使用匯出原則保護NFS存取安全

ONTAP 9

NetApp
February 12, 2026

目錄

使用匯出原則保護NFS存取安全 . . . 1
導出策略如何控制用戶端對 ONTAP NFS 磁碟區或 qtree 的存取 . . . 1
ONTAP NFS SVM 的預設導出策略 . . . 1
ONTAP NFS 導出規則的工作原理 . . . 1
管理具有未列出的安全性類型的 NFS 用戶端的 ONTAP SVM 訪問 . . . 3
ONTAP 安全性類型如何決定 NFS 用戶端存取級別 . . . 5
了解如何管理 ONTAP NFS 超級使用者存取請求 . . . 6
了解 ONTAP NFS 匯出策略緩存 . . . 8
了解 ONTAP NFS 存取快取 . . . 9
了解 ONTAP NFS 存取快取參數 . . . 9
從 ONTAP NFS qtree 中刪除匯出策略 . . . 10
驗證 ONTAP NFS qtree ID 以執行 qtree 檔案操作 . . . 10
ONTAP NFS FlexVol 磁碟區的匯出策略限制和巢狀連接 . . . 11

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。
`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

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
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

快取名稱	儲存的資訊類型
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。