配置 **NFS**

ONTAP 9

NetApp
January 08, 2026

目錄

配置 NFS

使用 ONTAP CLI 瞭解 NFS 組態

您可以使用ONTAP Sf9 CLI命令來設定NFS用戶端對新磁碟區或qtree中新儲存虛擬機器（SVM）所含檔案的存取。

如果您想要以下列方式設定對磁碟區或qtree的存取權、請使用下列程序：

- 您想要使用ONTAP 目前由支援的任何NFS版本：NFSv3、NFSv3、NFSv3、NFSv3 4.1、NFSSv4.2或NFSv3 4.1 with pNFS。
- 您想要使用命令列介面（CLI）、而非System Manager或自動化指令碼工具。

  若要使用 System Manager 設定 NAS 多重傳輸協定存取"同時使用NFS和SMB為Windows和Linux配置NAS儲存設備"、請參閱。

- 您想要使用最佳實務做法、而非探索每個可用選項。

  如需命令語法的詳細"指令參考資料ONTAP"資訊，請參閱。

- UNIX檔案權限將用於保護新磁碟區。
- 您擁有叢集管理員權限、而非SVM管理員權限。

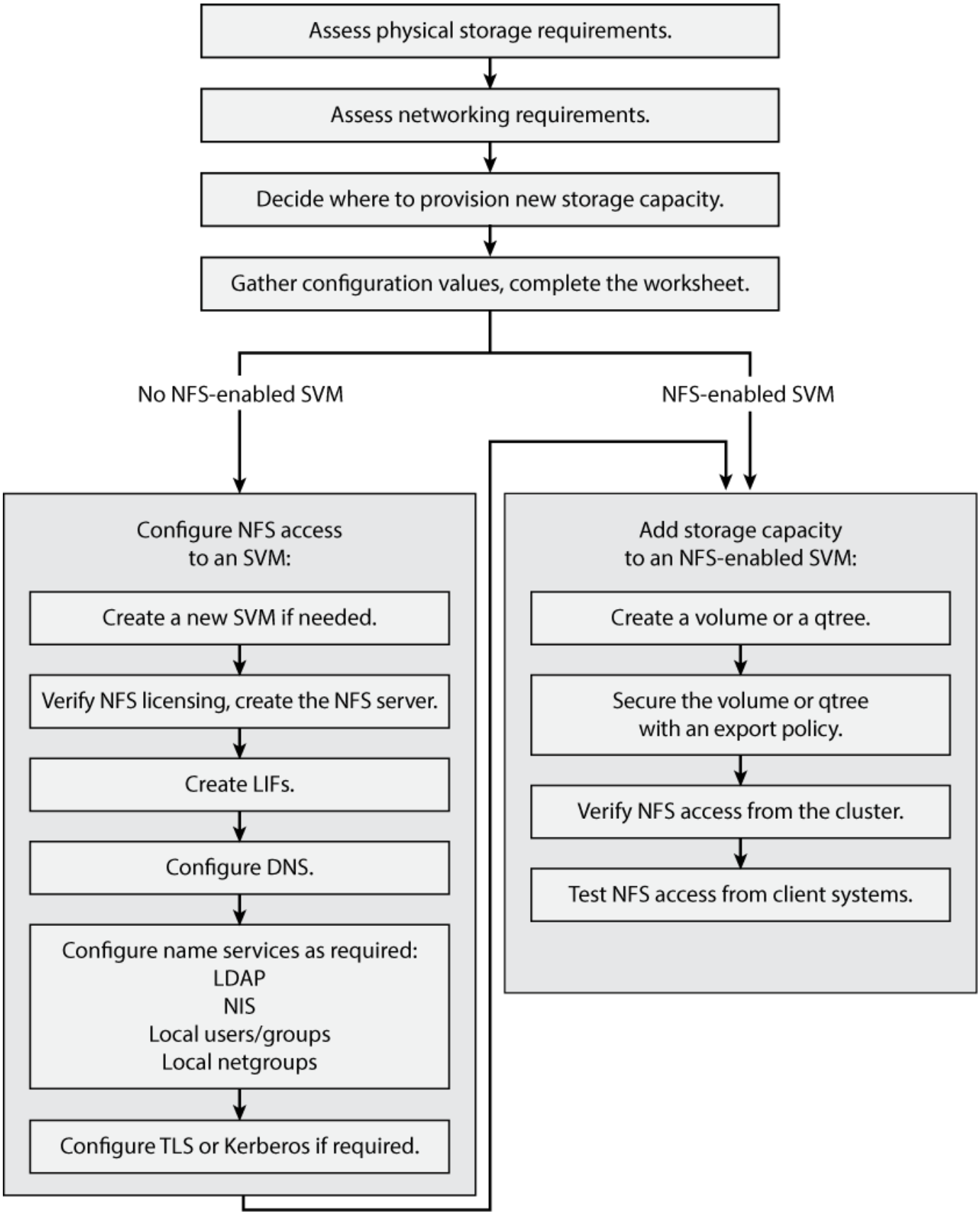
如需 ONTAP NFS 通訊協定功能範圍的詳細資訊，請參閱"了解 NFS 協定的 ONTAP 檔案訪問"。

其他方法可在**ONTAP** 不一樣的情況下執行

若要執行這些工作…	請參閱…
重新設計的System Manager（ONTAP 提供更新版本的更新版本）	"使用NFS為Linux伺服器配置NAS儲存設備"
System Manager Classic（ONTAP 適用於更新版本的更新版本	"NFS組態總覽"

了解 ONTAP NFS 設定工作流程

設定NFS需要評估實體儲存設備和網路需求、然後選擇專屬於您目標的工作流程、包括設定NFS存取新的或現有的SVM、或將Volume或qtree新增至已完全設定NFS存取的現有SVM。


Assess physical storage requirements.
Assess networking requirements.
Decide where to provision new storage capacity.
Gather configuration values, complete the worksheet.
No NFS-enabled SVM
NFS-enabled SVM
Configure NFS access to an SVM:
Create a new SVM if needed.
Verify NFS licensing, create the NFS server.
Create LIFs.
Configure DNS.
Configure name services as required:
LDAP
NIS
Local users/groups
Local netgroups
Configure TLS or Kerberos if required.
Add storage capacity to an NFS-enabled SVM:
Create a volume or a qtree.
Secure the volume or qtree with an export policy.
Verify NFS access from the cluster.
Test NFS access from client systems.

準備

評估 ONTAP NFS 實體儲存需求

在為用戶端配置NFS儲存設備之前、您必須確保現有的集合體中有足夠的空間可容納新磁碟區。如果沒有、您可以將磁碟新增至現有的Aggregate、或建立所需類型的新Aggregate。

步驟

1. 顯示現有Aggregate中的可用空間：

   ```
   storage aggregate show
   ```

   如果集合體有足夠的空間、請在工作表中記錄其名稱。

   ```
   cluster::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
   --------- -------- --------- ----- ------- ------ ------ -----------
   aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                             normal
   aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                             normal
   6 entries were displayed.
   ```

2. 如果沒有具有足夠空間的集合體、請使用將磁碟新增至現有的集合體 `storage aggregate add-disks` 或使用建立新的 Aggregate `storage aggregate create` 命令。

相關資訊

- "新增磁碟至本機層（Aggregate）"
- "存儲聚合添加磁碟"
- "儲存聚合創建"

評估 ONTAP NFS 網路配置需求

將NFS儲存設備提供給用戶端之前、您必須先確認網路設定正確、以符合NFS資源配置需求。

開始之前

必須設定下列叢集網路物件：

- 實體與邏輯連接埠
- 廣播網域
- 子網路（如有需要）
- IPspaces（視需要而定、除了預設IPspace）
- 容錯移轉群組（視需要、以及每個廣播網域的預設容錯移轉群組）
- 外部防火牆

步驟

1. 顯示可用的實體和虛擬連接埠：

   `network port show`

   - 如果可能、您應該使用資料網路速度最高的連接埠。
   - 資料網路中的所有元件必須具有相同的MTU設定、才能獲得最佳效能。
   - 如"指令參考資料ONTAP"需詳細 `network port show`資訊，請參閱。

2. 如果您打算使用子網路名稱來配置LIF的IP位址和網路遮罩值、請確認該子網路存在且有足夠的可用位址：+

   `network subnet show`

   如"指令參考資料ONTAP"需詳細 `network subnet show`資訊，請參閱。

   子網路包含屬於同一第3層子網路的IP位址集區。子網路是使用建立的 `network subnet create` 命令。

   如"指令參考資料ONTAP"需詳細 `network subnet create`資訊，請參閱。

3. 顯示可用的IPspaces：

   `network ipspace show`

   您可以使用預設IPspace或自訂IPspace。

   如"指令參考資料ONTAP"需詳細 `network ipspace show`資訊，請參閱。

4. 如果您要使用IPv6位址、請確認叢集上已啟用IPv6：

   `network options ipv6 show`

   如有需要、您可以使用啟用 IPv6 `network options ipv6 modify` 命令。

   深入瞭解 `network options ipv6 show`及 `network options ipv6 modify` "指令參考資料ONTAP"。

瞭解 ONTAP NFS 儲存容量配置

在建立新的NFS Volume或qtree之前、您必須先決定要將其放入新的或現有的SVM、以及SVM所需的組態量。此決定決定決定您的工作流程。

選擇

- 如果您想要在新的SVM上配置磁碟區或qtree、或是在已啟用NFS但尚未設定的現有SVM上配置、請完成「設定NFS存取SVM」和「將NFS儲存設備新增至啟用NFS的SVM」中的步驟。

  設定SVM的NFS存取

  將NFS儲存設備新增至啟用NFS的SVM

  如果符合下列任一項條件、您可以選擇建立新的SVM：

  - 您是第一次在叢集上啟用NFS。
  - 您在不想啟用NFS支援的叢集中有現有的SVM。
  - 您在叢集中有一個或多個NFS型SVM、而您想要在隔離的命名空間中使用另一個NFS伺服器（多租戶案例）。 您也應該選擇此選項、以便在已啟用NFS但尚未設定的現有SVM上配置儲存設備。如果您為SAN存取建立SVM、或是在建立SVM時未啟用任何傳輸協定、則可能會發生這種情況。

  在SVM上啟用NFS之後、請繼續配置磁碟區或qtree。

- 如果您想要在已完全設定為NFS存取的現有SVM上配置磁碟區或qtree、請完成「將NFS儲存設備新增至已啟用NFS的SVM」中的步驟。

  將NFS儲存設備新增至啟用NFS的SVM

ONTAP NFS 組態工作表

NFS組態工作表可讓您收集必要資訊、以便為用戶端設定NFS存取。

您應該根據您對儲存資源配置的決策、完成工作表的一或兩個區段：

如果您要設定SVM的NFS存取、請完成這兩個部分。

- 設定SVM的NFS存取
- 將儲存容量新增至啟用NFS的SVM

如果您要將儲存容量新增至啟用NFS的SVM、則只應完成下列步驟：

- 將儲存容量新增至啟用NFS的SVM

設定**SVM**的**NFS**存取

*用於建立SVM*的參數

您可以將這些值提供給 `vserver create` 命令、如果您要建立新的 SVM 。

欄位	說明	您的價值

`-vserver`	您為新SVM提供的名稱、可以是完整網域名稱（FQDN）、也可以遵循另一種在叢集內強制執行唯一SVM名稱的慣例。	
`-aggregate`	叢集中有足夠空間可容納新NFS儲存容量的集合體名稱。	
`-rootvolume`	您為SVM根磁碟區提供的唯一名稱。	
`-rootvolume-security-style`	使用SVM的UNIX安全樣式。	`unix`
`-language`	使用此工作流程中的預設語言設定。	`C.UTF-8`
`ipspace`	IPspaces是（儲存虛擬機器（SVM））所在的不同IP位址空間。	

建立**NFS**伺服器的參數

您可以將這些值提供給 `vserver nfs create` 命令：建立新的 NFS 伺服器並指定支援的 NFS 版本。

如果您要啟用NFSv4或更新版本、則應使用LDAP來改善安全性。

欄位	說明	您的價值
`-v3、 -v4.0、 -v4.1、 -v4.1 -pnfs`	視需要啟用NFS版本。 ONTAP 9.8 及更新版本也支援 V4.2 `v4.1` 已啟用。	
`-v4-id-domain`	ID對應網域名稱。	
`-v4-numeric-ids`	支援數字擁有者ID（啟用或停用）。	

*用於建立LIF*的參數

建立生命時，您可以使用命令來提供這些值 `network interface create`。如"指令參考資料ONTAP"需詳細`network interface create`資訊，請參閱。

如果您使用Kerberos、則應在多個LIF上啟用Kerberos。

欄位	說明	您的價值

`-lif`	您為新LIF提供的名稱。	
`-role`	在此工作流程中使用資料LIF角色。	`data`
`-data-protocol`	在此工作流程中僅使用NFS傳輸協定。	`nfs`
`-home-node`	LIF 在返回時返回的節點 `network interface revert` 命令會在LIF上執行。 如"指令參考資料ONTAP"需詳細 `network interface revert`資訊，請參閱。	
`-home-port`	LIF 在返回時傳回的連接埠或介面群組 `network interface revert` 命令會在LIF上執行。	
`-address`	叢集上的IPV4或IPv6位址、用於新LIF的資料存取。	
`-netmask`	LIF的網路遮罩和閘道。	
`-subnet`	IP位址集區。改用 `-address` 和 `-netmask` 自動指派位址和網路遮罩。	
`-firewall-policy`	在此工作流程中使用預設的資料防火牆原則。	`data`

- DNS主機名稱解析參數*

您可以將這些值提供給 `vserver services name-service dns create` 設定 DNS 時的命令。

欄位	說明	您的價值
`-domains`	最多五個DNS網域名稱。	
`-name-servers`	每個DNS名稱伺服器最多三個IP位址。	

名稱服務資訊

建立本機使用者的參數

如果您是使用建立本機使用者、請提供這些值 `vserver services name-service unix-user create`

命令。如果您是透過從統一資源識別元（URI）載入含有UNIX使用者的檔案來設定本機使用者、則不需要手動指定這些值。

	使用者名稱 (-user)	使用者ID (-id)	群組ID (-primary-gid)	全名 (-full-name)
範例	johnm	123.	100	John Miller
1.				
2.				
3.				
…				
n				

建立本機群組的參數

如果您是使用建立本機群組、請提供這些值 `vserver services name-service unix-group create` 命令。如果您是從URI載入含有UNIX群組的檔案來設定本機群組、則不需要手動指定這些值。

	群組名稱 (-name)	群組ID (-id)
範例	工程	100
1.		
2.		
3.		
…		
n		

- NIS的參數*

您可以將這些值提供給 `vserver services name-service nis-domain create` 命令。

這 `-nis-servers`字段替換 `-servers`字段。您可以使用 `-nis-servers`欄位指定 NIS 伺服器的主機名稱或 IP 位址。

欄位	說明	您的價值

`-domain`	SVM將用於名稱查詢的NIS網域。	
`-active`	作用中的NIS網域伺服器。	`true` 或 `false`
`-nis-servers`	網域配置使用的 NIS 伺服器的 IP 位址和主機名稱的逗號分隔清單。	

- LDAP*的參數

您可以將這些值提供給 `vserver services name-service ldap client create` 命令。

您也需要自我簽署的根 CA 憑證 `.pem` 檔案：

欄位	說明	您的價值
`-vserver`	您要為其建立LDAP用戶端組態的SVM名稱。	
`-client-config`	您指派給新LDAP用戶端組態的名稱。	
`-ldap-servers`	以逗號分隔的 LDAP 伺服器 IP 位址和主機名稱清單。	
`-query-timeout`	使用預設值 `3` 此工作流程的秒數。	`3`
`-min-bind-level`	最小連結驗證層級。預設值為 `anonymous`。必須設定為 `sasl` 如果已設定簽署和密封。	
`-preferred-ad-servers`	在以逗號分隔的清單中、依IP位址列出一或多個慣用的Active Directory伺服器。	
`-ad-domain`	Active Directory網域。	
`-schema`	要使用的架構範本。您可以使用預設或自訂架構。	
`-port`	使用預設的 LDAP 伺服器連接埠 `389` 適用於此工作流程。	`389`
`-bind-dn`	「連結」使用者辨別名稱。	

欄位	說明	您的價值
-base-dn	基礎辨別名稱。預設值為 "" （根目錄）。	
-base-scope	使用預設的基礎搜尋範圍 subnet 適用於此工作流程。	subnet
-session-security	啟用LDAP簽署或簽署及密封。預設值為 none。	
-use-start-tls	啟用LDAP over TLS。預設值為 false。	

- Kerberos驗證的參數*

您可以將這些值提供給 vserver nfs kerberos realm create 命令。部分值會因您使用Microsoft Active Directory做為金鑰發佈中心（Kdc）伺服器、MIT或其他UNIX Kdc伺服器而有所不同。

欄位	說明	您的價值
-vserver	與Kdc通訊的SVM。	
-realm	Kerberos領域。	
-clock-skew	用戶端與伺服器之間允許的時鐘偏移。	
-kdc-ip	Kdc IP位址。	
-kdc-port	Kdc連接埠號碼。	
-adserver-name	僅限Microsoft Kdc：AD伺服器名稱。	
-adserver-ip	僅限Microsoft Kdc：AD伺服器IP位址。	
-adminserver-ip	僅UNIX Kdc：管理伺服器IP位址。	
-adminserver-port	僅UNIX Kdc：管理伺服器連接埠號碼。	
-passwordserver-ip	僅UNIX Kdc：密碼伺服器IP位址。	
-passwordserver-port	僅UNIX Kdc：密碼伺服器連接埠。	

-kdc-vendor	Kdc廠商：	｛Microsoft
Other｝	-comment	任何想要的意見。

您可以將這些值提供給 vserver nfs kerberos interface enable 命令。

欄位	說明	您的價值
-vserver	您要為其建立Kerberos組態的SVM名稱。	
-lif	您要啟用Kerberos的資料LIF。您可以在多個LIF上啟用Kerberos。	
-spn	服務原則名稱（SPN-）	
-permitted-enc-types	Kerberos over NFS 允許的加密類型； aes-256 建議使用、視用戶端功能而定。	
-admin-username	用於直接從Kdc擷取SPN機密金鑰的Kdc系統管理員認證。需要密碼	
-keytab-uri	如果您沒有Kdc系統管理員認證、則會從包含SPN-Key的Kdc取得Keytab檔案。	
-ou	當您使用領域為Microsoft Kdc啟用Kerberos時、會在組織單位（OU）下建立Microsoft Active Directory伺服器帳戶。	

將儲存容量新增至啟用**NFS**的**SVM**

用於建立匯出原則與規則的參數

您可以將這些值提供給 vserver export-policy create 命令。

欄位	說明	您的價值
-vserver	將裝載新磁碟區的SVM名稱。	
-policyname	您為新的匯出原則提供的名稱。	

您可以為每個規則提供這些值 vserver export-policy rule create 命令。

欄位	說明	您的價值
`-clientmatch`	用戶端符合規格。	
`-ruleindex`	匯出規則在規則清單中的位置。	
`-protocol`	在此工作流程中使用NFS。	`nfs`
`-rorule`	唯讀存取的驗證方法。	
`-rwrule`	讀寫存取的驗證方法。	
`-superuser`	超級使用者存取的驗證方法。	
`-anon`	匿名使用者對應的使用者ID。	

您必須為每個匯出原則建立一或多個規則。

`-ruleindex`	**`-clientmatch`**	**`-rorule`**	**`-rwrule`**	**`-superuser`**	**`-anon`**
範例	0.00.0.0/0、@rootaccess_netgroup	任何	KRB5	系統	65534
1.					
2.					
3.					
…					
n					

建立**Volume**的參數

您可以將這些值提供給 `volume create` 如果您要建立的是 Volume 而非 qtree 、則為命令。

欄位	說明	您的價值
`-vserver`	將裝載新磁碟區的新SVM或現有SVM名稱。	
`-volume`	您為新磁碟區提供的唯一描述性名稱。	

`-aggregate`	叢集中有足夠空間可容納新NFS磁碟區的集合體名稱。	
`-size`	您為新磁碟區大小所提供的整數。	
`-user`	設定為磁碟區根目錄擁有者的使用者名稱或ID。	
`-group`	設定為磁碟區根目錄擁有者的群組名稱或ID。	
`--security-style`	使用UNIX安全樣式來執行此工作流程。	`unix`
`-junction-path`	要掛載新磁碟區的根目錄（/）下的位置。	
`-export-policy`	如果您打算使用現有的匯出原則、則可以在建立Volume時輸入其名稱。	

用於建立**qtree**的參數

您可以將這些值提供給 `volume qtree create` 如果您要建立 qtree 而非 Volume 、請執行命令。

欄位	說明	您的價值
`-vserver`	包含qtree之磁碟區所在的SVM名稱。	
`-volume`	將包含新qtree的磁碟區名稱。	
`-qtree`	您為新qtree提供的唯一描述性名稱、64個字元或更少。	
`-qtree-path`	格式中的 qtree path 引數 */vol/volume_name/qtree_name\>* 可以指定、而非將 Volume 和 qtree 指定為個別的引數。	
`-unix-permissions`	選用：qtree的UNIX權限。	
`-export-policy`	如果您打算使用現有的匯出原則、可以在建立qtree時輸入其名稱。	

相關資訊

- "指令參考資料ONTAP"

設定SVM的NFS存取

建立 ONTAP SVM 以進行 NFS 資料訪問

如果叢集中沒有至少一個SVM來提供NFS用戶端的資料存取、則必須建立一個SVM。

開始之前

- 從 ONTAP 9.13.1 開始，您可以設定儲存 VM 的最大容量。您也可以在 SVM 接近臨界值容量層級時設定警示。如需更多資訊、請參閱 管理 SVM 容量。

步驟

1. 建立SVM：

   `vserver create -vserver vserver_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style unix -language C.UTF-8 -ipspace ipspace_name`

   - 使用的 UNIX 設定 `-rootvolume-security-style` 選項。
   - 使用預設的 C.UTF-8 `-language` 選項。
   - 。 `ipspace` 設定為選用項目。

2. 驗證新建立的SVM的組態和狀態：

   `vserver show -vserver vserver_name`

   。 `Allowed Protocols` 欄位必須包含 NFS 。您可以稍後再編輯此清單。

   。 `Vserver Operational State` 欄位必須顯示 `running` 州/省。如果顯示 `initializing` 狀態、表示有些中繼作業（例如建立根磁碟區）失敗、您必須刪除 SVM 並重新建立它。

範例

下列命令會在IPspace ipspaceA中建立SVM以供資料存取：

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

下列命令顯示 SVM 是以 1 GB 的根磁碟區所建立、而且是自動啟動且位於中 `running` 州/省。根磁碟區具有預設的匯出原則、不含任何規則、因此根磁碟區在建立時不會匯出。

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                                Vserver Type: data
                             Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                                Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                        Vserver Admin State: running
                  Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                               IPspace Name: ipspaceA
```

從 ONTAP 9.13.1 開始，您可以設定調適性 QoS 原則群組範本，將處理量下限套用至 SVM 中的磁碟區。您只能在建立 SVM 之後套用此原則。若要深入瞭解此程序，請參閱設定調適性原則群組範本。

驗證 ONTAP SVM 上 NFS 協定的啟用情況

在SVM上設定及使用NFS之前、您必須先確認已啟用該傳輸協定。

關於這項工作

這通常是在 SVM 設定期間完成、但如果您在設定期間未啟用傳輸協定、您可以稍後使用加以啟用 `vserver add-protocols` 命令。

一旦建立LIF、您就無法從其新增或移除通訊協定。

您也可以使用停用 SVM 上的通訊協定 `vserver remove-protocols` 命令。

步驟

1. 檢查SVM目前啟用和停用的傳輸協定：

```
vserver show -vserver vserver_name -protocols
```

您也可以使用 `vserver show-protocols` 用於檢視叢集中所有 SVM 上目前啟用的通訊協定的命令。

2. 如有必要、請啟用或停用傳輸協定：
   - 若要啟用 NFS 傳輸協定：
     `vserver add-protocols -vserver vserver_name -protocols nfs`
   - 若要停用通訊協定：
     `vserver remove-protocols -vserver vserver_name -protocols protocol_name [,protocol_name,…]`
3. 確認已啟用和停用的傳輸協定已正確更新：

```
vserver show -vserver vserver_name -protocols
```

範例

下列命令顯示名為VS1的SVM上目前啟用和停用（允許和不允許）的傳輸協定：

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    ------------------------
vs1.example.com   nfs                       cifs, fcp, iscsi, ndmp
```

下列命令可新增以允許透過 NFS 存取 `nfs` 到名為 VS1 的 SVM 上已啟用的通訊協定清單：

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols nfs
```

在 **ONTAP SVM** 上開啟 **NFS** 用戶端訪問

SVM根磁碟區的預設匯出原則必須包含允許所有用戶端透過NFS開啟存取的規則。如果沒有這樣的規則、所有NFS用戶端都會被拒絕存取SVM及其磁碟區。

關於這項工作

建立新的SVM時、會自動為SVM的根Volume建立預設匯出原則（稱為預設）。您必須先為預設匯出原則建立一或多個規則、用戶端才能存取SVM上的資料。

您應該確認預設匯出原則中的所有NFS用戶端都已開啟存取權、之後再建立個別磁碟區或qtree的自訂匯出原則、以限制個別磁碟區的存取權。

步驟

1. 如果您使用現有的SVM、請檢查預設的根Volume匯出原則：

```
vserver export-policy rule show
```

命令輸出應類似下列內容：

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                    Vserver: vs1.example.com
                                Policy Name: default
                                 Rule Index: 1
                            Access Protocol:  nfs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                             RO Access Rule: any
                             RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                   Superuser Security Types: any
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

如果存在允許開啟存取的規則、則此工作即告完成。如果沒有、請繼續下一步。

2. 建立SVM根磁碟區的匯出規則：

   `vserver export-policy rule create -vserver` *`vserver_name`* `-policyname default -ruleindex 1 -protocol nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`

   如果 SVM 只包含受 Kerberos 保護的磁碟區、您可以設定匯出規則選項 `-rorule`、`-rwrule`和 `-superuser` 將根磁碟區移至 `krb5` 或 `krb5i`。例如：

   `-rorule krb5i -rwrule krb5i -superuser krb5i`

3. 使用驗證規則建立 `vserver export-policy rule show` 命令。

結果

任何NFS用戶端現在都可以存取在SVM上建立的任何Volume或qtree。

建立 **ONTAP NFS** 伺服器

在驗證 NFS 是否已在叢集上取得授權之後、您可以使用 `vserver nfs create` 命令在 SVM 上建立 NFS 伺服器、並指定其支援的 NFS 版本。

關於這項工作

SVM可設定為支援一或多個NFS版本。如果您支援NFSv4或更新版本：

- NFSv4使用者ID對應網域名稱在NFSv4伺服器和目標用戶端上必須相同。

  只要NFSv4伺服器和用戶端使用相同名稱、就不一定需要與LDAP或NIS網域名稱相同。

- 目標用戶端必須支援NFSv4數值ID設定。
- 基於安全考量、您應該在NFSv4部署中使用LDAP作為名稱服務。

開始之前

SVM必須已設定為允許NFS傳輸協定。

步驟

1. 驗證叢集上的NFS是否已獲得授權：

   ```
   system license show -package nfs
   ```

   如果沒有、請聯絡您的銷售代表。

2. 建立NFS伺服器：

   ```
   vserver nfs create -vserver vserver_name -v3 {enabled|disabled} -v4.0
   {enabled|disabled} -v4-id-domain nfsv4_id_domain -v4-numeric-ids
   {enabled|disabled} -v4.1 {enabled|disabled} -v4.1-pnfs {enabled|disabled}
   ```

   您可以選擇啟用任何NFS版本組合。如果您想要支援 pNFS 、則必須同時啟用兩者 `-v4.1` 和 `-v4.1-pnfs` 選項：

   如果您啟用v4或更新版本、也應該確定下列選項設定正確：

   - `-v4-id-domain`

     此選用參數指定NFSv4傳輸協定所定義之使用者和群組名稱字串形式的網域部分。根據預設、ONTAP如果已設定NIS網域、則會使用該NIS網域；如果未設定、則會使用DNS網域。您必須提供與目標用戶端所使用的網域名稱相符的值。

   - `-v4-numeric-ids`

     此選用參數可指定是否啟用NFSv4擁有者屬性中的數字字串識別碼支援。預設設定為已啟用、但您應該確認目標用戶端是否支援此設定。

   您可以稍後使用啟用其他 NFS 功能 `vserver nfs modify` 命令。

3. 確認NFS正在執行：

   ```
   vserver nfs status -vserver vserver_name
   ```

4. 確認NFS已設定為所需：

   ```
   vserver nfs show -vserver vserver_name
   ```

範例

下列命令會在名為VS1的SVM上建立NFS伺服器、並啟用NFSv3和NFSv4.0：

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id
-domain my_domain.com
```

下列命令可驗證名為VS1的新NFS伺服器的狀態和組態值：

```
vs1::> vserver nfs status -vserver vs1
The NFS server is running on Vserver "vs1".

vs1::> vserver nfs show -vserver vs1

                              Vserver: vs1
                    General NFS Access: true
                                NFS v3: enabled
                              NFS v4.0: enabled
                         UDP Protocol: enabled
                         TCP Protocol: enabled
                  Default Windows User: -
                   NFSv4.0 ACL Support: disabled
      NFSv4.0 Read Delegation Support: disabled
     NFSv4.0 Write Delegation Support: disabled
              NFSv4 ID Mapping Domain: my_domain.com
...
```

建立 ONTAP NFS 生命

LIF是與實體或邏輯連接埠相關聯的IP位址。如果元件發生故障、LIF可能會容錯移轉至不同的實體連接埠、或移轉至不同的實體連接埠、進而繼續與網路通訊。

開始之前

- 基礎實體或邏輯網路連接埠必須設定為管理 `up`狀態。如"指令參考資料ONTAP"需詳細 `up`資訊，請參閱。
- 如果您打算使用子網路名稱來配置LIF的IP位址和網路遮罩值、則該子網路必須已經存在。

  子網路包含屬於同一第3層子網路的IP位址集區。它們是使用建立的 `network subnet create` 命令。

  如"指令參考資料ONTAP"需詳細 `network subnet create`資訊，請參閱。

- 指定LIF處理之流量類型的機制已變更。對於僅適用於更新版本的版本、LIF會使用角色來指定其處理的流量類型。ONTAP從ONTAP Sf6開始、I生命 就會使用服務原則來指定處理的流量類型。

關於這項工作

- 您可以在同一個網路連接埠上同時建立IPV4和IPv6 LIF。
- 如果您使用Kerberos驗證、請在多個LIF上啟用Kerberos。
- 如果叢集中有大量的生命、您可以使用來驗證叢集上支援的 LIF 容量 `network interface capacity show` 命令和 LIF 容量、可透過使用在每個節點上支援 `network interface capacity details show` 命令（進階權限層級）。

  深入瞭解 `network interface capacity show`及 `network interface capacity details show` "指令參考資料ONTAP"。

- 從ONTAP NetApp 9.7開始、如果相同子網路中的SVM已存在其他LIF、您就不需要指定LIF的主連接埠。在相同的廣播網域中、系統會自動在指定的主節點上選擇隨機連接埠、如同在同一個子網路中設定的其他

LIF。ONTAP

從ONTAP 支援FFC-NVMe的支援功能到支援的功能表9.4開始。如果您要建立FC-NVMe LIF、應該注意下列事項：

- NVMe傳輸協定必須受到建立LIF的FC介面卡支援。
- FC-NVMe是資料生命中唯一的資料傳輸協定。
- 必須為每個支援SAN的儲存虛擬機器（SVM）設定一個LIF處理管理流量。
- NVMe LIF和命名空間必須裝載在同一個節點上。
- 每個SVM只能設定一個處理資料流量的NVMe LIF

步驟

1. 建立LIF：

   ```
   network interface create -vserver vserver_name -lif lif_name -role data -data
   -protocol nfs -home-node node_name -home-port port_name {-address IP_address
   -netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
   -revert {true|false}
   ```

   如"指令參考資料ONTAP"需詳細 `network interface create`資訊，請參閱。

選項	說明
《》第9.5版及更早版本* ONTAP	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`
版本**9.6**及更新版本 ONTAP	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`

- 。 `-role` 使用服務原則（從 ONTAP 9.6 開始）建立 LIF 時不需要參數。
- 。 `-data-protocol` 必須在建立 LIF 時指定參數、而且必須在稍後修改、才能銷毀及重新建立資料 LIF 。

  。 `-data-protocol` 使用服務原則建立 LIF 時不需要參數（從 ONTAP 9.6 開始）。

- `-home-node` 是 LIF 在返回時返回的節點 `network interface revert` 命令會在LIF上執行。

  您也可以指定 LIF 是否應該使用自動還原至主節點和主連接埠 `-auto-revert` 選項。

  如"指令參考資料ONTAP"需詳細 `network interface revert`資訊，請參閱。

- `-home-port` 是 LIF 在時傳回的實體或邏輯連接埠 `network interface revert` 命令會在LIF上執行。
- 您可以使用指定 IP 位址 `-address` 和 `-netmask` 或是您可以使用從子網路進行分配 `-subnet_name` 選項。
- 使用子網路提供IP位址和網路遮罩時、如果子網路是使用閘道定義、則使用該子網路建立LIF時、會自動將通往該閘道的預設路由新增至SVM。
- 如果您手動指派IP位址（不使用子網路）、則在不同IP子網路上有用戶端或網域控制器時、可能需要設定通往閘道的預設路由。在中深入瞭解 `network route create`並建立 SVM 內的靜態路由"指令參考資料 ONTAP"。
- 適用於 `-firewall-policy` 選項、請使用相同的預設值 `data` 成為 LIF 角色。

  如果需要、您可以稍後建立並新增自訂防火牆原則。

  > ⓘ 從ONTAP S振 分9.10.1開始、防火牆原則已過時、並完全由LIF服務原則取代。如需詳細資訊、請參閱 "設定lifs的防火牆原則"。

- `-auto-revert` 可讓您指定資料 LIF 是否在啟動、管理資料庫狀態變更或建立網路連線等情況下自動還原至其主節點。預設設定為 `false`**但您可以將其設定為** `false` 視環境中的網路管理原則而定。

  a. 使用確認 LIF 已成功建立 `network interface show` 命令。

  b. 確認已設定的IP位址可連線：

若要驗證...	使用...
IPV4位址	`network ping`
IPv6位址	`network ping6`

  c. 如果您使用Kerberos、請重複步驟1到3以建立其他生命週期。

  Kerberos必須在每個生命區上分別啟用。

範例

下列命令會建立 LIF 並使用指定 IP 位址和網路遮罩值 `-address` 和 `-netmask` 參數：

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol nfs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

下列命令會建立LIF、並從指定的子網路（名為client1_sub）指派IP位址和網路遮罩值：

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol nfs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

下列命令顯示叢集1中的所有LIF。資料生命週期1和資料傳輸3均設定為使用IPv4位址、而資料傳輸4則設定為使用IPv6位址：

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

下列命令顯示如何建立指派給的 NAS 資料 LIF `default-data-files` 服務原則：

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

相關資訊

- "網路ping"

- "網路介面"

為 ONTAP NFS SVM 主機名稱解析啟用 DNS

您可以使用 `vserver services name-service dns` 命令在 SVM 上啟用 DNS 、並將其設定為使用 DNS 進行主機名稱解析。使用外部DNS伺服器解析主機名稱。

開始之前

站台範圍的DNS伺服器必須可供主機名稱查詢。

您應該設定多個DNS伺服器、以避免單點故障。。 `vserver services name-service dns create` 如果只輸入一個 DNS 伺服器名稱、命令會發出警告。

關於這項工作

深入瞭解 "在 SVM 上設定動態 DNS"。

步驟

1. 在SVM上啟用DNS：

   `vserver services name-service dns create -vserver` *`vserver_name`* `-domains` *`domain_name`* `-name-servers` *`ip_addresses`* `-state enabled`

   下列命令可啟用SVM VS1上的外部DNS伺服器：

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   ⓘ 。 `vserver services name-service dns create` 如果 ONTAP 無法連絡名稱伺服器、命令會執行自動組態驗證、並回報錯誤訊息。

2. 使用顯示 DNS 網域組態 `vserver services name-service dns show` 命令。

   下列命令會顯示叢集中所有SVM的DNS組態：

   ```
   vserver services name-service dns show
                                                Name
   Vserver           State     Domains             Servers
   ----------------- --------- ------------------- -------------
   cluster1          enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   vs1.example.com   enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   ```

   下列命令會顯示SVM VS1的詳細DNS組態資訊：

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
          Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. 使用驗證名稱伺服器的狀態 `vserver services name-service dns check` 命令。

```
vserver services name-service dns check -vserver vs1.example.com

Vserver            Name Server     Status       Status Details
---------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

設定名稱服務

了解 **ONTAP NFS** 名稱服務

根據儲存系統的組態、ONTAP 支援功能需要能夠查詢主機、使用者、群組或網路群組資訊、才能正確存取用戶端。您必須設定名稱服務、才能讓ONTAP 支援功能支援使用本機或外部名稱服務來取得此資訊。

您應該使用名稱服務（例如NIS或LDAP）、以便在用戶端驗證期間進行名稱查詢。最好盡可能使用LDAP來提高安全性、尤其是在部署NFSv4或更新版本時。如果外部名稱伺服器無法使用、您也應該設定本機使用者和群組。

名稱服務資訊必須在所有來源上保持同步。

配置 **ONTAP NFS** 名稱服務切換表

您必須正確設定名稱服務交換器表、才能讓ONTAP 支援功能支援使用者參考本機或外部名稱服務、以擷取主機、使用者、群組、網路群組或名稱對應資訊。

開始之前

您必須決定要用於主機、使用者、群組、netgroup或名稱對應的名稱服務、以符合您的環境需求。

如果您打算使用netGroups、則必須依照RFC 5952中的指定、縮短及壓縮netGroups中指定的所有IPv6位址。

關於這項工作

請勿包含未使用的資訊來源。例如、如果您的環境中未使用 NIS 、請勿指定 `-sources nis` 選項。

步驟

1. 將必要的項目新增至名稱服務交換器表：

   `vserver services name-service ns-switch create -vserver vserver_name -database database_name -sources source_names`

2. 驗證名稱服務交換器表格是否包含所需順序的預期項目：

   `vserver services name-service ns-switch show -vserver vserver_name`

   如果您想要進行任何修正、您必須使用 `vserver services name-service ns-switch modify` 或 `vserver services name-service ns-switch delete` 命令。

範例

下列範例會在名稱服務交換器表中建立新項目、讓SVM VS1使用本機netgroup檔案和外部NIS伺服器、以該順序查詢netgroup資訊：

```
cluster::> vserver services name-service ns-switch create -vserver vs1
-database netgroup -sources files,nis
```

完成後

- 您必須設定您為SVM指定的名稱服務、才能提供資料存取。
- 如果您刪除SVM的任何名稱服務、也必須將其從名稱服務交換器表格中移除。

  如果您無法從名稱服務交換器表格中刪除名稱服務、用戶端對儲存系統的存取可能無法如預期般運作。

設定本機**UNIX**使用者和群組

了解 **ONTAP NFS SVM** 的本機 **UNIX** 使用者和群組

您可以使用SVM上的本機UNIX使用者和群組進行驗證和名稱對應。您可以手動建立UNIX使用者和群組、也可以從統一資源識別元（URI）載入包含UNIX使用者或群組的檔案。

叢集中的本機UNIX使用者群組和群組成員、預設上限為32、768。叢集管理員可以修改此限制。

在 **ONTAP NFS SVM** 上建立本機 **UNIX** 用戶

您可以使用 `vserver services name-service unix-user create` 建立本機 UNIX 使用者的命令。本機UNIX使用者是您在SVM上建立的UNIX使用者、是UNIX名稱服務選項、用於處理名稱對應。

步驟

1. 建立本機UNIX使用者：

   `vserver services name-service unix-user create -vserver vserver_name -user user_name -id integer -primary-gid integer -full-name full_name`

   `-user user_name` 指定使用者名稱。使用者名稱長度必須少於64個字元。

`-id` *integer* 指定您指派的使用者 ID 。

`-primary-gid` *integer* 指定主要群組 ID 。這會將使用者新增至主要群組。建立使用者之後、您可以手動將使用者新增至任何想要的其他群組。

範例

下列命令會在名為VS1的SVM上建立名為johnm（全名「John Miller」）的本機UNIX使用者。使用者的 ID 為 123 、主要群組 ID 為 100 。

```
node::> vserver services name-service unix-user create -vserver vs1 -user
johnm -id 123
-primary-gid 100 -full-name "John Miller"
```

在 **ONTAP NFS SVM** 上載入本機 **UNIX** 使用者列表

除了在 SVM 中手動建立個別的本機 UNIX 使用者之外、您也可以從統一的資源識別元（ URI ）將本機 UNIX 使用者清單載入 SVM 、以簡化工作。(`vserver services name-service unix-user load-from-uri`) 。

步驟

1. 建立包含您要載入之本機UNIX使用者清單的檔案。

   檔案必須包含 UNIX 中的使用者資訊 `/etc/passwd` 格式：

   `user_name: password: user_ID: group_ID: full_name`

   命令會捨棄的值 *`password`* 欄位和之後欄位的值 *`full_name`* 欄位 (*`home_directory`* 和 *`shell`*) 。

   支援的檔案大小上限為2.5 MB。

2. 確認清單中沒有任何重複資訊。

   如果清單包含重複的項目、則載入清單時會失敗並顯示錯誤訊息。

3. 將檔案複製到伺服器。

   儲存系統必須透過HTTP、HTTPS、FTP或FTPS連線至伺服器。

4. 判斷檔案的URI是什麼。

   URI是您提供給儲存系統的位址、用以指出檔案所在位置。

5. 從URI將包含本機UNIX使用者清單的檔案載入SVM：

   `vserver services name-service unix-user load-from-uri -vserver` *`vserver_name`* `-uri {ftp|http|ftps|https}://`*`uri`* `-overwrite {true|false}`

   `-overwrite {true false}` 指定是否覆寫項目。預設值為 `false`。

範例

下列命令會從 URI 載入本機 UNIX 使用者清單 `ftp://ftp.example.com/passwd` 進入名為 VS1 的 SVM 。SVM上的現有使用者不會被URI的資訊覆寫。

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

在 **ONTAP NFS SVM** 上建立本機 **UNIX** 群組

您可以使用 `vserver services name-service unix-group create` 建立 SVM 本機 UNIX 群組的命令。本機UNIX群組適用於本機UNIX使用者。

步驟

1. 建立本機UNIX群組：

   `vserver services name-service unix-group create -vserver` *`vserver_name`* `-name` *`group_name`* `-id` *`integer`*

   `-name` *`group_name`* 指定群組名稱。群組名稱長度必須少於64個字元。

   `-id` *`integer`* 指定您指派的群組 ID 。

範例

下列命令會在名為VS1的SVM上建立名為eng的本機群組。群組的ID為101。

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name
eng -id 101
```

將使用者新增至 **ONTAP NFS SVM** 上的本機 **UNIX** 群組

您可以使用 `vserver services name-service unix-group adduser` 命令、將使用者新增至 SVM 本機的輔助 UNIX 群組。

步驟

1. 新增使用者至本機UNIX群組：

`vserver services name-service unix-group adduser -vserver` *`vserver_name`* `-name` *`group_name`* `-username` *`user_name`*

`-name` *`group_name`* 指定要新增使用者的 UNIX 群組名稱、以及使用者的主要群組。

範例

下列命令會將名為max的使用者新增至名為VS1的SVM上名為eng的本機UNIX群組：

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name
eng
-username max
```

從 **ONTAP NFS SVM** 上的 **URI** 載入本機 **UNIX** 群組

除了手動建立個別的本機 UNIX 群組之外、您也可以使用、從統一的資源識別元（ URI ）將本機 UNIX 群組清單載入 SVM `vserver services name-service unix-group load-from-uri` 命令。

步驟

1. 建立包含您要載入之本機UNIX群組清單的檔案。

   檔案必須包含 UNIX 中的群組資訊 `/etc/group` 格式：

   `group_name: password: group_ID: comma_separated_list_of_users`

   命令會捨棄的值 *`password`* 欄位。

   支援的檔案大小上限為 1 MB 。

   群組檔案中每一行的長度上限為32、768個字元。

2. 確認清單中沒有任何重複資訊。

   清單不得包含重複的項目、否則載入清單將會失敗。如果 SVM 中已有項目、您必須設定 `-overwrite` 參數至 `true` 以新檔案覆寫所有現有項目、或確保新檔案不包含任何重複現有項目的項目。

3. 將檔案複製到伺服器。

   儲存系統必須透過HTTP、HTTPS、FTP或FTPS連線至伺服器。

4. 判斷檔案的URI是什麼。

   URI是您提供給儲存系統的位址、用以指出檔案所在位置。

5. 從URI將包含本機UNIX群組清單的檔案載入SVM：

   `vserver services name-service unix-group load-from-uri -vserver` *`vserver_name`* `-uri {ftp|http|ftps|https}://`*`uri`* `-overwrite {true|false}`

   `-overwrite true false}` 指定是否覆寫項目。預設值為 `false`。如果您將此參數指定為 `true`， ONTAP 會將指定 SVM 的整個現有本機 UNIX 群組資料庫，取代為您所載入檔案的項目。

範例

下列命令會從 URI 載入本機 UNIX 群組清單 `ftp://ftp.example.com/group` 進入名為 VS1 的 SVM 。SVM上的現有群組不會被URI的資訊覆寫。

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1
-uri ftp://ftp.example.com/group -overwrite false
```

使用**netGroups**

了解 **ONTAP NFS SVM** 上的網路群組

您可以使用netGroups進行使用者驗證、並在匯出原則規則中比對用戶端。您可以從外部名稱伺服器（ LDAP 或 NIS ）提供網路群組的存取權、也可以使用將網路群組從統一的資源識別碼（ URI ）載入 SVM `vserver services name-service netgroup load` 命令。

開始之前

在使用netGroups之前、您必須確保符合下列條件：

- 不論來源（NIS、LDAP或本機檔案）為何、網路群組中的所有主機都必須同時擁有轉送（A）和反向（PTr）DNS記錄、才能提供一致的轉送和反向DNS查詢。

  此外、如果用戶端的IP位址有多筆PTr記錄、則所有這些主機名稱都必須是netgroup的成員、並具有對應的A記錄。

- 不論來源（NIS、LDAP或本機檔案）為何、netGroups中所有主機的名稱都必須正確拼寫、並使用正確的大小寫。在netGroups中使用的主機名稱若不一致、可能會導致非預期的行為、例如匯出檢查失敗。
- 在netGroups中指定的所有IPv6位址都必須依照RFC 5952中的指定來縮短和壓縮。

  例如、2011：hu9：0：0：0：0：3：1必須縮短為2011：hu9：3：1。

關於這項工作

使用netGroups時、您可以執行下列作業：

- 您可以使用 `vserver export-policy netgroup check-membership` 用於確定客戶端 IP 是否是某個 netgroup 的成員的命令。
- 您可以使用 `vserver services name-service getxxbyyy netgrp` 用於檢查用戶端是否為 netgroup 的一部分的命令。

  執行查詢的基礎服務是根據設定的名稱服務交換器順序來選取。

從 **ONTAP NFS SVM** 上的 **URI** 載入網路組

您可以在匯出原則規則中使用符合用戶端的方法之一、就是使用netGroups中列出的主機。您可以將網路群組從統一的資源識別碼（ URI ）載入 SVM 、以取代使用儲存在外部名稱伺服器中的網路群組 (`vserver services name-service netgroup load`）。

開始之前

Netgroup檔案在載入SVM之前、必須符合下列要求：

- 檔案必須使用與NIS相同的適當netgroup文字檔格式。

  此功能可在載入netgroup文字檔格式之前檢查其內容。ONTAP如果檔案包含錯誤、則不會載入、並會顯示訊息、指出您必須在檔案中執行的修正。更正錯誤後、您可以將netgroup檔案重新載入指定的SVM。

- netgroup檔案中主機名稱中的任何字母字元都應為小寫。
- 支援的檔案大小上限為 5 MB 。
- 巢狀網路群組支援的最大層級為1000。
- 在netgroup檔案中定義主機名稱時、只能使用主要DNS主機名稱。

  為了避免匯出存取問題、不應使用DNS CNAME/或循環配置資源記錄來定義主機名稱。

- netgroup檔案中三個群組的使用者和網域部分應保持空白、因為ONTAP 無法支援它們。

  僅支援主機/IP部分。

關於這項工作

支援各主機的netgroup搜尋本機netgroup檔案。ONTAP載入netgroup檔案後ONTAP 、Syname會自動建立netgroup .byhost對應、以啟用逐主機的netgroup搜尋。這可大幅加速本機netgroup搜尋、以處理匯出原則規則來評估用戶端存取。

步驟

1. 從URI將網路群組載入SVM：

   `vserver services name-service netgroup load -vserver` *`vserver_name`* `-source {ftp|http|ftps|https}://`*`uri`*

   載入netgroup檔案並建置netgroup。byhost對應可能需要數分鐘的時間。

   如果要更新netgroup、您可以編輯該檔案、然後將更新的netgroup檔案載入SVM。

範例

下列命令會從 HTTP URL 將 netgroup 定義載入名為 VS1 的 SVM `http://intranet/downloads/corp-netgroup`：

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

驗證 **ONTAP NFS SVM** 網路組定義

將網路群組載入 SVM 後、您可以使用 `vserver services name-service netgroup status` 用於驗證 netgroup 定義狀態的命令。這可讓您判斷支援SVM的所有節點上的netgroup定義是否一致。

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 驗證netgroup定義的狀態：

```
vserver services name-service netgroup status
```

您可以在更詳細的檢視畫面中顯示其他資訊。

3. 返回管理權限層級：

```
set -privilege admin
```

範例

設定權限層級後、下列命令會顯示所有SVM的netgroup狀態：

```
vs1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when
         directed to do so by technical support.
Do you wish to continue? (y or n): y

vs1::*> vserver services name-service netgroup status
Virtual
Server    Node            Load Time           Hash Value
--------- --------------- -------------------
--------------------------------
vs1
          node1           9/20/2006 16:04:53
e6cb38ec1396a280c0d2b77e3a84eda2
          node2           9/20/2006 16:06:26
e6cb38ec1396a280c0d2b77e3a84eda2
          node3           9/20/2006 16:08:08
e6cb38ec1396a280c0d2b77e3a84eda2
          node4           9/20/2006 16:11:33
e6cb38ec1396a280c0d2b77e3a84eda2
```

為 **ONTAP NFS SVM** 建立 **NIS** 域配置

如果您的環境中使用網路資訊服務（ NIS ）來提供名稱服務、則必須使用為 SVM 建立 NIS 網域組態 `vserver services name-service nis-domain create` 命令。

開始之前

在SVM上設定NIS網域之前、所有已設定的NIS伺服器都必須可供使用且可連線。

如果您打算使用NIS進行目錄搜尋、則NIS伺服器中的對應每個項目不得超過1,024個字元。請勿指定不符合此限

制的NIS伺服器。否則、用戶端存取相依於NIS項目可能會失敗。

關於這項工作

如果您的 NIS 資料庫包含 `netgroup.byhost` MAP 、 ONTAP 可以使用它來加快搜尋速度。。`netgroup.byhost` 和 `netgroup` 目錄中的地圖必須隨時保持同步、以避免用戶端存取問題。從 ONTAP 9.7 開始、 NIS `netgroup.byhost` 您可以使用快取項目 `vserver services name-service nis-domain netgroup-database` 命令。

不支援使用 NIS 進行主機名稱解析。

步驟

1. 建立NIS網域組態：

   ```
   vserver services name-service nis-domain create -vserver vs1 -domain
   <domain_name> -nis-servers <IP_addresses>
   ```

   您最多可以指定10部NIS伺服器。

   > 這 `-nis-servers`字段替換 `-servers`字段。您可以使用 `-nis-servers`欄位指定 NIS 伺服器的主機名稱或 IP 位址。

2. 確認網域已建立：

   ```
   vserver services name-service nis-domain show
   ```

範例

下列命令會針對在 SVM 上以 IP 位址的 NIS 伺服器 `192.0.2.180`命名的 `vs1` NIS 網域建立 NIS 網域組態 `nisdomain`：

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -nis-servers 192.0.2.180
```

使用LDAP

了解如何在 ONTAP NFS SVM 上使用 LDAP 名稱服務

如果您的環境中使用LDAP來提供名稱服務、您必須與LDAP管理員合作、以判斷需求和適當的儲存系統組態、然後將SVM啟用為LDAP用戶端。

從ONTAP 功能支援的版本為：從功能支援的版本為：LDAP通道繫結、依預設會同時支援Active Directory和名稱服務LDAP連線。僅當啟用Start-TLS或LDAPS並將工作階段安全性設定為簽署或密封時、才能嘗試透過LDAP連線進行通道繫結。ONTAP若要停用或重新啟用與名稱伺服器的 LDAP 通道繫結、請使用 `-try-channel-binding` 參數 `ldap client modify` 命令。

如需詳細資訊、請參閱 "2020 LDAP通道繫結和LDAP簽署要求、適用於Windows"。

- 在設定LDAP ONTAP 以供使用之前、您應確認您的站台部署符合LDAP伺服器和用戶端組態的最佳實務做法。尤其必須符合下列條件：

- LDAP伺服器的網域名稱必須符合LDAP用戶端上的項目。
- LDAP伺服器支援的LDAP使用者密碼雜湊類型必須包含ONTAP 下列項目：
  - 加密（所有類型）和SHA-1（SHa、SSHA）。
  - 從ONTAP 《Sf9.8》、《SHA-2雜湊》（SHA-256、SSH-384、SHA-512、SSHA-256、 也支援SSHA-384和SSHA-512）。
- 如果LDAP伺服器需要工作階段安全性措施、您必須在LDAP用戶端中進行設定。

  下列工作階段安全性選項可供使用：

  - LDAP簽署（提供資料完整性檢查）及LDAP簽署與密封（提供資料完整性檢查與加密）
  - 啟動TLS
  - LDAPS（LDAP over TLS或SSL）
- 若要啟用已簽署和密封的LDAP查詢、必須設定下列服務：
  - LDAP伺服器必須支援GSPI（Kerberos）SASL機制。
  - LDAP伺服器必須在DNS伺服器上設定DNS A/AAAA記錄和PTr記錄。
  - Kerberos伺服器必須在DNS伺服器上存在SRV.記錄。
- 若要啟用Start TLS或LDAPS、應考慮下列事項。
  - 使用Start TLS而非LDAPS是NetApp最佳實務做法。
  - 如果使用LDAPS、則LDAP伺服器必須在ONTAP 支援TLS或支援SSL的情況下、於支援更新版本的支援更新版本中啟用。不支援SSL。ONTAP
  - 必須已在網域中設定憑證伺服器。
- 若要啟用LDAP參照追蹤（ONTAP 在更新版本的版本中）、必須滿足下列條件：
  - 這兩個網域都應設定下列其中一個信任關係：
    - 雙向
    - 單向、主要信任參照網域
    - 父-子
  - DNS必須設定為解析所有參照的伺服器名稱。
  - 網域密碼在-bind-as CIFS伺服器設定為true時、應相同進行驗證。

    LDAP參照追蹤不支援下列組態。

    - 所有ONTAP 版本：
      - 管理SVM上的LDAP用戶端
    - 適用於更新版本的支援功能（9.9.1及更新版本均支援）ONTAP ：
      - LDAP 簽署與密封（ `-session-security` 選項）
      - 加密 TLS 連線（ `-use-start-tls` 選項）
      - 透過 LDAPS 連接埠 636 （ `-use-ldaps-for-ad-ldap` 選項）

- 在SVM上設定LDAP用戶端時、您必須輸入LDAP架構。

  在大多數情況下、預設ONTAP 的架構之一將是適當的。不過、如果您環境中的LDAP架構與這些架構不同、則必須先建立新的LDAP用戶端架構ONTAP 以供使用、才能建立LDAP用戶端。請洽詢您的LDAP管理員、瞭解您環境的需求。

- 不支援使用LDAP進行主機名稱解析。

以取得更多資訊

- "NetApp技術報告4835：如何在ONTAP 功能方面設定LDAP"
- "在 ONTAP SMB SVM 上安裝自我簽署的根 CA 憑證"

為 **ONTAP NFS SVM** 建立新的 **LDAP** 用戶端模式

如果您環境中的LDAP架構不同於ONTAP 支援功能的預設值、您必須先建立新的LDAP用戶端架構ONTAP 以供使用、才能建立LDAP用戶端組態。

關於這項工作

大多數LDAP伺服器都可以使用ONTAP 由下列功能提供的預設架構：

- ms-AD-BIS（大多數Windows 2012及更新版本AD伺服器的偏好架構）
- AD-IDMU（Windows 2008、Windows 2012及更新版本的AD伺服器）
- AD-SFU（Windows 2003和舊版AD伺服器）
- RFC-2307（UNIX LDAP伺服器）

如果您需要使用非預設LDAP架構、則必須先建立該架構、再建立LDAP用戶端組態。在建立新架構之前、請先諮詢您的LDAP管理員。

無法修改由功能提供的預設LDAP架構ONTAP 。若要建立新架構、請建立複本、然後據此修改複本。

步驟

1. 顯示現有的LDAP用戶端架構範本、以識別您要複製的範本：

   ```
   vserver services name-service ldap client schema show
   ```

2. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

3. 複製現有的LDAP用戶端架構：

   ```
   vserver services name-service ldap client schema copy -vserver vserver_name
   -schema existing_schema_name -new-schema-name new_schema_name
   ```

4. 修改新的架構並針對您的環境自訂：

   ```
   vserver services name-service ldap client schema modify
   ```

5. 返回管理權限層級：

```
set -privilege admin
```

為 **ONTAP NFS** 存取建立 **LDAP** 用戶端配置

如果您想要 ONTAP 存取環境中的外部 LDAP 或 Active Directory 服務、則必須先在儲存系統上設定 LDAP 用戶端。

開始之前

Active Directory 網域解析清單中前三部伺服器之一必須為正常運作並提供資料。否則、此工作將會失敗。

有多部伺服器、其中有兩部以上的伺服器在任何時間點停機。

步驟

1. 請洽詢您的 LDAP 管理員、以決定的適當組態值 `vserver services name-service ldap client create` 命令：

   a. 指定與LDAP伺服器的網域型或位址型連線。

      ◦ `-ad-domain` 和 `-servers` 選項是互斥的。

      - 使用 `-ad-domain` 在 Active Directory 網域中啟用 LDAP 伺服器探索的選項。
        - 您可以使用 `-restrict-discovery-to-site` 將 LDAP 伺服器探索限制在指定網域的 CIFS 預設網站的選項。如果使用此選項、您也需要使用指定 CIFS 預設站台 `-default-site`。
      - 您可以使用 `-preferred-ad-servers` 選項可依以逗號分隔的清單中的 IP 位址來指定一或多個偏好的 Active Directory 伺服器。建立用戶端之後、您可以使用修改此清單 `vserver services name-service ldap client modify` 命令。
      - 使用 `-servers` 選項可依以逗號分隔的清單中的 IP 位址來指定一或多個 LDAP 伺服器（Active Directory 或 UNIX）。

        已棄用。 `-ldap-servers`字段替換 `-servers`場地。此欄位可取得 LDAP 伺服器的主機名稱或 IP 位址。

   b. 指定預設或自訂LDAP架構。

      大多數LDAP伺服器都可以使用ONTAP 由功能介紹的預設唯讀架構。除非有其他需求、否則最好使用這些預設架構。如果是、您可以複製預設架構（它們是唯讀的）、然後修改複本、藉此建立自己的架構。

      預設架構：

      - MS-AD-BIS

        根據RFC-2307bis、這是大多數標準Windows 2012及更新版本LDAP部署的慣用LDAP架構。

      - `AD-IDMU`

        根據Active Directory Identity Management for UNIX、此架構適用於大多數Windows 2008

、Windows 2012及更新的AD伺服器。

- `AD-SFU`

  此架構以Active Directory Services for UNIX為基礎、適用於大多數Windows 2003和舊版AD伺服器。

- `RFC-2307`

  根據RFC-2307（*an*方法使用*LDAP*做為網路資訊服務）、此架構適用於大多數UNIX AD伺服器。

c. 選取「連結值」。

- `-min-bind-level {anonymous|simple|sasl}` 指定最小繫結驗證層級。

  預設值為 **anonymous**。

- `-bind-dn` *`LDAP_DN`* 指定綁定用戶。

  對於Active Directory伺服器、您必須在帳戶（網域\使用者）或主體（user@domain.com）表單中指定使用者。否則、您必須以辨別名稱（CN=user,DC=domain,DC=com）格式指定使用者。

- `-bind-password` *`password`* 指定綁定密碼。

d. 如有需要、請選取工作階段安全選項。

如果LDAP伺服器需要、您可以啟用LDAP簽署和密封、或透過TLS啟用LDAP。

- `--session-security {none|sign|seal}`

  您可以啟用簽署 (`sign`、資料完整性）、簽署及密封 (`seal`或兩者皆非 `none`、無簽署或密封）。預設值為 `none`。

  您也應該設定 `-min-bind-level {sasl}` 除非您想讓繫結驗證回復為 **anonymous** 或 **simple** 如果簽署和密封綁定失敗。

- `-use-start-tls {true|false}`

  如果設為 **true** LDAP 伺服器也支援此功能、 LDAP 用戶端會使用加密的 TLS 連線連線至伺服器。預設值為 **false**。您必須安裝LDAP伺服器的自我簽署根CA憑證、才能使用此選項。

> 如果儲存 VM 已將 SMB 伺服器新增至網域、而 LDAP 伺服器是 SMB 伺服器主網域的其中一個網域控制器、則您可以修改 `-session-security-for-ad-ldap` 選項：使用 `vserver cifs security modify` 命令。

e. 選取連接埠、查詢和基礎值。

建議使用預設值、但您必須向LDAP管理員確認這些值是否適合您的環境。

- `-port` *`port`* 指定 LDAP 伺服器連接埠。

  預設值為 `389`。

如果您打算使用Start TLS來保護LDAP連線、則必須使用預設連接埠389。啟動TLS會以純文字連線的形式透過LDAP預設連接埠389開始、然後將該連線升級為TLS。如果您變更連接埠、啟動TLS就會失敗。

- `-query-timeout` *integer* 指定查詢逾時（以秒為單位）。

  允許的範圍為1到10秒。預設值為 3 秒。

- `-base-dn` *LDAP_DN* 指定基礎 DN 。

  如有需要、可輸入多個值（例如啟用LDAP參照追蹤）。預設值為 `""` （根目錄）。

- `-base-scope {base|onelevel|subtree}` 指定基本搜尋範圍。

  預設值為 `subtree`。

- `-referral-enabled {true|false}` 指定是否啟用 LDAP 參照追蹤。

  從ONTAP 功能介紹9.5開始、ONTAP 如果主要LDAP伺服器傳回LDAP參照回應、表示所需記錄存在於參照的LDAP伺服器上、即可讓功能介紹LDAP用戶端將查詢要求參照到其他LDAP伺服器。預設值為 **`false`**。

若要搜尋所參照LDAP伺服器中的記錄、必須將所參照記錄的基礎DN新增至基礎DN、做為LDAP用戶端組態的一部分。

2. 在儲存 VM 上建立 LDAP 用戶端組態：

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```

> 建立 LDAP 用戶端組態時、您必須提供儲存 VM 名稱。

3. 確認LDAP用戶端組態已成功建立：

```
vserver services name-service ldap client show -client-config
client_config_name
```

範例

下列命令會建立名為 ldap1 的新 LDAP 用戶端組態、讓儲存 VM VS1 與 Active Directory 伺服器 for LDAP 搭配使用：

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

下列命令會建立名為 ldap1 的新 LDAP 用戶端組態、讓儲存 VM VS1 與需要簽署和密封的 Active Directory 伺服器搭配使用、而 LDAP 伺服器探索則僅限於指定網域的特定站台：

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

下列命令會建立名為 ldap1 的新 LDAP 用戶端組態、讓儲存 VM VS1 與需要 LDAP 參照追蹤的 Active Directory 伺服器搭配使用：

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

下列命令會指定基礎 DN 、以修改儲存 VM VS1 的 LDAP 用戶端組態 ldap1 ：

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

下列命令可啟用參照追蹤功能、修改儲存 VM VS1 的 LDAP 用戶端組態 ldap1 ：

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com"  -referral-enabled true
```

將 **LDAP** 用戶端配置與 **ONTAP NFS SVM** 關聯

若要在 SVM 上啟用 LDAP 、您必須使用 `vserver services name-service ldap create` 用於將 LDAP 用戶端組態與 SVM 建立關聯的命令。

開始之前

- LDAP網域必須已存在於網路中、且SVM所在的叢集必須能夠存取。
- SVM上必須存在LDAP用戶端組態。

步驟

1. 在 SVM 上啟用 LDAP ：

   ```
   vserver services name-service ldap create -vserver vserver_name -client-config
   client_config_name
   ```

   這 `vserver services name-service ldap create`如果ONTAP無法聯繫名稱伺服器，則該命令將執行自動設定驗證並報告錯誤訊息。

   下列命令可在「VS1」SVM上啟用LDAP、並將其設定為使用「LDAP1」LDAP用戶端組態：

   ```
   cluster1::> vserver services name-service ldap create -vserver vs1
   -client-config ldap1 -client-enabled true
   ```

2. 使用vserver services name-service LDAP檢查命令來驗證名稱伺服器的狀態。

   下列命令可驗證SVM VS1上的LDAP伺服器。

   ```
   cluster1::> vserver services name-service ldap check -vserver vs1

   | Vserver: vs1                                                    |
   | Client Configuration Name: c1                                   |
   | LDAP Status: up                                                 |
   | LDAP Status Details: Successfully connected to LDAP server
   "10.11.12.13".                                                    |
   ```

驗證 **ONTAP NFS SVM** 的 **LDAP** 來源

您必須驗證SVM的名稱服務交換器表中是否正確列出名稱服務的LDAP來源。

步驟

1. 顯示目前名稱服務交換器表格內容：

   ```
   vserver services name-service ns-switch show -vserver svm_name
   ```

   下列命令顯示SVM My_SVM的結果：

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
                                Source
Vserver         Database        Order
--------------- ------------    ---------
My_SVM          hosts           files,
                                dns
My_SVM          group           files,ldap
My_SVM          passwd          files,ldap
My_SVM          netgroup        files
My_SVM          namemap         files
5 entries were displayed.
```

namemap 指定要搜尋名稱對應資訊的來源、以及搜尋順序。在純UNIX環境中、不需要輸入此項目。只有在同時使用UNIX和Windows的混合環境中才需要名稱對應。

2. 更新 ns-switch 視情況輸入：

如果您想要更新下列項目的**ns**交換器項目...	輸入命令...
使用者資訊	`vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files`
群組資訊	`vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files`
網路群組資訊	`vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files`

使用**Kerberos**搭配**NFS**以獲得強大的安全性

了解如何將 **Kerberos** 與 **ONTAP NFS** 結合使用以進行安全性驗證

如果您的環境使用Kerberos進行強式驗證、您必須與Kerberos管理員合作、以判斷需求和適當的儲存系統組態、然後將SVM啟用為Kerberos用戶端。

您的環境應符合下列準則：

- 您的站台部署應遵循Kerberos伺服器和用戶端組態的最佳實務做法、才能設定Kerberos ONTAP 以供執行效能。
- 如果可能、請使用NFSv4或更新版本（如果需要Kerberos驗證）。

  NFSv3可與Kerberos搭配使用。不過、Kerberos的完整安全效益只能在ONTAP NFSv4或更新版本的部署中實現。

- 若要提升備援伺服器存取、應在叢集中多個節點上使用相同的SPN-啟用 多個資料LIF上的Kerberos。
- 在SVM上啟用Kerberos時、必須根據NFS用戶端組態、在Volume或qtree的匯出規則中指定下列其中一種安全性方法。
  - `krb5` （ Kerberos v5 通訊協定）
  - `krb5i` （使用 checksum 進行完整性檢查的 Kerberos v5 通訊協定）
  - `krb5p` （ Kerberos v5 通訊協定與隱私權服務）

除了Kerberos伺服器和用戶端之外、還必須設定下列外部服務ONTAP 以支援Kerberos：

- 目錄服務

  您應該在環境中使用安全目錄服務、例如Active Directory或OpenLDAP、這類服務設定為使用LDAP over SSL/TLS。請勿使用NIS、因為NIS的要求會以純文字傳送、因此不安全。

- NTP

  您必須有執行NTP的工作時間伺服器。這是防止Kerberos驗證因時間偏移而失敗的必要步驟。

- 網域名稱解析（DNS）

  每個UNIX用戶端和每個SVM LIF都必須在Kdc的正向和反向對應區域下註冊適當的服務記錄（SRF）。所有參與者都必須透過DNS正確解析。

驗證 **ONTAP SVM** 上 **NFS Kerberos** 配置的 **UNIX** 權限

Kerberos需要為SVM根磁碟區及本機使用者和群組設定特定的UNIX權限。

步驟

1. 顯示SVM根磁碟區的相關權限：

   `volume show -volume` *`root_vol_name`*`-fields user,group,unix-permissions`

   SVM的根Volume必須具有下列組態：

名稱...	正在設定...
UID	root或ID 0
Gid	root或ID 0
UNIX權限	755

   如果未顯示這些值、請使用 `volume modify` 命令進行更新。

2. 顯示本機UNIX使用者：

   `vserver services name-service unix-user show -vserver` *`vserver_name`*

SVM必須設定下列UNIX使用者：

使用者名稱	使用者**ID**	主要群組**ID**	留言
NFS	500	0%	GSS初始化階段所需的項目。 NFS用戶端使用者的第一個使用者是使用者。 如果NFS用戶端使用者的SPN-UNIX名稱對應存在、則不需要NFS使用者。
根	0%	0%	安裝所需。

如果未顯示這些值、您可以使用 `vserver services name-service unix-user modify` 命令進行更新。

3. 顯示本機UNIX群組：

   `vserver services name-service unix-group show -vserver` *`vserver`* `_name`

   SVM必須設定下列UNIX群組：

群組名稱	群組**ID**
精靈	1.
根	0%

如果未顯示這些值、您可以使用 `vserver services name-service unix-group modify` 命令進行更新。

在 **ONTAP SVM** 上建立 **NFS Kerberos** 領域配置

如果您想ONTAP 要讓靜態存取環境中的外部Kerberos伺服器、必須先設定SVM使用現有的Kerberos領域。若要這麼做、您需要收集 Kerberos KDC 伺服器的組態值、然後使用 `vserver nfs kerberos realm create` 在 SVM 上建立 Kerberos 領域組態的命令。

開始之前

叢集管理員應已在儲存系統、用戶端和Kdc伺服器上設定NTP、以避免驗證問題。用戶端與伺服器之間的時間差異（時鐘偏移）是驗證失敗的常見原因。

步驟

1. 請洽詢您的 Kerberos 系統管理員、以決定提供的適當組態值 `vserver nfs kerberos realm create` 命令。

2. 在SVM上建立Kerberos領域組態：

   ```
   vserver nfs kerberos realm create -vserver vserver_name -realm realm_name
   {AD_KDC_server_values |AD_KDC_server_values} -comment "text"
   ```

3. 確認已成功建立Kerberos領域組態：

   ```
   vserver nfs kerberos realm show
   ```

範例

下列命令會為SVM VS1建立NFS Kerberos領域組態、該組態使用Microsoft Active Directory伺服器做為Kdc伺服器。Kerberos領域是AUTH.EXAMPLE.COM。Active Directory伺服器的名稱為ad-1、其IP位址為10.10.8.14。允許的時鐘偏移為300秒（預設值）。Kdc伺服器的IP位址為10.10.8.14、其連接埠號碼為88（預設）。「Microsoft Kerberos組態」是註解。

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

下列命令會為使用MIT Kdc的SVM VS1建立NFS Kerberos領域組態。Kerberos領域是SECURITY.EXAMPLE.COM。允許的時鐘偏移為300秒。Kdc伺服器的IP位址為10.10.9.1、其連接埠號碼為88。其他的Kdc廠商則表示UNIX廠商。管理伺服器的IP位址為10.10.9.1、其連接埠號碼為749（預設）。密碼伺服器的IP位址為10.10.9.1、其連接埠號碼為464（預設）。「UNIX Kerberos組態」是註解。

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

為 **ONTAP SVM** 配置 **NFS Kerberos** 允許的加密類型

根據預設ONTAP 、支援下列NFS Kerberos加密類型：DE、3DES、AES-128和AES-256。您可以使用設定每個 SVM 的允許加密類型、以符合特定環境的安全需求 `vserver nfs modify` 命令 `-permitted-enc-types` 參數。

關於這項工作

為了達到最大的用戶端相容性、ONTAP 根據預設、支援弱的Des和強式AES加密。例如、如果您想要提高安全性、而且環境支援、可以使用此程序來停用Des和3DES、並要求用戶端僅使用AES加密。

您應該使用目前最強大的加密功能。對於支援支援、也就是AES-256。ONTAP您應該向您的kdc管理員確認您的環境支援此加密層級。

- 在SVM上完全啟用或停用AES（AES-128和AES-256）會造成中斷、因為它會破壞原始的Des主體/索引標籤檔案、因此需要在SVM的所有生命體上停用Kerberos組態。

  在進行此變更之前、您應該確認NFS用戶端不依賴SVM上的AES加密。

- 啟用或停用Des或3DES不需要變更lifs上的Kerberos組態。

步驟

1. 啟用或停用所需的允許加密類型：

如果您要啟用或停用...	請遵循下列步驟...

DE或3DES	a. 設定 SVM 的 NFS Kerberos 允許加密類型：
	`vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types`
	
	以逗號分隔多種加密類型。
	
	b. 確認變更成功：
	`vserver nfs show -vserver vserver_name -fields permitted-enc-types`

AES-128 或 AES-256	a. 識別啟用哪個 SVM 和 LIF Kerberos ：
	`vserver nfs kerberos interface show`
	
	b. 在要修改其 NFS Kerberos 允許加密類型的 SVM 上、停用所有生命負載上的 Kerberos ：
	`vserver nfs kerberos interface disable -lif lif_name`
	
	c. 設定 SVM 的 NFS Kerberos 允許加密類型：
	`vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types`
	
	以逗號分隔多種加密類型。
	
	d. 確認變更成功：
	`vserver nfs show -vserver vserver_name -fields permitted-enc-types`
	
	e. 在 SVM 上的所有生命上重新啟用 Kerberos ：
	`vserver nfs kerberos interface enable -lif lif_name -spn service_principal_name`
	
	f. 驗證是否已在所有生命中啓用 Kerberos ：
	`vserver nfs kerberos interface show`

在 **ONTAP LIF** 上啟用 **NFS Kerberos**

您可以使用 `vserver nfs kerberos interface enable` 在資料 LIF 上啟用 Kerberos 的命令。這可讓SVM使用Kerberos安全服務來執行NFS。

關於這項工作

如果您使用Active Directory Kdc、則所使用的任何SPN前15個字元在領域或網域內的SVM之間必須是唯一的。

步驟

1. 建立NFS Kerberos組態：

   ```
   vserver nfs kerberos interface enable -vserver vserver_name -lif
   logical_interface -spn service_principal_name
   ```

   支援Kerberos介面時、需要使用來自Kdc的SPN秘密金鑰。ONTAP

   對於Microsoft KDC、會聯絡到KDC、並在CLI發出使用者名稱和密碼提示以取得秘密金鑰。如果您需要在 Kerberos 領域的不同 OU 中建立 SPN 、您可以指定選用的 `-ou` 參數。

   對於非Microsoft KDC、可使用下列兩種方法之一取得秘密金鑰：

如果您...	您也必須在命令中加入下列參數...
請讓Kdc系統管理員認證資料直接從Kdc擷取金鑰	`-admin-username` *kdc_admin_username*
不具有kdc系統管理員認證、但從包含金鑰的kdc取得Keytab檔案	`-keytab-uri` ｛FTP

2. 確認LIF上已啟用Kerberos：

   ```
   vserver nfs kerberos-config show
   ```

3. 重複步驟1和2、在多個LIF上啟用Kerberos。

範例

下列命令會在邏輯介面v03至D1上為名為VS1的SVM建立及驗證NFS Kerberos組態、並在OU lab2ou中使用SPn NFS/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM：

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
        Logical
Vserver Interface Address       Kerberos  SPN
------- --------- -------       --------- --------------------------------
vs0     ves01-a1
                  10.10.10.30   disabled  -
vs2     ves01-d1
                  10.10.10.40   enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

將儲存容量新增至啟用NFS的SVM

了解如何為啟用 ONTAP NFS 的 SVM 新增儲存容量

若要將儲存容量新增至啟用NFS的SVM、您必須建立一個Volume或qtree以提供儲存容器、並建立或修改該容器的匯出原則。然後、您可以從叢集驗證NFS用戶端存取、並測試用戶端系統的存取。

開始之前

- NFS必須在SVM上完全設定。
- SVM根磁碟區的預設匯出原則必須包含允許存取所有用戶端的規則。
- 您名稱服務組態的任何更新都必須完成。
- Kerberos組態的任何新增或修改都必須完成。

建立 ONTAP NFS 導出策略

在建立匯出規則之前、您必須先建立匯出原則以保留這些規則。您可以使用 `vserver export-policy create` 建立匯出原則的命令。

步驟

1. 建立匯出原則：

   `vserver export-policy create -vserver` *`vserver_name`* `-policyname` *`policy_name`*

   原則名稱最長可達256個字元。

2. 確認已建立匯出原則：

   `vserver export-policy show -policyname` *`policy_name`*

範例

下列命令會在名為VS1的SVM上建立並驗證名為exp1的匯出原則：

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
---------------  -------------------
vs1              exp1
```

在 ONTAP NFS 匯出策略中新增規則

如果沒有規則、匯出原則就無法讓用戶端存取資料。若要建立新的匯出規則、您必須識別用戶端並選取用戶端比對格式、選取存取和安全性類型、指定匿名使用者ID對應、選取規則索引編號、然後選取存取傳輸協定。然後您就可以使用 `vserver export-policy rule create` 命令將新規則新增至匯出原則。

開始之前

- 您要新增匯出規則的匯出原則必須已經存在。
- 必須在資料SVM上正確設定DNS、而且DNS伺服器必須為NFS用戶端設定正確的項目。

  這是因為ONTAP 針對某些用戶端比對格式、使用資料SVM的DNS組態執行DNS查詢、而匯出原則規則比對失敗則會妨礙用戶端資料存取。

- 如果您使用Kerberos進行驗證、則必須確定NFS用戶端使用下列哪些安全性方法：
  - `krb5` （ Kerberos V5 傳輸協定）
  - `krb5i` （使用 Checksum 進行完整性檢查的 Kerberos V5 傳輸協定）
  - `krb5p` （具有隱私權服務的 Kerberos V5 傳輸協定）

關於這項工作

如果匯出原則中的現有規則涵蓋了用戶端的相符和存取需求、則不需要建立新規則。

如果您正在使用 Kerberos 進行驗證、而且 SVM 的所有磁碟區都是透過 Kerberos 存取、您可以設定匯出規則選項 `-rorule`、 `-rwrule`和 `-superuser` 將根磁碟區移至 `krb5`、 `krb5i`或 `krb5p`。

步驟

1. 識別新規則的用戶端和用戶端比對格式。

   。 `-clientmatch` 選項指定規則所套用的用戶端。可以指定單一或多個用戶端符合值；多個值的規格必須以逗號分隔。您可以指定下列任一格式的相符項目：

用戶端比對格式	範例
網域名稱前面加上「.」字元	`.example.com` 或 `.example.com,.example.net,...`
主機名稱	`host1` 或 `host1,host2, ...`
IPV4位址	`10.1.12.24` 或 `10.1.12.24,10.1.12.25, ...`
以多位元表示子網路遮罩的IPv4位址	`10.1.12.10/4` 或 `10.1.12.10/4,10.1.12.11/4,...`
具有網路遮罩的IPV4位址	`10.1.16.0/255.255.255.0` 或 `10.1.16.0/255.255.255.0,10.1.17.0/255.255.255.0,...`
以點分格式提供IPv6位址	`::1.2.3.4` 或 `::1.2.3.4,::1.2.3.5,...`
IPv6 位址、子網路遮罩以位元數表示	`ff::00/32` 或 `ff::00/32,ff::01/32,...`
以@字元開頭的netgroup名稱為單一netgroup	`@netgroup1` 或 `@netgroup1,@netgroup2,...`

您也可以合併用戶端定義的類型、例如 `.example.com,@netgroup1`。

指定IP位址時、請注意下列事項：

- 不允許輸入IP位址範圍、例如10.12.10-10.12.70。

  此格式的項目會解譯為文字字串、並視為主機名稱。

- 在匯出規則中指定個別IP位址以精細管理用戶端存取時、請勿指定動態（例如DHCP）或暫時（例如IPv6）指派的IP位址。

  否則、當用戶端的IP位址變更時、就會失去存取權。

- 不允許使用網路遮罩輸入IPv6位址、例如ff:12/ff:00。

2. 選取用戶端相符項目的存取和安全性類型。

   您可以指定下列一或多種存取模式、以驗證具有指定安全性類型的用戶端：

   - `-rorule` （唯讀存取）
   - `-rwrule` （讀寫存取權）
   - `-superuser` （ root 存取權）

如果匯出規則也允許該安全性類型的唯讀存取權、則用戶端只能取得特定安全性類型的讀寫存取權。如果安全性類型的唯讀參數比讀寫參數的限制更多、用戶端可能無法取得讀寫存取權。超級使用者存取也是如此。

您可以為規則指定多種安全性類型的以逗號分隔的清單。如果您將安全性類型指定為 `any` 或 `never`，請勿指定任何其他安全類型。從下列有效的安全類型中選擇：

當安全性類型設定為...	相符的用戶端可以存取匯出的資料...
`any`	無論傳入的安全類型為何、
`none`	如果單獨列出、則會將具有任何安全類型的用戶端授予匿名存取權。如果列出其他安全性類型、則會授與具有指定安全性類型的用戶端存取權、而具有任何其他安全性類型的用戶端則會以匿名存取權。
`never`	永不、無論傳入的安全類型為何。
`krb5`	如果是由Kerberos 5驗證。 僅驗證：簽署每個要求和回應的標頭。
`krb5i`	如果通過Kerberos 5i驗證。 驗證與完整性：簽署每個要求與回應的標頭與實體。
`krb5p`	如果是由 Kerberos 5p 驗證。 驗證、完整性和隱私：簽署每個要求和回應的標頭和實體、並加密NFS資料有效負載。
`ntlm`	如果通過CIFS的NTLM驗證。
`sys`	如果是由NFS AUTH_SYS驗證的。

建議的安全類型為 `sys`或是使用 `Kerberos 、 `krb5、 krb5i`或 `krb5p。

如果將 Kerberos 與 NFSv3 搭配使用、則匯出原則規則必須允許 `-rorule` 和 `-rwrule` 存取 `sys` 此外 `krb5`。這是因為需要允許網路鎖定管理程式（NLM）存取匯出。

3. 指定匿名使用者ID對應。

。 `-anon` 選項會指定 UNIX 使用者 ID 或使用者名稱、該使用者 ID 會對應至以 0 （零）為使用者 ID 的用戶端要求、此 ID 通常與使用者名稱根目錄相關聯。預設值為 `65534`。NFS用戶端通常會將使用者ID 65534與使用者名稱nobody建立關聯（也稱為根系統衝突_）。在本功能中、此使用者ID與使用者pcuser相關聯。ONTAP若要停用使用者 ID 為 0 的任何用戶端存取、請指定值為 `65535`。

4. 選取規則索引順序。

。 `-ruleindex` 選項指定規則的索引編號。規則會根據索引編號清單中的順序來評估；索引編號較低的規則會先評估。例如、索引編號為1的規則會在索引編號為2的規則之前進行評估。

如果您要新增...	然後...
匯出原則的第一條規則	輸入 `1`。
匯出原則的其他規則	a. 在原則中顯示現有規則： `vserver export-policy rule show -instance -policyname your_policy` b. 根據新規則的評估順序、為新規則選取索引編號。

5. 選取適用的 NFS 存取值：{`nfs|nfs3|nfs4`} 。

   `nfs` 符合任何版本、 `nfs3` 和 `nfs4` 僅符合這些特定版本。

6. 建立匯出規則並將其新增至現有的匯出原則：

   ```
   vserver export-policy rule create -vserver vserver_name -policyname
   policy_name -ruleindex integer -protocol {nfs|nfs3|nfs4} -clientmatch { text |
   "text,text,…" } -rorule security_type -rwrule security_type -superuser
   security_type -anon user_ID
   ```

7. 顯示匯出原則的規則、以驗證是否存在新規則：

   ```
   vserver export-policy rule show -policyname policy_name
   ```

   命令會顯示該匯出原則的摘要、包括套用至該原則的規則清單。此功能會為每個規則指派一個規則索引編號。ONTAP知道規則索引編號之後、您可以使用它來顯示指定匯出規則的詳細資訊。

8. 確認已正確設定套用至匯出原則的規則：

   ```
   vserver export-policy rule show -policyname policy_name -vserver vserver_name
   -ruleindex integer
   ```

範例

下列命令會在名為RSR1的匯出原則中、在名為VS1的SVM上建立匯出規則、並驗證其建立。規則的索引編號為1。規則會比對網域eng.company.com和netgroup @netGroup1中的任何用戶端。此規則可啟用所有NFS存取。它可對驗證了AUTH_SYS的使用者啟用唯讀和讀寫存取權。除非透過Kerberos驗證、否則使用UNIX使用者ID 0（零）的用戶端會匿名。

```
vs1::> vserver export-policy rule create -vserver vs1 -policyname exp1
-ruleindex 1 -protocol nfs
-clientmatch .eng.company.com,@netgoup1 -rorule sys -rwrule sys -anon
65534 -superuser krb5

vs1::> vserver export-policy rule show -policyname nfs_policy
Virtual      Policy         Rule    Access    Client           RO
Server       Name           Index   Protocol  Match            Rule
------------ -------------- ------  --------  ---------------- ------
vs1          exp1           1       nfs       eng.company.com, sys
                                              @netgroup1

vs1::> vserver export-policy rule show -policyname exp1 -vserver vs1
-ruleindex 1

                                Vserver: vs1
                            Policy Name: exp1
                             Rule Index: 1
                          Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
                           RO Access Rule: sys
                           RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
                  Superuser Security Types: krb5
              Honor SetUID Bits in SETATTR: true
                 Allow Creation of Devices: true
```

下列命令會在名為expol2的匯出原則中、在名為VS2的SVM上建立匯出規則、並加以驗證。此規則的索引編號為21。此規則會將用戶端與netgroup dev_netgroup_main.此規則可啟用所有NFS存取。此功能可為使用AUTH_SYS驗證的使用者啟用唯讀存取、並需要Kerberos驗證才能進行讀寫和root存取。除非透過Kerberos進行驗證、否則使用UNIX使用者ID 0（零）的用戶端會被拒絕root存取。

```
vs2::> vserver export-policy rule create -vserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5

vs2::> vserver export-policy rule show -policyname nfs_policy
Virtual  Policy       Rule    Access    Client                RO
Server   Name         Index   Protocol  Match                 Rule
-------- ------------ ------  --------  ------------------    ------
vs2      expol2       21       nfs      @dev_netgroup_main    sys

vs2::> vserver export-policy rule show -policyname expol2 -vserver vs1
-ruleindex 21

                                   Vserver: vs2
                                Policy Name: expol2
                                 Rule Index: 21
                            Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
                                            @dev_netgroup_main
                             RO Access Rule: sys
                             RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
                   Superuser Security Types: krb5
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

建立Volume或qtree儲存容器

建立 ONTAP NFS 卷

您可以使用建立 Volume 並指定其連接點和其他屬性 `volume create` 命令。

關於這項工作

磁碟區必須包含_交會路徑_、才能讓用戶端使用其資料。您可以在建立新磁碟區時指定交會路徑。如果您在建立磁碟區時未指定連接路徑、則必須使用 _ 掛載 _ SVM 命名空間中的磁碟區 `volume mount` 命令。

開始之前

- NFS 應設定並執行。
- SVM 安全樣式必須是 UNIX 。
- 從 ONTAP 9.13.1 開始，您可以使用容量分析和活動追蹤功能來建立 Volume 。若要啟用容量或活動追蹤，請使用或 `-activity-tracking-state`設定為 `on`發出 `volume create`命令 `-analytics-state`。

  若要深入瞭解容量分析和活動追蹤、請參閱 "啟用檔案系統分析"。如"指令參考資料ONTAP"需詳細 `volume

create`資訊，請參閱。

步驟

1. 建立具有交會點的Volume：

   ```
   volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
   -size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
   -group group_name_or_number -junction-path junction_path [-policy
   export_policy_name]
   ```

   的選擇 `-junction-path` 以下是：

   - 直接位於根目錄下、例如 */new_vol*

     您可以建立新磁碟區、並指定將其直接掛載到SVM根磁碟區。

   - 在現有目錄下、例如 */existing_dir/new_vol*

     您可以建立新磁碟區、並指定將其掛載至現有磁碟區（在現有階層架構中）、以目錄形式表示。

     如果您想在新目錄中建立磁碟區（在新磁碟區下的新階層中）、例如：*`/new_dir/new_vol`*接著、您必須先建立與 SVM 根 Volume 相關的新父 Volume 。接著、您會在新父Volume（新目錄）的交會路徑中建立新的子Volume。

     如果您打算使用現有的匯出原則、則可以在建立磁碟區時指定。您也可以稍後使用新增匯出原則 `volume modify` 命令。

2. 確認已使用所需的交會點建立磁碟區：

   ```
   volume show -vserver svm_name -volume volume_name -junction
   ```

範例

下列命令會在SVM vs1.example.com和Aggr1上建立名為user1的新磁碟區。新的 Volume 可在取得 `/users`。磁碟區大小為750 GB、磁碟區保證為磁碟區類型（預設）。

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver           Volume   Active   Junction Path   Path Source
----------------- -------  -------- --------------- -----------
vs1.example.com   users1   true     /users          RW_volume
```

下列命令會在SVM「vs1.example.com」和Aggr1上建立名為「home4」的新磁碟區。目錄 `/eng/` VS1 SVM 的命名空間已存在、新的 Volume 可從取得 `/eng/home`、成為的主目錄 `/eng/` 命名空間。磁碟區大小為 750 GB 、其磁碟區保證屬於類型 `volume` （預設）。

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                           Junction                 Junction
Vserver          Volume  Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4   true     /eng/home       RW_volume
```

建立 **ONTAP NFS qtree**

您可以建立 qtree 來包含資料、並使用來指定其內容 `volume qtree create` 命令。

開始之前

- SVM和將要包含新qtree的Volume必須已經存在。
- SVM的安全樣式必須是UNIX、NFS應設定並執行。

步驟

1. 建立qtree：

   `volume qtree create -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `} -security-style unix [-policy` *`export_policy_name`*`]`

   您可以將 Volume 和 qtree 指定為個別的引數、或以格式指定 qtree 路徑引數 `/vol/`*`volume_name`*`/`*`_qtree_name`*。

   根據預設、qtree會繼承其父Volume的匯出原則、但可以設定為使用自己的原則。如果您打算使用現有的匯出原則、則可以在建立qtree時加以指定。您也可以稍後使用新增匯出原則 `volume qtree modify` 命令。

2. 確認qtree是以所需的交會路徑建立：

   `volume qtree show -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `}`

範例

以下範例建立一個 qtree 、名稱為 qt01 、位於 SVM vs1.example.com 上、具有交會路徑 `/vol/data1`：

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style unix
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                      Vserver Name: vs1.example.com
                       Volume Name: data1
                        Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                    Security Style: unix
                       Oplock Mode: enable
                  Unix Permissions: ---rwxr-xr-x
                          Qtree Id: 2
                      Qtree Status: normal
                     Export Policy: default
        Is Export Policy Inherited: true
```

使用匯出原則保護**NFS**存取安全

了解如何使用匯出策略保護 **ONTAP NFS** 訪問

您可以使用匯出原則、將NFS存取磁碟區或qtree的權限限制在符合特定參數的用戶端。配置新儲存設備時、您可以使用現有的原則和規則、新增規則至現有原則、或建立新的原則和規則。您也可以檢查匯出原則的組態

> 從ONTAP 功能表支援的支援範例9.3開始、您可以啟用匯出原則組態檢查、做為背景工作、將任何違反規則的行為記錄在錯誤規則清單中。。 `vserver export-policy config-checker` 命令會叫用檢查程式並顯示結果、您可以使用這些結果來驗證組態、並從原則中刪除錯誤的規則。這些命令只會驗證主機名稱、網路群組和匿名使用者的匯出組態。

管理 **ONTAP NFS** 匯出規則的處理順序

您可以使用 `vserver export-policy rule setindex` 手動設定現有匯出規則索引編號的命令。這可讓您指定ONTAP 將匯出規則套用至用戶端要求的優先順序。

關於這項工作

如果新的索引編號已經在使用中、命令會在指定的點插入規則、並據此重新排序清單。

步驟

1. 修改指定匯出規則的索引編號：

   ```
   vserver export-policy rule setindex -vserver virtual_server_name -policyname
   policy_name -ruleindex integer -newruleindex integer
   ```

範例

下列命令會將索引編號3的匯出規則索引編號變更為SVM上名為VS1的匯出原則RSR1編號2：

```
vs1::> vserver export-policy rule setindex -vserver vs1
-policyname rs1 -ruleindex 3 -newruleindex 2
```

將 ONTAP NFS 導出策略指派給磁碟區

SVM中包含的每個磁碟區都必須與包含匯出規則的匯出原則相關聯、以便用戶端存取磁碟區中的資料。

關於這項工作

您可以在建立磁碟區時或建立磁碟區後的任何時間、將匯出原則與磁碟區建立關聯。您可以將一個匯出原則與磁碟區建立關聯、不過一個原則可以與許多磁碟區建立關聯。

步驟

1. 如果在建立磁碟區時未指定匯出原則、請將匯出原則指派給磁碟區：

   ```
   volume modify -vserver vserver_name -volume volume_name -policy
   export_policy_name
   ```

2. 確認原則已指派給磁碟區：

   ```
   volume show -volume volume_name -fields policy
   ```

範例

下列命令會將匯出原則nfs_policy指派給SVM VS1上的Volume vol1、並驗證指派：

```
cluster::> volume modify -v1server vs1 -volume vol1 -policy nfs_policy

cluster::>volume show -volume vol -fields policy
vserver volume       policy
------- ------------ ----------------
vs1     vol1         nfs_policy
```

將 ONTAP NFS 導出策略指派給 qtree

您也可以在磁碟區上匯出特定qtree、讓用戶端直接存取、而非匯出整個磁碟區。您可以將匯出原則指派給qtree來匯出qtree。您可以在建立新的qtree或修改現有的qtree時指派匯出原則。

開始之前

匯出原則必須存在。

關於這項工作

根據預設、如果在建立時未另外指定、qtree會繼承包含Volume的父匯出原則。

您可以在建立qtree時或在建立qtree之後的任何時間、將匯出原則與qtree建立關聯。您可以將一個匯出原則與qtree建立關聯、不過一個原則可以與許多qtree建立關聯。

步驟

1. 如果在建立qtree時未指定匯出原則、請將匯出原則指派給qtree：

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy export_policy_name
   ```

2. 確認原則已指派給qtree：

   ```
   volume qtree show -qtree qtree_name -fields export-policy
   ```

範例

下列命令會將匯出原則nfs_policy指派給SVM VS1上的qtree qt1、並驗證指派：

```
cluster::> volume modify -v1server vs1 -qtree-path /vol/vol1/qt1 -policy
nfs_policy

cluster::>volume qtree show -volume vol1 -fields export-policy
vserver volume qtree export-policy
------- ------ ----- -------------
vs1     data1  qt01  nfs_policy
```

驗證叢集中的 **ONTAP NFS** 用戶端存取

您可以在UNIX管理主機上設定UNIX檔案權限、讓選取的用戶端存取共用區。您可以使用檢查用戶端存取 `vserver export-policy check-access` 命令、視需要調整匯出規則。

步驟

1. 在叢集上、使用檢查用戶端對匯出的存取權 `vserver export-policy check-access` 命令。

   下列命令會檢查IP位址為1.2.3.4的NFSv3用戶端對Volume Home2的讀取/寫入存取。命令輸出顯示該Volume 使用匯出原則 `exp-home-dir` 這種存取被拒絕。

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
-type read-write
                                        Policy    Policy     Rule
Path                    Policy          Owner     Owner Type Index  Access
----------------------- --------------- --------- ---------- ------
----------
/                       default         vs1_root  volume          1 read
/eng                    default         vs1_root  volume          1 read
/eng/home2              exp-home-dir    home2     volume          1 denied

3 entries were displayed.
```

2. 檢查輸出、判斷匯出原則是否如預期運作、以及用戶端存取行為是否如預期。

   具體而言、您應該確認磁碟區或qtree使用的匯出原則、以及用戶端因此而擁有的存取類型。

3. 如有必要、請重新設定匯出原則規則。

從客戶端系統測試 **ONTAP NFS** 存取

驗證NFS對新儲存物件的存取之後、您應該登入NFS管理主機、從SVM讀取資料並將資料寫入SVM、以測試組態。接著、您應該在用戶端系統上以非root使用者的身分重複此程序。

開始之前

- 用戶端系統必須具有您先前指定的匯出規則所允許的IP位址。
- 您必須擁有root使用者的登入資訊。

步驟

1. 在叢集上、驗證裝載新磁碟區之LIF的IP位址：

   ```
   network interface show -vserver svm_name
   ```

   如"指令參考資料ONTAP"需詳細 `network interface show`資訊，請參閱。

2. 以root使用者身分登入管理主機用戶端系統。
3. 將目錄變更為掛載資料夾：

   ```
   cd /mnt/
   ```

4. 使用SVM的IP位址建立及掛載新資料夾：

   a. 建立新資料夾：
      `mkdir /mnt/folder`

   b. 將新磁碟區掛載至此新目錄：

```
mount -t nfs -o hard IPAddress:/volume_name /mnt/folder
```

c. 將目錄變更為新資料夾：
```
cd folder
```

下列命令會建立名為test1的資料夾、將vol1磁碟區掛載到test1掛載資料夾的192.0.2.130 IP位址、然後變更為新的test1目錄：

```
host# mkdir /mnt/test1
host# mount -t nfs -o hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

5. 建立新檔案、確認檔案是否存在、然後將文字寫入：

a. 建立測試檔案：
```
touch filename
```

b. 確認檔案存在：
```
ls -l filename
```

c. 輸入：
```
cat > filename
```

輸入一些文字、然後按下Ctrl+D將文字寫入測試檔案。

d. 顯示測試檔案的內容。
```
cat filename
```

e. 移除測試檔案：
```
rm filename
```

f. 返回父目錄：
```
cd ..
```

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

6. 以root使用者的身份、在掛載的Volume上設定任何所需的UNIX擁有權和權限。

7. 在匯出規則中識別的UNIX用戶端系統上、以目前擁有新磁碟區存取權的授權使用者之一登入、然後重複步驟3到5中的程序、確認您可以掛載磁碟區並建立檔案。

在哪裡可以找到更多 ONTAP NFS 信息

成功測試NFS用戶端存取之後、您可以執行其他NFS組態或新增SAN存取。傳輸協定存取完成時、您應該保護儲存虛擬機器（SVM）的根磁碟區。

NFS 組態

您可以使用下列資訊和技術報告進一步設定NFS存取：

- "NFS管理"

  說明如何使用NFS設定及管理檔案存取。

- "NetApp技術報告4067：NFS最佳實務與實作指南"

  提供NFSv3和NFSv3作業指南、並概述ONTAP 以NFSv3為焦點的作業系統。

- "NetApp技術報告4073：安全統一化驗證"

  說明如何設定ONTAP 搭配UNIX型Kerberos第5版（krb5）伺服器使用的功能、以進行NFS儲存驗證、以及將Windows Server Active Directory（AD）設定為Kdc和輕量型目錄存取傳輸協定（LDAP）身分識別供應商。

- "NetApp技術報告3580：NFSv4增強功能與最佳實務做法指南Data ONTAP -實作"

  說明在掛接到執行ONTAP 此功能的系統上、在AIX、Linux或Solaris用戶端上實作NFSv4元件時應遵循的最佳實務做法。

網路組態

您可以使用下列資訊與技術報告、進一步設定網路功能與名稱服務：

- "NFS管理"

  說明如何設定及管理ONTAP 靜態網路。

- "NetApp技術報告4182：乙太網路儲存設計考量與叢集Data ONTAP 式的最佳實務做法"

  說明ONTAP 實作的環節、並提供常見的網路部署情境和最佳實務建議。

- "NetApp技術報告4668：名稱服務最佳實務做法指南"

  說明如何設定LDAP、NIS、DNS及本機檔案組態以進行驗證。

SAN傳輸協定組態

如果您想要提供或修改SAN對新SVM的存取、可以使用FC或iSCSI組態資訊、此資訊適用於多個主機作業系統。

根Volume保護

在SVM上設定傳輸協定之後、您應確保其根Volume受到保護：

- "資料保護"

  說明如何建立負載共用鏡像來保護SVM根磁碟區、這是NetApp啟用NAS的SVM最佳實務做法。同時也說明如何從負載共用鏡像中提升SVM根磁碟區、以快速從磁碟區故障或損失中恢復。

此功能與7-Mode匯出有何不同ONTAP

此功能與7-Mode匯出有何不同ONTAP

如果您不熟悉 ONTAP 如何實作 NFS 匯出、您可以比較 7-Mode 和 ONTAP 匯出組態工具、以及 7-Mode 範例 `/etc/exports` 具有叢集式原則和規則的檔案。

在 ONTAP 中沒有 `/etc/exports` 檔案與否 `exportfs` 命令。而是必須定義匯出原則。匯出原則可讓您以與7-Mode相同的方式來控制用戶端存取、但提供額外的功能、例如針對多個磁碟區重複使用相同的匯出原則。

相關資訊

"NFS管理"

"NetApp技術報告4067：NFS最佳實務與實作指南"

了解 7-模式和 ONTAP NFS 導出的比較

以功能為基礎的匯出ONTAP 是以不同於7-Mode環境的方式定義和使用。

差異領域	7-Mode	ONTAP
如何定義匯出	匯出是在中定義的 `/etc/exports` 檔案：	匯出是透過在SVM中建立匯出原則來定義。SVM可包含多個匯出原則。
匯出範圍	• 匯出會套用至指定的檔案路徑或qtree。 • 您必須在中建立個別項目 `/etc/exports` 針對每個檔案路徑或 qtree 。 • 只有在中定義匯出時、匯出才會持續進行 `/etc/exports` 檔案：	• 匯出原則適用於整個Volume、包括Volume中包含的所有檔案路徑和qtree。 • 如果需要、匯出原則可套用至多個Volume。 • 所有匯出原則都會在系統重新啟動時持續執行。

隔離（指定特定用戶端對相同資源的不同存取）	若要為特定用戶端提供對單一匯出資源的不同存取權、您必須在中列出每個用戶端及其允許的存取權 `/etc/exports` 檔案：	匯出原則是由許多個別的匯出規則所組成。每個匯出規則都會定義資源的特定存取權限、並列出擁有這些權限的用戶端。若要為特定用戶端指定不同的存取權限、您必須為每組特定的存取權限建立匯出規則、列出具有這些權限的用戶端、然後將規則新增至匯出原則。
名稱別名	定義匯出時、您可以選擇讓匯出名稱與檔案路徑名稱不同。您應該使用 `-actual` 在中定義此類匯出時的參數 `/etc/exports` 檔案：	您可以選擇讓匯出的Volume名稱不同於實際的Volume名稱。若要這麼做、您必須在SVM命名空間內以自訂的交會路徑名稱來掛載磁碟區。 根據預設、磁碟區會以其Volume名稱掛載。若要自訂磁碟區的交會路徑名稱、您需要卸載、重新命名、然後重新掛載。

了解 ONTAP NFS 導出策略範例

您可以檢閱範例匯出原則、進一步瞭解匯出原則在ONTAP 功能方面的運作方式。

7-Mode匯出的實作範例ONTAP

下列範例顯示的 7-Mode 匯出與中所顯示的相同 `/etc/export` 檔案：

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

若要將此匯出重新產生為叢集匯出原則、您必須建立具有三個匯出規則的匯出原則、然後將匯出原則指派給Volume vol1。

規則	元素	價值
規則1.	`-clientmatch` （用戶端規格）	`@readonly_netgroup`
`-ruleindex`（出口規則在規則清單中的位置）	`1`	`-protocol`
`nfs`	`-rorule`（允許唯讀存取）	`sys` （使用驗證的用戶端）
`-rwrule`（允許讀寫存取）	`never`	`-superuser`（允許超級使用者存取）

規則	元素	價值
none（根目錄 _ 分段 _ 至安納）	第2條	-clientmatch
@rootaccess_netgroup	-ruleindex	2
-protocol	nfs	-rorule
sys	-rwrule	sys
-superuser	sys	第 3 條
-clientmatch	@readwrite_netgroup1,@readwrite_netgroup2	-ruleindex
3	-protocol	nfs
-rorule	sys	-rwrule
sys	-superuser	none

1. 建立名為exp_vol1的匯出原則：

   ```
   vserver export-policy create -vserver NewSVM -policyname exp_vol1
   ```

2. 在base命令中建立三個具有下列參數的規則：
   - 基本命令：
     ```
     vserver export-policy rule create -vserver NewSVM -policyname exp_vol1
     ```
   - 規則參數：
     ```
     -clientmatch @readonly_netgroup -ruleindex 1 -protocol nfs -rorule sys
     -rwrule never -superuser none
     -clientmatch @rootaccess_netgroup -ruleindex 2 -protocol nfs -rorule sys
     -rwrule sys -superuser sys
     -clientmatch @readwrite_netgroup1,@readwrite_netgroup2 -ruleindex 3
     -protocol nfs -rorule sys -rwrule sys -superuser none
     ```
3. 將原則指派給Volume vol1：

   ```
   volume modify -vserver NewSVM -volume vol1 -policy exp_vol1
   ```

7-Mode匯出的整合範例

以下範例顯示 7-Mode `/etc/export` 每 10 個 qtree 包含一行的檔案：

```
/vol/vol1/q_1472 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1471 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1473 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1570 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1571 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_2237 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2238 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2239 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2240 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2241 -sec=sys,rw=host2057s,root=host2057s
```

在 ONTAP 中、每個 qtree 都需要兩個原則之一：一個原則包含規則 `-clientmatch host1519s`或具有規則的規則 `-clientmatch host2057s`。

1. 建立兩個匯出原則、稱為exp_vol1q1和exp_vol1q2：
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q1`
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q2`
2. 為每個原則建立規則：
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q1 -clientmatch host1519s -rwrule sys -superuser sys`
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q2 -clientmatch host1519s -rwrule sys -superuser sys`
3. 將原則套用至qtree：
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_1472 -export -policy exp_vol1q1`
   - [接下來的4個qtree …]
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_2237 -export -policy exp_vol1q2`
   - [接下來的4個qtree …]

如果您稍後需要為這些主機新增其他qtree、則會使用相同的匯出原則。