設定 ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

目錄

設定 ONTAP tools for VMware vSphere

將 vCenter Server 執行個體新增至 ONTAP tools

將 vCenter Server 執行個體新增至 ONTAP tools for VMware vSphere，即可在 vCenter Server 環境中設定、管理和保護虛擬資料存放區。新增多個 vCenter Server 執行個體時，需要自訂 CA 憑證，才能確保 ONTAP tools 與每個 vCenter Server 之間的安全通訊。

關於此任務

ONTAP tools 與 vCenter 伺服器整合，可直接從 vSphere 用戶端執行儲存設備工作，例如資源配置、Snapshot 快照技術和資料保護。

將 vCenter 伺服器執行個體新增至 ONTAP tools 會自動觸發以下動作：

- ONTAP tools 將 vCenter 用戶端外掛註冊為遠端外掛。
- 外掛和 API 的自訂權限會套用至 vCenter Server 執行個體。
- 建立自訂角色以管理使用者。
- 該外掛在 vSphere 使用者介面上顯示為捷徑。

開始之前

- 請確保 vCenter Server 憑證包含有效的「使用者備用名稱（SAN）」擴展，其中包含 DNS 和 IP 位址項目。例如：

```
X509v3 extensions:
    X509v3 Subject Alternative Name:
        DNS: vcenter.example.com, DNS: vcenter, IP Address: 192.168.0.50
```

  如果憑證不包含 SAN 擴充，或者 SAN 擴充不包含正確的 DNS 或 IP 位址值，ONTAP tools 操作可能會因憑證驗證錯誤而失敗。

- vCenter Server 的主網路識別碼（PNID）必須包含在 SAN 詳細資訊中。PNID 和 DNS 名稱應相同，並且可在 DNS 中解析。
- 建議使用完全限定網域名稱（FQDN）部署 vCenter Server，確保憑證中的 SAN 包含 DNS Name=machine_FQDN，以獲得最佳相容性和支援。
- 如需更多資訊，請參閱 VMware 文件：
  - "不同解決方案路徑的 vSphere 憑證需求"
  - "替換 vCenter Machine SSL 憑證自訂憑證授權單位簽署憑證"
  - "錯誤：主題備用名稱（SAN）欄位不包含 PNID。請提供有效的證書"

> ⓘ 如果 FQDN 不可用，您可以將 PNID 設定為 IP 位址，並將該 IP 位址包含在 SAN 中。但是，VMware 不建議這樣做。

步驟

1. 開啟網頁瀏覽器並造訪以下網址： `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 使用您在部署期間提供的 ONTAP tools for VMware vSphere 系統管理員憑證登入。
3. 選擇 **vCenters** > 新增 以就職 vCenter Server 執行個體。提供您的 vCenter IP 位址或主機名稱、使用者名稱、密碼和連接埠詳細資訊。
4. 在進階選項中，自動擷取 vCenter Server 憑證（授權）或手動上傳。

> 您無需系統管理員帳戶即可將 vCenter 執行個體新增至 ONTAP tools。您可以建立不含系統管理員帳戶且權限受限的自訂角色。詳情請參閱 "將 vCenter 伺服器 RBAC 與 ONTAP tools for VMware vSphere 10 搭配使用"。

在 ONTAP 工具中將 VASA Provider 註冊到 vCenter Server 執行個體

使用 ONTAP tools for VMware vSphere 將 VASA Provider 註冊到 vCenter Server 執行個體。這可實現原則型儲存設備管理、vVols 支援，以及與 ONTAP 系統上的 VMware Live Site Recovery 設備的整合。

VASA Provider 設定顯示所選 vCenter Server 的註冊狀態。

步驟

1. 登入 vSphere 用戶端。
2. 在外掛區段下，選擇 快捷方式 > **NetApp ONTAP tools**。
3. 選擇 **Settings** > **VASA Provider settings**。ONTAP tools 會顯示 VASA Provider 的註冊狀態為「未註冊」。
4. 選擇*註冊*按鈕以註冊 VASA Provider。
5. 請輸入 VASA Provider 的名稱和認證資料。使用者名稱只能包含字母、數字和底線。密碼長度必須介於 8 到 256 個字元之間。
6. 選擇 **Register**。
7. 註冊成功並重新整理頁面後，ONTAP tools 會顯示已註冊的 VASA Provider 的狀態、名稱和版本。

接下來

確認已入駐的 VASA Provider 是否已列入 vCenter 用戶端的 VASA Provider 名錄中：

步驟

1. 前往 vCenter Server 執行個體。
2. 使用系統管理員憑證登入。
3. 選取 **Storage Providers** > **Configure**。確認已加入的 VASA Provider 已正確列出。

使用 ONTAP tools 安裝 NFS VAAI 外掛

用於陣列整合的 NFS vStorage API （NFS VAAI）外掛可將 VMware vSphere 連接到 NFS 儲存陣列。使用 ONTAP tools for VMware vSphere 安裝 VAAI 外掛。這樣，NFS 儲

存陣列就可以處理某些儲存設備作業，而無需透過 ESXi 主機。

開始之前

- 下載 "NetApp 適用於 VMware VAAI 的 NFS 外掛" 安裝套件。
- 請確保您的 ESXi 主機版本為 vSphere 7.0 U3（最新修補程式或更高版本），ONTAP 為 9.14.1 或更高版本。
- 掛載 NFS 資料儲存。

步驟

1. 登入 vSphere 用戶端。
2. 在外掛區段下，選擇 快捷方式 > **NetApp ONTAP tools**。
3. 選擇 **Settings** > **NFS VAAI Tools**。
4. 如果您已將 VAAI 外掛上傳到 vCenter Server，請在「現有版本」中選擇「變更」。如果您尚未上傳，請選擇「上傳」。
5. 瀏覽並選擇 `.vib`檔案，然後選擇 **Upload** 將檔案上傳至 ONTAP tools。
6. 選擇 **Install on ESXi host**、選擇要安裝 NFS VAAI 插件的 ESXi 主機，然後選擇 **Install**。

   vSphere Web 用戶端僅顯示可安裝該外掛的 ESXi 主機。您可以在「最近工作」部分監控安裝進度。

7. 安裝後手動重新啟動 ESXi 主機。

   重新啟動 ESXi 主機後、ONTAP tools for VMware vSphere vSphere 會自動偵測並啟用 NFS VAAI 外掛程式。

接下來呢？

安裝 NFS VAAI 外掛並重新開機 ESXi 主機後，設定 VAAI 複本卸載的 NFS 匯出原則。確保匯出原則規則符合以下要求：

- 相關 ONTAP Volume 允許 NFSv4 呼叫。
- root 使用者仍為 root，且所有交會父 Volume 均允許使用 NFSv4。
- VAAI 支援選項已在相關的 NFS 伺服器上設定。

如需更多資訊，請參閱 "為 VAAI 複本卸載設定正確的 NFS 匯出原則"知識庫文章。

相關資訊

"支援 VMware vStorage over NFS"

"啟用或停用 NFSv4.0"

"ONTAP 支援 NFSv4.2"

在 ONTAP 工具中設定 ESXi 主機設定

設定 ESXi 伺服器的多重路徑和逾時設定有助於維護資料可用度和完整性。如果主要路徑無法使用，系統可自動容錯移轉至備份儲存設備路徑。

設定 **ESXi** 伺服器多重路徑和逾時設定

ONTAP tools for VMware vSphere 會檢查並設定最適合與 NetApp 儲存系統搭配使用的 ESXi 主機多重路徑設定和 HBA 逾時設定。

關於此任務

此過程可能需要一些時間，具體取決於您的設定和系統負載。您可以在「最近工作」面板中檢視進度。

步驟

1. 從 VMware vSphere Web 用戶端首頁，選擇「主機和叢集」。
2. 在 VMware vSphere Web 用戶端的捷徑頁面上，選擇外掛程式區段下的 **NetApp ONTAP tools**。
3. 前往 ONTAP tools for VMware vSphere 外掛的總覽（儀表板）中的 **ESXi** 主機法規遵循 卡片。
4. 選擇 **Apply Recommended Settings** 連結。
5. 在「套用建議主機設定」視窗中，選擇要更新為使用 NetApp 建議設定的主機，然後選擇「下一步」。

   您可以擴充 ESXi 主機以查看目前值。

6. 在設定頁面中，視需要選取建議值。
7. 在摘要窗格中，檢查各項值並選擇「完成」。您可以在最近工作面板中追蹤進度。

設定 **ESXi** 主機值

使用 ONTAP tools for VMware vSphere，可為 ESXi 主機設定逾時和其他值，以實現最佳效能和故障轉移。這些值是根據 NetApp 測試結果設定的。

您可以在 ESXi 主機上設定以下值：

HBA/CNA 介面卡設定

將以下參數設定為預設值：

- Disk.QFullSampleSize
- Disk.QFullThreshold
- Emulex FC HBA 逾時
- QLogic FC HBA 逾時

MPIO 設定

MPIO 設定會為 NetApp 儲存設備系統選擇最佳路徑。MPIO 設定會選擇最佳路徑並使用該路徑。

對於高效能環境或使用單一 LUN 資料儲存進行測試時，請調整輪詢 （VMW_PSP_RR） 路徑選擇原則 （PSP ） 的負載平衡設定以提高效能。將預設 IOPS 值從 1000 設定為 1。

MPIO 設定不適用於 NVMe、NVMe/FC 和 NVMe/TCP 協定。

NFS 設定

參數	將此值設為……
Net.TcpipHeapSize	32
Net.TcpipHeapMax	1024 MB
NFS.MaxVolumes	256
NFS41.MaxVolumes	256
NFS.MaxQueueDepth	128 或更高
NFS.HeartbeatMaxFailures	10
NFS.HeartbeatFrequency	12
NFS.HeartbeatTimeout	5

為 **ONTAP tools** 配置 **ONTAP** 使用者角色和權限

本部分用於設定儲存設備後端的 ONTAP 使用者角色和 Privileges，搭配 ONTAP tools for VMware vSphere 和 ONTAP System Manager。您可以使用提供的 JSON 檔案指派角色、手動建立使用者和角色，並為非系統管理員帳戶套用所需的最低 Privileges。

開始之前

- 使用 *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip* 從 ONTAP tools for VMware vSphere 下載 ONTAP Privileges 檔案。下載 zip 檔案後，您會找到兩個 JSON 檔案。設定 ASA r2 系統時，請使用 ASA r2 特有的 JSON 檔案。

  您可以在叢集層級建立使用者，也可以直接在儲存設備虛擬機器 （SVM） 層級建立使用者。如果您不使用 user_roles.json 檔案，請確保使用者擁有所需的最低 SVM 權限。

- 使用系統管理員權限登入儲存設備後端。

步驟

1. 解壓縮您下載的 *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip* 檔案。
2. 使用叢集的叢集管理 IP 位址存取 ONTAP System Manager。
3. 使用系統管理員權限登入叢集。若要設定使用者：
   a. 若要設定叢集 ONTAP tools 使用者，請選擇 **Cluster** > **Settings** > **Users and Roles** 窗格。
   b. 若要設定 SVM ONTAP tools 使用者，請選取 **Storage SVM** > **Settings** > **Users and Roles** 窗格。
   c. 在「使用者」下選擇「新增」。
   d. 在「新增使用者」對話方塊中，選擇「虛擬化產品」。
   e. 瀏覽 以選擇並上傳 ONTAP Privileges JSON 檔案。對於非 ASA r2 系統，請選擇 users_roles.json 檔案；對於 ASA r2 系統，請選擇 users_roles_ASAr2.json 檔案。

      ONTAP tools 會自動填入產品欄位。

   f. 從下拉式選單中選擇產品功能為 **VSC**、**VASA Provider** 和 **SRA**。

ONTAP tools 會根據您選擇的產品功能自動填入「角色」欄位。

g. 請輸入所需的使用者名稱和密碼。

h. 選擇使用者需要的 Privileges （Discovery、Create Storage、Modify Storage、Destroy Storage 、NAS/SAN Role），然後選擇 **Add**。

ONTAP tools 新增了新的角色和使用者。您可以檢視您設定的角色下的 Privileges。

SVM 彙總映射需求

使用 SVM 使用者憑證佈建資料儲存區時，ONTAP tools for VMware vSphere 會在資料儲存區 POST API 中指定的彙總上建立 Volume。ONTAP 會防止 SVM 使用者在未對應至該 SVM 的彙總上建立 Volume。在建立 Volume 之前，請先使用 ONTAP REST API 或 CLI 將 SVM 對應至所需的彙總。

REST API：

```
PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"aggregates":{"name":["aggr1","aggr2","aggr3"]}}'
```

ONTAP CLI：

```
sti115_vsim_ucs630f_aggr1 vserver show-aggregates
AvailableVserver        Aggregate      State         Size Type    SnapLock
Type-------------- -------------- ------- ---------- -------
--------------svm_test       sti115_vsim_ucs630f_aggr1
online     10.11GB vmdisk  non-snaplock
```

手動建立 ONTAP 使用者和角色

無需 JSON 檔案，手動建立使用者和角色。

1. 使用叢集的叢集管理 IP 位址存取 ONTAP System Manager。
2. 使用系統管理員權限登入叢集。
   a. 若要設定叢集 ONTAP tools 角色，請選擇 **Cluster** > **Settings** > **Users and Roles**。
   b. 若要設定叢集 SVM ONTAP tools 角色，請選擇 儲存 **SVM** > 設定 > 使用者和角色。
3. 建立角色：
   a. 在 **Roles** 表下選擇 **Add**。
   b. 請輸入*角色名稱*和*角色屬性*的詳細資料。

      新增 **REST API Path**，並從下拉清單中選擇存取。

   c. 新增所有需要的 API 並儲存變更。
4. 建立使用者：

a. 在 **Users** 表格下選取 **Add** 。
b. 在「新增使用者」對話方塊中，選取「System Manager」。
c. 請輸入*使用者名稱*。
d. 從上述「建立角色」步驟中建立的選項中選取 **Role**。
e. 輸入您要授予存取權限的應用程式以及驗證方法。ONTAPI 和 HTTP 是必要的應用程式、驗證類型為 **Password** 。
f. 設定*使用者密碼*並*儲存*使用者。

非管理員全域範圍叢集使用者所需的最低權限清單

本頁列出了非管理員全域作用域叢集使用者在沒有 JSON 檔案的情況下所需的最低權限。如果叢集處於本機作用域，請使用 JSON 檔案建立使用者，因為 ONTAP tools for VMware vSphere 在 ONTAP 上進行佈建所需的不只是讀取權限。

您可以透過使用 API 存取功能：

API	存取層級	用於
/api/cluster	唯讀	叢集組態探索
/api/cluster/licensing/licenses	唯讀	檢查通訊協定特定授權。
/api/cluster/nodes	唯讀	平台類型探索
/api/security/accounts	唯讀	Privilege 探索
/api/security/roles	唯讀	Privilege 探索
/api/storage/aggregates	唯讀	資料存放區/Volume 配置期間的彙總空間檢查
/api/storage/cluster	唯讀	取得叢集層級的空間和效率資料
/api/storage/disks	唯讀	取得彙總中關聯的磁碟
/api/storage/qos/policies	讀取/建立/修改	QoS 和 VM 原則管理
/api/svm/svms	唯讀	在本機新增叢集時取得 SVM 組態。
/api/network/ip/interfaces	唯讀	新增儲存設備後端 - 確定管理 LIF 範圍是叢集/SVM
/api/storage/availability-zones	唯讀	SAZ 探索。適用於 ONTAP 9.16.1 版本及更新版本和 ASA r2 系統。
/api/cluster/metrocluster	唯讀	取得 MetroCluster 狀態和組態詳情。

建立 **ONTAP tools for VMware vSphere** 基於 **ONTAP API** 的叢集範圍使用者

對資料存放區執行 PATCH 操作和自動回溯需要探索、建立、修改和毀損 Privileges。缺少 Privileges 可能會導致工作流程和清理問題。

具有探索、建立、修改和毀損 Privileges 的 ONTAP API 使用者可以管理 ONTAP tools 工作流程。

若要建立具有上述所有 Privileges 的叢集範圍使用者，請執行以下命令：

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all

security login rest-role create -role <role-name> -api
/api/private/cli/snapmirror -access all

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all

security login rest-role create -role <role-name> -api /api/storage/luns
-access all

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all

security login rest-role create -role <role-name> -api
/api/storage/qos/policies -access all

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create
```

```
security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify

security login rest-role create -role <role-name> -api /api/cluster
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly

security login rest-role create -role <role-name> -api
/api/cluster/licensing/licenses -access readonly

security login rest-role create -role <role-name> -api /api/cluster/nodes
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/ports -access readonly

security login rest-role create -role <role-name> -api
```

```
/api/network/ip/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/aggregates -access readonly

security login rest-role create -role <role-name> -api
/api/storage/cluster -access readonly

security login rest-role create -role <role-name> -api /api/storage/disks
-access readonly

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly

security login rest-role create -role <role-name> -api
/api/cluster/metrocluster -access readonly
```

此外、對於 ONTAP 9.16.0 及更高版本、請執行以下命令：

```
security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all
```

對於執行 ONTAP 9.16.1 及更高版本的 ASA r2 系統，請執行以下命令：

```
security login rest-role create -role <role-name> -api
/api/storage/availability-zones -access readonly
```

建立 **ONTAP tools for VMware vSphere** 基於 **ONTAP API** 的 **SVM** 範圍使用者

執行以下命令以建立具有所有 Privileges 的 SVM 作用域使用者：

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/private/cli/snapmirror -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/luns
-access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create -vserver <vserver-
name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
```

```
/api/network/fc/logins -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly -vserver <vserver-
name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly -vserver <vserver-name>
```

此外、對於 ONTAP 9.16.0 及更高版本、請執行以下命令：

```
security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all -vserver <vserver-name>
```

若要使用先前建立的 API 型角色建立新的 API 型使用者，請執行下列命令：

```
security login create -user-or-group-name <user-name> -application http
-authentication-method password -role <role-name> -vserver <cluster-or-
vserver-name>
```

範例：

```
security login create -user-or-group-name testvpsraall -application http
-authentication-method password -role
OTV_10_VP_SRA_Discovery_Create_Modify_Destroy -vserver C1_sti160-cluster_
```

執行以下命令解除鎖定帳戶並啟用管理介面存取：

```
security login unlock -user <user-name> -vserver <cluster-or-vserver-name>
```

範例：

```
security login unlock -username testvpsraall -vserver C1_sti160-cluster
```

將 **ONTAP tools for VMware vSphere 10.1** 使用者升級至 **10.3** 使用者

對於使用 JSON 檔案建立叢集範圍使用者的 ONTAP tools for VMware vSphere 10.1 使用者，請使用下列具有使用者系統管理員權限的 ONTAP CLI 命令升級至 10.3 版本。

產品功能方面：

- VSC
- VSC 和 VASA Provider
- VSC 和 SRA
- VSC、VASA Provider 和 SRA。

叢集 Privileges：

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace show" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem show" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host show" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map show" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host add" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map add" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace delete" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem delete" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host remove" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map remove" -access all

對於使用 json 檔案建立 SVM 範圍使用者的 ONTAP tools for VMware vSphere 10.1 使用者，請使用具有管理員使用者權限的 ONTAP CLI 命令升級至 10.3 版本。

SVM 權限：

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host add" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map add" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace delete" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem delete" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host remove" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map remove" -access all -vserver <vserver-name>

若要啟用下列命令，請將命令 *vserver nvme namespace show* 和 *vserver nvme subsystem show* 新增至現有角

色。

```
vserver nvme namespace create

vserver nvme namespace modify

vserver nvme subsystem create

vserver nvme subsystem modify
```

將 **ONTAP tools for VMware vSphere 10.3** 使用者升級至 **10.4** 使用者

從 ONTAP 9.16.1 開始，將 ONTAP tools for VMware vSphere 10.3 使用者升級至 10.4 使用者。

對於使用 JSON 檔案建立叢集範圍使用者的 ONTAP tools for VMware vSphere 10.3 使用者，以及 ONTAP 版本 9.16.1 或更高版本，請使用具有管理員使用者權限的 ONTAP CLI 命令升級至 10.4 版本。

產品功能方面：

- VSC
- VSC 和 VASA Provider
- VSC 和 SRA
- VSC、VASA Provider 和 SRA。

叢集 Privileges：

```
security login role create -role <existing-role-name> -cmddirname "storage
availability-zone show" -access all
```

為 **ONTAP tools** 新增儲存後端

使用 ONTAP tools for VMware vSphere，為 ESXi 主機新增和管理儲存設備後端。您可以就職叢集或 SVM、啟用 MetroCluster 支援，並驗證憑證以確保安全連線。您可以使用 ONTAP tools Manager 或 vSphere 用戶端設定儲存設備後端、監控憑證狀態，並在叢集變更後手動重新探索資源。

若要在本機新增儲存設備後端，請在 ONTAP tools 介面中使用叢集或 SVM 憑證。本機儲存設備後端僅對選定的 vCenter 伺服器可用。ONTAP tools 會將 SVM 對應到 vCenter 伺服器，用於 vVols 或 VMFS 資料儲存管理。對於 VMFS 資料儲存和 SRA 工作流程，您可以使用 SVM 憑證，無需全域映射叢集。

若要新增全域儲存設備後端，請在 ONTAP tools Manager 中使用 ONTAP 叢集憑證。全域儲存設備後端支援探索工作流程，以識別 vVol 管理所需的叢集資源。在多租戶環境中，您可以在本機新增 SVM 使用者來管理 vVols 資料存放區。

請參閱知識庫文章： "OTV 10：什麼是儲存後端全域和本機範圍" 以了解有關全域和本機儲存後端的更多資訊。

如果已在 ONTAP 中啟用 MetroCluster 支援，請將來源和目的地叢集就職為本地或全域儲存設備後端。

開始之前

確認憑證包含有效的「主體替代名稱」（SAN）欄位。ONTAP 系統使用 SAN 欄位來識別叢集和 SVM 管理 LIF。

使用 **ONTAP tools Manager**

在多租戶設定中，您可以全域新增儲存設備後端叢集，並在本機新增 SVM 以使用 SVM 使用者憑證。

步驟

1. 透過網頁瀏覽器啟動 ONTAP tools Manager：
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 使用您在部署期間提供的 ONTAP tools for VMware vSphere 系統管理員憑證登入。
3. 從側邊欄選取 **Storage Backends**。
4. 新增儲存設備後端並提供伺服器 IP 位址或 FQDN、使用者名稱和密碼等詳細資訊。

   支援 IPv4 和 IPv6 位址管理 LIF。

5. 自動取得 ONTAP 叢集憑證並授權該憑證，或透過瀏覽至憑證所在位置手動上傳該憑證。

   如有需要，您可以從維護控制台停用主題備用名稱 (SAN) 驗證。有關說明，請參閱"更改證書驗證標誌"。

6. 如果您新增的儲存設備後端是 MetroCluster 組態的一部分，ONTAP tools Manager 會顯示一則彈出訊息，提示您新增對等叢集。選擇 新增 並提供 MetroCluster 對等儲存設備後端的詳細資訊。

   ONTAP 系統執行切換和切換回復後，手動執行 ONTAP tools 探索。

使用 **vSphere** 用戶端使用者介面

vVols 資料儲存不支援透過 vSphere 用戶端使用者介面直接新增 SVM 使用者。

1. 登入 vSphere 用戶端。
2. 在捷徑頁面中，選擇外掛程式區段下的 **NetApp ONTAP tools**。
3. 從側邊欄選取 **Storage Backends**。
4. 新增儲存設備後端並提供伺服器 IP 位址、使用者名稱、密碼和連接埠詳細資訊。

   您可以使用基於叢集的憑證，透過 IPv4 或 IPv6 管理 LIF 新增儲存設備後端。若要直接新增 SVM 使用者，請提供基於 SVM 的憑證以及 SVM 管理 LIF。如果叢集已就職，則無法再次從該叢集就職 SVM 使用者。

5. 自動取得 ONTAP 叢集憑證並授權該憑證，或透過瀏覽至憑證所在位置手動上傳該憑證。
6. 如果新增的儲存設備後端已包含在 MetroCluster 組態中，ONTAP tools 將顯示「新增 MetroCluster 對等節點」畫面。選取「新增對等節點」以新增對等儲存設備後端。

   ONTAP 系統執行切換和切換回復後，手動執行 ONTAP tools 探索。

ONTAP tools 會在「儲存後端」頁面上列出新新增的儲存設備後端。如果憑證在 30 天或更短時間內過期，ONTAP tools 會在憑證過期日期欄中顯示警告。過期後，ONTAP tools 會將該儲存設備後端標記為未知，因為它無法連線至儲存系統。

相關資訊

"OTV 10：什麼是儲存後端全域和本機範圍"

"將叢集設定為 MetroCluster 組態"

在 ONTAP 工具中將儲存後端與 vCenter Server 執行個體建立關聯

將儲存設備後端與 vCenter 伺服器執行個體關聯，即可為所有 vCenter 伺服器執行個體啟用存取。若為 MetroCluster 組態，在關聯儲存設備後端叢集時，請確保也將其對等叢集與 vCenter 伺服器關聯。

步驟

1. 透過網頁瀏覽器啟動 ONTAP tools Manager：
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 使用您在部署期間提供的 ONTAP tools for VMware vSphere 系統管理員憑證登入。
3. 從側邊欄選取 vCenter。
4. 選擇要連接到儲存設備後端的 vCenter Server 執行個體旁邊的垂直省略號。
5. 從下拉式選單中選擇要與所選 vCenter Server 執行個體關聯的儲存設備後端。

在 ONTAP tools 中設定網路存取

預設情況下，除非您設定網路存取，否則從 ESXi 主機探索的所有 IP 位址都會自動新增至匯出原則。您可以修改匯出原則，僅允許特定 IP 位址存取。如果被排除在外的 ESXi 主機嘗試裝載作業，該作業將會失敗。

步驟

1. 登入 vSphere 用戶端。
2. 在插件部分的捷徑頁面中選擇 * NetApp ONTAP tools *。
3. 在 ONTAP tools 的左側窗格中，前往 **Settings** > **Manage Network Access** > **Edit**。

   若要新增多個 IP 位址，請以逗號、範圍、無類別域間路由 (CIDR) 或這三者的組合來分隔清單。

4. 選擇 **Save**。

在 ONTAP 工具中建立資料存放區

當您在主機叢集層級建立資料儲存區時，ONTAP tools 會將其裝載到所有目的地主機上，並且只有在您擁有所需權限時才會啟用該行動。

原生資料存放區與 **vCenter Server** 及 **ONTAP tools** 管理的資料存放區之間的互通性

從 ONTAP tools for VMware vSphere 10.4 開始，ONTAP tools 會為資料存放區建立巢狀 igroup，其中父 igroup 專屬於資料存放區，子 igroup 則對應至主機。您也可以從 ONTAP System Manager 建立扁平 igroup，並使用它們來建立 VMFS 資料存放區，而無需使用 ONTAP tools。如需詳細資訊，請參閱 "管理 SAN 發起程序和 igroup"。

儲存設備就職並執行資料儲存探索後，ONTAP tools 會將 VMFS 資料儲存中的扁平 igroup 變更為巢狀 igroup。您無法使用先前的扁平 igroup 建立新的資料儲存體。若要重複使用巢狀 igroup，請使用 ONTAP tools 介面或 REST API。

建立 **vVols** 資料存放區

從 ONTAP tools for VMware vSphere 10.3 開始，您可以在 ASA r2 系統上建立空間效率為精簡的 vVols 資料存放區。vVol。VASA Provider 在建立 vVol 資料存放區時會建立一個 Container 和所需的通訊協定端點。VASA Provider 不會為此 Container 指派任何後端 Volume。

開始之前

- 確保根 Aggregate 未對應至 SVM 。
- 確保 VASA Provider 已在所選的 vCenter 中註冊。
- 在 ASA r2 儲存系統中，SVM 應對應至 SVM 使用者的彙總。

步驟

1. 登入 vSphere 用戶端。
2. 右鍵點選主機系統、主機叢集或資料中心，然後選擇 **NetApp ONTAP tools** > 建立資料存放區。
3. 選擇 vVols 作為 **Datastore type** 。
4. 輸入*資料儲存名稱*和*協定*資訊。

   ASA r2 系統支援 iSCSI 和 FC 協定以供 vVols 使用。

5. 選擇要建立資料存放區的儲存 VM。
6. 在進階選項中：
   - 如果選擇*自訂匯出原則*，請確保在 vCenter 中對所有物件執行探索。建議不要使用此選項。
   - 您可以為 iSCSI 和 FC 傳輸協定選取*自訂啟動器群組*名稱。

   在 ASA r2 儲存系統類型 SVM 中，不會建立儲存單元（LUN/命名空間），因為資料存放區只是一個邏輯 Container。

7. 在「儲存屬性」窗格中，您可以建立新 Volume 或使用現有 Volume。但是，您不能將這兩種類型的 Volume 組合起來建立 vVols 資料存放區。

   建立新磁碟區時、您可以在資料存放區上啟用 QoS。根據預設、每個 LUN 建立要求都會建立一個磁碟區。對於 ASA r2 儲存系統上的 vVols 資料存放區、請跳過此步驟。

8. 在「摘要」窗格中檢視您的選擇，然後選取「完成」。

建立 **NFS** 資料存放區

NFS 資料儲存使用 NFS 協定將 ESXi 主機連接到共享儲存設備。它們簡單且靈活，常用於 VMware vSphere 環境中。

步驟

1. 登入 vSphere 用戶端。
2. 右鍵點選主機系統、主機叢集或資料中心，然後選擇 **NetApp ONTAP tools** > 建立資料存放區。
3. 在「資料儲存類型」欄位中選擇 NFS。
4. 在「名稱和協定」窗格中輸入資料存放區名稱、大小和協定資訊。在進階選項中選擇「資料存放區叢

集」和「Kerberos 驗證」。

只有在選擇 NFS 4.1 協定時，才能使用 Kerberos 驗證。

5. 在「儲存設備」窗格中選擇 **Platform** 和 **Storage VM**。
6. 如果在進階選項中選擇 自訂匯出原則，請在 vCenter 中對所有物件執行探索。建議不要使用此選項。

   您無法使用 SVM 的預設或根 Volume 原則建立 NFS 資料儲存。

   - 在進階選項中，只有在平台下拉式選單中選擇效能或容量時，才會顯示「非對稱」切換按鈕。
   - 當您在平台下拉式選單中選擇*任意*選項時，您可以看到 vCenter 中的所有 SVM。平台和非對稱標誌不會影響可見度。
7. 在「儲存屬性」窗格中選擇要建立 Volume 的彙總。在進階選項中，視需要選擇 **Space Reserve** 和 **Enable QoS**。
8. 查看「摘要」窗格中的選擇，然後選擇「完成」。

ONTAP tools 會建立 NFS 資料存放區，並將其裝載至所有主機。

建立 **VMFS** 資料存放區

VMFS 是一種用於儲存虛擬機器檔案的叢集檔案系統。多個 ESXi 主機可以同時存取相同的虛擬機器檔案，以實現 vMotion 和高可用性功能。

在受保護的叢集上：

- 您只能建立 VMFS 資料儲存。將 VMFS 資料儲存新增至受保護的叢集會自動保護該資料儲存。
- 您無法在包含一個或多個受保護主機叢集的資料中心建立資料存放區。
- 如果父主機叢集受到「自動故障轉移雙工原則」（統一或非統一組態）的保護，則無法在 ESXi 主機上建立資料儲存。
- 您只能在受非同步關係保護的 ESXi 主機上建立 VMFS 資料儲存。您無法在受「Automated Failover Duplex」原則保護的主機叢集中的 ESXi 主機上建立和裝載資料儲存。

開始之前

- 在 ONTAP 儲存設備端為每個協定啟用服務和 LIF。
- 將 SVM 對應到 ASA r2 儲存系統中 SVM 使用者的彙總。
- 如果您使用 NVMe/TCP 通訊協定，請設定 ESXi 主機：
  a. 檢閱 "VMware 相容性指南"

     VMware vSphere 7.0 U3 及更高版本支援 NVMe/TCP 協定。但是，建議使用 VMware vSphere 8.0 及更高版本。

  b. 檢查網路介面卡 (NIC) 廠商是否支援使用 NVMe/TCP 協定的 ESXi NIC。
  c. 根據網卡廠商規範，為 ESXi NIC 設定 NVMe/TCP。
  d. 使用 VMware vSphere 7 版本時,請依照 VMware 網站上的說明 "設定 NVMe over TCP 介面卡的 VMkernel 繫結"設定 NVMe/TCP 連接埠綁定。使用 VMware vSphere 8 版本時,請依照 "在 ESXi 上

設定基於 TCP 的 NVMe"設定 NVMe/TCP 連接埠綁定。

e. 對於 VMware vSphere 7 版本，請依照頁面上的說明 "啟用基於 RDMA 的 NVMe 或基於 TCP 的 NVMe 軟體介面卡"設定 NVMe/TCP 軟體介面卡。對於 VMware vSphere 8 版本，請依照 "新增軟體 NVMe over RDMA 或 NVMe over TCP 適配器"設定 NVMe/TCP 軟體介面卡。

f. 在 ESXi 主機上執行 "探索儲存系統和主機" 操作。如需更多資訊，請參閱 "如何在 vSphere 8.0 Update 1 和 ONTAP 9.13.1 上為 VMFS 資料存放區設定 NVMe/TCP"。

- 如果您使用的是 NVME/FC 通訊協定，請執行下列步驟來設定 ESXi 主機：

a. 如果尚未啟用，請在 ESXi 主機上啟用 NVMe over Fabrics（NVMe-oF）。

b. 完整的 SCSI 分區。

c. 確保 ESXi 主機和 ONTAP 系統在實體層和邏輯階層連接。

若要設定用於 FC 傳輸協定的 ONTAP SVM，請參閱 "為 FC 設定 SVM"。

有關在 VMware vSphere 8.0 中使用 NVMe/FC 協定的更多資訊，請參閱 "適用於 ESXi 8.x 與 ONTAP 的 NVMe-oF 主機組態"。

如需有關搭配 VMware vSphere 7.0 使用 NVMe/FC 的詳細資訊、請參閱 "ONTAP NVMe/FC 主機設定指南"和 "TR-4684"。

步驟

1. 登入 vSphere 用戶端。
2. 右鍵點選主機系統、主機叢集或資料中心，然後選擇 **NetApp ONTAP tools** > 建立資料存放區。
3. 選擇 VMFS 資料存放區類型。
4. 在「名稱和協定」窗格中輸入資料儲存名稱、大小和協定資訊。若要將新資料儲存體新增至現有 VMFS 集群，請在「進階選項」中選擇資料儲存集群。
5. 在 **Storage** 窗格中選取儲存 VM。根據需要，在「進階選項」區段中提供「自訂啟動器群組名稱」。您可以為資料儲存區選擇現有的啟動器群組，也可以建立具有自訂名稱的新啟動器群組。

   選擇 NVMe/FC 或 NVMe/TCP 協定時，系統會建立一個新的命名空間子系統，用於命名空間映射。ONTAP tools 會使用包含資料存放區名稱的自動產生名稱建立命名空間子系統。您可以在 **Storage** 窗格的進階選項中的 **custom namespace subsystem name** 欄位中重新命名命名空間子系統。

6. 從「儲存設備屬性」窗格中：

   a. 從下拉式選單選項中選取 **Aggregate**。

   對於 ASA r2 儲存系統，由於儲存設備已解耦，因此不會顯示 **Aggregate** 選項。當您選擇 ASA r2 儲存系統類型 SVM 時，儲存設備屬性頁面會顯示啟用 QoS 的選項。

   b. ONTAP tools 根據所選協定建立具有精簡空間保留的儲存設備單元（LUN/命名空間）。

   從 ONTAP 9.16.1 開始，ASA r2 儲存系統每個叢集最多支援 12 個節點。

   c. 為具有 12 個節點異質叢集 SVM 的 ASA r2 儲存系統選取*效能服務層級*。如果所選 SVM 是同質叢集或使用 SVM 使用者，則此選項無法使用。

「任意」是預設的效能服務層級 （PSL） 值。此設定使用 ONTAP 平衡放置演算法建立儲存設備單元。但是，您可以視需要選擇效能或極限選項。

d. 根據需要選擇 **Use existing volume**、**Enable QoS** 選項，並提供詳細資訊。

> 在 ASA r2 儲存類型中、磁碟區的建立或選擇不適用於儲存單元建立（LUN/Namespace）。因此、這些選項不會顯示。

> 您不能使用現有 Volume 建立採用 NVMe/FC 或 NVMe/TCP 協定的 VMFS 資料儲存體。請為 VMFS 資料儲存體建立新的 Volume。

7. 在 **Summary** 窗格中檢視資料存放區詳細資訊，然後選取 **Finish**。

> 如果在受保護的叢集上建立資料存放區，則可以看到唯讀訊息：「The datastore is being mounted on a protected Cluster.」

結果

ONTAP tools 建立 VMFS 資料儲存區並將其裝載至所有主機。