使用 NFS 設定檔案存取

ONTAP 9

NetApp
April 24, 2024

目錄

使用 NFS 設定檔案存取

使用NFS總覽設定檔案存取

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

匯出原則如何控制用戶端對磁碟區或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。

SVM的預設匯出原則

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。

匯出規則的運作方式

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。

使用未列出的安全性類型來管理用戶端

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
是的	否	唯讀為匿名
是的	是的	匿名讀寫

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 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。

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 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。

安全性類型如何決定用戶端存取層級

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`

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...
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。

管理超級使用者存取要求

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。

如何使用匯出原則快取**ONTAP**

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。

存取快取的運作方式

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。

存取快取參數的運作方式

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**qtree**移除匯出原則

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qtree檔案作業的qtree ID

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
```

匯出FlexVol 適用於Sfor Sfor Sfor Volume的原則限制和巢狀連接

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

支援Kerberos ONTAP

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NFS設定Kerberos的需求

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
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"

指定**NFSv4**的使用者**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

如何使用名稱服務交換器組態**ONTAP**

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
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

LDAP總覽

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LDAP伺服器必須在ONTAP 支援TLS或支援SSL的情況下、於支援更新版本的支援更新版本中啟用。不支援SSL。ONTAP
  - 必須已在網域中設定憑證伺服器。
- 若要啟用LDAP參照追蹤（ONTAP 在更新版本的版本中）、必須滿足下列條件：
  - 這兩個網域都應設定下列其中一個信任關係：
    - 雙向
    - 單向、主要信任參照網域
    - 父-子
  - DNS必須設定為解析所有參照的伺服器名稱。
  - 網域密碼應相同、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）

- 從功能性的版本起、您就可以開始使用ONTAP "用於nsswitch驗證的LDAP快速連結。"

- 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"。

LDAP簽署與密封概念

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。

LDAPS概念

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S69.5 - 9.8中ONTAP 、LDAPS只能在連接埠636上啟用。若要這麼做、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、請設定 `-ldaps-enabled` 參數至 `true` 並指定所需的 `-port` 參數。如需詳細資訊、請參閱 `vserver services name-service ldap client create` 手冊頁

> 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。

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。

您需要的產品

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
   ```

LDAP目錄搜尋的組態選項

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搜尋的基礎DN如果需要、可以輸入多個值（例如ONTAP 、如果在更新版本的支援版本中啟用LDAP參照追蹤）。
`-base-scope`	所有LDAP搜尋的基礎範圍
`-user-dn`	所有LDAP使用者搜尋的基礎DNS此參數也適用於使用者名稱對應搜尋。
`-user-scope`	所有LDAP使用者搜尋的基礎範圍此參數也適用於使用者名稱對應搜尋。
`-group-dn`	所有LDAP群組搜尋的基礎DNS
`-group-scope`	所有LDAP群組搜尋的基礎範圍
`-netgroup-dn`	所有LDAP網路群組搜尋的基礎DNS
`-netgroup-scope`	所有LDAP網路群組搜尋的基礎範圍

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）。

改善**LDAP**目錄網路群組各主機搜尋的效能

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。

您需要的產品

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。

> 從 ONTAP 9.2 開始 `-ldap-servers` 取代欄位 `-servers`。此新欄位可以使用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**快速連結進行**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`

   - 如需新的管理使用者、請參閱 "啟用LDAP或NIS帳戶存取。"

顯示 **LDAP** 統計資料

從功能完善的9.2開始ONTAP 、您可以在儲存系統上顯示儲存虛擬機器（SVM）的LDAP統計資料、以監控效能並診斷問題。

您需要的產品

- 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

以下範例顯示物件的效能資料 `secd_external_service_op`：

```
cluster::*> statistics show -vserver vserverName -object
secd_external_service_op -instance "vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1"

Object: secd_external_service_op
Instance: vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1
Start-time: 4/13/2016 22:15:38
End-time: 4/13/2016 22:15:38
Scope: vserverName
Counter                             Value
-------------------------------- --------------------------------
instance_name                       vserverName:LDAP (NIS & Name
                                    Mapping):GetUserInfoFromName:
                                    1.1.1.1
last_modified_time                  1460610787
node_name                           nodeName
num_not_found_responses             1
num_request_failures                1
num_requests_sent                   1
num_responses_received              1
num_successful_responses            0
num_timeouts                        0
operation                           GetUserInfoFromName
process_name                        secd
request_latency                     52131us
```

設定名稱對應

設定名稱對應總覽

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。

名稱對應的運作方式

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。

多網域會搜尋**UNIX**使用者對**Windows**使用者名稱對應

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。

名稱對應轉換規則

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。

建立名稱對應

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
   ```

   > ℹ。 `-pattern` 和 `-replacement` 陳述式可做為規則運算式。您也可以使用 `-replacement` 使用 null 置換字串明確拒絕對應至使用者的陳述 `" "` （空格字元）。請參閱 `vserver name-mapping create` 詳細資訊請參閱手冊頁。

   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
```

設定預設使用者

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`

用於管理名稱對應的命令

管理名稱對應時、會ONTAP 有特定的功能不全指令。

如果您想要...	使用此命令...
建立名稱對應	`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 限定條件項目時、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`

如需詳細資訊、請參閱每個命令的手冊頁。

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:\
   ```

在NFS用戶端上啟用NFS匯出的顯示

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。

從功能更新9.2開始ONTAP 、ONTAP 依預設、支援NFS用戶端檢視匯出清單。在舊版中、 `showmount` 的選項 `vserver nfs modify` 必須明確啟用命令。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)
```