



# 使用 **NFS** 管理檔案存取 ONTAP 9

NetApp  
September 12, 2024

# 目錄

使用 NFS 管理檔案存取 .....	1
啟用或停用 NFSv3 .....	1
啟用或停用 NFSv4.0 .....	1
啟用或停用 NFSv4.1 .....	1
管理 NFSv4 儲存工具限制 .....	2
啟用或停用 pNFS .....	4
透過 TCP 和 UDP 控制 NFS 存取 .....	5
從非保留連接埠控制 NFS 要求 .....	5
為未知的 UNIX 使用者處理 NTFS 磁碟區或 qtree 的 NFS 存取 .....	6
使用非保留連接埠掛載 NFS 匯出的用戶端考量 .....	7
透過驗證網域、對網路群組執行更嚴格的存取檢查 .....	7
修改用於 NFSv3 服務的連接埠 .....	8
用於管理 NFS 伺服器的命令 .....	10
疑難排解名稱服務問題 .....	11
驗證名稱服務連線 .....	14
用於管理名稱服務交換器項目的命令 .....	15
用於管理名稱服務快取的命令 .....	15
用於管理名稱對應的命令 .....	16
管理本機 UNIX 使用者的命令 .....	17
管理本機 UNIX 群組的命令 .....	17
本機 UNIX 使用者、群組和群組成員的限制 .....	18
管理本機 UNIX 使用者和群組的限制 .....	18
用於管理本機網路群組的命令 .....	19
用於管理 NIS 網域組態的命令 .....	19
用於管理 LDAP 用戶端組態的命令 .....	20
用於管理 LDAP 組態的命令 .....	20
用於管理 LDAP 用戶端架構範本的命令 .....	20
用於管理 NFS Kerberos 介面組態的命令 .....	21
管理 NFS Kerberos 領域組態的命令 .....	21
用於管理匯出原則的命令 .....	22
用於管理匯出規則的命令 .....	22
設定 NFS 認證快取 .....	23
管理匯出原則快取 .....	24
管理檔案鎖定 .....	28
FPolicy 首次讀取和首次寫入篩選器如何搭配 NFS 運作 .....	32
修改 NFSv4.1 伺服器實作 ID .....	33
管理 NFSv4 ACL .....	34
管理 NFSv4 檔案委派 .....	37
設定 NFSv4 檔案和記錄鎖定 .....	38

NFSv4參照的運作方式 .....	39
啟用或停用NFSv4參照 .....	40
顯示 NFS 統計資料 .....	40
顯示 DNS 統計資料 .....	41
顯示 NIS 統計資料 .....	43
支援VMware vStorage over NFS .....	45
啟用或停用NFS上的VMware vStorage .....	45
啟用或停用rquota支援 .....	46
透過修改TCP傳輸大小、可改善NFSv3和NFSv3效能 .....	46
修改NFSv3和NFSv4 TCP的最大傳輸大小 .....	47
設定NFS使用者所允許的群組ID數目 .....	48
控制root使用者對NTFS安全型資料的存取 .....	49

# 使用 NFS 管理檔案存取

## 啟用或停用 NFSv3

您可以修改來啟用或停用 NFSv3 -v3 選項。這可讓使用 NFSv3 傳輸協定的用戶端存取檔案。依預設、NFSv3已啟用。

### 步驟

1. 執行下列其中一項動作：

如果您想要...	輸入命令...
啟用NFSv3	<code>vserver nfs modify -vserver vserver_name -v3 enabled</code>
停用 NFSv3	<code>vserver nfs modify -vserver vserver_name -v3 disabled</code>

## 啟用或停用NFSv4.0

您可以修改來啟用或停用 NFSv4.0 -v4.0 選項。這可讓使用NFSv4.0傳輸協定的用戶端存取檔案。在更新版本中、NFSv4.0預設為啟用；在舊版中、預設為停用。ONTAP

### 步驟

1. 執行下列其中一項動作：

如果您想要...	輸入下列命令...
啟用 NFSv4.0	<code>vserver nfs modify -vserver vserver_name -v4.0 enabled</code>
停用NFSv4.0	<code>vserver nfs modify -vserver vserver_name -v4.0 disabled</code>

## 啟用或停用 NFSv4.1

您可以修改來啟用或停用 NFSv4.1 -v4.1 選項。這可讓使用 NFSv4.1 傳輸協定的用戶端存取檔案。在 ONTAP 9.9.1 中、預設會啟用 NFSv4.1 ；在舊版中、預設會停用 NFSv4.1 。

### 步驟

1. 執行下列其中一項動作：

如果您想要...	輸入下列命令...
啟用 NFSv4.1	<code>vserver nfs modify -vserver vserver_name -v4.1 enabled</code>
停用 NFSv4.1	<code>vserver nfs modify -vserver vserver_name -v4.1 disabled</code>

## 管理 NFSv4 儲存工具限制

從 ONTAP 9.13 開始、系統管理員可以讓 NFSv4 伺服器在達到每個用戶端儲存資源限制時、拒絕資源給 NFSv4 用戶端。當用戶端使用過多的 NFSv4 儲存工具資源時、這可能會導致其他 NFSv4 用戶端因為 NFSv4 儲存工具資源無法使用而遭到封鎖。

啟用此功能也可讓客戶檢視每個用戶端的作用中 storepool 資源使用量。如此一來、就能更輕鬆地識別耗盡系統資源的用戶端、並使每個用戶端的資源限制得以實施。

### 檢視已使用的 storepool 資源

。 `vserver nfs storepool show` 命令會顯示使用的 storepool 資源數量。storepool 是 NFSv4 用戶端所使用的資源集區。

#### 步驟

1. 以系統管理員身分執行 `vserver nfs storepool show` 命令顯示 NFSv4 用戶端的 storepool 資訊。

#### 範例

此範例顯示 NFSv4 用戶端的 storepool 資訊。

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-Ip: 10.0.1.1

Client-Ip Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount
-----
10.0.2.1      nfs4.1      true      2 1 0 4
10.0.2.2      nfs4.2      true      2 1 0 4

2 entries were displayed.
```

## 啟用或停用 **storepool** 限制控制項

系統管理員可以使用下列命令來啟用或停用 **storepool** 限制控制項。

### 步驟

- 身為管理員、請執行下列其中一項動作：

如果您想要...	輸入下列命令...
啟用 <b>storepool</b> 限制控制	<code>vserver nfs storepool config modify -limit-enforce enabled</code>
停用 <b>storepool</b> 限制控制項	<code>vserver nfs storepool config modify -limit-enforce disabled</code>

## 檢視封鎖的用戶端清單

如果已啟用 **storepool** 限制、則系統管理員可以查看哪些用戶端在達到其每個用戶端資源臨界值時遭到封鎖。系統管理員可以使用下列命令來查看哪些用戶端已標示為封鎖用戶端。

### 步驟

- 使用 `vserver nfs storepool blocked-client show` 顯示 NFSv4 封鎖用戶端清單的命令。

## 從封鎖的用戶端清單中移除用戶端

達到其每個用戶端臨界值的用戶端將會中斷連線、並新增至區塊用戶端快取。系統管理員可以使用下列命令、從

區塊用戶端快取中移除用戶端。這將允許用戶端連線至 ONTAP NFSv4 伺服器。

步驟

1. 使用 `vserver nfs storepool blocked-client flush -client-ip <ip address>` 用於清除 storepool 封鎖用戶端快取的命令。
2. 使用 `vserver nfs storepool blocked-client show` 用於驗證用戶端已從區塊用戶端快取移除的命令。

範例

此範例顯示封鎖的用戶端、其 IP 位址為 "10.2.1.1" 、正在從所有節點中清除。

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
-----
10.1.1.1

1 entries were displayed.
```

# 啟用或停用pNFS

pNFS可讓NFS用戶端直接並平行地在儲存裝置上執行讀寫作業、藉此改善效能、避免NFS伺服器成為潛在的瓶頸。若要啟用或停用 pNFS （平行 NFS ） 、您可以修改 `-v4.1 -pnfs` 選項。

如果ONTAP 這個版本是...	pNFS預設為...
9.8 或更新版本	已停用
9.7 或更早版本	已啟用

您需要的產品

需要NFSv4.1支援才能使用pNFS。

如果您要啟用pNFS、必須先停用NFS參照。兩者無法同時啟用。

如果您在SVM上使用pNFS搭配Kerberos、則必須在SVM上的每個LIF上啟用Kerberos。

步驟

1. 執行下列其中一項動作：

如果您想要...	輸入命令...
啟用pNFS	<code>vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled</code>
停用pNFS	<code>vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled</code>

#### 相關資訊

- [NFS 主幹總覽](#)

## 透過TCP和UDP控制NFS存取

您可以透過修改來啟用或停用透過 TCP 和 UDP 對儲存虛擬機器（SVM）的 NFS 存取 `-tcp` 和 `-udp` 參數。這可讓您控制NFS用戶端是否能在您的環境中透過TCP或UDP存取資料。

#### 關於這項工作

這些參數僅適用於NFS。它們不會影響輔助通訊協定。例如、如果停用NFS over TCP、則透過TCP掛載作業仍會成功。若要完全封鎖TCP或UDP流量、您可以使用匯出原則規則。



在停用TCP for NFS之前、您必須先關閉SnapDiff RPC伺服器、以免發生命令故障的錯誤。您可以使用命令停用 TCP `vserver snapdiff-rpc-server off -vserver vserver_name`。

#### 步驟

1. 執行下列其中一項動作：

如果您想要NFS存取...	輸入命令...
透過TCP啟用	<code>vserver nfs modify -vserver vserver_name -tcp enabled</code>
已透過TCP停用	<code>vserver nfs modify -vserver vserver_name -tcp disabled</code>
已透過udp啟用	<code>vserver nfs modify -vserver vserver_name -udp enabled</code>
已透過udp停用	<code>vserver nfs modify -vserver vserver_name -udp disabled</code>

## 從非保留連接埠控制NFS要求

您可以啟用來拒絕來自非保留連接埠的 NFS 掛載要求 `-mount-rootonly` 選項。若要拒絕來自非保留連接埠的所有 NFS 要求、您可以啟用 `-nfs-rootonly` 選項。

#### 關於這項工作



依預設、選項 `-mount-rootonly` 是 enabled。

依預設、選項 `-nfs-rootonly` 是 disabled。

這些選項不適用於空程序。

#### 步驟

1. 執行下列其中一項動作：

如果您想要...	輸入命令...
允許來自非保留連接埠的NFS掛載要求	<code>vserver nfs modify -vserver vserver_name -mount -rootonly disabled</code>
拒絕來自非保留連接埠的NFS掛載要求	<code>vserver nfs modify -vserver vserver_name -mount -rootonly enabled</code>
允許來自非保留連接埠的所有NFS要求	<code>vserver nfs modify -vserver vserver_name -nfs -rootonly disabled</code>
拒絕來自非保留連接埠的所有NFS要求	<code>vserver nfs modify -vserver vserver_name -nfs -rootonly enabled</code>

## 為未知的UNIX使用者處理NTFS磁碟區或qtree的NFS存取

如果ONTAP 無法識別嘗試連線至NTFS安全樣式之磁碟區或qtree的UNIX使用者、就無法將使用者明確對應至Windows使用者。您可以設定ONTAP 支援不允許存取此類使用者以獲得更嚴格的安全性、或將其對應至預設的Windows使用者、以確保所有使用者都能享有最低的存取層級。

#### 您需要的產品

若要啟用此選項、必須設定預設的Windows使用者。

#### 關於這項工作

如果UNIX使用者嘗試存取NTFS安全樣式的磁碟區或qtree、則必須先將UNIX使用者對應至Windows使用者、ONTAP 才能讓支援者正確評估NTFS權限。但是ONTAP 、如果無法在已設定的使用者資訊名稱服務來源中查詢UNIX使用者的名稱、就無法明確地將UNIX使用者對應至特定的Windows使用者。您可以決定如何以下列方式處理這類未知的UNIX使用者：

- 拒絕未知UNIX使用者的存取。

如此一來、所有UNIX使用者都需要明確對應、才能存取NTFS磁碟區或qtree、進而加強更嚴格的安全性。

- 將未知的UNIX使用者對應至預設的Windows使用者。

如此可確保所有使用者透過預設的Windows使用者、獲得對NTFS磁碟區或qtree的最低存取層級、進而降低安全性、但更為便利。

## 步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 執行下列其中一項動作：

如果您想讓未知UNIX使用者使用預設的Windows使用者...	輸入命令...
已啟用	<code>vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled</code>
已停用	<code>vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled</code>

3. 返回管理權限層級：

```
set -privilege admin
```

## 使用非保留連接埠掛載NFS匯出的用戶端考量

◦ `-mount-rootoonly` 必須在必須支援用戶端的儲存系統上停用此選項、即使使用者以 `root` 登入、也能使用非保留連接埠來掛載 NFS 匯出。這類用戶端包括HummingBird用戶端和Solaris NFS/IPv6用戶端。

如果是 `-mount-rootoonly` 此選項已啟用、ONTAP 不允許使用非保留連接埠的 NFS 用戶端（亦即數字大於 1,023 的連接埠）掛載 NFS 匯出。

## 透過驗證網域、對網路群組執行更嚴格的存取檢查

根據預設、ONTAP 在評估網路群組的用戶端存取時、會執行額外的驗證。額外檢查可確保用戶端的網域符合儲存虛擬機器（SVM）的網域組態。否則ONTAP、不允許用戶端存取。

### 關於這項工作

當針對用戶端存取評估匯出原則規則、且匯出原則規則包含netgroup時ONTAP、必須判斷用戶端的IP位址是否屬於netgroup。ONTAP為此目的、ONTAP 將用戶端的IP位址轉換成使用DNS的主機名稱、並取得完整網域名稱（FQDN）。

如果netgroup檔案只列出主機的簡短名稱、而且主機的簡短名稱存在於多個網域中、則不同網域的用戶端可以在不進行此檢查的情況下取得存取權。

為了避免這種情況ONTAP、此功能會將從DNS傳回的主機網域、與針對SVM設定的DNS網域名稱清單進行比較。如果符合、則允許存取。如果不相符、則會拒絕存取。

此驗證預設為啟用。您可以修改來管理 `-netgroup-dns-domain-search` 參數、可在進階權限層級使用。

## 步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 執行所需的動作：

如果您希望網路群組的網域驗證...	輸入...
已啟用	<pre>vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled</pre>
已停用	<pre>vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled</pre>

3. 將權限等級設為admin：

```
set -privilege admin
```

## 修改用於NFSv3服務的連接埠

儲存系統上的NFS伺服器會使用掛載精靈和網路鎖定管理程式等服務、透過特定的預設網路連接埠與NFS用戶端進行通訊。在大多數NFS環境中、預設連接埠都能正常運作、不需要修改、但如果您想在NFSv3環境中使用不同的NFS網路連接埠、您可以這麼做。

### 您需要的產品

變更儲存系統上的NFS連接埠需要所有NFS用戶端重新連線至系統、因此您應該在變更前先將此資訊傳達給使用者。

### 關於這項工作

您可以為每個儲存虛擬機器（SVM）設定NFS掛載精靈、網路鎖定管理程式、網路狀態監視器和NFS配額精靈服務所使用的連接埠。連接埠號碼變更會影響透過TCP和udp存取資料的NFS用戶端。

NFSv4和NFSv4.1的連接埠無法變更。

## 步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 停用NFS存取：

```
vserver nfs modify -vserver vserver_name -access false
```

3. 設定特定NFS服務的NFS連接埠：

```
vserver nfs modify -vserver vserver_namenfs_port_parameterport_number
```

NFS連接埠參數	說明	預設連接埠
-mountd-port	NFS掛載精靈	635
-nlm-port	網路鎖定管理程式	4045
-nsm-port	網路狀態監視器	4046
-rquotad-port	NFS配額精靈	4049

除了預設連接埠之外、允許的連接埠號碼範圍為1024到65535.每個NFS服務都必須使用唯一的連接埠。

4. 啟用NFS存取：

```
vserver nfs modify -vserver vserver_name -access true
```

5. 使用 `network connections listening show` 用於驗證連接埠號碼變更的命令。

6. 返回管理權限層級：

```
set -privilege admin
```

範例

下列命令會將SVM上名為VS1的NFS掛載Daemon連接埠設為1113：

```

vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
        them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true


vs1::*> network connections listening show
Vserver Name      Interface Name:Local Port      Protocol/Service
-----
Node: cluster1-01
Cluster           cluster1-01_clus_1:7700        TCP/ctlopcp
vs1               data1:4046                   TCP/sm
vs1               data1:4046                   UDP/sm
vs1               data1:4045                   TCP/nlm-v4
vs1               data1:4045                   UDP/nlm-v4
vs1               data1:1113                   TCP/mount
vs1               data1:1113                   UDP/mount
...
vs1::*> set -privilege admin

```

## 用於管理NFS伺服器的命令

管理ONTAP NFS伺服器時、會有特定的功能不一的指令。

如果您想要...	使用此命令...
建立NFS伺服器	<code>vserver nfs create</code>
顯示NFS伺服器	<code>vserver nfs show</code>
修改NFS伺服器	<code>vserver nfs modify</code>
刪除NFS伺服器	<code>vserver nfs delete</code>

隱藏 .snapshot NFSv3 掛載點下的目錄列表	vserver nfs 的命令 -v3-hide-snapshot 選項已啟用
 <p>明確存取 .snapshot 即使已啟用此選項、仍會允許目錄。</p>	

如需詳細資訊、請參閱每個命令的手冊頁。

## 疑難排解名稱服務問題

當用戶端因為名稱服務問題而發生存取失敗時、您可以使用 `vserver services name-service getxxbyyy` 命令系列可手動執行各種名稱服務查詢、並檢查查詢的詳細資料和結果、以協助進行疑難排解。

關於這項工作

- 您可以針對每個命令指定下列項目：
  - 執行查詢的節點或儲存虛擬機器（SVM）名稱。
  - 這可讓您測試特定節點或SVM的名稱服務查詢、以縮小搜尋名稱服務組態問題的範圍。
  - 是否顯示用於查詢的來源。
  - 這可讓您檢查是否使用了正確的來源。
- 根據設定的名稱服務交換器訂單、選擇執行查詢的服務。ONTAP
- 這些命令可在進階權限層級使用。

步驟

- 執行下列其中一項動作：

若要擷取...	使用命令...
主機名稱的IP位址	<code>vserver services name-service getxxbyyy getaddrinfo</code> <code>vserver services name-service getxxbyyy gethostbyname</code> （僅限 IPv4 位址）
依群組ID的群組成員	<code>vserver services name-service getxxbyyy getgrbygid</code>
群組成員（依群組名稱）	<code>vserver services name-service getxxbyyy getgrbyname</code>

使用者所屬的群組清單	<code>vserver services name-service getxxbyyy getgrlist</code>
IP位址的主機名稱	<code>vserver services name-service getxxbyyy getnameinfo vserver services name- service getxxbyyy gethostbyaddr</code> （僅限 IPv4 位址）
使用者名稱的使用者資訊	<code>vserver services name-service getxxbyyy getpwnbyname</code> 您可以指定來測試 RBAC 使用者的名 稱解析 <code>-use-rbac</code> 參數為 <code>true</code> 。
使用者ID的使用者資訊	<code>vserver services name-service getxxbyyy getpwbyuid</code> 您可以指定來測試 RBAC 使用者的名稱解析 <code>-use -rbac</code> 參數為 <code>true</code> 。
用戶端的網路群組成員資格	<code>vserver services name-service getxxbyyy netgrp</code>
使用netgroup by host搜尋的用戶端網路群組成員資格	<code>vserver services name-service getxxbyyy netgrpbyhost</code>

下列範例顯示SVM VS1的DNS查詢測試、嘗試取得主機acast1.eng.example.com的IP位址：

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

下列範例顯示SVM VS1的NIS查詢測試、嘗試擷取使用者的UID 501768使用者資訊：

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvC2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

下列範例顯示SVM VS1的LDAP查詢測試、嘗試擷取名稱為LDAP1之使用者的使用者資訊：

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

下列範例顯示SVM VS1的網路群組查詢測試、嘗試找出用戶端dnshost0是否為netgroup lnetgroup 136的成員：

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. 分析您執行的測試結果、並採取必要行動。

如果...	請查看...
主機名稱或IP位址查詢失敗或產生不正確的結果	DNS 組態
查詢查詢的來源不正確	名稱服務交換器組態



如果...	請查看...
使用者或群組查詢失敗或產生不正確的結果	<ul style="list-style-type: none"> <li>• 名稱服務交換器組態</li> <li>• 來源組態（本機檔案、NIS 網域、LDAP 用戶端）</li> <li>• 網路組態（例如、LIF和Routes）</li> </ul>
主機名稱查詢失敗或逾時、而且DNS伺服器不會解析DNS短名稱（例如host1）	頂層網域（頂級域）查詢的DNS組態。您可以使用停用 TLD 查詢 <code>-is-tld-query-enabled false</code> 選項 <code>vserver services name-service dns modify</code> 命令。

## 相關資訊

["NetApp技術報告4668：名稱服務最佳實務做法指南"](#)

## 驗證名稱服務連線

從ONTAP 功能9.2開始、您可以檢查DNS和LDAP名稱伺服器、以確認它們是否已連線ONTAP 至功能驗證。這些命令可在管理權限層級使用。

### 關於這項工作

您可以使用名稱服務組態檢查程式、視需要檢查有效的DNS或LDAP名稱服務組態。此驗證檢查可在命令列或系統管理員中啟動。

對於DNS組態、所有伺服器均已經過測試、需要進行設定才能視為有效。對於LDAP組態、只要任何伺服器都已啟動、組態就會生效。名稱服務命令會套用組態檢查程式、除非是 `skip-config-validation` 欄位為 `true`（預設為 `false`）。

### 步驟

1. 使用適當的命令來檢查名稱服務組態。UI會顯示已設定伺服器的狀態。

若要檢查...	使用此命令...
DNS組態狀態	<code>vserver services name-service dns check</code>
LDAP 組態狀態	<code>vserver services name-service ldap check</code>

```
cluster1::> vserver services name-service dns check -vserver vs0
```

Vserver	Name Server	Status	Status Details
vs0	10.11.12.13	up	Response time (msec): 55
vs0	10.11.12.14	up	Response time (msec): 70
vs0	10.11.12.15	down	Connection refused.

```
cluster1::> vserver services name-service ldap check -vserver vs0
```

```
| Vserver: vs0 |
| Client Configuration Name: c1 |
| LDAP Status: up |
| LDAP Status Details: Successfully connected to LDAP server |
"10.11.12.13". |
```

如果至少有一部已設定的伺服器（名稱伺服器/ LDAP伺服器）可連線並提供服務、則組態驗證會成功。如果部分伺服器無法連線、則會顯示警告。

## 用於管理名稱服務交換器項目的命令

您可以透過建立、顯示、修改及刪除名稱服務交換器項目來管理這些項目。

如果您想要...	使用此命令...
建立名稱服務交換器項目	<code>vserver services name-service ns-switch create</code>
顯示名稱服務交換器項目	<code>vserver services name-service ns-switch show</code>
修改名稱服務交換器項目	<code>vserver services name-service ns-switch modify</code>
刪除名稱服務交換器項目	<code>vserver services name-service ns-switch delete</code>

如需詳細資訊、請參閱每個命令的手冊頁。

相關資訊

["NetApp技術報告4668：名稱服務最佳實務做法指南"](#)

## 用於管理名稱服務快取的命令

您可以修改存留時間（TTL）值來管理名稱服務快取。TTL值決定名稱服務資訊在快取中持

續存在的時間長度。

如果您要修改下列項目的TTL值：	使用此命令...
UNIX使用者	<code>vserver services name-service cache unix-user settings</code>
UNIX群組	<code>vserver services name-service cache unix-group settings</code>
UNIX網路群組	<code>vserver services name-service cache netgroups settings</code>
主機	<code>vserver services name-service cache hosts settings</code>
群組成員資格	<code>vserver services name-service cache group-membership settings</code>

相關資訊

["指令參考資料ONTAP"](#)

## 用於管理名稱對應的命令

管理名稱對應時、會ONTAP 有特定的功能不全指令。

如果您想要...	使用此命令...
建立名稱對應	<code>vserver name-mapping create</code>
在特定位置插入名稱對應	<code>vserver name-mapping insert</code>
顯示名稱對應	<code>vserver name-mapping show</code>
交換兩個名稱對應的位置 附註：當名稱對應設定為 IP 限定條件項目時、不允許交換。	<code>vserver name-mapping swap</code>
修改名稱對應	<code>vserver name-mapping modify</code>
刪除名稱對應	<code>vserver name-mapping delete</code>
驗證正確的名稱對應	<code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code>

如需詳細資訊、請參閱每個命令的手冊頁。

## 管理本機UNIX使用者的命令

有特定ONTAP 的功能可用來管理本機UNIX使用者。

如果您想要...	使用此命令...
建立本機UNIX使用者	<code>vserver services name-service unix-user create</code>
從URI載入本機UNIX使用者	<code>vserver services name-service unix-user load-from-uri</code>
顯示本機UNIX使用者	<code>vserver services name-service unix-user show</code>
修改本機UNIX使用者	<code>vserver services name-service unix-user modify</code>
刪除本機UNIX使用者	<code>vserver services name-service unix-user delete</code>

如需詳細資訊、請參閱每個命令的手冊頁。

## 管理本機UNIX群組的命令

管理本機UNIX群組時、會ONTAP 有特定的指令檔。

如果您想要...	使用此命令...
建立本機UNIX群組	<code>vserver services name-service unix-group create</code>
新增使用者至本機UNIX群組	<code>vserver services name-service unix-group adduser</code>
從URI載入本機UNIX群組	<code>vserver services name-service unix-group load-from-uri</code>
顯示本機UNIX群組	<code>vserver services name-service unix-group show</code>
修改本機UNIX群組	<code>vserver services name-service unix-group modify</code>
從本機UNIX群組刪除使用者	<code>vserver services name-service unix-group deluser</code>
刪除本機UNIX群組	<code>vserver services name-service unix-group delete</code>

如需詳細資訊、請參閱每個命令的手冊頁。

## 本機UNIX使用者、群組和群組成員的限制

介紹叢集中UNIX使用者和群組的最大數量限制、以及管理這些限制的命令。ONTAP這些限制可防止系統管理員在叢集中建立過多的本機UNIX使用者和群組、有助於避免效能問題。

本機UNIX使用者群組和群組成員的總數有限制。本機UNIX使用者有不同的限制。限制是整個叢集的。每個新限制都會設定為預設值、您最多可以修改為預先指派的硬限制。

資料庫	預設限制	硬限制
本機UNIX使用者	32、768	65,536
本機UNIX群組和群組成員	32、768	65,536

## 管理本機UNIX使用者和群組的限制

我們提供特定ONTAP 的指令來管理本機UNIX使用者和群組的限制。叢集管理員可以使用這些命令來疑難排解叢集內的效能問題、這些問題被認為與大量的本機UNIX使用者和群組有關。

關於這項工作

叢集管理員可在進階權限層級使用這些命令。

步驟

1. 執行下列其中一項動作：

如果您想要...	使用命令...
顯示本機UNIX使用者限制的相關資訊	<code>vserver services unix-user max-limit show</code>
顯示本機UNIX群組限制的相關資訊	<code>vserver services unix-group max-limit show</code>
修改本機UNIX使用者限制	<code>vserver services unix-user max-limit modify</code>
修改本機UNIX群組限制	<code>vserver services unix-group max-limit modify</code>

如需詳細資訊、請參閱每個命令的手冊頁。

## 用於管理本機網路群組的命令

您可以從URI載入本機網路群組、驗證節點的狀態、顯示及刪除它們、藉此管理本機網路群組。

如果您想要...	使用命令...
從URI載入網路群組	<code>vserver services name-service netgroup load</code>
驗證各節點的網路群組狀態	<code>vserver services name-service netgroup status</code> 可在進階權限層級或更高層級使用。
顯示本機網路群組	<code>vserver services name-service netgroup file show</code>
刪除本機網路群組	<code>vserver services name-service netgroup file delete</code>

如需詳細資訊、請參閱每個命令的手冊頁。

## 用於管理NIS網域組態的命令

管理ONTAP NIS網域組態時、會有特定的功能不完整的指令。

如果您想要...	使用此命令...
建立NIS網域組態	<code>vserver services name-service nis-domain create</code>
顯示 NIS 網域組態	<code>vserver services name-service nis-domain show</code>
顯示NIS網域組態的繫結狀態	<code>vserver services name-service nis-domain show-bound</code>
顯示 NIS 統計資料	<code>vserver services name-service nis-domain show-statistics</code> 可在進階權限層級或更高層級使用。
清除NIS統計資料	<code>vserver services name-service nis-domain clear-statistics</code> 可在進階權限層級或更高層級使用。
修改NIS網域組態	<code>vserver services name-service nis-domain modify</code>
刪除NIS網域組態	<code>vserver services name-service nis-domain delete</code>
啟用網路群組各主機搜尋的快取	<code>vserver services name-service nis-domain netgroup-database config modify</code> 可在進階權限層級或更高層級使用。

如需詳細資訊、請參閱每個命令的手冊頁。

## 用於管理LDAP用戶端組態的命令

有特定ONTAP 的功能可用來管理LDAP用戶端組態。



SVM管理員無法修改或刪除由叢集管理員所建立的LDAP用戶端組態。

如果您想要...	使用此命令...
建立LDAP用戶端組態	<code>vserver services name-service ldap client create</code>
顯示LDAP用戶端組態	<code>vserver services name-service ldap client show</code>
修改LDAP用戶端組態	<code>vserver services name-service ldap client modify</code>
變更LDAP用戶端的BIND密碼	<code>vserver services name-service ldap client modify-bind-password</code>
刪除LDAP用戶端組態	<code>vserver services name-service ldap client delete</code>

如需詳細資訊、請參閱每個命令的手冊頁。

## 用於管理LDAP組態的命令

有特定ONTAP 的功能可用來管理LDAP組態。

如果您想要...	使用此命令...
建立LDAP組態	<code>vserver services name-service ldap create</code>
顯示LDAP組態	<code>vserver services name-service ldap show</code>
修改LDAP組態	<code>vserver services name-service ldap modify</code>
刪除LDAP組態	<code>vserver services name-service ldap delete</code>

如需詳細資訊、請參閱每個命令的手冊頁。

## 用於管理LDAP用戶端架構範本的命令

管理ONTAP LDAP用戶端架構範本時、會有特定的支援功能指令。



SVM管理員無法修改或刪除由叢集管理員所建立的LDAP用戶端架構。

如果您想要...	使用此命令...
複製現有的LDAP架構範本	<code>vserver services name-service ldap client schema copy</code> 可在進階權限層級或更高層級使用。
顯示LDAP架構範本	<code>vserver services name-service ldap client schema show</code>
修改LDAP架構範本	<code>vserver services name-service ldap client schema modify</code> 可在進階權限層級或更高層級使用。
刪除LDAP架構範本	<code>vserver services name-service ldap client schema delete</code> 可在進階權限層級或更高層級使用。

如需詳細資訊、請參閱每個命令的手冊頁。

## 用於管理NFS Kerberos介面組態的命令

管理ONTAP NFS Kerberos介面組態時、會有特定的功能不完整的指令。

如果您想要...	使用此命令...
在LIF上啟用NFS Kerberos	<code>vserver nfs kerberos interface enable</code>
顯示NFS Kerberos介面組態	<code>vserver nfs kerberos interface show</code>
修改NFS Kerberos介面組態	<code>vserver nfs kerberos interface modify</code>
停用LIF上的NFS Kerberos	<code>vserver nfs kerberos interface disable</code>

如需詳細資訊、請參閱每個命令的手冊頁。

## 管理NFS Kerberos領域組態的命令

管理ONTAP NFS Kerberos領域組態時、會有特定的功能不完整的指令。

如果您想要...	使用此命令...
建立NFS Kerberos領域組態	<code>vserver nfs kerberos realm create</code>
顯示NFS Kerberos領域組態	<code>vserver nfs kerberos realm show</code>



如果您想要...	使用此命令...
修改NFS Kerberos領域組態	<code>vserver nfs kerberos realm modify</code>
刪除NFS Kerberos領域組態	<code>vserver nfs kerberos realm delete</code>

如需詳細資訊、請參閱每個命令的手冊頁。

## 用於管理匯出原則的命令

管理匯出原則時、會ONTAP 有特定的指令。

如果您想要...	使用此命令...
顯示匯出原則的相關資訊	<code>vserver export-policy show</code>
重新命名匯出原則	<code>vserver export-policy rename</code>
複製匯出原則	<code>vserver export-policy copy</code>
刪除匯出原則	<code>vserver export-policy delete</code>

如需詳細資訊、請參閱每個命令的手冊頁。

## 用於管理匯出規則的命令

管理匯出規則時、會ONTAP 有一些特定的指令。

如果您想要...	使用此命令...
建立匯出規則	<code>vserver export-policy rule create</code>
顯示匯出規則的相關資訊	<code>vserver export-policy rule show</code>
修改匯出規則	<code>vserver export-policy rule modify</code>
刪除匯出規則	<code>vserver export-policy rule delete</code>



如果您已設定多個符合不同用戶端的相同匯出規則、請務必在管理匯出規則時保持同步。

如需詳細資訊、請參閱每個命令的手冊頁。

# 設定NFS認證快取

## 修改NFS認證快取即時時間的理由

使用認證快取來儲存NFS匯出存取使用者驗證所需的資訊、以加快存取速度並改善效能。ONTAP您可以設定資訊儲存在認證快取中的時間長度、以便針對您的環境進行自訂。

修改NFS認證快取存留時間（TTL）有幾種情況可協助解決問題。您應該瞭解這些情境、以及進行這些修改的後果。

### 理由

在下列情況下、請考慮變更預設TTL：

問題	補救行動
您環境中的名稱伺服器因為ONTAP 來自VMware的大量要求而效能降低。	增加快取的正向和負向認證的TTL、以減少ONTAP 從功能驗證到名稱伺服器的要求數量。
名稱伺服器管理員進行變更、以允許存取先前遭拒的NFS使用者。	減少快取負面認證的TTL、以縮短NFS使用者等待ONTAP 來自外部名稱伺服器的更新認證要求、以便存取的時間。
名稱伺服器管理員進行變更、以拒絕先前允許的NFS使用者存取。	減少快取正向認證資料的TTL、縮短ONTAP 從外部名稱伺服器要求新認證資料的時間、讓NFS使用者現在無法存取。

### 後果

您可以個別修改快取正面和負面認證的時間長度。不過、您應該瞭解這樣做的優點和缺點。

如果您...	優勢在於...	缺點是...
增加正向認證快取時間	不常將認證要求傳送至名稱伺服器、減少名稱伺服器的負載。ONTAP	拒絕存取先前允許存取但不再允許的NFS使用者所需的時間較長。
縮短正向認證快取時間	拒絕存取先前允許存取但不再允許的NFS使用者所需的時間較短。	利用此功能、將認證要求更頻繁地傳送至名稱伺服器、增加名稱伺服器的負載。ONTAP
增加負面認證快取時間	不常將認證要求傳送至名稱伺服器、減少名稱伺服器的負載。ONTAP	將存取權限授予先前不允許存取但現在不允許存取的NFS使用者所需的時間較長。
減少負面認證快取時間	將存取權限授予先前不允許存取但現在不允許存取的NFS使用者所需的時間較短。	利用此功能、將認證要求更頻繁地傳送至名稱伺服器、增加名稱伺服器的負載。ONTAP

## 設定快取NFS使用者認證的即時時間

您可以ONTAP 修改儲存虛擬機器（SVM）的NFS伺服器、設定將NFS使用者認證儲存在內部快取（生存時間或TTL）的時間長度。這可讓您減輕與名稱伺服器負載過高或認證變更影響NFS使用者存取有關的某些問題。

關於這項工作

這些參數可在進階權限層級使用。

步驟

- 1. 將權限層級設為進階：

```
set -privilege advanced
```

- 2. 執行所需的動作：

如果您要修改快取的TTL ...	使用命令...
正面認證	<div><pre>vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live</pre></div> <div>TTL的測量單位為毫秒。從 ONTAP 9.10.1 及更新版本開始、預設值為 1 小時（ 3,600,000 毫秒）。在 ONTAP 9.9.1 及更早版本中、預設值為 24 小時（ 86,400,000 毫秒）。此值允許的範圍為1分鐘（60000毫秒）到7天（604,800,000毫秒）。</div>
負面認證	<div><pre>vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live</pre></div> <div>TTL的測量單位為毫秒。預設值為2小時（7、200、000毫秒）。此值允許的範圍為1分鐘（60000毫秒）到7天（604,800,000毫秒）。</div>

- 3. 返回管理權限層級：

```
set -privilege admin
```

## 管理匯出原則快取

### 排清匯出原則快取

使用多個匯出原則快取來儲存匯出原則相關資訊、以加快存取速度。ONTAP手動排清匯出原則快取 (vserver export-policy cache flush) 移除可能過期的資訊、並強制ONTAP 從適當的外部資源擷取目前資訊。這有助於解決與用戶端存取NFS匯出相關的各種問題。

關於這項工作

匯出原則快取資訊可能因為下列原因而過期：

- 最近對匯出原則規則所做的變更
- 最近變更名稱伺服器中的主機名稱記錄
- 最近在名稱伺服器中變更netgroup項目
- 從網路中斷中恢復、避免網路群組完全載入

## 步驟

1. 如果您未啟用名稱服務快取、請在預先權限模式中執行下列其中一項動作：

如果您想要清除...	輸入命令...
所有匯出原則快取（showmount除外）	<code>vserver export-policy cache flush -vserver vserver_name</code>
匯出原則規則存取快取	<code>vserver export-policy cache flush -vserver vserver_name -cache access</code> 您可以加入選用的 <code>-node</code> 用於指定要清除存取快取的節點的參數。
主機名稱快取	<code>vserver export-policy cache flush -vserver vserver_name -cache host</code>
netgroup快取	<code>vserver export-policy cache flush -vserver vserver_name -cache netgroup</code> 網路群組的處理需要大量資源。如果您嘗試解決由舊網路群組所造成的用戶端存取問題、則只能清除網路群組快取。
showmount快取	<code>vserver export-policy cache flush -vserver vserver_name -cache showmount</code>

2. 如果已啟用名稱服務快取、請執行下列其中一項動作：

如果您想要清除...	輸入命令...
匯出原則規則存取快取	<code>vserver export-policy cache flush -vserver vserver_name -cache access</code> 您可以加入選用的 <code>-node</code> 用於指定要清除存取快取的節點的參數。
主機名稱快取	<code>vserver services name-service cache hosts forward-lookup delete-all</code>

如果您想要清除...	輸入命令...
netgroup快取	<pre>vserver services name-service cache netgroups ip-to-netgroup delete-all vserver services name-service cache netgroups members delete-all</pre> 網路群組的處理需要大量資源。如果您嘗試解決由舊網路群組所造成的用戶端存取問題、則只能清除網路群組快取。
showmount快取	<pre>vserver export-policy cache flush -vserver vserver_name -cache showmount</pre>

## 顯示匯出原則netgroup佇列和快取

在匯入及解析網路群組時、使用netgroup佇列、並使用netgroup快取來儲存產生的資訊。ONTAP疑難排解匯出原則網路群組相關問題時、您可以使用 `vserver export-policy netgroup queue show` 和 `vserver export-policy netgroup cache show` 用於顯示 netgroup 隊列狀態和 netgroup 高速緩存內容的命令。

### 步驟

1. 執行下列其中一項動作：

若要顯示匯出原則netgroup ...	輸入命令...
佇列	<pre>vserver export-policy netgroup queue show</pre>
快取	<pre>vserver export-policy netgroup cache show -vserver vserver_name</pre>

如需詳細資訊、請參閱每個命令的手冊頁。

## 檢查用戶端IP位址是否為網路群組的成員

疑難排解與網路群組相關的 NFS 用戶端存取問題時、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。

### 關於這項工作

檢查netgroup成員資格可讓您判斷ONTAP 是否知道客戶端是或不是netgroup的成員。它也能讓您知道ONTAP、在重新整理netgroup資訊的同時、該功能是否處於暫時性狀態。此資訊可協助您瞭解為何用戶端可能會被意外授予或拒絕存取。

### 步驟

1. 檢查用戶端 IP 位址的 netgroup 成員資格：`vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

命令可傳回下列結果：

- 用戶端是netgroup的成員。

這是透過反向查詢掃描或逐主機搜尋網路群組來確認的。

- 用戶端是netgroup的成員。

這是ONTAP 在foundnetgroup快取中找到的。

- 用戶端不是netgroup的成員。
- 由於目前正在重新整理網路群組快取、所以無法判斷用戶端的成員資格ONTAP。

除非如此、否則無法明確排除成員資格。使用 `vserver export-policy netgroup queue show` 命令來監控 netgroup 的載入、並在完成後重試檢查。

## 範例

下列範例會檢查IP位址為172.17.16.72的用戶端是否為SVM VS1上的netgroup水銀成員：

```
cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup mercury -client-ip 172.17.16.72
```

## 最佳化存取快取效能

您可以設定數個參數來最佳化存取快取、並在效能與儲存在存取快取中的資訊目前狀態之間找到適當的平衡點。

### 關於這項工作

當您設定存取快取重新整理期間時、請謹記下列事項：

- 較高的值表示項目在存取快取中的時間較長。

優勢在於效能更佳、ONTAP 因為用較少資源來重新整理存取快取項目。缺點是、如果匯出原則規則發生變更、而存取快取項目因而變得過時、則更新這些規則所需的時間會較長。因此、應該存取的用戶端可能會遭到拒絕、而應該遭到拒絕的用戶端可能會取得存取權。

- 較低的值代表ONTAP 更常更新存取快取項目。

優點是項目較新、用戶端較可能被正確授予或拒絕存取。缺點是效能降低、因為ONTAP 用更多資源重新整理存取快取項目。

## 步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 執行所需的動作：

若要修改...	輸入...
正項目的重新整理期間	<code>vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value</code>
否定項目的重新整理期間	<code>vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value</code>
舊項目的逾時期間	<code>vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value</code>

### 3. 驗證新的參數設定：

```
vserver export-policy access-cache config show-all-vservers
```

### 4. 返回管理權限層級：

```
set -privilege admin
```

## 管理檔案鎖定

### 關於在傳輸協定之間鎖定檔案

檔案鎖定是用戶端應用程式用來防止使用者存取先前由其他使用者開啟的檔案的方法。如何鎖定檔案取決於用戶端的傳輸協定。ONTAP

如果用戶端是NFS用戶端、則鎖定為建議事項；如果用戶端是SMB用戶端、則鎖定為必要項目。

由於NFS與SMB檔案鎖定之間的差異、NFS用戶端可能無法存取先前由SMB應用程式開啟的檔案。

當NFS用戶端嘗試存取SMB應用程式鎖定的檔案時、會發生下列情況：

- 在混合或 NTFS 磁碟區中、檔案處理作業、例如 `rm`、`rmdir` 和 `mv` 可能導致 NFS 應用程式失敗。
- SMB拒絕讀取和拒絕寫入開啟模式會分別拒絕NFS讀取和寫入作業。
- 當檔案的寫入範圍遭專屬SMB bytelock鎖定时、NFS寫入作業會失敗。

在UNIX安全型磁碟區中、NFS取消連結和重新命名作業會忽略SMB鎖定狀態、並允許存取檔案。UNIX安全型磁碟區上的所有其他NFS作業都會遵守SMB鎖定狀態。

### 如何處理唯讀位元ONTAP

唯讀位元是逐一檔案設定、以反映檔案是可寫入（停用）或唯讀（啟用）。

使用Windows的SMB用戶端可以設定每個檔案的唯讀位元。NFS用戶端不會設定每個檔案的唯讀位元、因

為NFS用戶端沒有任何使用每個檔案唯讀位元的傳輸協定作業。

當使用Windows的SMB用戶端建立檔案時、可以在檔案上設定唯讀位元。ONTAP在NFS用戶端和SMB用戶端之間共用檔案時、也可以設定唯讀位元。ONTAP有些軟體在NFS用戶端和SMB用戶端使用時、需要啟用唯讀位元。

為了在NFS用戶端和SMB用戶端之間共用的檔案上保留適當的讀取和寫入權限、它會根據下列規則來處理唯讀位元：ONTAP

- NFS會將任何啟用唯讀位元的檔案視為未啟用寫入權限位元。
- 如果NFS用戶端停用所有寫入權限位元、且至少有一個位元先前已啟用、ONTAP 則會啟用該檔案的唯讀位元。
- 如果NFS用戶端啟用任何寫入權限位元、ONTAP 則無法使用該檔案的唯讀位元。
- 如果已啟用檔案的唯讀位元、且NFS用戶端嘗試探索檔案的權限、則檔案的權限位元不會傳送至NFS用戶端；ONTAP 而是將權限位元傳送至NFS用戶端、並遮罩寫入權限位元。
- 如果已啟用檔案的唯讀位元、且SMB用戶端停用唯讀位元、ONTAP 則會啟用檔案的擁有者寫入權限位元。
- 啟用唯讀位元的檔案只能由root寫入。



檔案權限的變更會立即在SMB用戶端上生效、但如果NFS用戶端啟用屬性快取、則可能不會立即在NFS用戶端上生效。

在處理共用路徑元件上的鎖定時、此功能與**Windows**有何**ONTAP** 不同

不像Windows、ONTAP 在檔案開啟時、不會鎖定開啟檔案路徑的每個元件。此行為也會影響SMB共用路徑。

由於無法鎖定路徑的每個元件、因此可以重新命名開啟檔案或共用區上方的路徑元件、這可能會對某些應用程式造成問題、也可能導致SMB組態中的共用路徑無效。ONTAP這可能導致無法存取共用區。

為了避免重新命名路徑元件所造成的問題、您可以套用Windows存取控制清單（ACL）安全性設定、防止使用者或應用程式重新命名重要目錄。

深入瞭解 ["如何防止在用戶端存取目錄時重新命名目錄"](#)。

## 顯示鎖定的相關資訊

您可以顯示目前檔案鎖定的相關資訊、包括鎖定的類型、鎖定狀態、位元組範圍鎖定、共用鎖定模式、委派鎖定及投機鎖定的詳細資料、以及鎖定是以耐久或持續的控點開啟。

關於這項工作

無法針對透過NFSv4或NFSv4.1建立的鎖定顯示用戶端IP位址。

依預設、命令會顯示所有鎖定的相關資訊。您可以使用命令參數來顯示特定儲存虛擬機器（SVM）的鎖定資訊、或是根據其他條件篩選命令的輸出。

◦ `vserver locks show` 命令會顯示四種鎖定類型的相關資訊：

- 位元組範圍鎖定、僅鎖定部分檔案。



- 共用鎖定、可鎖定開啟的檔案。
- 投機鎖定、可控制SMB上的用戶端快取。
- 委派：透過NFSv4.x控制用戶端快取

藉由指定選用參數、您可以決定每種鎖定類型的重要資訊。如需詳細資訊、請參閱命令的手冊頁。

#### 步驟

1. 使用顯示鎖定的相關資訊 `vserver locks show` 命令。

#### 範例

以下範例顯示具有路徑之檔案上 NFSv4 鎖定的摘要資訊 `/vol1/file1`。共享鎖定存取模式為WRITE拒絕\_nONE、且鎖定是以寫入委派授予的：

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path          LIF          Protocol  Lock Type  Client
-----
vol1    /vol1/file1              lif1         nfsv4     share-level -
                                     Sharelock Mode: write-deny_none
                                     delegation  -
                                     Delegation Type: write
```

以下範例顯示有關 SMB 鎖定的詳細 oplock 和共享鎖定資訊、這些資訊位於具有路徑的檔案上 `/data2/data2_2/intro.pptx`。對於IP位址為10.3.1.3的用戶端、檔案上會以寫入拒絕的共用鎖定存取模式授予可持久使用的控制代碼。批次oplock層級的租賃oplock已授予：

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

Vserver: vs1
Volume: data2_2
Logical Interface: lif2
Object Path: /data2/data2_2/intro.pptx
Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
Lock Protocol: cifs
Lock Type: share-level
Node Holding Lock State: node3
Lock State: granted
Bytelock Starting Offset: -
Number of Bytes Locked: -
Bytelock is Mandatory: -
Bytelock is Exclusive: -
Bytelock is Superlock: -
Bytelock is Soft: -
```

```

        Oplock Level: -
    Shared Lock Access Mode: write-deny_none
        Shared Lock is Soft: false
        Delegation Type: -
        Client Address: 10.3.1.3
        SMB Open Type: durable
        SMB Connect State: connected
SMB Expiration Time (Secs): -
        SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

        Vserver: vs1
        Volume: data2_2
    Logical Interface: lif2
        Object Path: /data2/data2_2/test.pptx
        Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
        Lock Protocol: cifs
        Lock Type: op-lock
    Node Holding Lock State: node3
        Lock State: granted
Bytelock Starting Offset: -
    Number of Bytes Locked: -
        Bytelock is Mandatory: -
        Bytelock is Exclusive: -
        Bytelock is Superlock: -
        Bytelock is Soft: -
        Oplock Level: batch
    Shared Lock Access Mode: -
        Shared Lock is Soft: -
        Delegation Type: -
        Client Address: 10.3.1.3
        SMB Open Type: -
        SMB Connect State: connected
SMB Expiration Time (Secs): -
        SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

```

## 打破鎖定

當檔案鎖定阻礙用戶端存取檔案時、您可以顯示目前保留的鎖定資訊、然後中斷特定鎖定。您可能需要中斷鎖定的案例包括偵錯應用程式。

### 關於這項工作

- `vserver locks break` 命令只能在進階權限層級及更高層級使用。命令的手冊頁包含詳細資訊。

### 步驟

1. 若要尋找打破鎖定所需的資訊、請使用 `vserver locks show` 命令。

命令的手冊頁包含詳細資訊。

2. 將權限層級設為進階：

```
set -privilege advanced
```

3. 執行下列其中一項動作：

如果您要指定...來中斷鎖定	輸入命令...
SVM名稱、Volume名稱、LIF名稱及檔案路徑	<code>vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif</code>
鎖定ID	<code>vserver locks break -lockid UUID</code>

4. 返回管理權限層級：

```
set -privilege admin
```

## FPolicy首次讀取和首次寫入篩選器如何搭配NFS運作

當使用外部FPolicy伺服器啟用FPolicy、並將讀寫作業設為監控事件時、NFS用戶端在讀寫要求的高流量期間會經歷較長的回應時間。對於NFS用戶端、在FPolicy中使用第一讀取和第一寫入篩選器可減少FPolicy通知的數量、並改善效能。

在NFS中、用戶端會擷取檔案的控制代碼來執行I/O作業。在重新啟動伺服器和用戶端之後、此處理程序可能仍有效。因此、用戶端可自由快取處理代碼並傳送要求、而無需再次擷取處理代碼。在一般工作階段中、會將許多讀取/寫入要求傳送至檔案伺服器。如果針對所有這些要求產生通知、可能會導致下列問題：

- 由於額外的通知處理和更高的回應時間、所以負載較大。
- 即使伺服器不受所有通知影響、仍有大量通知會傳送至FPolicy伺服器。

從用戶端收到特定檔案的第一次讀取/寫入要求後、就會建立快取項目、而且讀取/寫入計數也會遞增。此要求會標示為第一次讀取/寫入作業、並產生FPolicy事件。在規劃及建立NFS用戶端的FPolicy篩選器之前、您應該先瞭解FPolicy篩選器的基本運作方式。

- 第一讀取：篩選用戶端的第一讀取要求。

當此篩選器用於NFS事件時 `-file-session-io-grouping-count` 和 `-file-session-io-grouping-duration` 設定決定處理 FPolicy 的第一讀取要求。

- 第一寫入：篩選用戶端的第一寫入要求。

當此篩選器用於NFS事件時 `-file-session-io-grouping-count` 和 `-file-session-io-grouping-duration` 設定決定 FPolicy 處理的第一次寫入要求。

NFS伺服器資料庫中會新增下列選項。

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

# 修改NFSv4.1伺服器實作ID

NFSv4.1傳輸協定包含一個伺服器實作ID、其中記錄伺服器網域、名稱和日期。您可以修改伺服器實作ID預設值。變更預設值很有用、例如收集使用量統計資料或疑難排解互通性問題時。如需詳細資訊、請參閱RFC 5661。

關於這項工作  
這三個選項的預設值如下：

選項	選項名稱	預設值
NFSv4.1實作ID網域	-v4.1-implementation -domain	netapp.com
NFSv4.1實作ID名稱	-v4.1-implementation-name	叢集版本名稱
NFSv4.1實作ID日期	-v4.1-implementation-date	叢集版本日期

## 步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 執行下列其中一項動作：

如果您想要修改NFSv4.1實作識別碼...	輸入命令...
網域	<code>vserver nfs modify -v4.1 -implementation-domain domain</code>
名稱	<code>vserver nfs modify -v4.1 -implementation-name name</code>
日期	<code>vserver nfs modify -v4.1 -implementation-date date</code>

### 3. 返回管理權限層級：

```
set -privilege admin
```

## 管理NFSv4 ACL

### 啟用NFSv4 ACL的優點

啟用NFSv4 ACL有許多好處。

啟用NFSv4 ACL的好處包括：

- 更精細地控制使用者對檔案和目錄的存取
- 更好的NFS安全性
- 改善與CIFS的互通性
- 移除每位使用者16個群組的NFS限制

### NFSv4 ACL的運作方式

使用NFSv4 ACL的用戶端可以設定及檢視系統上檔案和目錄的ACL。當在具有ACL的目錄中建立新檔案或子目錄時、新檔案或子目錄會繼承ACL中標記有適當繼承旗標的所有ACL項目（ACE）。

當檔案或目錄是因NFSv4要求而建立時、產生的檔案或目錄上的ACL取決於檔案建立要求是否包含ACL或僅包含標準UNIX檔案存取權限、以及父目錄是否具有ACL：

- 如果要求包含ACL、則會使用該ACL。
- 如果要求僅包含標準UNIX檔案存取權限、但父目錄具有ACL、則只要將ACE標記為適當的繼承旗標、父目錄ACL中的ACE就會由新檔案或目錄繼承。



即使是、父 ACL 也會繼承 `-v4.0-acl` 設為 `off`。

- 如果要求僅包含標準UNIX檔案存取權限、且父目錄沒有ACL、則會使用用戶端檔案模式來設定標準UNIX檔案存取權限。
- 如果要求僅包含標準UNIX檔案存取權限、且父目錄具有不可繼承的ACL、則只會以模式位元建立新物件。



如果是 `-chown-mode` 參數已設為 `restricted` 使用中的命令 `vserver nfs` 或 `vserver export-policy rule` 系列產品、檔案擁有權只能由超級使用者變更、即使使用 NFSv4 ACL 設定的磁碟上權限允許非 `root` 使用者變更檔案擁有權。如需詳細資訊、請參閱相關的手冊頁。

### 啟用或停用NFSv4 ACL的修改

當 ONTAP 收到 `chmod` 具有 ACL 之檔案或目錄的命令、依預設會保留及修改 ACL、以反映模式位元變更。您可以停用 `-v4-acl-preserve` 如果您想要刪除 ACL、請使用此參數來變更行為。

## 關於這項工作

使用統一化安全性樣式時、此參數也會指定當用戶端傳送檔案或目錄的chmod、chgroup或chown命令時、是否保留或捨棄NTFS檔案權限。

此參數的預設值為啟用。

## 步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 執行下列其中一項動作：

如果您想要...	輸入下列命令...
啟用現有NFSv4 ACL的保留與修改 (預設)	<code>vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled</code>
變更模式位元時、請停用保留和丟棄NFSv4 ACL	<code>vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled</code>

3. 返回管理權限層級：

```
set -privilege admin
```

## 如何使用**NFSv4 ACL**來判斷是否可以刪除檔案**ONTAP**

為了判斷是否能刪除檔案、ONTAP 它使用檔案的刪除位元組合、以及包含目錄的刪除子位元。如需詳細資訊、請參閱NFS 4.1 RFC 5661。

## 啟用或停用**NFSv4 ACL**

若要啟用或停用 NFSv4 ACL、您可以修改 `-v4.0-acl` 和 `-v4.1-acl` 選項：這些選項預設為停用。

## 關於這項工作

◦ `-v4.0-acl` 或 `-v4.1-acl` 選項可控制 NFSv4 ACL 的設定和檢視、但無法控制這些 ACL 的存取檢查強制執行。

## 步驟

1. 執行下列其中一項動作：

如果您想要...	然後...
----------	-------

啟用NFSv4.0 ACL	輸入下列命令：  <code>vserver nfs modify -vserver vserver_name -v4.0-acl enabled</code>
停用NFSv4.0 ACL	輸入下列命令：  <code>vserver nfs modify -vserver vserver_name -v4.0-acl disabled</code>
啟用 NFSv4.1 ACL	輸入下列命令：  <code>vserver nfs modify -vserver vserver_name -v4.1-acl enabled</code>
停用 NFSv4.1 ACL	輸入下列命令：  <code>vserver nfs modify -vserver vserver_name -v4.1-acl disabled</code>

## 修改NFSv4 ACL的最大ACE限制

您可以修改參數、以修改每個 NFSv4 ACL 允許的 ACE 數量上限 `-v4-acl-max-aces`。根據預設、每個ACL的限制設為400個ACE。增加此限制有助於確保資料成功移轉、ACL中包含超過400個ACE、以移轉至執行ONTAP 效益測試的儲存系統。

關於這項工作

增加此限制可能會影響使用NFSv4 ACL存取檔案的用戶端效能。

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 修改NFSv4 ACL的最大ACE限制：

```
vserver nfs modify -v4-acl-max-aces max_ace_limit
```

的有效範圍

`max_ace_limit` 是 192 至 1024.

3. 返回管理權限層級：

```
set -privilege admin
```

# 管理NFSv4檔案委派

## 啟用或停用NFSv4讀取檔案委派

若要啟用或停用 NFSv4 讀取檔案委派、您可以修改 `-v4.0-read-delegation`或 選項。啟用讀取檔案委派、您就能免除開啟和關閉檔案所產生的大部分訊息負荷。

關於這項工作

預設會停用讀取檔案委派。

啟用讀取檔案委派的缺點是、伺服器及其用戶端必須在伺服器重新開機或重新啟動、用戶端重新開機或重新啟動、或發生網路分割區之後、才能恢復委派。

### 步驟

1. 執行下列其中一項動作：

如果您想要...	然後...
啟用NFSv4讀取檔案委派	輸入下列命令：  <code>vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled</code>
啟用 NFSv4.1 讀取檔案委派	輸入下列命令：  + <code>vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled</code>
停用NFSv4讀取檔案委派	輸入下列命令：  <code>vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled</code>
停用 NFSv4.1 讀取檔案委派	輸入下列命令：  <code>vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled</code>

### 結果

檔案委派選項會在變更後立即生效。不需要重新開機或重新啟動NFS。

## 啟用或停用NFSv4寫入檔案委派

若要啟用或停用寫入檔案委派、您可以修改 `-v4.0-write-delegation`或 選項。啟用寫入檔案委派之後、除了開啟和關閉檔案之外、您還可以免除與檔案和記錄鎖定相關的大部分訊息負荷。



關於這項工作

預設會停用寫入檔案委派。

啟用寫入檔案委派的缺點是、伺服器及其用戶端必須在伺服器重新開機或重新啟動、用戶端重新開機或重新啟動、或發生網路分割之後、執行其他工作來恢復委派。

步驟

1. 執行下列其中一項動作：

如果您想要...	然後...
啟用NFSv4寫入檔案委派	輸入下列命令： <code>vserver nfs modify -vserver vserver_name -v4.0-write -delegation enabled</code>
啟用 NFSv4.1 寫入檔案委派	輸入下列命令： <code>vserver nfs modify -vserver vserver_name -v4.1-write -delegation enabled</code>
停用NFSv4寫入檔案委派	輸入下列命令： <code>vserver nfs modify -vserver vserver_name -v4.0-write -delegation disabled</code>
停用 NFSv4.1 寫入檔案委派	輸入下列命令： <code>vserver nfs modify -vserver vserver_name -v4.1-write -delegation disabled</code>

結果

檔案委派選項會在變更後立即生效。不需要重新開機或重新啟動NFS。

## 設定NFSv4檔案和記錄鎖定

關於NFSv4檔案與記錄鎖定

對於NFSv4用戶端、ONTAP 支援NFSv4檔案鎖定機制、在租賃型模式下維持所有檔案鎖定的狀態。

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

指定NFSv4鎖定租期

若要指定 NFSv4 鎖定租用期間（也就是 ONTAP 不可撤銷地授予用戶端鎖定的期間）、您可以修改 `-v4-lease-seconds` 選項。較短的租用期間可加速伺服器恢復、而較長的租用期間則有利於處理大量用戶端的伺服器。

關於這項工作

根據預設、此選項設為 30。此選項的最小值為 10。此選項的最大值是鎖定寬限期、您可以使用設定 `locking.lease_seconds` 選項。

#### 步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 輸入下列命令：

```
vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
```

3. 返回管理權限層級：

```
set -privilege admin
```

## 指定NFSv4鎖定寬限期

若要指定 NFSv4 鎖定寬限期（也就是用戶端在伺服器恢復期間嘗試從 ONTAP 重新取得鎖定狀態的時間週期）、您可以修改 `-v4-grace-seconds` 選項。

關於這項工作

根據預設、此選項設為 45。

#### 步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 輸入下列命令：

```
vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
```

3. 返回管理權限層級：

```
set -privilege admin
```

## NFSv4參照的運作方式

啟用NFSv4轉介時ONTAP、支援將「IN-SVM」轉介給NFSv4用戶端。SVM內部參照是指接收NFSv4要求的叢集節點將NFSv4用戶端參照至儲存虛擬機器（SVM）上的另一個邏輯介面（LIF）。

NFSv4用戶端應該從該點開始存取目標LIF接收參照的路徑。當原始叢集節點判斷SVM中存在存留在資料磁碟區所在叢集節點上的LIF時、會提供此類參照、進而讓用戶端能夠更快存取資料、並避免額外的叢集通訊。

## 啟用或停用NFSv4參照

您可以啟用選項、在儲存虛擬機器（SVM）上啟用 NFSv4 參照 `-v4-fsid-change` 和 `-v4.0-referrals` 或。啟用 NFSv4 參照可讓支援此功能的 NFSv4 用戶端更快存取資料。

您需要的產品

如果您想要啟用 NFS 參照、必須先停用平行 NFS。您無法同時啟用兩者。

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 執行下列其中一項動作：

如果您想要...	輸入命令...
啟用 NFSv4 參照	<pre>vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled</pre>
停用 NFSv4 參照	<pre>vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled</pre>
啟用 NFSv4.1 參照	<pre>vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled</pre>
停用 NFSv4.1 參照	<pre>vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled</pre>

3. 返回管理權限層級：

```
set -privilege admin
```

## 顯示 NFS 統計資料

您可以在儲存系統上顯示儲存虛擬機器（SVM）的 NFS 統計資料、以監控效能並診斷問題。

步驟

1. 使用 `statistics catalog object show` 用於識別可從中檢視資料之 NFS 物件的命令。

```
statistics catalog object show -object nfs*
```

2. 使用 `statistics start` 和選用 `statistics stop` 從一或多個物件收集資料範例的命令。

3. 使用 `statistics show` 命令以檢視範例資料。

範例：監控**NFSv3**效能

下列範例顯示NFSv3傳輸協定的效能資料。

下列命令會啟動新範例的資料收集：

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

下列命令會指定計數器來顯示範例中的資料、這些計數器會顯示成功讀取和寫入要求的數目、以及讀取和寫入要求的總數：

```
vs1::> statistics show -sample-id nfs_sample -counter  
read_total|write_total|read_success|write_success
```

Object: nfsv3

Instance: vs1

Start-time: 2/11/2013 15:38:29

End-time: 2/11/2013 15:38:41

Cluster: cluster1

Counter	Value
read_success	40042
read_total	40042
write_success	1492052
write_total	1492052

相關資訊

["效能監控設定"](#)

## 顯示 DNS 統計資料

您可以顯示儲存系統上儲存虛擬機器（SVM）的 DNS 統計資料、以監控效能並診斷問題。

步驟

1. 使用 `statistics catalog object show` 用於識別可從中檢視資料的 DNS 物件的命令。

```
statistics catalog object show -object external_service_op*
```

2. 使用 `statistics start` 和 `statistics stop` 從一或多個物件收集資料範例的命令。
3. 使用 `statistics show` 命令以檢視範例資料。

## 監控 DNS 統計資料

下列範例顯示DNS查詢的效能資料。下列命令會開始收集新範例的資料：

```
vs1::*> statistics start -object external_service_op -sample-id  
dns_sample1  
vs1::*> statistics start -object external_service_op_error -sample-id  
dns_sample2
```

下列命令會指定計數器來顯示範例中的資料、這些計數器會顯示所傳送的DNS查詢數、以及所接收、失敗或逾時的DNS查詢數：

```
vs1::*> statistics show -sample-id dns_sample1 -counter  
num_requests_sent|num_responses_received|num_successful_responses|num_time  
outs|num_request_failures|num_not_found_responses
```

```
Object: external_service_op  
Instance: vs1:DNS:Query:10.72.219.109  
Start-time: 3/8/2016 11:15:21  
End-time: 3/8/2016 11:16:52  
Elapsed-time: 91s  
Scope: vs1
```

Counter	Value
num_not_found_responses	0
num_request_failures	0
num_requests_sent	1
num_responses_received	1
num_successful_responses	1
num_timeouts	0

6 entries were displayed.

下列命令會指定計數器顯示特定伺服器上DNS查詢收到特定錯誤的次數、以顯示範例中的資料：

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count
```

```
Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1
```

Counter	Value
count	1
error_string	NXDOMAIN
server_ip_address	10.72.219.109

3 entries were displayed.

相關資訊

["效能監控設定"](#)

## 顯示 NIS 統計資料

您可以顯示儲存系統上儲存虛擬機器（SVM）的 NIS 統計資料、以監控效能並診斷問題。

步驟

1. 使用 `statistics catalog object show` 用於識別可從中檢視資料的 NIS 物件的命令。

```
statistics catalog object show -object external_service_op*
```

2. 使用 `statistics start` 和 `statistics stop` 從一或多個物件收集資料範例的命令。
3. 使用 `statistics show` 命令以檢視範例資料。

## 監控NIS統計資料

下列範例顯示NIS查詢的效能資料。下列命令會開始收集新範例的資料：

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

下列命令會指定計數器來顯示範例中的資料、這些計數器會顯示已傳送的NIS查詢數、以及已接收、失敗或逾時的NIS查詢數：

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses
```

Object: external\_service\_op  
Instance: vs1:NIS:Query:10.227.13.221  
Start-time: 3/8/2016 11:27:39  
End-time: 3/8/2016 11:27:56  
Elapsed-time: 17s  
Scope: vs1

Counter	Value
num_not_found_responses	0
num_request_failures	1
num_requests_sent	2
num_responses_received	1
num_successful_responses	1
num_timeouts	0

6 entries were displayed.

下列命令會指定計數器來顯示範例中的資料、這些計數器會顯示特定伺服器上的NIS查詢收到特定錯誤的次數：

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count
```

Object: external\_service\_op\_error  
Instance: vs1:NIS:Query:YP\_NOTFOUND:10.227.13.221  
Start-time: 3/8/2016 11:33:05  
End-time: 3/8/2016 11:33:10  
Elapsed-time: 5s  
Scope: vs1

Counter	Value
count	1
error_string	YP_NOTFOUND
server_ip_address	10.227.13.221

3 entries were displayed.

相關資訊

["效能監控設定"](#)

# 支援VMware vStorage over NFS

支援某些VMware vStorage API、以利在NFS環境中整合陣列（VAAI）功能。ONTAP

## 支援的功能

支援下列功能：

- 複本卸載

可讓ESXi主機直接在來源與目的地資料儲存區位置之間複製虛擬機器或虛擬機器磁碟（VMDK）、而不需涉及主機。這可節省ESXi主機CPU週期和網路頻寬。如果來源磁碟區很少、複本卸載可保留空間效率。

- 保留空間

保留空間以保證VMDK檔案的儲存空間。

## 限制

VMware vStorage over NFS具有下列限制：

- 複本卸載作業可能會在下列情況下失敗：
  - 在來源或目的地Volume上執行wafliron時、因為它會暫時將Volume離線
  - 同時移動來源或目的地Volume
  - 同時移動來源或目的地LIF
  - 執行接管或恢復作業時
  - 執行切換或切換作業時

- 伺服器端複製可能會因為下列案例中的檔案處理格式差異而失敗：

您嘗試從目前或先前已將qtree匯出至從未匯出qtree的SVM複製資料。若要解決此限制、您可以在目的地SVM上匯出至少一個qtree。

## 相關資訊

["哪些VAAI卸載作業受Data ONTAP 支援？"](#)

## 啟用或停用NFS上的VMware vStorage

您可以使用來啟用或停用儲存虛擬機器（SVM）上透過NFS對VMware vStorage的支援 `vserver nfs modify` 命令。

## 關於這項工作

預設會停用透過NFS支援VMware vStorage。

## 步驟

1. 顯示SVM目前的vStorage支援狀態：



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

2. 執行下列其中一項動作：

如果您想要...	輸入下列命令...
啟用VMware vStorage支援	<pre>vserver nfs modify -vserver vserver_name -vstorage enabled</pre>
停用VMware vStorage支援	<pre>vserver nfs modify -vserver vserver_name -vstorage disabled</pre>

完成後

您必須先安裝適用於VMware VAAI的NFS外掛程式、才能使用此功能。如需詳細資訊、請參閱\_安裝適用於VMware VAAI的NetApp NFS外掛程式。

相關資訊

["NetApp文件：適用於VMware VAAI的NetApp NFS外掛程式"](#)

## 啟用或停用rquota支援

支援遠端配額傳輸協定第1版（rquota v1）ONTAP。rquota傳輸協定可讓NFS用戶端從遠端機器取得使用者的配額資訊。您可以使用在儲存虛擬機器（SVM）上啟用 rquota vserver nfs modify 命令。

關於這項工作

預設會停用rquota。

步驟

1. 執行下列其中一項動作：

如果您想要...	輸入下列命令...
啟用SVM的rquota支援	<pre>vserver nfs modify -vserver vserver_name -rquota enable</pre>
停用SVM的rquota支援	<pre>vserver nfs modify -vserver vserver_name -rquota disable</pre>

如需配額的詳細資訊、請參閱 ["邏輯儲存管理"](#)。

## 透過修改TCP傳輸大小、可改善NFSv3和NFSv3效能

您可以修改TCP最大傳輸大小、藉此改善透過高延遲網路連線至儲存系統的NFSv3和NFSv4用戶端效能。

當用戶端透過延遲時間超過10毫秒的廣域網路（WAN）或城域網路（MAN）存取儲存系統時、您可能可以修改TCP最大傳輸大小來改善連線效能。在低延遲網路（例如區域網路（LAN））中存取儲存系統的用戶端、可能無法從修改這些參數中獲益。如果處理量改善並不超過延遲影響、則不應使用這些參數。

若要判斷您的儲存環境是否能從修改這些參數中獲益、您應該先對效能不佳的NFS用戶端進行全面的效能評估。檢閱低效能是否是因為用戶端的往返延遲過大和要求較少。在這些情況下、用戶端和伺服器無法完全使用可用頻寬、因為他們大部分的工作週期都在等待透過連線傳輸的小要求和回應。

藉由增加NFSv3和NFSv4要求大小、用戶端和伺服器可以更有效地使用可用頻寬、以每單位時間移動更多資料、進而提高連線的整體效率。

請記住、儲存系統與用戶端之間的組態可能有所不同。儲存系統和用戶端支援最大1 MB的傳輸作業大小。不過、如果您將儲存系統設定為支援1 MB的最大傳輸大小、但用戶端僅支援64 KB、則掛載傳輸大小限制為64 KB或更小。

在修改這些參數之前、您必須注意、這會在組裝和傳輸大量回應所需的一段時間內、在儲存系統上產生額外的記憶體使用量。與儲存系統的高延遲連線越多、額外的記憶體使用量就越高。高記憶體容量的儲存系統可能因為這項變更而幾乎沒有任何影響。記憶體容量過低的儲存系統可能會發生明顯的效能降低。

成功使用這些參數取決於從叢集的多個節點擷取資料的能力。叢集網路固有的延遲可能會增加回應的整體延遲。使用這些參數時、整體延遲通常會增加。因此、對延遲敏感的工作負載可能會產生負面影響。

## 修改NFSv3和NFSv4 TCP的最大傳輸大小

您可以修改 `-tcp-max-xfer-size` 使用 NFSv3 和 NFSv4.x 通訊協定、為所有 TCP 連線設定最大傳輸大小的選項。

關於這項工作

您可以針對每個儲存虛擬機器（SVM）個別修改這些選項。

從 ONTAP 9 開始 `v3-tcp-max-read-size` 和 `v3-tcp-max-write-size` 選項已過時。您必須使用 `-tcp-max-xfer-size` 選項。

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 執行下列其中一項動作：

如果您想要...	輸入命令...
修改NFSv3或NFSv4 TCP最大傳輸大小	<pre>vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size</pre>

選項	範圍	預設
<code>-tcp-max-xfer-size</code>	8192至1048576位元組	65536 位元組



您輸入的最大傳輸大小必須是4 KB（4096位元組）的倍數。未適當調整的要求會對效能造成負面影響。

3. 使用 `vserver nfs show -fields tcp-max-xfer-size` 用於驗證變更的命令。
4. 如果有任何用戶端使用靜態掛載、請卸載並重新掛載新的參數大小以使其生效。

#### 範例

下列命令會將SVM上的NFSv3和NFSv4.x TCP最大傳輸大小設為1048576位元組、名稱為VS1：

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

## 設定NFS使用者所允許的群組ID數目

根據預設、ONTAP 使用Kerberos (RPCSEC\_GSS) 驗證處理NFS使用者認證時、支援最多32個群組ID。使用AUTH\_SYS驗證時、預設的群組ID最大數量為16、如RFC 5531所定義。如果您的使用者成員超過預設群組數、則最多可增加1,024個。

#### 關於這項工作

如果使用者的認證中有超過預設的群組ID數目、則其餘的群組ID會被刪減、而且使用者在嘗試從儲存系統存取檔案時可能會收到錯誤訊息。您應該將每個SVM的最大群組數設定為代表環境中最大群組數的數字。

下表顯示的兩個參數 `vserver nfs modify` 決定三個範例組態中群組 ID 最大數目的命令：

參數	設定	產生的群組ID限制
<code>-extended-groups-limit</code>	32	RPCSEC_GSS : 32
<code>-auth-sys-extended-groups</code>	disabled	AUTH_SYS : 16
	這些是預設設定。	
<code>-extended-groups-limit</code>	256	RPCSEC_GSS : 256
<code>-auth-sys-extended-groups</code>	disabled	AUTH_SYS : 16
<code>-extended-groups-limit</code>	512	RPCSEC_GSS : 512
<code>-auth-sys-extended-groups</code>	enabled	驗證系統 : 512

#### 步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 執行所需的動作：

如果您要設定允許的輔助群組數目上限...	輸入命令...
僅適用於RPCSEC_GSS、並將AUTH_SYS設為預設值16	<code>vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled</code>
適用於RPCSEC_GSS和AUTH_SYS	<code>vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled</code>

3. 驗證 `-extended-groups-limit` 並驗證 `AUTH_SYS` 是否使用延伸群組：`vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`

4. 返回管理權限層級：

```
set -privilege admin
```

#### 範例

下列範例可啟用`AUTH_SYS`驗證的延伸群組、並將`AUTH_SYS`和`RPCSEC_GSS`驗證的延伸群組數目上限設為512。這些變更僅適用於存取名為`VS1`的SVM的用戶端：

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
        them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
-----
vs1      enabled                      512

vs1::*> set -privilege admin
```

## 控制root使用者對NTFS安全型資料的存取

您可以設定ONTAP 讓NFS用戶端存取NTFS安全型資料和NTFS用戶端、以存取NFS安全型資料。在NFS資料儲存區上使用NTFS安全樣式時、您必須決定如何處理root使用者的存取、並據此設定儲存虛擬機器（SVM）。

關於這項工作

當root使用者存取NTFS安全型資料時、您有兩種選擇：

- 將root使用者對應至Windows使用者、就像任何其他NFS使用者一樣、並根據NTFS ACL來管理存取。
- 忽略NTFS ACL並提供root的完整存取權。

#### 步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 執行所需的動作：

如果您希望root使用者...	輸入命令...
對應至Windows使用者	<code>vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled</code>
略過NT ACL檢查	<code>vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled</code>

預設會停用此參數。

如果啟用此參數、但root使用者沒有名稱對應、ONTAP 則使用預設的SMB系統管理員認證來進行稽核。

3. 返回管理權限層級：

```
set -privilege admin
```

## 版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

## 商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。