管理 **NFS**

ONTAP 9

NetApp
January 08, 2026

目錄

管理 NFS

了解 NFS 協定的 ONTAP 檔案訪問

包含NFS傳輸協定可用的檔案存取功能。ONTAP您可以啟用NFS伺服器並匯出Volume或qtree。

您可在下列情況下執行這些程序：

- 您想要瞭解ONTAP 各種不同的NFS傳輸協定功能。
- 您想要執行較不常見的組態和維護工作、而非基本NFS組態。
- 您想要使用命令列介面（CLI）、而非System Manager或自動化指令碼工具。

瞭解NAS檔案存取

命名空間和交會點

了解 ONTAP NAS 命名空間和連接點

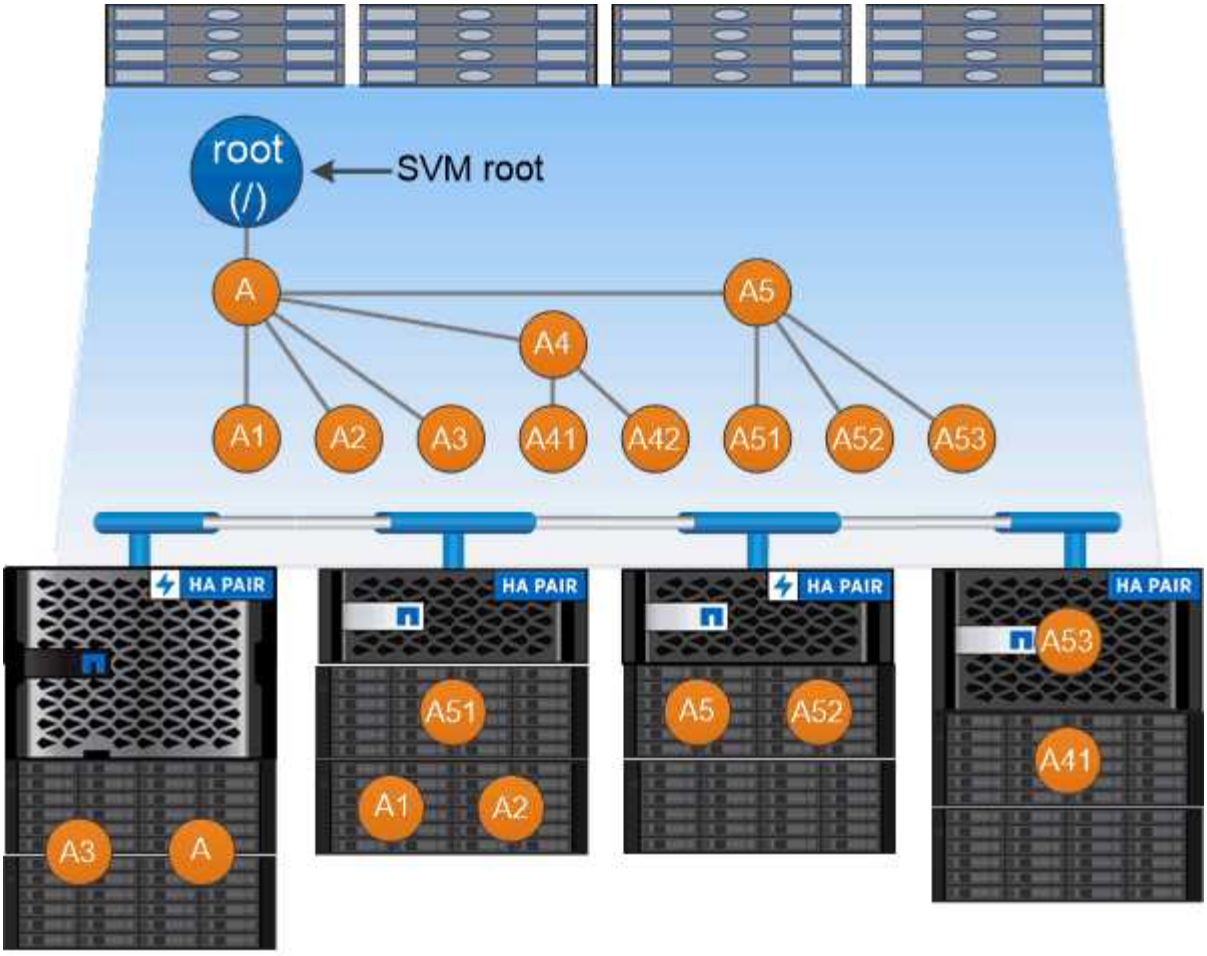
NAS *namespacity*_是一個邏輯群組、集合在_交會點、以建立單一檔案系統階層架構。具有足夠權限的用戶端可存取命名空間中的檔案、而無需指定檔案在儲存設備中的位置。未分段的磁碟區可位於叢集中的任何位置。

NAS用戶端不會掛載每個包含感興趣檔案的磁碟區、而是掛載NFS _EX出口_或存取SMB共享區。_匯出或共用區代表整個命名空間或命名空間內的中繼位置。用戶端只會存取裝載於其存取點下方的磁碟區。

您可以視需要將磁碟區新增至命名空間。您可以直接在父磁碟區交會下方或磁碟區內的目錄上建立交會點。名稱為「 'vol3' 」的 Volume 交會路徑可能是 `/vol1/vol2/vol3`或 `/vol1/dir2/vol3`或甚至 `/dir1/dir2/vol3`。路徑稱為_junction路徑。_

每個SVM都有一個獨特的命名空間。SVM根磁碟區是命名空間階層架構的起點。

> 為了確保資料在節點中斷或容錯移轉的情況下仍然可用、您應該為SVM根磁碟區建立_load-sharing mirror _複本。



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

範例

以下範例建立一個名為「 'home4' 」的 Volume 、該 Volume 位於 SVM VS1 上、且具有交會路徑 `/eng/home` ：

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

了解 **ONTAP NAS** 命名空間架構

您可以在建立SVM名稱空間時、使用幾種典型的NAS命名空間架構。您可以選擇符合業務和工作流程需求的命名空間架構。

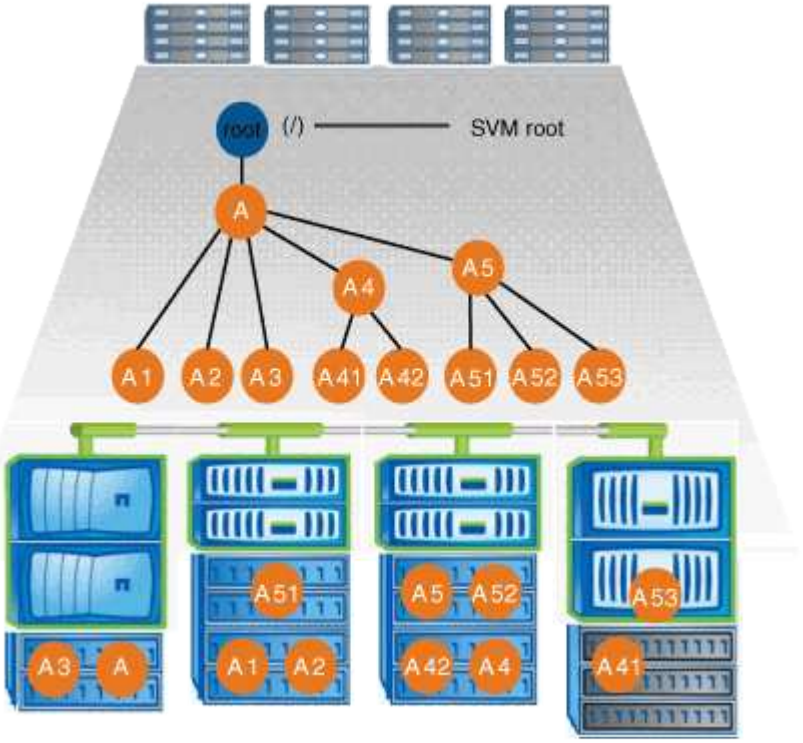
命名空間的頂端永遠是根磁碟區、以斜槓（/）表示。根目錄下的命名空間架構可分為三個基本類別：

- 單一分支樹狀結構、只有一個連接點可連接至命名空間的根
- 多個分支樹狀結構、並有多個交會點指向命名空間的根目錄

- 多個獨立磁碟區、每個磁碟區都有一個指向名稱空間根的獨立交會點

具有單一分支樹狀結構的命名空間

具有單一分支樹狀結構的架構具有單一插入點、可插入SVM命名空間的根目錄。單一插入點可以是輔助磁碟區、也可以是根目錄下的目錄。所有其他磁碟區都會安裝在單一插入點下方的交會點（可以是磁碟區或目錄）。

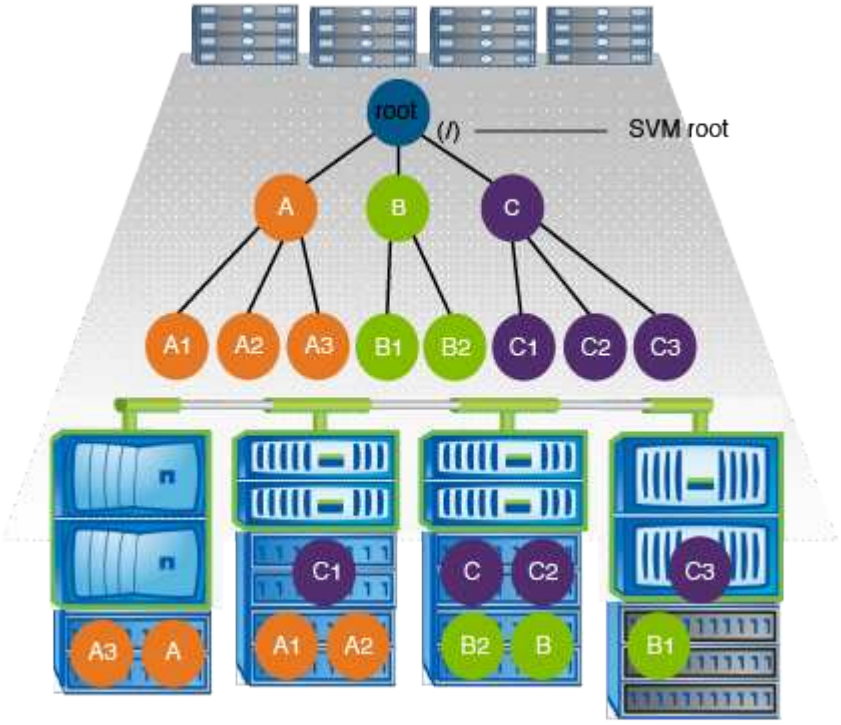


例如、具有上述命名空間架構的典型Volume交會組態可能類似下列組態、其中所有磁碟區都會連結到單一插入點下方、亦即名為「data'」的目錄：

```
                    Junction                          Junction
Vserver Volume      Active   Junction Path            Path Source
------- ----------- -------- -------------------      -----------
vs1     corp1       true     /data/dir1/corp1         RW_volume
vs1     corp2       true     /data/dir1/corp2         RW_volume
vs1     data1       true     /data/data1              RW_volume
vs1     eng1        true     /data/data1/eng1         RW_volume
vs1     eng2        true     /data/data1/eng2         RW_volume
vs1     sales       true     /data/data1/sales        RW_volume
vs1     vol1        true     /data/vol1               RW_volume
vs1     vol2        true     /data/vol2               RW_volume
vs1     vol3        true     /data/vol3               RW_volume
vs1     vs1_root    -        /                        -
```

具有多個分支樹狀結構的命名空間

具有多個分支樹狀結構的架構具有多個插入點、可插入到SVM命名空間的根目錄。插入點可以是輔助磁碟區、也可以是根目錄下的目錄。所有其他磁碟區都會安裝在插入點下方的交會點（可以是磁碟區或目錄）。

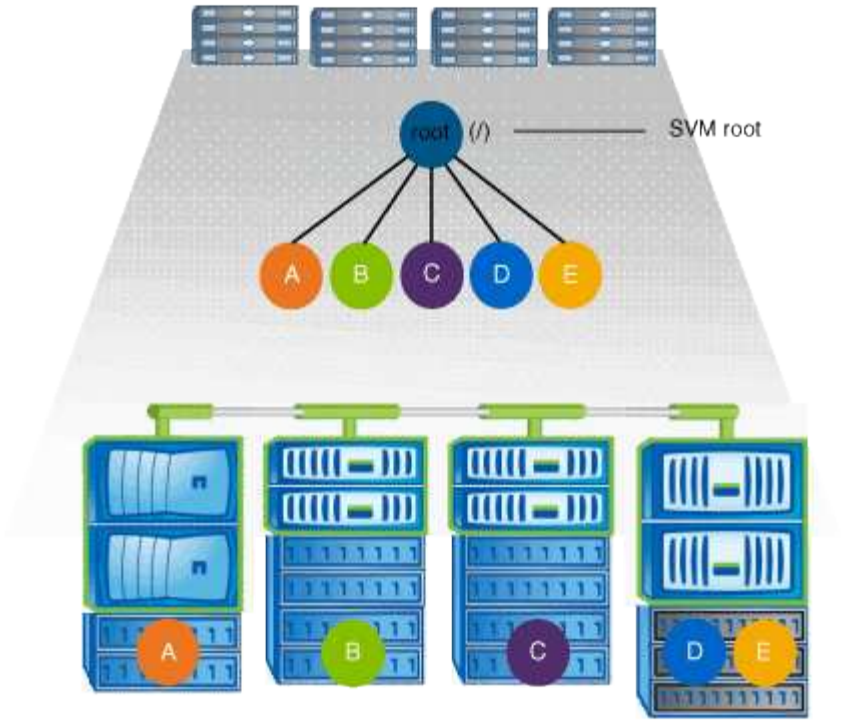


例如、具有上述命名空間架構的典型Volume交會組態可能類似下列組態、其中有三個插入點可插入SVM的根Volume。兩個插入點是名為「dATA」和「專案」的目錄。其中一個插入點是名為「稽核」的輔助磁碟區：

```
                    Junction                          Junction
Vserver Volume      Active   Junction Path            Path Source
------- ----------- -------- -------------------      -----------
vs1     audit       true     /audit                   RW_volume
vs1     audit_logs1 true     /audit/logs1             RW_volume
vs1     audit_logs2 true     /audit/logs2             RW_volume
vs1     audit_logs3 true     /audit/logs3             RW_volume
vs1     eng         true     /data/eng                RW_volume
vs1     mktg1       true     /data/mktg1              RW_volume
vs1     mktg2       true     /data/mktg2              RW_volume
vs1     project1    true     /projects/project1       RW_volume
vs1     project2    true     /projects/project2       RW_volume
vs1     vs1_root    -        /                        -
```

具有多個獨立磁碟區的命名空間

在具有獨立磁碟區的架構中、每個磁碟區都有一個插入點、指向SVM命名空間的根目錄、但是該磁碟區並未與另一個磁碟區連結。每個磁碟區都有一個獨特的路徑、可以直接連接到根目錄下方、也可以連接到根目錄下方的目錄下。



例如、具有上述命名空間架構的典型Volume交會組態可能類似下列組態、其中有五個插入點指向SVM的根Volume、每個插入點代表一個Volume的路徑。

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- --------------------   -----------
vs1     eng         true     /eng                   RW_volume
vs1     mktg        true     /vol/mktg              RW_volume
vs1     project1    true     /project1              RW_volume
vs1     project2    true     /project2              RW_volume
vs1     sales       true     /sales                 RW_volume
vs1     vs1_root    -        /                      -
```

如何控制對檔案的存取ONTAP

了解 **ONTAP NAS** 檔案存取控制

根據您指定的驗證型和檔案型限制、支援對檔案的存取。ONTAP

當用戶端連線至儲存系統以存取檔案時ONTAP 、必須執行兩項工作：

- 驗證

  透過驗證信任來源的身分識別、即可驗證用戶端。ONTAP此外、用戶端的驗證類型是一種方法、可用來判斷用戶端在設定匯出原則時是否能存取資料（CIFS為選用）。

- 授權

透過比較使用者的認證資料與檔案或目錄上設定的權限、以及決定要提供的存取類型（如果有）、即可授權使用者。ONTAP

為了妥善管理檔案存取控制、ONTAP 必須與外部服務（例如NIS、LDAP和Active Directory伺服器）通訊。若要使用CIFS或NFS設定檔案存取的儲存系統、必須視ONTAP 您的環境而定、設定適當的服務。

了解 **ONTAP NAS SVM** 基於身份驗證的限制

有了驗證型限制、您可以指定哪些用戶端機器、以及哪些使用者可以連線至儲存虛擬機器（SVM）。

支援UNIX和Windows伺服器的Kerberos驗證。ONTAP

了解 **ONTAP NAS SVM** 的基於檔案的限制

此功能可評估三種安全層級、以判斷實體是否有權針對位於SVM上的檔案和目錄執行要求的動作。ONTAP存取權取決於評估三種安全層級後的有效權限。

任何儲存物件最多可包含三種類型的安全層：

- 匯出（NFS）和共用（SMB）安全性

  匯出及共用安全性適用於用戶端存取特定NFS匯出或SMB共用區。具有管理權限的使用者可以從SMB和NFS用戶端管理匯出和共用層級的安全性。

- 儲存層級的存取保護檔案和目錄安全性

  儲存層級的存取保護安全性適用於存取SVM磁碟區的SMB和NFS用戶端。僅支援NTFS存取權限。為了對UNIX使用者執行安全性檢查、以存取已套用Storage Level Access Guard的磁碟區上的資料、UNIX使用者必須對應至擁有該磁碟區的SVM上的Windows使用者。ONTAP

  > ⓘ 如果您從NFS或SMB用戶端檢視檔案或目錄的安全性設定、就不會看到儲存層級的存取保護安全性。即使是系統（Windows或UNIX）管理員、也無法從用戶端撤銷儲存層級的存取保護安全性。

- NTFS、UNIX及NFSv4原生檔案層級安全性

  代表儲存物件的檔案或目錄中存在原生檔案層級安全性。您可以從用戶端設定檔案層級的安全性。無論使用SMB或NFS存取資料、檔案權限都有效。

ONTAP 如何處理 NFS 用戶端驗證

了解 **NAS** 用戶端的 **ONTAP** 驗證

NFS用戶端必須經過適當驗證、才能存取SVM上的資料。利用您所設定的名稱服務來檢查UNIX認證、藉此驗證用戶端。ONTAP

當NFS用戶端連線至SVM時、ONTAP 根據SVM的名稱服務組態、透過檢查不同的名稱服務來取得使用者的UNIX認證。可檢查本機UNIX帳戶、NIS網域及LDAP網域的認證資料。ONTAP至少必須設定其中一

項、ONTAP 才能讓支援中心成功驗證使用者。您可以指定多個名稱服務及ONTAP 其搜尋順序。

在純NFS環境中使用UNIX Volume安全性樣式、此組態足以驗證並為從NFS用戶端連線的使用者提供適當的檔案存取。

如果您使用混合、NTFS或統一磁碟區安全樣式、ONTAP 則必須為UNIX使用者取得SMB使用者名稱、才能使用Windows網域控制器進行驗證。這可能是因為使用本機UNIX帳戶或LDAP網域來對應個別使用者、或改用預設的SMB使用者。您可以指定ONTAP 名稱服務以何種順序搜尋、或指定預設的SMB使用者。

了解 **ONTAP** 如何使用名稱服務

使用名稱服務取得使用者和用戶端的相關資訊。ONTAP使用此資訊驗證使用者存取或管理儲存系統上的資料、並在混合式環境中對應使用者認證資料。ONTAP

當您設定儲存系統時、必須指定ONTAP 要使用哪些名稱服務來取得使用者認證以進行驗證。支援下列名稱服務：ONTAP

- 本機使用者（檔案）
- 外部NIS網域（NIS）
- 外部 LDAP 網域（ LDAP ）

您可以使用 `vserver services name-service ns-switch` 命令系列可將 SVM 設定為使用來源來搜尋網路資訊、以及搜尋這些資訊的順序。這些命令可提供的等效功能 `/etc/nsswitch.conf` UNIX 系統上的檔案。

當NFS用戶端連線至SVM時、ONTAP 此功能會檢查指定的名稱服務、以取得使用者的UNIX認證資料。如果名稱服務設定正確、ONTAP 而且能夠取得UNIX認證資料、ONTAP 則無法成功驗證使用者。

在混合式安全型態的環境中ONTAP 、可能必須對應使用者認證資料。您必須針對環境適當設定名稱服務、以便ONTAP 讓支援功能能夠正確對應使用者認證資料。

此外、還會使用名稱服務來驗證SVM系統管理員帳戶。ONTAP在設定或修改名稱服務交換器時、您必須謹記此點、以免意外停用SVM系統管理員帳戶的驗證。如需SVM管理使用者的詳細資訊、請參閱 "系統管理員驗證與RBAC"。

授予從 **NFS** 用戶端存取 **ONTAP SMB** 檔案的權限

使用Windows NT檔案系統（NTFS）安全性語意、判斷UNIX使用者是否能在NFS用戶端上存取具有NTFS權限的檔案。ONTAP

為達成此目的、可將使用者的UNIX使用者ID（UID）轉換成SMB認證、然後使用SMB認證來驗證使用者是否擁有檔案的存取權限。ONTAPSMB認證包含主要安全性識別碼（SID）、通常是使用者的Windows使用者名稱、以及對應於使用者所屬Windows群組的一或多個群組SID。

將UNIX UID轉換為SMB認證所需的時間ONTAP 可從數十毫秒轉換為數百毫秒、因為此程序涉及連絡網域控制器。此功能可將UID對應至SMB認證、並在認證快取中輸入對應、以縮短轉換所造成的驗證時間。ONTAP

ONTAP NFS 憑證快取的工作原理

當NFS使用者要求存取儲存系統上的NFS匯出時、ONTAP 必須從外部名稱伺服器或從本機檔案擷取使用者認證資料、才能驗證使用者。然後將這些認證資料儲存在內部認證快取

中、以供日後參考。ONTAP瞭解NFS認證快取的運作方式、可讓您處理潛在的效能和存取問題。

如果沒有認證快取、ONTAP 每當NFS使用者要求存取時、就必須查詢名稱服務。在許多使用者存取的忙碌儲存系統上、這很快就會導致嚴重的效能問題、造成不必要的延遲、甚至使NFS用戶端存取遭到拒絕。

利用認證快取功能、ONTAP 當NFS用戶端傳送另一個要求時、將會擷取使用者認證資料、然後儲存預先決定的時間量、以便快速輕鬆地存取。此方法具有下列優點：

- 它可處理較少的外部名稱伺服器（例如NIS或LDAP）要求、進而減輕儲存系統的負載。
- 它能減少傳送要求給外部名稱伺服器的次數、進而減輕其負載。
- 它可免除從外部來源取得認證的等待時間、以便驗證使用者、進而加速使用者存取。

支援將正面和負面的認證資料儲存在認證快取中。ONTAP正向認證表示使用者已通過驗證並獲得存取權。負面認證表示使用者未通過驗證、因此被拒絕存取。

根據預設、ONTAP 將正向認證資料儲存24小時；也就是ONTAP 在初始驗證使用者之後、將快取認證資料用於該使用者24小時內的任何存取要求。如果使用者在24小時後要求存取、週期就會開始：ONTAP 由下列項目開始：循環捨棄快取的認證資料、並從適當的名稱服務來源再次取得認證資料。如果在過去24小時內、名稱伺服器上的認證有所變更、ONTAP 則會快取更新的認證資料、以供未來24小時使用。

根據預設、ONTAP 功能不正常的情況下、將負面認證資料儲存兩小時；也就是ONTAP 在一開始拒絕使用者存取之後、該使用者在兩小時內仍拒絕任何存取要求。如果使用者在2小時後要求存取、則週期將從下列項目開始：ONTAP 再次從適當的名稱服務來源取得認證。如果在過去兩小時內、名稱伺服器上的認證資料有所變更、ONTAP 則會快取更新的認證資料、以供未來兩小時使用。

在NAS命名空間中建立及管理資料磁碟區

使用指定的連接點建立 ONTAP NAS 卷

您可以在建立資料Volume時指定交會點。結果Volume會自動掛載於交會點、並可立即設定以進行NAS存取。

開始之前

- 您要在其中建立磁碟區的集合體必須已經存在。
- 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。

> 下列字元無法用於連接路徑： `* # " > < | ? \`

此外、交會路徑長度不得超過255個字元。

步驟

1. 建立具有交會點的Volume：

```
volume create -vserver <vserver_name> -volume <volume_name> -aggregate
<aggregate_name> -size {integer[KB|MB|GB|TB|PB]} -security-style
{ntfs|unix|mixed} -junction-path <junction_path>
```

交會路徑必須以根（/）開頭、且可同時包含目錄和輔助磁碟區。交會路徑不需要包含磁碟區名稱。交會路徑與磁碟區名稱無關。

指定Volume安全樣式為選用項目。如果您未指定安全樣式、ONTAP 則會以套用至儲存虛擬機器（SVM）根磁碟區的相同安全樣式來建立磁碟區。不過、根磁碟區的安全樣式可能不是您要套用至所建立資料磁碟區的安全樣式。建議您在建立磁碟區時指定安全樣式、以將難以疑難排解的檔案存取問題降至最低。

接合路徑不區分大小寫； `/ENG` 與相同 `/eng`。如果您建立CIFS共用區、Windows會將交會路徑視為區分大小寫。例如、如果交會是 `/ENG`， SMB 共享的路徑必須以開頭 `/ENG`、不是 `/eng`。

您可以使用許多選用參數來自訂資料Volume。如"指令參考資料ONTAP"需詳細 `volume create`資訊，請參閱。

2. 確認已使用所需的交會點建立磁碟區：

```
volume show -vserver <vserver_name> -volume <volume_name> -junction
```

範例

以下範例建立一個名為 SVM VS1 的磁碟區，該磁碟區 `home4`**具有連接路徑** `/eng/home`：

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

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

建立沒有特定連接點的 **ONTAP NAS** 卷

您可以建立資料Volume而不指定交會點。結果Volume不會自動掛載、也無法設定NAS存取。您必須先掛載磁碟區、才能設定該磁碟區的SMB共用區或NFS匯出。

開始之前

- 您要在其中建立磁碟區的集合體必須已經存在。
- 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. 使用下列命令建立沒有交會點的磁碟區：

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate
   aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
   {ntfs|unix|mixed}
   ```

   指定Volume安全樣式為選用項目。如果您未指定安全樣式、ONTAP 則會以套用至儲存虛擬機器（SVM）根磁碟區的相同安全樣式來建立磁碟區。不過、根磁碟區的安全樣式可能不是您要套用到資料磁碟區的安全樣式。建議您在建立磁碟區時指定安全樣式、以將難以疑難排解的檔案存取問題降至最低。

   您可以使用許多選用參數來自訂資料Volume。如"指令參考資料ONTAP"需詳細 `volume create`資訊，請參閱。

2. 驗證是否在沒有連接點的情況下建立磁碟區：

   ```
   volume show -vserver vserver_name -volume volume_name -junction
   ```

範例

下列範例建立名為「shes」的磁碟區、位於SVM VS1上、但未掛載於交會點：

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      -        -               -
```

在 NAS 命名空間中掛載或卸載 ONTAP NFS 卷

磁碟區必須先掛載到NAS命名空間、才能設定NAS用戶端存取儲存虛擬機器（SVM）磁碟區中所含的資料。如果目前未掛載磁碟區、您可以將其掛載至交會點。您也可以卸載Volume。

關於這項工作

如果您卸載磁碟區並使其離線、則 NAS 用戶端無法存取連接點內的所有資料、包括位於未掛載磁碟區命名空間內具有連接點的磁碟區中的資料。

> 若要停止NAS用戶端對磁碟區的存取、只是卸載磁碟區是不夠的。您必須將磁碟區離線、或採取其他步驟、確保用戶端檔案處理快取無效。如需詳細資訊、請參閱下列知識庫文章：
>
> "NFSv3用戶端在從ONTAP 靜態命名空間移除後、仍可存取Volume"

當您卸載磁碟區並離線時、磁碟區內的資料不會遺失。此外、在磁碟區或未掛載磁碟區內的目錄和交會點上建立的現有磁碟區匯出原則和SMB共用也會保留下來。如果您重新掛載未掛載的Volume、NAS用戶端可以使用現有的匯出原則和SMB共用來存取磁碟區內的資料。

步驟

1. 執行所需的動作：

如果您想要...	輸入命令...
掛載Volume	`volume mount -vserver svm_name -volume volume_name -junction-path junction_path`

卸載Volume	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. 驗證磁碟區是否處於所需的掛載狀態：

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

範例

以下範例將位於 SVM 'VS1' 的名為 """""""s'" 的 Volume 裝入連接點 "'/sales" ：

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

以下範例將卸載並離線位於 SVM 「'VS1 」上的名為「 dATA 」的磁碟區：

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

顯示 **ONTAP NAS Volume** 裝載和交會點資訊

您可以顯示儲存虛擬機器（SVM）掛載磁碟區的相關資訊、以及掛載磁碟區的交會點。您也可以決定哪些磁碟區未掛載到交會點。您可以使用此資訊來瞭解及管理SVM命名空間。

步驟

1. 執行所需的動作：

如果您要顯示…	輸入命令…
SVM上掛載與卸載磁碟區的摘要資訊	`volume show -vserver` *`vserver_name`* `-junction`
SVM上掛載與卸載磁碟區的詳細資訊	`volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-instance`
有關SVM上掛載和卸載磁碟區的特定資訊	a. 如有必要、您可以顯示的有效欄位 `-fields` 使用下列命令的參數： `volume show -fields ?` b. 使用顯示所需資訊 `-fields` 參數： `volume show -vserver` *`vserver_name`* `-fields` *`fieldname`*`,…`

範例

下列範例顯示SVM VS1上掛載與卸載磁碟區的摘要：

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

下列範例顯示SVM VS2上磁碟區的指定欄位資訊：

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

設定安全樣式

安全樣式如何影響資料存取

了解 **ONTAP NAS** 安全模式

共有四種不同的安全型態：UNIX、NTFS、混合式及統一化。每種安全樣式對資料權限的處理方式都有不同的影響。您必須瞭解不同的影響、以確保為您的目的選擇適當的安全型

態。

請務必瞭解、安全樣式並未決定哪些用戶端類型可以或無法存取資料。安全樣式只會決定ONTAP 用來控制資料存取的權限類型、以及哪些用戶端類型可以修改這些權限。

例如、如果某個磁碟區使用UNIX安全型態、則SMB用戶端仍可存取資料（前提是他們必須正確驗證及授權）、因為ONTAP 此為多重傳輸協定的本質。不過ONTAP 、VMware使用UNIX權限、只有UNIX用戶端可以使用原生工具進行修改。

安全風格	可以修改權限的用戶端	用戶端可以使用的權限	打造出有效的安全風格	可存取檔案的用戶端
UNIX	NFS	NFSv3模式位元	UNIX	NFS與SMB
		NFSv4.x ACL		
NTFS	中小企業	NTFS ACL	NTFS	
混合	NFS或SMB	NFSv3模式位元	UNIX	
		NFSv4.ACL		
		NTFS ACL	NTFS	
統一化 （僅適用於Infinite Volume 、ONTAP 9.4 及更早版本。）	NFS或SMB	NFSv3模式位元	UNIX	
		NFSv4.1 ACL		
		NTFS ACL	NTFS	

支援UNIX、NTFS和混合式安全型態的支援。FlexVol當安全性樣式混合或統一化時、有效權限取決於上次修改權限的用戶端類型、因為使用者是個別設定安全性樣式。如果上次修改權限的用戶端是NFSv3用戶端、則權限為UNIX NFSv3模式位元。如果最後一個用戶端是NFSv4用戶端、則權限為NFSv4 ACL。如果最後一個用戶端是SMB用戶端、則權限為Windows NTFS ACL。

統一化的安全風格僅適用於無限個Volume、ONTAP 而不再支援於更新版本的版本。如需詳細資訊、請參閱 介紹Volume管理總覽FlexGroup。

這 `show-effective-permissions`參數 `vserver security file-directory`命令可讓您顯示授予 Windows 或 UNIX 使用者在指定檔案或資料夾路徑上的有效權限。此外，選用參數 `-share-name`可讓您顯示有效共用權限。如"指令參考資料ONTAP"需詳細 `vserver security file-directory show-effective-permissions`資訊，請參閱。

> 最初設定部分預設檔案權限。ONTAP根據預設、UNIX、混合式及統一化安全樣式磁碟區中所有資料的有效安全樣式為UNIX、有效權限類型為UNIX模式位元（0755、除非另有說明）、直到用戶端依照預設安全性樣式所允許的方式進行設定為止。根據預設、NTFS安全型磁碟區中所有資料的有效安全樣式為NTFS、並具有ACL、可讓所有人完全掌控。

相關資訊

- "指令參考資料ONTAP"

了解 **ONTAP NFS FlexVol** 磁碟區的安全模式

安全樣式可在FlexVol 支援樹狀結構（根或資料磁碟區）和qtree上設定。安全樣式可在建立時手動設定、自動繼承或稍後變更。

確定在 **ONTAP NAS SVM** 上使用哪種安全模式

為了協助您決定要在磁碟區上使用哪種安全樣式、您應該考慮兩個因素。主要因素是管理檔案系統的系統管理員類型。次要因素是存取磁碟區上資料的使用者或服務類型。

在Volume上設定安全樣式時、您應該考慮環境的需求、以確保您選擇最佳的安全樣式、並避免管理權限時發生問題。下列考量事項可協助您決定：

安全風格	選擇是否…
UNIX	• 檔案系統由UNIX管理員管理。 • 大多數使用者是NFS用戶端。 • 存取資料的應用程式會使用UNIX使用者做為服務帳戶。
NTFS	• 檔案系統由Windows管理員管理。 • 大多數使用者是 SMB 用戶端。 • 存取資料的應用程式會使用Windows使用者做為服務帳戶。
混合	• 檔案系統由UNIX和Windows系統管理員管理、使用者同時由NFS和SMB用戶端組成。

瞭解 **ONTAP NFS** 安全風格的繼承

如果您在建立新FlexVol 的流通量或qtree時未指定安全樣式、它會以不同的方式繼承其安全風格。

安全樣式會以下列方式繼承：

- 此功能會繼承包含SVM的根磁碟區安全樣式。FlexVol
- qtree會繼承其包含FlexVol 的不穩定區的安全樣式。
- 檔案或目錄會繼承其包含FlexVol 的不穩定磁碟區或qtree的安全樣式。

了解 **ONTAP NFS UNIX** 權限保留

當Windows應用程式編輯並儲存目前具有UNIX權限的FlexVol 檔案時ONTAP 、即可保留UNIX權限。

當Windows用戶端上的應用程式編輯及儲存檔案時、他們會讀取檔案的安全性內容、建立新的暫存檔、將這些內容套用至暫存檔、然後為暫存檔提供原始檔案名稱。

當Windows用戶端執行安全性內容查詢時、會收到完全代表UNIX權限的建構ACL。此建構ACL的唯一目的是在Windows應用程式更新檔案時、保留檔案的UNIX權限、以確保產生的檔案具有相同的UNIX權限。不使用建構的ACL來設定任何NTFS ACL。ONTAP

如果您想要在混合式安全型磁碟區或SVM上的qtree中、處理檔案或資料夾的UNIX權限、可以使用Windows用戶端上的「安全性」索引標籤。或者、您也可以使用可查詢及設定Windows ACL的應用程式。

- 修改UNIX權限

  您可以使用「Windows安全性」索引標籤來檢視及變更混合式安全性型磁碟區或qtree的UNIX權限。如果您使用Windows安全性主索引標籤來變更UNIX權限、則必須先移除您要編輯的現有ACE（這會將模式位元設為0）、才能進行變更。或者、您也可以使用進階編輯器來變更權限。

  如果使用模式權限、您可以直接變更所列的UID、GID和其他（電腦上有帳戶的其他人）的模式權限。例如、如果顯示的UID具有r-x權限、您可以將UID權限變更為rwx。

- 將UNIX權限變更為NTFS權限

  您可以使用「Windows安全性」索引標籤、將UNIX安全性物件取代為混合式安全性型磁碟區或qtree上的Windows安全性物件、其中檔案和資料夾具有UNIX有效的安全性樣式。

  您必須先移除所有列出的UNIX權限項目、才能將其取代為所需的Windows使用者和群組物件。然後您可以在Windows使用者和群組物件上設定NTFS型ACL。只要移除所有UNIX安全性物件、並將Windows使用者和群組新增至混合式安全性型磁碟區或qtree中的檔案或資料夾、即可將檔案或資料夾上的有效安全性樣式從UNIX變更為NTFS。

  變更資料夾的權限時、預設的Windows行為是將這些變更傳播到所有子資料夾和檔案。因此、如果您不想將安全性樣式的變更傳播到所有子資料夾、子資料夾和檔案、則必須將傳播選項變更為所需的設定。

在 **ONTAP NFS SVM** 根磁碟區上設定安全模式

您可以設定儲存虛擬機器（SVM）根磁碟區安全樣式、以決定SVM根磁碟區上資料所使用的權限類型。

步驟

1. 使用 `vserver create` 命令 `-rootvolume-security-style` 定義安全樣式的參數。

   根 Volume 安全樣式的可能選項為 `unix`、 `ntfs`或 `mixed`。

2. 顯示並驗證組態、包括您所建立SVM的根磁碟區安全樣式：

   `vserver show -vserver` *`vserver_name`*

在 **ONTAP NFS FlexVol** 磁碟區上設定安全樣式

您可以設定FlexVol 「靜態Volume」安全樣式、以判斷FlexVol 儲存虛擬機器（SVM）的各個版本上的資料所使用的權限類型。

步驟

1. 執行下列其中一項動作：

如果FlexVol 是這個問題…	使用命令…
尚不存在	`volume create` 並包含 `-security-style` 指定安全樣式的參數。
已存在	`volume modify` 並包含 `-security-style` 指定安全樣式的參數。

FlexVol Volume 安全樣式的可能選項為 `unix`、 `ntfs`或 `mixed`。

如果您在建立FlexVol 一個穩定區時未指定安全樣式、則此磁碟區會繼承根磁碟區的安全樣式。

如需更多關於的資訊、請參閱 `volume create` 或 `volume modify` 命令、請參閱 "邏輯儲存管理"。

2. 若要顯示組態、包括FlexVol 您所建立的穩定功能、請輸入下列命令：

```
volume show -volume volume_name -instance
```

在 ONTAP NFS qtree 上設定安全模式

您可以設定qtree Volume安全樣式、以決定用於qtree上資料的權限類型。

步驟

1. 執行下列其中一項動作：

如果qtree …	使用命令…
尚未存在	`volume qtree create` 並包含 `-security-style` 指定安全樣式的參數。
已存在	`volume qtree modify` 並包含 `-security-style` 指定安全樣式的參數。

qtree 安全樣式的可能選項為 `unix`、 `ntfs`或 `mixed`。

如果在建立 qtree 時未指定安全樣式、則預設的安全樣式為 `mixed`。

如需更多關於的資訊、請參閱 `volume qtree create` 或 `volume qtree modify` 命令、請參閱 "邏輯儲存管理"。

2. 若要顯示組態、包括您建立的 qtree 安全樣式、請輸入下列命令： `volume qtree show -qtree` *`qtree_name`* `-instance`

使用 NFS 設定檔案存取

了解如何在 ONTAP SVM 上設定 NFS 檔案訪問

您必須完成許多步驟、才能讓用戶端使用NFS存取儲存虛擬機器（SVM）上的檔案。根據您環境的目前組態、還有一些額外的選用步驟。

若要讓用戶端能夠使用NFS存取SVM上的檔案、您必須完成下列工作：

1. 在SVM上啟用NFS傳輸協定。

   您必須設定SVM、以便透過NFS從用戶端存取資料。

2. 在SVM上建立NFS伺服器。

   NFS伺服器是SVM上的邏輯實體、可讓SVM透過NFS提供檔案服務。您必須建立NFS伺服器、並指定您要允許的NFS傳輸協定版本。

3. 在SVM上設定匯出原則。

   您必須設定匯出原則、讓用戶端可使用磁碟區和qtree。

4. 視網路和儲存環境而定、使用適當的安全性和其他設定來設定NFS伺服器。

   此步驟可能包括設定Kerberos、LDAP、NIS、名稱對應及本機使用者。

使用匯出原則保護**NFS**存取安全

導出策略如何控制用戶端對 **ONTAP NFS** 磁碟區或 **qtree** 的存取

匯出原則包含一或多個用以處理每個用戶端存取要求的_EXPORT規則_。此程序的結果決定了用戶端是被拒絕還是被授予存取權限、以及存取層級。儲存虛擬機器（SVM）上必須存在具有匯出規則的匯出原則、用戶端才能存取資料。

您只需將一個匯出原則與每個Volume或qtree建立關聯、即可設定用戶端對Volume或qtree的存取。SVM可包含多個匯出原則。這可讓您針對具有多個磁碟區或qtree的SVM執行下列作業：

- 為SVM的每個Volume或qtree指派不同的匯出原則、以便個別用戶端存取控制到SVM中的每個Volume或qtree。
- 將相同的匯出原則指派給SVM的多個磁碟區或qtree、以獲得相同的用戶端存取控制、而不需要為每個磁碟區或qtree建立新的匯出原則。

如果用戶端提出的存取要求不受適用的匯出原則允許、則要求會以拒絕權限的訊息失敗。如果用戶端不符合匯出原則中的任何規則、則會拒絕存取。如果匯出原則是空的、則所有存取都會隱含拒絕。

您可以在執行ONTAP 不正常運作的系統上動態修改匯出原則。

ONTAP NFS SVM 的預設導出策略

每個SVM都有一個預設匯出原則、不含任何規則。用戶端必須先存在具有規則的匯出原則、才能存取SVM上的資料。SVM中包含的每FlexVol 個SVM磁碟區都必須與匯出原則相關聯。

建立 SVM 時、儲存系統會自動建立名為的預設匯出原則 `default` 適用於 SVM 的根 Volume 。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。或者、您也可以建立具有規則的自訂匯出原則。您可以修改及重新命名預設匯出原則、但無法刪除預設匯出原則。

當您在FlexVol 包含SVM的磁碟區中建立一個SVM時、儲存系統會建立該磁碟區、並將該磁碟區與SVM根磁碟區的預設匯出原則建立關聯。根據預設、在SVM中建立的每個Volume都會與根Volume的預設匯出原則相關聯。您可以針對SVM中包含的所有磁碟區使用預設匯出原則、也可以針對每個磁碟區建立唯一的匯出原則。您可以將多個磁碟區與相同的匯出原則建立關聯。

ONTAP NFS 導出規則的工作原理

匯出規則是匯出原則的功能要素。匯出規則會根據您設定的特定參數、將用戶端存取要求與磁碟區相符、以決定如何處理用戶端存取要求。

匯出原則必須包含至少一個匯出規則、才能允許存取用戶端。如果匯出原則包含多個規則、則會依照規則在匯出原則中的顯示順序來處理這些規則。規則順序由規則索引編號決定。如果規則符合用戶端、則會使用該規則的權限、而且不會再處理其他規則。如果沒有符合的規則、用戶端就會被拒絕存取。

您可以使用下列準則來設定匯出規則、以決定用戶端存取權限：

- 傳送要求的用戶端所使用的檔案存取傳輸協定、例如NFSv4或SMB。
- 用戶端識別碼、例如主機名稱或IP位址。

  的最大大小 `-clientmatch` 欄位為 4096 個字元。

- 用戶端用來驗證的安全性類型、例如Kerberos v5, NTL,或AUTH_SYS。

如果規則指定多個準則、用戶端必須符合所有準則、才能套用規則。

> 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。

範例

匯出原則包含具有下列參數的匯出規則：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

用戶端存取要求是使用NFSv3傳輸協定傳送、用戶端的IP位址為10.1.17.37。

即使用戶端存取傳輸協定相符、用戶端的IP位址仍位於與匯出規則中指定的子網路不同的子網路中。因此、用戶端比對失敗、此規則不適用於此用戶端。

範例

匯出原則包含具有下列參數的匯出規則：

- `-protocol nfs`

- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

用戶端存取要求是使用NFSv4傳輸協定傳送、用戶端的IP位址為10.1.16.54。

用戶端存取傳輸協定相符、用戶端的IP位址位於指定的子網路中。因此、用戶端配對成功、此規則適用於此用戶端。無論用戶端的安全類型為何、都能取得讀寫存取權。

範例

匯出原則包含具有下列參數的匯出規則：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

用戶端#1的IP位址為10.1.16.207、使用NFSv3傳輸協定傳送存取要求、並使用Kerberos v5進行驗證。

用戶端#2的IP位址為10.1.16.211、使用NFSv3傳輸協定傳送存取要求、並透過AUTH_SYS進行驗證。

兩個用戶端的用戶端存取傳輸協定和IP位址都相符。唯讀參數允許所有用戶端的唯讀存取權、無論其驗證的安全類型為何。因此這兩個用戶端都能取得唯讀存取權。但是、只有用戶端#1會取得讀寫存取權、因為它使用核准的安全性類型Kerberos v5.x進行驗證。用戶端#2無法取得讀寫存取權。

管理具有未列出的安全性類型的 **NFS** 用戶端的 **ONTAP SVM** 訪問

當用戶端呈現未列在匯出規則存取參數中的安全性類型時、您可以選擇拒絕用戶端存取、或改用選項將其對應至匿名使用者 ID `none` 在存取參數中。

用戶端可能會出現未列在存取參數中的安全性類型、因為它是以不同的安全性類型驗證、或根本未驗證（安全性類型AUTH_NONE）。根據預設、用戶端會自動拒絕存取該層級。不過、您可以新增選項 `none` 存取參數。因此、具有未列出安全性樣式的用戶端會對應至匿名使用者ID。。 `-anon` 參數決定指派給這些用戶端的使用者 ID。為指定的使用者 ID `-anon` 參數必須是有效的使用者、且必須設定您認為適合匿名使用者的權限。

的有效值 `-anon` 參數範圍從 `0` 至 `65535`。

指派給的使用者 **ID** `-anon`	最終處理用戶端存取要求
`0 - 65533`	用戶端存取要求會對應至匿名使用者ID、並根據為此使用者設定的權限而取得存取權。
`65534`	用戶端存取要求會對應至使用者nobody、並根據為此使用者設定的權限而取得存取權。這是預設值。

指派給的使用者 **ID** `-anon`	最終處理用戶端存取要求
`65535`	任何用戶端的存取要求都會在對應至此ID時遭到拒絕、而用戶端會顯示安全性類型AUTH_NONE。當用戶ID為0的用戶端對應至此ID時、會拒絕該用戶端的存取要求、而用戶端會顯示任何其他安全類型。

使用選項時 `none`請務必記住、唯讀參數會先處理。針對未列出的安全性類型用戶端設定匯出規則時、請考慮下列準則：

唯讀包含 `none`	讀寫包括 `none`	產生未列出安全性類型之用戶端的存取權
否	否	已拒絕
否	是的	因為先處理唯讀而遭拒
是的	否	唯讀為匿名
是的	是的	匿名讀寫

範例

以下範例展示了一個出口策略，該策略包含： `-rwrule any` 範圍：

匯出原則包含具有下列參數的匯出規則：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

用戶端#1的IP位址為10.1.16.207、使用NFSv3傳輸協定傳送存取要求、並使用Kerberos v5進行驗證。

用戶端#2的IP位址為10.1.16.211、使用NFSv3傳輸協定傳送存取要求、並透過AUTH_SYS進行驗證。

用戶端#3的IP位址為10.1.16.234、使用NFSv3傳輸協定傳送存取要求、但未驗證（亦即安全性類型AUTH_NONE）。

這三個用戶端的用戶端存取傳輸協定和IP位址都相符。唯讀參數允許以驗證為AUTH_SYS的自有使用者ID來唯讀存取用戶端。唯讀參數允許匿名使用者以使用者ID 70的身分存取使用任何其他安全性類型驗證的用戶端。讀寫參數允許對任何安全類型進行讀寫存取、但在這種情況下、僅適用於已由唯讀規則篩選的用戶端。

因此、用戶端#1和#3只能以使用者ID 70的匿名使用者身分取得讀寫存取權。用戶端#2使用自己的使用者ID取得讀寫存取權。

以下範例展示了一個出口策略，該策略包含： `-rwrule none` 範圍：

匯出原則包含具有下列參數的匯出規則：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule none`
- `-anon 70`

用戶端#1的IP位址為10.1.16.207、使用NFSv3傳輸協定傳送存取要求、並使用Kerberos v5進行驗證。

用戶端#2的IP位址為10.1.16.211、使用NFSv3傳輸協定傳送存取要求、並透過AUTH_SYS進行驗證。

用戶端#3的IP位址為10.1.16.234、使用NFSv3傳輸協定傳送存取要求、但未驗證（亦即安全性類型AUTH_NONE）。

這三個用戶端的用戶端存取傳輸協定和IP位址都相符。唯讀參數允許以驗證為AUTH_SYS的自有使用者ID來唯讀存取用戶端。唯讀參數允許匿名使用者以使用者ID 70的身分存取使用任何其他安全性類型驗證的用戶端。讀寫參數只允許匿名使用者進行讀寫存取。

因此、用戶端#1和用戶端#3只能以使用者ID 70的匿名使用者身分取得讀寫存取權。用戶端#2使用自己的使用者ID取得唯讀存取權、但拒絕讀寫存取。

ONTAP 安全性類型如何決定 **NFS** 用戶端存取級別

用戶端驗證的安全性類型在匯出規則中扮演特殊角色。您必須瞭解安全性類型如何決定用戶端存取Volume或qtree的層級。

三種可能的存取層級如下：

1. 唯讀
2. 讀寫
3. 超級使用者（適用於使用者ID為0的用戶端）

由於依安全性類型評估存取層級的順序如下、因此在匯出規則中建構存取層級參數時、您必須遵守下列規則：

若要讓用戶端取得存取層級...	這些存取參數必須符合用戶端的安全類型...
一般使用者唯讀	唯讀 (`-rorule`)
一般使用者讀寫	唯讀 (`-rorule`) 和讀寫 (`-rwrule`)
超級使用者唯讀	唯讀 (`-rorule`) 和 `-superuser`
超級使用者讀寫	唯讀 (`-rorule`) 和讀寫 (`-rwrule`) 和 `-superuser`

以下是這三種存取參數的有效安全類型：

- any
- none
- never

  此安全性類型不適用於 -superuser 參數。

- krb5
- krb5i
- krb5p
- ntlm
- sys

將用戶端的安全類型與三個存取參數中的每個參數配對時、可能會產生三種結果：

如果用戶端的安全類型...	然後用戶端...
符合存取參數中指定的。	使用自己的使用者ID取得該層級的存取權。
與指定的不相符、但存取參數包含選項 none。	取得該層級的存取權、但以匿名使用者的身分、使用由指定的使用者 ID -anon 參數。
與指定的不相符、存取參數不包含選項 none。	無法取得該層級的任何存取權。這不適用於 -superuser 參數、因為它永遠包含在內 none 即使未指定、

範例

匯出原則包含具有下列參數的匯出規則：

- -protocol nfs3
- -clientmatch 10.1.16.0/255.255.255.0
- -rorule any
- -rwrule sys,krb5
- -superuser krb5

用戶端#1的IP位址為10.1.16.207、使用者ID為0、使用NFSv3傳輸協定傳送存取要求、並使用Kerberos v5進行驗證。

用戶端#2的IP位址為10.1.16.211、使用者ID為0、使用NFSv3傳輸協定傳送存取要求、並以AUTH_SYS驗證。

用戶端#3的IP位址為10.1.16.234、使用者ID為0、使用NFSv3傳輸協定傳送存取要求、但未驗證（AUTH_NONE）。

用戶端存取傳輸協定和IP位址符合這三個用戶端。唯讀參數允許所有用戶端的唯讀存取權、無論安全類型為何。讀寫參數允許以驗證為AUTH_SYS或Kerberos v5的用戶ID讀寫用戶端存取。超級使用者參數可讓超級使用者存取使用Kerberos v5驗證的用戶ID 0用戶端。

因此、用戶端#1會取得超級使用者讀寫存取權、因為它會符合所有三個存取參數。用戶端#2可取得讀寫存取權、但不具備超級使用者存取權。用戶端#3可取得唯讀存取權、但無法取得超級使用者存取權。

了解如何管理 **ONTAP NFS** 超級使用者存取請求

設定匯出原則時、您必須考量儲存系統收到使用者ID為0的用戶端存取要求（表示以超級使用者身分）時、會發生什麼情況、並據此設定匯出規則。

在UNIX世界中、使用者ID為0的使用者稱為超級使用者、通常稱為root、在系統上擁有無限存取權限。使用進階使用者權限可能會有危險、原因包括系統和資料安全性遭到破壞。

根據預設ONTAP 、功能表會將使用者ID為0的用戶端對應至匿名使用者。不過、您可以指定 - superuser 匯出規則中的參數、可決定如何處理使用者 ID 0 呈現的用戶端、視其安全性類型而定。下列是的有效選項 -superuser 參數：

- any
- none

  如果您未指定、這是預設設定 -superuser 參數。

- krb5
- ntlm
- sys

根據的不同、有兩種不同的方式來處理以使用者 ID 0 呈現的用戶端 -superuser 參數組態：

如果是 **-superuser** 參數和用戶端的安全類型 **...**	然後用戶端**...**
相符	以使用者ID 0取得超級使用者存取權。
不相符	以匿名使用者的身分取得存取權、並使用指定的使用者 ID -anon 參數及其指派的權限。無論唯讀或讀寫參數是否指定選項、都是如此 none。

如果用戶端提供使用者 ID 0 來存取具有 NTFS 安全性樣式的磁碟區、以及 -superuser 參數設定為 none，ONTAP 使用匿名使用者的名稱對應來取得適當的認證。

範例

匯出原則包含具有下列參數的匯出規則：

- -protocol nfs3
- -clientmatch 10.1.16.0/255.255.255.0
- -rorule any
- -rwrule krb5,ntlm
- -anon 127

用戶端 1 的 IP 位址為 10.16.207 、使用者 ID 746 、使用 NFSv3 傳輸協定傳送存取要求、並使用 Kerberos v5 進行驗證。

用戶端#2的IP位址為10.1.16.211、使用者ID為0、使用NFSv3傳輸協定傳送存取要求、並以AUTH_SYS驗證。

兩個用戶端的用戶端存取傳輸協定和IP位址都相符。唯讀參數允許所有用戶端的唯讀存取權、無論其驗證的安全類型為何。但是、只有用戶端#1會取得讀寫存取權、因為它使用核准的安全性類型Kerberos v5.x進行驗證。

用戶端#2無法取得超級使用者存取權。而是會對應至匿名、因為 `-superuser` 未指定參數。這表示預設為 `none` 並自動將使用者 ID 0 對應至匿名。用戶端#2也只會取得唯讀存取權、因為其安全性類型與讀寫參數不符。

範例

匯出原則包含具有下列參數的匯出規則：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

用戶端#1的IP位址為10.1.16.207、使用者ID為0、使用NFSv3傳輸協定傳送存取要求、並使用Kerberos v5進行驗證。

用戶端#2的IP位址為10.1.16.211、使用者ID為0、使用NFSv3傳輸協定傳送存取要求、並以AUTH_SYS驗證。

兩個用戶端的用戶端存取傳輸協定和IP位址都相符。唯讀參數允許所有用戶端的唯讀存取權、無論其驗證的安全類型為何。但是、只有用戶端#1會取得讀寫存取權、因為它使用核准的安全性類型Kerberos v5.x進行驗證。用戶端#2無法取得讀寫存取權。

匯出規則可讓使用者ID為0的用戶端擁有超級使用者存取權。用戶端 #1 獲得超級使用者存取權、因為它符合唯讀和的使用者 ID 和安全類型 `-superuser` 參數。用戶端 #2 無法取得讀寫或超級使用者存取權、因為其安全性類型與讀寫參數或不相符 `-superuser` 參數。而是將用戶端#2對應至匿名使用者、在此案例中、該使用者ID為0。

了解 **ONTAP NFS** 匯出策略緩存

為了提升系統效能、ONTAP 此功能使用本機快取來儲存主機名稱和網路群組等資訊。相較於從外部來源擷取資訊、這樣的功能可讓ONTAP 支援部門更快處理匯出原則規則。瞭解快取內容及其功能有助於疑難排解用戶端存取問題。

您可以設定匯出原則來控制用戶端對NFS匯出的存取。每個匯出原則都包含規則、而且每個規則都包含參數、可讓規則符合要求存取的用戶端。有些參數需要ONTAP 使用支援功能來聯絡外部來源、例如DNS或NIS伺服器、才能解析網域名稱、主機名稱或網路群組等物件。

這些與外部來源的通訊只需要很短的時間。為了提升效能ONTAP 、利用將資訊儲存在多個快取的每個節點上、藉此減少解析匯出原則規則物件所需的時間。

快取名稱	儲存的資訊類型
存取	用戶端對應至對應的匯出原則
名稱	UNIX使用者名稱對應至對應的UNIX使用者ID
ID	UNIX使用者ID對應至對應的UNIX使用者ID和延伸UNIX群組ID
主機	將主機名稱對應至對應的IP位址
網路群組	網路群組對應至成員對應的IP位址
showmount	從SVM命名空間匯出的目錄清單

如果在擷取並儲存於本機之後、變更環境中外部名稱伺服器的資訊ONTAP 、快取現在可能會包含過時的資訊。雖然在特定時間段後、會自動重新整理快取、但不同的快取會有不同的過期時間、重新整理時間和演算法。ONTAP

另一個快取包含過時資訊的可能原因是ONTAP 、當某些人嘗試重新整理快取的資訊、但嘗試與名稱伺服器通訊時卻遭遇失敗。如果發生這種情況、ONTAP 則會繼續使用目前儲存在本機快取中的資訊、以防止用戶端中斷運作。

因此、原本應該成功的用戶端存取要求可能會失敗、而原本應該失敗的用戶端存取要求可能會成功。疑難排解此類用戶端存取問題時、您可以檢視並手動清除部分匯出原則快取。

了解 **ONTAP NFS** 存取快取

使用存取快取來儲存匯出原則規則評估的結果、以便用戶端存取磁碟區或qtree的作業。ONTAP這會提高效能、因為每次用戶端傳送I/O要求時、從存取快取中擷取資訊的速度比執行匯出原則規則評估程序快得多。

每當NFS用戶端傳送I/O要求以存取磁碟區或qtree上的資料時、ONTAP 必須評估每個I/O要求、以判斷是否要授予或拒絕I/O要求。此評估包括檢查與Volume或qtree相關之匯出原則的每個匯出原則規則。如果通往Volume或qtree的路徑涉及跨越一或多個交會點、則可能需要對路徑上的多個匯出原則執行此檢查。

請注意、這項評估是針對從NFS用戶端傳送的每個I/O要求進行、例如讀取、寫入、清單、複製及其他作業；不只是針對初始掛載要求。

在確定適用的匯出原則規則並決定是否允許或拒絕該要求之後ONTAP 、即可在存取快取中建立一個項目來儲存此資訊。ONTAP

當NFS用戶端傳送I/O要求時、ONTAP 請注意用戶端的IP位址、SVM的ID、以及與目標Volume或qtree相關的匯出原則、然後先檢查存取快取是否有相符的項目。如果存取快取中存在相符的項目、ONTAP 則使用儲存的資訊來允許或拒絕I/O要求。如果不存在相符的項目、ONTAP 那麼就會依照上述說明、完成評估所有適用原則規則的正常程序。

未使用的存取快取項目不會重新整理。如此可減少使用外部名稱服務的不必要和浪費通訊。

從存取快取中擷取資訊的速度遠勝過針對每個I/O要求執行整個匯出原則規則評估程序。因此、使用存取快取可減少用戶端存取檢查的負荷、大幅提升效能。

了解 ONTAP NFS 存取快取參數

多個參數可控制存取快取中項目的重新整理期間。瞭解這些參數的運作方式、可讓您修改這些參數、以調整存取快取、並在效能與儲存資訊的最新程度之間取得平衡。

存取快取會儲存包含一或多個匯出規則的項目、這些規則適用於嘗試存取磁碟區或qtree的用戶端。這些項目會在重新整理之前儲存一段時間。重新整理時間取決於存取快取參數、並取決於存取快取項目的類型。

您可以指定個別SVM的存取快取參數。如此可讓參數根據SVM存取需求而有所不同。未使用的存取快取項目不會重新整理、如此可減少使用外部名稱服務的不必要和浪費通訊。

存取快取項目類型	說明	重新整理期間（以秒為單位）
正面項目	存取快取項目未導致用戶端存取遭拒。	最低：300 上限：86400 預設：3、600
負項目	存取快取項目導致拒絕用戶端存取。	最低： 60 上限：86400 預設：3、600

範例

NFS用戶端嘗試存取叢集上的磁碟區。將用戶端比對至匯出原則規則、並根據匯出原則規則組態來判斷用戶端是否可存取。ONTAP將匯出原則規則儲存在存取快取中、做為正面項目。ONTAP根據預設、ONTAP 功能表會在存取快取中保留正面項目一小時（3、600秒）、然後自動重新整理項目以保持資訊最新。

為了避免存取快取不必要地填滿、有一個額外的參數可以清除在特定時間段內尚未使用的現有存取快取項目、以決定用戶端存取。這 `-harvest-timeout` 參數的允許範圍為 60 到 2,592,000 秒、預設設定為 86,400 秒。

從 ONTAP NFS qtree 中刪除匯出策略

如果您決定不再想將特定的匯出原則指派給qtree、您可以修改qtree來移除匯出原則、改為繼承包含Volume的匯出原則。您可以使用來執行此作業 `volume qtree modify` 命令 `-export-policy` 參數和空白名稱字串（""）。

步驟

1. 若要從qtree移除匯出原則、請輸入下列命令：

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

2. 驗證qtree是否已相應修改：

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

驗證 ONTAP NFS qtree ID 以執行 qtree 檔案操作

可選擇性地執行qtree ID的額外驗證。ONTAP此驗證可確保用戶端檔案作業要求使用有效的qtree ID、而且用戶端只能在同一個qtree內移動檔案。您可以修改來啟用或停用此驗證 `-validate-qtree-export` 參數。此參數預設為啟用。

關於這項工作

此參數僅在您已將匯出原則直接指派給儲存虛擬機器（SVM）上的一或多個qtree時有效。

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**qtree ID**驗證…	輸入下列命令…
已啟用	`vserver nfs modify -vserver vserver_name -validate-qtree-export enabled`
已停用	`vserver nfs modify -vserver vserver_name -validate-qtree-export disabled`

3. 返回管理權限層級：

   ```
   set -privilege admin
   ```

ONTAP NFS FlexVol 磁碟區的匯出策略限制和巢狀連接

如果您將匯出原則設定為在巢狀連接點上設定較少限制的原則、但在較高層連接點上設定較嚴格的原則、則對較低層連接點的存取可能會失敗。

您應確保較高層級的匯接器比較低層級的匯接器具有較少的匯出原則限制。

使用Kerberos搭配NFS以獲得強大的安全性

ONTAP NFS 對 Kerberos 的支持

Kerberos為用戶端/伺服器應用程式提供強大的安全驗證功能。驗證可驗證伺服器的使用者和處理程序身分。在支援VMware的環境中ONTAP 、Kerberos可在儲存虛擬機器（SVM）和NFS用戶端之間提供驗證。

在發揮作用的過程中、支援下列Kerberos功能：ONTAP

- Kerberos 5驗證搭配完整性檢查（krb5i）

  Krb5i使用Checksum來驗證用戶端與伺服器之間傳輸的每個NFS訊息完整性。這項功能在安全性方面非常實用（例如、確保資料未遭竄改）、也有助於確保資料完整性（例如、在不可靠的網路上使用NFS時、可防止資料毀損）。

- Kerberos 5驗證搭配隱私權檢查（krb5p）

  Krb5p使用Checksum加密用戶端與伺服器之間的所有流量。這更安全、也會產生更多負載。

- 128位元和256位元AES加密

  進階加密標準（AES）是一種加密演算法、用於保護電子資料安全。ONTAP 支援採用 128 位元金鑰（ AES-128 ）的 AES 、以及採用 256 位元金鑰（ AES-256 ）加密的 AES 、以提供更強大的安全性。

- SVM層級Kerberos領域組態

  SVM系統管理員現在可以在SVM層級建立Kerberos領域組態。這表示SVM管理員不再需要仰賴叢集管理員來進行Kerberos領域組態、也能在多租戶環境中建立個別的Kerberos領域組態。

使用 **ONTAP NFS** 設定 **Kerberos** 的要求

在系統上使用NFS設定Kerberos之前、您必須先確認網路和儲存環境中的某些項目已正確設定。

> 設定環境的步驟取決於您所使用的用戶端作業系統、網域控制器、Kerberos、DNS等版本和類型。記錄所有這些變數不在此文件範圍之內。如需詳細資訊、請參閱各元件的相關文件。
>
> 如需ONTAP 如何在使用Windows Server 2008 R2 Active Directory和Linux主機的環境中使用NFSv3和NFSv3設定支援功能的支援功能和Kerberos 5的詳細範例、請參閱技術報告4073。

應先設定下列項目：

網路環境需求

- Kerberos

  您必須使用金鑰發佈中心（Kdc）進行有效的Kerberos設定、例如Windows Active Directory型Kerberos或MIT Kerberos。

  NFS 伺服器必須使用 `nfs` 作為其機器主體的主要元件。

- 目錄服務

  您必須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。

- 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。

- 使用者帳戶

  每個用戶端都必須在Kerberos領域中擁有使用者帳戶。NFS伺服器必須使用「NFS」作為其機器主體的主要元件。

NFS 用戶端需求

- NFS

  每個用戶端都必須正確設定、才能使用NFSv3或NFSv4透過網路進行通訊。

  用戶端必須支援RFC1964和RFC2203。

- Kerberos

  每個用戶端都必須正確設定、才能使用Kerberos驗證、包括下列詳細資料：

  - 已啟用TGS通訊的加密。

    AES-256提供最強大的安全性。

  - 已啟用TGTT通訊最安全的加密類型。
  - Kerberos領域和網域已正確設定。
  - GSS 已啟用。

    使用機器認證時：

  - 請勿執行 `gssd` 使用 `-n` 參數。
  - 請勿執行 `kinit` 作為 root 使用者。

- 每個用戶端都必須使用最新且更新的作業系統版本。

  這可為使用Kerberos的AES加密提供最佳的相容性與可靠性。

- DNS

  每個用戶端都必須正確設定、才能使用DNS進行正確的名稱解析。

- NTP

  每個用戶端都必須與NTP伺服器同步。

- 主機與網域資訊

  每個用戶端 `/etc/hosts` 和 `/etc/resolv.conf` 檔案必須分別包含正確的主機名稱和 DNS 資訊。

- Keytab檔案

  每個用戶端都必須有來自於Kdc的Keytab檔案。領域必須以大寫字母顯示。加密類型必須為AES-256、才能獲得最強的安全性。

- 選用：為獲得最佳效能、用戶端可享有至少兩個網路介面：一個用於與區域網路通訊、另一個用於與儲存網路通訊。

儲存系統需求

- NFS授權

  儲存系統必須安裝有效的NFS授權。

- CIFS 授權

  CIFS授權為選用授權。只有在使用多重傳輸協定名稱對應時、才需要檢查Windows認證。在純UNIX的嚴格環境中、不需要這項功能。

- SVM

  您必須在系統上設定至少一個SVM。

- SVM上的DNS

  您必須在每個SVM上設定DNS。

- NFS 伺服器

  您必須在SVM上設定NFS。

- AES加密

  為了獲得最強大的安全性、您必須設定NFS伺服器、使其僅允許Kerberos使用AES-256加密。

- SMB 伺服器

  如果您執行的是多重傳輸協定環境、則必須在SVM上設定SMB。多重傳輸協定名稱對應需要SMB伺服器。

- 磁碟區

  您必須有根磁碟區和至少一個設定供SVM使用的資料磁碟區。

- 根Volume

  SVM的根Volume必須具有下列組態：

名稱	設定
安全風格	UNIX
UID	root或ID 0

名稱	設定
Gid	root或ID 0
UNIX權限	7777

相較於根磁碟區、資料磁碟區可以有任一種安全樣式。

- UNIX 群組

  SVM必須設定下列UNIX群組：

群組名稱	群組**ID**
精靈	1.
根	0%
pcuser	65534（ONTAP 建立SVM時由SVM自動建立）

- UNIX 使用者

  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 NFS用戶端使用者的第一個使用者是使用者。
pcuser	65534	65534	NFS 和 CIFS 多重傳輸協定的使用需求 建立 SVM 時、由 ONTAP 自動建立並新增至 pcuser 群組。
根	0%	0%	安裝所需

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。

- 匯出原則與規則

  您必須設定匯出原則、並針對根磁碟區、資料磁碟區和qtree設定必要的匯出規則。如果透過 Kerberos 存取 SVM 的所有磁碟區、您可以設定匯出規則選項 `-rorule`、 `-rwrule`和 `-superuser` 將根磁碟區移至 `krb5` 、 `krb5i`或 `krb5p`。

- Kerberos UNIX名稱對應

  如果您想讓NFS用戶端使用者的使用者具有root權限、您必須建立一個指向root的名稱對應。

相關資訊

"NetApp技術報告4073：安全統一化驗證"

"NetApp 互通性對照表工具"

"系統管理"

"邏輯儲存管理"

為 **NFSv4** 指定 **ONTAP** 使用者 **ID** 網域

若要指定使用者 ID 網域、您可以設定 `-v4-id-domain` 選項。

關於這項工作

根據預設ONTAP 、如果已設定NFSv4使用者ID對應、則使用NIS網域。如果未設定NIS網域、則會使用DNS網域。例如、如果您有多個使用者ID網域、則可能需要設定使用者ID網域。網域名稱必須符合網域控制器上的網域組態。NFSv3不需要此功能。

步驟

1. 輸入下列命令：

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

設定名稱服務

瞭解 **ONTAP NFS** 名稱服務交換器組態

ONTAP 會將名稱服務組態資訊儲存在相當於的表格中 `/etc/nsswitch.conf` UNIX 系統上的檔案。您必須瞭解表格的功能及ONTAP 其使用方式、以便根據環境適當設定。

這個名稱服務交換器表決定哪些名稱服務來源可以查詢、以便擷取特定類型名稱服務資訊的資訊。ONTAP ONTAP針對每個SVM維護個別的名稱服務交換器表。ONTAP

資料庫類型

此表格會針對下列每一種資料庫類型儲存個別的名稱服務清單：

資料庫類型	定義名稱服務來源：	有效來源為...
主機	將主機名稱轉換為IP位址	檔案、DNS
群組	查詢使用者群組資訊	檔案、NIS、LDAP
密碼	查詢使用者資訊	檔案、NIS、LDAP

資料庫類型	定義名稱服務來源：	有效來源為...
網路群組	查詢netgroup資訊	檔案、NIS、LDAP
名稱	對應使用者名稱	檔案、LDAP

來源類型

這些來源會指定要用於擷取適當資訊的名稱服務來源。

指定來源類型...	若要查詢資訊...	由命令系列管理...

檔案	本機來源檔案	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

NIS	在SVM的NIS網域組態中指定的外部NIS伺服器	`vserver services name-service nis-domain`
LDAP	在SVM的LDAP用戶端組態中指定的外部LDAP伺服器	`vserver services name-service ldap`
DNS	在SVM的DNS組態中指定的外部DNS伺服器	`vserver services name-service dns`

即使您計畫同時使用 NIS 或 LDAP 來進行資料存取和 SVM 管理驗證、您仍應納入 `files` 並將本機使用者設定為在 NIS 或 LDAP 驗證失敗時的後援。

用於存取外部來源的傳輸協定

若要存取伺服器的外部來源、ONTAP 可使用下列通訊協定：

外部名稱服務來源	用於存取的傳輸協定
NIS	UDP
DNS	UDP
LDAP	TCP

範例

下列範例顯示SVM SVM_1的名稱服務交換器組態：

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                 Source
Vserver         Database         Order
--------------- ------------     ---------
svm_1           hosts            files,
                                 dns
svm_1           group            files
svm_1           passwd           files
svm_1           netgroup         nis,
                                 files
```

若要查詢主機的IP位址、ONTAP 請先查詢本機來源檔案。如果查詢未傳回任何結果、則會勾選DNS伺服器。

若要查詢使用者或群組資訊、ONTAP 僅查詢本機來源檔案。如果查詢未傳回任何結果、則查詢會失敗。

若要查詢netgroup資訊、ONTAP 請先諮詢外部NIS伺服器。如果查詢未傳回任何結果、則會勾選本機netgroup檔案。

SVM SVM_1的表格中沒有名稱對應的名稱服務項目。因此ONTAP 、根據預設、僅查詢本機來源檔案。

相關資訊

"NetApp技術報告4668：名稱服務最佳實務做法指南"

使用**LDAP**

了解適用於 **ONTAP NFS SVM** 的 **LDAP**

LDAP（輕量型目錄存取傳輸協定）伺服器可讓您集中維護使用者資訊。如果您將使用者資料庫儲存在環境中的LDAP伺服器上、您可以設定儲存系統、以便在現有的LDAP資料庫中查詢使用者資訊。

- 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，則必須在ONTAP 9.5 及更高版本中為 TLS 或 SSL 啟用 LDAP 伺服器。 ONTAP 9.4 - 9.0 不支援 SSL。
- 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。
- 網域密碼應相同、以在何時進行驗證 `--bind-as-cifs-server` 設為 true 。

> 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）

- 從 ONTAP 9.11.1 開始，您可以使用"使用 LDAP 快速綁定對 ONTAP NFS SVM 進行 nsswitch 驗證。"
- 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。

如需其他資訊、請參閱 "NetApp技術報告4835：如何在ONTAP 功能方面設定LDAP"。

了解 **ONTAP NFS SVM** 的 **LDAP** 簽章和密封

從ONTAP 功能支援功能支援功能支援功能支援功能、從功能支援功能支援功能升級至功能性管理功能。您必須在儲存虛擬機器（ SVM ）上設定 NFS 伺服器安全性設定、使其對應於 LDAP 伺服器上的設定。

簽署可確認LDAP有效負載資料使用秘密金鑰技術的完整性。「密封」會加密LDAP有效負載資料、以避免以純文字傳輸敏感資訊。「*LDAP*安全性層級」選項會指出LDAP流量是否需要簽署、簽署及密封、或兩者皆不需要。預設值為 `none`。測試

在 SVM 上啟用 SMB 流量的 LDAP 簽署與密封功能 `-session-security-for-ad-ldap` 選項 `vserver cifs security modify` 命令。

了解適用於 **ONTAP NFS SVM** 的 **LDAPS**

您必須瞭ONTAP 解有關如何保護LDAP通訊的某些詞彙與概念。支援使用start TLS或LDAPS、在Active Directory整合式LDAP伺服器或UNIX型LDAP伺服器之間設定驗證工作階段。ONTAP

術語

您應該瞭ONTAP 解某些詞彙、瞭解如何使用LDAPS來保護LDAP通訊安全。

- * LDAP *

  （輕量型目錄存取傳輸協定）一種用於存取和管理資訊目錄的傳輸協定。LDAP是用來儲存使用者、群組和網路群組等物件的資訊目錄。LDAP也提供目錄服務、可管理這些物件並滿足LDAP用戶端的LDAP要求。

- * SSL *

  （安全通訊端層）一種通訊協定、專為透過網際網路安全傳送資訊而開發。ONTAP 9 及更新版本支援 SSL 、但已不再採用 TLS 。

- * TLS *

  （傳輸層安全性）一種根據舊版SSL規格追蹤傳輸協定的IETF標準。這是SSL的後續版本。ONTAP 9.5 及更新版本支援 TLS 。

- * LDAPS（LDAP over SSL或TLS）*

  一種傳輸協定、使用TLS或SSL來保護LDAP用戶端與LDAP伺服器之間的通訊安全。術語 *LDAP over SSL* 和 *LDAP over TLS* 有時會互換使用。ONTAP 9.5 及更新版本支援 LDAPS 。

  - 在ONTAP 9.8-9.5 中，LDAPS 只能在連接埠 636 上啟用。為此，請使用 `-use-ldaps-for-ad-ldap`參數 `vserver cifs security modify`命令。
  - 從ONTAP 推出《支援支援支援支援服務的支援服務：支援服務器支援服務」、從功能支援服務的支援服務開始、您可以在任何連接埠上啟用LDAPS、但連接埠636仍為預設若要這麼做，請將參數設定 `-ldaps-enabled`為 `true`，並指定所需的 `-port`參數。如"指令參考資料ONTAP"需詳細 `vserver services name-service ldap client create`資訊，請參閱。

    使用Start TLS而非LDAPS是NetApp最佳實務做法。

- 啟動**TLS**

  （也稱為_start_tls_、_startTLs_和_StartTLS）一種機制、可透過TLS傳輸協定提供安全的通訊。

  支援使用STARTTLS來保護LDAP通訊安全、並使用預設的LDAP連接埠（389）與LDAP伺服器通訊。ONTAPLDAP伺服器必須設定為允許透過LDAP連接埠389進行連線、否則SVM與LDAP伺服器之間的LDAP TLS連線將會失敗。

如何使用**LDAPS ONTAP**

支援TLS伺服器驗證、可讓SVM LDAP用戶端在連結作業期間確認LDAP伺服器的身分。ONTAP啟用TLS的LDAP用戶端可使用公開金鑰密碼編譯的標準技術、檢查伺服器的憑證和公開ID是否有效、以及是否已由用戶端信任CA清單中所列的憑證授權單位（CA）核發。

LDAP支援使用TLS加密通訊的ARTTLS。StartTLS會以純文字連線形式透過標準LDAP連接埠（389）開始、然後將該連線升級為TLS。

支援下列項目：ONTAP

- LDAPS用於Active Directory整合式LDAP伺服器與SVM之間的SMB相關流量
- LDAP流量的LDAPS、用於名稱對應和其他UNIX資訊

  Active Directory整合式LDAP伺服器或UNIX型LDAP伺服器均可用來儲存LDAP名稱對應和其他UNIX資訊的資訊、例如使用者、群組和網路群組。

- 自我簽署的根CA憑證

  使用Active Directory整合式LDAP時、會在網域中安裝Windows Server憑證服務時產生自我簽署的根憑證。使用UNIX LDAP伺服器進行LDAP名稱對應時、會使用適合該LDAP應用程式的方法、產生並儲存自我簽署的根憑證。

根據預設、LDAPS會停用。

為 **ONTAP NFS SVM** 啟用 **LDAP RFC2307bis** 支援

如果您想要使用LDAP並需要額外的功能來使用巢狀群組成員資格、您可以設定ONTAP 支援功能以啟用LDAP RFC2307bis。

開始之前

您必須已建立要使用的預設LDAP用戶端架構之一的複本。

關於這項工作

在LDAP用戶端架構中、群組物件使用memberUid屬性。此屬性可包含多個值、並列出屬於該群組的使用者名稱。在啟用RFC2307bis的LDAP用戶端架構中、群組物件會使用uniqueMember屬性。此屬性可包含LDAP目錄中其他物件的完整辨別名稱（DN）。這可讓您使用巢狀群組、因為群組可以有其他群組作為成員。

使用者不應是256個以上群組的成員、包括巢狀群組。不考慮超過256個群組限制的任何群組。ONTAP

根據預設、會停用RFC2307bis支援。

當ONTAP 使用MS -AD-BIS架構建立LDAP用戶端時、即可在功能上自動啟用RFC2307bis支援。

如需其他資訊、請參閱 "NetApp技術報告4835：如何在ONTAP 功能方面設定LDAP"。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 修改複製的RFC2307 LDAP用戶端架構、以啟用RFC2307bis支援：

   ```
   vserver services name-service ldap client schema modify -vserver vserver_name
   -schema schema-name -enable-rfc2307bis true
   ```

3. 修改架構以符合LDAP伺服器支援的物件類別：

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -group-of-unique-names-object-class object_class
   ```

4. 修改架構以符合LDAP伺服器支援的屬性名稱：

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -unique-member-attribute attribute_name
   ```

5. 返回管理權限層級：

   ```
   set -privilege admin
   ```

用於 **LDAP** 目錄搜尋的 **ONTAP NFS** 設定選項

您可以設定ONTAP 支援使用者、群組和netgroup資訊等方式、將LDAP用戶端設定為以最適合您環境的方式連線至LDAP伺服器、藉此最佳化LDAP目錄搜尋。您需要瞭解預設的LDAP基礎和範圍搜尋值何時足夠、以及指定自訂值何時更合適的參數。

使用者、群組和netgroup資訊的LDAP用戶端搜尋選項、有助於避免LDAP查詢失敗、進而避免用戶端無法存取儲存系統。它們也有助於確保搜尋作業盡可能有效率、以避免用戶端效能問題。

預設基礎和範圍搜尋值

LDAP基礎是LDAP用戶端用來執行LDAP查詢的預設基礎DN。所有搜尋、包括使用者、群組和網路群組搜尋、都是使用基礎DN來完成。當您的LDAP目錄相對較小、且所有相關項目都位於相同的DN中時、此選項是適當的。

如果未指定自訂基礎 DN 、則預設值為 `root`。這表示每個查詢都會搜尋整個目錄。雖然如此一來、LDAP查詢的成功機會就會最大化、但效率卻會降低、而且大型LDAP目錄的效能也會大幅降低。

LDAP基礎範圍是LDAP用戶端用來執行LDAP查詢的預設搜尋範圍。所有搜尋、包括使用者、群組和netgroup搜尋、都是使用基礎範圍來完成。它決定LDAP查詢只搜尋命名項目、DN下一層的項目、或DN下的整個子樹狀結構。

如果未指定自訂基礎範圍、則預設為 `subtree`。這表示每個查詢都會搜尋DN下方的整個子樹狀結構。雖然如此

一來、LDAP查詢的成功機會就會最大化、但效率卻會降低、而且大型LDAP目錄的效能也會大幅降低。

自訂基礎和範圍搜尋值

您也可以為使用者、群組和netgroup搜尋指定個別的基礎和範圍值。以這種方式限制搜尋基礎和查詢範圍、可大幅提升效能、因為它會將搜尋範圍限制在LDAP目錄的較小子部分。

如果指定自訂基礎和範圍值、則會覆寫一般預設搜尋基礎和範圍、以供使用者、群組和netgroup搜尋。可在進階權限層級使用指定自訂基礎和範圍值的參數。

LDAP用戶端參數…	指定自訂…
`-base-dn`	所有 LDAP 搜尋的基準 DN。如果需要，可以輸入多個值（例如，如果在 ONTAP 9.5 及更高版本中啟用了 LDAP 引用追蹤）。
`-base-scope`	所有 LDAP 搜尋的基本範圍。
`-user-dn`	所有 LDAP 使用者搜尋的基本 DN。此參數也適用於使用者名稱映射搜尋。
`-user-scope`	所有 LDAP 使用者搜尋的基本範圍。此參數也適用於使用者名稱映射搜尋。
`-group-dn`	所有 LDAP 群組搜尋的基本 DN。
`-group-scope`	所有 LDAP 群組搜尋的基本範圍。
`-netgroup-dn`	所有 LDAP 網路群組搜尋的基本 DN。
`-netgroup-scope`	所有 LDAP 網路組搜尋的基本範圍。

多個自訂基礎**DN**值

如果您的LDAP目錄結構較為複雜、您可能需要指定多個基礎DNS、以搜尋LDAP目錄的多個部分以取得特定資訊。您可以為使用者、群組和netgroup DN參數指定多個DNS、方法是以分號（；）分隔這些DNS、並以雙引號（"）括住整個DN搜尋清單。如果DN包含分號、您必須在DN中的分號前面新增轉義字元（\）。

請注意、此範圍適用於為對應參數指定的整個DNS清單。例如、如果您為使用者範圍指定三個不同使用者DNS和子樹狀結構的清單、則LDAP使用者會搜尋三個指定DNS中的每個子樹狀結構。

從ONTAP 功能介紹9.5開始、您也可以指定LDAP _Referring Chasing _、以便ONTAP 在主要LDAP伺服器未傳回LDAP參照回應時、讓該支援功能可將查詢要求參照到其他LDAP伺服器。用戶端會使用該參照資料、從參照資料中所述的伺服器擷取目標物件。若要搜尋參照LDAP伺服器中的物件、可將參照物件的基礎DN新增至基礎DN、做為LDAP用戶端組態的一部分。不過、只有在啟用參照追蹤（使用 `-referral-enabled true` 選項）。

自訂 **LDAP** 搜尋篩選器

您可以使用 LDAP 組態選項參數來建立自訂搜尋篩選器。此 `-group-membership-filter`參數指定從 LDAP 伺服

器查詢群組成員資格時所使用的搜尋篩選器。

有效篩選的範例包括：

```
(cn=*99), (cn=1*), (|(cn=*22)(cn=*33))
```

深入瞭解 "如何在 ONTAP 中設定 LDAP"。

提高 ONTAP NFS SVM 的 LDAP 目錄網路群組按主機搜尋的效能

如果您的LDAP環境已設定為允許依主機進行網路群組搜尋、您可以設定ONTAP 支援使用此功能的支援、並依主機執行網路群組搜尋。如此可大幅加快網路群組搜尋速度、並減少網路群組搜尋期間的延遲所導致的NFS用戶端存取問題。

開始之前

您的 LDAP 目錄必須包含 `netgroup.byhost` 地圖。

您的DNS伺服器應同時包含NFS用戶端的轉送（A）和反轉（PTr）查詢記錄。

當您在netGroups中指定IPv6位址時、必須一律縮短並壓縮RFC 5952中指定的每個位址。

關於這項工作

NIS 伺服器會將網路群組資訊儲存在三個不同的對應中、稱為 `netgroup`、 `netgroup.byuser`和 `netgroup.byhost`。的用途 `netgroup.byuser` 和 `netgroup.byhost` 地圖是為了加速網路群組搜尋。支援在NIS伺服器上執行各主機的網路群組搜尋、以縮短掛載回應時間。ONTAP

根據預設、 LDAP 目錄沒有這樣的 `netgroup.byhost` 對應 NIS 伺服器。不過、在協力廠商工具的協助下、可以匯入 NIS `netgroup.byhost` 映射到 LDAP 目錄以啓用逐主機快速 netgroup 搜索。如果您已將 LDAP 環境設定為允許逐主機網路群組搜尋、則可以使用來設定 ONTAP LDAP 用戶端 `netgroup.byhost` 對應名稱、 DN 和搜尋範圍、可更快速地逐主機搜尋 netgroup-by host 。

當ONTAP NFS用戶端要求存取匯出時、若能更快接收各主機的網路群組搜尋結果、則可讓支援者更快處理匯出規則。如此可降低網路群組搜尋延遲問題導致存取延遲的機率。

步驟

1. 取得確切完整的 NIS 辨別名稱 `netgroup.byhost` 將您匯入 LDAP 目錄的對應。

   對應DN可能會因您用於匯入的協力廠商工具而異。若要獲得最佳效能、您應該指定確切的對應DN。

2. 將權限層級設為進階： `set -privilege advanced`
3. 在儲存虛擬機器（ SVM ）的 LDAP 用戶端組態中、啟用逐主機網路群組搜尋： `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost-dn netgroup-by-host_map_distinguished_name -netgroup-byhost-scope netgroup-by-host_search_scope`

   `-is-netgroup-byhost-enabled {true false}` 啓用或禁用逐主機對 LDAP 目錄的 netgroup 搜索。預設值為 `false`。

`-netgroup-byhost-dn netgroup-by-host_map_distinguished_name` 指定的辨別名稱 `netgroup.byhost` 在 LDAP 目錄中對應。它會覆寫基礎DN、以便依主機搜尋網路群組。如果您未指定此參數、ONTAP 則使用基礎DN。

`-netgroup-byhost-scope {base|onelevel subtree}` 指定 netgroup-by host 搜尋的搜尋範圍。如果您未指定此參數、則預設值為 `subtree`。

如果 LDAP 用戶端組態尚不存在、您可以在使用建立新的 LDAP 用戶端組態時、指定這些參數來啟用逐主機網路群組搜尋 `vserver services name-service ldap client create` 命令。

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

4. 返回管理權限層級： `set -privilege admin`

範例

下列命令會修改名為「 `LDAP_corp` 」的現有 LDAP 用戶端組態、以使用啟用逐主機網路群組搜尋 `netgroup.byhost` 名爲 "`nisMapName="netgroup.byhost" 、 DC=corp 、 DC=example 、 DC=com 的地圖和默認搜索範圍 `subtree`：

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

完成後

。 `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。

相關資訊

"IETF RFC 5952：IPv6位址文字呈現的建議"

使用 **LDAP** 快速綁定對 **ONTAP NFS SVM** 進行 **nsswitch** 驗證

從SURF9.11.1開始ONTAP 、您可以利用LDAP _fast bind_Functionality（也稱為_並行 連結）、以更快、更簡單的用戶端驗證要求。若要使用此功能、LDAP伺服器必須支援快速連結功能。

關於這項工作

如果沒有快速連結、ONTAP 則使用LDAP Simple Bind來驗證LDAP伺服器的管理使用者。利用這種驗證方法、ONTAP 將使用者或群組名稱傳送至LDAP伺服器、接收儲存的雜湊密碼、並將伺服器雜湊代碼與本機使用者密碼產生的雜湊密碼進行比較。如果完全相同、ONTAP 則此功能會授予登入權限。

利用快速連結功能、ONTAP 透過安全連線、僅將使用者認證（使用者名稱和密碼）傳送至LDAP伺服器。然後LDAP伺服器會驗證這些認證資料、並指示ONTAP 資訊技術授予登入權限。

快速連結的優點之一是ONTAP 、不需要支援LDAP伺服器所支援的每一種新雜湊演算法、因為密碼雜湊是由LDAP伺服器執行。

"深入瞭解如何使用快速連結。"

您可以使用現有的LDAP用戶端組態進行LDAP快速連結。不過、強烈建議將LDAP用戶端設定為TLS或LDAPS、否則密碼會以純文字透過線路傳送。

若要在ONTAP 整個環境中啟用LDAP快速連結、您必須滿足下列需求：

- 必須在支援快速連結的LDAP伺服器上設定支援使用者的支援。ONTAP
- 必須在名稱服務交換器（nsswitch）資料庫中設定LDAP的支援功能。ONTAP
- 必須使用FAST Bind設定NS交換 器驗證的使用者和群組帳戶。ONTAP

步驟

1. 請向LDAP管理員確認LDAP伺服器支援LDAP快速連結。
2. 確保ONTAP LDAP伺服器上已設定了這個使用者認證資料。
3. 確認已針對LDAP快速連結正確設定管理或資料SVM。

   a. 若要確認LDAP FAST Bind伺服器已列在LDAP用戶端組態中、請輸入：

      `vserver services name-service ldap client show`

      "瞭解LDAP用戶端組態。"

   b. 以確認 `ldap` 是 nsswitch 設定的來源之一 `passwd` 資料庫、輸入：

      `vserver services name-service ns-switch show`

   "深入瞭解nsswitch組態。"

4. 確保管理使用者正在使用nsswitch進行驗證、且其帳戶中已啟用LDAP快速連結驗證。

   ◦ 對於現有使用者、請輸入 `security login modify` 並驗證下列參數設定：

      `-authentication-method nsswitch`

      `-is-ldap-fastbind true`

   如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

   ◦ 對於新的管理員使用者，請參閱"啟用 LDAP 或 NIS ONTAP 帳戶存取"。

顯示 **ONTAP NFS SVM** 的 **LDAP** 統計資訊

您可以顯示儲存系統上的儲存虛擬機器 (SVM) 的 LDAP 統計訊息，以監控效能和診斷問題。

開始之前

- 您必須在SVM上設定LDAP用戶端。
- 您必須已識別可從中檢視資料的LDAP物件。

步驟

1. 檢視計數器物件的效能資料：

```
statistics show
```

範例

下列範例顯示計數器名稱為 **SMPL_1** 的範例統計資料： Avg_processor_busy 和 CPU_busy

```
cluster1::*> statistics start -object system -counter
avg_processor_busy|cpu_busy -sample-id smpl_1
Statistics collection is being started for Sample-id: smpl_1

cluster1::*> statistics stop -sample-id smpl_1
Statistics collection is being stopped for Sample-id: smpl_1

cluster1::*> statistics show -sample-id smpl_1
Object: system
Instance: cluster
Start-time: 8/2/2012 18:27:53
End-time: 8/2/2012 18:27:56
Cluster: cluster1
   Counter                                                     Value
   -------------------------------- --------------------------------
   avg_processor_busy                                             6%
   cpu_busy
```

相關資訊

- "統計數據顯示"
- "統計開始"
- "統計停止"

設定名稱對應

了解 **ONTAP NAS SVM** 的名稱對映配置

ONTAP 使用名稱對應將 SMB 身分識別對應至 UNIX 身分識別、將 Kerberos 身分識別對應至 UNIX 身分識別、以及將 UNIX 身分識別對應至 SMB 身分識別。無論是從 NFS 用戶端或 SMB 用戶端連線、 IT 都需要這些資訊來取得使用者認證、並提供適當的檔案存取。

您不需要使用名稱對應的情況有兩種例外：

- 您可以設定純 UNIX 環境、而不打算在磁碟區上使用 SMB 存取或 NTFS 安全樣式。
- 您可以設定要使用的預設使用者。

  在此案例中、不需要名稱對應、因為不會對應每個個別用戶端認證、而是將所有用戶端認證對應至相同的預設使用者。

請注意、您只能針對使用者使用名稱對應、而不能針對群組使用名稱對應。

不過、您可以將一組個別使用者對應至特定使用者。例如、您可以將開頭或結尾的所有AD使用者對應至特定UNIX使用者、以及使用者的UID。

了解 **ONTAP NAS SVM** 的名稱映射

當必須對應使用者的認證資料時、它會先檢查本機名稱對應資料庫和LDAP伺服器、以找出現有的對應。ONTAP無論是檢查一項或兩項、或是按SVM的名稱服務組態來決定順序。

- 適用於Windows至UNIX對應

  如果找不到對應、ONTAP 則此功能會檢查UNIX網域中的Windows使用者名稱是否為有效的使用者名稱。如果這不管用、它會使用預設的UNIX使用者、前提是已設定。如果未設定預設UNIX使用者、ONTAP 且無法以這種方式取得對應、則對應會失敗、並傳回錯誤。

- 適用於UNIX至Windows對應

  如果找不到對應、ONTAP 則嘗試尋找與SMB網域中UNIX名稱相符的Windows帳戶。如果這不管用、它會使用預設的SMB使用者、前提是已設定。如果預設的SMB使用者未設定、ONTAP 且無法以此方式取得對應、則對應會失敗、並傳回錯誤。

依預設、機器帳戶會對應至指定的預設UNIX使用者。如果未指定預設UNIX使用者、則機器帳戶對應會失敗。

- 從功能表9.5開始ONTAP 、您可以將機器帳戶對應至預設UNIX使用者以外的使用者。
- 在更新版本的版本中、您無法將機器帳戶對應到其他使用者。ONTAP

  即使已定義機器帳戶的名稱對應、也會忽略對應。

在 **ONTAP NAS SVM** 上進行多域搜尋以尋找 **UNIX** 到 **Windows** 使用者名稱映射

將UNIX使用者對應至Windows使用者時、支援多網域搜尋。ONTAP在傳回相符結果之前、會搜尋所有探索到的信任網域是否符合取代模式。或者、您也可以設定偏好的信任網域清單、以取代探索到的信任網域清單、並依序搜尋、直到傳回相符的結果為止。

網域信任如何影響**UNIX**使用者對**Windows**使用者名稱對應搜尋

若要瞭解多網域使用者名稱對應的運作方式、您必須瞭解網域信任如何搭配ONTAP 使用。Active Directory 與 SMB 伺服器主網域之間的信任關係可以是雙向信任、也可以是兩種單向信任類型之一、可以是傳入信任或傳出信任。主網域是 SVM 上 SMB 伺服器所屬的網域。

- 雙向信任

  透過雙向信任、這兩個網域彼此信任。如果 SMB 伺服器的主網域與其他網域具有雙向信任、則主網域可以驗證並授權屬於信任網域的使用者、反之亦然。

  UNIX使用者對Windows使用者名稱對應搜尋只能在主網域與其他網域之間具有雙向信任的網域上執行。

- 傳出信任_

透過傳出信任、主網域信任其他網域。在此情況下、主網域可以驗證及授權屬於傳出信任網域的使用者。

執行UNIX使用者對Windows使用者名稱對應搜尋時、會搜尋具有主網域外傳信任的網域。

- 傳入信任_

  透過傳入信任、另一個網域會信任 SMB 伺服器的主網域。在此情況下、主網域無法驗證或授權屬於傳入信任網域的使用者。

  在執行UNIX使用者對Windows使用者名稱對應搜尋時、會搜尋具有主網域傳入信任的網域。

如何使用萬用字元（*）來設定多網域搜尋名稱對應

在Windows使用者名稱的網域區段中使用萬用字元、可協助進行多網域名稱對應搜尋。下表說明如何在名稱對應項目的網域部分使用萬用字元來啟用多網域搜尋：

模式	更換	結果
根	｛星號｝ ｛反斜槓｝ ｛反斜槓｝管理員	UNIX使用者「root」會對應至名為「Administrator」的使用者。搜尋所有信任的網域、直到找到第一個相符的使用者「'Administrator」為止。
*	｛星號｝ ｛反斜槓｝ ｛反斜槓｝ ｛星號｝	有效的UNIX使用者會對應至對應的Windows使用者。會依序搜尋所有信任的網域、直到找到第一個與該名稱相符的使用者為止。 模式｛星號｝ ｛反斜槓｝ ｛反斜槓｝ ｛星號｝僅適用於從UNIX到Windows的名稱對應、而非其他方式。

執行多網域名稱搜尋的方式

您可以選擇兩種方法之一來決定用於多網域名稱搜尋的信任網域清單：

- 使用ONTAP 由資訊更新所編譯的自動探索雙向信任清單
- 使用您所編譯的慣用信任網域清單

如果UNIX使用者以萬用字元對應至使用者名稱的網域區段、則Windows使用者會在所有信任的網域中查詢、如下所示：

- 如果已設定慣用的信任網域清單、則對應的Windows使用者只會依序在搜尋清單中查詢。
- 如果未設定信任網域的慣用清單、則會在主網域的所有雙向信任網域中查詢Windows使用者。
- 如果主網域沒有雙向信任的網域、則會在主網域中查詢該使用者。

如果UNIX使用者對應至使用者名稱中沒有網域區段的Windows使用者、則會在主網域中查詢Windows使用者。

ONTAP NAS SVM 的名稱對映轉換規則

這個系統可為每個SVM保留一組轉換規則。ONTAP每個規則包含兩個部分：*Pattern_* 和*_replace*。轉換從適當清單的開頭開始、並根據第一個相符規則執行替代。模式是UNIX樣式的規則運算式。取代是包含轉義序列的字串、代表模式中的子運算式、如同 UNIX `sed` 方案。

為 ONTAP NAS SVM 建立名稱映射

您可以使用 `vserver name-mapping create` 建立名稱對應的命令。您可以使用名稱對應來讓Windows使用者存取UNIX安全樣式的磁碟區和相反的磁碟區。

關於這項工作

針對每個SVM、ONTAP 支援最多12、500個各個方向的名稱對應。

步驟

1. 建立名稱對應：

```
vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-
unix|unix-win} -position integer -pattern text -replacement text
```

> ⓘ `-pattern`和 `-replacement`陳述式可做為規則運算式來表示。您也可以使用 `-replacement` null
> 置換字串（空格字元），使用陳述式明確拒絕對應至使用者 `" "`
> 。如link:https://docs.netapp.com/us-en/ontap-cli/vserver-name-mapping-create.html["指令參考資料ONTAP"^]需詳細 `vserver name-mapping create`資訊，請參閱。

建立Windows對UNIX的對應時、ONTAP 在建立新對應時、任何與該系統有開放連線的SMB用戶端、都必須登出並重新登入、才能看到新的對應。

範例

下列命令會在名為VS1的SVM上建立名稱對應。對應是從UNIX到Windows的對應、位於優先順序清單中的位置1。對應會將UNIX使用者johnd對應至Windows使用者ENH\JohnDoe。

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

下列命令會在名為VS1的SVM上建立另一個名稱對應。對應是從Windows到UNIX的對應、位於優先順序清單中的位置1。這裏的模式和替換包括正則表達式。對應會將網域中的每個CIFS使用者對應到與SVM相關聯的LDAP網域中的使用者。

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

下列命令會在名為VS1的SVM上建立另一個名稱對應。在此模式中、Windows使用者名稱中的「$」元素必須轉義、對應會將Windows使用者ENH\ John$ops對應至UNIX使用者john_ops。

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

為 **ONTAP NAS SVM** 配置預設用戶

您可以將預設使用者設定為在使用者的所有其他對應嘗試失敗時使用、或是不想在UNIX與Windows之間對應個別使用者時使用。或者、如果您想要驗證未對應的使用者失敗、則不應設定預設使用者。

關於這項工作

對於CIFS驗證、如果您不想將每個Windows使用者對應至個別的UNIX使用者、則可以改為指定預設的UNIX使用者。

對於NFS驗證、如果您不想將每個UNIX使用者對應至個別的Windows使用者、則可以改為指定預設的Windows使用者。

步驟

1. 執行下列其中一項動作：

如果您想要...	輸入下列命令...
設定預設UNIX使用者	`vserver cifs options modify -default-unix-user user_name`
設定預設的Windows使用者	`vserver nfs modify -default-win-user user_name`

用於管理 **NFS** 名稱對應的 **ONTAP** 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	`vserver name-mapping create`
在特定位置插入名稱對應	`vserver name-mapping insert`

顯示名稱對應	`vserver name-mapping show`
交換兩個名稱對應的位置附註：當名稱對應設定為IP辨識符號項目時、不允許交換。	`vserver name-mapping swap`
修改名稱對應	`vserver name-mapping modify`
刪除名稱對應	`vserver name-mapping delete`
驗證正確的名稱對應	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

如"指令參考資料ONTAP"需詳細 `vserver name-mapping`資訊，請參閱。

為 ONTAP SVM 啟用 Windows NFS 用戶端的存取

支援從Windows NFSv3用戶端存取檔案。ONTAP這表示執行支援 NFSv3 之 Windows 作業系統的用戶端可以存取叢集上 NFSv3 匯出的檔案。若要成功使用此功能、您必須正確設定儲存虛擬機器（SVM）、並注意某些需求和限制。

關於這項工作

依照預設、Windows NFSv3用戶端支援會停用。

開始之前

必須在SVM上啟用NFSv3。

步驟

1. 啟用Windows NFSv3用戶端支援：

   ```
   vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly disabled
   ```

2. 在所有支援 Windows NFSv3 用戶端的 SVM 上、停用 `-enable-ejukebox` 和 `-v3-connection-drop` 參數：

   ```
   vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection -drop disabled
   ```

   Windows NFSv3用戶端現在可以在儲存系統上掛載匯出。

3. 請指定、確保每個 Windows NFSv3 用戶端都使用硬掛載 `-o mtype=hard` 選項。

   這是確保可靠掛載的必要條件。

   ```
   mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
   ```

啟用 **ONTAP SVM** 的 **NFS** 用戶端上的匯出顯示

NFS 用戶端可以使用 `showmount -e` 命令以查看 ONTAP NFS 伺服器可用的匯出清單。這有助於使用者識別要掛載的檔案系統。

ONTAP預設允許 NFS 用戶端查看匯出清單。在舊版中， `showmount`必須明確啟用命令選項 `vserver nfs modify`。若要檢視匯出清單、應在SVM上啟用NFSv3。

範例

下列命令顯示名為VS1的SVM上的showmount功能：

```
clusterl : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
------- ---------
vs1     enabled
```

在NFS用戶端上執行的下列命令會顯示NFS伺服器上IP位址為10.63.21.9的匯出清單：

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix         (everyone)
/unix/unixl   (everyone)
/unix/unix2   (everyone)
/             (everyone)
```

使用 **NFS** 管理檔案存取

為 **ONTAP SVM** 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	`vserver nfs modify -vserver vserver_name -v3 enabled`
停用 NFSv3	`vserver nfs modify -vserver vserver_name -v3 disabled`

為 **ONTAP SVM** 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	`vserver nfs modify -vserver vserver_name -v4.0 enabled`
停用NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 disabled`

為 **ONTAP SVM** 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	`vserver nfs modify -vserver vserver_name -v4.1 enabled`
停用 NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 disabled`

管理 **ONTAP NFSv4** 儲存池限制

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

1. 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 storepool 限制控制	`vserver nfs storepool config modify -limit-enforce enabled`
停用 storepool 限制控制項	`vserver nfs storepool config modify -limit-enforce disabled`

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

1. 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.
```

為 ONTAP SVM 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

開始之前

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	`vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled`
停用pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled`

相關資訊

- NFS 主幹總覽

控制 ONTAP SVM 透過 TCP 和 UDP 進行的 NFS 訪問

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	`vserver nfs modify -vserver vserver_name -tcp enabled`
已透過TCP停用	`vserver nfs modify -vserver vserver_name -tcp disabled`
已透過udp啟用	`vserver nfs modify -vserver vserver_name -udp enabled`
已透過udp停用	`vserver nfs modify -vserver vserver_name -udp disabled`

控制來自 ONTAP SVM 非保留埠的 NFS 請求

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	`vserver nfs modify -vserver vserver_name -mount -rootonly disabled`
拒絕來自非保留連接埠的NFS掛載要求	`vserver nfs modify -vserver vserver_name -mount -rootonly enabled`
允許來自非保留連接埠的所有NFS要求	`vserver nfs modify -vserver vserver_name -nfs -rootonly disabled`
拒絕來自非保留連接埠的所有NFS要求	`vserver nfs modify -vserver vserver_name -nfs -rootonly enabled`

處理未知 **UNIX** 使用者對 **ONTAP NTFS** 磁碟區或 **qtree** 的 **NFS** 訪問

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。

開始之前

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	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled`
已停用	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled`

3. 返回管理權限層級：

   ```
   set -privilege admin
   ```

在非保留連接埠上掛載 **ONTAP NFS** 匯出的用戶端的注意事項

。 `-mount-rootonly` 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-rootonly` 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 **ONTAP NFS SVM** 的網域來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	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled`
已停用	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled`

3. 將權限等級設為admin：

   ```
   set -privilege admin
   ```

修改 **ONTAP SVM** 的 **NFSv3** 服務所使用的連接埠

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。

開始之前

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。

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

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 **ONTAP** 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	`vserver nfs create`
顯示NFS伺服器	`vserver nfs show`
修改NFS伺服器	`vserver nfs modify`
刪除NFS伺服器	`vserver nfs delete`

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

如"指令參考資料ONTAP"需詳細 `vserver nfs`資訊，請參閱。

解決 ONTAP NAS SVM 的名稱服務問題

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

1. 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	`vserver services name-service getxxbyyy getaddrinfo vserver services name-service getxxbyyy gethostbyname` （僅限IPv4 位址）
依群組ID的群組成員	`vserver services name-service getxxbyyy getgrbygid`
群組成員（依群組名稱）	`vserver services name-service getxxbyyy getgrbyname`
使用者所屬的群組清單	`vserver services name-service getxxbyyy getgrlist`

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

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
使用者或群組查詢失敗或產生不正確的結果	• 名稱服務交換器組態 • 來源組態（本機檔案、 NIS 網域、 LDAP 用戶端） • 網路組態（例如、LIF和Routes）
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 `-is-tld-query-enabled false` 選項 `vserver services name-service dns modify` 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 ONTAP NAS SVM 的名稱服務連接

您可以檢查 DNS 和輕量級目錄存取協定 (LDAP) 名稱伺服器以驗證它們是否已連接到ONTAP。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	`vserver services name-service dns check`
LDAP 組態狀態	`vserver services name-service ldap check`

```
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 **NAS** 名稱服務交換器條目的 **ONTAP** 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	`vserver services name-service ns-switch create`
顯示名稱服務交換器項目	`vserver services name-service ns-switch show`
修改名稱服務交換器項目	`vserver services name-service ns-switch modify`
刪除名稱服務交換器項目	`vserver services name-service ns-switch delete`

如"指令參考資料ONTAP"需詳細 `vserver services name-service ns-switch`資訊，請參閱。

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 NAS 名稱服務快取的 ONTAP 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	`vserver services name-service cache unix-user settings`
UNIX群組	`vserver services name-service cache unix-group settings`
UNIX網路群組	`vserver services name-service cache netgroups settings`
主機	`vserver services name-service cache hosts settings`
群組成員資格	`vserver services name-service cache group-membership settings`

相關資訊

"指令參考資料ONTAP"

用於管理 NFS 名稱對應的 ONTAP 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	`vserver name-mapping create`

在特定位置插入名稱對應	`vserver name-mapping insert`
顯示名稱對應	`vserver name-mapping show`
交換兩個名稱對應的位置附註：當名稱對應設定為IP辨識符號項目時、不允許交換。	`vserver name-mapping swap`
修改名稱對應	`vserver name-mapping modify`
刪除名稱對應	`vserver name-mapping delete`
驗證正確的名稱對應	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

如"指令參考資料ONTAP"需詳細 `vserver name-mapping`資訊，請參閱。

用於管理 NAS 本機 UNIX 使用者的 ONTAP 指令

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	`vserver services name-service unix-user create`
從URI載入本機UNIX使用者	`vserver services name-service unix-user load-from-uri`
顯示本機UNIX使用者	`vserver services name-service unix-user show`
修改本機UNIX使用者	`vserver services name-service unix-user modify`
刪除本機UNIX使用者	`vserver services name-service unix-user delete`

如"指令參考資料ONTAP"需詳細 `vserver services name-service unix-user`資訊，請參閱。

用於管理 NAS 本機 UNIX 群組的 ONTAP 指令

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	`vserver services name-service unix-group create`

新增使用者至本機UNIX群組	`vserver services name-service unix-group adduser`
從URI載入本機UNIX群組	`vserver services name-service unix-group load-from-uri`
顯示本機UNIX群組	`vserver services name-service unix-group show`
修改本機UNIX群組	`vserver services name-service unix-group modify`
從本機UNIX群組刪除使用者	`vserver services name-service unix-group deluser`
刪除本機UNIX群組	`vserver services name-service unix-group delete`

如"指令參考資料ONTAP"需詳細 `vserver services name-service unix-group`資訊，請參閱。

ONTAP NFS SVM 的本機 UNIX 使用者、群組和群組成員限制

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 ONTAP NFS SVM 的本機 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	`vserver services unix-user max-limit show`
顯示本機UNIX群組限制的相關資訊	`vserver services unix-group max-limit show`
修改本機UNIX使用者限制	`vserver services unix-user max-limit modify`
修改本機UNIX群組限制	`vserver services unix-group max-limit modify`

如"指令參考資料ONTAP"需詳細 `vserver services unix`資訊，請參閱。

用於管理 **NFS** 本機網路群組的 **ONTAP** 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	`vserver services name-service netgroup load`
驗證各節點的網路群組狀態	`vserver services name-service netgroup status` 可在進階權限層級或更高層級使用。
顯示本機網路群組	`vserver services name-service netgroup file show`
刪除本機網路群組	`vserver services name-service netgroup file delete`

如"指令參考資料ONTAP"需詳細 `vserver services name-service netgroup file`資訊，請參閱。

用於管理 **NFS NIS** 網域配置的 **ONTAP** 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	`vserver services name-service nis-domain create`
顯示 NIS 網域組態	`vserver services name-service nis-domain show`

顯示NIS網域組態的繫結狀態	`vserver services name-service nis-domain show-bound`
顯示 NIS 統計資料	`vserver services name-service nis-domain show-statistics` 可在進階權限層級或更高層級使用。
清除NIS統計資料	`vserver services name-service nis-domain clear-statistics` 可在進階權限層級或更高層級使用。
修改NIS網域組態	`vserver services name-service nis-domain modify`
刪除NIS網域組態	`vserver services name-service nis-domain delete`
啟用網路群組各主機搜尋的快取	`vserver services name-service nis-domain netgroup-database config modify` 可在進階權限層級或更高層級使用。

如"指令參考資料ONTAP"需詳細 `vserver services name-service nis-domain`資訊，請參閱。

用於管理 **NFS LDAP** 用戶端設定的 **ONTAP** 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	`vserver services name-service ldap client create`
顯示LDAP用戶端組態	`vserver services name-service ldap client show`
修改LDAP用戶端組態	`vserver services name-service ldap client modify`
變更LDAP用戶端的BIND密碼	`vserver services name-service ldap client modify-bind-password`
刪除LDAP用戶端組態	`vserver services name-service ldap client delete`

如"指令參考資料ONTAP"需詳細 `vserver services name-service ldap client`資訊，請參閱。

用於管理 **NFS LDAP** 配置的 **ONTAP** 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	`vserver services name-service ldap create`
顯示LDAP組態	`vserver services name-service ldap show`
修改LDAP組態	`vserver services name-service ldap modify`
刪除LDAP組態	`vserver services name-service ldap delete`

如"指令參考資料ONTAP"需詳細 `vserver services name-service ldap`資訊，請參閱。

用於管理 **NFS LDAP** 用戶端架構模板的 **ONTAP** 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	`vserver services name-service ldap client schema copy` 可在進階權限層級或更高層級使用。
顯示LDAP架構範本	`vserver services name-service ldap client schema show`
修改LDAP架構範本	`vserver services name-service ldap client schema modify` 可在進階權限層級或更高層級使用。
刪除LDAP架構範本	`vserver services name-service ldap client schema delete` 可在進階權限層級或更高層級使用。

如"指令參考資料ONTAP"需詳細 `vserver services name-service ldap client schema`資訊，請參閱。

用於管理 **NFS Kerberos** 介面設定的 **ONTAP** 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	`vserver nfs kerberos interface enable`
顯示NFS Kerberos介面組態	`vserver nfs kerberos interface show`
修改NFS Kerberos介面組態	`vserver nfs kerberos interface modify`

停用LIF上的NFS Kerberos	`vserver nfs kerberos interface disable`

如"指令參考資料ONTAP"需詳細 `vserver nfs kerberos interface`資訊，請參閱。

用於管理 **NFS Kerberos** 領域配置的 **ONTAP** 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	`vserver nfs kerberos realm create`
顯示NFS Kerberos領域組態	`vserver nfs kerberos realm show`
修改NFS Kerberos領域組態	`vserver nfs kerberos realm modify`
刪除NFS Kerberos領域組態	`vserver nfs kerberos realm delete`

如"指令參考資料ONTAP"需詳細 `vserver nfs kerberos realm`資訊，請參閱。

用於管理匯出策略的 **ONTAP** 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	`vserver export-policy show`
重新命名匯出原則	`vserver export-policy rename`
複製匯出原則	`vserver export-policy copy`
刪除匯出原則	`vserver export-policy delete`

如"指令參考資料ONTAP"需詳細 `vserver export-policy`資訊，請參閱。

用於管理匯出規則的 **ONTAP** 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	`vserver export-policy rule create`

顯示匯出規則的相關資訊	`vserver export-policy rule show`
修改匯出規則	`vserver export-policy rule modify`
刪除匯出規則	`vserver export-policy rule delete`

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"指令參考資料ONTAP"需詳細 `vserver export-policy`資訊，請參閱。

設定NFS認證快取

修改 **ONTAP SVM** 的 **NFS** 憑證快取生存時間的原因

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。

如果您...	優勢在於...	缺點是...
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

為 **ONTAP SVM** 配置快取 **NFS** 使用者憑證的生存時間

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	`vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live` 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）。
負面認證	`vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live` 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）。

3. 返回管理權限層級：

```
set -privilege admin
```

管理匯出原則快取

刷新 **ONTAP NAS SVM** 的匯出策略快取

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）	`vserver export-policy cache flush -vserver vserver_name`
匯出原則規則存取快取	`vserver export-policy cache flush -vserver vserver_name -cache access` 您可以加入選用的 `-node` 用於指定要清除存取快取的節點的參數。
主機名稱快取	`vserver export-policy cache flush -vserver vserver_name -cache host`
netgroup快取	`vserver export-policy cache flush -vserver vserver_name -cache netgroup` 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	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

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	`vserver export-policy cache flush -vserver vserver_name -cache access` 您可以加入選用的 `-node` 用於指定要清除存取快取的節點的參數。
主機名稱快取	`vserver services name-service cache hosts forward-lookup delete-all`
netgroup快取	`vserver services name-service cache netgroups ip-to-netgroup delete-all` `vserver services name-service cache netgroups members delete-all` 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	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

顯示 ONTAP NFS SVM 的匯出策略網路群組佇列和快取

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	`vserver export-policy netgroup queue show`
快取	`vserver export-policy netgroup cache show -vserver vserver_name`

如"指令參考資料ONTAP"需詳細 `vserver export-policy netgroup`資訊，請參閱。

檢查客戶端 IP 位址是否為 ONTAP NFS 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
```

優化 **ONTAP NFS SVM** 的存取快取效能

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	`vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value`
否定項目的重新整理期間	`vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value`
舊項目的逾時期間	`vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value`

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

了解 ONTAP NFS SVM 協定之間的檔案鎖定

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鎖定時、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。

了解 **ONTAP NFS SVM** 的唯讀位

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。

唯讀位元以下列方式與 ACL 和 Unix 模式位元互動：

當檔案設定了唯讀位元：

- 該文件的 ACL 不會發生任何變更。 NFS用戶端將看到與設定唯讀位元之前相同的 ACL。
- 任何允許對檔案進行寫入存取的 Unix 模式位元都會被忽略。
- NFS 和 SMB 用戶端都可以讀取該文件，但不能修改它。
- ACL 和 UNIX 模式位元將被忽略，取而代之的是唯讀位元。這意味著，即使 ACL 允許寫入訪問，只讀位元也會阻止修改。

當檔案未設定唯讀位元：

- ONTAP根據 ACL 和 UNIX 模式位元決定存取權限。
  - 如果 ACL 或 UNIX 模式位元拒絕寫入訪問，則 NFS 和 SMB 用戶端無法修改該檔案。
  - 如果 ACL 和 UNIX 模式位元均不拒絕寫入訪問，則 NFS 和 SMB 用戶端可以修改該檔案。

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。

了解 **ONTAP NFS** 和 **Windows** 在處理共用路徑元件鎖定方面有何不同

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"。

顯示有關 **ONTAP NFS SVM** 的鎖定訊息

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"指令參考資料ONTAP"需詳細 `vserver locks show`資訊，請參閱。

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 **ONTAP NFS SVM** 的檔案鎖

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

此 `vserver locks break`命令僅適用於進階權限層級及更高層級。如"指令參考資料ONTAP"需詳細 `vserver locks break`資訊，請參閱。

步驟

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

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

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	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
鎖定ID	`vserver locks break -lockid UUID`

4. 返回管理權限層級：

   ```
   set -privilege admin
   ```

了解 ONTAP FPolicy 首次讀取和首次寫入過濾器如何與 NFS 配合使用

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 ONTAP SVM 的 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	`vserver nfs modify -v4.1 -implementation-domain domain`
名稱	`vserver nfs modify -v4.1 -implementation-name name`
日期	`vserver nfs modify -v4.1 -implementation-date date`

3. 返回管理權限層級：

   ```
   set -privilege admin
   ```

管理NFSv4 ACL

了解為 ONTAP SVM 啟用 NFSv4 ACL 的好處

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

了解 **ONTAP SVM** 的 **NFSv4 ACL**

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。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 中所有已標記適當繼承旗標的存取控制項目（ 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。

如果參數已設為 `restricted`或 `vserver export-policy rule`系列中的命令 `vserver nfs`，則`-chown-mode`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，進階使用者也只能變更檔案擁有權。如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

為 **ONTAP SVM** 啟用或停用 **NFSv4 ACL** 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）	`vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled`
變更模式位元時、請停用保留和丟棄NFSv4 ACL	`vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled`

3. 返回管理權限層級：

```
set -privilege admin
```

了解 **ONTAP** 如何使用 **NFSv4 ACL** 來決定是否可以刪除文件

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。

為 **ONTAP SVM** 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： `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`
停用NFSv4.0 ACL	輸入下列命令： `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`
啟用 NFSv4.1 ACL	輸入下列命令： `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`

停用 NFSv4.1 ACL	輸入下列命令： `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

修改 **ONTAP SVM** 的 **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

為 **ONTAP SVM** 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： `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled`
啟用 NFSv4.1 讀取檔案委派	輸入下列命令： + `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled`
停用NFSv4讀取檔案委派	輸入下列命令： `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled`
停用 NFSv4.1 讀取檔案委派	輸入下列命令： `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled`

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。

為 **ONTAP SVM** 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：`vserver nfs modify -vserver vserver_name -v4.0-write -delegation enabled`

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

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

了解 ONTAP SVM 的 NFSv4 檔案和記錄鎖定

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 ONTAP SVM 的 NFSv4 鎖定租賃期

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
```

為 ONTAP SVM 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
   ```

了解 ONTAP SVM 的 NFSv4 引用

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 ONTAP SVM 的 NFSv4 引用

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。

開始之前

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	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled`
停用NFSv4參照	`vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled`
啟用 NFSv4.1 參照	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled`
停用 NFSv4.1 參照	`vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled`

3. 返回管理權限層級：

   ```
   set -privilege admin
   ```

顯示 **ONTAP NFS SVM** 的統計訊息

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"
- "統計目錄物件顯示"
- "統計數據顯示"
- "統計開始"
- "統計停止"

顯示 ONTAP NFS SVM 的 DNS 統計訊息

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"
- "統計目錄物件顯示"
- "統計數據顯示"
- "統計開始"
- "統計停止"

顯示 ONTAP NFS SVM 的 NIS 統計資訊

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"
- "統計目錄物件顯示"
- "統計數據顯示"
- "統計開始"
- "統計停止"

了解對 **VMware vStorage over ONTAP NFS** 的支持

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？"

啟用或停用基於 **ONTAP NFS** 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	`vserver nfs modify -vserver vserver_name -vstorage enabled`
停用VMware vStorage支援	`vserver nfs modify -vserver vserver_name -vstorage disabled`

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 VAA__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"

在 ONTAP NFS SVM 上啟用或停用 rquota 支持

遠端配額傳輸協定（ rquota ）可讓 NFS 用戶端從遠端機器取得使用者的配額資訊。rquota 版本的支援會因您的 ONTAP 版本而異。

- ONTAP 9 及更新版本支援 rquota v1 。
- ONTAP 9.12.1 及更新版本支援 rquota v2 。

  如果您從 rquota v1 升級到 rquota v2，您可能會注意到用戶配額限制發生了意外變化。此變化是由於 rquota v1 和 rquota v2 之間的配額計算方式不同所造成的。欲了解更多信息，請參閱"NetApp知識庫：用戶配額限制為何意外變化"。

關於這項工作

預設會停用rquota。

步驟

1. 啟用或停用 rquota ：

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

如需配額的詳細資訊、請參閱 "邏輯儲存管理"。

了解 NFSv3 和 NFSv4 效能改進以及 ONTAP SVM 的 TCP 傳輸大小

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 **ONTAP SVM** 的 **NFSv3** 和 **NFSv4 TCP** 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	`vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size`

選項	範圍	預設
`-tcp-max-xfer-size`	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
```

配置 ONTAP SVM 的 NFS 使用者允許的群組 ID 數量

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。

了解啟用擴充組的 AUTH_SYS 驗證先決條件(`-auth-sys-extended-groups`) 使用超出預設最大 16 個群組 ID，請參閱"NetApp知識庫：啟用 auth-sys-extended-groups 的先決條件是什麼？"

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

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`32`
	
	`disabled`
	
	這些是預設設定。
		RPCSEC_GSS：32
		
		AUTH_SYS：16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`256`
	
	`disabled`
		RPCSEC_GSS ： 256
		
		AUTH_SYS：16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`512`
	
	`enabled`
		RPCSEC_GSS ： 512
		
		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	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled`
適用於RPCSEC_GSS和AUTH_SYS	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled`

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
```

相關資訊

- "NetApp知識庫：針對ONTAP 9 的 NFS 驗證的 AUTH_SYS 擴充組更改"

控制根用戶對 ONTAP SVM 的 NTFS 安全模式資料的存取

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	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled`
略過NT ACL檢查	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled`

   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
   ```

支援的NFS版本和用戶端

了解支援的 ONTAP NFS 版本和用戶端

在網路中使用NFS之前、您必須先知道哪些NFS版本和用戶端ONTAP 支援哪些NFS。

下表指出ONTAP 、在預設情況下、當支援主要和次要NFS傳輸協定版本時、依預設、支援並不表示這是ONTAP 支援該NFS傳輸協定的最早版本。

版本	支援	引進
NFSv3.	是的	所有 ONTAP 版本
NFSv4.0	是的	版本8 ONTAP
NFSv4.1	是的	版本8.1 ONTAP

版本	支援	引進
NFSv4.2	是的	部分9.8 ONTAP
pNFS	是的	版本8.1 ONTAP

如需NFS用戶端ONTAP 所支援的最新資訊、請參閱互通性對照表。

"NetApp 互通性對照表工具"

了解 **ONTAP** 對 **NFSv4.0** 功能的支持

除了SPKM3和LIPKEYY安全機制、支援NFSv4.0中的所有必要功能。ONTAP

支援下列NFSv4功能：

- 複合

  允許用戶端在單一遠端程序呼叫（RPC）要求中要求多個檔案作業。

- 檔案委派

  可讓伺服器將檔案控制權委派給某些類型的用戶端、以進行讀取和寫入存取。

- 虛擬**FS**

  由NFSv4伺服器用來判斷儲存系統上的掛載點。NFSv4中沒有掛載傳輸協定。

- 鎖定

  租賃型。NFSv4中沒有個別的網路鎖定管理程式（NLM）或網路狀態監視器（NSM）傳輸協定。

如需NFSv4.0傳輸協定的詳細資訊、請參閱RFC 3530。

了解 **ONTAP** 對 **NFSv4** 的支援限制

您應該瞭ONTAP 解NFSv4支援的若干項功能限制。

- 委派功能不受每種用戶端類型支援。
- 在更新版本的版本中、除了UTF8磁碟區之外、其他磁碟區上的非Ascii字元名稱會被儲存系統拒絕。ONTAP

  在更新版本的發行版中、使用utf8mb4語言設定建立並使用NFS v4掛載的Volume不再受此限制。ONTAP

- 所有檔案處理常式；伺服器不會提供揮發性檔案處理常式。
- 不支援移轉與複寫。
- NFSv4用戶端不支援唯讀負載共用鏡像。

  將NFSv4用戶端路由至負載共用鏡射的來源、以進行直接讀取和寫入存取。ONTAP

- 不支援命名屬性。
- 支援所有建議的屬性、但下列項目除外：
  - `archive`
  - `hidden`
  - `homogeneous`
  - `mimetype`
  - `quota_avail_hard`
  - `quota_avail_soft`
  - `quota_used`
  - `system`
  - `time_backup`

> 雖然它不支援 `quota*` 屬性、 ONTAP 確實透過 RQUOTA 側頻傳輸協定支援使用者和群組配額。

了解 **ONTAP** 對 **NFSv4.1** 的支持

從功能不支援的問題9.8開始ONTAP 、NFSv4.1啟用時、預設會提供nconnect功能。

較早的NFS用戶端實作只使用單一TCP連線與掛載。在鏈接功能中、單一TCP連線可能會成為瓶頸、導致IOPS增加。ONTAP

nconnect 透過允許單一掛載點建立多個 TCP 連線（最多 16 個），提高了 NFS 用戶端的效能，有助於克服隨著 IOPS 增加，單一 TCP 連線可能出現的效能瓶頸。

NFSv4.1預設會在ONTAP 更新版本的版本中啟用。在舊版中、您可以透過指定來啟用 `-v4.1` 選項並將其設定為 `enabled` 在儲存虛擬機器（ SVM ）上建立 NFS 伺服器時。

不支援NFSv4.1目錄和檔案層級委派。ONTAP

相關資訊

"了解 nconnect 如何提升 NFS 效能"。

了解 **ONTAP** 對 **NFSv4.2** 的支持

從 ONTAP 9.8 開始、 ONTAP 支援 NFSv4.2 傳輸協定、以允許啟用 NFSv4.2 的用戶端存取。

ONTAP 9.9.1 及更高版本預設為啟用 NFSv4.2。在ONTAP 9.8 中，需要透過指定以下參數手動啟用 v4.2： `-v4.2`選項並將其設為 `enabled`在儲存虛擬機器 (SVM) 上建立 NFS 伺服器時。啟用 NFSv4.1 也允許客戶端在掛載為 v4.2 時使用 NFSv4.1 的功能。

後續的 ONTAP 版本擴大支援 NFSv4.2 選用功能。

開始於...	**NFSv4.2** 選用功能包括 ...
ONTAP 9.12.1	• NFS擴充屬性 • 稀疏檔案 • 空間保留
部分9.9.1 ONTAP	標示為NFS的強制存取控制（MAC）

NFS v4.2 安全性標籤

從ONTAP 推出支援NFS9.9.1的功能開始、就能啟用NFS安全標籤。依預設會停用。

使用NFS v4.2安全性標籤時、ONTAP 即可識別出需求性的NFS伺服器存取控制（MAC）、儲存及擷取用戶端傳送的sec_label屬性。

如需詳細資訊、請參閱 "RFC 7240"。

從ONTAP S廳9.12.1開始、支援NDMP傾印作業的NFS v4.2安全標籤。如果在舊版的檔案或目錄上遇到安全性標籤、傾印就會失敗。

步驟

1. 將權限設定變更為進階：

```
set -privilege advanced
```

2. 啟用安全性標籤：

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel enabled
```

NFS擴充屬性

從S廳9.12.1開始ONTAP 、預設會啟用NFS擴充屬性（xattro）。

延伸屬性是定義的標準NFS屬性 "RFC 8276" 並在現代化的NFS用戶端中啟用。它們可用於將使用者定義的中繼資料附加至檔案系統物件、而且對進階安全性部署非常感興趣。

NDMP傾印作業目前不支援NFS擴充屬性。如果在檔案或目錄上遇到延伸屬性、傾印會繼續進行、但不會備份這些檔案或目錄上的延伸屬性。

如果您需要停用延伸屬性、請使用 `vserver nfs modify -v4.2-xattrs disabled` 命令。

了解 **nconnect** 如何提升 **NFS** 效能

從ONTAP 9.8 開始，啟用 NFSv4.1 時，nconnect 功能預設可用。 nconnect 透過允許單一掛載點建立多個 TCP 連線來提升 NFS 用戶端效能。

nconnect 的工作原理

較早的NFS用戶端實作只使用單一TCP連線與掛載。在鏈接功能中、單一TCP連線可能會成為瓶頸、導致IOPS增加。ONTAP

啟用 nconnect 的用戶端可以為單一 NFS 掛載點建立多個 TCP 連線（最多 16 個）。 nconnect 僅使用一個 IP 位址，並透過該 IP 位址建立多個 TCP 連線來掛載 NFS 匯出。NFS 用戶端以輪詢方式將檔案操作指派到多個 TCP 連線上，從而從可用的網路頻寬中獲得更高的吞吐量。

支援的 NFS 版本

- 建議將 nconnect 用於 NFSv3、NFSv4.2 和 NFSv4.1 掛載。
- 不建議將 nconnect 用於 NFSv4.0 掛載。

> 為了獲得最佳效能， NetApp建議使用 nconnect 搭配 NFSv4.1，而不是 NFSv4.0。雖然 NFSv4.0 支援多個連接，但 NFSv4.1 與 nconnect 結合使用可提供更好的負載分配和更高的吞吐量。

客戶支援

請參閱NFS用戶端文件、確認您的用戶端版本是否支援nconnect。

相關資訊

- "了解 ONTAP 對 NFSv4.1 的支持"
- "了解 ONTAP 對 NFSv4.2 的支持"

了解 ONTAP 對平行 NFS 的支持

支援平行NFS（pNFS）ONTAP 。pNFS傳輸協定可讓用戶端直接存取分散在叢集多個節點上的一組檔案資料、藉此提升效能。它可協助用戶端找到磁碟區的最佳路徑。

了解 ONTAP NFS 硬掛載

疑難排解掛載問題時、您必須確定使用正確的掛載類型。NFS支援兩種掛載類型：軟掛載和硬掛載。基於可靠性考量、您只能使用硬體掛載。

您不應該使用軟掛載、尤其是在NFS逾時頻繁的情況下。競爭情況可能是因為這些逾時而發生、可能導致資料毀損。

並行 NFS

簡介

了解ONTAP中的平行 NFS (pNFS)

並行 NFS 於 2010 年 1 月作為 RFC 標準 RFC-5661 推出，旨在透過分離元資料和資料路

徑，允許客戶端直接存取 NFSv4.1 伺服器上的檔案資料。這種直接存取方式透過資料本地化、CPU效率和操作並行化帶來效能優勢。2018 年編寫了後續的 RFC，涵蓋 pNFS 佈局類型（RFC-8434），其中定義了文件、區塊和物件佈局的標準。ONTAP利用 pNFS 操作的檔案佈局類型。

> 從 2024 年 7 月開始，先前以 PDF 形式發布的技術報告內容已與ONTAP產品文件整合。ONTAP NFS 儲存管理文件現在包含了來自 *TR-4063： NetApp ONTAP* 中的平行網路檔案系統 *(pNFS)* 的內容。

多年來，NFSv3 一直是 NFS 協定的標準版本，幾乎適用於所有用例。然而，該協定存在一些局限性，例如缺乏狀態性、權限模型簡陋以及基本的鎖定功能。NFSv4.0 (RFC 7530) 在 NFSv3 的基礎上進行了一系列改進，隨後的 NFSv4.1 (RFC 5661) 和 NFSv4.2 (RFC 7862) 版本進一步改進了這些改進，增加了並行 NFS (pNFS) 等功能。

NFSv4.x 的優勢

NFSv4.x 相較於 NFSv3 有下列優勢：

- 由於 NFSv4 僅使用單一連接埠（2049）進行操作，因此對防火牆友善。
- 進階且積極的快取管理，例如 NFSv4.x 中的委託機制
- 採用密碼學的強大 RPC 安全選項
- 字元國際化
- 複合操作
- 僅支援 TCP
- 有狀態協定（不像NFSv3那樣是無狀態的）
- 全面整合 Kerberos，實現高效率的身份驗證機制
- NFS轉診
- 支援與 UNIX 和 Windows 相容的存取控制
- 基於字串的使用者和群組標識符
- pNFS（NFSv4.1）
- 擴展屬性（NFSv4.2）
- 安全標籤（NFSv4.2）
- 稀疏檔案操作（FALLOCATE）（NFSv4.2）

有關 NFSv4.x 的更多信息，包括最佳實踐和功能詳情，請參閱 "NetApp技術報告4067：NFS最佳實務與實作指南"。

相關資訊

- "NFS組態總覽"
- "NFS 管理概述"
- "資料區管理FlexGroup"
- "NFS 主幹總覽"

- https://www.netapp.com/pdf.html?item=/media/19370-tr-4523.pdf
- "NetApp技術報告4616：ONTAP NFS Kerberos in Some with Microsoft Active Directory"

了解**ONTAP**中的 **pNFS** 架構

pNFS 架構由三個主要元件組成：支援 pNFS 的 NFS 用戶端、為元資料操作提供專用路徑的元資料伺服器以及提供檔案本地化路徑的資料伺服器。

用戶端存取 pNFS 需要與 NFS 伺服器上的資料和元資料路徑建立網路連線。如果 NFS 伺服器包含用戶端無法存取的網路接口，則伺服器可能會向客戶端通告無法存取的資料路徑，從而導致服務中斷。

元資料伺服器

當用戶端使用 NFSv4.1 或更高版本發起掛載，且 NFS 伺服器上啟用了 pNFS 時，pNFS 中的元資料伺服器就會建立。完成此操作後，所有元資料流量都將透過此連接發送，並在掛載期間保持在此連接上，即使介面遷移到另一個節點。

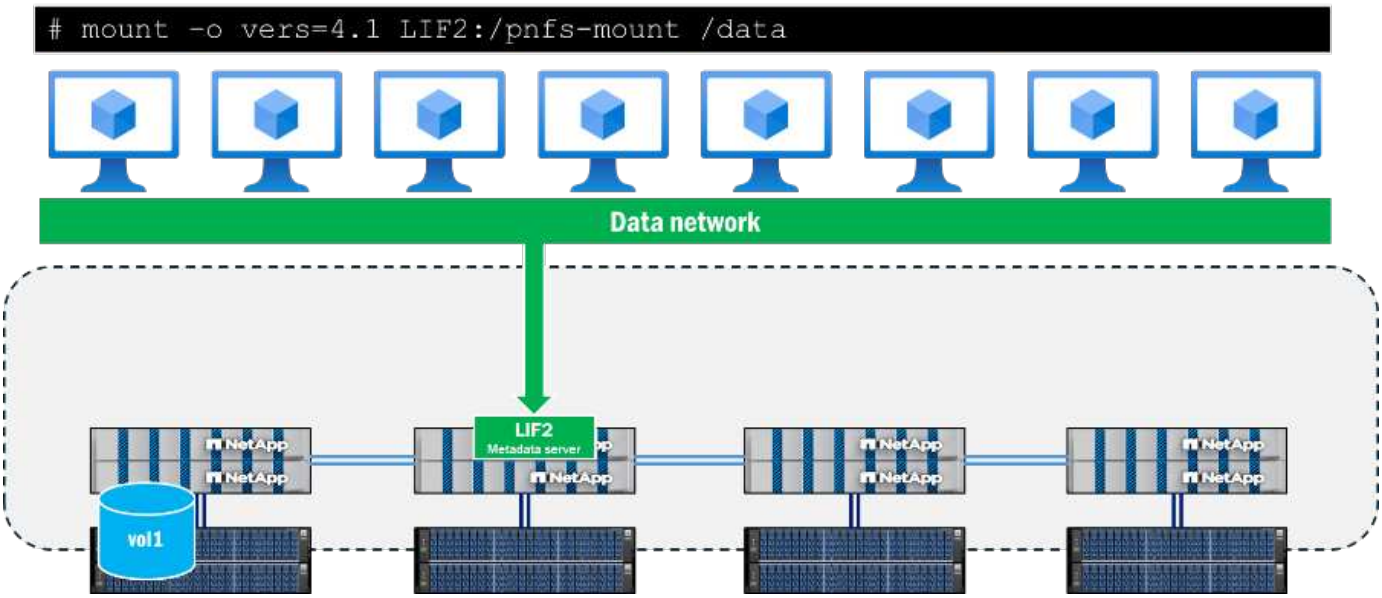


圖 **1.** 在**ONTAP**的 **pNFS** 中建立元資料伺服器

pNFS 支援是在掛載呼叫期間確定的，具體是在 EXCHANGE_ID 呼叫中確定的。在 NFS 操作下方的封包擷取中可以看到這個標誌。當 pNFS 標誌 `EXCHGID4_FLAG_USE_PNFS_DS` 和 `EXCHGID4_FLAG_USE_PNFS_MDS` 如果設定為 1，則該介面符合 pNFS 中的資料和元資料操作條件。

```
Operations (count: 1)
  Opcode: EXCHANGE_ID (42)
      Status: NFS4_OK (0)
      clientid: 0x004050a97100001c
      seqid: 0x00000001
    flags: 0x00060100, EXCHGID4_FLAG_USE_PNFS_DS, EXCHGID4_FLAG_USE_PNFS_MDS, EXCHGID4_FLAG_BIND_PRINC
        0... .... .... .... .... .... .... .... = EXCHGID4_FLAG_CONFIRMED_R: Not set
        .0.. .... .... .... .... .... .... .... = EXCHGID4_FLAG_UPD_CONFIRMED_REC_A: Not set
        .... .... .... .1.. .... .... .... .... = EXCHGID4_FLAG_USE_PNFS_DS: Set
        .... .... .... ..1. .... .... .... .... = EXCHGID4_FLAG_USE_PNFS_MDS: Set
        .... .... .... ...0 .... .... .... .... = EXCHGID4_FLAG_USE_NON_PNFS: Not set
        .... .... .... .... .... ...1 .... .... = EXCHGID4_FLAG_BIND_PRINC_STATEID: Set
        .... .... .... .... .... .... .... ..0. = EXCHGID4_FLAG_SUPP_MOVED_MIGR: Not set
        .... .... .... .... .... .... .... ...0 = EXCHGID4_FLAG_SUPP_MOVED_REFER: Not set
```

圖 **2. pNFS**掛載的資料包捕獲

NFS 中的元資料通常包括檔案和資料夾屬性，例如檔案句柄、權限、存取和修改時間以及所有權資訊。元資料還可以包括建立和刪除呼叫、連結和取消連結呼叫以及重新命名。

在 pNFS 中，還有一部分元資料呼叫是 pNFS 特性特有的，這些呼叫將在後續章節中進行更詳細的介紹。 "RFC 5661"。這些呼叫用於協助確定 pNFS 合格設備、設備到資料集的映射以及其他所需資訊。下表列出了 pNFS 特有的元資料操作。

營運	說明
佈局獲取	從元資料伺服器取得資料伺服器對應。
佈局委員會	伺服器提交佈局並更新元資料映射。
佈局返回	返回佈局；如果資料被修改，則傳回新佈局。
取得設備資訊	客戶端取得儲存叢集中資料伺服器的最新資訊。
取得設備列表	客戶端請求提供參與儲存叢集的所有資料伺服器的清單。
CB_LAYOUTRECALL	如果偵測到衝突，伺服器會從客戶端呼叫資料佈局。
CB_RECALL_ANY	將所有佈局傳回給元資料伺服器。
CB_NOTIFY_DEVICEID	設備 ID 發生任何變更時發出通知。

資料路徑資訊

元資料伺服器建立並開始資料操作後， ONTAP開始追蹤符合 pNFS 讀取和寫入操作條件的設備 ID，以及將叢集中的磁碟區與本機網路介面關聯起來的設備對應。當對掛載點執行讀取或寫入操作時，就會發生此程序。元資料調用，例如 `GETATTR`不會觸發這些設備映射。因此，運行一個 `ls` 掛載點內的命令不會更新映射。

可以使用ONTAP CLI 的高階權限查看設備和映射，如下所示。

```
::*> pnfs devices show -vserver DEMO
  (vserver nfs pnfs devices show)
Vserver Name     Mapping ID      Volume MSID     Mapping Status
Generation
---------------  --------------- --------------- ---------------
-------------
DEMO             16              2157024470      available       1

::*> pnfs devices mappings show -vserver SVM
  (vserver nfs pnfs devices mappings show)
Vserver Name    Mapping ID      Dsid            LIF IP
--------------  --------------- --------------- --------------------
DEMO            16              2488            10.193.67.211
```

這些指令中沒有磁碟區名稱。相反，將使用與這些磁碟區關聯的數字 ID：主集 ID (MSID) 和資料集 ID (DSID)。若要尋找與映射相關的體積，您可以使用 `volume show -dsid [dsid_numeric]` 或者 `volume show -msid [msid_numeric]` 具備ONTAP CLI 的高階權限。

當客戶端嘗試讀取或寫入位於遠離元資料伺服器連接的節點上的檔案時，pNFS 將協商適當的存取路徑，以確保這些操作的資料本地性，並且客戶端將重定向到已發布的 pNFS 設備，而不是嘗試穿越叢集網路來存取該檔案。這有助於降低CPU佔用率和網路延遲。

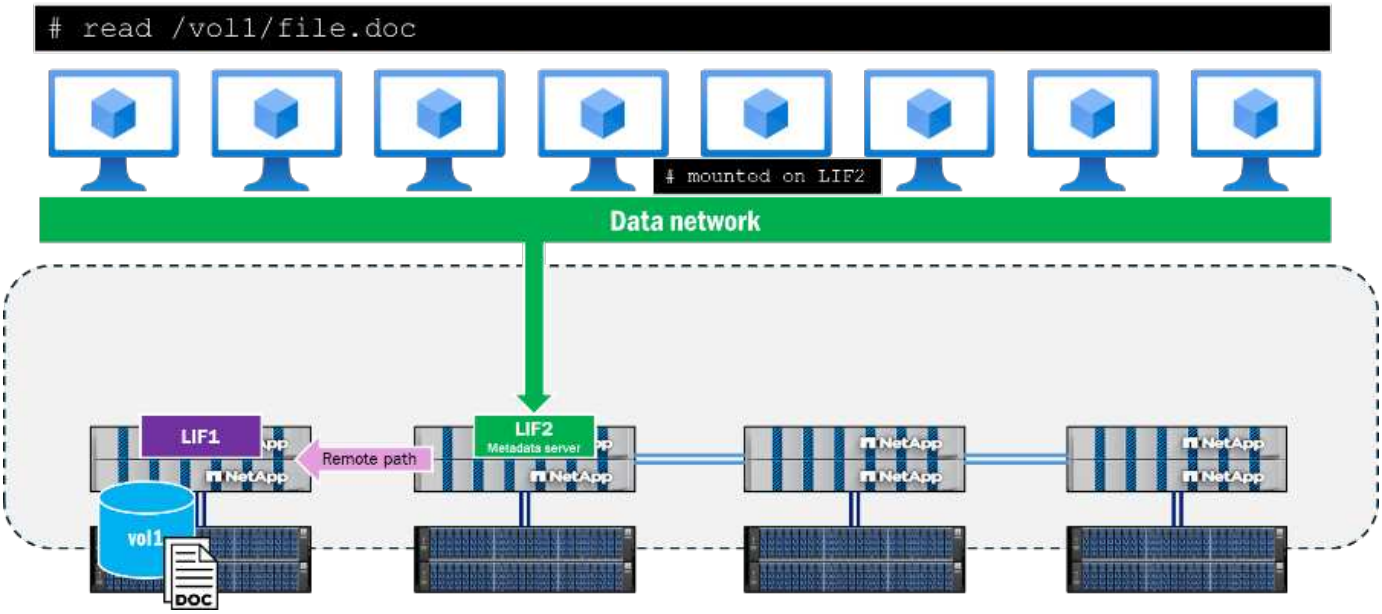


圖 3. 使用 **NFSv4.1** 的遠端讀取路徑，無需 **pNFS**

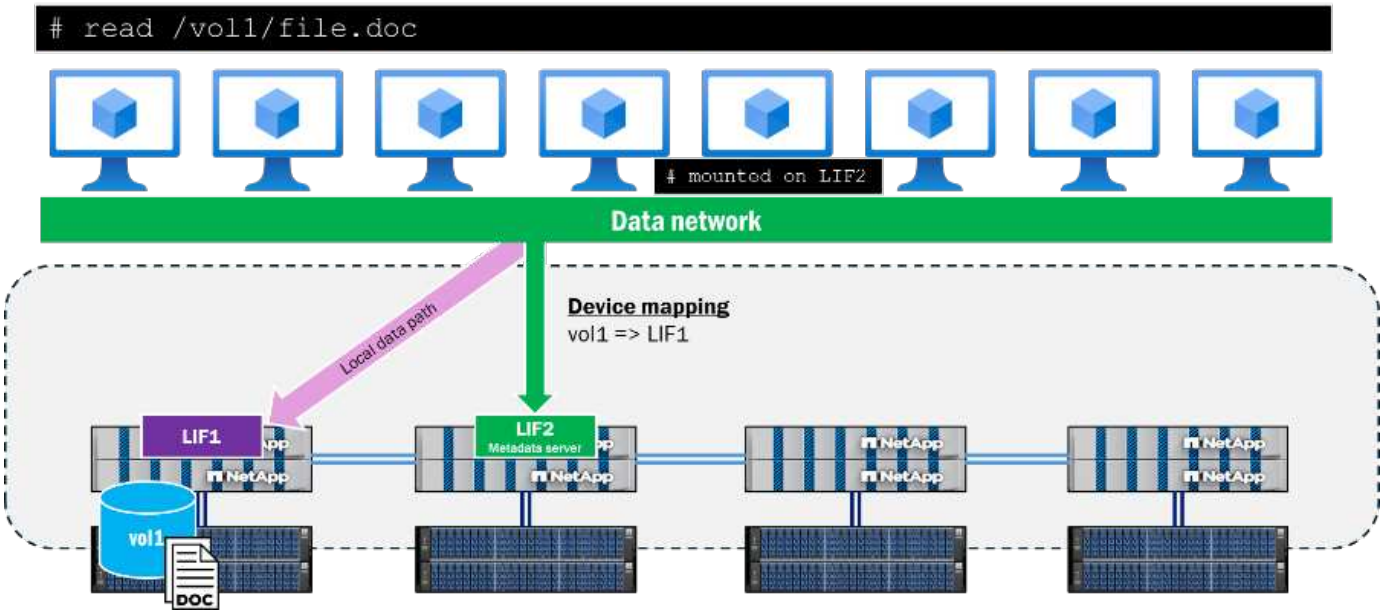


圖 **4.** 使用 **pNFS** 的本地化讀取路徑

pNFS 控制路徑

除了 pNFS 的元資料和資料部分之外，還有一個 pNFS 控制路徑。控制路徑由 NFS 伺服器用於同步檔案系統資訊。在ONTAP集群中，後端集群網路會定期複製，以確保所有 pNFS 設備和設備映射保持同步。

pNFS 設備群組工作流程

以下描述了客戶端請求讀取或寫入磁碟區中的檔案後，pNFS 設備如何在ONTAP中填入。

1. 客戶端請求讀取或寫入；執行 OPEN 操作並檢索檔案句柄。
2. 執行 OPEN 操作後，用戶端透過元資料伺服器連接，以 LAYOUTGET 呼叫的方式將檔案句柄傳送至儲存裝置。
3. LAYOUTGET 向客戶端傳回有關文件佈局的信息，例如狀態 ID、條帶大小、文件段和裝置 ID。
4. 然後客戶端取得裝置 ID，並向伺服器發送 GETDEVINFO 呼叫以檢索與該裝置關聯的 IP 位址。
5. 儲存裝置會傳送回覆，其中包含用於本機存取該裝置的關聯 IP 位址清單。
6. 用戶端透過儲存設備傳回的本機 IP 位址繼續進行 NFS 通訊。

pNFS與FlexGroup體積的交互

ONTAP中的FlexGroup磁碟區將儲存呈現為跨越叢集中多個節點的FlexVol volume組成部分，從而允許工作負載利用多個硬體資源，同時保持單一掛載點。由於多個具有多個網路介面的節點與工作負載交互，因此在ONTAP中看到遠端流量穿越後端叢集網路是很自然的結果。

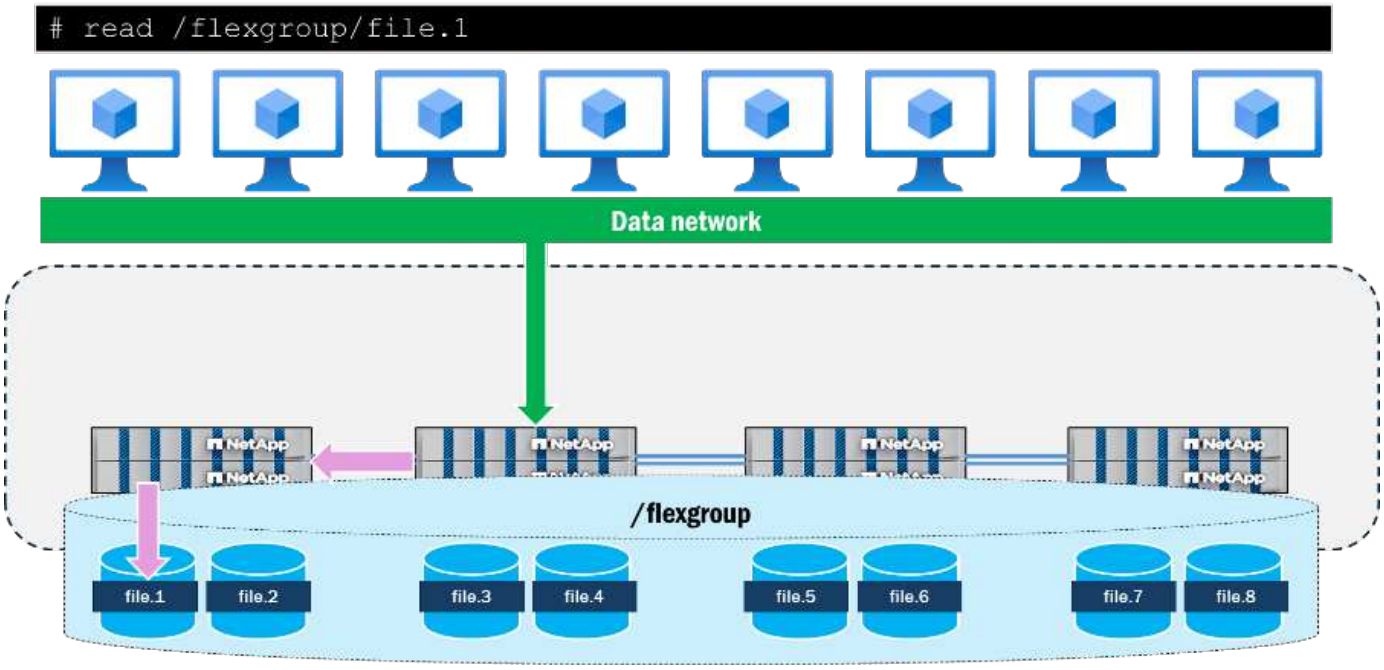


圖 **5.** 在不使用 **pNFS** 的情況下，透過**FlexGroup**磁碟區存取單一文件

使用 pNFS 時， ONTAP會追蹤FlexGroup磁碟區的檔案和磁碟區佈局，並將它們對應到叢集中的本機資料介面。例如，如果包含正在存取的檔案的組成磁碟區位於節點 1 上，則ONTAP將通知用戶端將資料流量重新導向至節點 1 上的資料介面。

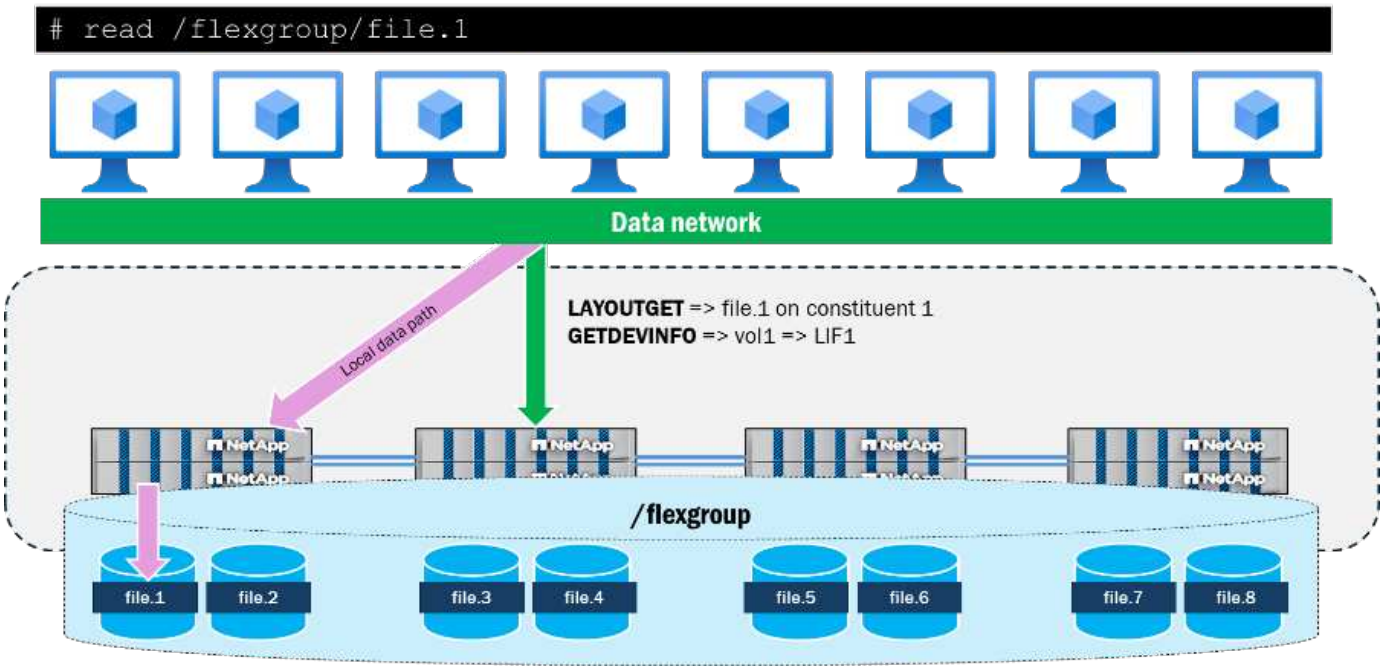


圖 **6.** 在**FlexGroup**區中使用 **pNFS** 進行單一檔案存取

pNFS 也提供了從單一客戶端呈現平行網路路徑到檔案的功能，而沒有 pNFS 的 NFSv4.1 則不具備此功能。例如，如果用戶端想要使用 NFSv4.1（不使用 pNFS）從相同掛載點同時存取四個文件，則所有文件都將使用相同的網路路徑， ONTAP叢集將改為向這些文件發送遠端請求。掛載路徑可能會成為操作的瓶頸，因為它們都遵循一條路徑到達同一個節點，並且還要處理元資料操作以及資料操作。

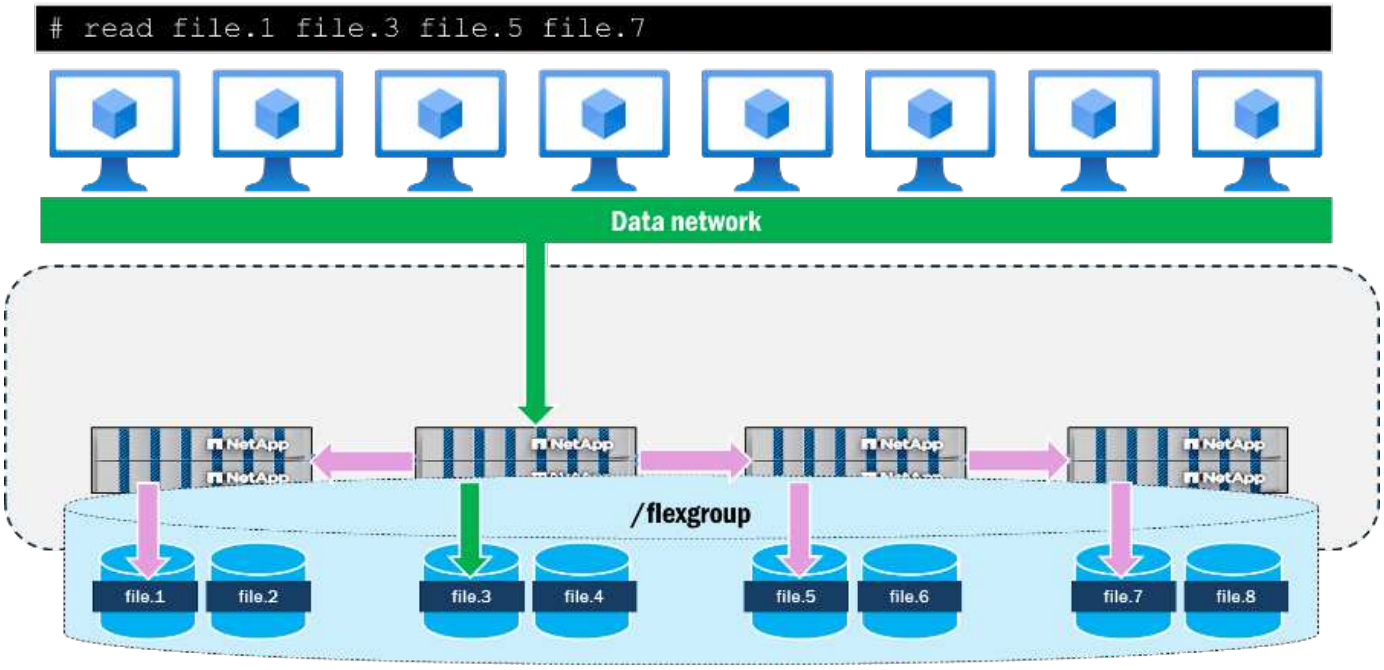


圖 **7.** 在不使用 **pNFS** 的情況下， **FlexGroup**磁碟區中可同時存取多個檔案。

當使用 pNFS 從單一客戶端同時存取相同的四個檔案時，用戶端和伺服器會協商每個節點上的檔案本機路徑，並使用多個 TCP 連線進行資料操作，而掛載路徑則作為所有元資料操作的位置。這樣既可以利用本地檔案路徑來降低延遲，也可以透過使用多個網路介面來提高吞吐量，前提是客戶端可以發送足夠的資料來使網路飽和。

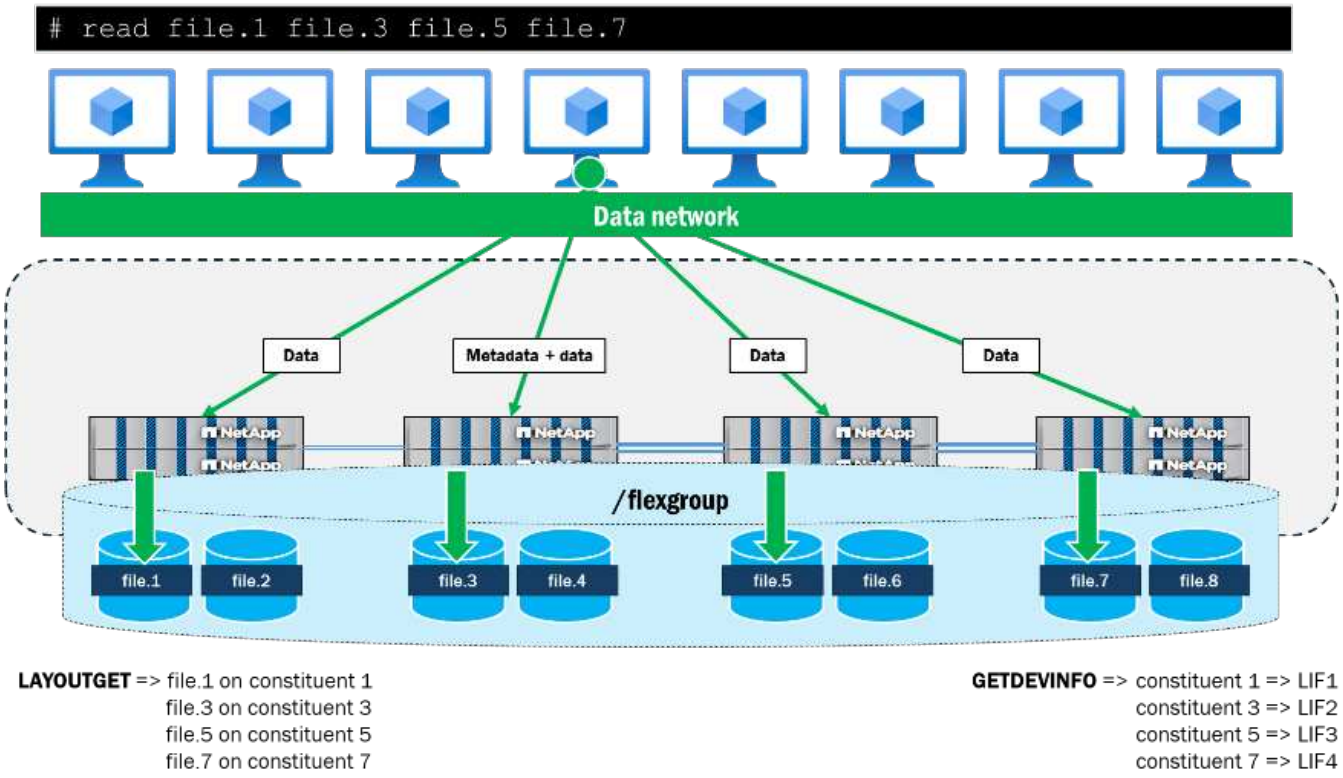


圖 **8.** 在**FlexGroup**卷中使用 **pNFS** 實現多個文件同時訪問

以下顯示的是在單一 RHEL 9.5 用戶端上進行簡單測試運行的結果，其中使用 dd 並行讀取四個 10GB 檔案（全部位於兩個ONTAP叢集節點的不同組成磁碟區上）。使用 pNFS 時，每個檔案的整體吞吐量和完成時間都提高了。當不使用 pNFS 而使用 NFSv4.1 時，掛載點本機檔案和遠端檔案之間的效能差異比使用 pNFS 時更大。

測試	每個檔案的吞吐量（**MB/s**）	每個文件的完成時間
NFSv4.1：無 pNFS	• 文件 1–228（本地） • 文件.2–227（本地） • 文件.3–192（遠端） • 文件.4–192（遠端）	• 文件 1–46（本地） • 文件.2–46.1（本地） • 文件.3–54.5（遠端） • 文件.4–54.5（遠端）
NFSv4.1：與 pNFS	• 文件 1–248（本地） • 文件.2–246（本地） • 文件.3–244（本地透過pNFS） • 文件.4–244（本地透過pNFS）	• 文件.1–42.3（本地） • 文件.2–42.6（本地） • 文件.3–43（本地透過pNFS） • 文件 4–43（本地透過 pNFS）

相關資訊

- "資料區管理FlexGroup"
- "NetApp技術報告 4571： FlexGroup最佳實踐"

ONTAP中的 **pNFS** 用例

pNFS 可以與ONTAP 的各種功能一起使用，以提高效能並為 NFS 工作負載提供更大的靈活性。

使用 **nconnect** 的 **pNFS**

NFS 為一些較新的客戶端和伺服器引入了一種新的掛載選項，該選項提供了一種在掛載單一 IP 位址的同時提供多個 TCP 連線的方法。這提供了一種機制，可以更好地並行化操作，繞過 NFS 伺服器和客戶端的限制，並有可能為某些工作負載提供更高的整體效能。 ONTAP 9.8 及更高版本支援 nconnect，前提是用戶端支援 nconnect。

當使用 nconnect 連接 pNFS 時，將使用 nconnect 選項並行連接 NFS 伺服器通告的每個 pNFS 裝置。例如，如果 nconnect 設置為 4，並且有 4 個符合 pNFS 條件的接口，則每個掛載點創建的連接總數最多為 16 個（4 個 nconnect x 4 個 IP 位址）。

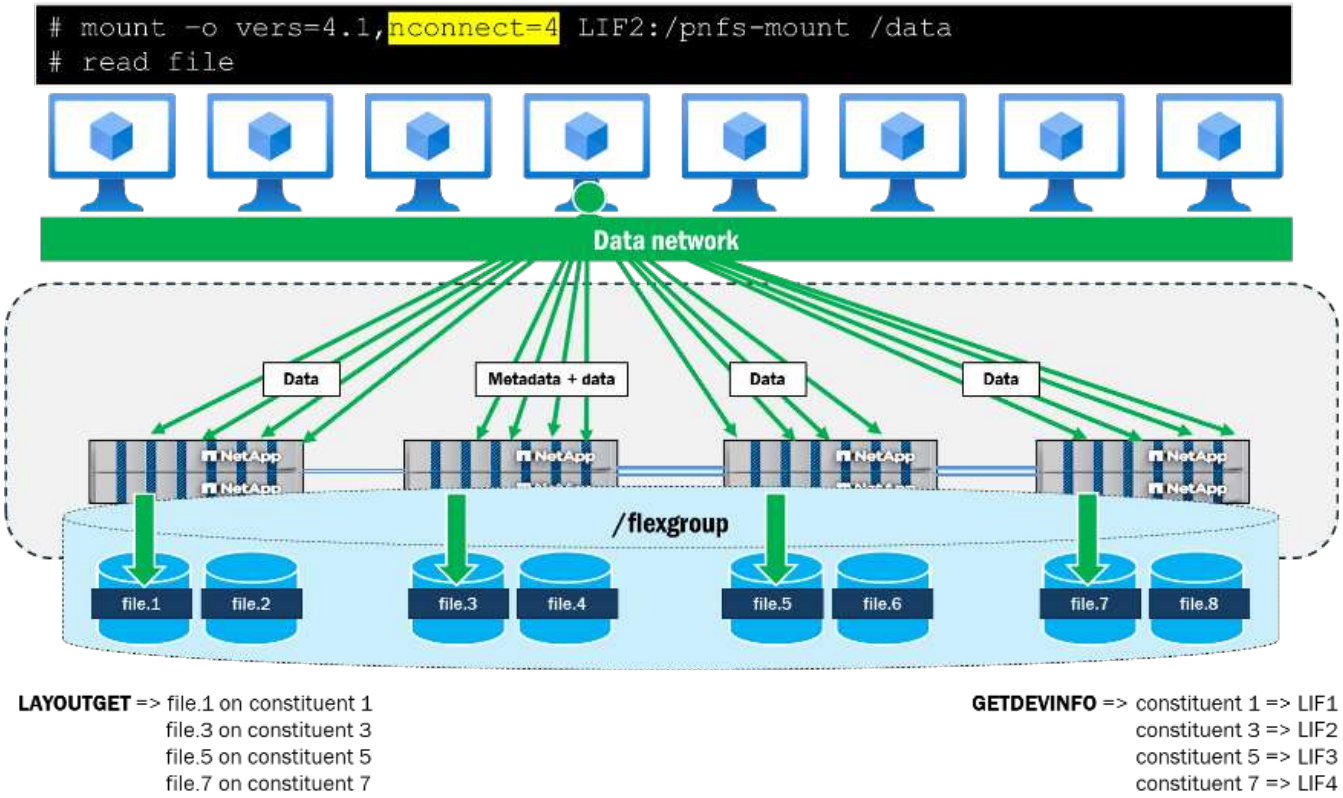


圖 **9. pNFS** 的 **nconnect** 設定為 **4**

"了解更多關於ONTAP對 NFSv4.1 的支持"

pNFS 與 NFSv4.1 會話中繼

NFSv4.1 會話中繼 ("RFC 5661，第 2.10.5 節") 是指在客戶端和伺服器之間使用多個 TCP 連線來提高資料傳輸速度。ONTAP 9.14.1 新增了對 NFSv4.1 會話中繼的支持，必須與也支援會話中繼的用戶端一起使用。

在ONTAP中，會話中繼可以跨叢集中的多個節點使用，以提供額外的吞吐量和連接冗餘。

會話中繼可以透過多種方式建立：

- 透過掛載選項自動發現： 大多數現代 NFS 用戶端可以透過掛載選項建立會話中繼（請查看您的作業系統供應商的文件），該選項會向 NFS 伺服器發出訊號，以便將有關會話中繼的資訊傳送回用戶端。此資訊以 NFS 資料包的形式出現。 `fs_location4` 稱呼。

  所使用的掛載選項取決於客戶端的作業系統版本。例如，Ubuntu Linux 的各種版本通常使用 `max_connect=n` 表示要使用會話中繼。在 RHEL Linux 發行版中， `trunkdiscovery` 使用了掛載選項。

  Ubuntu 範例

  ```
  mount -o vers=4.1,max_connect=8 10.10.10.10:/pNFS /mnt/pNFS
  ```

  RHEL 範例

  ```
  mount -o vers=4.1,trunkdiscovery 10.10.10.10:/pNFS /mnt/pNFS
  ```

如果您嘗試使用 `max_connect` 在 RHEL 發行版上，它將被視為 nconnect，會話中繼將無法如預期般運作。

- 手動建立： 您可以透過將每個單獨的 IP 位址掛載到相同的匯出路徑和掛載點來手動建立會話中繼。例如，如果同一個節點上有兩個 IP 位址（10.10.10.10 和 10.10.10.11），用於匯出路徑，`/pNFS`你需要運行兩次 mount 指令：

```
mount -o vers=4.1 10.10.10.10:/pNFS /mnt/pNFS
mount -o vers=4.1 10.10.10.11:/pNFS /mnt/pNFS
```

對所有要參與主幹的介面重複此程序。

每個節點都有自己的會話主幹。主幹不經過節點。

使用 pNFS 時，僅使用會話中繼_或_ nconnect。同時使用兩者會導致不良行為，例如只有元資料伺服器連線才能獲得 nconnect 的好處，而資料伺服器只能使用單一連線。

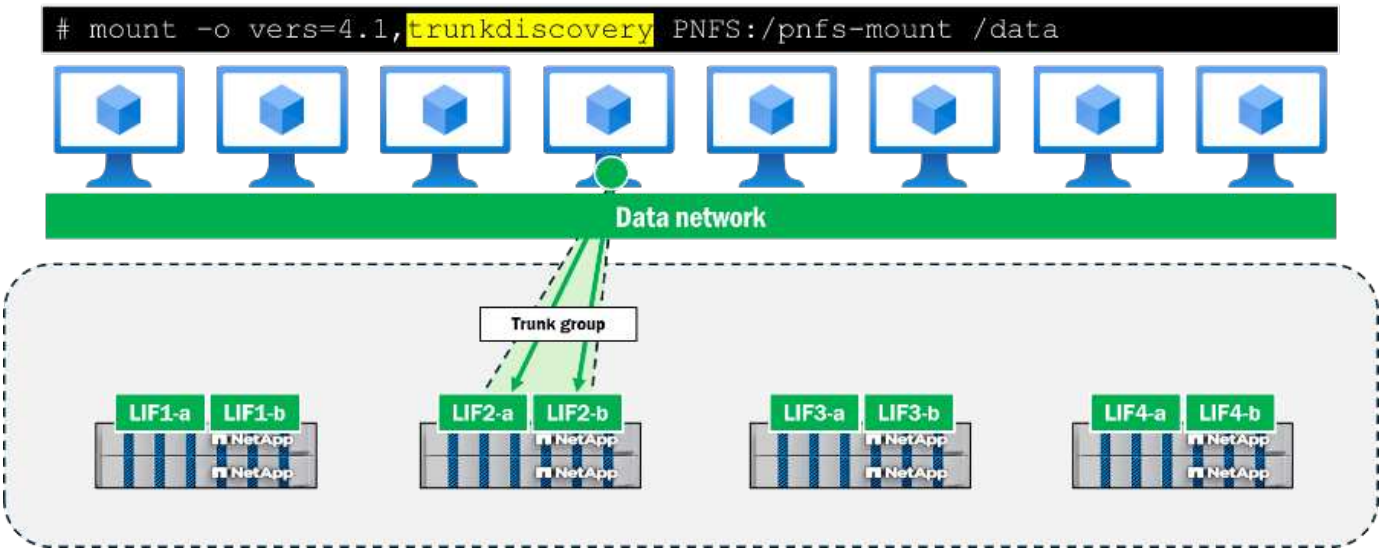
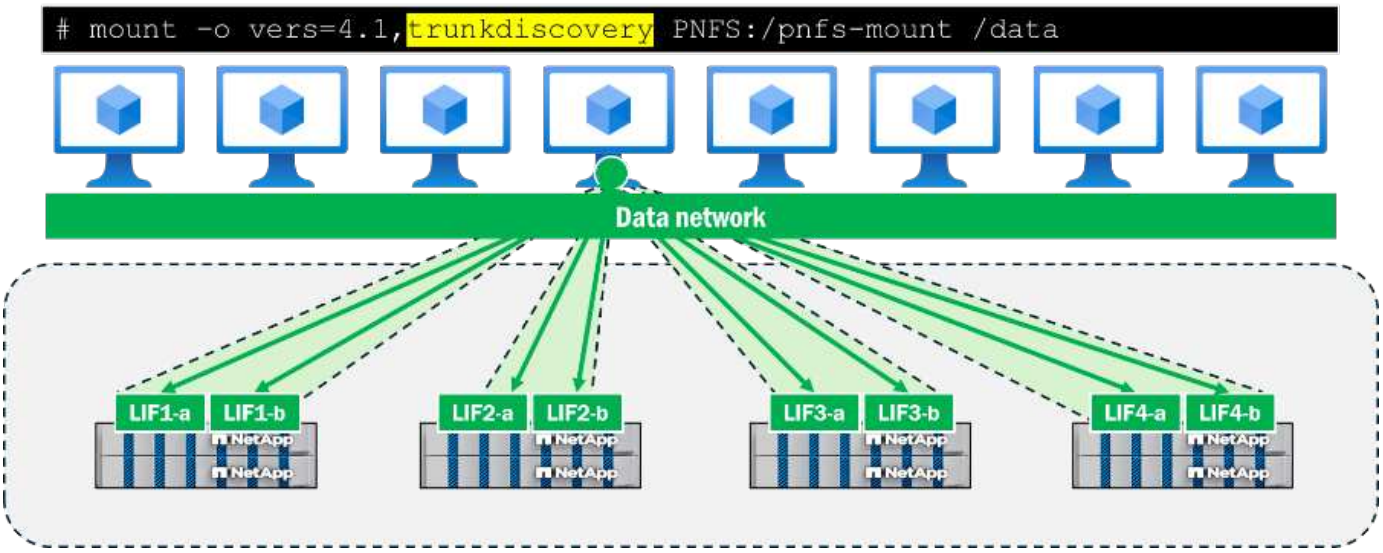


圖 **10. ONTAP**中的 **NFSv4.1** 會話中繼

pNFS 可以為叢集中的每個參與節點提供本機路徑，並且當與會話中繼一起使用時，pNFS 可以利用每個節點的會話中繼來最大限度地提高整個叢集的吞吐量。



什麼時候 `trunkdiscovery` 如果使用，則會利用附加的 GETATTR 呼叫 (FS_Locations) 來取得 NFS 伺服器節點上所列的會話中繼接口，該節點是掛載介面所在的位置。一旦這些位址返回，後續的掛載點就會指向返回的位址。這可以從掛載過程中的資料包擷取中看出。

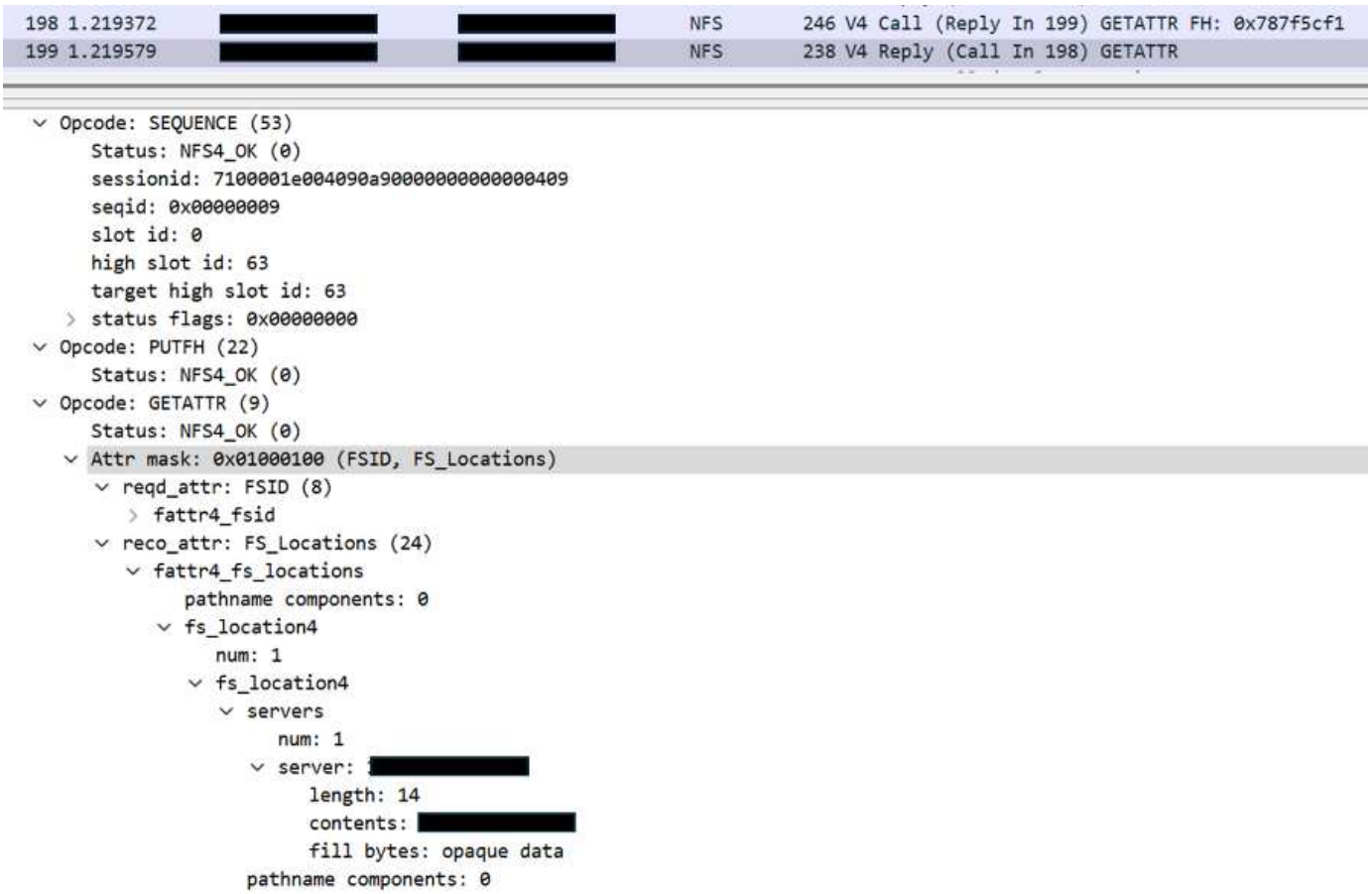


圖 **11.** 掛載期間的 **NFS** 會話主幹發現：資料包捕獲

"了解更多關於NFS中繼的信息"

pNFS 與 NFSv4.1 轉診

NFSv4.1 參考提供了一種初始掛載路徑重新導向模式，該模式會在發出掛載請求時將用戶端引導至磁碟區的位

置。NFSv4.1 轉介功能在單一 SVM 內運作。此功能嘗試將 NFS 掛載點定位到與資料磁碟區位於相同節點上的網路介面。如果該介面或磁碟區在掛載到客戶端時移動到另一個節點，則資料路徑將不再本地化，直到建立新的掛載點為止。

pNFS 不會嘗試定位掛載路徑。相反，它會使用掛載路徑建立一個元資料伺服器，然後根據需要動態地本地化資料路徑。

NFSv4.1 引用可以與 pNFS 一起使用，但此功能沒有必要。啟用 pNFS 的轉診功能不會產生明顯效果。

"啟用或停用 NFSv4 引用"

pNFS與高階容量平衡的交互

"進階容量平衡" ONTAP會將檔案資料的一部分寫入FlexGroup磁碟區的各個組成磁碟區（單一FlexVol磁碟區不支援此功能）。隨著檔案的成長， ONTAP決定開始將資料寫入不同的組成磁碟區上的新的多部分 inode，該組成磁碟區可能位於同一節點上，也可能位於不同的節點上。對這些多 inode 檔案進行的寫入、讀取和元資料操作對客戶端是透明的，不會造成乾擾。先進的容量平衡技術改善了FlexGroup各組成磁碟區之間的空間管理，從而提供了更穩定的效能。

pNFS 可以根據 NFS 伺服器中儲存的檔案佈局訊息，將資料 I/O 重新導向到本機網路路徑。當一個大檔案被分成多個部分，分佈在多個組成磁碟區中，而這些磁碟區可能跨越叢集中的多個節點時， ONTAP中的 pNFS 仍然可以為每個檔案部分提供本機流量，因為ONTAP也維護了所有檔案部分的檔案佈局資訊。讀取檔案時，資料路徑的局部性會根據需要而改變。

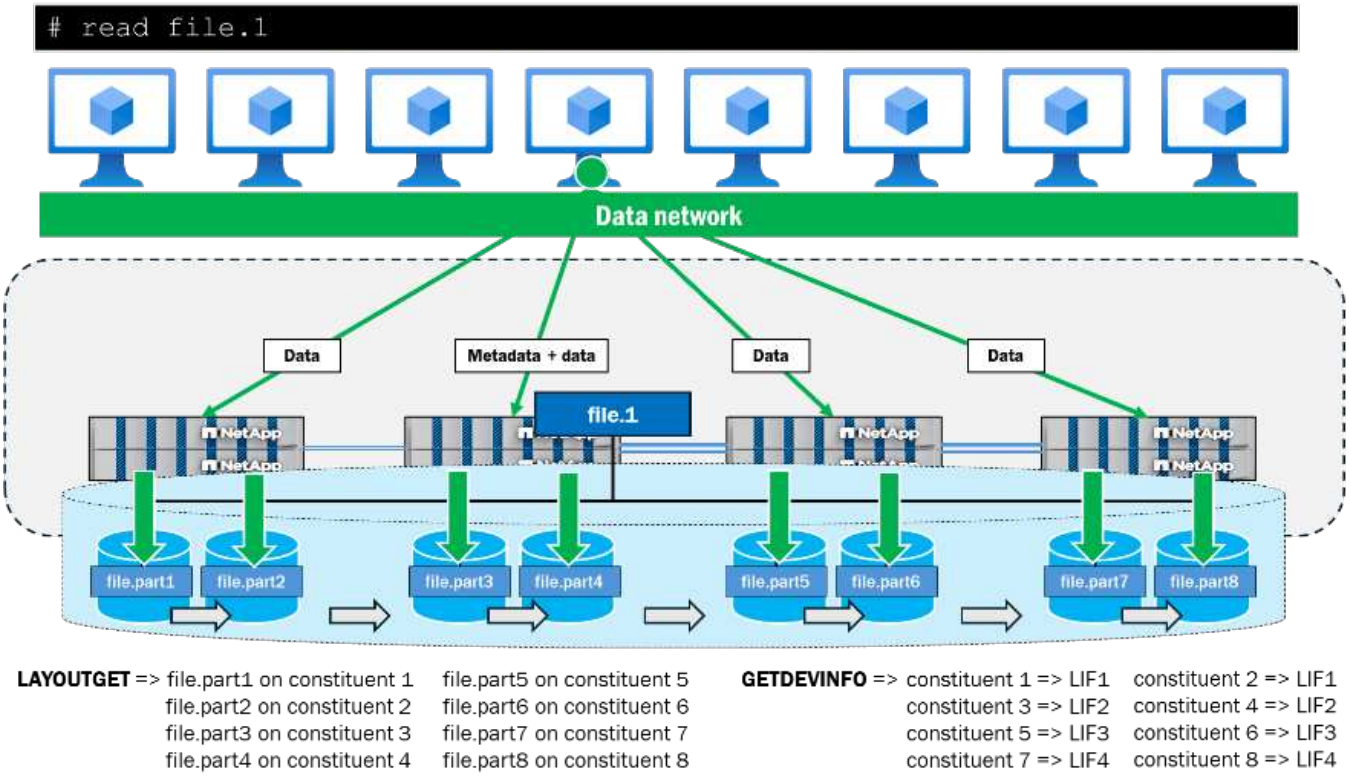


圖 **12.** 基於 **pNFS** 的高階容量平衡

相關資訊

- "FlexGroup卷配置"

ONTAP中的 **pNFS** 部署策略

pNFS 的引入是為了改進傳統的 NFS，它分離元資料和資料路徑，提供資料本地化，並支援平行操作。

傳統**NFS**的挑戰與**pNFS**的優勢

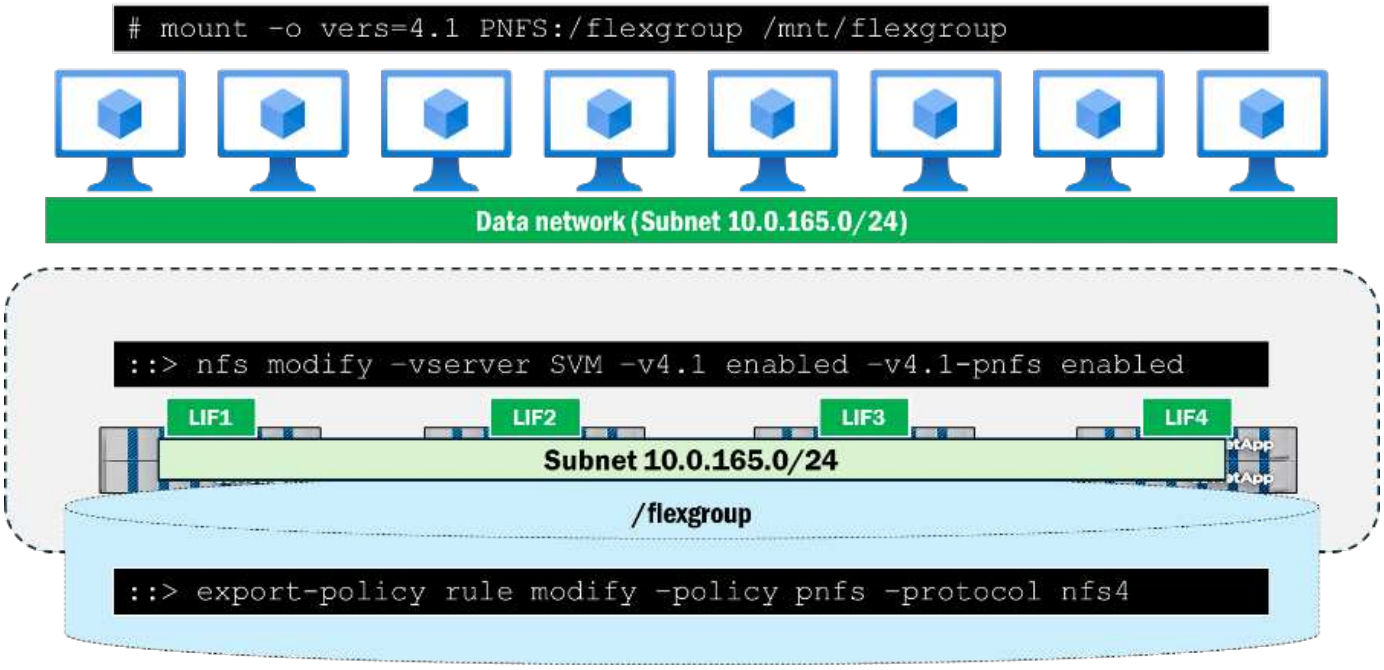
下表列出了傳統 NFS 面臨的挑戰，並解釋了ONTAP中的 pNFS 如何解決這些挑戰。

挑戰	**pNFS** 獲益
元資料和資料走同一條路徑 在傳統的 NFS 中，元資料和資料走同一條路徑，這可能會導致網路和 CPU 飽和，因為一條路徑會連接到叢集中的單一硬體節點。當許多用戶嘗試存取同一個 NFS 匯出時，這種情況會更加嚴重。	元資料和資料路徑分離，資料路徑並行化 透過分離 NFS 流量的元資料和資料路徑，並為資料路徑提供多條網路路徑， ONTAP叢集中的 CPU 和網路資源得到最大化利用，從而提高了工作負載的擴展性。
工作負載分配挑戰 在ONTAP NAS 叢集中，最多可以有 24 個節點，每個節點都可以有自己的一組資料捲和網路介面。每個磁碟區都可以承載自己的工作負載，或是工作負載的子集；而使用FlexGroup卷，為了簡化操作，工作負載可以存在於存取單一命名空間的多個節點上。當客戶端掛載 NFS 匯出時，網路流量將在單一節點上建立。當被存取的資料位於叢集中的單獨節點上時，就會發生遠端流量，這會增加工作負載的延遲和管理的複雜性。	本地並行資料結構路徑 由於 pNFS 將資料路徑與元資料分離，並根據磁碟區在叢集中的位置提供多個並行資料路徑，因此可以透過減少叢集中網路流量的距離以及利用叢集中的多個硬體資源來降低延遲。此外，由於ONTAP中的 pNFS 會自動重新導向資料流量，管理員無需管理多個匯出路徑和位置。
NFS 掛載點遷移 掛載點建立後，卸載並重新掛載磁碟區會造成乾擾。ONTAP提供了在節點之間遷移網路介面的功能，但這會增加管理開銷，並且會對使用 NFSv4.x 的有狀態 NFS 連線造成乾擾。重新定位掛載點的部分原因與資料本地性挑戰有關。	自動路徑重定位 使用 pNFS 時，NFS 伺服器會維護一個網路介面和磁碟區位置的表。當客戶端透過 pNFS 中的元資料路徑請求資料結構時，伺服器將向客戶端提供最佳化的網路路徑，然後客戶端將使用該路徑進行資料操作。這大大降低了工作負載的管理開銷，並且在某些情況下可以提高效能。

配置要求

在NetApp ONTAP中設定 pNFS 需要以下步驟：

- 支援 pNFS 且掛載於 NFSv4.1 或更高版本的 NFS 用戶端
- ONTAP中的 NFS 伺服器已啟用 NFSv4.1 (`nfs modify -v4.1 enabled`（預設為關閉）
- ONTAP中的 NFS 伺服器已啟用 pNFS (`nfs modify -v4.1-pnfs enabled`（預設為禁用）
- 每個節點至少需要一個可路由至 NFS 用戶端的網路介面。
- SVM 中具有允許 NFSv4 導出策略和規則的資料卷



滿足上述配置要求後，pNFS 即可自行運作。

相關資訊

- "NFS 組態"
- "ONTAP對 NFSv4.1 的支持"
- "pNFS 的網路介面連接"

規劃

pNFS部署計劃

在您的環境中部署 pNFS 之前，請確保滿足先決條件，並了解互通性要求和配置限制。

先決條件

在ONTAP中啟用和使用 pNFS 之前，請確保符合以下要求：

- NFS伺服器上已啟用NFSv4.1或更高版本
- 至少一個 "每個節點都存在資料 LIF。" 在託管 NFS 伺服器的 SVM 叢集中
- 全部 "SVM 中的資料 LIF 是可路由的" 致 NFS 用戶端
- NFS 用戶端支援 pNFS（2014 年及以後的大多數現代 Linux 發行版均支援）。
- 客戶端與SVM中所有資料LIF之間的網路連線正常
- 所有資料 LIF 的 DNS 解析（如果使用主機名稱）均已正確配置。
- "資料量FlexGroup" 已配置（建議使用以獲得最佳效果）
- "NFSv4.x ID 域匹配" 客戶與ONTAP之間
- "NFS Kerberos" （如果使用）在 SVM 中的所有資料 LIF 上啟用。

最佳實務總結

在您的環境中部署 pNFS 時，請遵循以下最佳實務：

- 使用 "資料量FlexGroup" 為了獲得最佳性能和容量擴展性
- 確保所有 "SVM中的網路介面是可路由的。" 致客戶
- "停用NFSv4.0" 確保客戶端使用 NFSv4.1 或更高版本
- 分散掛載點到多個網路介面和節點
- 使用輪詢 DNS "負載平衡元資料伺服器"
- 核實 "NFSv4.x ID 域匹配" 在客戶端和伺服器上
- 執行 "網路介面遷移" 和 "儲存故障轉移" 維護窗口期
- 使能夠 "NFS Kerberos" 如果使用 Kerberos 安全機制，則所有資料 LIF 都會受到影響。
- 避免使用 "NFSv4.1 轉介" 使用 pNFS 時
- 測試 "nconnect 設定" 謹慎操作，避免超出 TCP 連線限制
- 考慮 "會話中繼" 作為替代方案 "n 連接" （請勿同時使用兩者）
- 核實 "客戶端作業系統供應商支持" 部署前先對 pNFS 進行處理

互通性

ONTAP中的 pNFS 設計用於與符合 RFC 標準的 NFS 用戶端搭配使用。以下幾點要考慮：

- 最現代 "2014 年及以後的 Linux 發行版" 支援 pNFS（RHEL 6.4、Fedora 17 及更高版本）
- 請向您的用戶端作業系統供應商確認是否支援 pNFS。
- pNFS 可與FlexVol和 "資料量FlexGroup"
- pNFS 支援 NFSv4.1 和 "NFSv4.2"
- pNFS 可以與…一起使用 "NFS Kerberos" （krb5、krb5i、krb5p），但性能可能會受到影響
- pNFS 可以與…一起使用 "n 連接" 或者 "會話中繼" （但不能同時進行）
- pNFS 無法在 "NFSv4.0"

限制

以下限制適用於ONTAP中的 pNFS：

- "TCP 連線限制" 每個節點的具體限制因平台而異（請查看NetAppHardware Universe以了解特定限制）。
- 最大檔案大小：取決於磁碟區類型和ONTAP版本
- 最大文件數：最多 2000 億個文件 "資料量FlexGroup"
- 最大容量：高達 60 PB "資料量FlexGroup"
- "網路介面數量"每個節點至少需要一個資料 LIF；負載平衡可能需要更多。

使用時 "nconnect 與 pNFS"請注意，TCP 連線數會迅速成長：

- 每個使用 nconnect 的客戶端掛載都會為每個資料 LIF 建立多個 TCP 連線。

- 由於許多客戶使用了較高的 nconnect 值， "TCP 連線限制" 可以超過
- TCP連線數超過限制會阻止建立新連接，直到現有連線被釋放為止。

相關資訊

- "pNFS 的網路介面連接"
- "啟用或停用 NFSv4.1"
- "ONTAP對 NFSv4.1 的支持"
- "ONTAP對 NFSv4.2 的支持"
- "NetApp Hardware Universe"

pNFS調優與效能最佳實踐

在ONTAP中使用 pNFS 時，請遵循以下注意事項和最佳實踐，以獲得最佳結果。

容量類型推薦

ONTAP中的 pNFS 可以與FlexVol捲和FlexGroup磁碟區一起使用，但為了獲得最佳的整體效果，請使用FlexGroup磁碟區。

FlexGroup卷提供：

- 單一掛載點可以跨越叢集中的多個硬體資源，同時允許 pNFS 本地化資料流量。
- 海量儲存容量（高達 60 PB）和高檔案數量（高達 2000 億個檔案）
- 支援多部分文件以實現容量平衡和潛在的性能優勢
- 支援對單一工作負載的捲和硬體進行並行訪問

"了解FlexGroup磁碟區管理"

客戶推薦

並非所有 NFS 用戶端都支援 pNFS，但大多數現代客戶端都支援。 RHEL 6.4 和 Fedora 17 是最早支援 pNFS 的用戶端（大約在 2014 年），因此可以合理地假設過去幾年發布的客戶端版本都完全支援此功能。ONTAP 對 NFS 的支援立場是「如果用戶端支援該功能且符合 RFC 標準，而我們也支援該功能，那麼這種組合就是受支援的」。但是，最佳實踐是確保客戶端作業系統供應商支援 pNFS。

成交量變動

ONTAP能夠以非中斷的方式在同一叢集中的節點或聚合之間移動捲，從而提供容量和效能平衡的靈活性。當ONTAP中發生磁碟區移動時，pNFS 設備對應會自動更新，以便在必要時通知客戶端使用新的捲到介面關係。

"了解如何移動卷"

網路介面遷移

ONTAP能夠將網路介面遷移到同一叢集中的不同節點，從而實現效能平衡和維護靈活性。與磁碟區遷移類似，當ONTAP中發生網路介面遷移時，pNFS 設備對應會自動更新，以便在必要時通知用戶端使用新的捲到介面關係。

然而，由於 NFSv4.1 是有狀態協議，網路介面遷移可能會對正在積極使用 NFS 掛載的客戶端造成乾擾。最佳實踐是在維護視窗期間進行網路介面遷移，並通知客戶可能出現的網路中斷。

儲存故障轉移/恢復

pNFS 遵循與 NFSv4.1 相同的儲存故障轉移考量。這些內容在下文有詳細介紹。 "NetApp技術報告4067：NFS最佳實務與實作指南"一般來說，任何涉及 pNFS 的儲存故障轉移/復原都應該在維護視窗內進行，由於協定的狀態性，可能會出現儲存中斷。

元資料工作負載

元資料操作的規模很小，但數量可能很大，具體取決於工作負載（您是否正在建立大量檔案？）您是否正在執行“查找”命令？ ）以及文件總數。因此，元資料呼叫量高的工作負載會佔用 NFS 伺服器大量的 CPU 資源，並可能導致單一連線瓶頸。 pNFS（以及一般的 NFSv4.x）並不適合對效能要求較高的元資料工作負載，因為該協定版本的狀態性、鎖定機制以及某些安全特性會對 CPU 使用率和延遲產生負面影響。這些工作負載類型（例如高 GETATTR 或 SETATTR）通常在 NFSv3 中表現較好。

元資料伺服器

pNFS 中的元資料伺服器是在 NFS 匯出首次掛載時建立的。安裝點一旦建立，就會一直保持原位，直到重新安裝或移動資料介面為止。因此，最佳實務是確保多個客戶端存取同一磁碟區時掛載到 SVM 的不同節點和資料介面。這種方法可以實現跨節點和 CPU 資源的元資料伺服器負載平衡，同時最大限度地利用叢集中的網路介面。實現此目的的一種方法是建立輪詢 DNS 設置，這在下文中有所介紹。 "NetApp技術報告 4523： ONTAP中的 DNS 負載平衡"。

NFSv4.x ID 域

NFSv4.x 透過多種方式提供安全功能（詳見下文）。 "NetApp技術報告4067：NFS最佳實務與實作指南" ）。NFSv4.x ID 網域是實作 NFS 匯出時客戶端和伺服器必須就 ID 網域進行驗證的方法之一。ID 網域不匹配的副作用之一是，使用者或群組會顯示為匿名使用者（本質上是被壓制），以防止未經授權的存取。對於 NFSv4.x（以及 pNFS），最佳實踐是確保客戶端和伺服器上的 NFSv4.x ID 網域匹配。

n 連接

如前所述， ONTAP中的 nconnect 可以幫助提高某些工作負載的效能。對於 pNFS，需要了解的是，雖然 nconnect 可以透過大幅增加與儲存系統的 TCP 連線總數來提高效能，但當許多客戶端利用掛載選項時，它也可能透過使儲存上的 TCP 連接過載而造成問題。NetAppHardware Universe涵蓋了每個節點的 TCP 連線限制。

當節點的 TCP 連線數超過限制時，在現有連線釋放之前，不允許建立新的 TCP 連線。這可能會為可能遭遇暴風雪的地區帶來複雜情況。

下表顯示了使用 nconnect 的 pNFS 如何可能超出 TCP 連線限制：

客戶數量	**nconnect** 值	每個掛載點每個節點的潛在 **TCP** 連線總數
1.	4.	4.
100	4.	400
1000	8.	8000
10000.	8.	80000
10000.	16.	160000 [1]

[1] 超出大多數ONTAP單節點 TCP 連線限制

NFSv4.1 工作階段主幹

ONTAP中的會話中繼可用於提高 NFSv4.x 掛載的吞吐量和路徑彈性。與 pNFS 一起使用時，叢集中的每個節點都可以建立會話中繼。但是，會話中繼需要每個節點至少兩個接口，而 pNFS 需要每個節點至少有一個接口才能按預期工作。此外，SVM 中的所有介面都必須能夠路由到 NFS 用戶端。同時使用 nconnect 時，會話中繼和 pNFS 無法正常運作。將 nconnect 和會話中繼視為互斥的功能。

"了解NFS中繼"

網路介面連接

pNFS 需要叢集中每個節點都具有可路由的網路介面才能正常運作。如果與託管 pNFS 的 NFS 伺服器位於同一 SVM 中，且存在其他無法路由到 NFS 用戶端的網路接口，則ONTAP仍會在設備映射中向客戶端通告這些接口。當 NFS 用戶端嘗試透過不同子網路中的介面存取資料時，將無法連接，導致服務中斷。最佳實踐是，在使用 pNFS 時，只允許 SVM 中的網路介面可供客戶端存取。

> 預設情況下，pNFS 要求 SVM 中的任何資料 LIF 都可路由到 NFS 用戶端上的接口，因為 pNFS 設備清單將填入 SVM 中的任何資料 LIF。因此，可能會選擇不可路由的資料 LIF，這可能會造成中斷情況。最佳實踐是，僅在使用 pNFS 時配置可路由資料 LIF。
>
> 從ONTAP 9.18.1 RC1 及更高版本開始，您可以按子網路指定哪些介面符合 pNFS 流量的條件，從而允許混合使用可路由介面和不可路由介面。請聯絡NetApp支援部門以取得有關指令的資訊。

NFSv4.0

NFSv4.0 是ONTAP NFS 伺服器中可以與 NFSv4.1 一起啟用的選項。但是，pNFS 不能在 NFSv4.0 上運作。如果 NFS 伺服器啟用了 NFSv4.0，則用戶端可能會在不知情的情況下掛載該協定版本，並且無法利用 pNFS。因此，在使用 pNFS 時，最佳實踐是明確停用 NFSv4.0。NFSv4.1 仍需啟用，並且可以獨立於 NFSv4.0 運作。

NFSv4.1 轉介

NFSv4.1 引用會將客戶端的掛載路徑本地化到擁有該磁碟區的節點上的網路介面。 pNFS 在地化資料路徑，而掛載路徑則成為元資料伺服器。

雖然這兩個功能可以實際一起使用，但將 NFSv4.1 引用與 pNFS 一起使用可能會導致在同一節點上堆疊多個元資料伺服器，從而降低將元資料伺服器分散到多個叢集節點的能力，這種效果並不理想。在使用 pNFS 時，如果元資料伺服器沒有均勻分佈在叢集中，那麼單一節點的 CPU 可能會被元資料請求淹沒，從而造成效能瓶頸。

因此，在使用 pNFS 時，最好避免使用 NFSv4.1 引用。相反，應將掛載點分散到叢集中的多個網路介面和節點上。

"了解如何啟用或停用 NFSv4 轉儲"

NFS Kerberos

使用 NFS Kerberos，可以對 krb5 進行身份驗證加密，並進一步對封包進行 krb5i 和 krb5p 加密。在SVM中，此功能是基於每個網路介面啟用的，詳情請參見[此處]。 "NetApp技術報告4616：ONTAP NFS Kerberos in Some with Microsoft Active Directory"。

由於 pNFS 可以將資料流量重定向到 SVM 中的節點和網路接口，因此 SVM 中的每個網路介面都必須啟用 NFS Kerberos 並使其正常運作。如果 SVM 中的任何網路介面未啟用 Kerberos，則 pNFS 在嘗試存取這些介面上的

資料磁碟區時將無法正常運作。

例如，當在具有兩個網路介面（只有一個啟用了 Kerberos）的 pNFS 支援的 SVM 上使用並行 dd 運行讀取測試時，位於啟用了 Kerberos 的介面上的檔案效能良好，而位於未啟用 Kerberos 的介面上的節點上的檔案始終無法完成讀取。當兩個介面都啟用 Kerberos 時，所有檔案都能如預期運作。

只要在 SVM 的所有網路介面上啟用了 NFS Kerberos，NFS Kerberos 就可以與 pNFS 一起使用。請記住，由於封包的加密/解密，NFS Kerberos 可能會造成效能損失，因此最佳實踐是使用工作負載徹底測試 pNFS 與 NFS Kerberos，以確保任何效能損失都不會對工作負載造成過大的影響。

下面是一個在 RHEL 9.5 用戶端上使用 pNFS 並結合 krb5（身份驗證）和 krb5p（端對端加密）時的平行讀取效能範例。Krb5p 在這項測試中表現下降了 70%。

克爾貝羅斯口味	**MB/**秒	完成時間
KRB5	• File1-243 • File2-243 • File3-238 • File4-238	• File1-43 • File2-43.1 • File3-44 • File4-44.1
krb5p	• File1-72.9 • File2-72.8 • File3-71.4 • File4-71.2	• File1-143.9 • File2-144.1 • File3-146.9 • File4-147.3

"了解 NFS 中的 Kerberos，以實現強大的安全性"

NFSv4.2

NFSv4.2 已加入ONTAP 9.8 中，是目前可用的最新 NFSv4.x 版本 (RFC-7862)。NFSv4.2 沒有明確的選項來啟用/停用它。相反，它是與 NFSv4.1 一起啟用/停用的。（`-4.1 enabled`）。如果用戶端支援 NFSv4.2，則在掛載命令期間，除非另有指定，否則它將協商支援的最高 NFS 版本。 `minorversion=2` 安裝選項。

ONTAP中的 NFSv4.2 支援以下功能：

- 安全標籤（MAC標籤）
- 延伸屬性
- 稀疏文件操作（FALLOCATE）

pNFS 隨 NFSv4.1 引入，但也受 NFSv4.2 及其相關功能的支援。

"了解 ONTAP 對 NFSv4.2 的支持"

pNFS 指令、統計資料和事件日誌

這些ONTAP CLI 指令專門用於 pNFS。您可以使用它們進行配置、故障排除和收集統計資料。

啟用 **NFSv4.1**

```
nfs modify -vserver SVM -v4.1 enabled
```

啟用**pNFS**

```
nfs modify -vserver SVM -v4.1-pnfs enabled
```

顯示 **pNFS** 設備（進階權限）

```
pnfs devices show -vserver SVM
```

```
Vserver Name     Mapping ID      Volume MSID     Mapping Status
Generation
---------------  --------------- --------------- ---------------
-------------
SVM              17              2157024470      notavailable    2
SVM              18              2157024463      notavailable    2
SVM              19              2157024469      available       3
SVM              20              2157024465      available       4
SVM              21              2157024467      available       3
SVM              22              2157024462      available       1
```

顯示 **pNFS** 裝置對映（高階權限）

```
pnfs devices mappings show -vserver SVM
```

```
Vserver Name    Mapping ID      Dsid            LIF IP
--------------  --------------- --------------- --------------------
SVM             19              2449            10.x.x.x
SVM             20              2512            10.x.x.y
SVM             21              2447            10.x.x.x
SVM             22              2442            10.x.x.y
```

擷取 **pNFS** 特有的效能計數器（進階權限）

```
statistics start -object nfsv4_1 -vserver SVM -sample-id [optional-name]
```

查看 **pNFS** 特有的效能計數器（進階權限）

```
statistics show -object nfsv4_1 -vserver SVM
```

查看 **pNFS** 特有計數器清單（進階權限）

```
statistics catalog counter show -object nfsv4_1 -counter *layout*|*device*
```

```
Object: nfsv4_1

Counter                      Description
---------------------------- ----------------------------------------------
getdeviceinfo_avg_latency    Average latency of NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_error          The number of failed NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_percent        Percentage of NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_success        The number of successful NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_total          Total number of NFSv4.1 GETDEVICEINFO
operations.
getdevicelist_avg_latency    Average latency of NFSv4.1 GETDEVICELIST
operations.
getdevicelist_error          The number of failed NFSv4.1 GETDEVICELIST
operations.
getdevicelist_percent        Percentage of NFSv4.1 GETDEVICELIST
operations.
getdevicelist_success        The number of successful NFSv4.1 GETDEVICELIST
operations.
getdevicelist_total          Total number of NFSv4.1 GETDEVICELIST
operations.
layoutcommit_avg_latency     Average latency of NFSv4.1 LAYOUTCOMMIT
operations.
layoutcommit_error           The number of failed NFSv4.1 LAYOUTCOMMIT
operations.
layoutcommit_percent         Percentage of NFSv4.1 LAYOUTCOMMIT operations.
layoutcommit_success         The number of successful NFSv4.1 LAYOUTCOMMIT
operations.
layoutcommit_total           Total number of NFSv4.1 LAYOUTCOMMIT
operations.
layoutget_avg_latency        Average latency of NFSv4.1 LAYOUTGET
operations.
layoutget_error              The number of failed NFSv4.1 LAYOUTGET
```

```
operations.
layoutget_percent           Percentage of NFSv4.1 LAYOUTGET operations.
layoutget_success           The number of successful NFSv4.1 LAYOUTGET
operations.
layoutget_total             Total number of NFSv4.1 LAYOUTGET operations.
layoutreturn_avg_latency    Average latency of NFSv4.1 LAYOUTRETURN
operations.
layoutreturn_error          The number of failed NFSv4.1 LAYOUTRETURN
operations.
layoutreturn_percent        Percentage of NFSv4.1 LAYOUTRETURN operations.
layoutreturn_success        The number of successful NFSv4.1 LAYOUTRETURN
operations.
layoutreturn_total          Total number of NFSv4.1 LAYOUTRETURN
operations.
```

查看 **NFS** 的活動網路連接

您可以使用以下命令驗證是否與 SVM 建立了多個 TCP 連線： `network connections active show` 命令。

例如，如果要查看 NFS 會話中繼，請尋找來自相同客戶端在每個節點的不同介面上的連線：

```
cluster::*> network connections active show -node cluster-0* -vserver PNFS
              Vserver   Interface         Remote
      CID Ctx Name      Name:Local Port   Host:Port
Protocol/Service
--------- --- --------- ----------------- --------------------
----------------
Node: node-01
2304333128 14 PNFS      data1:2049        ubuntu22-224:740     TCP/nfs
2304333144 10 PNFS      data3:2049        ubuntu22-224:864     TCP/nfs
2304333151  5 PNFS      data1:2049        ubuntu22-226:848     TCP/nfs
2304333167 15 PNFS      data3:2049        ubuntu22-226:684     TCP/nfs
Node: node-02
2497668321 12 PNFS      data2:2049        ubuntu22-224:963     TCP/nfs
2497668337 18 PNFS      data4:2049        ubuntu22-224:859     TCP/nfs
2497668344 14 PNFS      data2:2049        ubuntu22-226:675     TCP/nfs
2497668360  7 PNFS      data4:2049        ubuntu22-226:903     TCP/nfs
```

查看已連接客戶端的 **NFS** 版本信息

您也可以使用以下方式查看 NFS 連線： `nfs connected-clients show` 命令。請注意，此處顯示的客戶名單是過去 48 小時內有活躍 NFS 流量的客戶。空閒的 NFS 用戶端（即使仍然掛載）可能要等到存取掛載點時才會顯示出來。您可以透過指定以下參數來篩選這些客戶端，使其僅顯示最近造訪過的用戶端： `-idle-time` 特徵。

例如，要查看過去 10 分鐘內 pNFS SVM 中有活動的客戶：

```
cluster::*> nfs connected-clients show -vserver PNFS -idle-time <10m>

 Node: node-01

Vserver: PNFS Data-Ip: 10.x.x.x Local Remote Client-Ip Protocol Volume
Policy Idle-Time Reqs Reqs Trunking

10.x.x.a nfs4.2 PNFS_root default 9m 10s 0 149 false 10.x.x.a nfs4.2
FG_0001 default 9m 10s 135847 0 false 10.x.x.b nfs4.2 PNFS_root default 8m
12s 0 157 false 10.x.x.b nfs4.2 FG_0001 default 8m 12s 52111 0 false
```

相關資訊

- "了解ONTAP中的平行 NFS (pNFS)"

NFS和SMB檔案及目錄命名相依性

了解 ONTAP NFS 和 SMB 檔案和目錄命名依賴關係

檔案和目錄命名慣例取決於網路用戶端的作業系統和檔案共用傳輸協定、以及ONTAP 在叢集和用戶端上的語言設定。

作業系統和檔案共用傳輸協定決定下列事項：

- 檔案名稱可使用的字元
- 檔案名稱的大小寫敏感度

根據發行版的資訊、支援檔案、目錄和qtree名稱中的多位元組字元。ONTAP ONTAP

了解 ONTAP NFS SVM 在不同作業系統中的有效字符

如果您從具有不同作業系統的用戶端存取檔案或目錄、則應使用兩個作業系統中有效的字元。

例如、如果您使用UNIX建立檔案或目錄、請勿在名稱中使用分號（：）、因為在MS－DOS檔案或目錄名稱中不允許使用分號。由於有效字元的限制因作業系統而異、請參閱用戶端作業系統的說明文件、以取得有關禁止字元的詳細資訊。

了解 ONTAP NFS 多協定環境中檔案和目錄名稱的大小寫敏感性

檔案和目錄名稱對NFS用戶端區分大小寫、對SMB用戶端則不區分大小寫、但大小寫保留。您必須瞭解多重傳輸協定環境的影響、以及在建立SMB共用區時指定路徑以及存取共用區內資料時、可能需要採取的行動。

如果 SMB 用戶端建立名為的目錄 `testdir`， SMB 和 NFS 用戶端都會將檔案名稱顯示為 `testdir`。不過、如果 SMB 使用者稍後嘗試建立目錄名稱 `TESTDIR`，不允許使用該名稱，因爲對於 SMB 客戶端，該名稱當前存在。如果 NFS 使用者稍後建立名為的目錄 `TESTDIR`NFS 和 SMB 用戶端會以不同方式顯示目錄名稱、如下所

示：

- 例如、在 NFS 用戶端上、您會看到兩個目錄名稱都是建立的 `testdir` 和 `TESTDIR`，因爲目錄名稱區分大小寫。
- SMB用戶端使用8.3名稱來區分這兩個目錄。一個目錄有基礎檔案名稱。其他目錄會指派8.3檔名。
  - 在 SMB 用戶端上、您會看到 `testdir` 和 `TESTDI~1`。
  - ONTAP 會建立 `TESTDI~1` 用於區分兩個目錄的目錄名稱。

    在這種情況下、您必須在建立或修改儲存虛擬機器（SVM）上的共用區時、使用8.3名稱來指定共用路徑。

同樣地、如果 SMB 用戶端建立檔案 `test.txt`， SMB 和 NFS 用戶端都會將檔案名稱顯示為 `text.txt`。不過、如果 SMB 使用者稍後嘗試建立 `Test.txt`，不允許使用該名稱，因爲對於 SMB 客戶端，該名稱當前存在。如果 NFS 使用者稍後建立名為的檔案 `Test.txt`NFS 和 SMB 用戶端會以不同方式顯示檔案名稱、如下所示：

- 在 NFS 用戶端上、您會看到兩個檔案名稱都是建立的、 `test.txt` 和 `Test.txt`，因爲文件名區分大小寫。
- SMB用戶端使用8.3名稱來區分這兩個檔案。一個檔案有基礎檔案名稱。其他檔案會指派8.3檔名。
  - 在 SMB 用戶端上、您會看到 `test.txt` 和 `TEST~1.TXT`。
  - ONTAP 會建立 `TEST~1.TXT` 檔案名稱可區分這兩個檔案。

> 如果使用 vserver CIFS 字元對應命令建立字元對應、通常不區分大小寫的 Windows 查詢可能會變成區分大小寫的查詢。這表示只有在建立字元對應且檔案名稱使用該字元對應時、檔案名稱查詢才會區分大小寫。

了解如何建立 **ONTAP NFS** 檔案和目錄名稱

在任何可從SMB用戶端存取的目錄中、利用此程式建立並維護兩個檔案或目錄名稱：原始的長名稱和8.3格式的名稱。ONTAP

若檔案或目錄名稱超過八個字元名稱或三個字元副檔名限制（檔案）、ONTAP 則會產生8.3格式的名稱、如下所示：

- 如果名稱超過六個字元、則會將原始檔案或目錄名稱刪減為六個字元。
- 它會在檔案或目錄名稱中附加一個或多個數字（從一到五）、這些名稱在被截短後不再是唯一的。

  如果因為有五個以上的相似名稱而導致號碼不足、就會建立一個與原始名稱無關的唯一名稱。

- 如果是檔案、則會將副檔名縮短為三個字元。

例如、如果 NFS 用戶端建立名為的檔案 `specifications.html`，由 ONTAP 建立的 8.3 格式檔案名稱為 `specif~1.htm`。如果此名稱已經存在、ONTAP 則在檔案名稱結尾處使用不同的編號。例如、如果 NFS 用戶端接著建立另一個名為的檔案 `specifications_new.html`的 `8.3` 格式 `specifications_new.html` 是 `specif~2.htm`。

了解 ONTAP NFS 對多位元組檔案、目錄和 qtree 名稱的處理

從支援4位元組的UTF-8編碼名稱開始、即可建立及顯示包含基本多語言平面（BMP）以外之統一碼輔助字元的檔案、目錄和樹狀名稱。ONTAP在早期版本中、這些補充字元無法在多重傳輸協定環境中正確顯示。

若要啟用 4 位元組 UTF-8 編碼名稱的支援、可使用新的 *utf8mb4* 語言代碼 `vserver` 和 `volume` 命令系列。

- 您必須以下列其中一種方式建立新的Volume：
- 設定音量 `-language` 選項明確：

  ```
  volume create -language utf8mb4 {…}
  ```

- 繼承 Volume `-language` SVM 中的選項、此選項已針對選項建立或修改：

  ```
  vserver [create|modify] -language utf8mb4 {…}``volume create {…}
  ```

- 如果您使用的是 ONTAP 9.6 及更早版本、則無法修改現有的 Volume 以獲得 utf8mb4 支援；您必須建立新的 utf8mb4 就緒 Volume 、然後使用用戶端型複本工具移轉資料。

  如果您使用的是 ONTAP 9.7P1 或更新版本、您可以透過支援要求修改 utf8mb4 的現有磁碟區。如需詳細資訊、請參閱 "是否可以在 ONTAP 中建立後變更 Volume 語言？"。

  您可以更新SVM以取得utf8mb4支援、但現有磁碟區仍保留其原始語言代碼。

  目前不支援使用4位元組utf-8字元的LUN名稱。

- 在Windows檔案系統應用程式中、通常會使用16位元的統一碼轉換格式（UTF-16）來表示統一碼字元資料、在使用8位元的統一碼轉換格式（UTF-8）的NFS檔案系統中則代表統一碼字元資料。

  在發行版不含更新版本的版本中、Windows用戶端所建立的名稱（包括UTF-16輔助字元）會正確顯示給其他Windows用戶端、但不會正確轉譯為適用於NFS用戶端的UTF-8。ONTAP同樣地、已建立NFS用戶端的名稱若含有UTF-8補充字元、則無法正確轉譯為適用於Windows用戶端的UTF-16。

- 當您在執行ONTAP 包含有效或無效補充字元的系統上建立檔案名稱時ONTAP 、不接受檔案名稱、並傳回無效的檔案名稱錯誤。

  若要避免此問題、請在檔案名稱中僅使用BMP字元、避免使用補充字元、或升級ONTAP 至版本號（或更新版本）。

qtree名稱中允許使用統一碼字元。

- 您可以使用 `volume qtree` 命令系列或系統管理程式來設定或修改 qtree 名稱。
- qtree名稱可以包含多位元組的統一碼格式字元、例如日文和中文字元。
- 在版本不含支援的版本中、僅支援使用BMP字元（也就是可以以3個位元組表示的字元）ONTAP 。

在發行版之前的版本中、qtree父磁碟區的交會路徑可以包含qtree和含有統一碼字元的目錄名稱。ONTAP。 `volume show` 當父磁碟區具有 UTF-8 語言設定時、命令會正確顯示這些名稱。不過、如果父Volume語言不是UTF-8語言設定之一、則會使用數值NFS替代名稱來顯示交會路徑的某些部分。

- 在9.5及更新版本中、如果qtree位於啟用utf8mb4的Volume中、則qtree名稱中支援4位元組字元。

在 **ONTAP NFS** 磁碟區上配置 **SMB** 檔案名稱轉換的字元映射

NFS用戶端可以建立檔案名稱、其中包含對SMB用戶端和某些Windows應用程式無效的字元。您可以設定磁碟區上檔案名稱轉譯的字元對應、讓SMB用戶端能夠存取NFS名稱、否則將無效。

關於這項工作

當SMB用戶端存取NFS用戶端所建立的檔案時、ONTAP 即可查看檔案名稱。如果名稱不是有效的SMB檔案名稱（例如、如果名稱有內嵌的結腸「」字元）、ONTAP 則無法返回每個檔案所保留的8.3檔名。不過、這會對將重要資訊編碼成長檔名的應用程式造成問題。

因此、如果您要在不同作業系統上的用戶端之間共用檔案、則應該在兩個作業系統中都有效的檔案名稱中使用字元。

不過、如果您有NFS用戶端建立的檔案名稱包含SMB用戶端無效檔案名稱的字元、您可以定義將無效NFS字元轉換成SMB和某些Windows應用程式所接受的統一碼字元的對應。例如、此功能支援CATIA MCAD和Mathatica應用程式、以及其他有此需求的應用程式。

您可以依Volume設定字元對應。

在磁碟區上設定字元對應時、必須謹記下列事項：

- 字元對應不會套用至交叉點。

  您必須明確設定每個交會Volume的字元對應。

- 您必須確定用於表示無效或非法字元的unicode字元是通常不會出現在檔案名稱中的字元、否則會產生不必要的對應。

  例如、如果您嘗試將一個分號（：）對應至連字號（-）、但檔案名稱中正確使用連字號（-）、則嘗試存取名為「a-b」的檔案的Windows用戶端會將其要求對應至NFS名稱「a:b」（而非所需結果）。

- 套用字元對應之後、如果對應仍包含無效的Windows字元、ONTAP 則將還原為Windows 8.3檔名。
- 在FPolicy通知、NAS稽核記錄和安全追蹤訊息中、會顯示對應的檔案名稱。
- 建立DP類型的SnapMirror關係時、來源磁碟區的字元對應不會複寫到目的地DP磁碟區。
- 區分大小寫：由於對應的Windows名稱會變成NFS名稱、因此名稱的查詢會遵循NFS語義。這包括NFS查詢區分大小寫。這表示存取對應共用的應用程式不得仰賴Windows不區分大小寫的行為。但是8.3名稱是可用的、而且不區分大小寫。
- 部分或無效對應：在將名稱對應至執行目錄列舉（「dir」）的用戶端之後、會檢查所產生的UNICODE名稱是否為Windows有效性。如果該名稱中仍有無效字元、或Windows的名稱無效（例如結尾為「.」或空白）、則會傳回8.3名稱而非無效名稱。

步驟

1. 設定字元對應：

   ```
   vserver cifs character-mapping create -vserver vserver_name -volume
   volume_name -mapping mapping_text, ...
   ```

   對應包含以「」分隔的來源目標字元配對清單。這些字元是以十六進位數字輸入的統一碼字元。例如：3c：E03C。

   每個值的第一個值 `mapping_text` 以冒號分隔的配對是您要轉譯之 NFS 字元的十六進位值、第二個值是 SMB 使用的 Unicode 值。對應配對必須是唯一的（一對一對應應該存在）。

   - 來源對應

     下表顯示來源對應的允許UNICODE字元集：

統一碼字元	列印字元	說明
01-0x19	不適用	非列印控制字元
0x5C	\	反斜槓
x3A.	：	結腸
0X2A	*	星號
x3F	？	問號
x22	"	引號
x3C	<	小於
x3E	>	大於
x7C		
垂直線	0xB1	±

   - 目標對應

     您可以在下列範圍內指定「Private Use Area」（私有使用區域）中的目標字元：u+E0000…U+F8FF。

範例

下列命令會在儲存虛擬機器（SVM）VS1上、針對名為「dATA」的磁碟區建立字元對應：

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  -------------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

用於管理 **SMB** 檔案名稱轉換的字元對映的 **ONTAP NFS** 命令

您可以建立、修改、顯示有關資訊、或刪除FlexVol 在支援使用於支援SMB檔案名稱轉譯的檔案字元對應、來管理字元對應。

如果您想要...	使用此命令...
建立新的檔案字元對應	`vserver cifs character-mapping create`
顯示檔案字元對應的相關資訊	`vserver cifs character-mapping show`
修改現有的檔案字元對應	`vserver cifs character-mapping modify`
刪除檔案字元對應	`vserver cifs character-mapping delete`

如"指令參考資料ONTAP"需詳細 `vserver cifs character-mapping`資訊，請參閱。