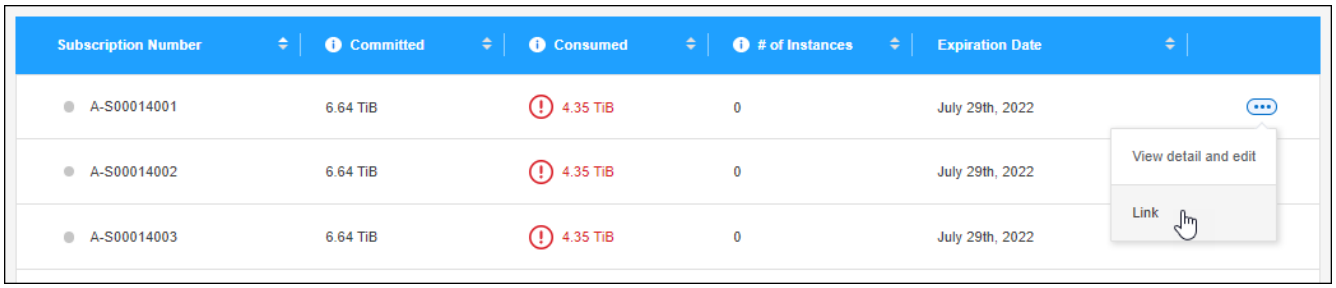


連結訂閱

NetApp 授權您的帳戶後、您可以連結 Keystone 訂閱以搭配 Cloud Volumes ONTAP 使用。此動作可讓使用者選擇訂閱做為新Cloud Volumes ONTAP 版的功能表系統的充電方法。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 選取 * Keystone * 。
3. 如需您要連結的訂閱、請按一下 ••• 然後選取*連結*。



結果

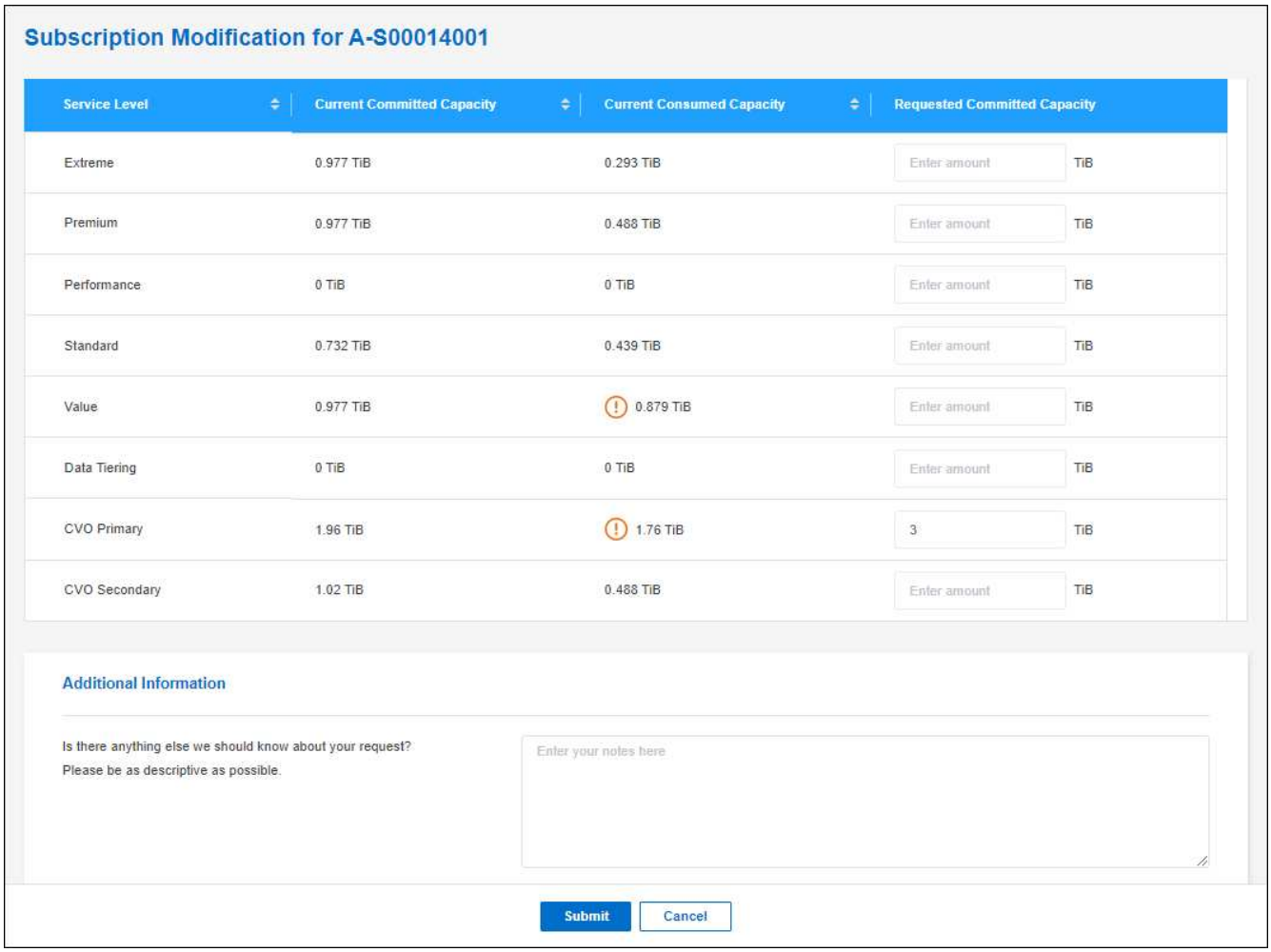
訂閱內容現已連結至您的BlueXP帳戶、可在建立Cloud Volumes ONTAP 運作環境時選擇。

申請更多或更少的已認可容量

如果您想要變更訂閱服務層級的認可容量、可以直接從 BlueXP 傳送要求至 NetApp 。為服務層級要求額外容量、可為內部部署叢集或 Cloud Volumes ONTAP 系統提供更多儲存空間。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 選取 * Keystone * 。
3. 如需調整容量的訂閱、請按一下 ••• 然後選取*檢視詳細資料並編輯*。
4. 輸入一或多個訂閱所需的已提交容量。



5. 向下捲動、輸入申請的任何其他詳細資料、然後按一下*提交*。

結果

您的申請會在NetApp系統中建立Ticket以供處理。

監控使用率

BlueXP 數位顧問儀表板可讓您監控 Keystone 訂閱使用量並產生報告。

"深入瞭解監控訂閱使用率"

取消訂閱連結

如果您不想再使用 Keystone Subscription with BlueXP 、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 的訂閱內容的訂閱。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 選取 * Keystone * 。
3. 若要取消連結訂閱、請按一下 ••• 然後選取*取消連結*。

結果

訂閱內容會從您的BlueXP帳戶中取消連結、因此在建立Cloud Volumes ONTAP 運作中的環境時無法再選取。

管理節點型授權

在 BlueXP 數位錢包中管理節點型授權、以確保每個 Cloud Volumes ONTAP 系統都擁有具有所需容量的有效授權。

_Node型授權_是前一代授權模式（不適用於新客戶）：

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

_BlueXP 數位錢包 _ 可讓您從單一位置管理 Cloud Volumes ONTAP 的授權。您可以新增授權並更新現有授權。

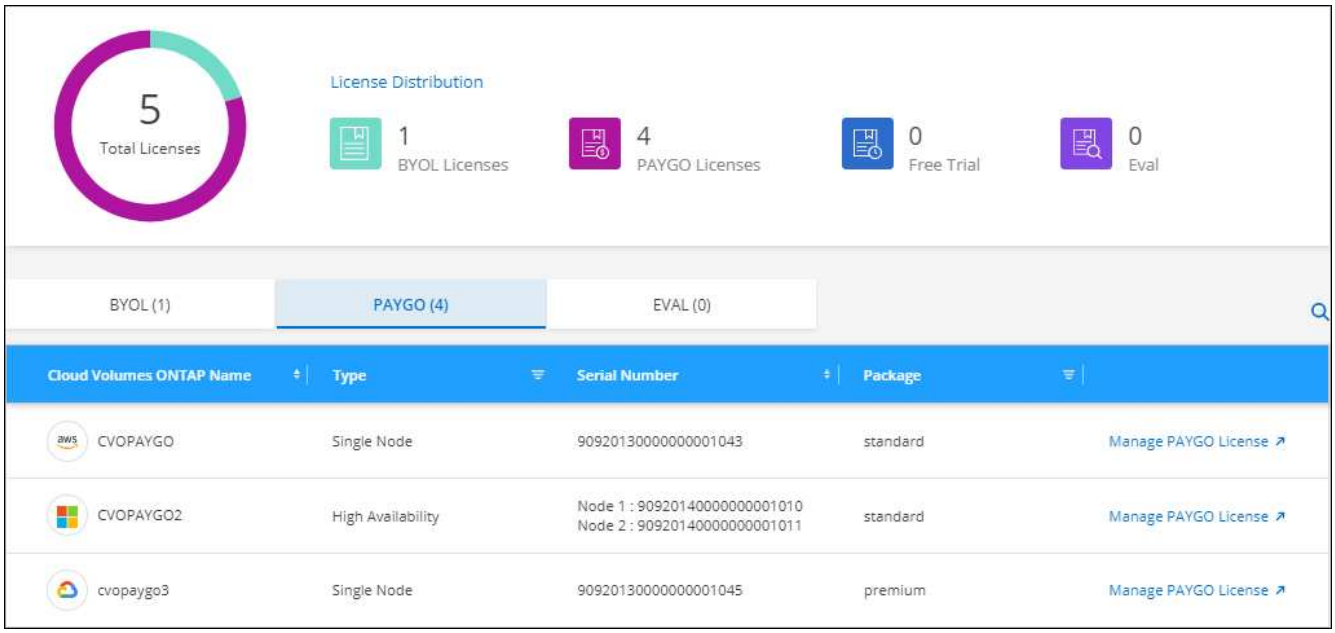
"深入瞭Cloud Volumes ONTAP 解不知如何取得授權"。

管理**PAYGO**授權

BlueXP 數位錢包頁面可讓您檢視每個 PAYGO Cloud Volumes ONTAP 系統的詳細資料、包括序號和 PAYGO 授權類型。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在* Cloud Volumes ONTAP 《》*索引標籤上、從下拉式清單中選取「*節點型授權」。
3. 按一下* PAYGO*。
4. 請在表格中檢視每個PAYGO授權的詳細資料。



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

管理 **BYOL** 授權

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

新增未指派的授權

將節點型授權新增至 BlueXP 數位錢包、以便在建立新的 Cloud Volumes ONTAP 系統時選取授權。數位錢包會將這些授權識別為 *disally*.

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在* Cloud Volumes ONTAP 《》*索引標籤上、從下拉式清單中選取「*節點型授權」。
3. 按一下*未指派*。
4. 按一下「新增未指派的授權」。
5. 輸入授權的序號或上傳授權檔案。

   如果您還沒有授權檔案、請參閱下列章節。

6. 按一下「 * 新增授權 * 」。

結果

BlueXP 將授權新增至數位錢包。授權將被識別為未指派、直到您將其與新Cloud Volumes ONTAP 的一套系統關聯為止。之後、授權便會移至數位錢包中的 * BYOL* 標籤。

Exchange未指派的節點型授權

如果您尚未使用未指派的 Cloud Volumes ONTAP 節點型授權、則可將授權轉換為 BlueXP 備份與還原授權、BlueXP 分類授權或 BlueXP 分層授權、以交換授權。

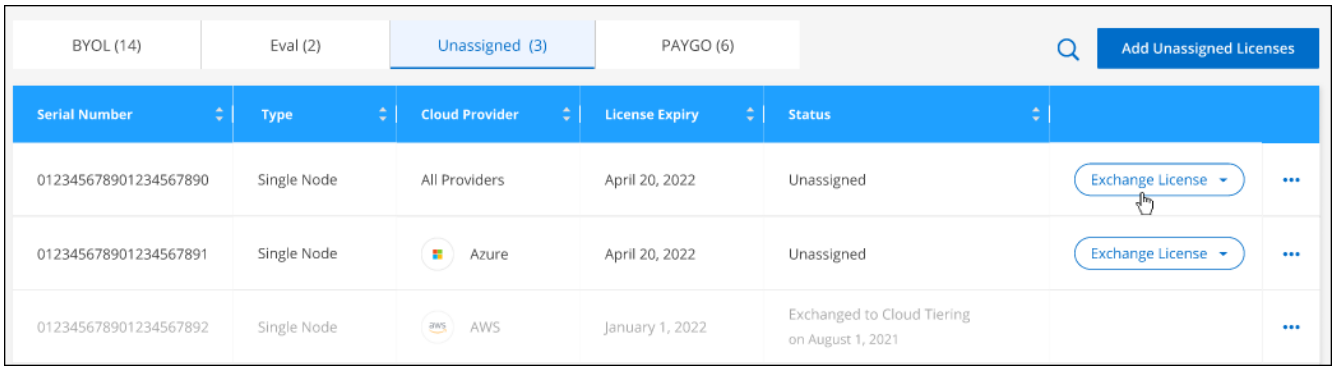
交換授權會撤銷Cloud Volumes ONTAP 該服務的不含美元的授權、並為該服務建立相當於美元的授權：

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

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

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在* Cloud Volumes ONTAP 《》*索引標籤上、從下拉式清單中選取「*節點型授權」。
3. 按一下*未指派*。
4. 按一下「* Exchange授權*」。



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

結果

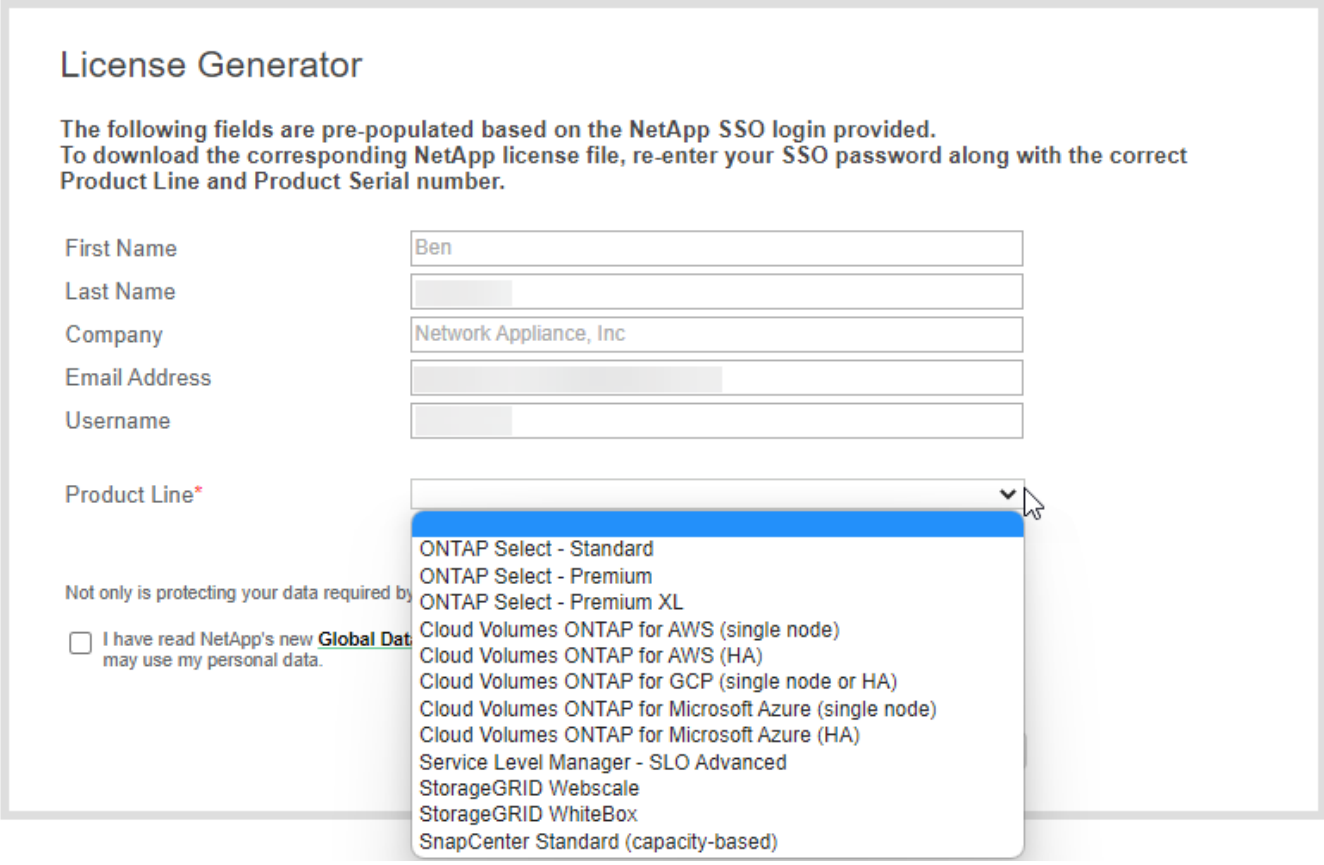
BlueXP會將未指派的授權轉換成您選取的服務。您可以在「資料服務授權」標籤中檢視新授權。

取得系統授權檔案

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

步驟

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



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

更新系統授權

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

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

步驟

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

結果

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

管理額外容量授權

您可以購買Cloud Volumes ONTAP 額外容量授權給某個不含BYOL的系統、以配置超過368TiB的BYOL系統授

權容量。例如、您可以購買一個額外的授權容量、以配置多達736 TiB的容量來Cloud Volumes ONTAP 供使用。或者、您也可以購買三份額外容量授權、最多可取得1.4 PIB。

單一節點系統或 HA 配對可購買的授權數量不受限制。

新增容量授權

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

步驟

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

更新容量授權

如果您延長額外容量授權的期限、則需要更新BlueXP中的授權。

步驟

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

移除容量授權

如果額外的容量授權過期且不再使用、您可以隨時將其移除。

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在* Cloud Volumes ONTAP 《》*索引標籤上、從下拉式清單中選取「*節點型授權」。
3. 在「* BYOL*」標籤中、展開Cloud Volumes ONTAP 關於某個系統的詳細資料。
4. 按一下容量授權旁的動作功能表、然後選取*移除授權*。
5. 按一下「移除」。

將試用版授權轉換為**BYOL**

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

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

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

步驟

1. 從BlueXP導覽功能表中、選取*管理>數位錢包*。
2. 在* Cloud Volumes ONTAP 《》*索引標籤上、從下拉式清單中選取「*節點型授權」。
3. 按一下* Eval*。
4. 在表格中、按一下*「轉換成BYOL授權*」以取得Cloud Volumes ONTAP 一套系統。
5. 輸入序號或上傳授權檔案。
6. 按一下*「轉換授權*」。

結果

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

在**PAYGO**和**BYOL**之間切換

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

步驟

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

   "瞭解如何在系統之間複寫資料"

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

   "瞭解如何刪除Cloud Volumes ONTAP 功能不正常的工作環境"。

Volume與LUN管理

建立**FlexVol** 功能區

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

BlueXP提供多種建立新磁碟區的方法：

- 指定新磁碟區的詳細資料、讓BlueXP為您處理基礎資料集合體。 深入瞭解
- 在您選擇的資料集合體上建立磁碟區。 深入瞭解
- 在HA組態的第二個節點上建立磁碟區。 深入瞭解

開始之前

關於Volume資源配置的幾點注意事項：

- 建立iSCSI磁碟區時、BlueXP會自動為您建立LUN。我們只要在每個磁碟區建立一個 LUN 、就能輕鬆完成工作、因此不需要管理。建立磁碟區之後、 "使用 IQN 從主機連線至 LUN"。
- 您可以從 System Manager 或 CLI 建立其他 LUN 。
- 如果您想在 AWS 中使用 CIFS 、則必須設定 DNS 和 Active Directory 。如需詳細資訊、請參閱 "AWS 的 Cloud Volumes ONTAP 網路需求"。
- 如果Cloud Volumes ONTAP 您的支援Amazon EBS彈性Volume功能的組態、您可能會想要 "深入瞭解建立Volume時會發生什麼事"。

建立**Volume**

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

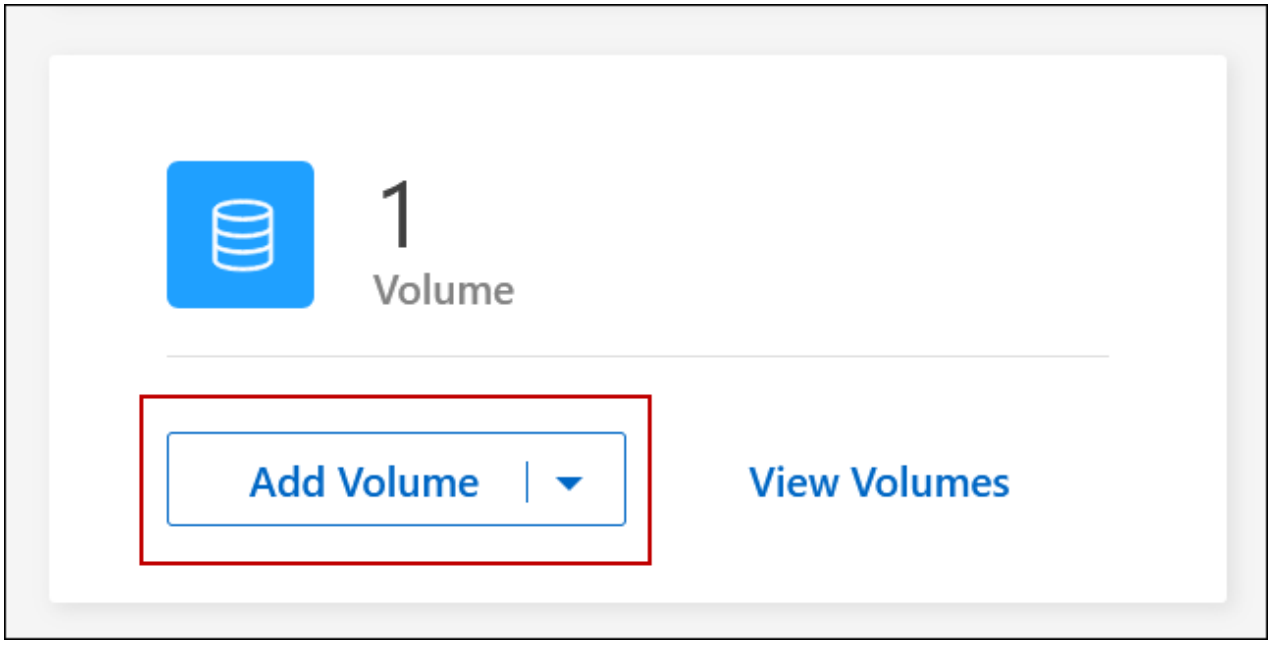
步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按兩下Cloud Volumes ONTAP 您要在其中配置FlexVol 一份「功能區」的「功能區」系統名稱。
3. 請讓BlueXP為您處理磁碟配置、或為磁碟區選擇特定的集合體、以建立新的磁碟區。

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

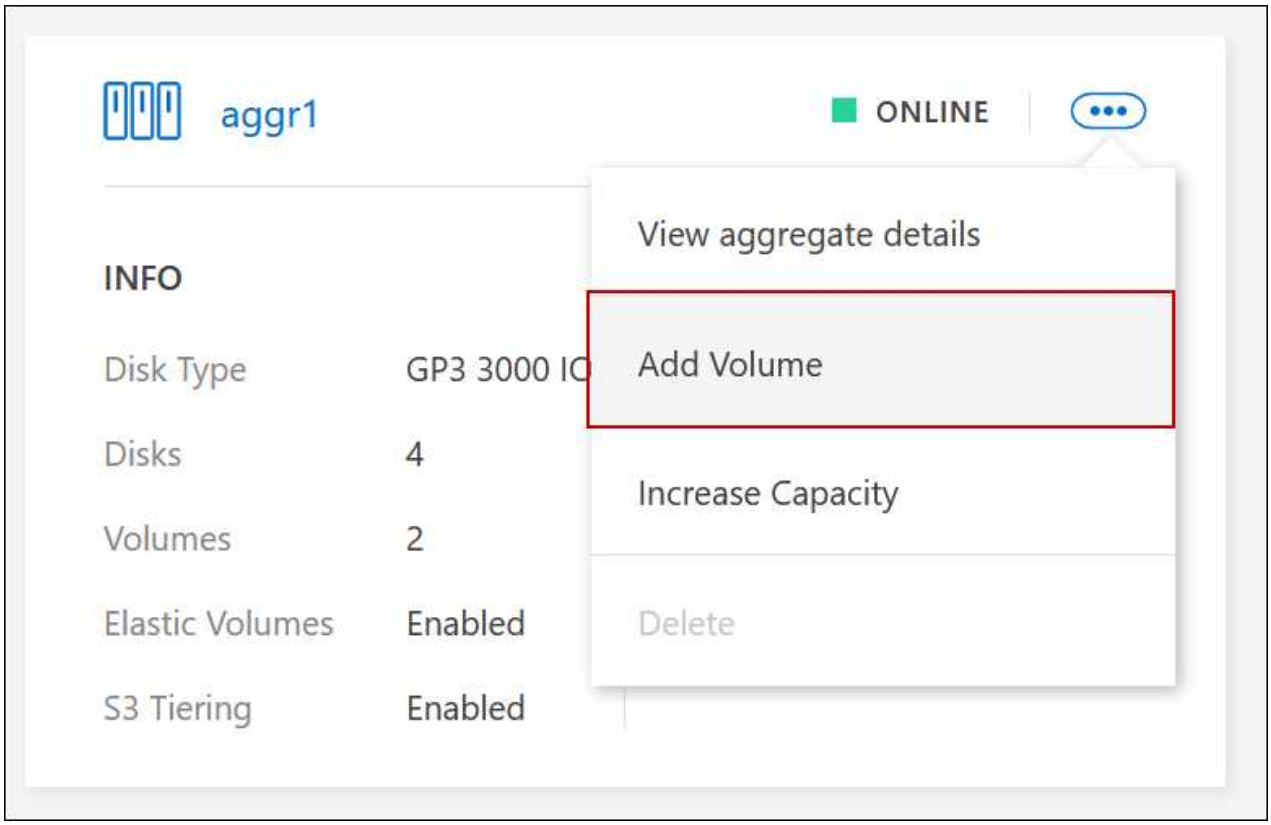
任何**Aggregate**

在「概觀」標籤上、瀏覽至「 Volume 」磚、然後按一下「 * 新增 Volume * 」。



特定**Aggregate**

在 Aggregate 索引標籤上、瀏覽至所需的 Aggregate 動態磚。按一下功能表圖示、然後按一下 * 新增 Volume * 。



4. 依照精靈中的步驟建立磁碟區。

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

      此頁面上的部分欄位是不知自明的。下列清單說明您可能需要指引的欄位：

欄位	說明
Volume名稱	您可以為新磁碟區輸入的可識別名稱。
Volume大小	您可以輸入的最大大小、主要取決於您是否啟用精簡配置、這可讓您建立比目前可用實體儲存容量更大的磁碟區。
儲存 VM （ SVM ）	儲存虛擬機器是 ONTAP 執行於支援內部的虛擬機器、可為您的用戶端提供儲存與資料服務。您可能知道這是 SVM 或 Vserver 。根據預設、系統會設定一個儲存 VM 、但部分組態會支援額外的儲存 VM 。 Cloud Volumes ONTAP 您可以為新的 Volume 指定儲存 VM 。
Snapshot 原則	Snapshot 複製原則會指定自動建立的 NetApp Snapshot 複本的頻率和數量。NetApp Snapshot 複本是一種不影響效能的時間點檔案系統映像、需要最少的儲存容量。您可以選擇預設原則或無。您可以針對暫時性資料選擇「無」：例如、 Microsoft SQL Server 的 Tempdb 。

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

      如果您選取CIFS、但未設定伺服器、則在您按一下*「下一步」*之後、BlueXP會提示您設定CIFS連線功能。

      "瞭解支援的用戶端傳輸協定和版本"。

      以下各節將說明您可能需要指引的欄位。說明會依傳輸協定加以組織。

NFS

存取控制

選擇自訂匯出原則、讓用戶端可以使用磁碟區。

匯出原則

定義子網路中可存取磁碟區的用戶端。根據預設、BlueXP會輸入一個值、以供存取子網路中的所有執行個體。

CIFS

權限與使用者/群組

可讓您控制使用者和群組存取SMB共用區的層級（也稱為存取控制清單或ACL）。您可以指定本機或網域 Windows 使用者或群組、或 UNIX 使用者或群組。如果您指定網域Windows使用者名稱、則必須使用網域\使用者名稱格式來包含使用者的網域。

DNS 主要和次要 **IP** 位址

提供 CIFS 伺服器名稱解析的 DNS 伺服器 IP 位址。列出的 DNS 伺服器必須包含所需的服務位置記錄（ SRV), 才能找到 CIFS 伺服器要加入之網域的 Active Directory LDAP 伺服器和網域控制器。

如果您要設定Google Managed Active Directory、AD預設可透過169.254.169.254 IP位址存取。

要加入的 **Active Directory** 網域

您要 CIFS 伺服器加入之 Active Directory （ AD ）網域的 FQDN 。

授權加入網域的認證資料

具有足夠權限的 Windows 帳戶名稱和密碼、可將電腦新增至 AD 網域內的指定組織單位（ OU ）。

CIFS 伺服器 **NetBios** 名稱

AD 網域中唯一的 CIFS 伺服器名稱。

組織單位

AD 網域中與 CIFS 伺服器相關聯的組織單位。預設值為「 CN= 電腦」。

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

DNS 網域

適用於整個儲存虛擬 Cloud Volumes ONTAP 機器（ SVM ）的 DNS 網域。在大多數情況下、網域與 AD 網域相同。

NTP 伺服器

選擇 * 使用 Active Directory 網域 * 來使用 Active Directory DNS 設定 NTP 伺服器。如果您需要使用不同的位址來設定 NTP 伺服器、則應該使用 API 。請參閱 "藍圖XP自動化文件" 以取得詳細資料。

請注意、您只能在建立CIFS伺服器時設定NTP伺服器。您建立CIFS伺服器之後、就無法進行設定。

iSCSI

LUN

iSCSI 儲存目標稱為 LUN （邏輯單元）、以標準區塊裝置的形式呈現給主機。建立iSCSI磁碟區時、BlueXP會自動為您建立LUN。我們只要在每個磁碟區建立一個LUN、就能輕鬆完成工作、因此不需要管理。建立磁碟區之後、 "使用 IQN 從主機連線至 LUN"。

啟動器群組

啟動器群組（igroup）指定哪些主機可以存取儲存系統上的指定LUN

主機啟動器（**IQN**）

iSCSI 目標可透過標準乙太網路介面卡（ NIC ）、 TCP 卸載引擎（ TOE ）卡（含軟體啟動器）、整合式網路介面卡（ CNA ）或專用主機匯流排介面卡（ HBA ）連線至網路、並由 iSCSI 合格名稱（ IQN ）識別。

a. 磁碟類型：根據您的效能需求和成本需求、為磁碟區選擇基礎磁碟類型。
   - "在 AWS 中調整系統規模"
     - "在 Azure 中調整系統規模"
     - "在Google Cloud中調整系統規模"

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

   包含多項儲存效率功能、可減少您所需的總儲存容量。 ONTAPNetApp 儲存效率功能提供下列效益：

   資源隨需配置

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

   重複資料刪除

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

   壓縮

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

6. 審查：檢閱磁碟區的詳細資料、然後按一下*新增*。

結果

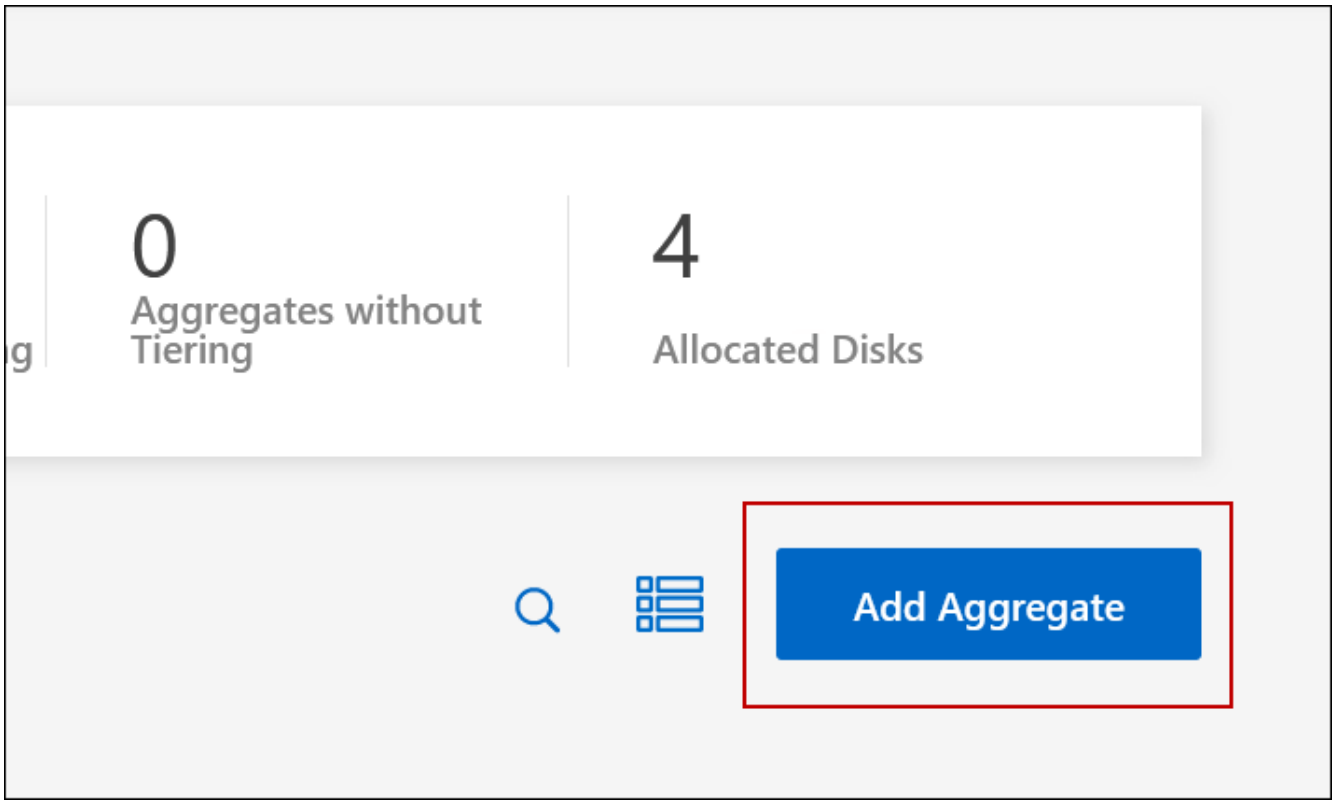
BlueXP會在Cloud Volumes ONTAP 整個系統上建立磁碟區。

在**HA**組態的第二個節點上建立磁碟區

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

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按兩下 Cloud Volumes ONTAP 您要管理集合體的運作環境名稱。
3. 在 Aggregate 索引標籤上、按一下 * 新增 Aggregate * 。
4. 從 _ 新增 Aggregate _ 畫面建立 Aggregate 。



5. 對於主節點、請在 HA 配對中選擇第二個節點。
6. 在BlueXP建立Aggregate之後、選取該集合體、然後按一下「*建立Volume *」。
7. 輸入新磁碟區的詳細資料、然後按一下「 * 建立 * 」。

結果

BlueXP會在HA配對的第二個節點上建立磁碟區。

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

建立**Volume**之後

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

如果要將配額套用至磁碟區、則必須使用 System Manager 或 CLI 。配額可讓您限制或追蹤使用者、群組或 qtree 所使用的磁碟空間和檔案數量。

管理現有磁碟區

BlueXP可讓您管理磁碟區和CIFS伺服器。它也會提示您移動磁碟區、以避免發生容量問題。

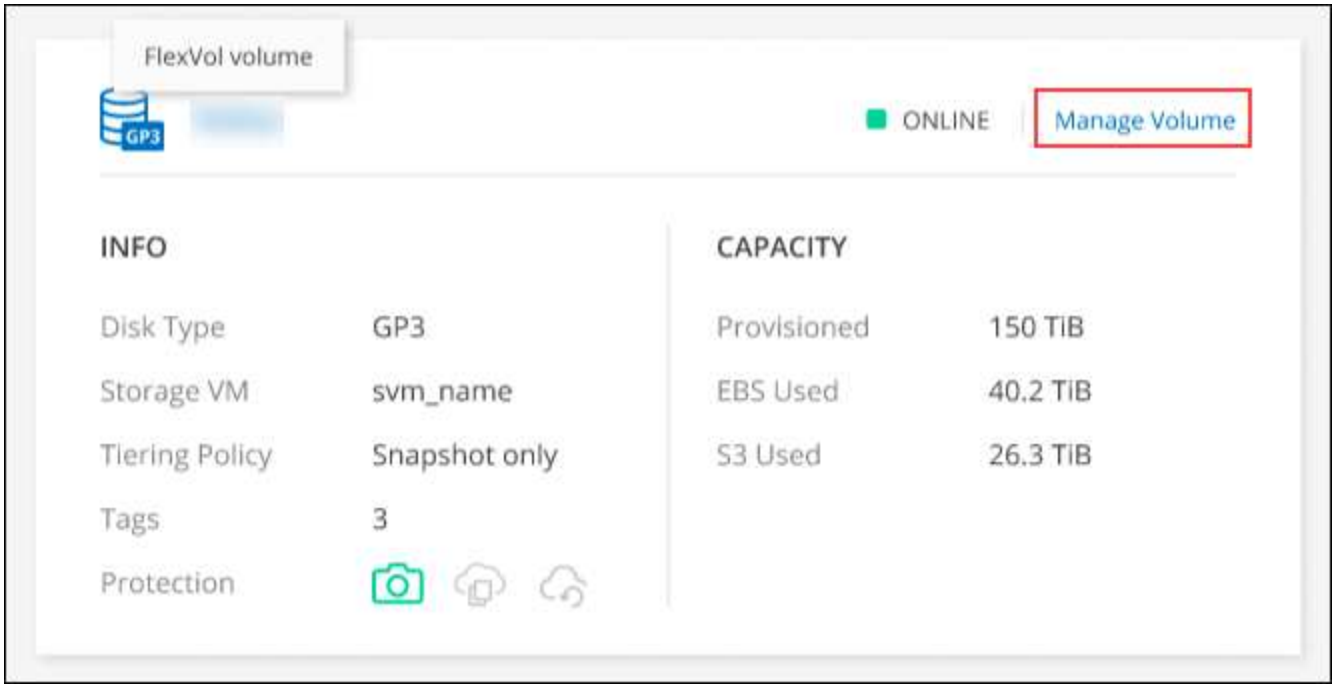
您可以在 BlueXP 標準檢視或進階檢視中管理磁碟區。「標準檢視」提供一組有限的選項來修改您的磁碟區。進階檢視提供進階管理層級、例如複製、調整大小、變更反勒索軟體的設定、分析、保護和活動追蹤、以及跨階層移動磁碟區。請參閱 "使用進階檢視來管理Cloud Volumes ONTAP"。

管理磁碟區

透過 BlueXP 標準檢視、您可以根據儲存需求來管理磁碟區。您可以檢視、編輯、複製、還原及刪除磁碟區。

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按兩下 Cloud Volumes ONTAP 您要管理磁碟區的「功能區」工作環境。
3. 在工作環境中、按一下 * Volumes （磁碟區） * 標籤。



4. 在 Volumes （磁碟區）索引標籤上、瀏覽至所需的磁碟區標題、然後按一下 * Manage Volumes （管理磁碟區） * 以存取 Manage Volumes （管理磁碟區）右側面板。

工作	行動
檢視磁碟區的相關資訊	在「管理磁碟區」面板的「 Volume Actions 」（ Volume 動作）下、按一下「 * 檢視磁碟區詳細資料 * 」

工作	行動
取得 NFS 掛載命令	a. 在「管理磁碟區」面板的「 Volume Actions 」（ Volume 動作）下、按一下「 * 掛載命令 * 」。 b. 按一下 * 複本 * 。
複製磁碟區	a. 在「管理磁碟區」面板的「 Volume Actions 」（磁碟區動作）下、按一下「 * Clone the volume * 」（ b. 視需要修改複本名稱、然後按一下 * Clone （複製） * 。 此程序會建立 FlexClone Volume 。FlexClone Volume 是可寫入的時間點複本、空間效率極高、因為它會使用少量的空間作為中繼資料、然後只會在資料變更或新增時耗用額外空間。 若要深入瞭解 FlexClone Volume 、請參閱 "《 9 邏輯儲存管理指南》ONTAP"。
編輯磁碟區（僅限讀寫磁碟區）	a. 在「管理磁碟區」面板的「 Volume Actions 」（磁碟區動作）下、按一下 * 「 Edit Volume settings* 」（ b. 修改磁碟區的 Snapshot 原則、 NFS 傳輸協定版本、 NFS 存取控制清單（匯出原則）或共用權限、然後按一下 * 套用 * 。 ⓘ 如果您需要自訂 Snapshot 原則、可以使用 System Manager 來建立。
刪除 Volume	a. 在「管理磁碟區」面板的「 Volume Actions 」（磁碟區動作）下、按一下「 * 刪除磁碟區 * 」 b. 在「刪除 Volume 」視窗下、輸入您要刪除的 Volume 名稱。 c. 再按一下 * 刪除 * 以確認。
隨需建立 Snapshot 複本	a. 在「管理磁碟區」面板的「保護動作」下、按一下 * 建立 Snapshot 複本 * 。 b. 視需要變更名稱、然後按一下「 * 建立 * 」。
將資料從 Snapshot 複本還原至新的 Volume	a. 在「管理磁碟區」面板的「保護動作」下、按一下 * 從 Snapshot 複本還原 * 。 b. 選取 Snapshot 複本、輸入新磁碟區的名稱、然後按一下 * 還原 * 。
變更基礎磁碟類型	a. 在「管理磁碟區」面板的「進階動作」下、按一下 * 變更磁碟類型 * 。 b. 選取磁碟類型、然後按一下 * 變更 * 。 ⓘ BlueXP會將磁碟區移至使用所選磁碟類型的現有Aggregate、或為磁碟區建立新的Aggregate。

工作	行動
變更分層原則	a. 在「管理磁碟區」面板的「進階動作」下、按一下 * 變更階層原則 * 。 b. 選取不同的原則、然後按一下 * 變更 * 。 BlueXP會將磁碟區移至現有的Aggregate、該集合體使用所選的磁碟類型進行分層、或是為磁碟區建立新的Aggregate。
刪除 Volume	a. 選取磁碟區、然後按一下 * 刪除 * 。 b. 在對話方塊中輸入磁碟區的名稱。 c. 再按一下 * 刪除 * 以確認。

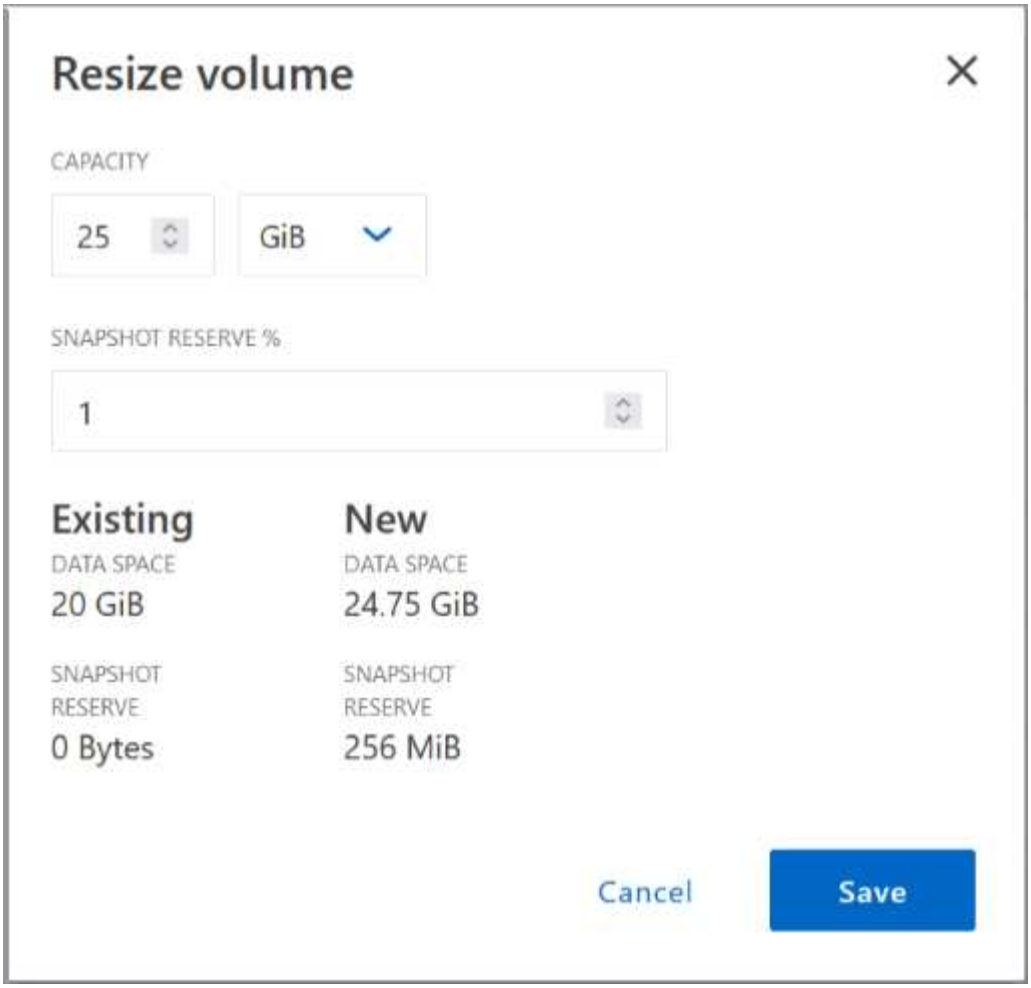
調整磁碟區大小

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

如果您需要調整磁碟區大小、可以從 BlueXP 的「進階檢視」進行調整。

步驟

1. 開啟「進階檢視」、透過 System Manager 調整磁碟區大小。請參閱 "如何開始使用"。
2. 從左側導覽功能表中、選取 * 儲存 > 磁碟區 * 。
3. 從磁碟區清單中、找出您應該調整大小的磁碟區。
4. 按一下選項圖示 ⋮ 。
5. 選取 * 調整大小 * 。
6. 在 * 調整 Volume 大小 * 畫面上、視需要編輯容量和 Snapshot 保留百分比。您可以將現有的可用空間與修改後的容量進行比較。
7. 按一下「 * 儲存 * 」。



調整磁碟區大小時、請務必將系統的容量限制列入考量。前往 "發行說明 Cloud Volumes ONTAP" 以取得更多詳細資料。

修改**CIFS**伺服器

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

步驟

1. 在工作環境的「總覽」標籤中、按一下右側面板下方的「功能」標籤。
2. 在 "CIFS Setup （ CIFS 設置） " 字段下，單擊 *p鉛筆 圖標 * 以顯示 "CIFS Setup （ CIFS 設置） " 窗口。
3. 指定 CIFS 伺服器的設定：

工作	行動
選取儲存 VM （ SVM ）	選取 Cloud Volume ONTAP 儲存虛擬機器（ SVM ） 會顯示其已設定的 CIFS 資訊。
要加入的 Active Directory 網域	您要 CIFS 伺服器加入之 Active Directory （ AD ） 網域的 FQDN 。
授權加入網域的認證資料	具有足夠權限的 Windows 帳戶名稱和密碼、可將電腦新增至 AD 網域內的指定組織單位（ OU ）。

工作	行動
DNS 主要和次要 IP 位址	提供 CIFS 伺服器名稱解析的 DNS 伺服器 IP 位址。列出的 DNS 伺服器必須包含所需的服務位置記錄（SRV), 才能找到 CIFS 伺服器要加入之網域的 Active Directory LDAP 伺服器和網域控制器。ifdef：：GCP[]如果您正在設定Google Managed Active Directory、則AD預設可透過169.254.169.254 IP位址存取。endif::GCP[]
DNS 網域	適用於整個儲存虛擬 Cloud Volumes ONTAP 機器（SVM）的 DNS 網域。在大多數情況下、網域與 AD 網域相同。
CIFS 伺服器 NetBios 名稱	AD 網域中唯一的 CIFS 伺服器名稱。
組織單位	AD 網域中與 CIFS 伺服器相關聯的組織單位。預設值為「CN= 電腦」。 • 若要將AWS託管Microsoft AD設定為Cloud Volumes ONTAP AD伺服器以供使用、請在此欄位中輸入* OID=computers,O=corp*。 • 若要將Azure AD網域服務設定為Cloud Volumes ONTAP AD伺服器以供使用、請在此欄位中輸入* OID=AADDC computers*或* OID=AADDC使用者*。"Azure 說明文件：在 Azure AD 網域服務託管網域中建立組織單位（OU）" • 若要將Google託管Microsoft AD設定為Cloud Volumes ONTAP AD伺服器以供使用、請在此欄位中輸入* OU=computers,OU=Cloud *。"Google Cloud文件：Google託管Microsoft AD的組織單位"

4. 按一下 * 設定 * 。

結果

利用變更更新 CIFS 伺服器。 Cloud Volumes ONTAP

移動Volume

移動磁碟區以提高容量使用率、改善效能、並達成服務層級協議。

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

步驟

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

   在大多數情況下、您可以使用 System Manager 來移動磁碟區。

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

當BlueXP顯示「需要採取行動」訊息時、請移動磁碟區

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

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

步驟

1. [找出如何修正容量問題]。
2. 根據您的分析、移動磁碟區以避免容量問題：
   - [將磁碟區移至其他系統、以避免發生容量問題]。
   - 將磁碟區移至其他Aggregate、以避免容量問題。

找出如何修正容量問題

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

步驟

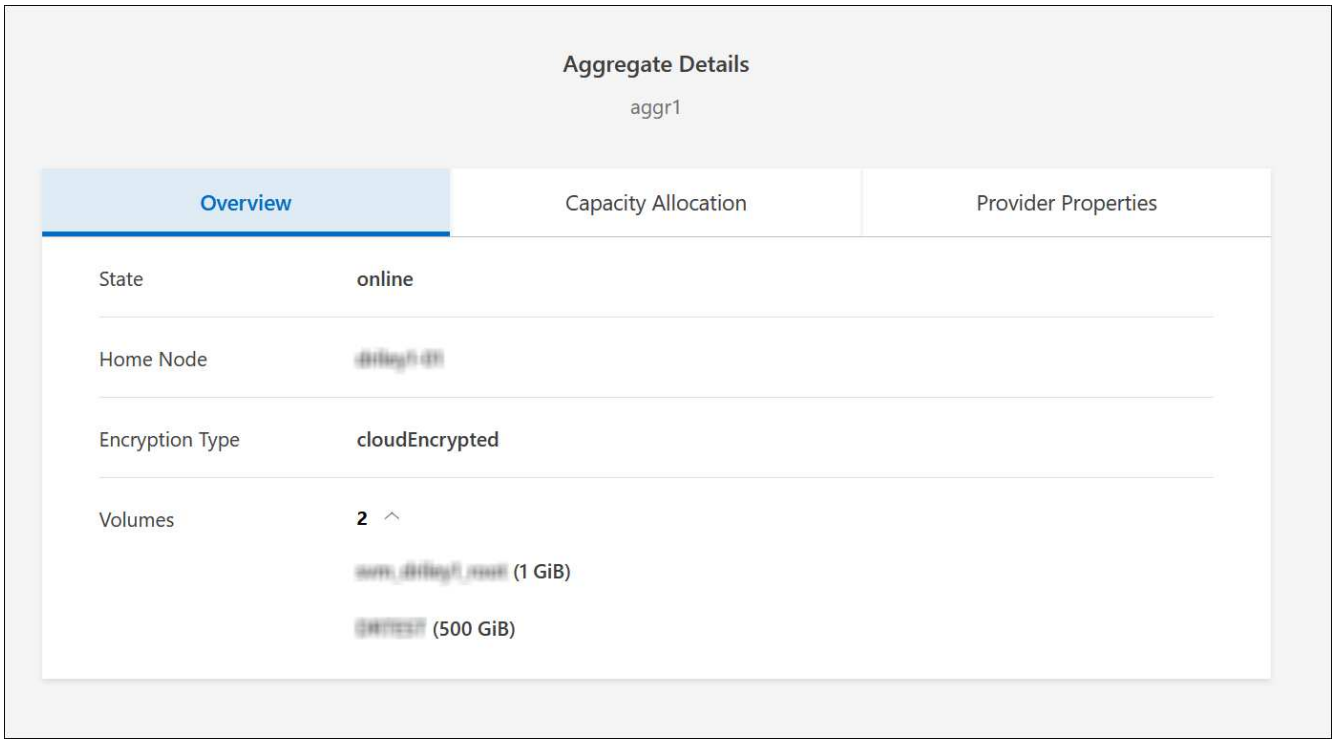
1. 檢視必要行動訊息中的進階資訊、以識別已達到容量上限的集合體。

   例如、進階資訊應該說類似以下的內容： Aggr1 已達到其容量上限。

2. 識別一個或多個要從集合體移出的磁碟區：

   a. 在工作環境中、按一下 * Aggregate 標籤 * 。
   b. 瀏覽至所需的 Aggregate 方塊、然後按一下 * 。 （橢圓圖示） > 檢視 Aggregate 詳細資料 * 。
   c. 在 Aggregate Details 畫面的 Overview （概觀）索引標籤下、檢閱每個 Volume 的大小、然後選擇一個或多個要移出 Aggregate 的 Volume 。

      您應該選擇足夠大的磁碟區來釋放集合體中的空間、以避免未來發生額外的容量問題。



3. 如果系統尚未達到磁碟限制、您應該將磁碟區移至同一個系統上的現有集合體或新集合體。

   如需詳細資訊、請參閱 將磁碟區移至其他Aggregate、以避免容量問題。

4. 如果系統已達到磁碟限制、請執行下列任何一項：
   a. 刪除所有未使用的磁碟區。
   b. 重新排列磁碟區、以釋放集合體上的空間。

      如需詳細資訊、請參閱 將磁碟區移至其他Aggregate、以避免容量問題。

   c. 將兩個或多個磁碟區移至另一個有空間的系統。

      如需詳細資訊、請參閱 將磁碟區移至其他Aggregate、以避免容量問題。

將磁碟區移至其他系統、以避免發生容量問題

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

關於這項工作

您可以依照此工作中的步驟來修正下列必要行動訊息：

> 移動磁碟區是避免容量問題的必要步驟、不過、由於系統已達到磁碟限制、因此BlueXP無法為您執行此動作。

步驟

1. 找出 Cloud Volumes ONTAP 具備可用容量的系統、或是部署新系統。

2. 將來源工作環境拖放到目標工作環境、以執行磁碟區的一次性資料複寫。

   如需詳細資訊、請參閱 "在系統之間複寫資料"。

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

   如需詳細資訊、請參閱 "管理資料複寫排程和關係"。

4. 設定磁碟區以進行資料存取。

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

5. 刪除原始 Volume 。

   如需詳細資訊、請參閱 "管理磁碟區"。

將磁碟區移至其他**Aggregate**、以避免容量問題

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

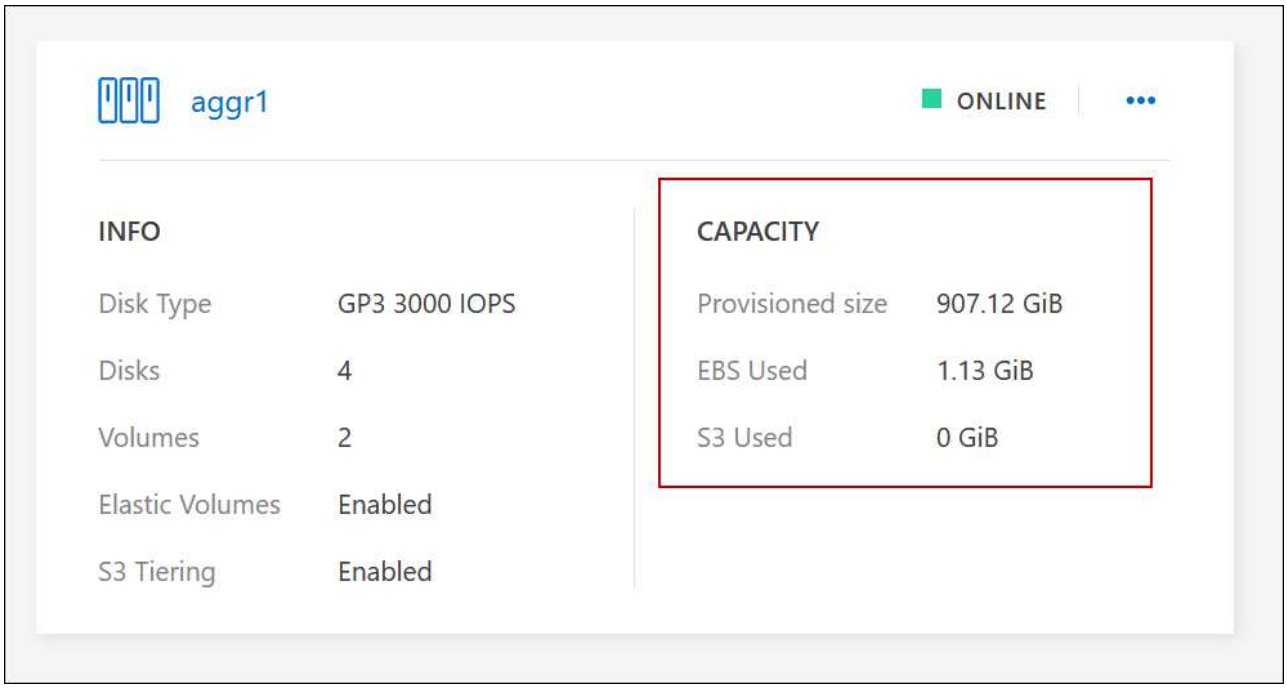
關於這項工作

您可以依照此工作中的步驟來修正下列必要行動訊息：

> 為了避免容量問題、必須移動兩個以上的磁碟區；不過、BlueXP無法為您執行此動作。

步驟

1. 驗證現有的 Aggregate 是否具有您需要移動的磁碟區可用容量：
   a. 在工作環境中、按一下 * Aggregate 標籤 * 。
   b. 瀏覽至所需的 Aggregate 方塊、然後按一下 * 。 （橢圓圖示） > 檢視 Aggregate 詳細資料 * 。
   c. 在 Aggregate 方塊下、檢視可用容量（資源配置大小減去使用的 Aggregate 容量）。



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

   如需詳細資訊、請參閱 "建立 Aggregate"。

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

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

磁碟區移動可能會緩慢執行的原因

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

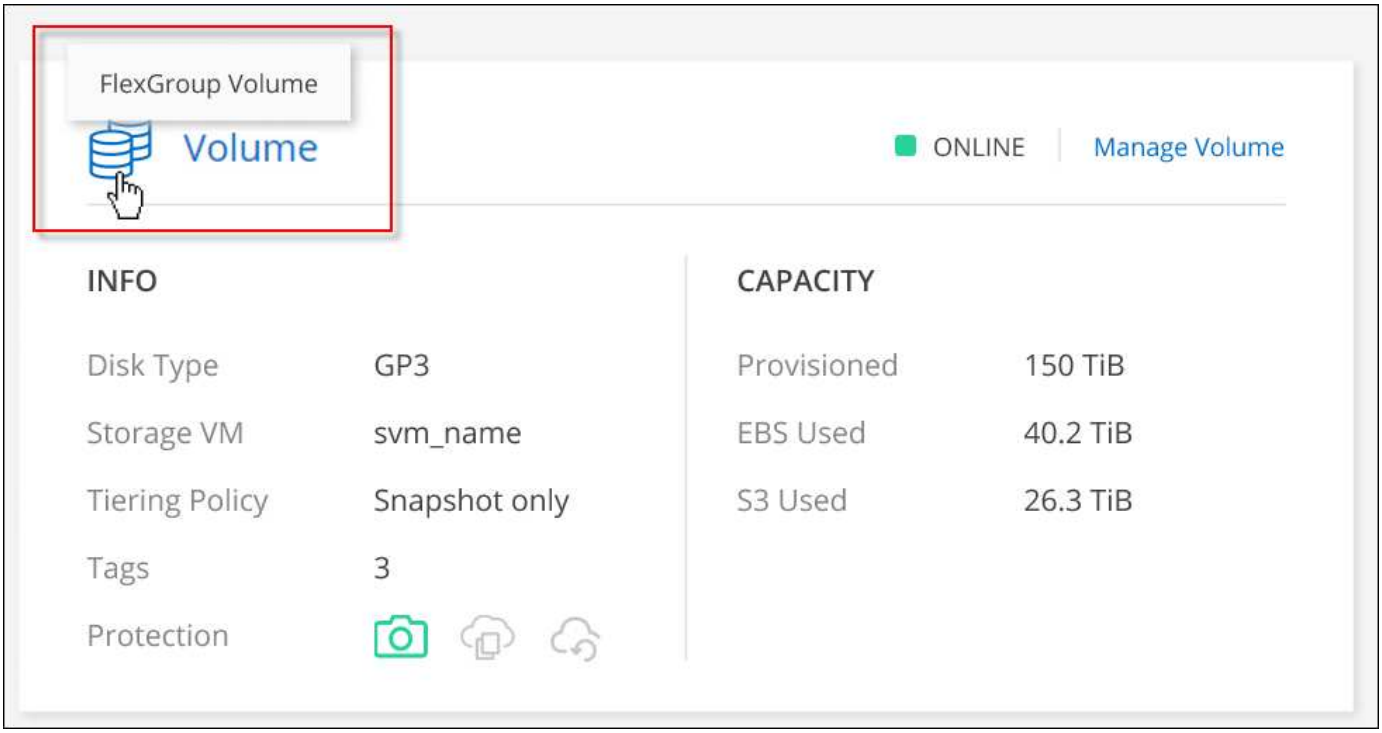
- 磁碟區是複製的。
- Volume 是實體複本的父實體。
- 來源或目的地 Aggregate 具有單一資料處理量最佳化 HDD （ ST1 ）磁碟。
- 其中一個集合體使用舊的物件命名配置。兩個 Aggregate 都必須使用相同的名稱格式。

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

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

檢視 **FlexGroup Volume**

您可以直接透過 BlueXP 中的 Volumes （磁碟區）標籤、檢視透過 CLI 或系統管理員建立的 FlexGroup 磁碟區。BlueXP 與提供給 FlexVol Volume 的資訊相同、透過專用的 Volumes 方塊、提供建立的 FleGroup Volume 的詳細資訊。在「 Volume （磁碟區）」磚下方、您可以透過圖示的暫留文字來識別每個 FlexGroup 磁碟區群組。此外、您也可以透過 Volume 樣式欄、在 Volume 清單檢視下識別及排序 FlexGroup Volume 。



目前、您只能在 BlueXP 下檢視現有的 FlexGroup 磁碟區。在 BlueXP 中建立 FlexGroup 磁碟區的功能無法使用、但已計畫在未來版本中使用。

將非作用中資料分層至低成本物件儲存設備

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

若要設定資料分層、您需要執行下列動作：

1. 選擇支援的組態

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

2. 確保 **Cloud Volumes ONTAP** 在物件儲存設備與物件儲存設備之間建立連線

- 對於 AWS 、您需要 VPC 端點對 S3 。 深入瞭解。
- 對於Azure而言、只要BlueXP具備必要的權限、您就不需要執行任何操作。 深入瞭解。

- 若為Google Cloud、您需要設定私有Google Access的子網路、並設定服務帳戶。 深入瞭解。

3 請確定您已啟用分層功能、並有一個 **Aggregate**

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

4 建立、修改或複寫磁碟區時、請選擇分層原則

在建立、修改或複寫磁碟區時、BlueXP會提示您選擇分層原則。

- "在讀寫磁碟區上分層資料"
- "在資料保護磁碟區上分層資料"

> 什麼是資料分層不需要的？ **#8217** ？
>
> - 您不需要安裝功能授權、就能進行資料分層。
> - 您不需要為容量層建立物件存放區。BlueXP能為您實現這項目標。
> - 您不需要在系統層級啟用資料分層。
>
> 在系統建立時、BlueXP會為Cold資料建立物件存放區、 只要沒有連線或權限問題。之後、您只需要在磁碟區上啟用資料分層功能（在某些情況下、 在 Aggregate 上）。

支援資料分層的組態

您可以在使用特定組態和功能時啟用資料分層。

AWS支援

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

> 使用處理量最佳化的HDD（ST1）時、不建議將資料分層至物件儲存設備。

支援**Azure**

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

支援**Google Cloud**

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

功能互通性

- 加密技術支援資料分層。
- 必須在磁碟區上啟用精簡配置。

需求

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

將冷資料分層至 **AWS S3** 的需求

確保 Cloud Volumes ONTAP 與 S3 建立連線。提供此連線的最佳方法是建立 VPC 端點至 S3 服務。如需相關指示、請參閱 "AWS 文件：建立閘道端點"。

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

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

將冷資料分層至 **Azure Blob** 儲存設備的需求

只要BlueXP具備必要的權限、您就不需要在效能層與容量層之間建立連線。如果Connector的自訂角色具有下列權限、則BlueXP會為您啟用vnet服務端點：

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

根據預設、權限會包含在自訂角色中。 "檢視Azure對Connector的權限"

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

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

  "瞭解如何設定此服務帳戶"。

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

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

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

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

在實作需求之後啟用資料分層

只要沒有連線或權限問題、在建立系統時、BlueXP就會建立Cold資料的物件存放區。如果您在建立系統之後才實作上述需求、則需要透過建立物件存放區的 API 或系統管理員手動啟用分層功能。

> 未來的 Cloud Volumes ONTAP 版本將提供透過 BlueXP 使用者介面進行分層的功能。

確保在 **Aggregate** 上啟用分層

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

- * 新磁碟區 *

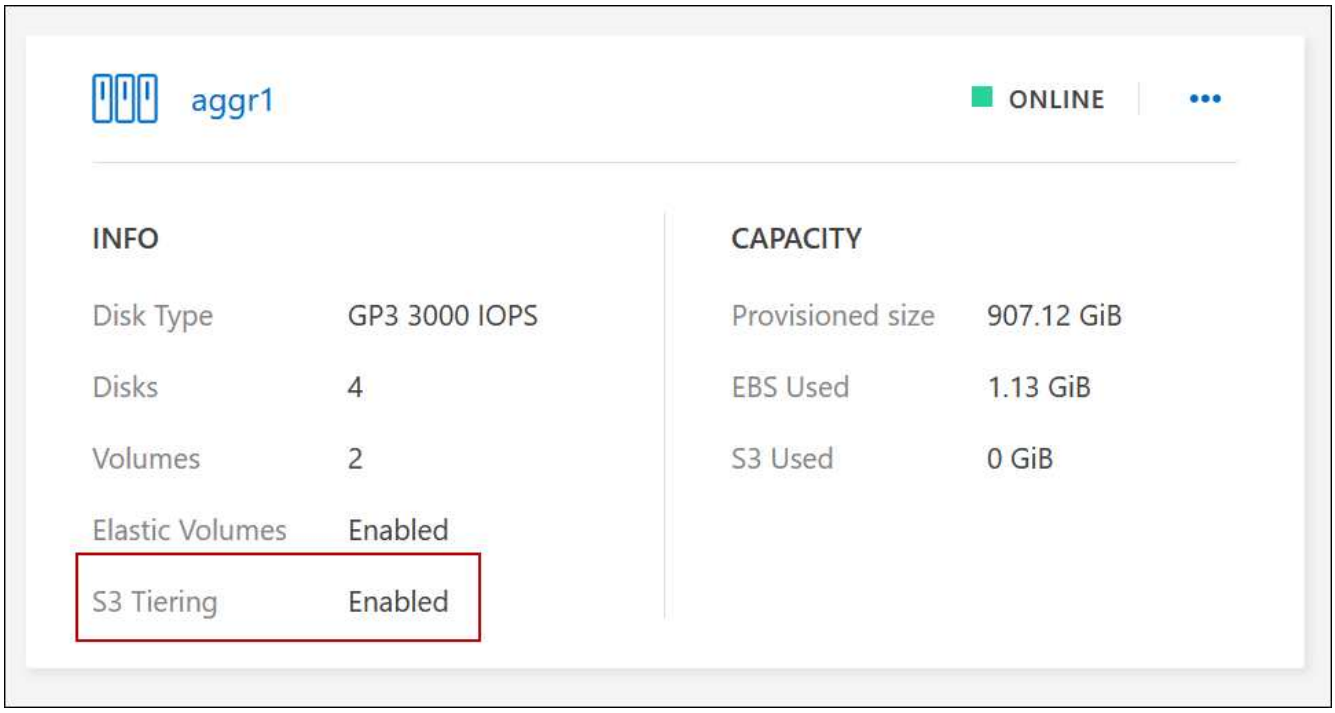
  如果您要在新磁碟區上啟用資料分層功能、就不需要擔心在集合體上啟用資料分層功能。BlueXP會在已啟用分層功能的現有Aggregate上建立磁碟區、或是在啟用資料分層功能的Aggregate不存在的情況下、為磁碟區建立新的Aggregate。

- * 現有磁碟區 *

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

確認是否在 **Aggregate** 上啟用分層的步驟

1. 在BlueXP中開啟工作環境。
2. 按一下 Aggregate 索引標籤。
3. 瀏覽至所需的方塊、並驗證是否已在 Aggregate 上啟用或停用分層。



在集合體上啟用分層的步驟

1. 在 System Manager 中、按一下 * Storage > Tiers* 。

2. 按一下 Aggregate 的動作功能表、然後選取 * 附加 Cloud Tiers* 。
3. 選取要附加的雲端層、然後按一下「 * 儲存 * 」。

接下來呢？

您現在可以在新的和現有的磁碟區上啟用資料分層、如下一節所述。

從讀寫磁碟區分層資料

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

步驟

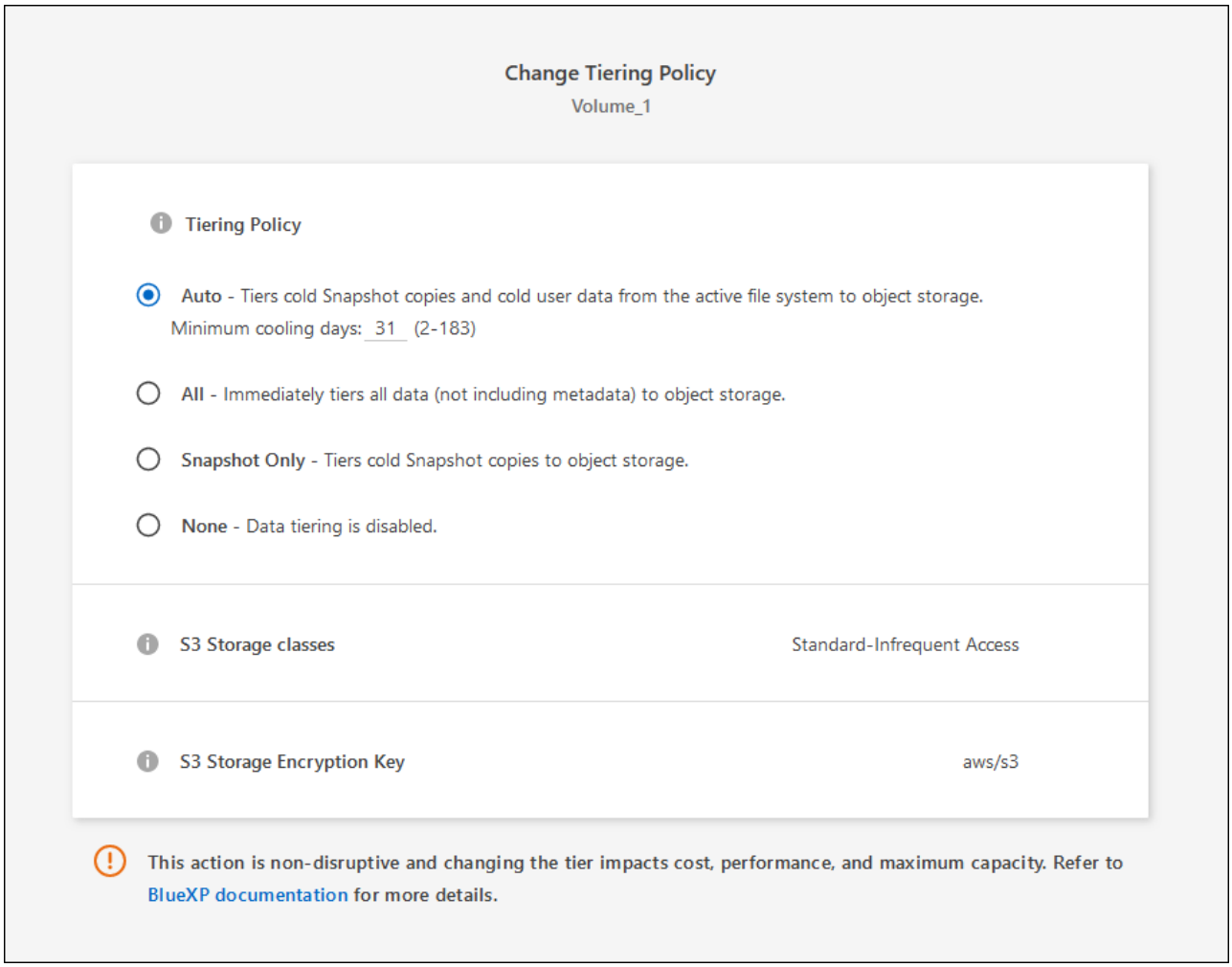
1. 在工作環境下的 Volumes （磁碟區）標籤中、建立新的磁碟區或變更現有磁碟區的層級：

工作	行動
建立新的 Volume	按一下「 * 新增 Volume * 」。
修改現有的 Volume	選取所需的磁碟區方塊、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 * 進階動作 * 和 * 變更分層原則 * 。

2. 選取分層原則。

   如需這些原則的說明、請參閱 "資料分層總覽"。

   - 範例 *



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

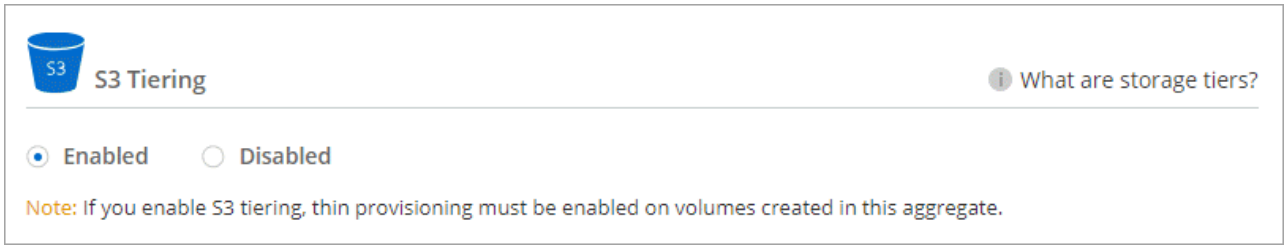
從資料保護磁碟區分層資料

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

步驟

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

    - 範例 *



如需複寫資料的說明、請參閱 "在雲端之間複寫資料"。

變更階層式資料的儲存類別

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

階層式資料的儲存類別是全系統的、並非每個 Volume 都有。

如需支援的儲存類別資訊、請參閱 "資料分層總覽"。

步驟

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

變更資料分層的可用空間比率

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

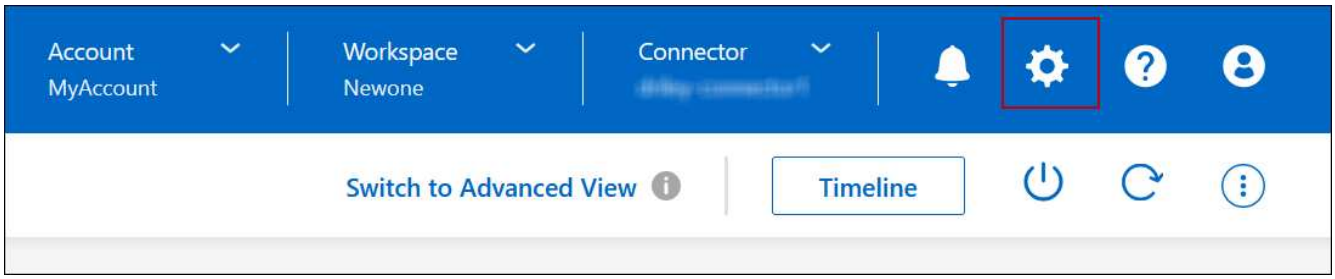
例如、您可以選擇少於10%的可用空間、以確保您使用購買的容量。然後、當需要額外容量時、BlueXP可以為您購買額外的磁碟（直到達到Aggregate的磁碟限制為止）。

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

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

步驟

1. 在 BlueXP 主控台的右上角、按一下 * 設定 * 圖示、然後選取 * Cloud Volumes ONTAP 設定 * 。



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

變更自動分層原則的冷卻週期

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

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

自動分層原則的預設冷卻期間為31天。您可以變更冷卻期間、如下所示：

- 9.8或更新版本：2天至183天
- 9.7或更早：2天至63天

步驟

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

將**LUN**連接至主機

建立iSCSI磁碟區時、BlueXP會自動為您建立LUN。我們只要在每個磁碟區建立一個LUN、就能輕鬆完成工作、因此不需要管理。建立磁碟區之後、請使用 IQN 從主機連線至 LUN 。

請注意下列事項：

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

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按兩下 Cloud Volumes ONTAP 您要管理磁碟區的「功能區」工作環境。
3. 在工作環境中、按一下 * Volumes （磁碟區） * 標籤。
4. 在 Volumes （磁碟區）索引標籤上、瀏覽至所需的磁碟區標題、然後按一下 * Manage Volumes （管理磁碟區） * 以存取 Manage Volumes （管理磁碟區）右側面板。
5. 按一下 * 目標 IQN* 。
6. 按一下「 * 複製 * 」以複製 IQN 名稱。
7. 設定從主機到 LUN 的 iSCSI 連線。
    - "適用於 Red Hat Enterprise Linux 的支援 9 iSCSI Express 組態：啟動目標的 iSCSI 工作階段 ONTAP"
    - "適用於 Windows 的 S89 iSCSI Express 組態：以目標啟動 iSCSI 工作階段 ONTAP"
    - "SAN主機組態ONTAP"

利用**NetApp**功能加速資料存取**FlexCache**

FlexCache Volume 是一種儲存磁碟區、可從來源（或來源）磁碟區快取 SMB 和 NFS 讀取資料。後續讀取快取資料會加快該資料的存取速度。

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

BlueXP 提供 FlexCache 磁碟區的管理功能 "BlueXP Volume 快取" 服務：

您也可以使用 ONTAP CLI 或 ONTAP 系統管理員來建立及管理 FlexCache 磁碟區：

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

BlueXP 會為所有新的 Cloud Volumes ONTAP 系統產生 FlexCache 授權。授權包含500 GiB使用限制。

Aggregate管理

建立Aggregate

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

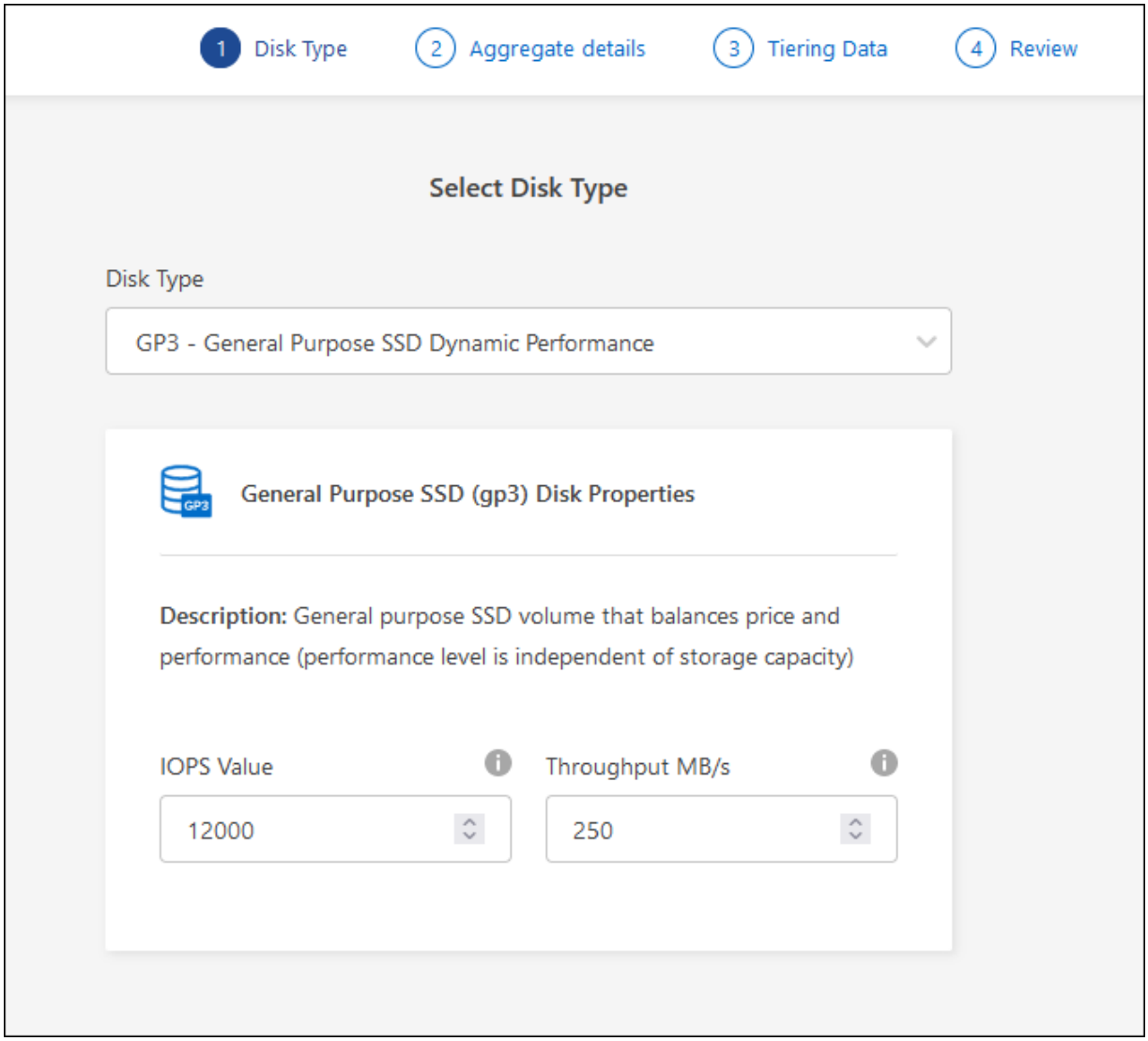
> 所有磁碟和集合體都必須直接從BlueXP建立和刪除。您不應從其他管理工具執行這些動作。這樣做可能會影響系統穩定性、阻礙未來新增磁碟的能力、並可能產生備援雲端供應商費用。

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按兩下 Cloud Volumes ONTAP 您要管理集合體的實例名稱。
3. 在 Aggregate 索引標籤上、按一下 * 新增 Aggregate * 、然後指定 Aggregate 的詳細資料。

AWS

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



"深入瞭解彈性磁碟區的支援"。

Azure

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

Google Cloud

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

4. 按一下「 * 執行 * 」、然後按一下「 * 核准並購買 * 」。

管理集合體

新增磁碟、檢視有關集合體的資訊、以及刪除這些磁碟來管理集合體。

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

開始之前

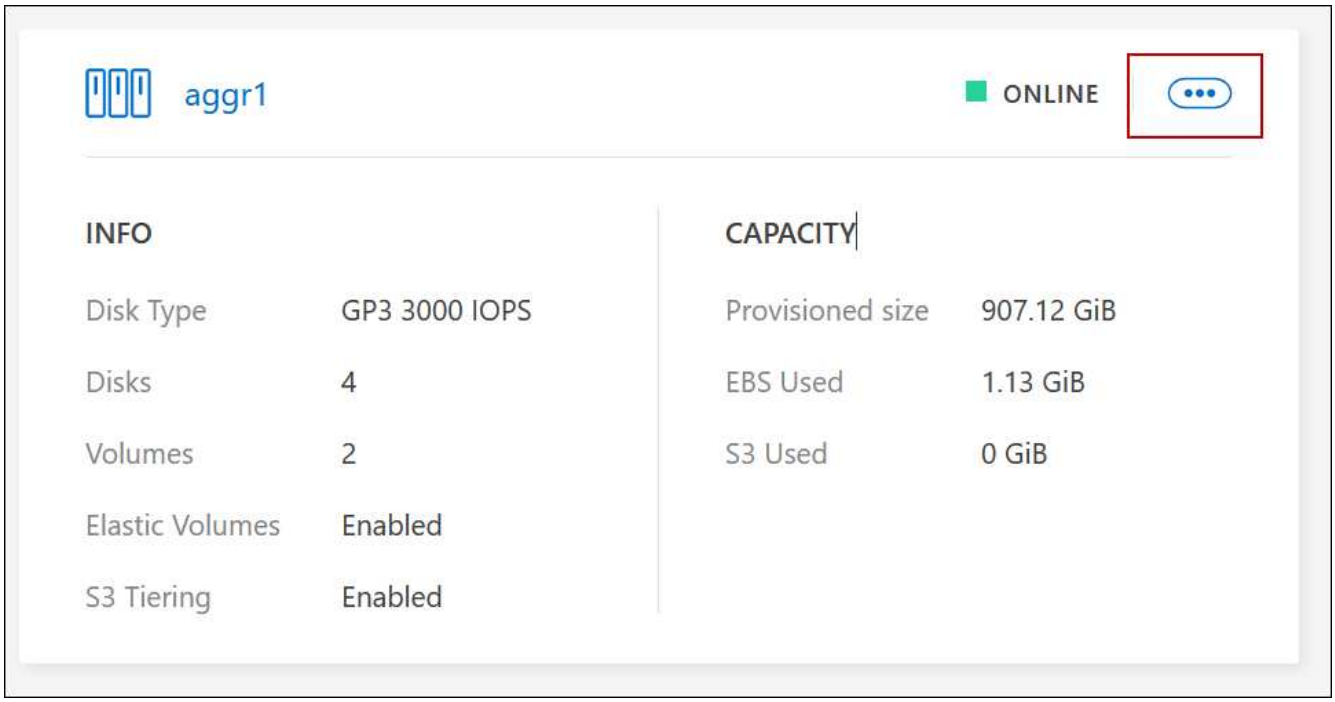
如果您要刪除 Aggregate 、則必須先刪除 Aggregate 中的磁碟區。

關於這項工作

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

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按兩下 Cloud Volumes ONTAP 您要管理集合體的功能性工作環境。
3. 在工作環境中、按一下 * Aggregate * 標籤。
4. 在 Aggregate 索引標籤上、瀏覽至所需標題、然後按一下 * 。 （橢圓圖示） * 。



5. 管理您的 Aggregate ：

工作	行動
檢視有關 Aggregate 的資訊	在 … 下 （橢圓圖示）功能表、按一下 * 檢視 Aggregate details* 。
在特定 Aggregate 上建立磁碟區	在 … 下 （橢圓圖示）功能表、按一下 * 新增 Volume * 。

工作	行動
將磁碟新增至 Aggregate	a. 在 … 下 （橢圓圖示）功能表、按一下 * 新增磁碟 * 。 b. 選取您要新增的磁碟數目、然後按一下「 * 新增 * 」。 集合體中的所有磁碟大小必須相同。
增加支援Amazon EBS彈性Volume的Aggregate容量	a. 在 … 下 （橢圓圖示）功能表、按一下 * 增加容量 * 。 b. 輸入您要新增的額外容量、然後按一下 * 增加 * 。 請注意、您必須將Aggregate的容量增加至少256 GiB或集合體大小的10%。 例如、如果您有1.77 TiB Aggregate、則10%為181 GiB。此值低於256 GiB、因此集合體的大小必須至少增加256 GiB。
刪除 Aggregate	a. 選取不包含任何磁碟區的 Aggregate tile 按一下 * 。 （橢圓圖示） > 刪除 * 。 b. 再按一下 * 刪除 * 以確認。

管理**Connector**上的容量設定

每個Connector都有設定、可決定其如何管理Cloud Volumes ONTAP 用於實現效益的Aggregate容量。

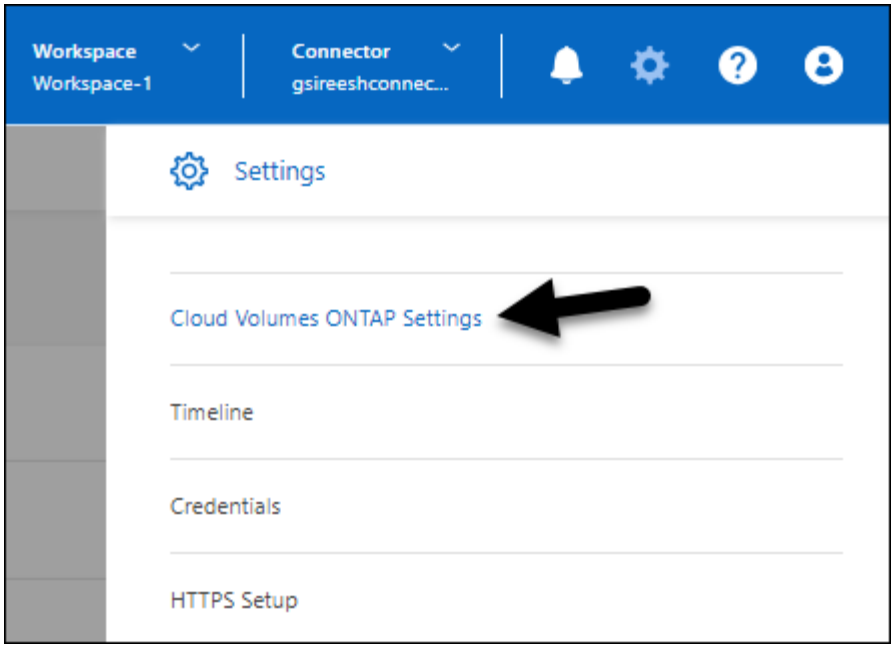
這些設定會影響Cloud Volumes ONTAP 由Connector管理的所有功能不全系統。如果您有另一個Connector、則可以以不同的方式設定。

必要權限

修改 Cloud Volumes ONTAP 設定需要帳戶管理權限。

步驟

1. 在 BlueXP 主控台的右上角、按一下「設定」圖示、然後選取 * 「 Cloud Volumes ONTAP 設定 * 」。



2. 在* Capacity *下、修改下列任何設定：

容量管理模式

選擇BlueXP是否通知您儲存容量決策、或是BlueXP是否自動為您管理容量需求。

"瞭解容量管理模式的運作方式"。

Aggregate Capacity 臨界值 **-** 可用空間比率

此比率是容量管理決策的關鍵參數、無論您是處於自動或手動的容量管理模式、瞭解其影響都是不可或缺的。建議您根據您的特定儲存需求和預期成長來設定此臨界值、以在資源使用率和成本之間維持平衡。

在手動模式中、如果集合體上的可用空間比率降至低於指定臨界值、就會觸發通知、提醒您應採取行動來解決可用空間比率過低的問題。請務必監控這些通知、並手動管理彙總容量、以避免服務中斷並確保最佳效能。

可用空間比率的計算方式如下：
（Aggregate capcap處理 能力- Aggregate上的總使用容量）/ Aggregate cap處理 能力

請參閱 "自動容量管理" 若要立即瞭解、容量會自動在 Cloud Volumes ONTAP 中管理。

Aggregate Capacity 臨界值 **-** 資料分層的可用空間比率

定義將資料分層至容量層（物件儲存）時、效能層（磁碟）需要多少可用空間。

這種比率對於災難恢復方案非常重要。從容量層讀取資料時Cloud Volumes ONTAP 、將資料移至效能層、以提供更好的效能。如果空間不足、Cloud Volumes ONTAP 則無法移動資料。

3. 按一下「 * 儲存 * 」。

儲存VM管理

在BlueXP中管理儲存VM

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

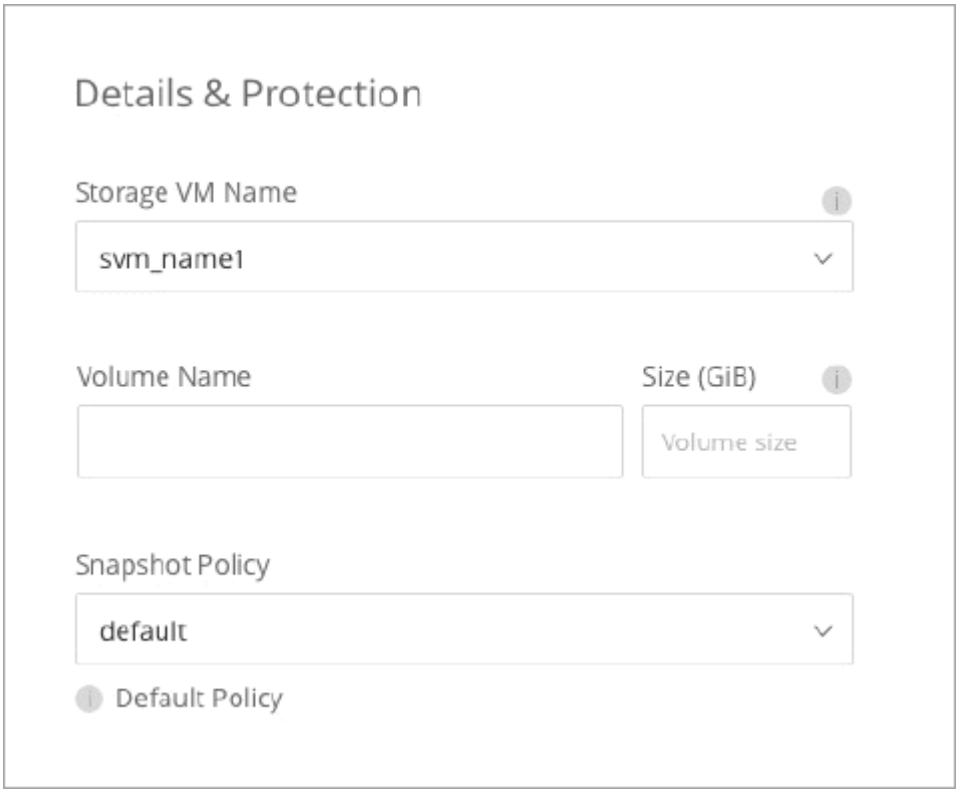
支援的儲存 VM 數量

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

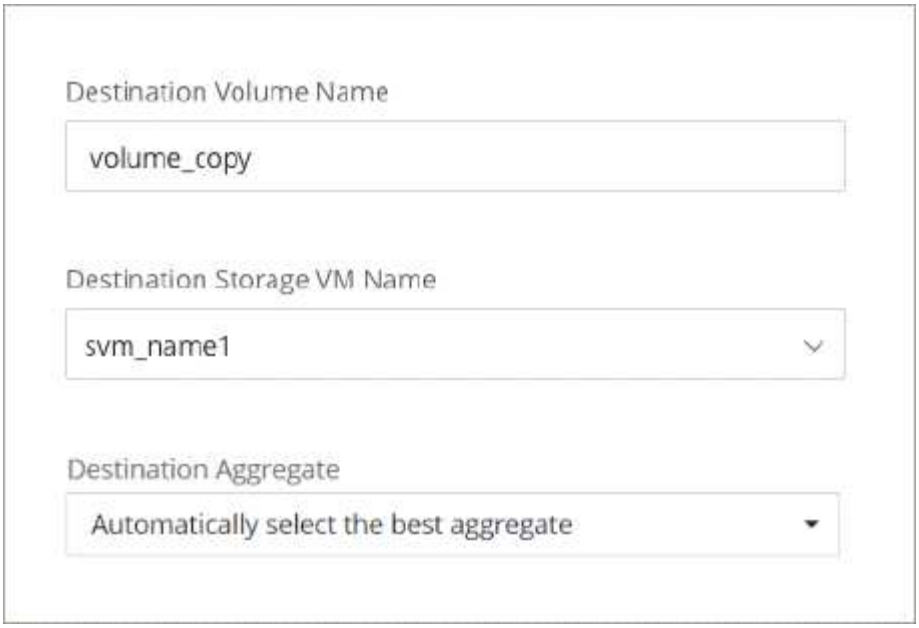
使用多個儲存VM

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

例如、下圖顯示如何在建立 Volume 時選擇儲存 VM 。



下圖顯示如何在將磁碟區複寫至其他系統時、選擇儲存 VM 。



修改預設儲存**VM**的名稱

BlueXP會自動命名為其所建立的Cloud Volumes ONTAP 單一儲存VM、以利執行效能。如果您有嚴格的命名標準、則可以從 System Manager 、 CLI 或 API 修改儲存 VM 的名稱。例如、您可能希望名稱與您為 ONTAP 自己的叢集命名儲存虛擬機器的方式相符。

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

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

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

支援的儲存 **VM** 數量

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

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

驗證組態的限制

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

步驟

1. 請選擇 "《不知》中的「儲存限制」區段Cloud Volumes ONTAP"。
2. 識別執行個體類型的每個介面IP位址數目上限。

3. 請記下這個數字、因為您在AWS中分配IP位址時、會在下一節中需要這個數字。

在**AWS**中分配**IP**位址

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

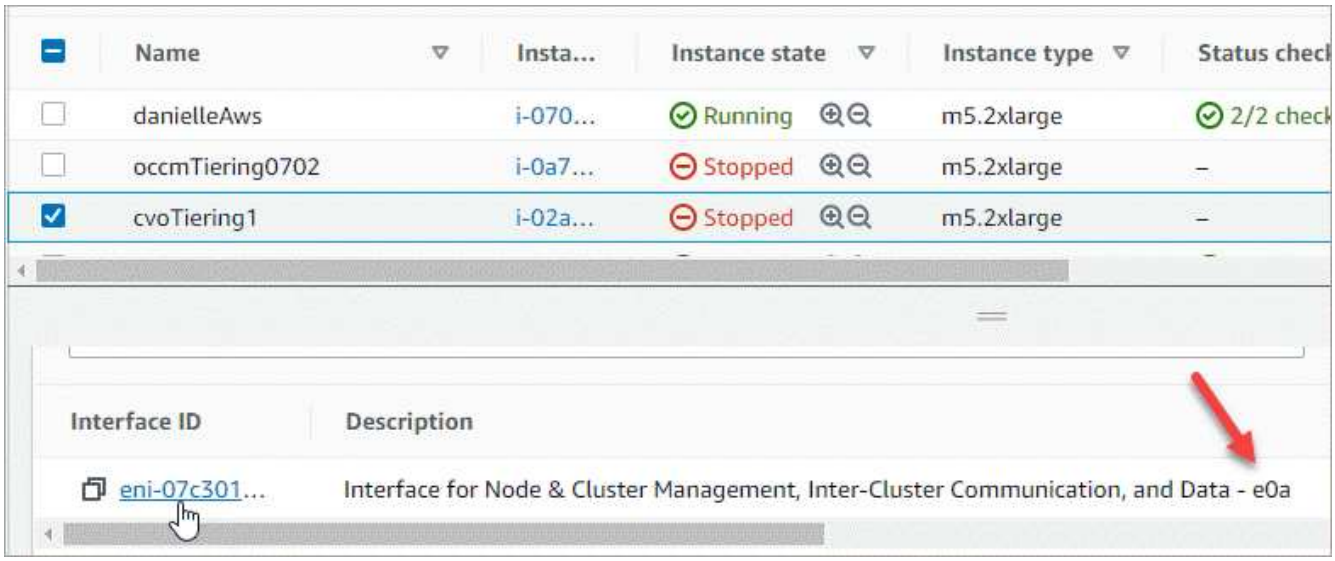
請注意、儲存VM的選用管理LIF需要在單一節點系統和單一AZ的HA配對上使用私有IP位址。此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

步驟

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

   如果您要在HA配對上建立儲存VM、請選取節點1。

3. 向下捲動至*網路介面*、然後按一下*介面ID*以取得連接埠e0a。



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

      您應該已經在本頁上一節中找出每個介面支援的IP位址上限。

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

      如果IP位址未在使用中、您可以將其與新的儲存VM搭配使用。

7. 回到AWS主控台、按一下*指派新的IP位址*、根據新儲存VM所需的容量來指派額外的IP位址。
   - 單節點系統：需要一個未使用的次要私有IP。

     若要在儲存VM上建立管理LIF、則需要選用的次要私有IP。

- 單一AZ中的HA配對：節點1上需要一個未使用的次要私有IP。

  若要在儲存VM上建立管理LIF、則需要選用的次要私有IP。

- 多個AZs中的HA配對：每個節點需要一個未使用的次要私有IP。

8. 如果您要在單一AZ中分配HA配對的IP位址、請啟用*允許重新指派次要私有IPV4位址*。
9. 按一下「 * 儲存 * 」。
10. 如果您在多個AZs中有HA配對、則必須針對節點2重複這些步驟。

在單一節點系統上建立儲存VM

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

步驟

1. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

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

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

2. 建立NAS LIF。

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

   其中_Private IP x是e0a上未使用的次要私有IP。

3. 選用：建立儲存VM管理LIF。

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

   其中_Private IP是e0a上另一個未使用的次要私有IP。

4. 將一個或多個集合體指派給儲存VM。

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

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

在單一**AZ**的**HA**配對上建立儲存**VM**

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

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

步驟

1. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

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

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

2. 在節點1上建立NAS LIF。

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

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

3. 選用：在節點1上建立儲存VM管理LIF。

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

其中_Private IP是e0a上另一個未使用的次要私有IP。

4. 將一個或多個集合體指派給儲存VM。

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

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

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

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

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

在多個**AZs**的**HA**配對上建立儲存**VM**

這些步驟可在多個AZs的HA配對上建立新的儲存VM。

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

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

步驟

1. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

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

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

2. 在節點1上建立NAS LIF。

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

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

3. 選用：在節點1上建立儲存VM管理LIF。

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

4. 在節點1上建立iSCSI LIF。

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmask nodei1Mask -lif
ip_node1_iscsi_2 -home-node cvo-node1
```

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

5. 在節點2上建立iSCSI LIF。

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

- 此iSCSI LIF是支援儲存VM中浮動IP的LIF移轉所必需的。它不一定是iSCSI LIF、但無法設定在節點之間移轉。
- 「服務原則預設資料區塊」表示IP位址不會在節點之間移轉。
- _Private IP是CVO節點2的eth0（e0a）上未使用的次要私有IP位址。

6. 將一個或多個集合體指派給儲存VM。

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

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

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

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

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

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

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

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

> 若要執行其他 NIC 相關工作、您可以在 Azure 中指派具有適當權限的網路參與者角色或自訂角色。如需這些 NIC 相關權限的詳細資訊、請參閱 "Microsoft Azure 文件"。

支援的儲存 **VM** 數量

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

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

在**Azure**中配置**IP**位址

您必須先在Azure中配置IP位址、才能建立儲存VM並分配LIF。

單一節點系統

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

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

步驟

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

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

如果您要建立SVM管理LIF、請重複這些步驟以建立其他IP位址。

完成後

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

HA配對

如何為HA配對分配IP位址、取決於您使用的儲存傳輸協定。

iSCSI

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

您需要建立下列IP位址：

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

  此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

步驟

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

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

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

NFS

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

您需要建立下列IP位址：

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

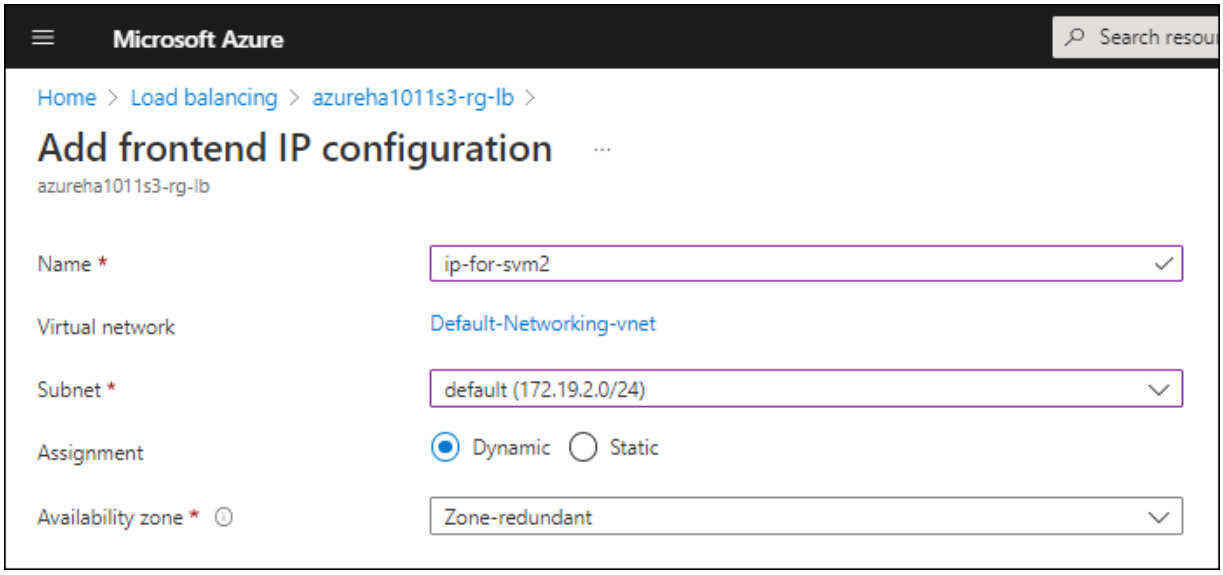
  DNS通訊需要iSCSI LIF。iSCSI LIF用於此用途、因為它不會在容錯移轉時移轉。

  此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

步驟

1. 在Azure入口網站中、開啟*負載平衡器*服務。
2. 按一下HA配對的負載平衡器名稱。

3. 從節點1建立資料LIF存取的前端IP組態、從節點2存取資料LIF的前端IP組態、以及儲存VM（SVM）管理LIF的另一個選用前端IP。
   a. 在*設定*下、按一下*前端IP組態*。
   b. 按一下「 * 新增 * 」。
   c. 輸入前端IP的名稱、選取Cloud Volumes ONTAP 該子網路做為「靜態HA配對」、保留「動態」選項、並在「可用區域」中保留「區域-備援」選項、以確保區域故障時IP位址仍可繼續使用。

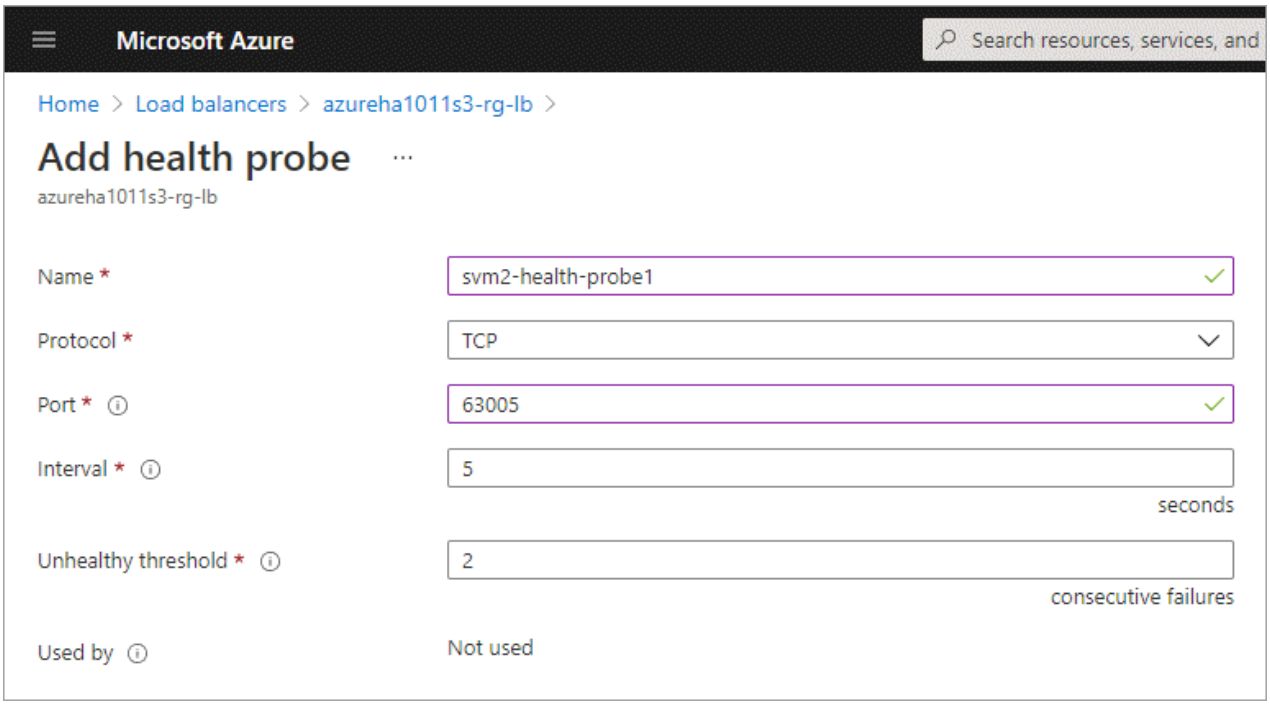


   d. 按一下您剛才建立的前端IP組態名稱、將*指派*變更為*靜態*、然後按一下*儲存*。

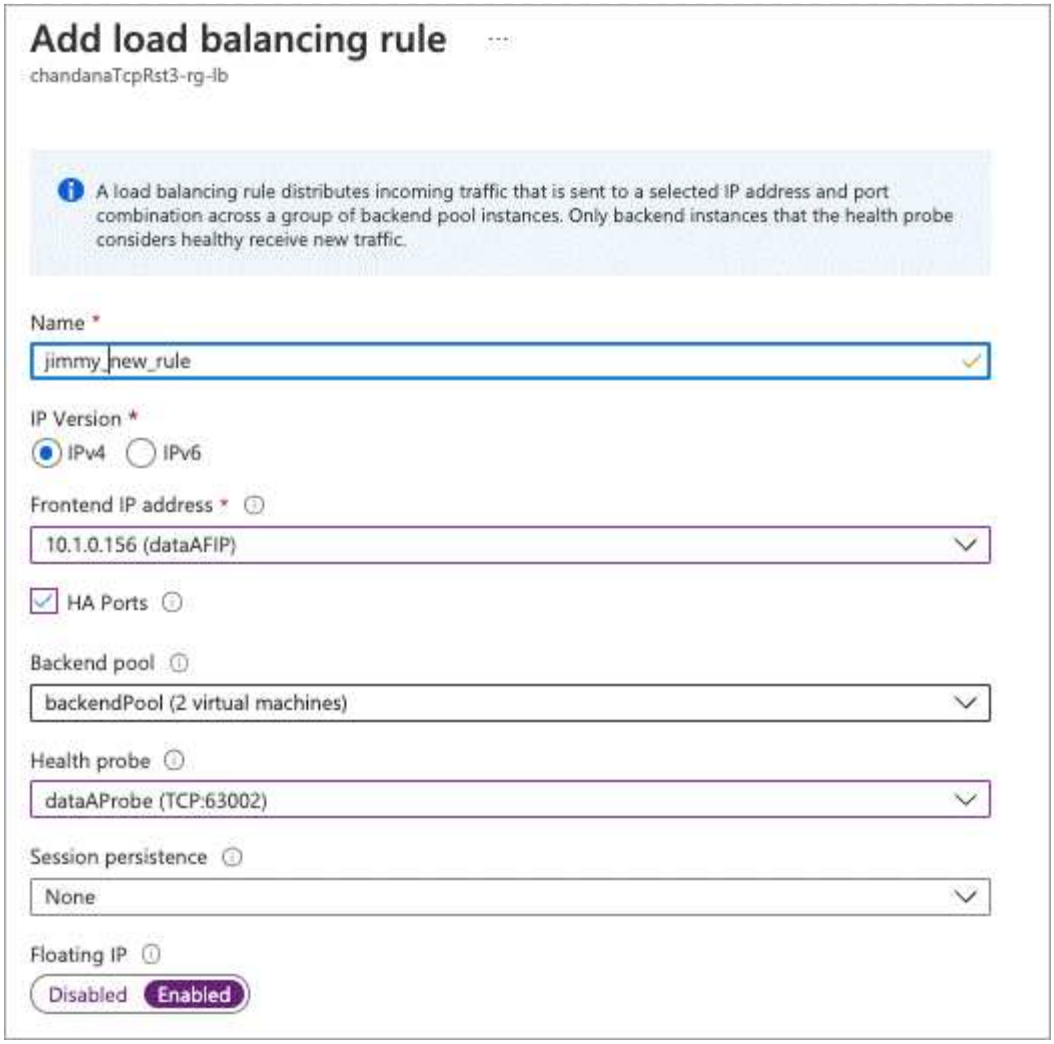
      最好使用靜態IP位址、因為靜態IP可確保IP位址不會變更、有助於避免不必要的應用程式中斷運作。

4. 為您剛建立的每個前端IP新增健全狀況探查。
   a. 在負載平衡器的*設定*下、按一下*健全狀況探查*。
   b. 按一下「 * 新增 * 」。
   c. 輸入健全狀況探針的名稱、然後輸入介於63005和65000之間的連接埠號碼。保留其他欄位的預設值。

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



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



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

中小企業

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

您需要在負載平衡器中建立下列IP位址：

- 單一IP位址、可從節點1存取NAS資料LIF
- 單一IP位址、可從節點2存取NAS資料LIF
- 每個VM各自的NIC 0中節點1上iSCSI LIF的一個IP位址
- 節點2上iSCSI LIF的一個IP位址

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

- 儲存VM（SVM）管理LIF的選用IP位址

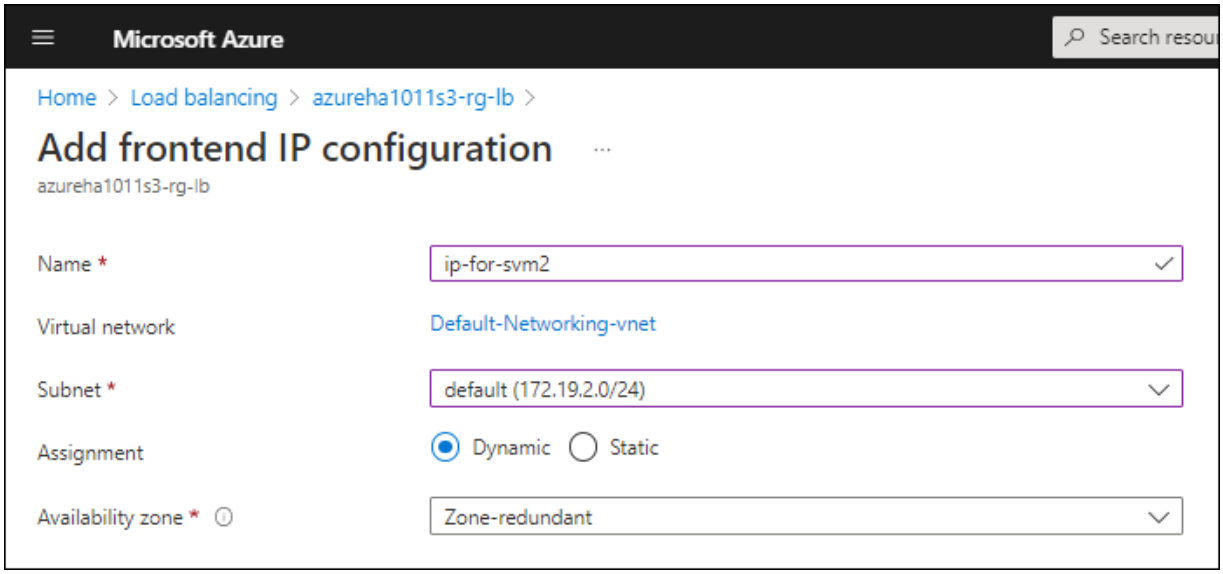
  此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

步驟

1. 在Azure入口網站中、開啟*負載平衡器*服務。
2. 按一下HA配對的負載平衡器名稱。
3. 僅為資料和SVM LIF建立所需的前端IP組態數目：

> 前端IP只能在每個對應SVM的NIC 0下建立。如需如何將IP位址新增至SVM NIC 0的詳細資訊、請參閱「步驟7 [hyperlink]」

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

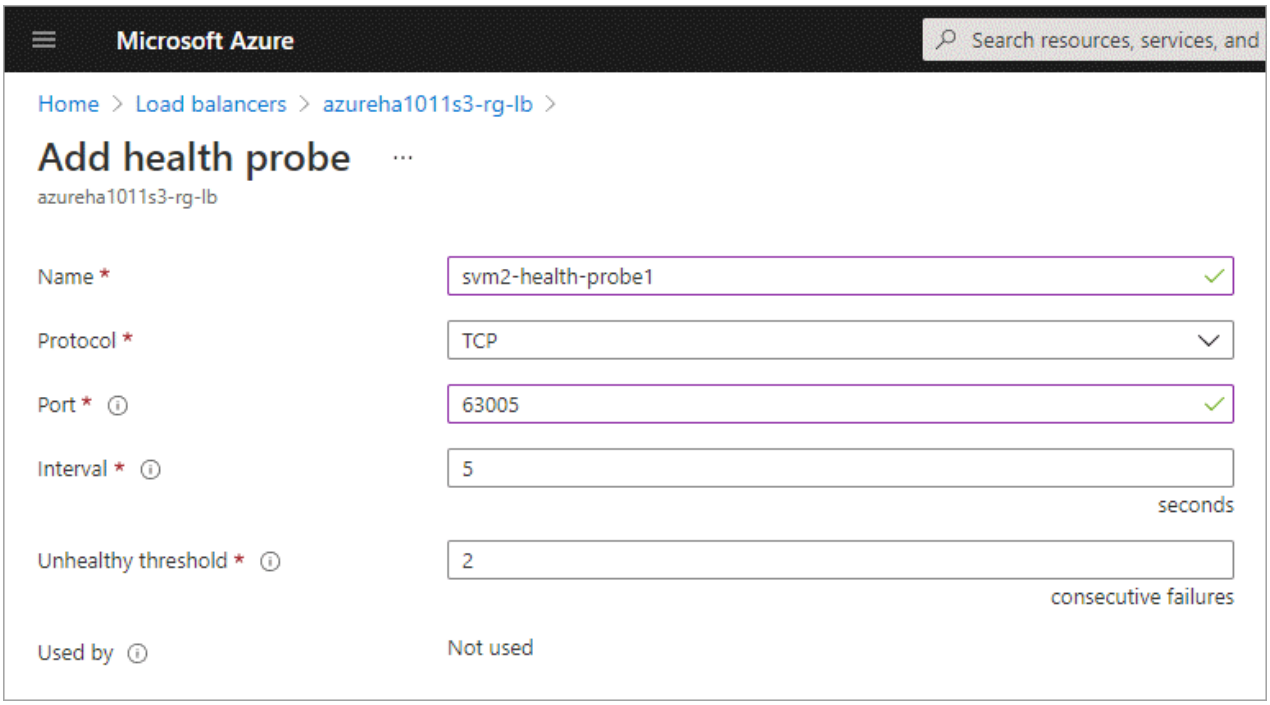


   d. 按一下您剛才建立的前端IP組態名稱、將*指派*變更為*靜態*、然後按一下*儲存*。

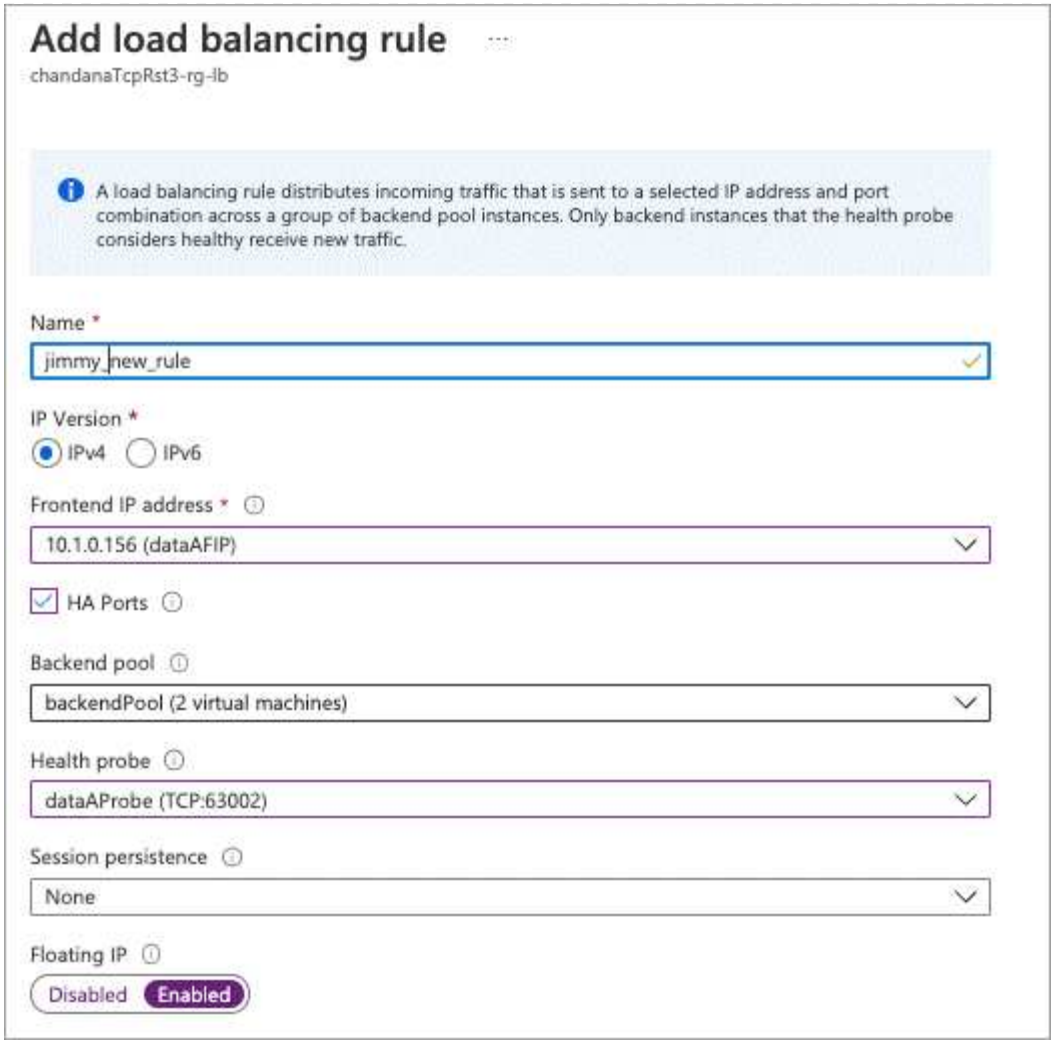
      最好使用靜態IP位址、因為靜態IP可確保IP位址不會變更、有助於避免不必要的應用程式中斷運作。

4. 為您剛建立的每個前端IP新增健全狀況探查。
   a. 在負載平衡器的*設定*下、按一下*健全狀況探查*。
   b. 按一下「 * 新增 * 」。
   c. 輸入健全狀況探針的名稱、然後輸入介於63005和65000之間的連接埠號碼。保留其他欄位的預設值。

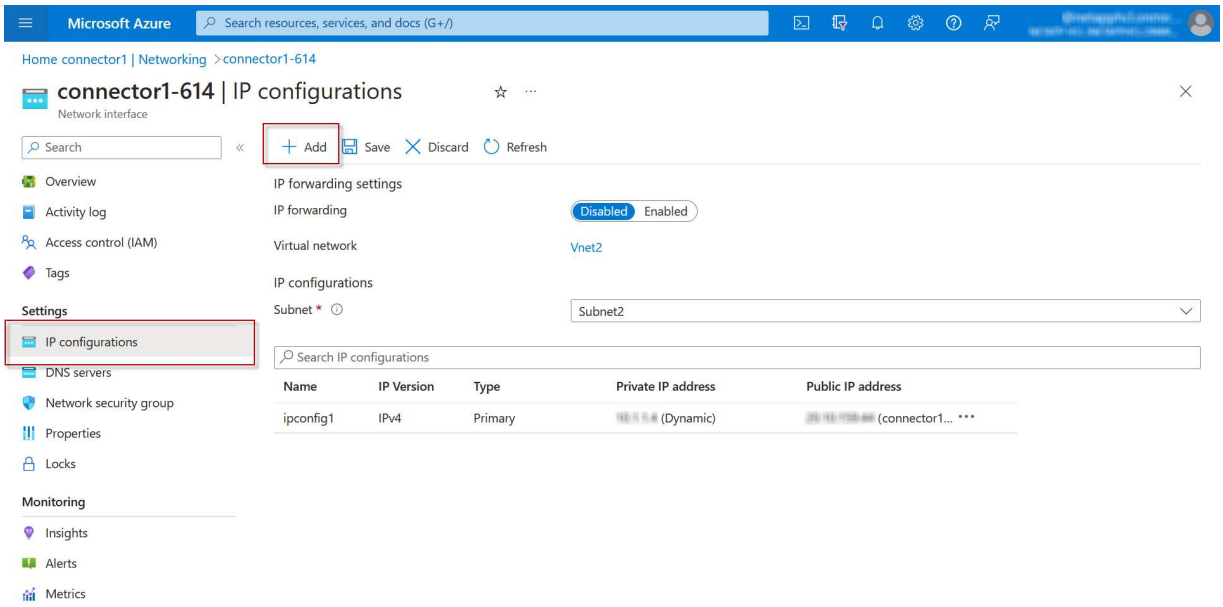
      連接埠號碼必須介於63005和65000之間。例如、如果您要建立三個健全狀況探針、可以輸入使用連接埠編號63005、63006和63007的探針。



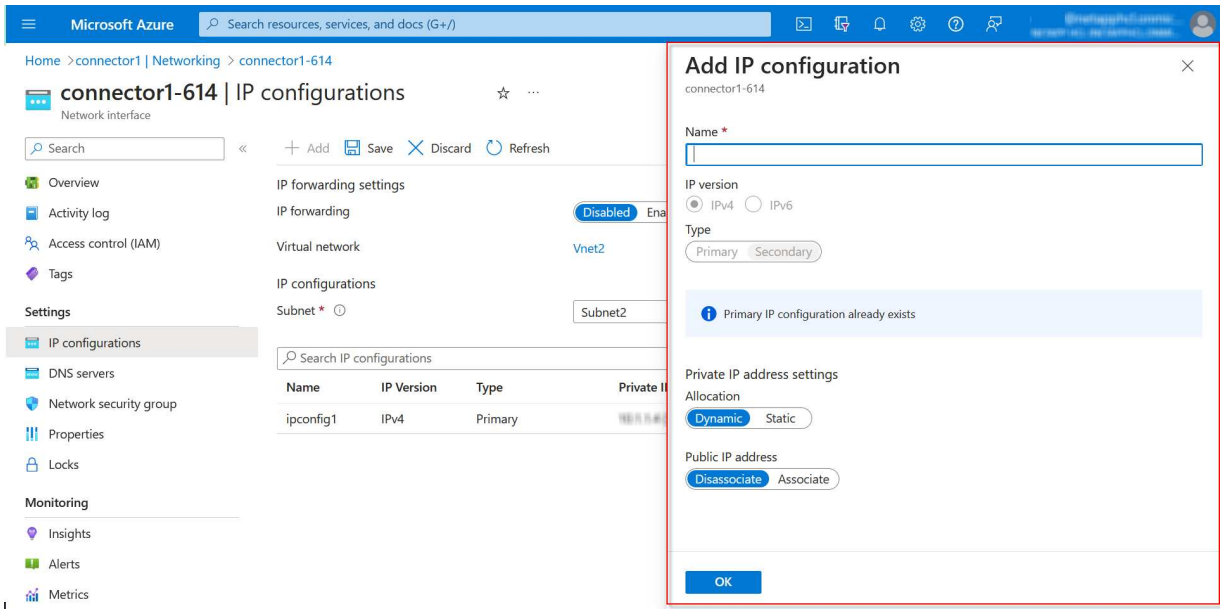
5. 為每個前端IP建立新的負載平衡規則。
   a. 在負載平衡器的*設定*下、按一下*負載平衡規則*。
   b. 按一下*「Add*（新增*）」、然後輸入所需資訊：
      - 名稱：輸入規則的名稱。
      - * IP Version ：選取 IPV*。
      - 前端**IP**位址：選取您剛建立的前端IP位址之一。
      - * HA連接埠*：啟用此選項。
      - 後端集區：保留已選取的預設後端集區。
      - 健全狀況探查：選取您為所選前端IP所建立的健全狀況探查。
      - 工作階段持續性：選取*無*。
      - 浮動**IP**：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



6. 確認Cloud Volumes ONTAP 適用於此功能的網路安全群組規則可讓負載平衡器針對上述步驟4所建立的健全狀況探查傳送TCP探查。請注意、這是預設允許的。
7. 對於iSCSI LIF、請新增NIC 0的IP位址。
   a. 按一下Cloud Volumes ONTAP 「不完整虛擬機器」的名稱。
   b. 按一下*網路*。
   c. 按一下nic0的網路介面名稱。
   d. 在「設定」下、按一下「* IP組態*」。
   e. 按一下「 * 新增 * 」。



f. 輸入IP組態的名稱、選取動態、然後按一下*確定*。



g. 按一下您剛才建立的IP組態名稱、將指派變更為靜態、然後按一下*儲存*。

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

完成後

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

建立儲存VM和LIF

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

如何在單一節點系統上建立儲存VM和LIF、取決於您使用的儲存傳輸協定。

iSCSI

請依照下列步驟建立新的儲存VM、以及所需的LIF。

步驟

1. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

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

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

2. 建立資料LIF：

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

3. 選用：建立儲存VM管理LIF。

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

4. 將一個或多個集合體指派給儲存VM。

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

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

NFS

請依照下列步驟建立新的儲存VM、以及所需的LIF。

步驟

1. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

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

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

2. 建立資料LIF：

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

3. 選用：建立儲存VM管理LIF。

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

4. 將一個或多個集合體指派給儲存VM。

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

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

中小企業

請依照下列步驟建立新的儲存VM、以及所需的LIF。

步驟

1. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

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

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

2. 建立資料LIF：

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

3. 選用：建立儲存VM管理LIF。

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

4. 將一個或多個集合體指派給儲存VM。

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

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

HA配對

如何在HA配對上建立儲存VM和LIF、取決於您使用的儲存傳輸協定。

iSCSI

請依照下列步驟建立新的儲存VM、以及所需的LIF。

步驟

1. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

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

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

2. 建立資料生命量：

   a. 使用下列命令在節點1上建立iSCSI LIF。

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

   b. 使用下列命令在節點2上建立iSCSI LIF。

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

3. 選用：在節點1上建立儲存VM管理LIF。

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

   此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

4. 將一個或多個集合體指派給儲存VM。

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

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

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

   a. 輸入下列命令以存取進階模式。

   ```
   ::> set adv -con off
   ```

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

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

NFS

請依照下列步驟建立新的儲存VM、以及所需的LIF。

步驟

1. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

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

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

2. 建立資料生命量：
   a. 使用下列命令在節點1上建立NAS LIF。

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

   b. 使用下列命令在節點2上建立NAS LIF。

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

3. 建立iSCSI LIF以提供DNS通訊：
   a. 使用下列命令在節點1上建立iSCSI LIF。

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

   b. 使用下列命令在節點2上建立iSCSI LIF。

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

4. 選用：在節點1上建立儲存VM管理LIF。

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

此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

5. 選用：在節點1上建立儲存VM管理LIF。

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

此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

6. 將一個或多個集合體指派給儲存VM。

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

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

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

   a. 輸入下列命令以存取進階模式。

   ```
   ::> set adv -con off
   ```

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

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

中小企業

請依照下列步驟建立新的儲存VM、以及所需的LIF。

步驟

1. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

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

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

2. 建立NAS資料生命量：
   a. 使用下列命令在節點1上建立NAS LIF。

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

   b. 使用下列命令在節點2上建立NAS LIF。

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

3. 建立iSCSI LIF以提供DNS通訊：
   a. 使用下列命令在節點1上建立iSCSI LIF。

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

   b. 使用下列命令在節點2上建立iSCSI LIF。

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

4. 選用：在節點1上建立儲存VM管理LIF。

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

此管理LIF可連線至SnapCenter 諸如VMware等管理工具。

5. 將一個或多個集合體指派給儲存VM。

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

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

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

   a. 輸入下列命令以存取進階模式。

   ```
   ::> set adv -con off
   ```

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

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

接下來呢？

在HA配對上建立儲存VM之後、最好先等待12小時、再在該SVM上配置儲存設備。從發行版的《21》開始、BlueXP會以12小時的時間間隔掃描HA配對負載平衡器的設定。Cloud Volumes ONTAP如果有新的SVM、則BlueXP會啟用可縮短非計畫性容錯移轉的設定。

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

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

支援的儲存 **VM** 數量

從9.11.1版開始、Cloud Volumes ONTAP Google Cloud中的特定支援功能可支援多個儲存VM。前往 "發行說明 Cloud Volumes ONTAP" 驗證Cloud Volumes ONTAP 支援的儲存VM數量是否適用於您的版本的支援。

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

建立儲存**VM**

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

單一節點系統

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

步驟

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

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

"Google Cloud文件：新增別名IP範圍至現有執行個體"

2. 建立儲存虛擬機器和通往儲存虛擬機器的路由。

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

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

3. 指定您在Google Cloud中新增的IP位址、以建立資料LIF。

iSCSI

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

NFS或SMB

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

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

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

5. 將一個或多個集合體指派給儲存VM。

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

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

HA配對

您必須使用BlueXP API在Cloud Volumes ONTAP Google Cloud的某個系統上建立儲存VM。由於BlueXP會使用所需的LIF服務來設定儲存VM、以及輸出SMB/CIFS通訊所需的iSCSI LIF、因此需要使用API（而非System Manager或CLI）。

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

必要的Google Cloud權限

Connector需要特定權限、才能建立及管理Cloud Volumes ONTAP 儲存VM、以利執行各種HA配對。所需權限包含在中 "NetApp 提供的原則"。

步驟

1. 使用下列API呼叫建立儲存VM：

「POST /occm/api/gcp/ha/辦公 環境/｛we_ID｝/svm/」

申請機構應包括下列項目：

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

管理HA配對上的儲存VM

BlueXP API也支援在HA配對上重新命名及刪除儲存VM。

重新命名儲存VM

如有需要、您可以隨時變更儲存VM的名稱。

步驟

1. 使用下列API呼叫重新命名儲存VM：

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

   申請機構應包括下列項目：

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

刪除儲存VM

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

步驟

1. 使用下列API呼叫來刪除儲存VM：

   「刪除/occm/api/gcp/ha/工作 環境/｛we_ID｝/Svm/｛Svm_name｝」

設定 SVM 災難恢復

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

如果在兩個 Cloud Volumes ONTAP 系統之間設定 SnapMirror SVM 複寫、複寫必須介於兩個 HA 配對系統或兩個單一節點系統之間。您無法在 HA 配對和單一節點系統之間設定 SnapMirror SVM 複寫。

如需 CLI 指示、請參閱下列文件。

- "SVM 災難恢復準備快速指南"

- "SVM Disaster Recovery Express 指南"

安全性與資料加密

使用 **NetApp** 加密解決方案加密磁碟區

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

外部金鑰管理程式支援NVE和NAE。

使用 **AWS** 金鑰管理服務管理金鑰

您可以使用 "AWS 的金鑰管理服務（ KMS ）" 保護 AWS 部署應用程式中的 ONTAP 加密金鑰。

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

使用 KMS 時、請注意、根據預設、資料 SVM 的 LIF 會用於與雲端金鑰管理端點通訊。節點管理網路用於與 AWS 的驗證服務進行通訊。如果叢集網路設定不正確、叢集將無法正確使用金鑰管理服務。

開始之前

- Cloud Volumes ONTAP 必須執行 9.12.0 版或更新版本
- 您必須已安裝 Volume Encryption （ VE ）授權和
- 您必須已安裝多租戶加密金鑰管理（ MTEKM ）授權。
- 您必須是叢集或SVM管理員
- 您必須擁有有效的 AWS 訂閱

> 您只能設定資料 SVM 的金鑰。

組態

AWS

1. 您必須建立 "授予" 適用於管理加密的 IAM 角色所使用的 AWS KMS 金鑰。IAM 角色必須包含允許下列作業的原則：
   - `DescribeKey`
   - `Encrypt`
   - `Decrypt`
     若要建立授予、請參閱 "AWS文件"。
2. "將原則新增至適當的 IAM 角色。" 原則應支援 `DescribeKey`、 `Encrypt`和 `Decrypt` 營運：

Cloud Volumes ONTAP

1. 切換至您的 Cloud Volumes ONTAP 環境。

2. 切換至進階權限等級：「et -priv榮幸 進階」
3. 啟用 AWS 金鑰管理程式：
   `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、請輸入秘密金鑰。
5. 確認 AWS KMS 已正確設定：
   `security key-manager external aws show -vserver svm_name`

使用**Azure Key Vault**管理金鑰

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

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

使用AKV的金鑰管理可透過CLI或ONTAP REST API來啟用。

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

開始之前

- 必須執行9.10.1版或更新版本Cloud Volumes ONTAP
- 已安裝Volume Encryption（VE）授權（NetApp Volume Encryption授權會自動安裝在Cloud Volumes ONTAP 向NetApp支援註冊的每個支援系統上）
- 您必須擁有多租戶加密金鑰管理（MT_EK-Mgmt）授權
- 您必須是叢集或SVM管理員
- 現用Azure訂閱

限制

- AKV只能在資料SVM上設定
- Nae 不可使用 AKV 。Nae 需要外部支援的 KMIP 伺服器。

組態程序

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

- Azure應用程式註冊
- 建立Azure用戶端機密
- 建立Azure Key Vault
- 建立加密金鑰
- 建立Azure Active Directory端點（僅限HA）

- 組態Cloud Volumes ONTAP

Azure應用程式註冊

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

建立**Azure**用戶端機密

1. 在Azure入口網站中註冊Azure Key Vault應用程式、選取「**憑證與機密」窗格。
2. 選取「**新用戶端密碼」。輸入有意義的用戶端機密名稱。NetApp建議使用24個月到期日、不過您的特定雲端治理原則可能需要不同的設定。
3. 按一下「新增」以建立用戶端機密。複製「Value*」欄中所列的秘密字串、並將其儲存在安全的位置以供稍後使用 組態Cloud Volumes ONTAP。在您離開頁面後、不會再顯示機密值。

建立**Azure Key Vault**

1. 如果您有現有的Azure Key Vault、您可以將其連線至Cloud Volumes ONTAP 您的整套組態；不過、您必須根據此程序中的設定來調整存取原則。
2. 在Azure入口網站中、瀏覽至「**關鍵故障」區段。
3. 按一下「***+**建立」、然後輸入所需資訊、包括資源群組、地區及價格層級。此外、請輸入保留刪除的保存庫的天數、然後在金鑰保存庫中選取「*啟用清除保護」。
4. 選擇「*下一步」以選擇存取原則。
5. 選取下列選項：
   a. 在「存取組態*」下、選取「資料庫存取原則*」。
   b. 在「資源存取*」下、選取「 Azure磁碟加密」以進行Volume加密*。
6. 選取「**+建立」以新增存取原則。
7. 在「從範本*設定」下、按一下下拉式功能表、然後選取「**金鑰、秘密及憑證管理」範本。
8. 選擇每個下拉式權限功能表（金鑰、秘密、憑證）、然後在功能表清單頂端選擇所有*、以選取所有可用的權限。您應該擁有：
   - 關鍵權限：已選取20項
   - **機密權限：選擇8項
   - 認證權限：16項已選取

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

- [x] Select all
- [x] Get
- [x] List
- [x] Update
- [x] Create
- [x] Import
- [x] Delete
- [x] Recover
- [x] Backup
- [x] Restore

Cryptographic Operations

- [x] Select all
- [x] Decrypt
- [x] Encrypt
- [x] Unwrap Key
- [x] Wrap Key
- [x] Verify
- [x] Sign

Privileged Key Operations

- [x] Select all
- [x] Purge
- [x] Release

Rotation Policy Operations

- [x] Select all
- [x] Rotate
- [x] Get Rotation Policy
- [x] Set Rotation Policy

Secret permissions

Secret Management Operations

- [x] Select all
- [x] Get
- [x] List
- [x] Set
- [x] Delete
- [x] Recover
- [x] Backup
- [x] Restore

Privileged Secret Operations

- [x] Select all
- [x] Purge

Certificate permissions

Certificate Management Operations

- [x] Select all
- [x] Get
- [x] List
- [x] Update
- [x] Create
- [x] Import
- [x] Delete
- [x] Recover
- [x] Backup
- [x] Restore
- [x] Manage Contacts
- [x] Manage Certificate Authorities
- [x] Get Certificate Authorities
- [x] List Certificate Authorities
- [x] Set Certificate Authorities
- [x] Delete Certificate Authorities

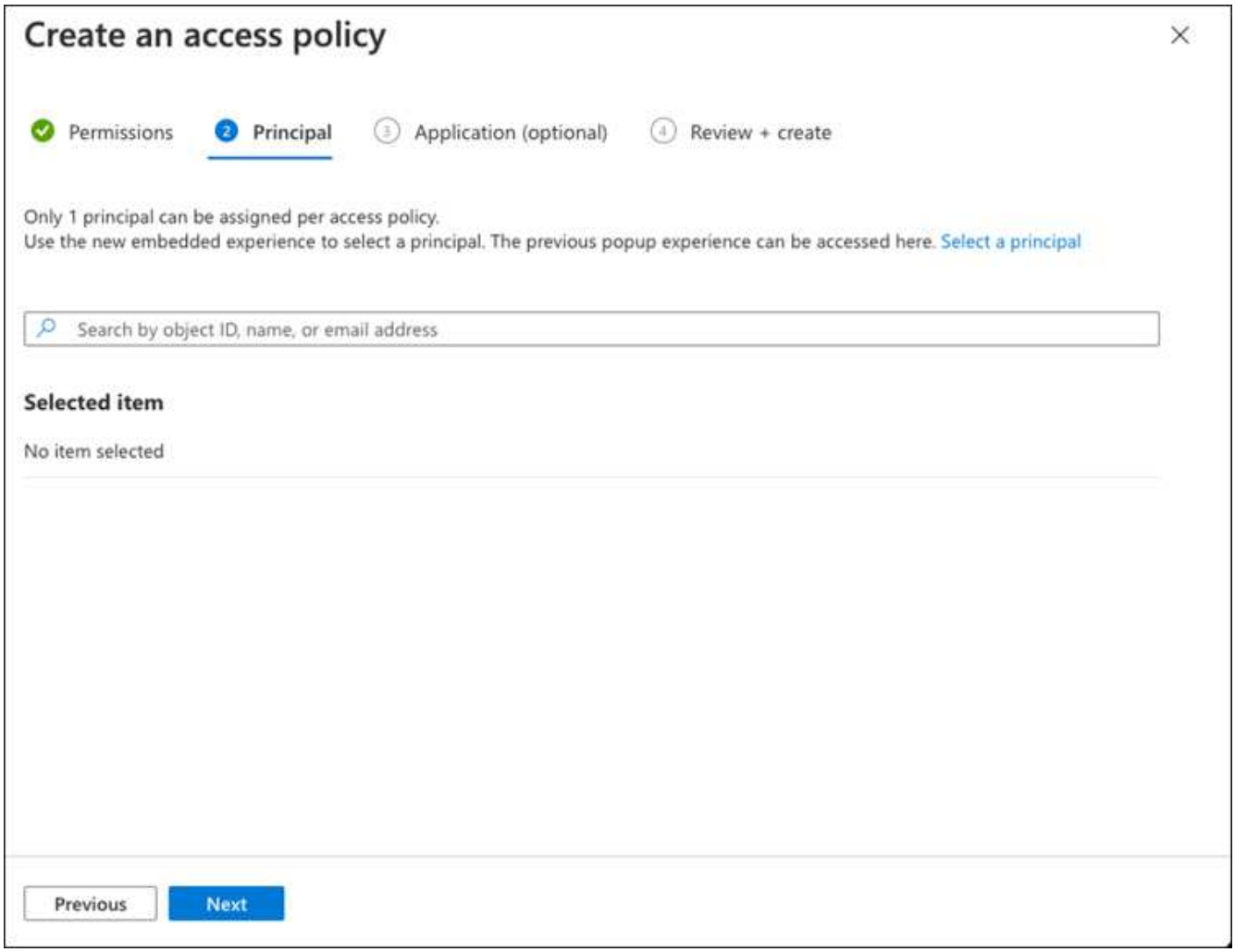
Privileged Certificate Operations

- [x] Select all
- [x] Purge

Previous Next

9. 按一下「下一步」以選取您在其中建立的「*主要」* Azure註冊應用程式 Azure應用程式註冊。選擇「下一步」。

> 每個原則只能指派一個主體。



10. 按兩次「下一步」、直到您抵達「審查並建立」為止。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「審查+建立」來建立金鑰保存庫。（網路存取方法可能由治理原則或您的企業雲端安全團隊規定。）
13. 記錄金鑰庫URI：在您建立的金鑰庫中、瀏覽至「總覽」功能表、然後從右側欄複製「** Vault URI」。您需要此功能、以便稍後進行。

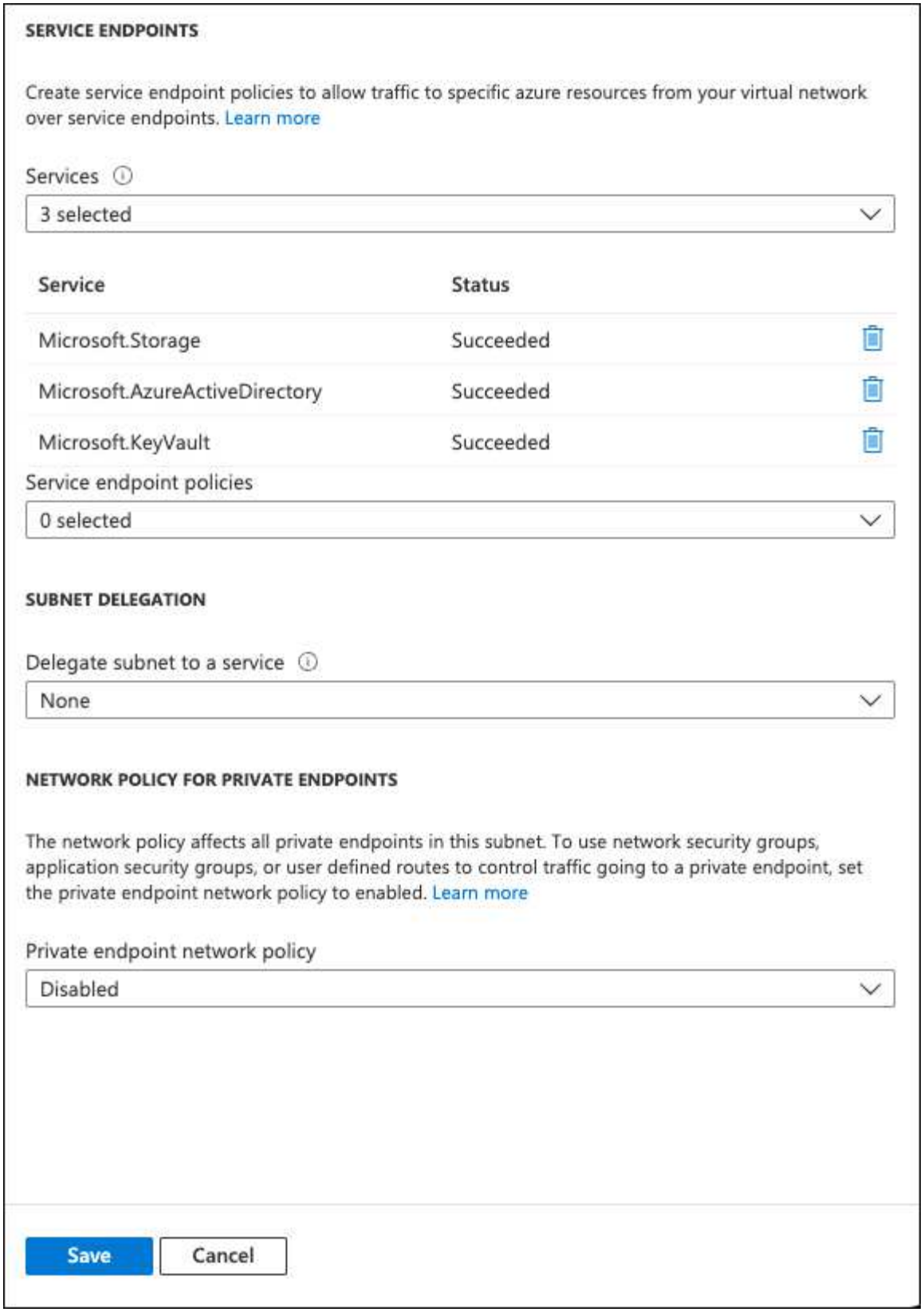
建立加密金鑰

1. 在您為Cloud Volumes ONTAP 之建立的Key Vault功能表中、瀏覽至「** Keys」選項。
2. 選取「產生/匯入」以建立新的金鑰。
3. 將預設選項設為「**產生」。
4. 提供下列資訊：
    - 加密金鑰名稱

    - 金鑰類型：RSA
    - RSA金鑰大小：2048
    - 已啟用：是
5. 選取「建立」以建立加密金鑰。
6. 返回「**按鍵」功能表、然後選取您剛建立的按鍵。
7. 在「目前版本」下方選取金鑰ID、即可檢視金鑰內容。
8. 找到「**金鑰識別碼」欄位。將URI複製到但不包括十六進位字串。

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

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



6. 選取「**儲存」以擷取您的設定。

組態**Cloud Volumes ONTAP**

1. 使用您偏好的SSH用戶端連線至叢集管理LIF。
2. 進入進階權限模式ONTAP ：

```
set advanced -con off
```

3. 識別所需的資料SVM、並驗證其DNS組態：「vserver services name-service DNS show」
   a. 如果所需資料SVM的DNS項目存在、且其中包含Azure DNS項目、則不需要採取任何行動。如果沒有、請為資料SVM新增DNS伺服器項目、以指向Azure DNS、私有DNS或內部部署伺服器。這應該符合叢集管理SVM的項目：「vserver services name-service DNS create -vserver *svm_name*-domain_-name -servers *ip_address*」
   b. 確認已為資料SVM建立DNS服務：「vserver services name-service DNS show」
4. 使用應用程式登錄後儲存的用戶端ID和租戶ID來啟用Azure Key Vault：
   `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`*

   > ◦ `_full_key_URI` 價值必須運用 `<https:// <key vault host name>/keys/<key label>` 格式。

5. 成功啟用 Azure Key Vault 後、請輸入 `client secret value` 出現提示時。
6. 檢查金鑰管理程式的狀態：「安全金鑰管理程式外部azure檢查」輸出內容如下：

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

Vserver: data_svm_name
Node: akvlab01-01

Category: service_reachability
    Status: OK

Category: 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.
```

   如果是 `service_reachability` 狀態不是 `OK`、SVM無法以所有必要的連線和權限來連線至Azure Key Vault服務。請確保您的Azure網路原則和路由不會封鎖您的私有vNet、使其無法到達Azure KeyVault Public端點。如果有、請考慮使用Azure私有端點、從vNet內存取金鑰庫。您可能還需要在SVM上新增靜態主機項目、以解析端點的私有IP位址。

   ◦ `kms_wrapped_key_status` 將會報告 `UNKNOWN` 初始組態時。其狀態將變更為 `OK` 加密第一個磁碟區之後。

7. 選用：建立測試Volume以驗證NVE的功能。

「vol create -vserver *Svm_name*-volume *volVolume _name*-Aggregate *aggr _-size _size*-state online -policy default」

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

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

利用Google的雲端金鑰管理服務來管理金鑰

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

雲端KMS的金鑰管理可透過CLI或ONTAP REST API啟用。

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

開始之前

- 必須執行9.10.1版或更新版本Cloud Volumes ONTAP
- 已安裝Volume Encryption（VE）授權
- 安裝多租戶加密金鑰管理（MTEKM）授權、從Cloud Volumes ONTAP 版本號為E59.12.1 GA開始。
- 您必須是叢集或SVM管理員
- 現用Google Cloud Platform訂閱

限制

- 雲端KMS只能在資料SVM上設定

組態

Google Cloud

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

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

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

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

Cloud Volumes ONTAP

1. 使用您偏好的SSH用戶端連線至叢集管理LIF。
2. 切換至進階權限等級：「et -priv榮幸 進階」
3. 為資料SVM建立DNS。「建立網域C_<project >_.internal -name-servers *server_address*-vserver *Svm_name*」
4. 建立CMEK項目：「安全金鑰管理程式外部GCP啟用-vserver *Svm_name*-project -id *project _-key-ring_name _key_ring_name*-key-ring_location *key_ring_stip*-key-name *key_name*」
5. 出現提示時、請從GCP帳戶輸入服務帳戶Json金鑰。
6. 確認啟用的程序成功：「安全金鑰管理程式外部GCP檢查-vserver *svm_name*」
7. 選用：建立磁碟區以測試加密「volvol create *volvolvole_name*-Aggregate *Aggregate _-vserver _vserver_name*-size 10G」

疑難排解

如果您需要疑難排解、可以跳接上述最後兩個步驟中的原始REST API記錄：

1. "以d為準"
2. "ystemShell -node_node_-command tail -f /mroot/etc/log/mlog/kmip2_client.log"

改善防範勒索軟體的能力

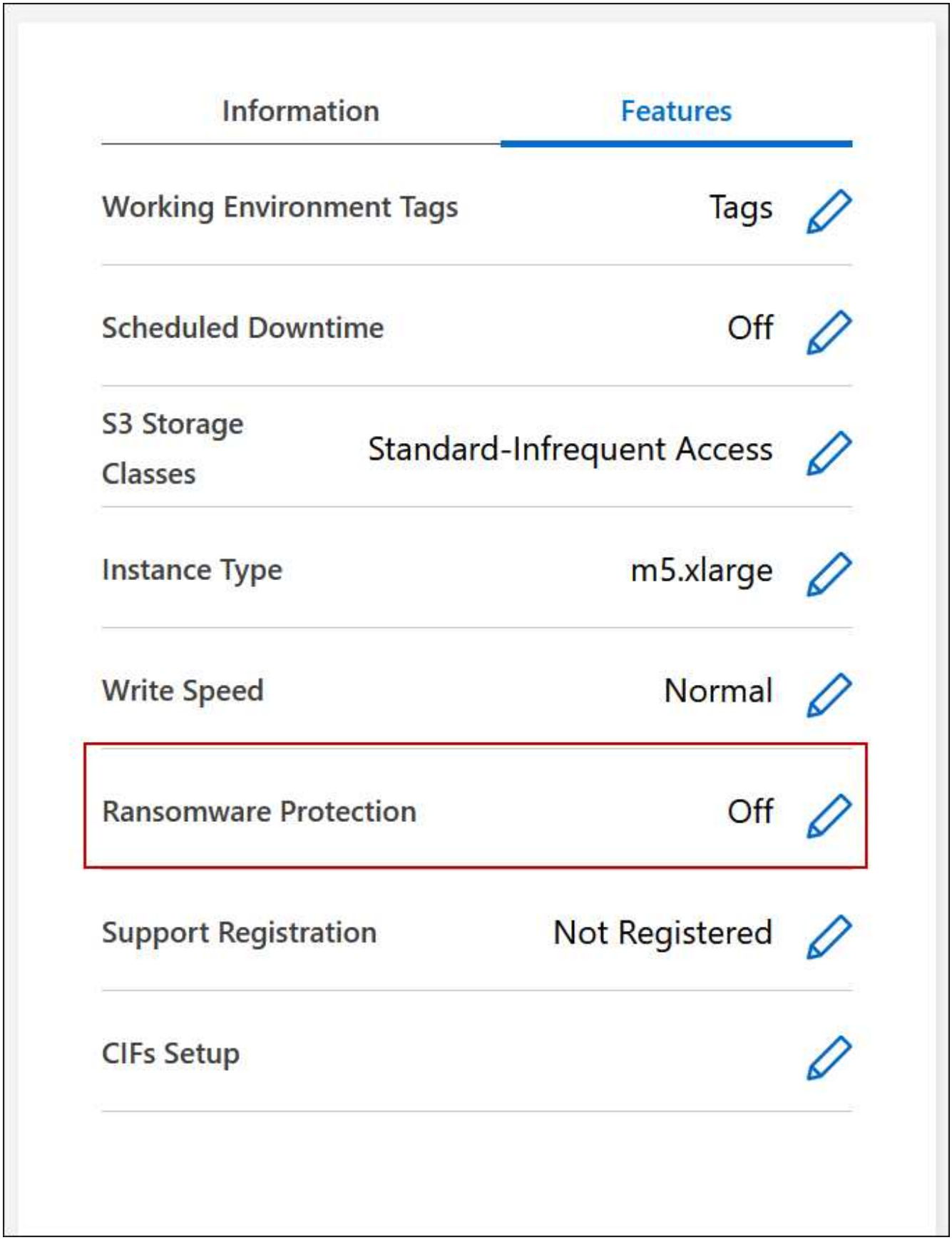
勒索軟體攻擊可能會耗費一定的時間、資源和商譽。BlueXP 可讓您針對勒索軟體實作兩種 NetApp 解決方案：防範常見的勒索軟體副檔名和自動勒索軟體保護（ARP）。這些解決方案可提供有效的工具、以利可見度、偵測和補救。

防止常見勒索軟體檔案副檔名

透過 BlueXP 、勒索軟體保護設定可讓您利用 ONTAP FPolicy 功能來防範常見的勒索軟體檔案副檔名類型。

步驟

1. 在 Canvas 頁面上、按兩下您設定為勒索軟體保護的系統名稱。
2. 在「概述」索引標籤上、按一下「功能」面板、然後按一下 * 勒索軟體保護 * 旁的鉛筆圖示。



3. 實作 NetApp 勒索軟體解決方案：

   a. 如果您的磁碟區未啟用 Snapshot 原則、請按一下「 * 啟動 Snapshot Policy* 」。

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

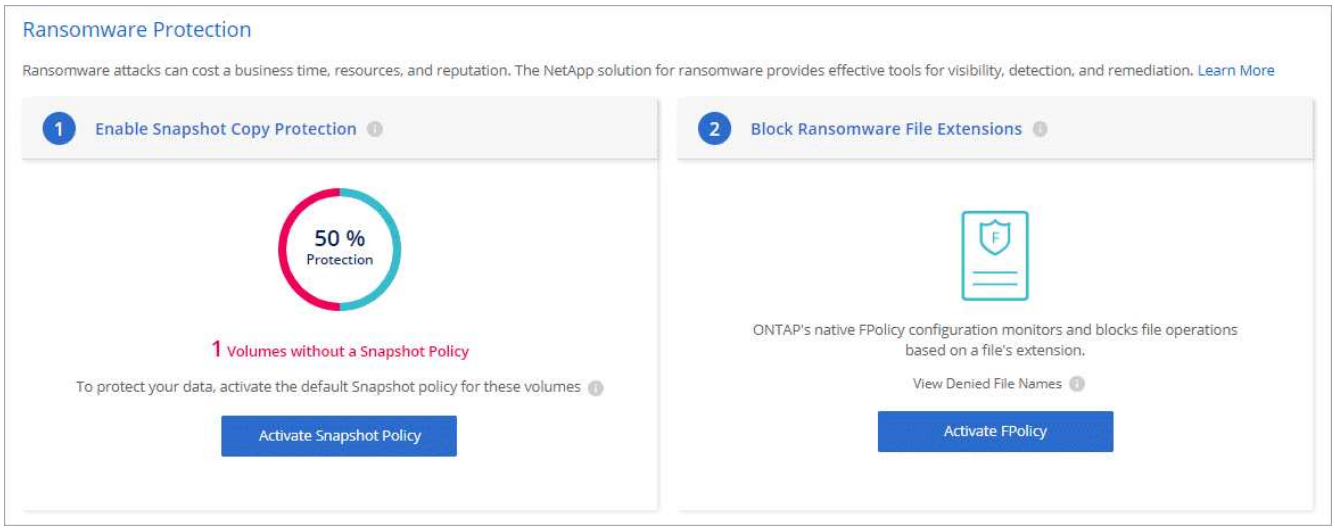
b. 按一下「 * 啟動 FPolicy* 」以啟用 ONTAP 的 FPolicy 解決方案、此解決方案可根據檔案副檔名來封鎖檔案作業。

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

預設FPolicy範圍會封鎖下列副檔名的檔案：

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

> 當您啟動Cloud Volumes ONTAP 有關功能的FPolicy時、BlueXP就會建立這個範圍。此清單是根據常見的勒索軟體檔案類型。您可以使用Cloud Volumes ONTAP 來自於整個CLI的_vserver fpolicy scoon__命令來自訂封鎖的副檔名。



自主勒索軟體保護

Cloud Volumes ONTAP 支援「自動勒索軟體保護」（ARP）功能、可對工作負載執行分析、主動偵測並警告可能表示勒索軟體攻擊的異常活動。

與透過提供的檔案副檔名保護分開 "勒索軟體保護設定"、 ARP 功能會使用工作負載分析、根據偵測到的「異常活動」來警示使用者可能遭受的攻擊。勒索軟體保護設定和 ARP 功能均可搭配使用、以提供全面的勒索軟體保護。

ARP 功能僅適用於以節點為基礎的授權模式和以容量為基礎的授權模式、且僅適用於 BYOL 授權（1 至 36 個月期限）。您必須聯絡您的 NetApp 銷售代表、以購買新的獨立附加授權、以搭配 Cloud Volumes ONTAP 中的 ARP 功能使用。

ARP 授權被視為「浮動」授權、這表示它不受限於單一 Cloud Volumes ONTAP 執行個體、而且可以套用至多個 Cloud Volumes ONTAP 環境。

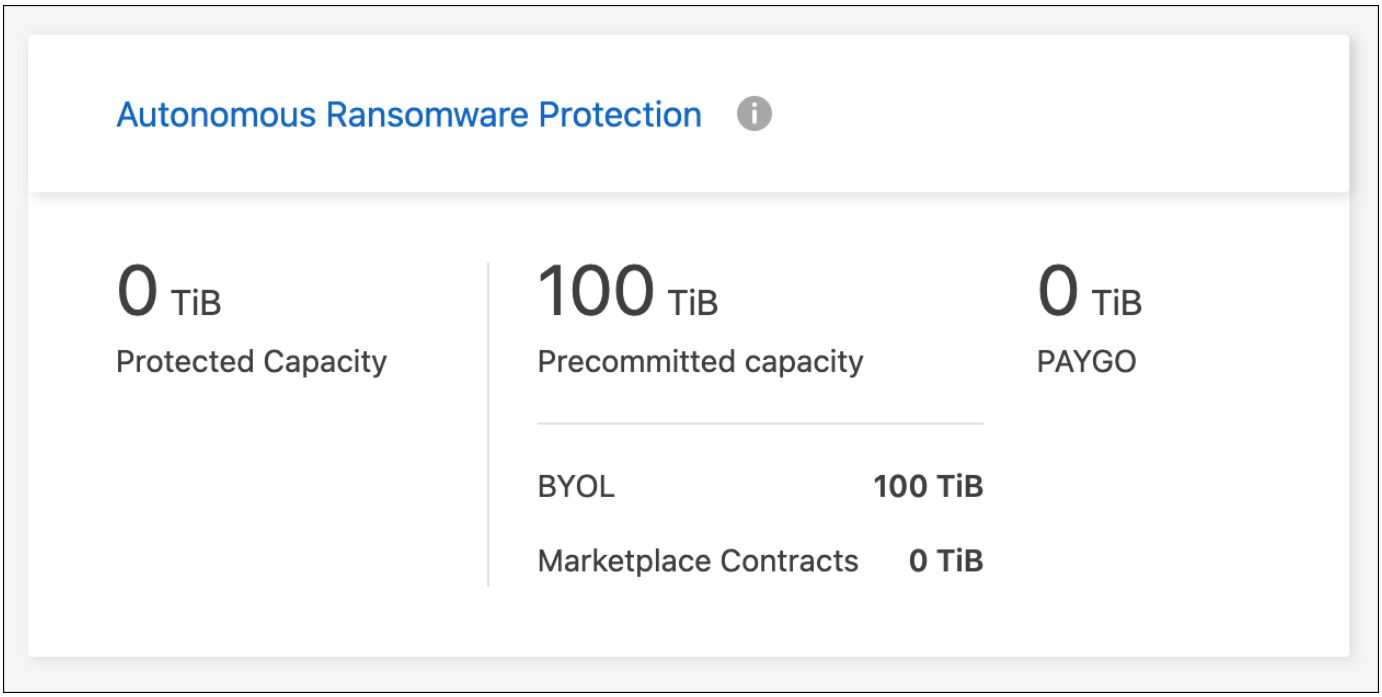
> 在節點型 Cloud Volumes ONTAP 授權中使用 ARP 功能的情況、目前並未反映在 Digital Wallet 中。未來版本的 Digital Wallet 將提供檢視節點型 ARP 使用率的功能。

購買附加授權並將其新增至 Digital Wallet 後、您可以使用 Cloud Volumes ONTAP 以每個磁碟區為基礎來啟用 ARP 。ARP 的收費是根據已啟用 ARP 功能的已配置磁碟區總容量、以磁碟區層級計量。最低授權容量為 1TB 。不過、 ARP 功能沒有最低容量充電量。

已啟用 ARP 的磁碟區具有「學習模式」或「作用中」的指定狀態。任何 ARP 狀態為「已停用」的磁碟區都會排除在充電之外。例如、具有 30 TiB 已配置容量的 Cloud Volumes ONTAP 環境、可選擇僅擁有 15 個 TiB 磁碟區的子集、並啟用 ARP 。

磁碟區的 ARP 組態是透過 ONTAP 系統管理員和 ONTAP CLI 執行。

如需如何使用 ONTAP 系統管理員和 CLI 啟用 ARP 的詳細資訊、請參閱 "啟用自發勒索軟體保護"。



若未取得授權、則無法使用授權功能。

系統管理

升級**Cloud Volumes ONTAP** 版軟體

從Cloud Volumes ONTAP BlueXP升級以取得最新的新功能與增強功能。升級軟體之前、您應該先準備 Cloud Volumes ONTAP 好用的不一樣系統。

升級總覽

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

僅從**BlueXP**升級

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

如何升級

BlueXP提供兩種升級Cloud Volumes ONTAP 途徑：

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

支援的升級途徑

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

目前版本	您可以直接升級至的版本
9.14.0%	9.14.1.
9.13.1.12.9.12.9.	9.14.1.
	9.14.0%
9.13.0	9.13.1.12.9.12.9.
9.12.1%	9.13.1.12.9.12.9.
	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
9.0	9.1
8.3	9.0

請注意下列事項：

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

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

修補程式版本

自 2024 年 1 月起、只有在 BlueXP 中、如果是三個最新版 Cloud Volumes ONTAP 的修補程式版本、才能進行修補程式升級。我們使用最新的 GA 版本來判斷在 BlueXP 中顯示的三個最新版本。例如、如果目前的 GA 版本為 9.13.1 、則 BlueXP 中會出現 9.11.1.9.13.1 的修補程式。如果您想要升級至 9.11.1 版或更低版本的修補程式版本、您需要使用手動升級程序 下載 ONTAP 映像。

根據補充程式（P）版本的一般規則、您可以從一個版本版本升級至目前執行版本或下一個版本的任何 P 版本。

以下是幾個範例：

- 9.13.0 > 9.13.1P15
- 9.12.1 > 9.13.1P2

還原或降級

不Cloud Volumes ONTAP 支援還原或降級至先前版本的功能。

支援註冊

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

> 尚未註冊支援的系統仍會在新版本推出時收到在BlueXP中顯示的軟體更新通知。但您必須先註冊系統、才能升級軟體。

HA中介程序的升級

BlueXP也會在Cloud Volumes ONTAP 更新過程中視需要更新中介執行個體。

使用 C4 、 M4 和 R4 EC2 執行個體類型在 AWS 中升級

Cloud Volumes ONTAP 不再支援 C4 、 M4 和 R4 EC2 執行個體類型。您可以使用這些執行個體類型、將現有部署升級至 Cloud Volumes ONTAP 9.89.12.1 版。在您升級之前、我們建議您 變更執行個體類型。如果您無法變更執行個體類型、則需要 啟用增強的網路功能 升級之前。請閱讀下列各節、深入瞭解如何變更執行個體類型及啟用增強網路功能。

在執行 9.13.0 版及更新版本的 Cloud Volumes ONTAP 中、您無法使用 C4 、 M4 及 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、然後再減少 變更執行個體類型 或是使用 C5 、 m5 和 R5 EC2 執行個體類型部署新的 HA 配對組態、然後移轉資料。

變更執行個體類型

相較於 C5 、 m5 和 R5 EC2 執行個體類型、 C4 、 M4 和 R4 EC2 執行個體類型、每個節點的磁碟數量都會增加。如果您執行的 C4 、 M4 或 R4 EC2 執行個體的每個節點磁碟數低於 C5 、 m5 和 R5 執行個體的每個節點磁碟可用量上限、您可以將 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EC2執行個體類型Cloud Volumes ONTAP 以供使用"

如果您無法變更執行個體類型、請遵循中的步驟 [啟用增強的網路功能]。

啟用增強的網路功能

若要升級至 Cloud Volumes ONTAP 9.8 版及更新版本、您必須在執行 C4 、 M4 或 R4 執行個體類型的叢集上啟用 *Enhanced networking* 。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 等增強型網路"。

準備升級

執行升級之前、您必須先確認系統已就緒、並進行任何必要的組態變更。

- [計畫停機時間]
- [確認自動恢復功能仍啟用]
- 暫停SnapMirror傳輸
- 驗證Aggregate是否在線上
- [確認所有的生命都在主連接埠上]

計畫停機時間

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

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

工作階段導向的通訊協定可能會在升級期間對某些區域的用戶端和應用程式造成不良影響。如需詳細資訊、 "請參閱 ONTAP 文件"

確認自動恢復功能仍啟用

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

"供應說明文件：設定自動恢復的命令 ONTAP"

暫停**SnapMirror**傳輸

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

> 雖然 BlueXP 備份與還原使用 SnapMirror 實作來建立備份檔案（稱為 SnapMirror Cloud ）、但系統升級時不需要暫停備份。

關於這項工作

這些步驟說明如何使用系統管理程式來執行 9.3 版及更新版本。

步驟

1. 從目的地系統登入System Manager。

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

   > 您要從哪個電腦存取BlueXP、必須有連到Cloud Volumes ONTAP 該系統的網路連線。例如、您可能需要從雲端供應商網路中的跨接主機登入BlueXP。

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

驗證**Aggregate**是否在線上

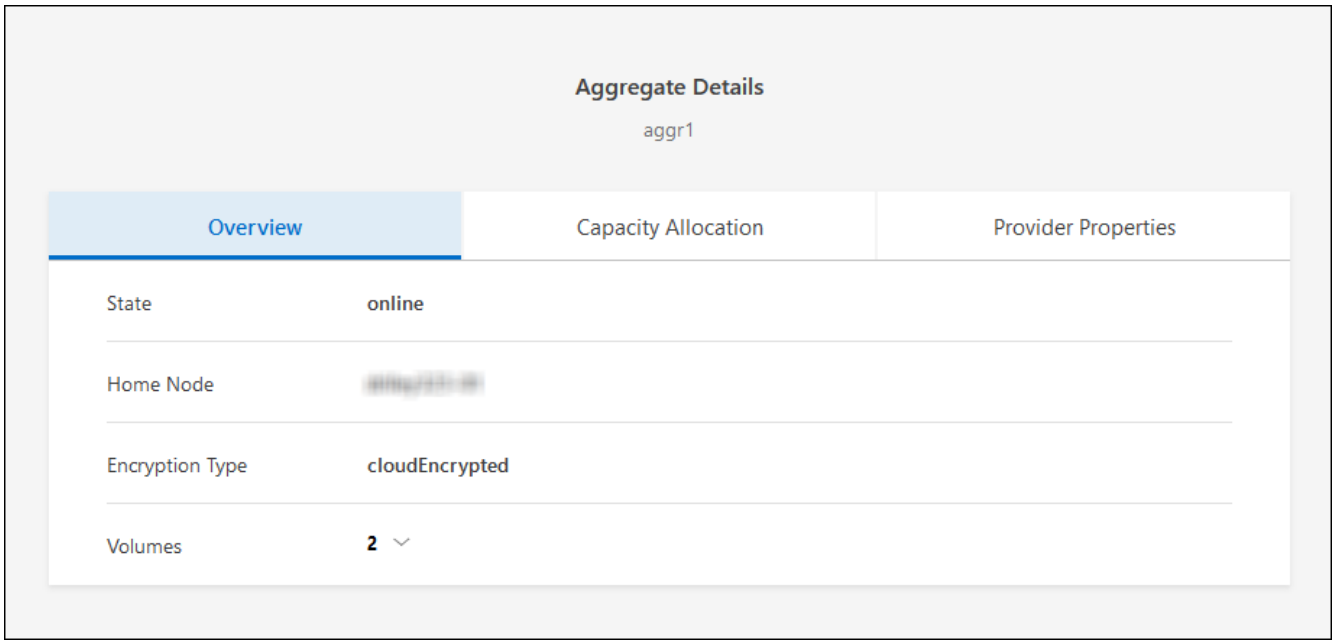
更新軟體之前、必須先在線上安裝適用於 Cloud Volumes ONTAP 此功能的 Aggregate 。在大多數的組態中、Aggregate 都應該處於線上狀態、但如果沒有、則應該將其上線。

關於這項工作

這些步驟說明如何使用系統管理程式來執行 9.3 版及更新版本。

步驟

1. 在工作環境中、按一下 * Aggregate * 標籤。
2. 在 Aggregate 標題下、按一下「橢圓」按鈕、然後選取 * 檢視 Aggregate details* 。



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

確認所有的生命都在主連接埠上

在升級之前、所有的生命體都必須位於主連接埠上。請參閱的 ONTAP 文件 "確認所有的生命都在主連接埠上"。

如果發生升級失敗錯誤、請參閱 "知識庫文章「 Cloud Volumes ONTAP 升級失敗」"。

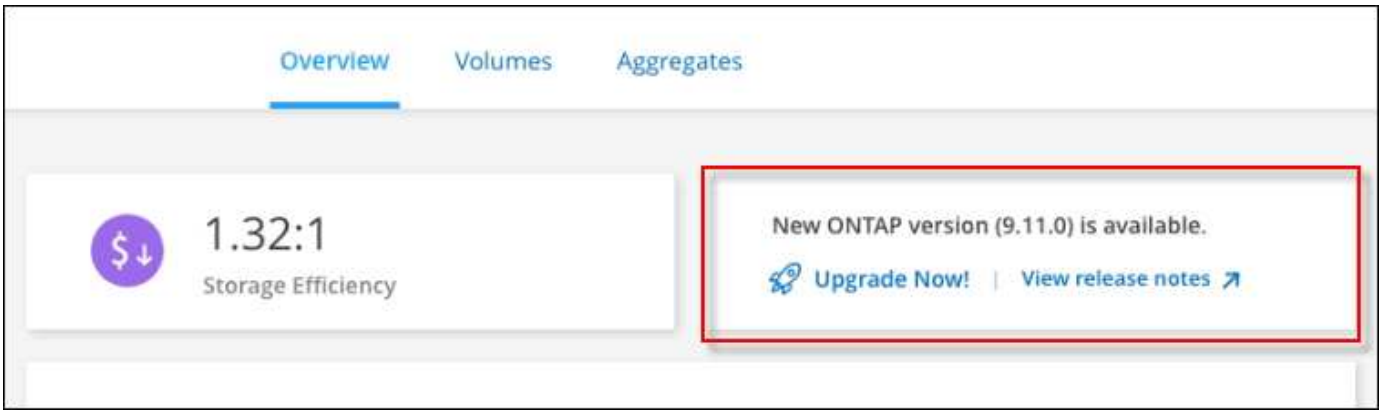
升級Cloud Volumes ONTAP

當有新版本可供升級時、BlueXP會通知您。您可以從此通知開始升級程序。如需詳細資訊、請參閱 從BlueXP通知升級。

使用外部URL上的映像執行軟體升級的另一種方法。如果BlueXP無法存取S3儲存區來升級軟體、或是您已獲得修補程式、此選項很有幫助。如需詳細資訊、請參閱 從URL提供的映像升級。

從BlueXP通知升級

當Cloud Volumes ONTAP 有新版Cloud Volumes ONTAP 的功能時、BlueXP會在不工作環境中顯示通知：



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

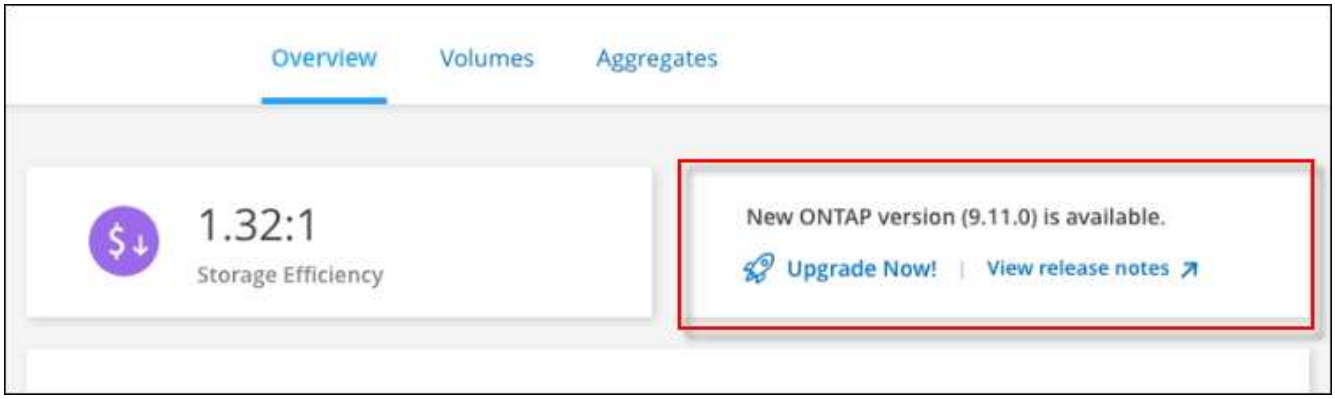
開始之前

在Cloud Volumes ONTAP 這個系統上、不能進行諸如Volume或Aggregate建立等BlueXP作業。

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 選取工作環境。

   如果有新版本可用、則會在「概觀」索引標籤中顯示通知：

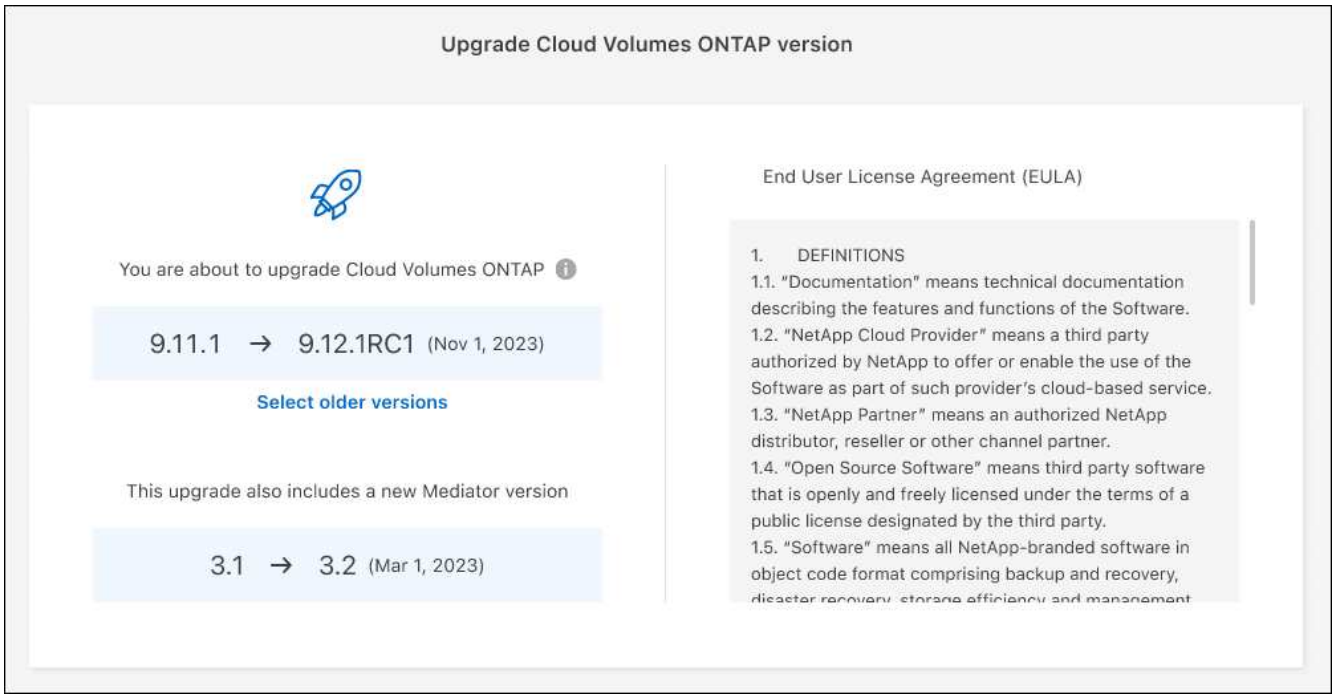


3. 如果有新版本可用、請按一下 * 立即升級！ *

> 您必須先擁有 NetApp 支援網站 帳戶、才能透過 BlueXP 通知升級 Cloud Volumes ONTAP 。

4. 在「升級 Cloud Volumes ONTAP 」頁面中、閱讀 EULA 、然後選取 * 我閱讀並核准 EULA * 。
5. 按一下*升級*。

> 「升級 Cloud Volumes ONTAP 」頁面預設會選取最新可用的 Cloud Volumes ONTAP 版本進行升級。如果有舊版 Cloud Volumes ONTAP 、您可以按一下 * 選擇舊版 * 來選擇升級版本。請參閱 "支援的升級路徑清單" 根據您目前的 Cloud Volumes ONTAP 版本、取得適當的升級路徑。



6. 若要檢查升級狀態、請按一下「設定」圖示、然後選取 * 時間表 * 。

結果

BlueXP會啟動軟體升級。軟體更新完成後、您可以在工作環境中執行動作。

完成後

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

從**URL**提供的映像升級

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

開始之前

- 在Cloud Volumes ONTAP 這個系統上、不能進行諸如Volume或Aggregate建立等BlueXP作業。
- 如果您使用HTTPS來裝載ONTAP 資訊影像、升級可能會因為SSL驗證問題而失敗、因為遺失憑證。因應措施是產生並安裝CA簽署的憑證、以用於ONTAP 在EXP和BlueXP之間進行驗證。

  前往NetApp知識庫檢視逐步指示：

  "NetApp KB：如何將BlueXP設定為HTTPS伺服器、以裝載升級映像"

步驟

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

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

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

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

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

   有兩種路徑可供使用。正確的路徑取決於您的Connector版本。

   - 「/opt/application/netapp/cloudmanager/dock_occm/data/ontap / imes/」
   - /op/application/NetApp/cloudmanager/ontONTAP /映像/
5. 在 BlueXP 的工作環境中、按一下 * 。 （橢圓圖示） * 、然後按一下 * 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 * 變更映像 * 。

   如果您將軟體映像複製到上述路徑中的Connector、請輸入下列URL：

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

   在 URL 中， * image-file-name* 必須遵循格式 "cot.image.9.13.1p2.tgz" 。

7. 按 * Proceed* 確認。

結果

BlueXP會啟動軟體更新。軟體更新完成後、即可在工作環境中執行動作。

完成後

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

修正使用**Google Cloud NAT**閘道時的下載失敗

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

步驟

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

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

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

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

"深入瞭解/occm/config API呼叫"。

註冊隨用隨付系統

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

向 NetApp 註冊 PAYGO 系統時、必須 ONTAP 使用任何方法來升級 __LW_NETAPP 軟體 "本頁說明"。

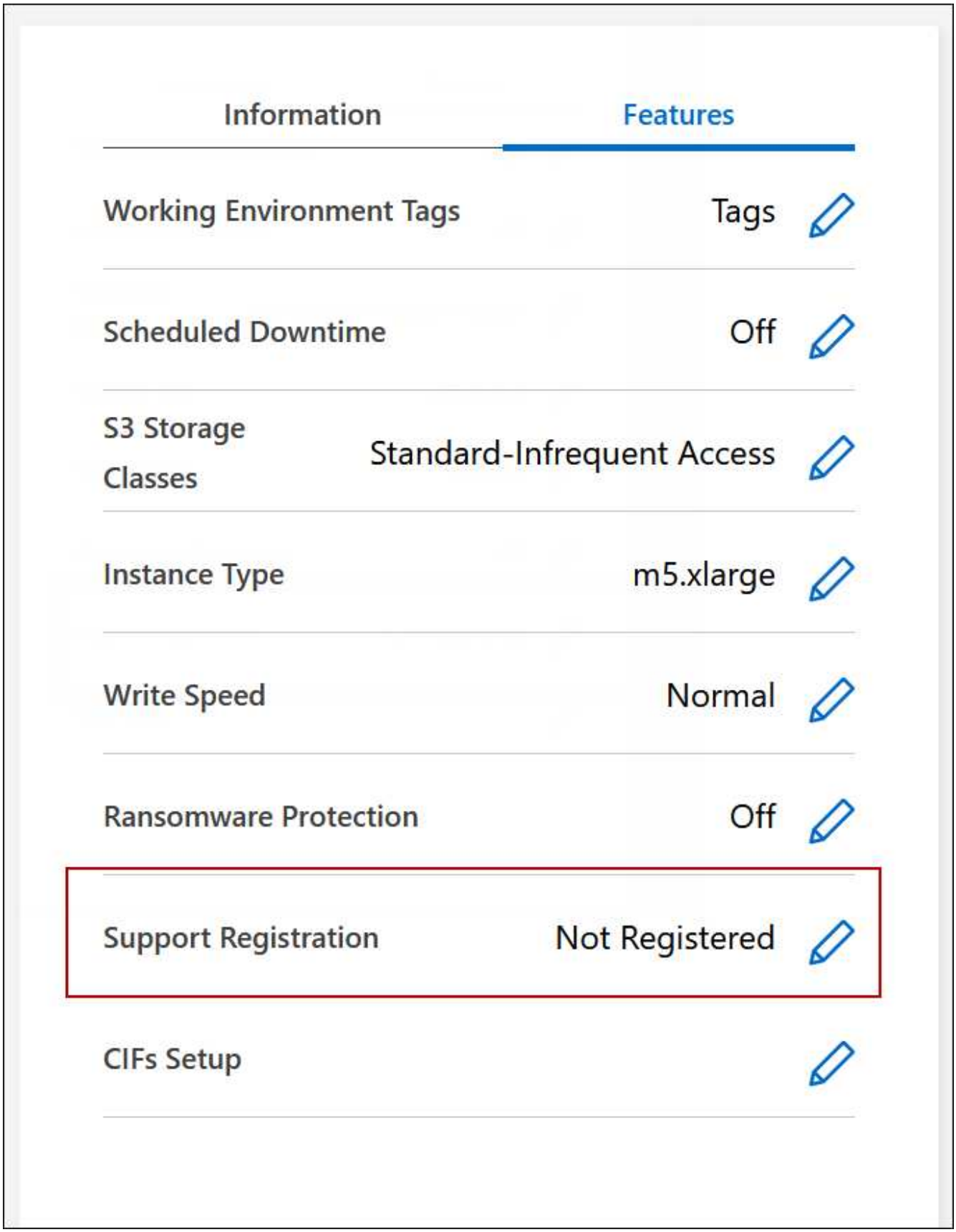
尚未註冊支援的系統仍會在新版本推出時收到在BlueXP中顯示的軟體更新通知。但您必須先註冊系統、才能升級軟體。

步驟

1. 如果NetApp 支援網站 您尚未將您的支援帳戶新增至藍圖XP、請前往*帳戶設定*、立即新增。

   "瞭解如何新增 NetApp 支援網站帳戶"。

2. 在「 Canvas 」頁面上、按兩下您要登錄的系統名稱。
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 支援網站帳戶、然後按一下 * 註冊 * 。

結果

BlueXP向NetApp註冊系統。

管理 **Cloud Volumes ONTAP** 功能不全

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

排程 **Cloud Volumes ONTAP** 自動關閉功能

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

關於這項工作

- 當您排程自動關閉Cloud Volumes ONTAP 您的作業系統時、如果正在進行作用中的資料傳輸、則BlueXP會將關機時間延後。

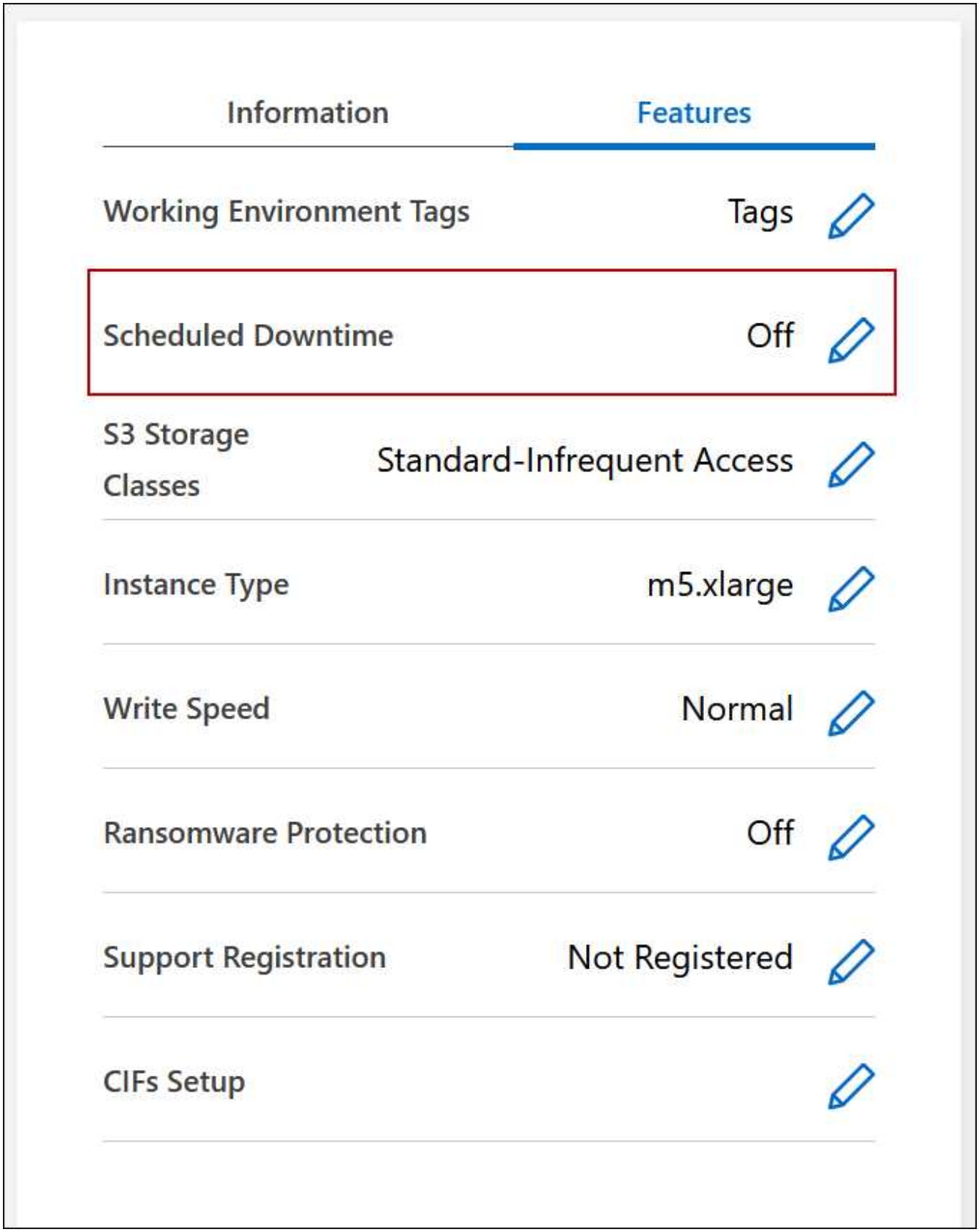
  在傳輸完成後、BlueXP會關閉系統。

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

  只有在執行手動關機時、才會自動建立快照、如下一節所述。

步驟

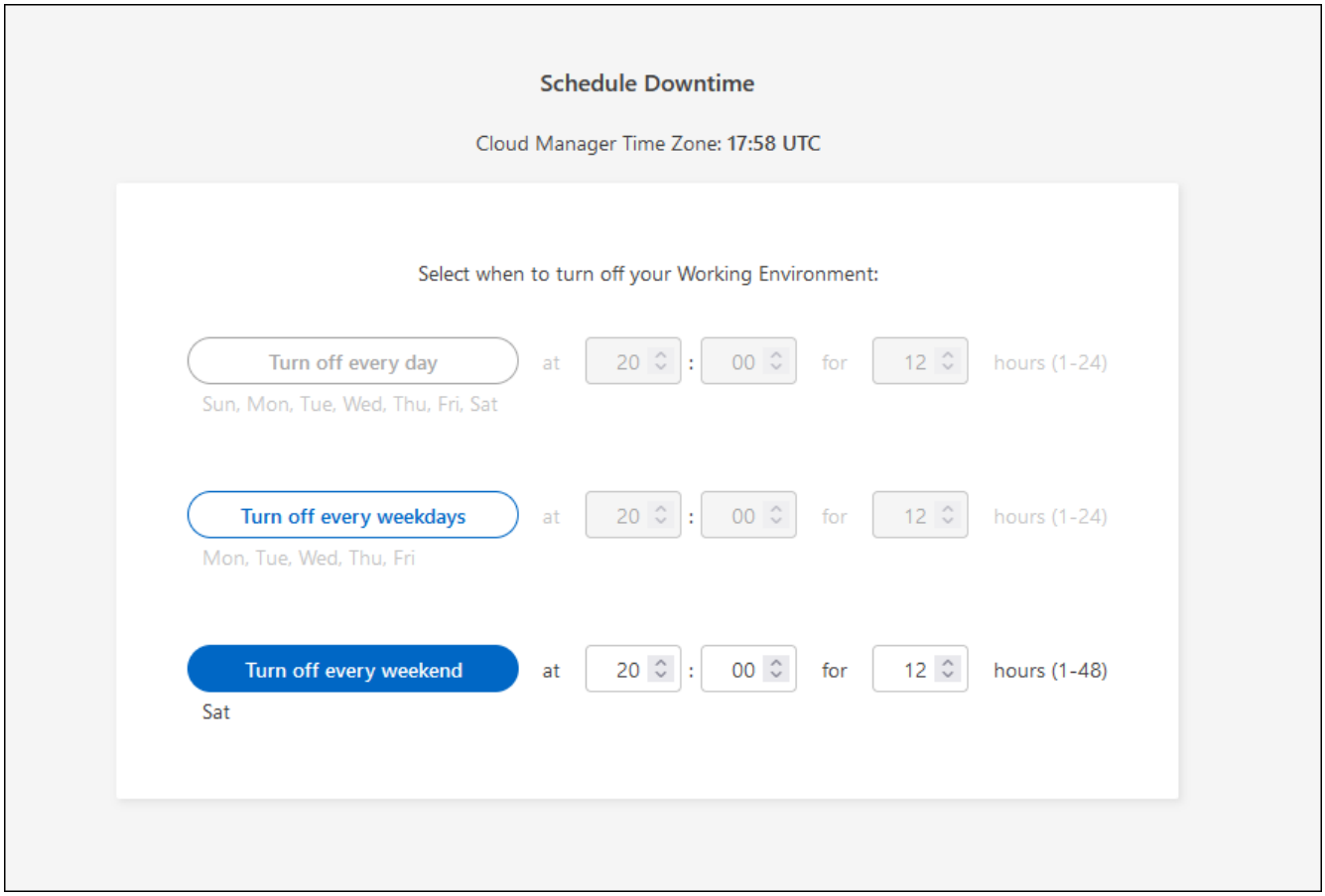
1. 在 Canvas 頁面上、按兩下所需的工作環境。
2. 在「總覽」索引標籤上、按一下「功能」面板、然後按一下 * 排程停機 * 旁的鉛筆圖示。



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

- 範例 *

下圖顯示一個排程、指示 BlueXP 每週六下午 20 ： 00 關閉系統（下午 8 ： 00） 12 小時。每週一上午12：00、BlueXP會重新啟動系統



4. 按一下「 * 儲存 * 」。

結果

BlueXP會儲存排程。「功能」面板下方的對應排程停機項目會顯示為「開啟」。

停止 **Cloud Volumes ONTAP**

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

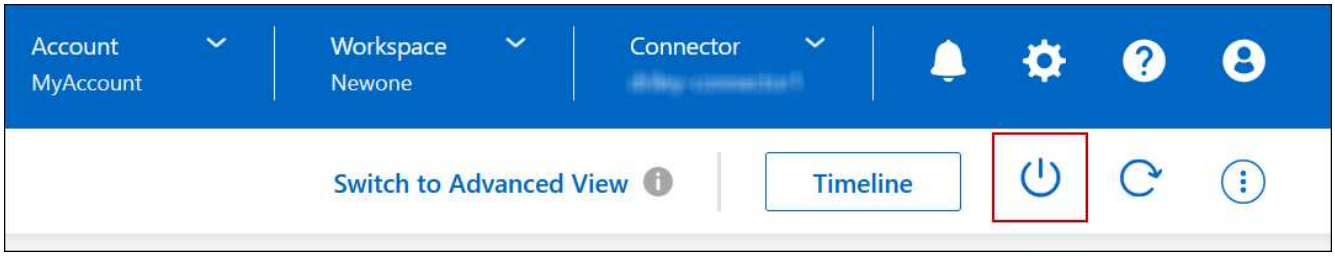
> 為降低成本、BlueXP會定期刪除較舊的根磁碟和開機磁碟快照。根磁碟和開機磁碟只會保留兩個最新的快照。

關於這項工作

當您停止HA配對時、BlueXP會關閉兩個節點。

步驟

1. 在工作環境中、按一下 * 關閉 * 圖示。



2. 保留建立快照的選項、因為快照可以啟用系統還原。
3. 按一下 * 關閉 * 。

   停止系統可能需要幾分鐘的時間。您可以稍後從工作環境頁面重新啟動系統。

   快照會在重新開機時自動建立。

使用 NTP 同步系統時間

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

使用指定NTP伺服器 "BlueXP API" 或從使用者介面進行 "建立CIFS伺服器"。

修改系統寫入速度

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

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

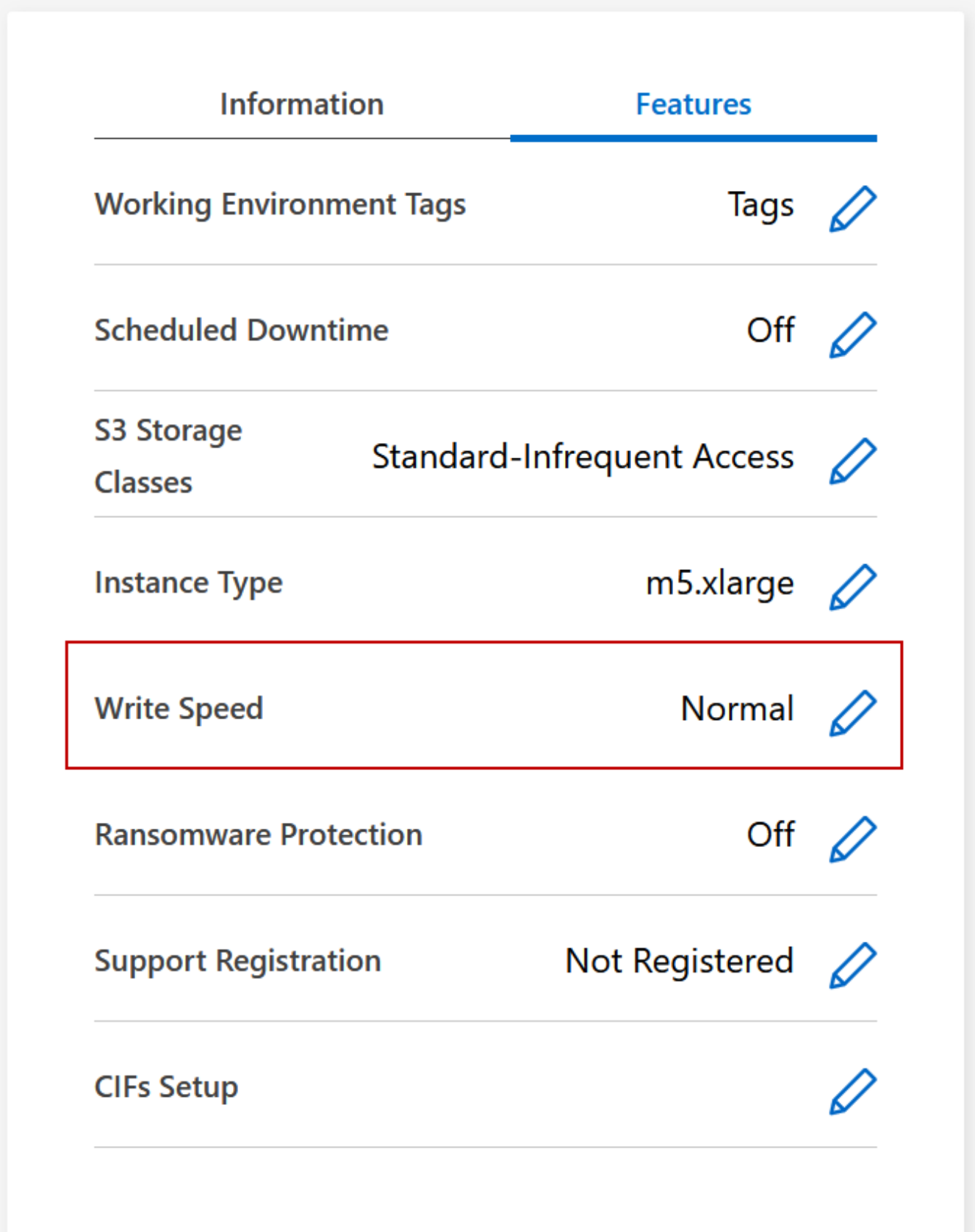
在變更寫入速度之前、您應該先進行 "瞭解一般與高設定之間的差異"。

關於這項工作

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

步驟

1. 在「 Canvas 」頁面上、按兩下您設定為寫入速度的系統名稱。
2. 在「總覽」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」、則必須閱讀「我瞭解 … 」聲明、並勾選方塊以確認。

> 從9.13.0版開始、Google Cloud中的「*高速*寫入速度Cloud Volumes ONTAP 」選項可搭配支援。

4. 按一下 * 儲存 * 、檢閱確認訊息、然後按一下 * 核准 * 。

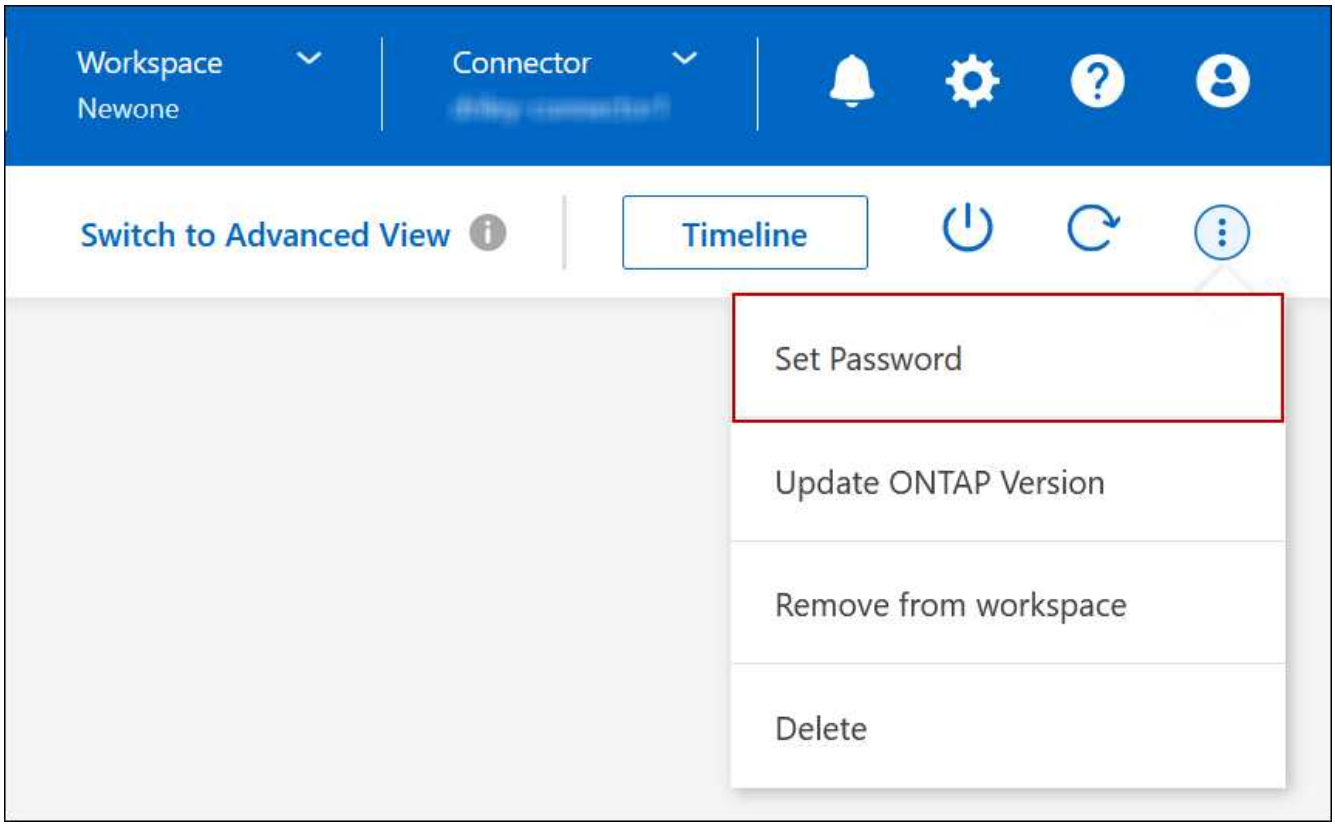
變更Cloud Volumes ONTAP 密碼以供使用

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

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

步驟

1. 在「畫布」頁面上、按兩下 Cloud Volumes ONTAP 工作環境的名稱。
2. 在 BlueXP 主控台的右上角、按一下橢圓圖示、然後選取 * 設定密碼 * 。



新密碼必須與您最近使用的六個密碼之一不同。

新增、移除或刪除系統

將現有Cloud Volumes ONTAP 的不只是系統新增至藍圖XP

您可以探索並新增Cloud Volumes ONTAP 現有的元件系統至藍圖XP。如果您部署了新

的BlueXP系統、您可能會這麼做。

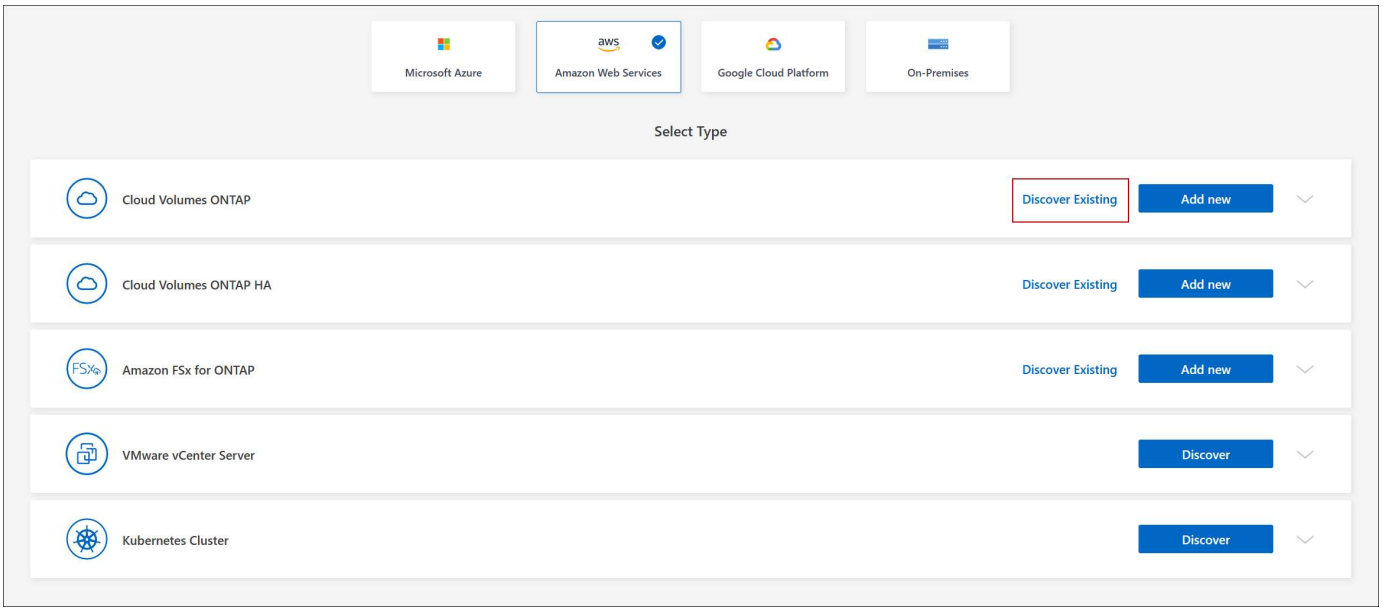
開始之前

您必須知道 Cloud Volumes ONTAP 該密碼才能使用此功能。

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按一下「 * 新增工作環境 * 」。
3. 選取系統所在的雲端供應商。
4. 選擇 Cloud Volumes ONTAP 哪種類型的系統。
5. 按一下連結以探索現有系統。

+



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

結果

BlueXP會將Cloud Volumes ONTAP 這個實例新增到工作區。

移除 **Cloud Volumes ONTAP** 運作環境

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

關於這項工作

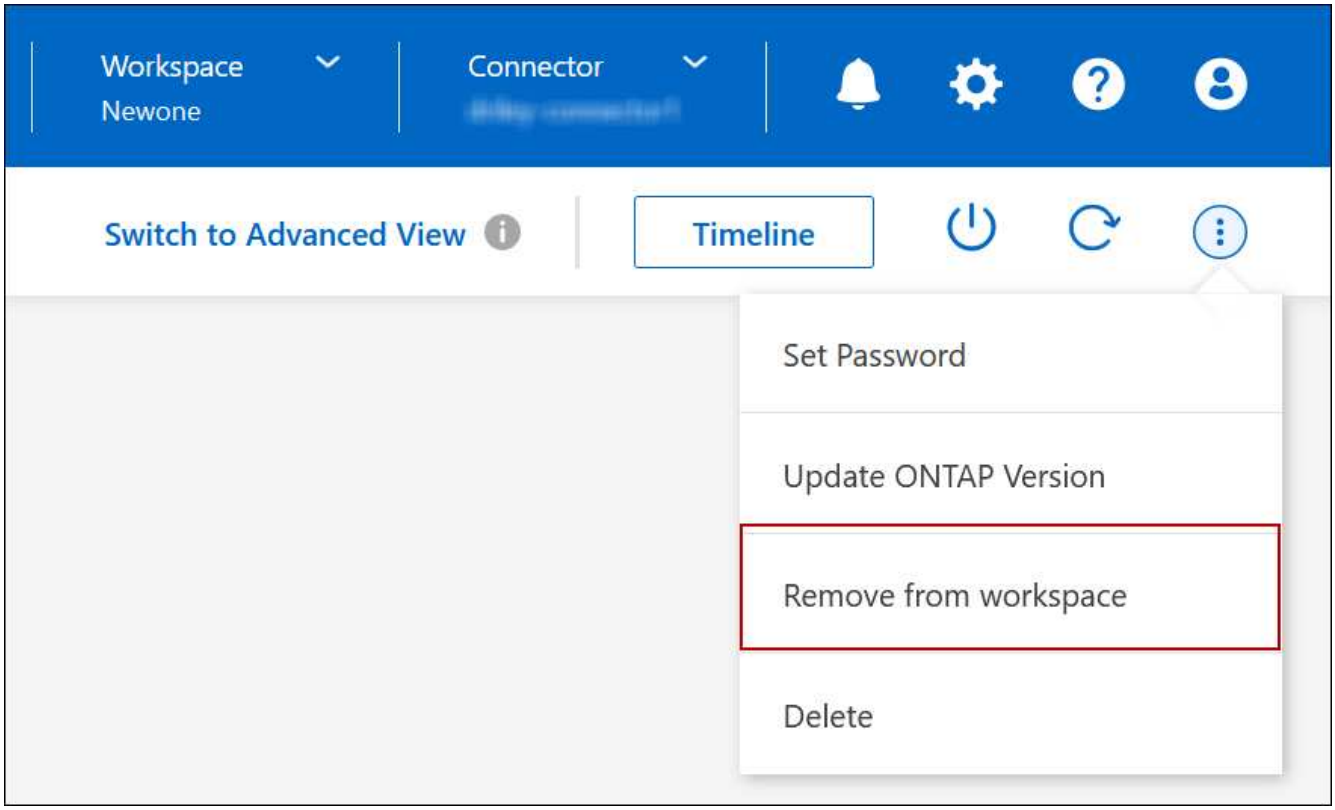
移除Cloud Volumes ONTAP 功能不正常的環境、將其從藍圖XP移除。它不會刪除 Cloud Volumes ONTAP 此作業系統。您稍後可以重新探索工作環境。

從BlueXP移除工作環境可讓您執行下列動作：

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

步驟

1. 在 Canvas 頁面上、按兩下您要移除的工作環境。
2. 在 BlueXP 主控台的右上角、按一下橢圓圖示、然後選取 * 從工作區移除 * 。



3. 在「從工作區檢閱」視窗中、按一下 * 移除 * 。

結果

BlueXP移除工作環境。使用者可隨時從「畫版」頁面重新探索此工作環境。

刪除**Cloud Volumes ONTAP** 一個系統

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

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

當您刪除工作環境時、其他服務所管理的資源、例如 BlueXP 備份和還原的備份、以及 BlueXP 分類的執行個體、都不會被刪除。您必須自行手動刪除。如果您沒有、您將繼續收取這些資源的費用。

當您Cloud Volumes ONTAP 的雲端供應商部署了支援功能時、就能在執行個體上提供終止保護。此選項有助於防止意外終止。

步驟

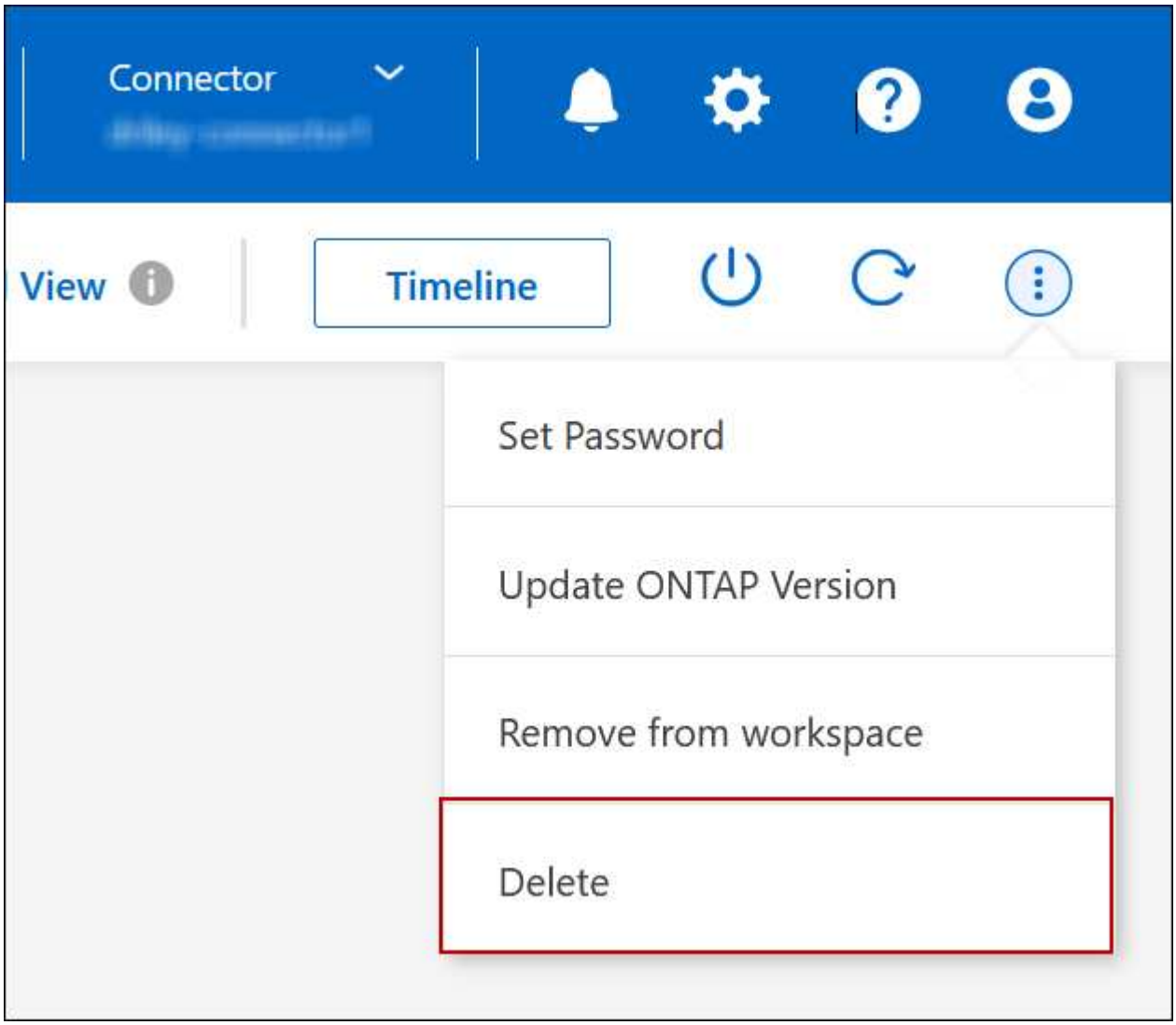
1. 如果您在工作環境中啟用 BlueXP 備份與還原、請先判斷是否仍需要備份資料、然後再決定 "如有必要、請刪除備份"。

   BlueXP 備份與還原在設計上不受 Cloud Volumes ONTAP 的保護。BlueXP 備份與還原不會在您刪除 Cloud Volumes ONTAP 系統時自動刪除備份、而且在刪除系統之後、 UI 目前不支援刪除備份。

2. 如果您在此工作環境中啟用 BlueXP 分類、且沒有其他工作環境使用此服務、則您必須刪除該服務的執行個體。

   "深入瞭解 BlueXP 分類執行個體"。

3. 刪除Cloud Volumes ONTAP 這個作業環境。
   a. 在「畫版」頁面上、按兩下Cloud Volumes ONTAP 您要刪除的「紙張工作環境」名稱。
   b. 在 BlueXP 主控台的右上角、按一下橢圓圖示、然後選取 * 刪除 * 。



c. 在刪除工作環境視窗下、輸入工作環境的名稱、然後按一下 * 刪除 * 。

   刪除工作環境最多可能需要 5 分鐘。

AWS管理

變更EC2執行個體類型Cloud Volumes ONTAP 以供使用

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

關於這項工作

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

  "供應說明文件：設定自動恢復的命令 ONTAP"

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

  對於單一節點系統、 I/O 會中斷。

  對於 HA 配對、變更不中斷營運。HA 配對可繼續提供資料。

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

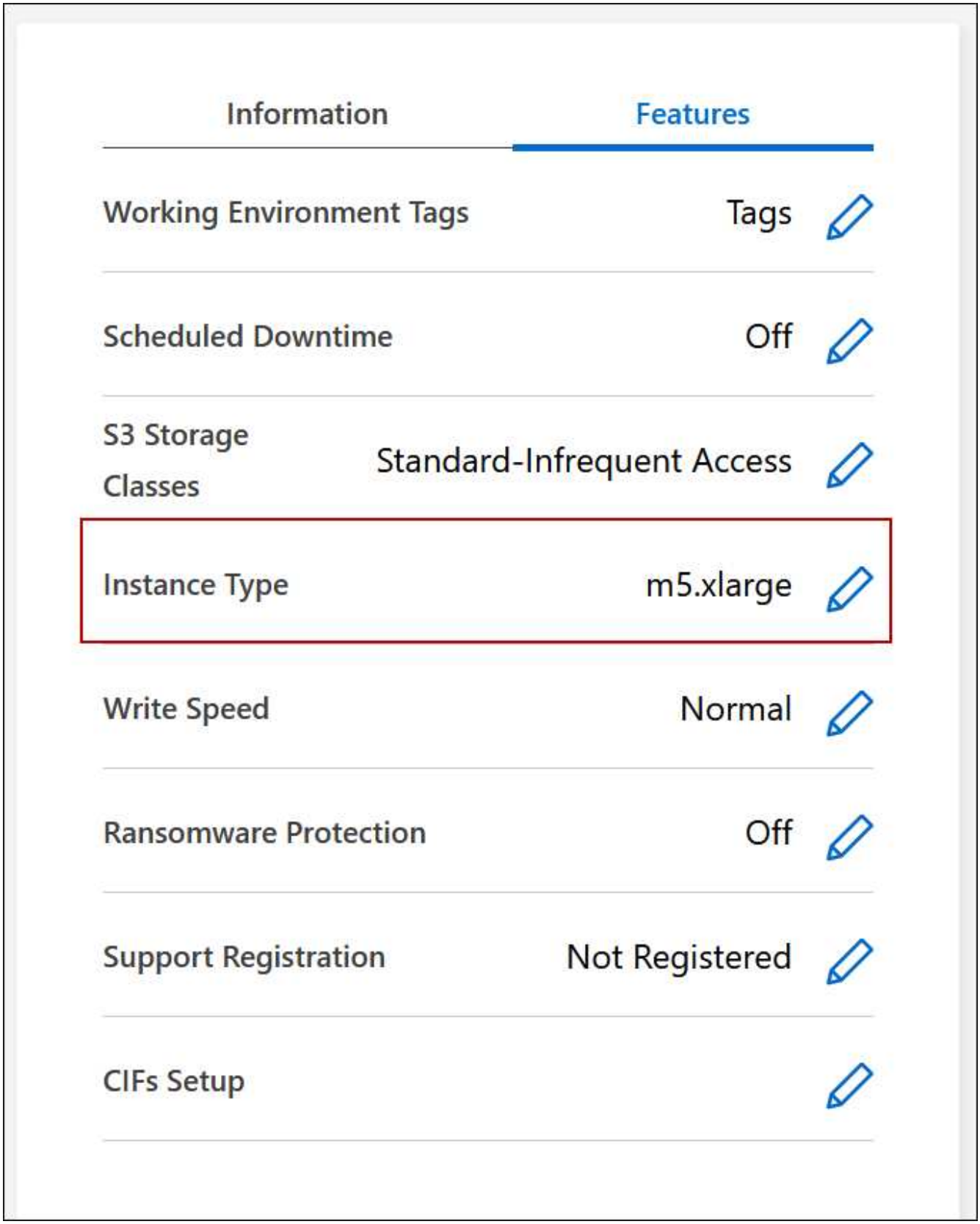
參考資料

如需 AWS 中支援的執行個體類型清單、請參閱 "支援的 EC2 執行個體"。

如果您無法從 C4 、 M4 或 R4 執行個體變更執行個體類型、請參閱知識庫文章 "無法將執行個體類型從 R4 變更為 R5 、但發生磁碟數錯誤"。

步驟

1. 在 Canvas 頁面上、選取工作環境。
2. 在「概述」標籤上、按一下「功能」面板、然後按一下「 * 執行個體類型 * 」旁邊的鉛筆圖示。



a. 如果您使用的是節點型 PAYGO 授權、您可以選擇不同的授權和執行個體類型、方法是按一下 * 授權類型 * 旁的鉛筆圖示。

3. 選擇執行個體類型、選取核取方塊以確認您瞭解變更的影響、然後按一下 * 變更 * 。

結果

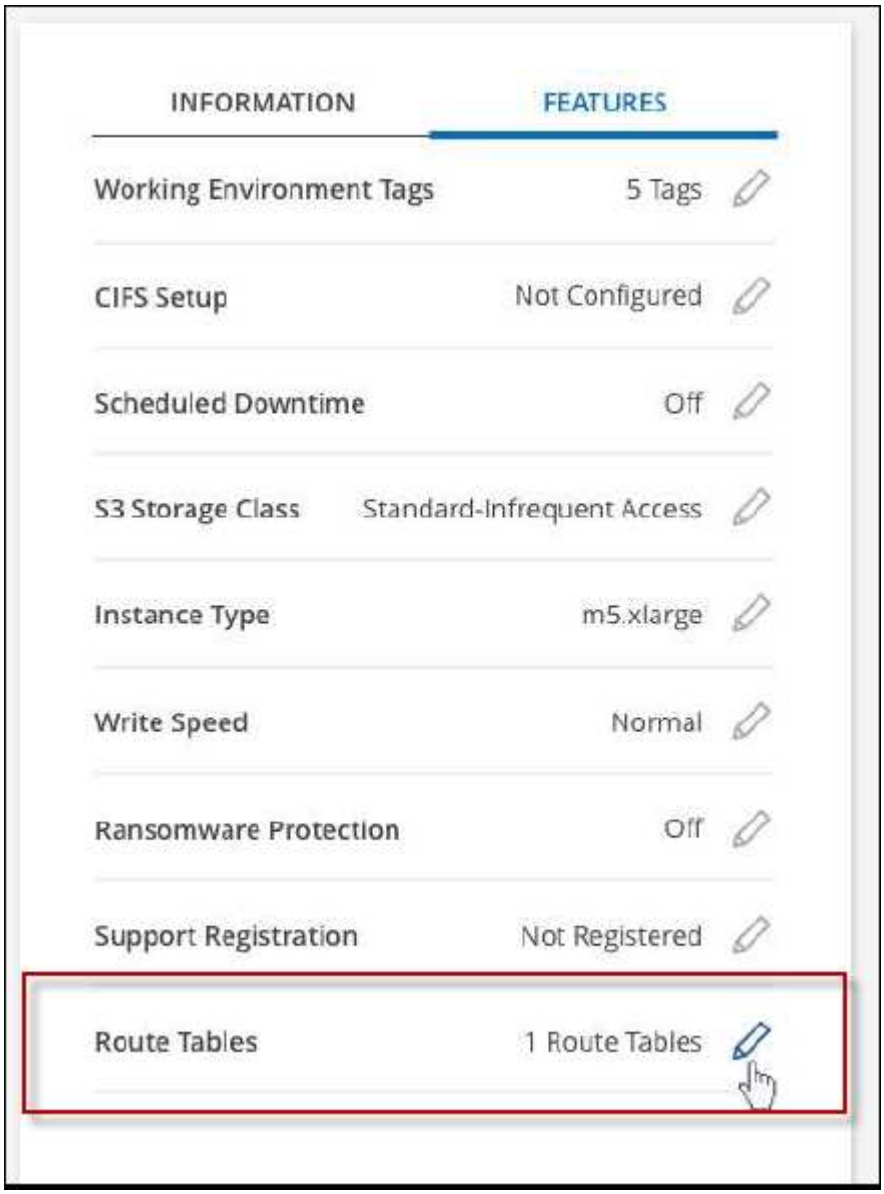
以新組態重新開機。 Cloud Volumes ONTAP

在多個**AZs**中變更**HA**配對的路由表

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

步驟

1. 在 Canvas 頁面上、選取工作環境。
2. 在「總覽」標籤上、按一下「功能」面板、然後按一下「 * 路由表 * 」旁邊的鉛筆圖示。



3. 修改所選路由表的清單、然後按一下「 * 儲存 * 」。

結果

BlueXP會傳送AWS要求來修改路由表。

Azure管理

變更Azure VM類型Cloud Volumes ONTAP 以供使用

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

關於這項工作

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

  "供應說明文件：設定自動恢復的命令 ONTAP"

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

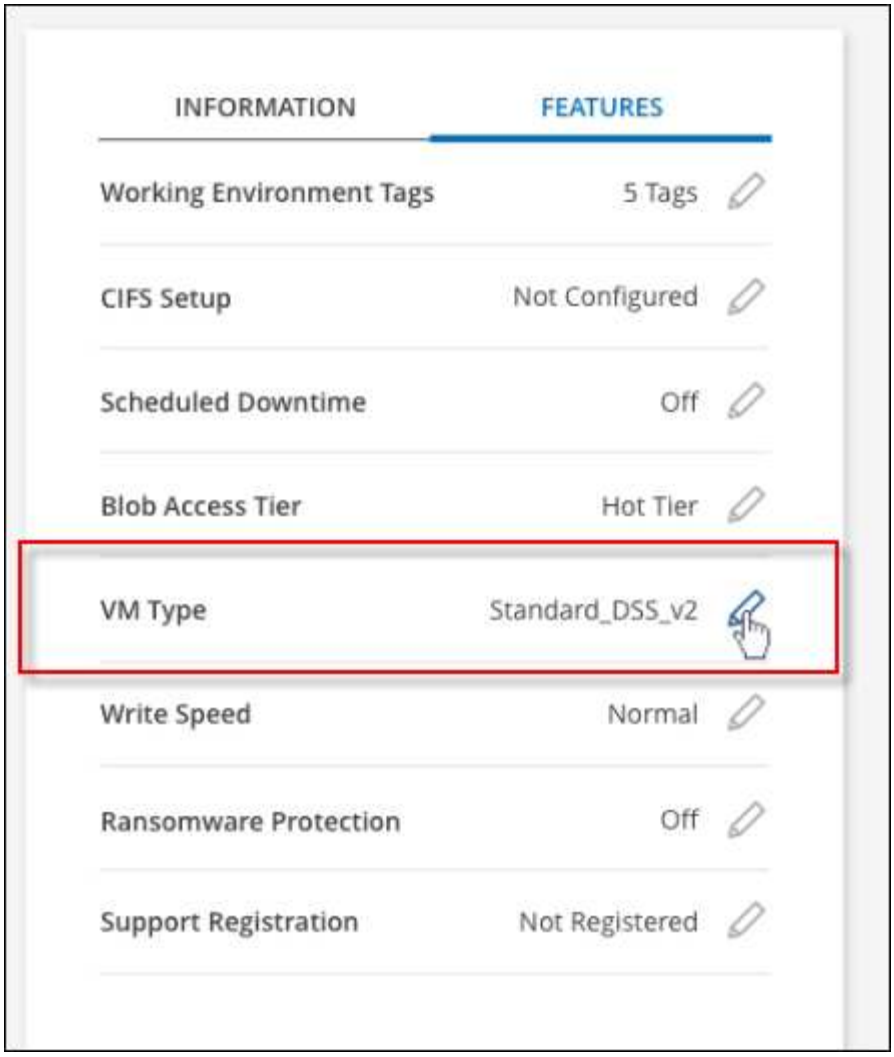
  對於單一節點系統、 I/O 會中斷。

  對於 HA 配對、變更不中斷營運。HA 配對可繼續提供資料。

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

步驟

1. 在 Canvas 頁面上、選取工作環境。
2. 按一下 [概觀] 索引標籤上的 [功能] 面板，然後按一下 *VM 類型 * 旁邊的鉛筆圖示。



a. 如果您使用的是節點型 PAYGO 授權、您可以選擇不同的授權和 VM 類型、方法是按一下 * 授權類型 * 旁的鉛筆圖示。

3. 選取 VM 類型、選取核取方塊以確認您瞭解變更的影響、然後按一下 * 變更 * 。

結果

以新組態重新開機。 Cloud Volumes ONTAP

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

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

關於這項工作

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

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

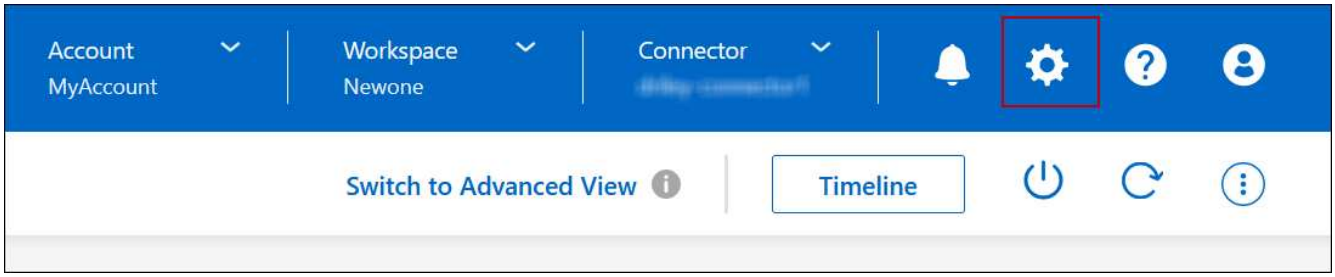
此程序可能會對 CIFS 用戶端造成破壞。未從 CIFS 用戶端提交的資料可能會遺失。

您需要的產品

您必須先建立連接器、才能變更BlueXP設定。 "瞭解方法"。

步驟

1. 在 BlueXP 主控台的右上角、按一下「設定」圖示、然後選取 * 「 Cloud Volumes ONTAP 設定 * 」 。



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

使用**Azure**私有連結或服務端點

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

總覽

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

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

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

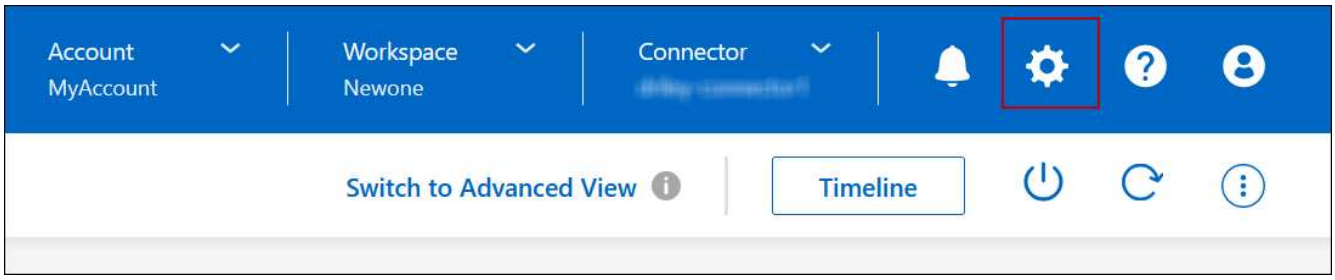
停用**Azure**私有連結、改用服務端點

如果貴企業需要、您可以變更BlueXP中的設定、使Cloud Volumes ONTAP 其設定使用服務端點、而非Azure私有連結。變更此設定會套用Cloud Volumes ONTAP 至您所建立的新版資訊系統。服務端點僅在中受支援 "Azure區域配對" 連接器與Cloud Volumes ONTAP 胎心之間。

連接器應部署在Cloud Volumes ONTAP 其所管理的或所管理的各個系統所在的Azure區域 "Azure區域配對" 適用於整個系統。Cloud Volumes ONTAP

步驟

1. 在 BlueXP 主控台的右上角、按一下「設定」圖示、然後選取 * 「 Cloud Volumes ONTAP 設定 * 」 。



2. 在* Azure 下、按一下*使用**Azure Private Link**。
3. 取消選擇* Cloud Volumes ONTAP 在不同時使用*私有連結的情況下、連接到儲存帳戶*。
4. 按一下「 * 儲存 * 」。

完成後

如果您停用Azure私有連結、且Connector使用Proxy伺服器、則必須啟用直接API流量。

"瞭解如何在Connector上啟用直接API流量"

使用**Azure**私有連結

在大多數情況下、您不需要做任何事、就能使用Cloud Volumes ONTAP 下列功能來設定Azure私有連結：BlueXP會為您管理Azure私有連結。但如果您使用現有的Azure私有DNS區域、則必須編輯組態檔。

自訂**DNS**的需求

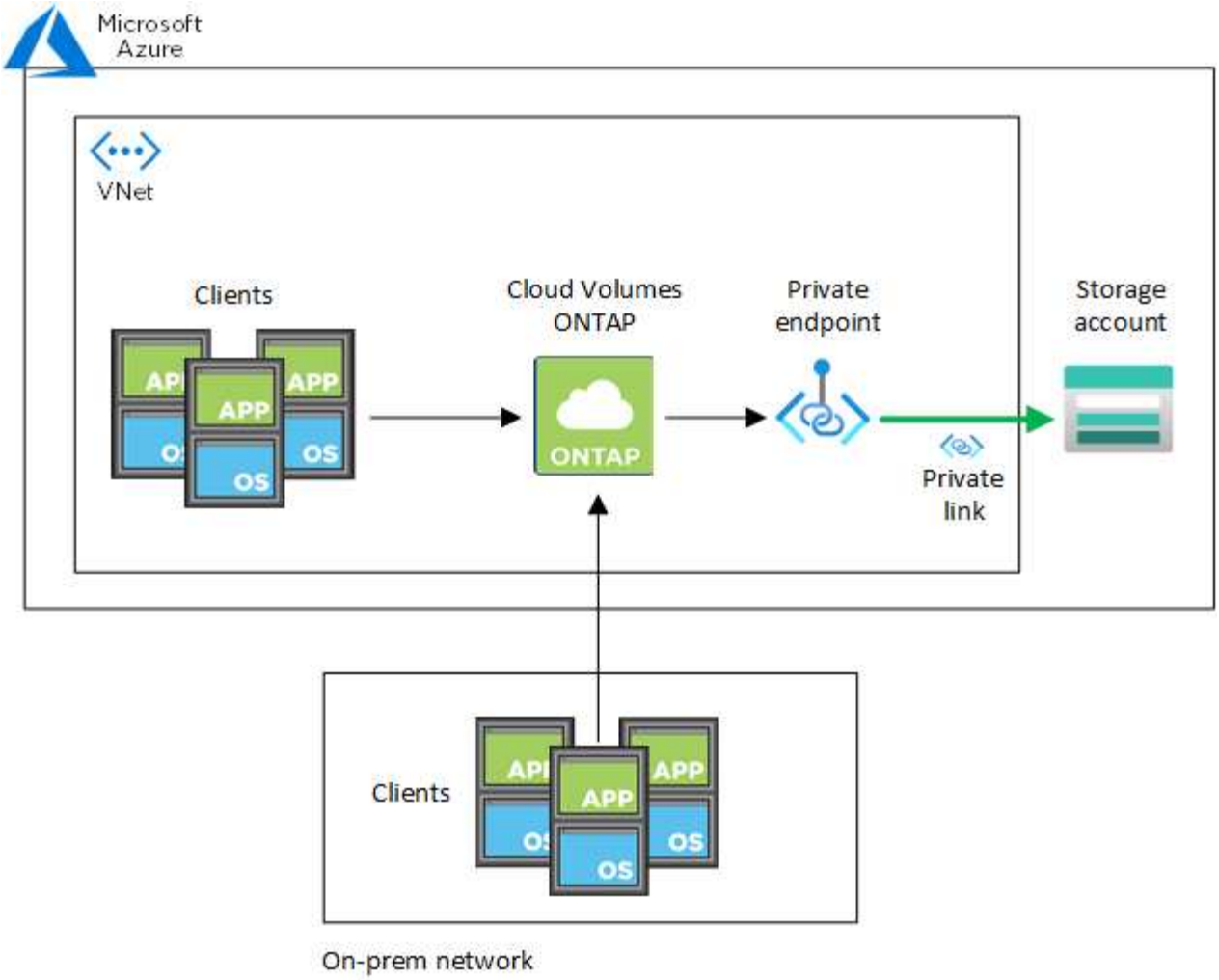
或者、如果您使用自訂DNS、則需要從自訂DNS伺服器建立條件轉寄站、以前往Azure私有DNS區域。若要深入瞭解、請參閱 "Azure關於使用DNS轉寄站的文件"。

私有連結連線的運作方式

當BlueXP在Cloud Volumes ONTAP Azure中部署時、它會在資源群組中建立一個私有端點。私有端點與Cloud Volumes ONTAP 用於實現功能不均的儲存帳戶相關聯。因此Cloud Volumes ONTAP 、存取資料可透過Microsoft主幹網路存取。

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

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



如果連接器和Cloud Volumes ONTAP 物件系統部署在不同的VNets中、則您必須在部署連接器的vnet和Cloud Volumes ONTAP 部署了該系統的vnet之間設定vnet對等關係。

提供您**Azure**私有**DNS**的詳細資料給**BlueXP**

如果您使用 "Azure 私有 DNS"然後您需要修改每個 Connector 上的組態檔。否則、BlueXP無法在Cloud Volumes ONTAP 支援的儲存帳戶之間啟用Azure Private Link連線。

請注意、 DNS 名稱必須符合 Azure DNS 命名需求 "如 Azure 文件所示"。

步驟

1. SSH 連接至 Connector 主機並登入。
2. 瀏覽至下列目錄：/opp/application/netapp/cloudmanager/docker_occm/data
3. 使用下列關鍵字-值配對新增「user-Private - DNS"區域設定參數、以編輯app.conf：

```
"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
}
```

此參數應與「system-id」輸入的層級相同、如下所示：

```
"system-id" : "<system ID>",
"user-private-dns-zone-settings" : {
```

請注意、只有當私有DNS區域的訂閱與Connector不同時、才需要訂購關鍵字。

4. 儲存檔案並登出 Connector 。

   不需要重新開機。

在故障時啟用復原功能

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

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

如果您啟用復原、則BlueXP會停止動作、並回溯作為行動一部分所建立的所有資源。

您可以透過API或更新app.conf檔案來啟用復原功能。

*透過API*啟用復原功能

步驟

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

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

更新**app.conf**以啟用復原功能

步驟

1. SSH 連接至 Connector 主機並登入。
2. 瀏覽至下列目錄：/opp/application/netapp/cloudmanager/docker_occm/data
3. 新增下列參數和值以編輯 app.conf ：

```
 "rollback-on-private-link-failure": true
. 儲存檔案並登出 Connector 。
```

不需要重新開機。

正在移動資源群組

支援Azure資源群組移動、但工作流程僅發生在Azure主控台。Cloud Volumes ONTAP

您可以在同一Azure訂閱中、將工作環境從一個資源群組移至Azure中的其他資源群組。不支援在不同Azure訂閱之間移動資源群組。

步驟

1. 從* Canvas*移除工作環境。

   若要瞭解如何移除工作環境、請參閱 "移除 Cloud Volumes ONTAP 運作環境"。

2. 在Azure主控台執行資源群組搬移。

   若要完成移動、請參閱 "將資源移至新的資源群組或訂閱Microsoft Azure文件中"。

3. 在* Canvas*中、探索工作環境。
4. 在工作環境的資訊中尋找新的資源群組。

結果

工作環境及其資源（VM、磁碟、儲存帳戶、網路介面、快照）位於新的資源群組中。

分離 **Azure** 中的 **SnapMirror** 流量

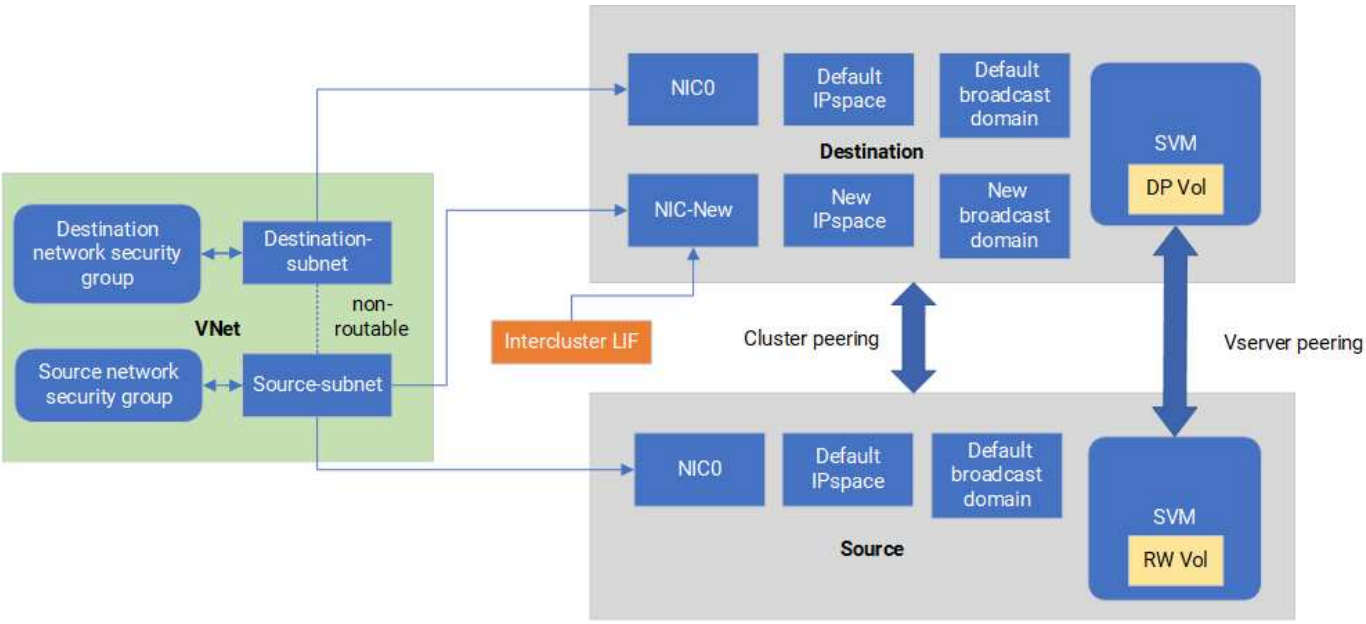
有了 Azure 中的 Cloud Volumes ONTAP 、您可以將 SnapMirror 複寫流量與資料和管理流量區隔。若要將 SnapMirror 複寫流量與資料流量區隔、您需要新增網路介面卡（ NIC ）、相關的叢集間 LIF 和不可路由的子網路。

關於 **Azure** 中的 **SnapMirror** 流量分隔

根據預設、 BlueXP 會在相同子網路上的 Cloud Volumes ONTAP 部署中設定所有 NIC 和生命。在此類組態中、 SnapMirror 複寫流量和資料與管理流量使用相同的子網路。分離 SnapMirror 流量會利用無法路由傳送至現有子網路的額外子網路、用於資料和管理流量。

圖 **1.**

下圖顯示 SnapMirror 複寫流量與其他 NIC 、相關的叢集間 LIF 和單一節點部署中不可路由的子網路之間的分隔。HA 配對部署稍有不同。



開始之前

請檢閱下列考量事項：

- 您只能將單一 NIC 新增至 Cloud Volumes ONTAP 單一節點或 HA 配對部署（ VM 執行個體）、以進行 SnapMirror 流量分隔。
- 若要新增 NIC 、您部署的 VM 執行個體類型必須有未使用的 NIC 。
- 來源叢集和目的地叢集應可存取相同的虛擬網路（ vnet ）。目的地叢集是 Azure 中的 Cloud Volumes ONTAP 系統。來源叢集可以是 Azure 中的 Cloud Volumes ONTAP 系統、也可以是 ONTAP 系統。

步驟 1 ：建立額外的 NIC 並附加至目的地 VM

本節提供如何建立其他 NIC 並將其附加至目的地 VM 的說明。目的地 VM 是 Azure 中 Cloud Volumes ONTAP 的單一節點或 HA 配對系統、您可以在其中設定額外的 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 環境來停止節點。
   a. 停止節點。

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

b. 取消分配節點。

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

4. 設定網路安全性群組規則、使兩個子網路（來源叢集子網路和目的地叢集子網路）無法彼此路由。
   a. 在目的地 VM 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. 在目的 VM 上建立新的 NIC 、並提供來源叢集子網路的子網路 ID 。在此輸入新 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. 儲存私有 IP 位址。此 IP 位址 <new_added_nic_primary_addr> 用於在中建立叢集間 LIF 廣播網域、新 NIC 的叢集間 LIF。
5. 將新的 NIC 連接至 VM 。

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

6. 啟動 VM （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 新的）存在且已啟用加速網路連線。

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

對於 HA 配對部署、請針對合作夥伴節點重複這些步驟。

步驟 2 ：為新 NIC 建立新的 IPspace 、廣播網域和叢集間 LIF

叢集間生命體的獨立 IPspace 可在叢集之間進行複寫的網路功能之間提供邏輯分隔。

請使用 ONTAP CLI 執行下列步驟。

步驟

1. 建立新的 IPspace （ new_IPSpace ）。

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

2. 在新的 IPspace （ new_IPSpace ）上建立廣播網域、然後新增 NIC 新連接埠。

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

3. 對於單節點系統、新增的連接埠為 *e0b* 。對於具有託管磁碟的 HA 配對部署、新增的連接埠為 *e0d* 。對於具有頁面 Blobs 的 HA 配對部署、新增的連接埠為 *e0e* 。使用節點名稱而非 VM 名稱。執行即可找到節點名稱 `node show`。

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

4. 在新的廣播網域（ new_bd ）和新的 NIC （ NIC 新）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. 驗證新叢集間 LIF 的建立。

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

對於 HA 配對部署、請針對合作夥伴節點重複這些步驟。

步驟 3 ：驗證來源和目的地系統之間的叢集對等關係

本節提供如何驗證來源和目的地系統之間對等關係的指示。

請使用 ONTAP CLI 執行下列步驟。

步驟

1. 確認目的地叢集的叢集間 LIF 可以 ping 通來源叢集的叢集間 LIF 。由於目的地叢集執行此命令、因此目的

地 IP 位址是來源上的叢集間 LIF IP 位址。

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

2. 確認來源叢集的叢集間 LIF 可以 ping 通目的地叢集的叢集間 LIF 。目的地是在目的地上建立的新 NIC 的 IP 位址。

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

對於 HA 配對部署、請針對合作夥伴節點重複這些步驟。

步驟 4 ：在來源與目的地系統之間建立 SVM 對等關係

本節提供如何在來源與目的地系統之間建立 SVM 對等關係的指示。

請使用 ONTAP CLI 執行下列步驟。

步驟

1. 使用來源叢集間 LIF IP 位址做為、在目的地上建立叢集對等關係 `-peer-addrs`。對於 HA 配對、請將兩個節點的來源叢集間 LIF IP 位址列為 `-peer-addrs`。

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

2. 輸入並確認通行密碼。
3. 使用目的地叢集 LIF IP 位址做為、在來源上建立叢集對等關係 `peer-addrs`。對於 HA 配對、請將兩個節點的目的地叢集間 LIF IP 位址列為 `-peer-addrs`。

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

4. 輸入並確認通行密碼。
5. 檢查叢集是否已對等連接。

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

在可用度欄位中成功的對等顯示 * 可用 * 。

6. 在目的地上建立 SVM 對等關係。來源和目的地 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 對等關係。

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

8. 請檢查 SVM 是否有問題。

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

對等狀態顯示 **`peered`** 並顯示對等應用程式 **`snapmirror`**。

步驟 5 ：在來源與目的地系統之間建立 SnapMirror 複寫關係

本節提供如何在來源與目的地系統之間建立 SnapMirror 複寫關係的指示。

若要移動現有的 SnapMirror 複寫關係、您必須先中斷現有的 SnapMirror 複寫關係、然後再建立新的 SnapMirror 複寫關係。

請使用 ONTAP CLI 執行下列步驟。

步驟

1. 在目的地 SVM 上建立資料保護的 Volume 。

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

2. 在目的地上建立 SnapMirror 複寫關係、其中包括 SnapMirror 原則和複寫排程。

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

3. 初始化目的地上的 SnapMirror 複寫關係。

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

4. 在 ONTAP CLI 中、執行下列命令以驗證 SnapMirror 關係狀態：

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

關係狀態為 `Snapmirrored` 而關係的健全狀況就是 `true`。

5. 可選：在 ONTAP CLI 中，運行以下命令查看 SnapMirror 關係的操作歷史記錄。

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

或者、您可以掛載來源和目的地磁碟區、將檔案寫入來源磁碟區、並驗證磁碟區是否正在複寫到目的地。

Google Cloud管理

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

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

關於這項工作

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

  "供應說明文件：設定自動恢復的命令 ONTAP"

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

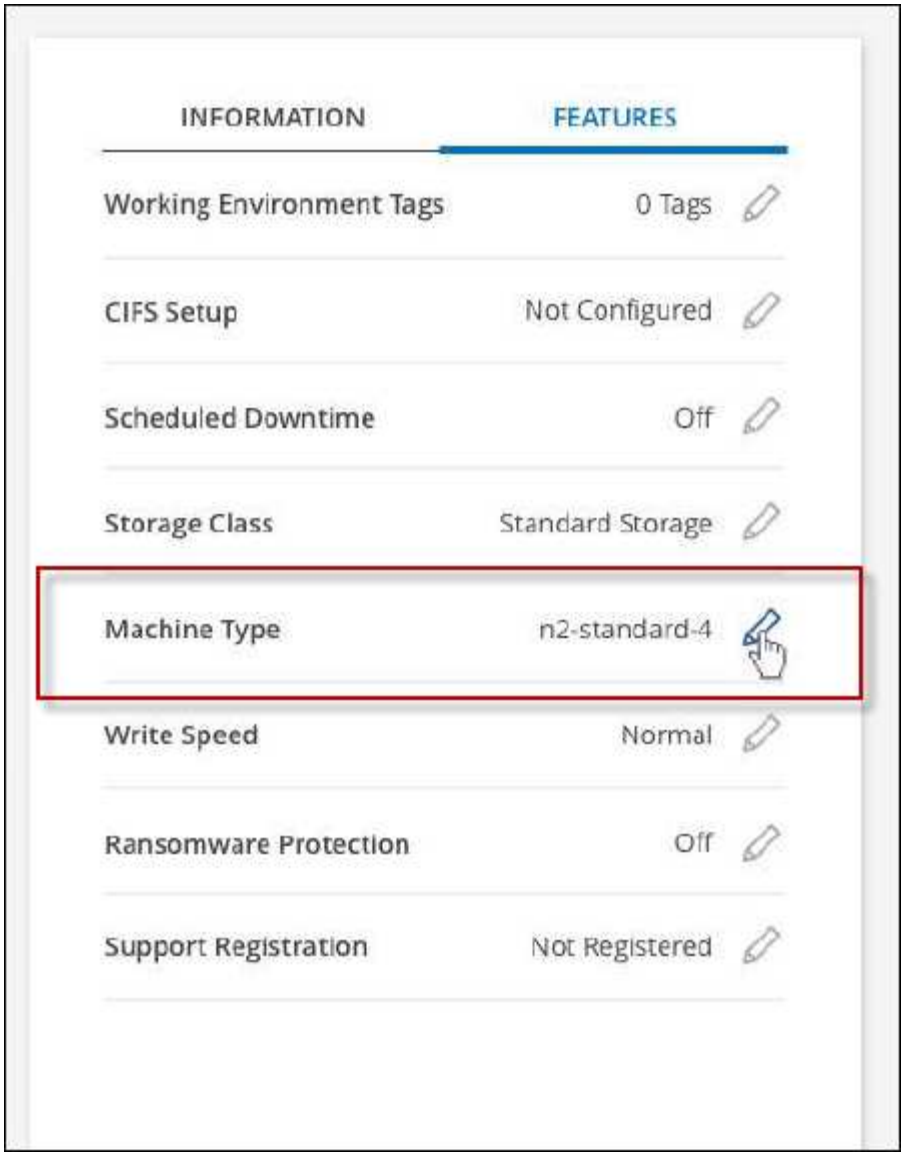
  對於單一節點系統、 I/O 會中斷。

  對於 HA 配對、變更不中斷營運。HA 配對可繼續提供資料。

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

步驟

1. 在 Canvas 頁面上、選取工作環境。
2. 在「概述」索引標籤上、按一下「功能」面板、然後按一下「 * 機器類型 * 」旁邊的鉛筆圖示。



a. 如果您使用的是節點型 PAYGO 授權、您可以選擇不同的授權和機器類型、方法是按一下 * 授權類型 * 旁的鉛筆圖示。

3. 選擇機器類型、勾選核取方塊以確認您瞭解變更的影響、然後按一下 * 變更 * 。

結果

以新組態重新開機。 Cloud Volumes ONTAP

使用進階檢視來管理**Cloud Volumes ONTAP**

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

功能

BlueXP的進階檢視可讓您存取其他管理功能：

- 進階儲存管理

  管理一致性群組、共用區、qtree、配額和儲存VM。

- 網路管理

  管理IPspace、網路介面、連接埠集和乙太網路連接埠。

- 活動與工作

  檢視事件記錄、系統警示、工作和稽核記錄。

- 進階資料保護

  保護儲存VM、LUN及一致性群組。

- 主機管理

  設定SAN啟動器群組和NFS用戶端。

支援的組態

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

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

限制

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

- BlueXP 分層

  Cloud Volumes ONTAP 不支援 BlueXP 分層服務。建立磁碟區時、必須直接從BlueXP的標準檢視畫面設定將資料分層至物件儲存設備。

- 階層

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

- 韌體升級

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

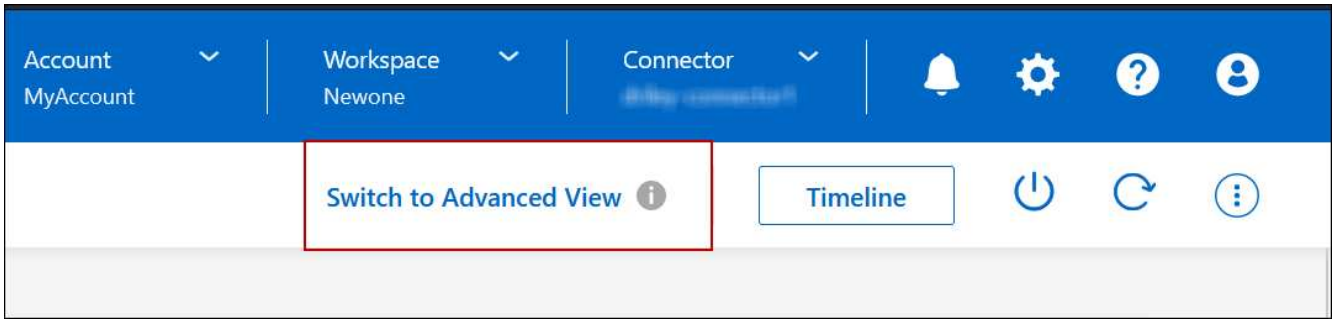
此外、不支援System Manager的角色型存取控制。

如何開始使用

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

步驟

1. 從左側導覽功能表中、選取*儲存設備> Canvas*。
2. 在「畫版」頁面上、按兩下Cloud Volumes ONTAP 某個系統的名稱。
3. 在右上角、按一下*切換至進階檢視*。



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

協助使用**System Manager**

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

- "Volume與LUN管理"
- "網路管理"
- "資料保護"

從**Cloud Volumes ONTAP CLI**管理

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

開始之前

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

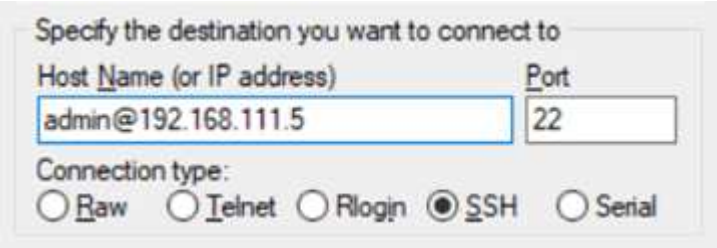
> 當部署於多個 AZs 時 Cloud Volumes ONTAP 、使用浮動 IP 位址進行叢集管理介面、這表示外部路由無法使用。您必須從屬於同一個路由網域的主機連線。

步驟

1. 在BlueXP中、識別叢集管理介面的IP位址：
   a. 從左側導覽功能表中、選取*儲存設備> Canvas*。
   b. 在「畫版」頁面上、選取 Cloud Volumes ONTAP 「系統」。
   c. 複製右窗格中顯示的叢集管理 IP 位址。
2. 使用 SSH 連線至使用管理帳戶的叢集管理介面 IP 位址。

- 範例 *

  下圖顯示使用 Putty 的範例：



3. 在登入提示下、輸入 admin 帳戶的密碼。

   - 範例 *

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

系統健全狀況與事件

驗**AutoSupport** 證此設定

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

唯一必要的組態步驟是確保Cloud Volumes ONTAP 使用者能夠連線到傳出的網際網路。如需詳細資料、請參閱雲端供應商的網路需求。

需求**AutoSupport**

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

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

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

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

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

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

文件：設定檔ONTAP AutoSupport"。

疑難排解**AutoSupport** 您的**VMware**組態

如果傳出連線無法使用、且BlueXP無法將Cloud Volumes ONTAP 您的作業系統設定為使用Connector做為Proxy伺服器、您將會收到來自BlueXP的通知、標題為「<工作環境名稱>無法傳送AutoSupport 靜態訊息」。

您很可能因為網路問題而收到此訊息。

請依照下列步驟來解決此問題。

步驟

1. SSH到Cloud Volumes ONTAP 支援系統、以便從CLI管理系統。

   "瞭解如何從SSH到Cloud Volumes ONTAP 功能"。

2. 顯示AutoSupport 資訊子系統的詳細狀態：

   《不知詳情》AutoSupport

   回應應類似下列內容：

```
    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類別的狀態為「ok」、表示AutoSupport 已正確設定、並可傳送訊息。

3. 如果狀態不正常、請驗證每Cloud Volumes ONTAP 個節點的Proxy URL：

   《AutoSupport 鏈接：字段proxy-url'》

4. 如果Proxy URL參數是空的、請設定Cloud Volumes ONTAP 使用連接器做為Proxy：

   《AutoSupport 支援：modify -proxy-URL http://<connector Private IP>:3128》

5. 再次驗AutoSupport 證此狀態：

   《不知詳情》AutoSupport

6. 如果狀態仍然失敗、請驗證Cloud Volumes ONTAP 透過連接埠3128驗證顯示的是在連接埠之間與連接器之

間是否有連線。

7. 如果狀態ID在驗證是否有連線後仍失敗、請使用SSH連線至連接器。

   "深入瞭解連接至Linux VM for the Connector的相關資訊"

8. 請前往「/opt/sapplication/netapp/cloudmanager/dock_occm/data/`」
9. 開啟Proxy組態檔「shquid.conf」

   檔案的基本結構如下：

```
http_port 3128
acl localnet src 172.31.0.0/16
acl azure_aws_metadata dst 169.254.169.254

http_access allow localnet
http_access deny azure_aws_metadata
http_access allow localhost
http_access deny all
```

   localnet src值是Cloud Volumes ONTAP 指整個過程中的CIDR。

10. 如果Cloud Volumes ONTAP 無法在檔案中指定的範圍內更新整個系統的CIDR區塊、請更新該值或新增下列項目：

    「ACL cv網 卡來源<CIDR >」

    如果您新增此新項目、請別忘了新增允許項目：

    "http存取允許cvonet"

    範例如下：

```
http_port 3128
acl localnet src 172.31.0.0/16
acl cvonet src 172.33.0.0/16
acl azure_aws_metadata dst 169.254.169.254

http_access allow localnet
http_access allow cvonet
http_access deny azure_aws_metadata
http_access allow localhost
http_access deny all
```

11. 編輯組態檔之後、請重新啟動Proxy容器作為Sudo：

    「Docker重新啟動sid」

12. 返回Cloud Volumes ONTAP 到還原CLI、確認Cloud Volumes ONTAP 功能不只能傳送AutoSupport 功能不實的訊息：

    《不知詳情》AutoSupport

設定EMS

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

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