系統管理
Cloud Volumes ONTAP

NetApp
February 26, 2026

目錄

系統管理

升級Cloud Volumes ONTAP

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

升級概述

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

僅從控制台升級

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

控制台提供了兩種升級Cloud Volumes ONTAP 的方法：

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

支援的升級路徑

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

AWS 支援的升級路徑

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

目前版本	可直接升級到的版本
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

Azure 支援的升級路徑

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

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

- 9.7 P7 → 9.8 P18

- 9.8 P18 → 9.9.1 P15
- 9.9.1 P15 → 9.10.1 P12
- 9.10.1 P12 → 9.11.1 P20

Google Cloud 支援的升級路徑

目前版本	可直接升級到的版本
9.17.1 P1	9.18.1
9.16.1	9.17.1 P1
9.15.1	9.16.1
9.15.0	9.15.1
9.14.1	9.15.1
	9.15.0
9.14.0	9.14.1
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1
9.12.1	9.13.1
	9.13.0
9.12.0	9.12.1
9.11.1	9.12.1
	9.12.0
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9.8	9.9.1
9.7	9.8
9.6	9.7
9.5	9.6
9.4	9.5
9.3	9.4
9.2	9.3

目前版本	可直接升級到的版本
9.1	9.2
9.0	9.1
8.3	9.0

請注意以下事項：

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

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

補丁版本

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

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

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

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

以下是幾個例子：

- 9.13.0 → 9.13.1 P15
- 9.12.1 → 9.13.1 P2

恢復或降級

不支援將Cloud Volumes ONTAP還原或降級到先前的版本。

支援註冊

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

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

HA 調解器的升級

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

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

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

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

更改實例類型

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

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

如果您無法變更實例類型，請依照[啟用增強連網]。

啟用增強連網

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

準備升級

在執行升級之前，您必須驗證系統已準備就緒並進行任何必要的配置變更。

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

規劃停機時間

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

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

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

驗證自動交還是否仍然啟用

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

"ONTAP文件：用於設定自動交還的命令"

暫停**SnapMirror**傳輸

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

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

關於此任務

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

步驟

1. 從目標系統登入系統管理員。

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

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

2. 點選*保護>關係*。
3. 選擇關係並點選*操作>靜默*。

驗證聚合是否在線

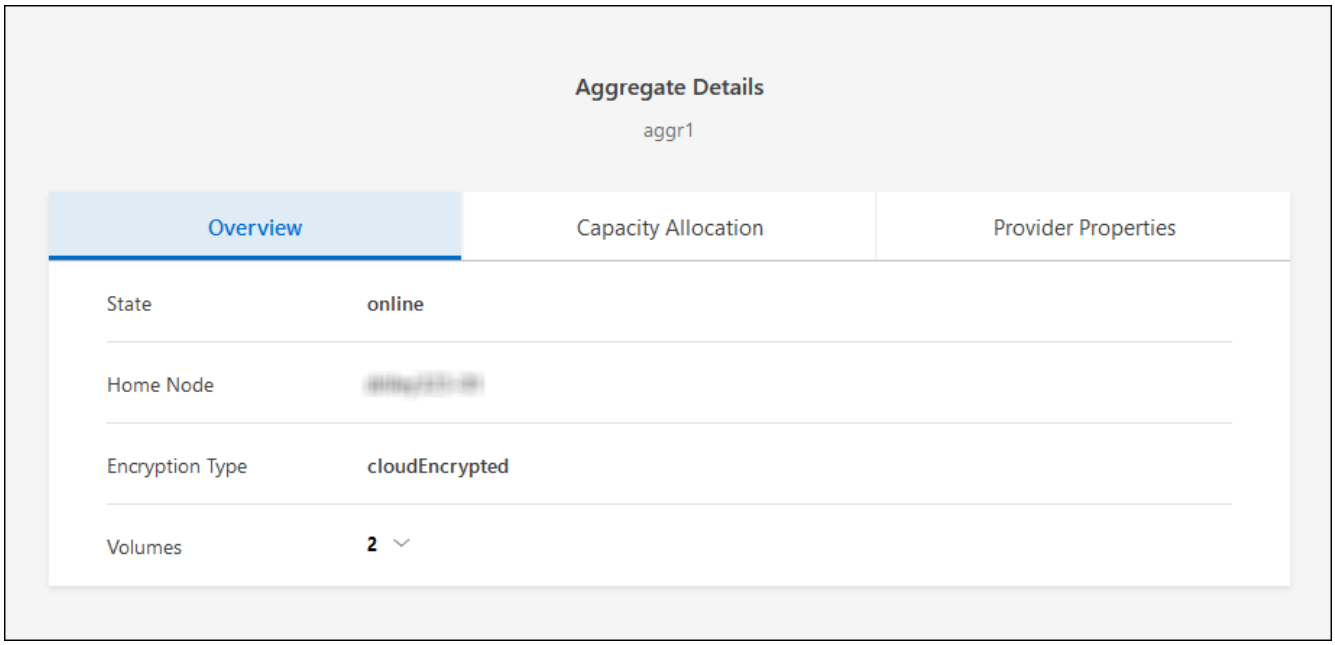
在更新軟體之前， Cloud Volumes ONTAP的聚合必須處於線上狀態。在大多數配置中，聚合應該處於線上狀態，但如果沒有，則應將其置於線上狀態。

關於此任務

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

步驟

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



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

驗證所有 **LIF** 是否位於主端口

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

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

升級Cloud Volumes ONTAP

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

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

從控制台通知升級

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

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

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

開始之前

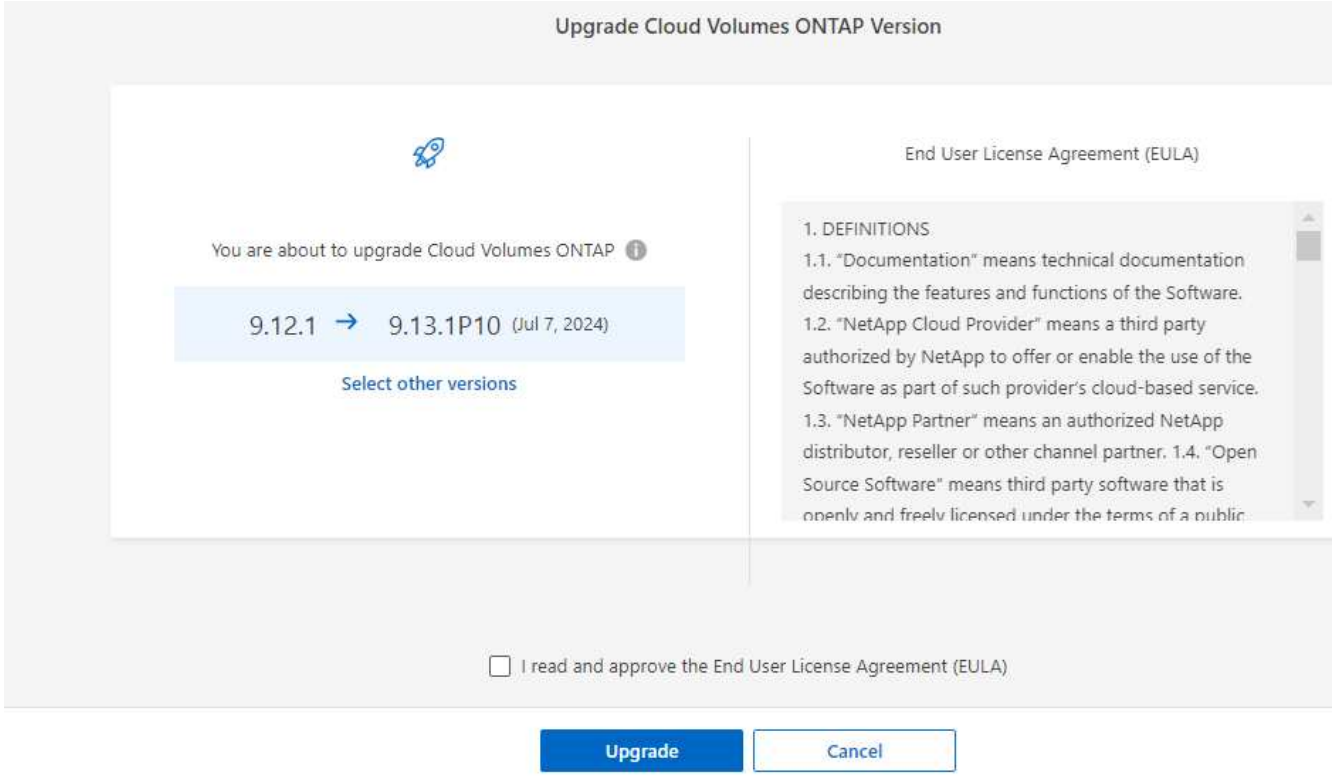
Cloud Volumes ONTAP系統上不得進行磁碟區或聚合建立等操作。

步驟

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

   如果有新版本可用，概覽標籤中會出現通知：

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

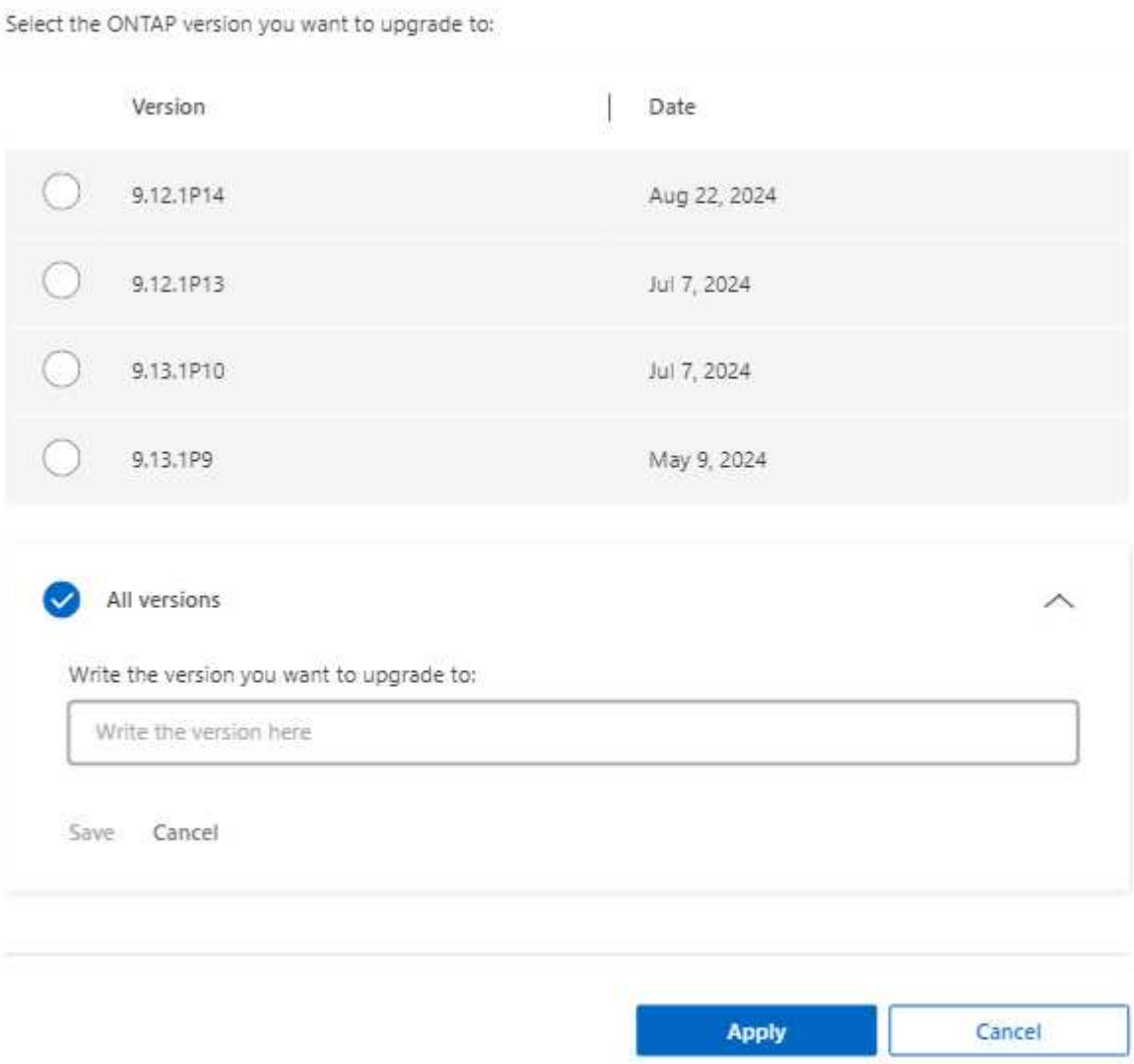


   若要升級到其他版本，請點選*選擇其他版本*。您會看到所列的最新Cloud Volumes ONTAP版本也與您系統上安裝的版本相容。例如，您的系統上安裝的版本是9.12.1P3，並且有以下相容版本可用：

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

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

5. 按一下“儲存”，然後按一下“應用”



。

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

結果

控制台開始軟體升級。軟體更新完成後，您可以在系統上執行操作。

完成後

如果您暫停了SnapMirror傳輸，請使用系統管理員恢復傳輸。

透過 **URL** 上的可用影像進行升級

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

開始之前

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

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

  前往NetApp知識庫查看逐步說明：

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

步驟

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

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

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

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

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

   有兩條路徑可用。正確的路徑取決於您的控制台代理版本。

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

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

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

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

7. 按一下“繼續”進行確認。

結果

控制台開始軟體更新。軟體更新完成後，您就可以在系統上執行操作。

完成後

如果您暫停了SnapMirror傳輸，請使用系統管理員恢復傳輸。

修復使用 **Google Cloud NAT** 閘道時下載失敗的問題

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

步

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

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

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

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

"了解有關 /occm/config API 呼叫的更多信息" 。

註冊Cloud Volumes ONTAP即用即付系統

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

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

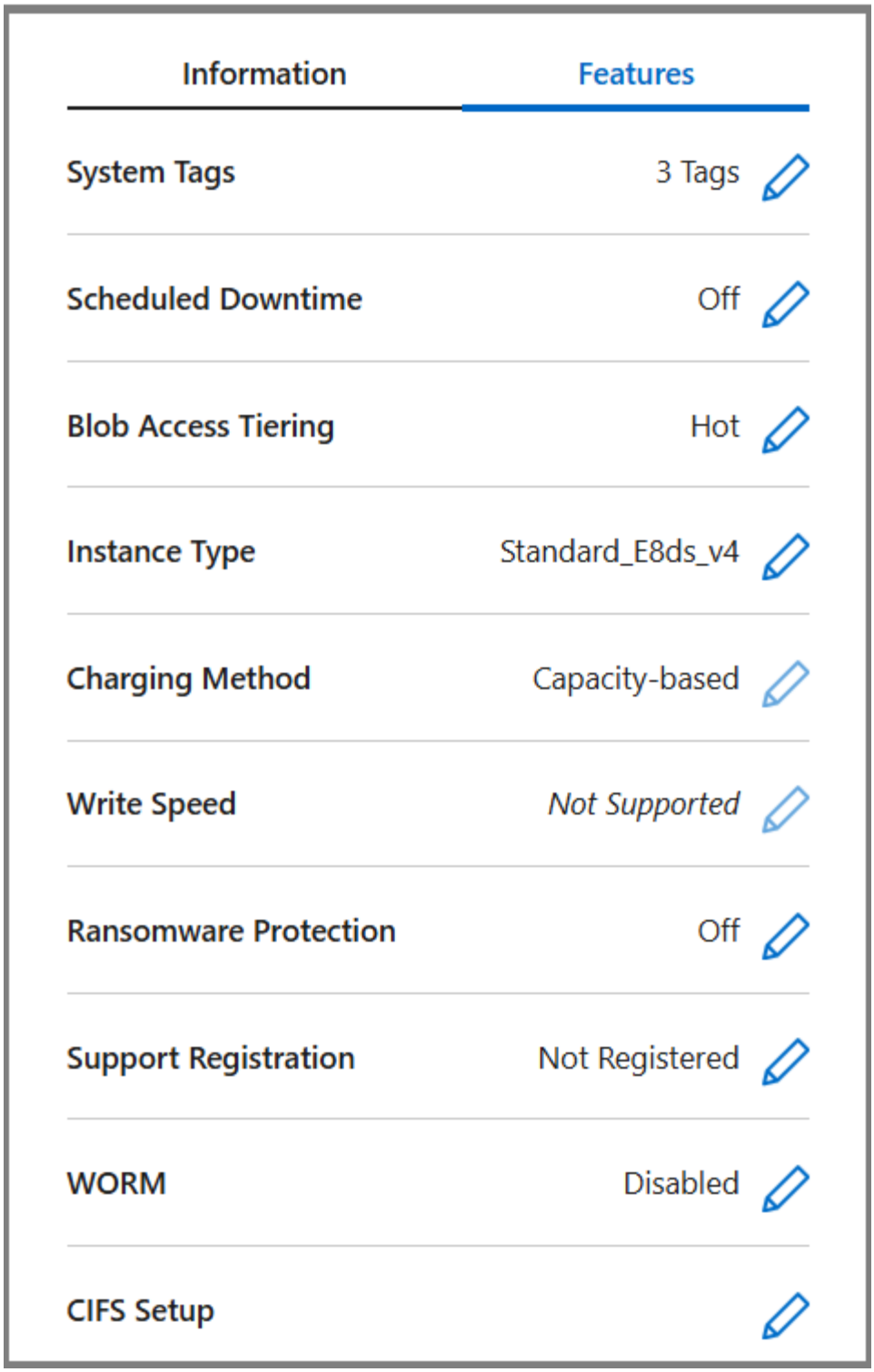
未註冊支援的系統仍會在有新版本可用時收到NetApp Console中顯示的軟體更新通知。但您需要先註冊系統才能升級軟體。

步驟

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

   "了解如何新增NetApp支援網站帳戶" 。

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



4. 選擇NetApp支援網站帳號並點選「註冊」。

結果

該系統已在NetApp註冊。

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

在基於節點的許可證的可用性終止 (EOA) 之後，您應該使用NetApp Console中的許可證轉換工具過渡到基於容量的許可證。

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

有關 EOA 和 EOS 的信息，請參閱"基於節點的許可證的可用性終止"。

關於此任務

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

開始之前

- 您應該擁有一個具有客戶存取權限或管理員存取權限的 NSS 帳戶。
- 您的 NSS 帳戶應使用您用於存取控制台的使用者憑證進行註冊。
- Cloud Volumes ONTAP系統應連結至具有客戶存取權限或管理員存取權限的 NSS 帳戶。
- 您應該擁有有效的基於容量的許可證，可以是 BYOL 許可證或市場訂閱。
- 您的帳戶中應該有基於容量的許可證。此授權可以是市場訂閱，也可以是控制台中 **Licenses and subscriptions** 下提供的 BYOL/私人優惠包。
- 在選擇目的地套餐之前，請先了解以下標準：
  - 如果帳戶具有基於容量的 BYOL 許可證，則所選目標包應與帳戶的 BYOL 基於容量的許可證保持一致：
    - 什麼時候 `Professional`被選為目標包，該帳戶應具有帶有專業包的 BYOL 許可證：

- 什麼時候 `Essentials`被選為目標包，該帳戶應具有 Essentials 包的 BYOL 授權。

- 如果目標套件與帳戶的 BYOL 授權可用性不一致，則表示基於容量的授權可能不包含所選套件。在這種情況下，我們將透過您的市場訂閱向您收費。
- 如果沒有基於容量的 BYOL 授權而只有市場訂閱，則應確保所選包包含在基於容量的市場訂閱中。
- 如果您現有的基於容量的許可證中沒有足夠的容量，並且您有市場訂閱來對額外的容量使用收費，那麼您將透過市場訂閱為額外的容量付費。
- 如果您現有的基於容量的許可證中沒有足夠的容量，並且您沒有市場訂閱來收取額外容量使用的費用，則無法進行轉換。您應該添加市場訂閱來收取額外容量或將可用容量擴展到您目前的授權。
- 如果目標套件與帳戶的 BYOL 授權可用性不一致，且您現有的基於容量的授權中沒有足夠的容量，那麼您將透過市場訂閱付費。

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

步驟

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

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

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

完成後

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

不同超標量中的定價

有關定價的詳細信息，請訪問 "NetApp Console網站"。

有關特定超標量中的私人優惠的信息，請寫信至：

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

啟動並停止Cloud Volumes ONTAP系統

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

安排Cloud Volumes ONTAP自動關閉

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

關於此任務

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

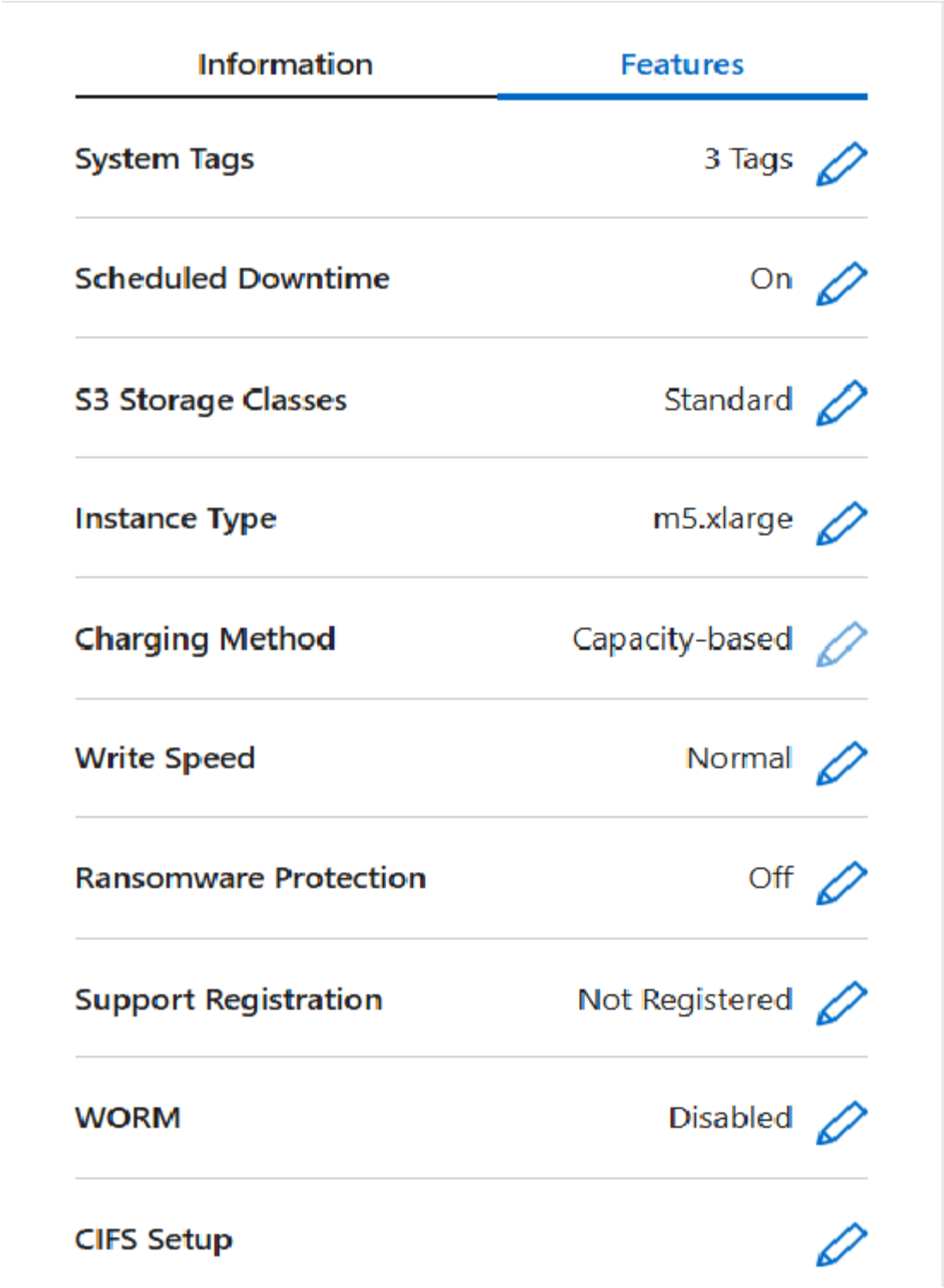
  傳輸完成後，系統將關閉。

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

  如下一節所述，只有在執行手動關機時才會自動建立快照。

步驟

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



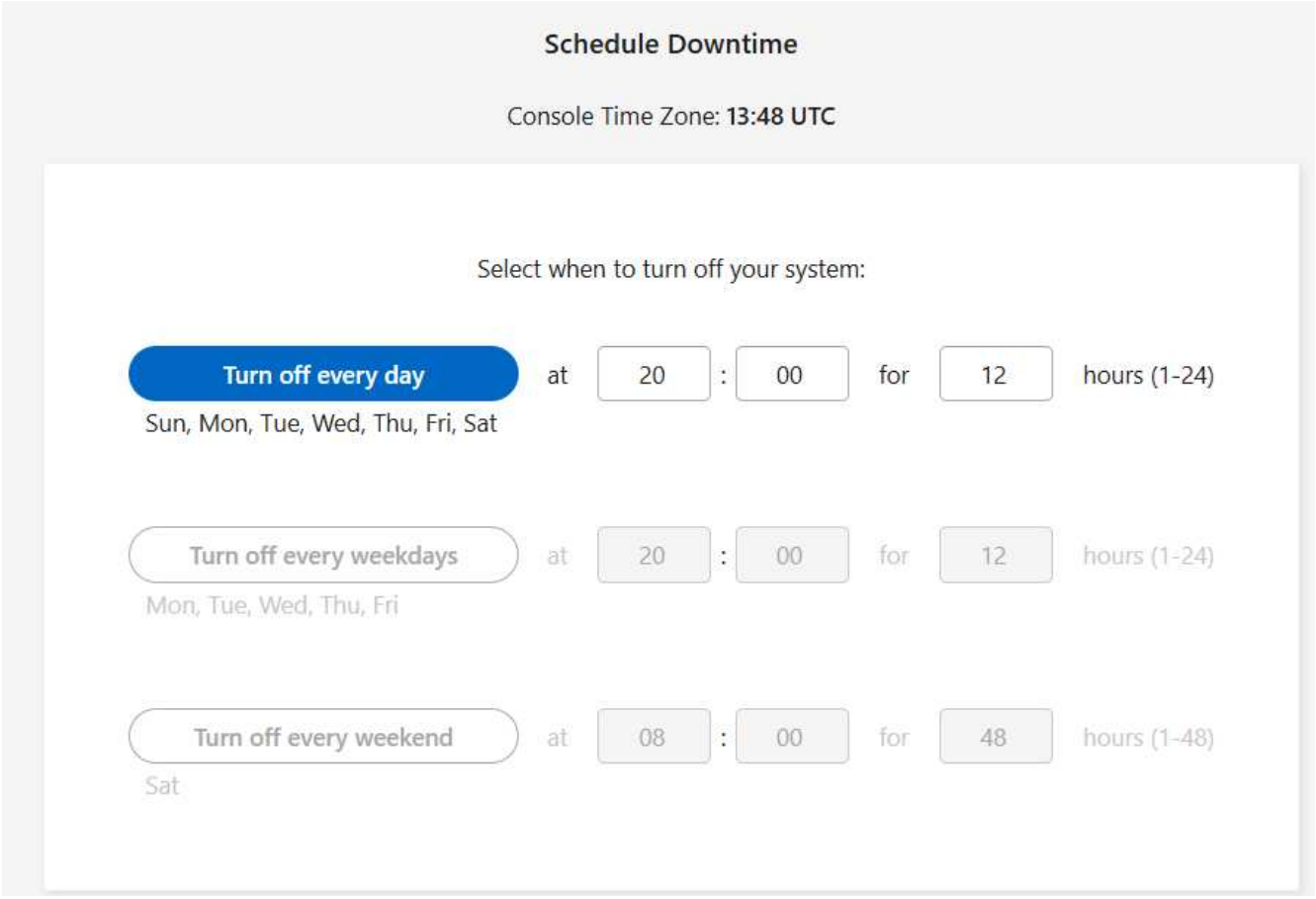
3. 指定關機計劃：

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

   b. 指定您想要關閉系統的時間以及關閉系統的時間長度。

      例子

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



4. 點選“儲存”。

結果

時間表已儲存。功能面板下對應的計劃停機時間行項目顯示「開啟」。

停止Cloud Volumes ONTAP

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

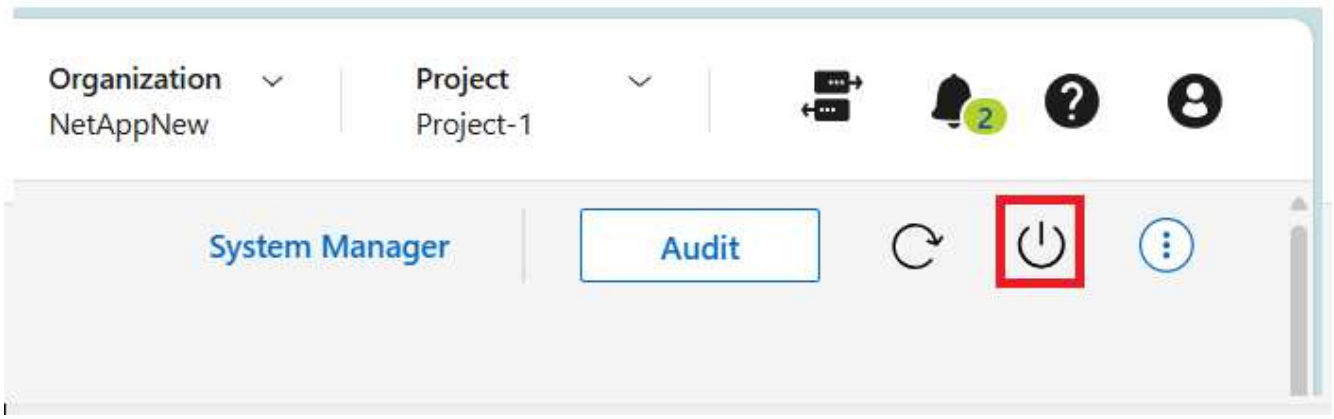
為了降低成本，控制台會定期刪除根和啟動磁碟的舊快照。根磁碟和啟動磁碟僅保留最近的兩個快照。

關於此任務

當您停止 HA 對時，控制台將關閉兩個節點。

步驟

1. 在系統中，按一下「關閉」圖示。



2. 保持建立快照的選項處於啟用狀態，因為快照可以啟用系統復原。
3. 按一下“關閉”。

   停止系統可能需要幾分鐘的時間。您可以稍後從*系統*頁面重新啟動系統。

   重新啟動時會自動建立快照。

使用 NTP 伺服器同步Cloud Volumes ONTAP系統時間

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

如果您未設定 NTP 伺服器，可能會遇到服務中斷和時間同步不準確的情況。

您可以使用以下命令指定 NTP 伺服器：

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

相關連結

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

修改系統寫入速度

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

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

在更改寫入速度之前，您應該"了解正常設定和高設定之間的差異"。

關於此任務

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

步驟

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

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

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

4. 按一下“儲存”，查看確認訊息，然後按一下“核准”。

變更Cloud Volumes ONTAP叢集管理員密碼

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

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

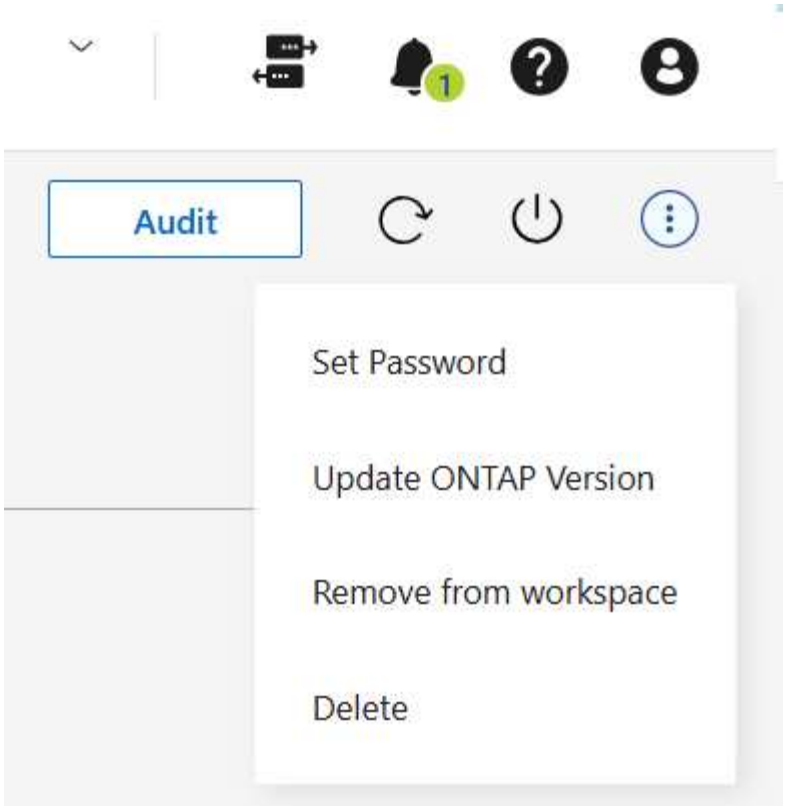
關於此任務

密碼必須遵守一些規則。新密碼：

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

步驟

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



新增、移除或刪除系統

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

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

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

您無法探索、檢視或管理已註冊到其他帳戶或組織的系統。

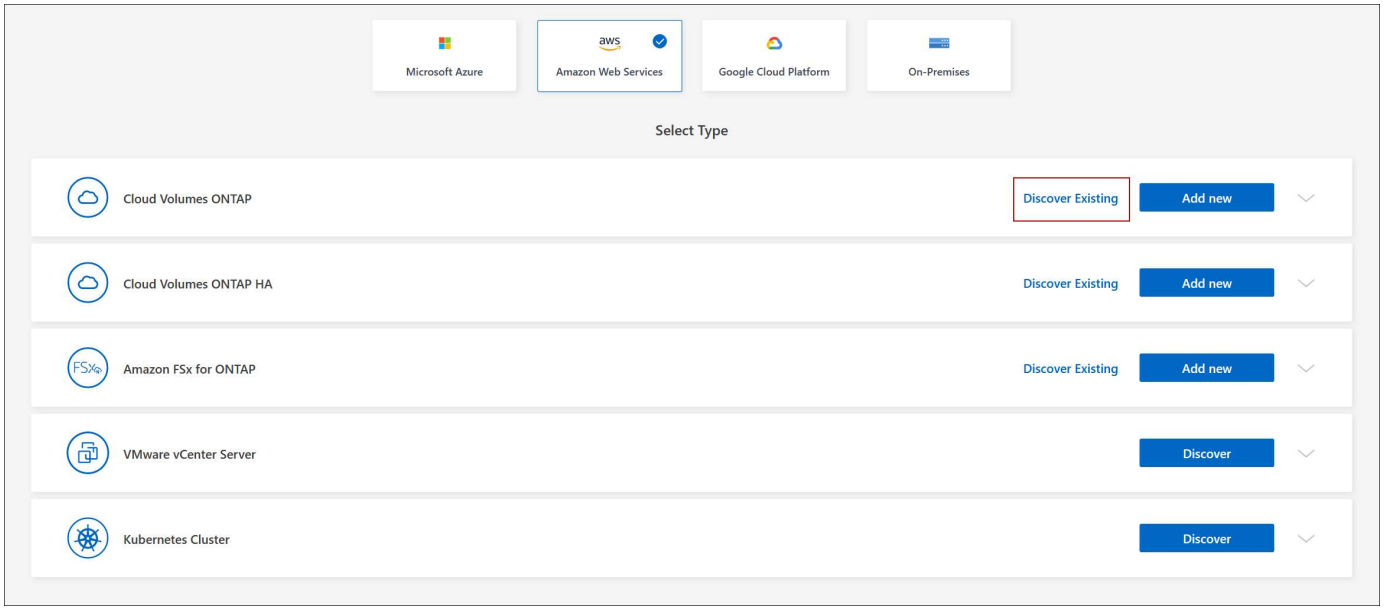
開始之前

您必須知道Cloud Volumes ONTAP管理員使用者帳號的密碼。

步驟

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

+



1. 在「區域」頁面上，選擇一個區域。您可以看到在所選區域中運作的系統。

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

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

結果

控制台將Cloud Volumes ONTAP系統新增至 系統 頁面。

從NetApp Console移除Cloud Volumes ONTAP系統

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

關於此任務

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

步驟

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

結果

控制台刪除系統。使用者可以隨時從*系統*頁面重新發現已刪除的系統。

從NetApp Console移除Cloud Volumes ONTAP系統

您應該始終從NetApp Console中刪除Cloud Volumes ONTAP系統，而不是從雲端提供者的應用程式中刪除。例如，如果您終止了雲端提供者授權的Cloud Volumes ONTAP實例，則

您不能將該授權金鑰用於另一個實例。您必須從控制台中刪除Cloud Volumes ONTAP系統才能釋放許可證。

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

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

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

步驟

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

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

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

   "了解有關資料分類實例的更多信息" 。

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

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

AWS 管理

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

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

關於此任務

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

  "ONTAP 9 文件：用於設定自動交還的命令"

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

  對於單節點系統， I/O 會中斷。

對於 HA 對來說，這種變化是無中斷的。 HA 對繼續提供數據。

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

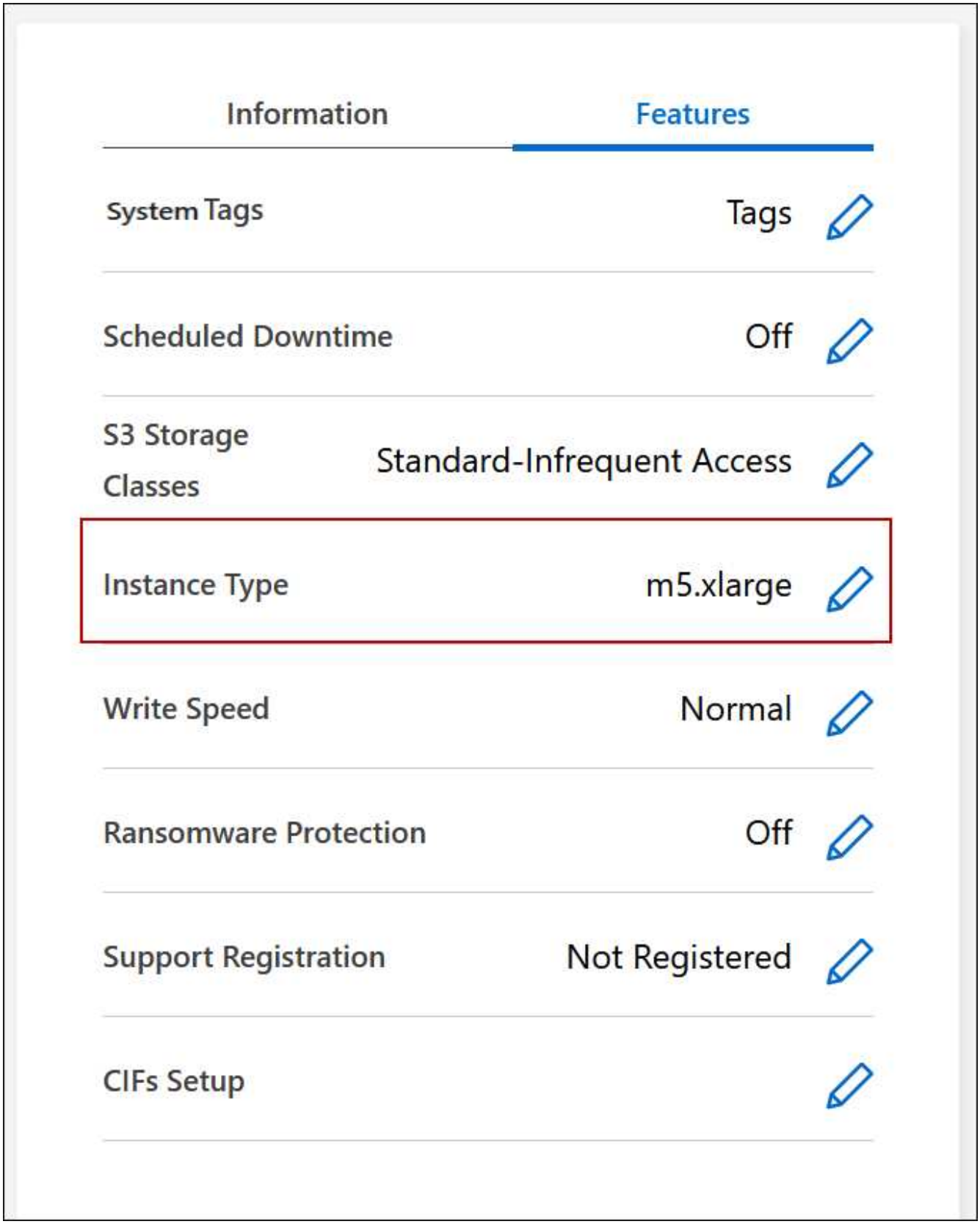
參考

有關 AWS 支援的實例類型列表，請參閱"支援的 EC2 實例"。

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

步驟

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



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

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

結果

Cloud Volumes ONTAP使用新設定重新啟動。

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

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

步驟

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

結果

NetApp Console傳送 AWS 請求來修改路由表。

Azure 管理

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

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

關於此任務

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

  "ONTAP 9 文件：用於設定自動交還的命令"

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

  對於單節點系統， I/O 會中斷。

  對於 HA 對來說，這種變化是無中斷的。 HA 對繼續提供數據。

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

步驟

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

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

選擇不同的許可證和 VM 類型。

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

結果

Cloud Volumes ONTAP使用新設定重新啟動。

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

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

關於此任務

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

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

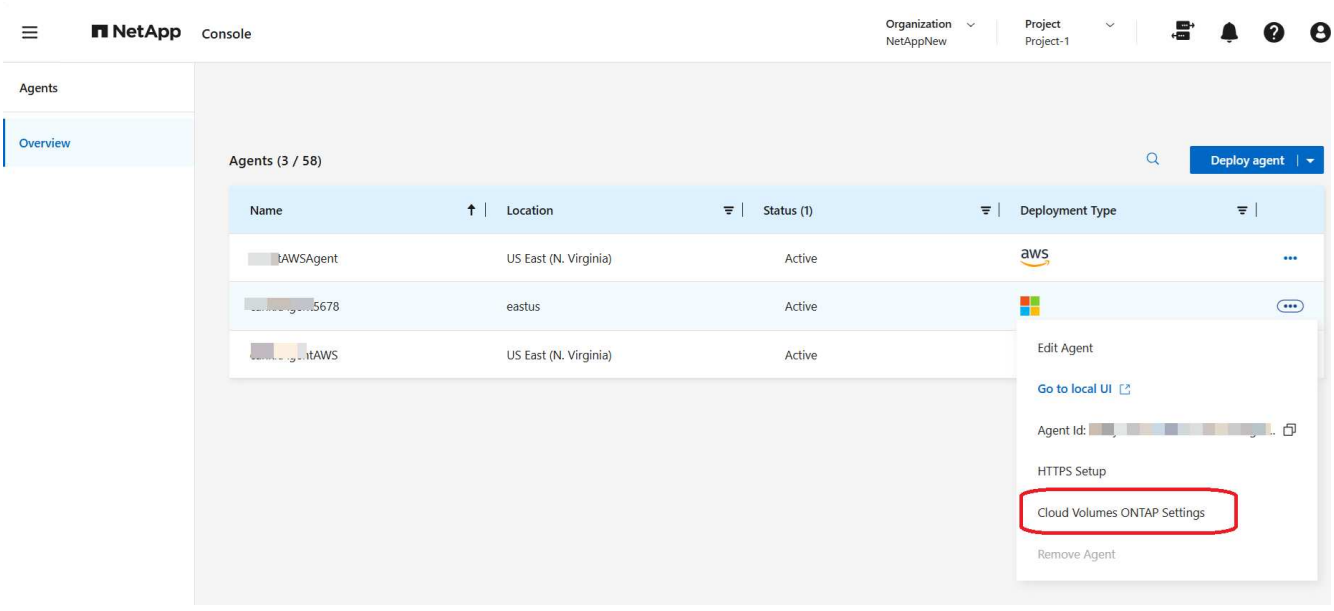
此過程可能會對 CIFS 用戶端造成破壞。 CIFS 用戶端未提交的資料可能會遺失。

開始之前

您需要先建立控制台代理，然後才能變更控制台設定。 "學習使用" 。

步驟

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



4. 在「Azure」下，按一下「Azure HA 系統的 Azure CIFS 鎖定」。

5. 按一下複選框以啟用該功能，然後按一下“儲存”。

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

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

概況

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

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

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

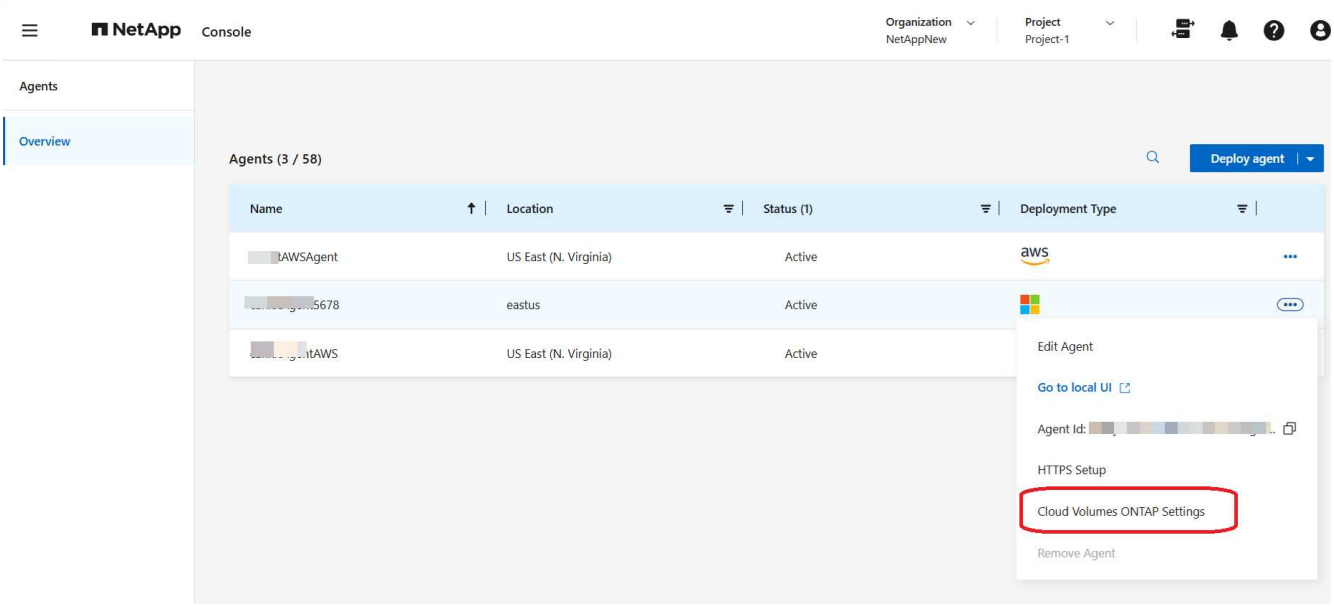
停用 **Azure Private Links** 並改用服務終點

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

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

步驟

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



4. 在「**Azure**」下，按一下「使用 **Azure** 專用連結」。

5. 取消選擇* Cloud Volumes ONTAP和儲存帳戶之間的專用連結連線*。
6. 點選“儲存”。

完成後

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

"了解如何在控制台代理上啟用直接 API 流量"

使用 **Azure Private Links**

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

自訂 **DNS** 的要求

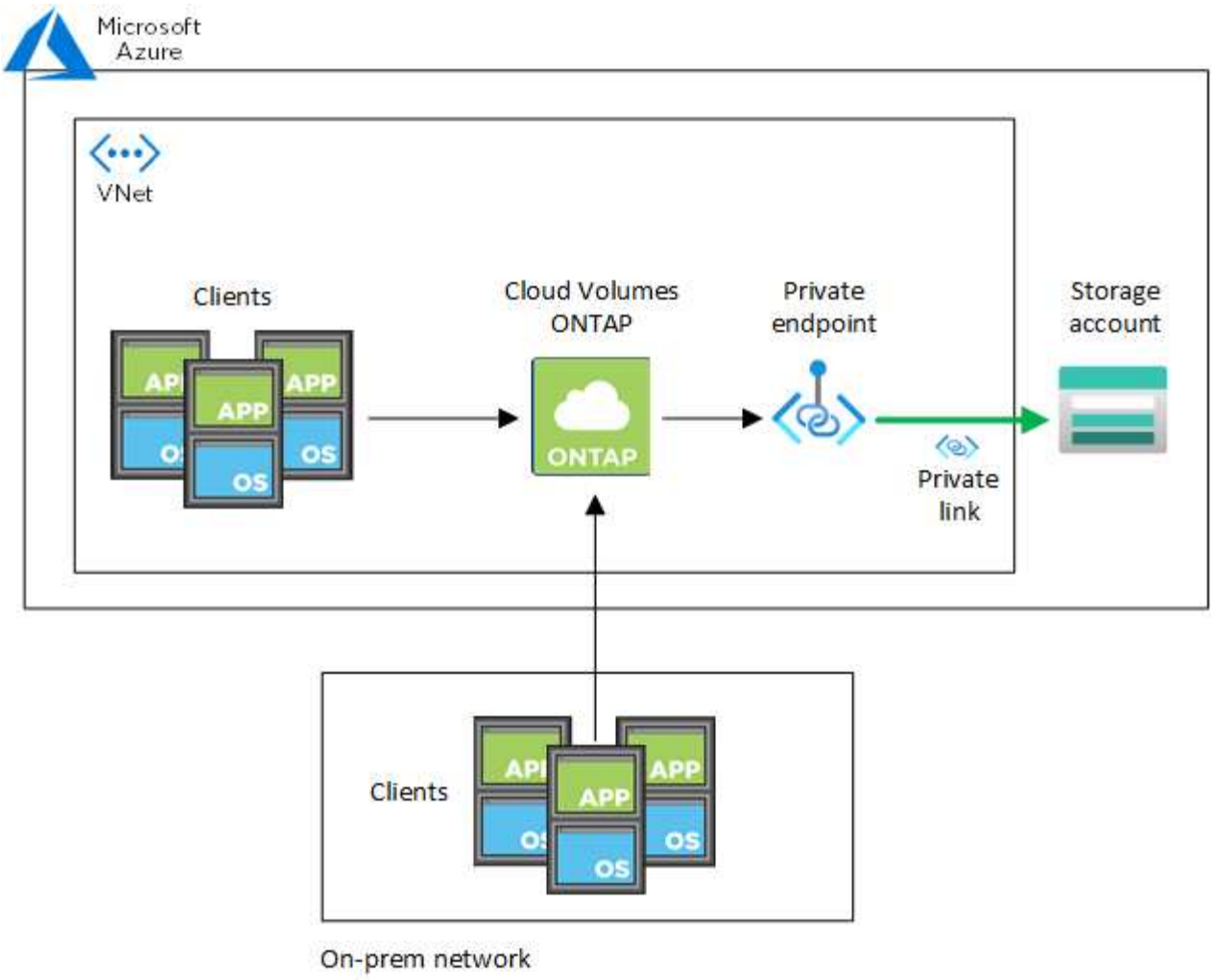
或者，如果您使用自訂 DNS，則需要從自訂 DNS 伺服器建立至 Azure 私人 DNS 區域的條件轉送器。要了解更多信息，請參閱"Azure 關於使用 DNS 轉送器的文檔"。

專用連結連接的工作原理

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

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

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



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

提供有關 **Azure** 專用 **DNS** 的詳細信息

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

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

步驟

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

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

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

4. 儲存檔案並登出控制台代理程式。

   不需要重新啟動。

啟用故障回滾

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

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

如果啟用回滾，控制台將停止該操作並回滾作為該操作的一部分所建立的所有資源。

您可以透過 API 或更新 app.conf 檔案來啟用回滾。

透過 **API** 啟用回滾

步

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

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

透過更新 **app.conf** 啟用回滾

步驟

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

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

. 儲存檔案並登出控制台代理程式。

   不需要重新啟動。

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

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

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

步驟

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

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

3. 在*系統*頁面上，發現系統。
4. 在系統資訊中尋找新的資源組。

結果

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

在 **Azure** 中隔離**SnapMirror**流量

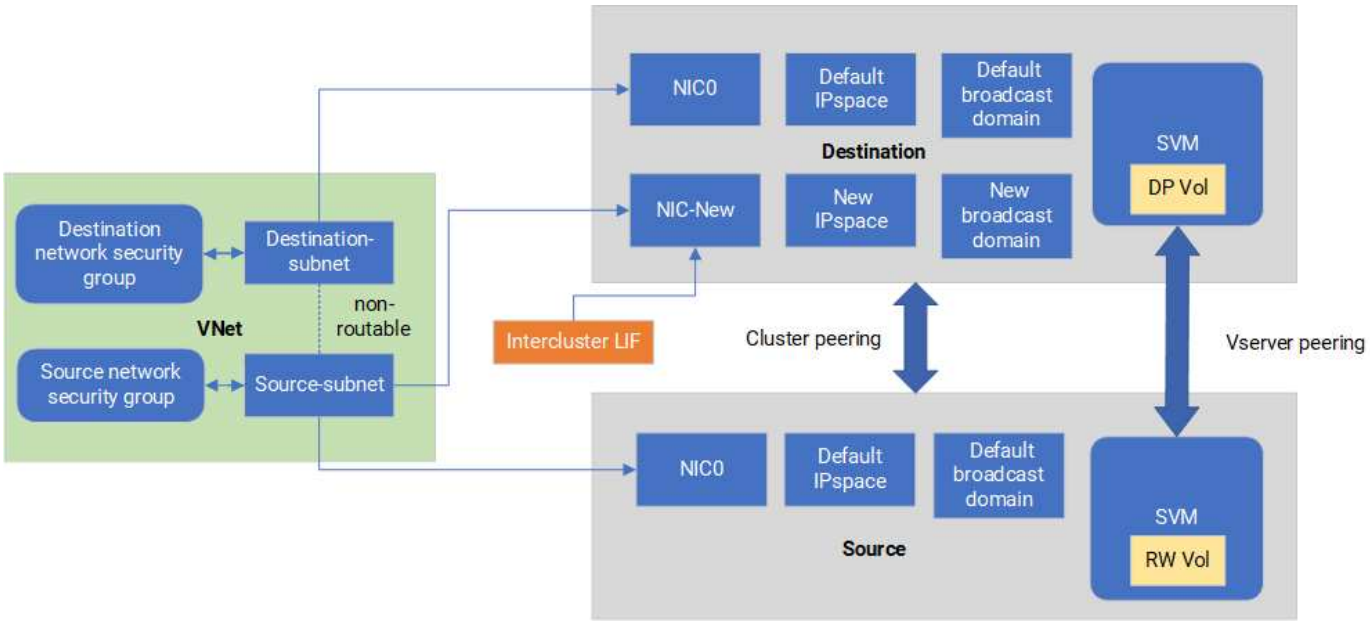
使用 Azure 中的Cloud Volumes ONTAP ，您可以將SnapMirror複製流量與資料和管理流量分開。為了將SnapMirror複製流量與資料流量隔離，您需要新增一個新的網路介面卡 (NIC)、一個相關的群集間 LIF 和一個不可路由的子網路。

關於 **Azure** 中的**SnapMirror**流量隔離

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

圖 1

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



開始之前

回顧以下注意事項：

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

步驟 **1**：建立額外的 **NIC** 並連接到目標 **VM**

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

步驟

1. 在ONTAP CLI 中，停止節點。

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

2. 在 Azure 入口網站中，檢查 VM（節點）狀態是否已停止。

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

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

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

b. 解除分配節點。

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

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

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

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

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

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

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

6. 啟動虛擬機器（節點）。

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

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

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

對於 HA 對部署，請對合作夥伴節點重複這些步驟。

步驟 **2**：為新 **NIC** 建立新的 **IP** 空間、廣播域和群集間 **LIF**

群集間 LIF 的單獨 IP 空間為群集間複製的網路功能提供了邏輯分離。

使用ONTAP CLI 執行以下步驟。

步驟

1. 建立新的 IP 空間（new_ipspace）。

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

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

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

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

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

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

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

5. 驗證新的集群間 LIF 的建立。

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

對於 HA 對部署，請對合作夥伴節點重複這些步驟。

步驟 **3**：驗證來源系統和目標系統之間的叢集對等連接

本節提供有關如何驗證來源系統和目標系統之間的對等關係的說明。

使用ONTAP CLI 執行以下步驟。

步驟

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

因此目標 IP 位址是來源上的群集間 LIF IP 位址。

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

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

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

對於 HA 對部署，請對合作夥伴節點重複這些步驟。

步驟 **4**：在來源系統和目標系統之間建立 **SVM** 對等連接

本節提供如何在來源系統和目標系統之間建立 SVM 對等的說明。

使用ONTAP CLI 執行以下步驟。

步驟

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

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

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

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

4. 輸入並確認密碼。
5. 檢查集群是否對等。

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

成功的對等連線在可用性欄位中顯示 可用。

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

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

7. 接受 SVM 對等連線。

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

8. 檢查 SVM 是否已對等。

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

同行國家顯示*peered* 和對等應用程式顯示*snapmirror*.

步驟 **5**：在來源系統和目標系統之間建立**SnapMirror**複製關係

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

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

使用ONTAP CLI 執行以下步驟。

步驟

1. 在目標 SVM 上建立資料保護磁碟區。

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

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

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

3. 在目標上初始化SnapMirror複製關係。

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

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

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

關係狀態是 `Snapmirrored`關係的健康是 `true`。

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

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

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

Google Cloud 管理

變更Cloud Volumes ONTAP的 Google Cloud 機器類型

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

關於此任務

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

  "ONTAP 9 文件：用於設定自動交還的命令"

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

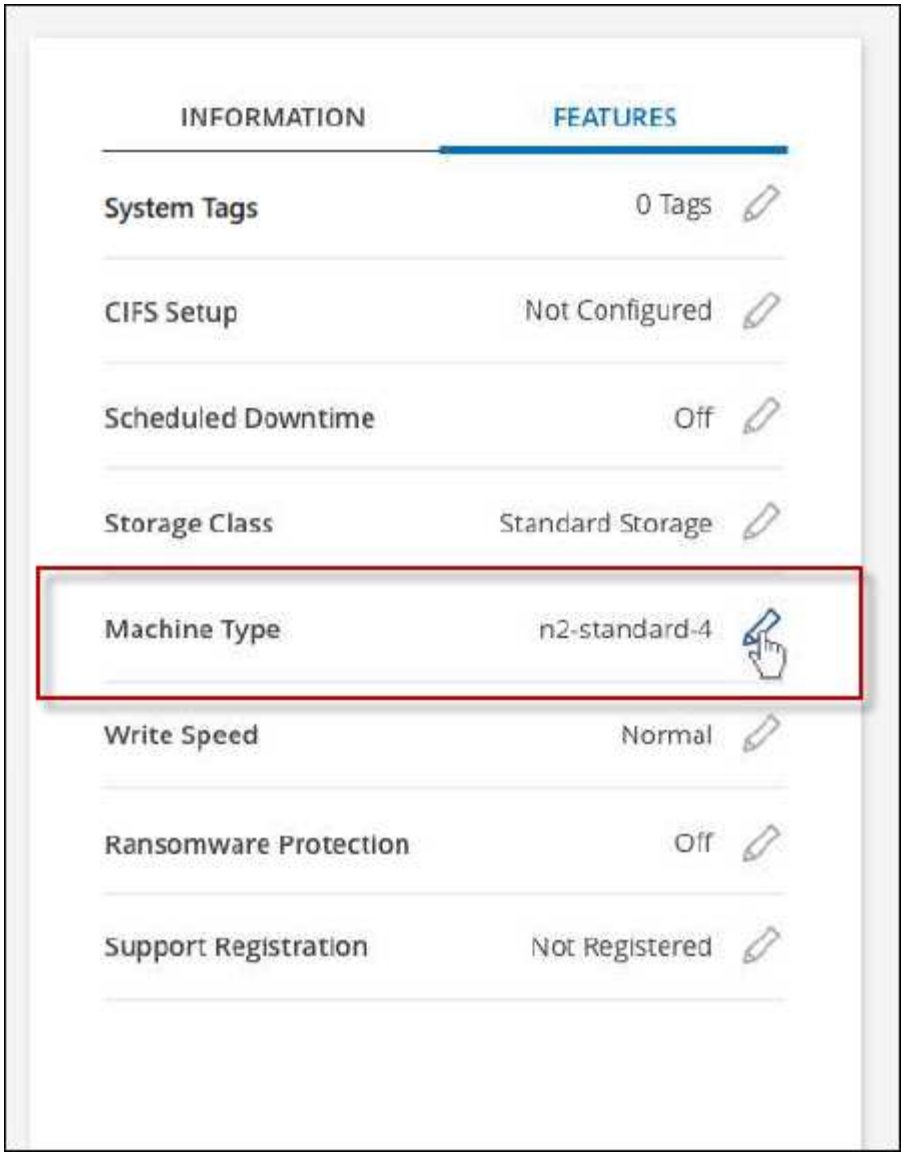
  對於單節點系統， I/O 會中斷。

  對於 HA 對來說，這種變化是無中斷的。 HA 對繼續提供數據。

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

步驟

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



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

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

結果

Cloud Volumes ONTAP使用新設定重新啟動。

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

自 2026 年 2 月 9 日起，Google Cloud 中新的 Cloud Volumes ONTAP 部署可以使用 Google Cloud Infrastructure Manager。Google 即將棄用 Google Cloud Deployment Manager，改用 Infrastructure Manager。因此，您需要手動執行遷移工具，將現有的 Cloud Volumes ONTAP 部署從 Deployment Manager 遷移到 Infrastructure Manager。此程序只需執行一次，之後您的系統將自動開始使用 Infrastructure Manager。

關於此任務

過渡工具可在 "NetApp 支援網站"中使用，並建立下列工件：

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

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

- `gs://netapp-cvo-infrastructure-manager-<project id>`：用於新的 Cloud Volumes ONTAP 部署的 ONTAP 版本和 SVM Terraform 範本。在此內， `dm-to-im-convert` 儲存桶包含 Cloud Volumes ONTAP Terraform 檔案。
- `<gcp project number>-<region>-blueprint-config`：用於儲存 Google Cloud Terraform 工件。

開始之前

- 請確保您的 Cloud Volumes ONTAP 系統版本為 9.16.1 或更高版本。
- 確保沒有透過 Google Cloud Console 手動編輯過任何 Cloud Volumes ONTAP 資源或其屬性。
- 請確保已啟用 Google Cloud API。請參閱 "啟用 Google Cloud API"。請確保除了其他 API 之外，還啟用了 Google Cloud Quotas API。
- 請確認 NetApp Console agent 的服務帳戶擁有所有必要的權限。請參閱 "控制台代理的 Google Cloud 權限"。

  對於私有模式部署，請確保滿足下列附加前提條件：

  - 請確保您已安裝最新版本的 Console 代理程式。從 NetApp Support Site 下載產品安裝程式，然後手動將代理程式安裝到您的主機上，以便代理程式可以使用 Infrastructure Manager API。
  - 如果您以私有模式執行該工具，請確保除了其他 API 之外，還啟用了 Cloud Build API "啟用 Google Cloud API"。
  - 請確保您已完成網路配置並為私有模式部署建立了工作池。請參閱 "私有模式部署的 Infrastructure Manager 組態"。

- 轉換工具使用以下網域。在您的網路中於連接埠 443 上啟用它們：

網域	港口	協定	方向	目的
cloudresourcemanager.googleapis.com	443	TCP	外傳	專案驗證
deploymentmanager.googleapis.com	443	TCP	外傳	部署探索

網域	港口	協定	方向	目的
config.googleapis.com	443	TCP	外傳	Infrastructure Manager API
storage.googleapis.com	443	TCP	外傳	GCS 儲存貯體作業
iam.googleapis.com	443	TCP	外傳	服務帳戶驗證
compute.googleapis.com	443	TCP	外傳	Google Cloud 和 Terraform Import 與 Plan 使用的運算 API 呼叫
cloudbuild.googleapis.com	443	TCP	外傳	僅私有模式需要建置操作
openidconnect.googleapis.com	443	TCP	外傳	驗證
oauth2.googleapis.com	443	TCP	外傳	OAuth2 權杖交換
registry.terraform.io	443	TCP	外傳	Terraform 提供者登錄
releases.hashicorp.com	443	TCP	外傳	Terraform 二進位下載
apt.releases.hashicorp.com	443	TCP	外傳	HashiCorp APT 存儲庫
us-central1-docker.pkg.dev	443	TCP	外傳	GCP Artifact Registry
metadata.google.internal	80	HTTP	內部	VM 元資料和驗證權杖
pypi.org	443	TCP	外傳	Python 套件索引
files.pythonhosted.org	443	TCP	外傳	Python 套件下載
checkpoint-api.hashicorp.com	443	TCP	外傳	Terraform 版本檢查
download.docker.com	443	TCP	外傳	Docker APT 儲存庫
security.ubuntu.com	80/443	TCP	外傳	Ubuntu 安全更新
*.gce.archive.ubuntu.com	80	TCP	外傳	Ubuntu 軟體包鏡像

準備執行工具的環境

執行工具之前，請先執行這些步驟。

步驟

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

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

      為私有模式部署新增額外權限

      如果您以私有模式執行該工具，請同時將 `cloudbuild.workerpools.get` 權限新增至 YAML 檔案。

   b. 在 Google Cloud 中建立自訂角色，並賦予其 YAML 檔案中定義的權限。
      `gcloud iam roles create dmtoim_convert_tool_role --project=PROJECT_ID \
      --file=YAML_FILE_PATH`如需詳細資訊，請參閱 "建立和管理自訂角色"。
   c. 將自訂角色附加到您將用於建立 VM 的服務帳戶。
   d. 將 `roles/iam.serviceAccountUser`角色新增至此服務帳戶。請參閱 "服務帳戶概覽"。

2. 建立一個具有以下組態的 VM 。您可以在此 VM 上執行此工具。
   - 機器類型：Google Compute Engine 機器類型 e2-medium
   - 作業系統：根據您的需求、選擇以下任一映像：
     - Ubuntu 25.10 AMD64 Minimal（映像：ubuntu-minimal-2510-amd64）
     - SUSE Linux Enterprise Server 15 SP7 x86_64
   - 網路：防火牆允許 HTTP 和 HTTPs
   - 磁碟大小：20GB
   - 安全性：服務帳戶：您建立的服務帳戶
   - 安全性：存取範圍 - 為每個 API 設定存取權限：
     - 雲端平台：已啟用
     - Compute Engine ：唯讀
     - 儲存：唯讀 （預設）
     - Google Cloud Logging（以前稱為 Stackdriver Logging）API：僅寫入（預設）
     - Stackdriver Monitoring（現為 Google Cloud Operations 的一部分）API：僅寫入（預設）
     - 服務管理：唯讀 （預設）
     - 服務控制：已啟用 （預設）
     - Google Cloud Trace（以前稱為 Stackdriver Trace）：僅寫入（預設）
3. 使用 SSH 連線至新建立的 VM： `gcloud compute ssh dmtoim-convert-executor-vm --zone <region where VM is deployed>`
4. 使用您的 NSS 憑證從 "NetApp 支援網站"下載轉換工具： `wget <download link from NetApp Support site>`
5. 解壓縮下載的 TAR 檔： `unzip <downloaded file name>`

Ubuntu

1. 下載並安裝以下必備套件：
   - Docker：28.2.2 build 28.2.2-0ubuntu1 或更新版本
   - Terraform：1.14.1 或更高版本
   - Python：3.13.7、python3-pip、python3 venv

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

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

SUSE Linux Enterprise Server

1. 設定 Python： `sudo update-alternatives --install /usr/bin/python3 python3 /usr/bin/python3.11 2`
2. 安裝 pip3 以安裝套件： `python3.11 -m ensurepip --upgrade`
3. 安裝 Terraform：

   ```
   wget
   https://releases.hashicorp.com/terraform/1.7.4/terraform_1.7.4_linux
   _amd64.zip
   unzip terraform_1.7.4_linux_amd64.zip
   sudo mv terraform /usr/local/bin/
   rm terraform_1.7.4_linux_amd64.zip
   ```

4. 安裝 Google Cloud SDK（gcloud）

   ```
   curl https://sdk.cloud.google.com | bash
   exec -l $SHELL
   ```

執行轉換工具

這些步驟適用於 Ubuntu 和 SUSE Linux Enterprise Server 上執行轉換工具。

步驟

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

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

2. 安裝轉換工具：

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

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

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

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

在私有模式部署中執行該工具

指定 `--worker-pool` 參數以在私有模式部署中執行該工具。有關工作池配置，請參閱 "私有模式部署的 Infrastructure Manager 組態"。

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

完成後

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

> 轉換完成後，請勿在 Google Cloud Console 中刪除 Deployment Manager 的部署物件。此部署物件包含您可能需要用來回滾已轉換系統的資訊。

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

復原轉換

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

步驟

1. 在同一個 您為執行該工具而建立的 VM 上，執行以下命令：

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

2. 請等待復原完成。

相關連結

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

使用系統管理員管理Cloud Volumes ONTAP

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

特徵

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

- 進階儲存管理：管理一致性群組、共用、qtree、配額和儲存虛擬機器。
- 成交量變動： "將磁碟區移動到不同的聚合。"
- 網路管理：管理 IP 空間、網路介面、連接埠集和乙太網路連接埠。
- 管理FlexGroup磁碟區：您只能透過系統管理員建立和管理FlexGroup磁碟區。 BlueXP控制台不支

援FlexGroup磁碟區建立。

- 事件和作業：查看事件日誌、系統警報、作業和稽核日誌。
- 進階資料保護：保護儲存虛擬機器、LUN 和一致性群組。
- 主機管理：設定 SAN 啟動器群組和 NFS 用戶端。
- ONTAP S3 物件儲存管理：Cloud Volumes ONTAP 中的 ONTAP S3 儲存管理功能僅在 System Manager 中可用，而不在 Console 中可用。

支援的配置

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

限制

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

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

配置存取系統管理員的身份驗證

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

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

所需權限

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

步驟

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

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

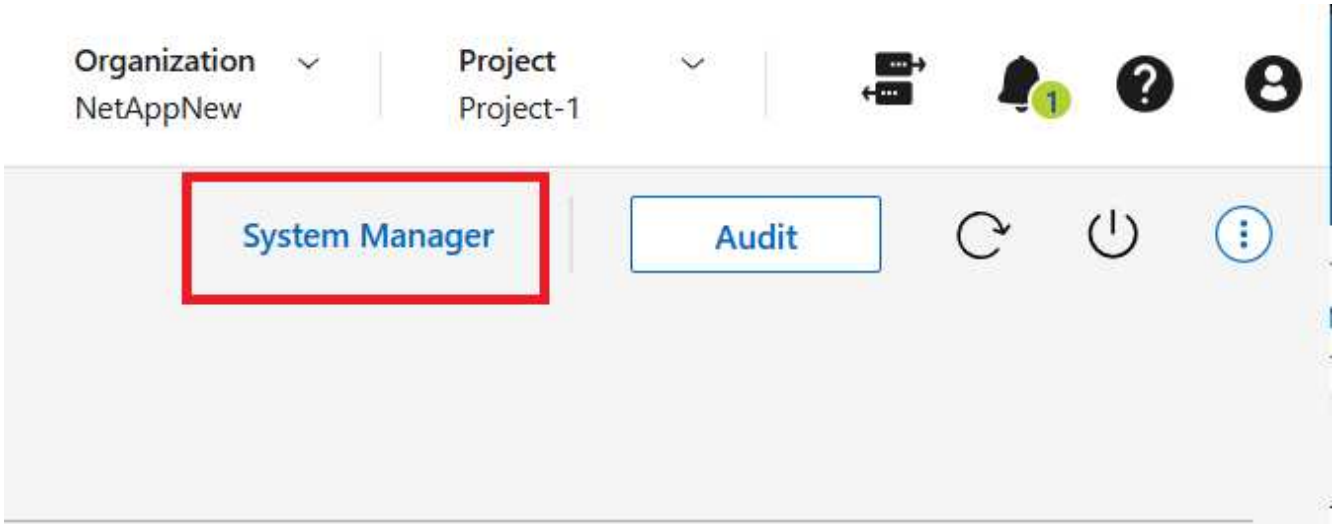
4. 點選“儲存”。

開始使用系統管理員

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

步驟

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



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

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

有關使用系統管理員的協助

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

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

從 CLI 管理Cloud Volumes ONTAP

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

開始之前

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

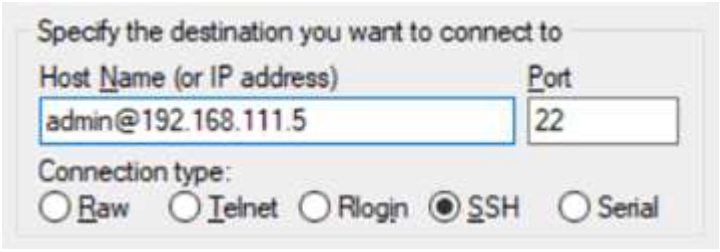
當部署在多個 AZ 中時， Cloud Volumes ONTAP HA 配置使用浮動 IP 位址作為叢集管理接口，這表示外部路由不可用。您必須從屬於相同路由域的主機進行連線。

步驟

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

   例子

   下圖顯示了使用 PuTTY 的範例：



3. 在登入提示字元下，輸入管理員帳戶的密碼。

   例子

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