使用SMB設定檔案存取

ONTAP 9

NetApp
February 12, 2026

目錄

使用SMB設定檔案存取

設定安全樣式

安全樣式如何影響資料存取

瞭解 **ONTAP SMB** 安全風格及其影響

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"

瞭解設定 **ONTAP SMB** 安全風格的地點和時機

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。

決定在 **ONTAP VM** 上使用哪些 **SMB** 安全樣式

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 SMB** 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。

瞭解如何保留 **ONTAP SMB FlexVol** 磁碟區的 **UNIX** 權限

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

瞭解如何使用適用於 **ONTAP SMB** 伺服器的 **Windows** 安全性索引標籤來管理 **UNIX** 權限

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 SVM** 根磁碟區上設定 **SMB** 安全樣式

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 FlexVol 磁碟區上設定 SMB 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 qtree 上設定 SMB 安全樣式

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`

在NAS命名空間中建立及管理資料磁碟區

瞭解如何在 NAS 命名空間中建立及管理 ONTAP SMB 資料磁碟區

若要管理NAS環境中的檔案存取、您必須管理儲存虛擬機器（SVM）上的資料磁碟區和交會點。這包括規劃命名空間架構、建立具有或不含交會點的磁碟區、掛載或卸載磁碟區、以及顯示資料磁碟區和NFS伺服器或CIFS伺服器命名空間的相關資訊。

使用指定的交會點建立 ONTAP SMB 資料磁碟區

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。

> 下列字元無法用於交會路徑：*#"><|？\
>
> 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`、 CIFS 共用路徑必須以開頭 `/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「 '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

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 ONTAP SMB 資料磁碟區而不指定交會點

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。

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現有的 ONTAP SMB 磁碟區

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 SMB 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`

如果您要顯示...	輸入命令...
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 -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
```

設定名稱對應

瞭解 **ONTAP SMB** 名稱對應組態

利用名稱對應功能、將CIFS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、並將UNIX身分識別對應至CIFS身分識別。ONTAP無論是從NFS用戶端或CIFS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、但不打算在磁碟區上使用CIFS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。

瞭解 **ONTAP SMB** 名稱對應

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。如果未設定預設的 CIFS 使用者、且 ONTAP 也無法以這種方式取得對應、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。

瞭解 **ONTAP SMB** 多網域搜尋 **UNIX** 使用者至 **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CIFS伺服器主網域的信任關係可以是雙向信任關係、也可以是兩種單向信任關係之一、即傳入信任關係或傳出信任關係。主網域是SVM上CIFS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CIFS伺服器的主網域與另一個網域具有雙向信任、主網域可以驗證及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_

在傳入信任的情況下、其他網域會信任CIFS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	*\系統管理員	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。
*	**	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「*」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。

瞭解 **ONTAP SMB** 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 ONTAP SMB 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*`

> ⓘ `-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
```

設定預設的 ONTAP SMB 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 SMB 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。

設定多網域名稱對應搜尋

啟用或停用 **ONTAP SMB** 多網域名稱對應搜尋

透過多網域名稱對應搜尋、您可以在設定UNIX使用者至Windows使用者名稱對應時、在Windows名稱的網域部分使用萬用字元（*）。在名稱的網域部分使用萬用字元（*）、ONTAP 可讓Sylsin搜尋所有與包含CIFS伺服器電腦帳戶之網域具有雙向信任的網域。

關於這項工作

除了搜尋雙向信任的所有網域之外、您也可以設定偏好的信任網域清單。設定偏好的信任網域清單時ONTAP 、將使用偏好的信任網域清單、而非雙向探索的信任網域、來執行多網域名稱對應搜尋。

- 預設會啟用多網域名稱對應搜尋。
- 此選項適用於進階權限層級。

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：

如果您想要多網域名稱對應搜尋...	輸入命令...
已啟用	`vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled true`
已停用	`vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled false`

3. 返回管理權限層級： `set -privilege admin`

相關資訊

可用的伺服器選項

重設並重新探索信任的 ONTAP SMB 網域

您可以強制重新探索所有信任的網域。當受信任的網域伺服器沒有適當回應或信任關係變更時、此功能就很有用。只會探索主網域具有雙向信任的網域、亦即包含CIFS伺服器電腦帳戶的網域。

步驟

1. 使用重設及重新探索信任的網域 `vserver cifs domain trusts rediscover` 命令。

```
vserver cifs domain trusts rediscover -vserver vs1
```

相關資訊

顯示探索到的信任網域相關資訊

顯示探索到的受信任 ONTAP SMB 網域相關資訊

您可以顯示CIFS伺服器主網域（包含CIFS伺服器電腦帳戶的網域）的已探索信任網域資訊。當您想要知道要探索哪些信任網域、以及如何在探索到的信任網域清單中排序時、這項功能就很有用。

關於這項工作

只會探索具有主網域雙向信任的網域。由於主網域的網域控制器（DC）會依照DC決定的順序傳回信任網域清單、因此無法預測清單中網域的順序。藉由顯示信任網域的清單、您可以決定多網域名稱對應搜尋的搜尋順序。

顯示的信任網域資訊會依節點和儲存虛擬機器（SVM）分組。

步驟

1. 使用顯示探索到的信任網域相關資訊 `vserver cifs domain trusts show` 命令。

```
vserver cifs domain trusts show -vserver vs1
```

```
   Node: node1
Vserver: vs1

Home Domain             Trusted Domain
---------------------   ----------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM

   Node: node2
Vserver: vs1

Home Domain             Trusted Domain
---------------------   ----------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM
```

相關資訊

重設並重新探索信任的網域

在偏好的清單中新增，移除或取代信任的 ONTAP SMB 網域

您可以從SMB伺服器的慣用信任網域清單中新增或移除信任的網域、也可以修改目前的清單。如果您設定慣用的信任網域清單、則執行多網域名稱對應搜尋時、會使用此清單而非探索到的雙向信任網域。

關於這項工作

- 如果您要將信任的網域新增至現有清單、新清單會與現有清單合併、新項目會放在最後系統會依照信任網域清單中顯示的順序來搜尋信任的網域。
- 如果您要從現有清單中移除信任的網域、但未指定清單、則會移除指定儲存虛擬機器（SVM）的整個信任網域清單。
- 如果您修改現有的信任網域清單、新清單會覆寫現有清單。

> 您應該只在慣用的信任網域清單中輸入雙向信任的網域。即使您可以將傳出或傳入的信任網域輸入偏好的網域清單、但在執行多網域名稱對應搜尋時仍不會使用這些網域。跳過單向網域的項目、然後移至清單中的下一個雙向信任網域。ONTAP

步驟

1. 執行下列其中一項動作：

如果您要使用偏好的信任網域清單執行下列動作...	使用命令...
將信任的網域新增至清單	`vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...`
從清單中移除信任的網域	`vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]`
修改現有清單	`vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...`

範例

下列命令會將兩個信任的網域（cifs1.example.com和cifs2.example.com）新增至SVM VS1所使用的慣用信任網域清單：

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

下列命令會從SVM VS1使用的清單中移除兩個信任的網域：

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

下列命令會修改SVM VS1所使用的信任網域清單。新清單會取代原始清單：

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

相關資訊

顯示偏好信任網域清單的相關資訊

顯示偏好的受信任 **ONTAP SMB** 網域清單的相關資訊

您可以顯示偏好的信任網域清單中的信任網域資訊、以及啟用多網域名稱對應搜尋時的搜尋順序。您可以將偏好的信任網域清單設定為使用自動探索的信任網域清單的替代方法。

步驟

1. 執行下列其中一項動作：

如果您要顯示下列項目的相關資訊...	使用命令...
叢集中依儲存虛擬機器（SVM）分組的所有慣用信任網域	`vserver cifs domain name-mapping-search show`
指定SVM的所有慣用信任網域	`vserver cifs domain name-mapping-search show -vserver vserver_name`

下列命令會顯示叢集上所有慣用信任網域的相關資訊：

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver          Trusted Domains
--------------   ---------------------------------
vs1              CIFS1.EXAMPLE.COM
```

相關資訊

在首選清單中新增、刪除或取代受信任網域

建立及設定SMB共用區

瞭解如何建立及設定 ONTAP SMB 共用

在使用者和應用程式能夠透過SMB存取CIFS伺服器上的資料之前、您必須先建立和設定SMB共用、這是磁碟區中的命名存取點。您可以指定共用參數及共用屬性來自訂共用區。您可以隨時修改現有的共用區。

當您建立SMB共用時ONTAP 、利用「完全控制」權限、針對每個人建立共用區的預設ACL。

SMB共用會繫結至儲存虛擬機器（SVM）上的CIFS伺服器。如果刪除SVM、或從SVM中刪除與其相關聯的CIFS伺服器、則會刪除SMB共用。如果您在SVM上重新建立CIFS伺服器、則必須重新建立SMB共用。

相關資訊

- 了解本地用戶和群組
- "Microsoft Hyper-V和SQL Server的SMB組態"
- 配置卷上的檔案名稱轉換的字元映射

瞭解預設的管理 ONTAP SMB 共用

當您在儲存虛擬機器（SVM）上建立CIFS伺服器時、系統會自動建立預設的管理共用區。您應該瞭解這些預設共用是什麼、以及它們的使用方式。

建立CIFS伺服器時、會建立下列預設管理共用：ONTAP

從功能支援的9.8開始ONTAP 、系統將不再預設建立admin$共用區。

- IPC$
- admin$（ONTAP 僅限用作更新版本的版本）
- C$

因為以$字元結尾的共用是隱藏共用、所以「我的電腦」不會顯示預設的管理共用、但您可以使用「共用資料夾」來檢視這些共用。

如何使用**IPC$**和**admin$**預設共用

IPC$和admin$共用是ONTAP 由Windows管理員使用、無法用來存取位於SVM上的資料。

- IPC$共用

  IPC$共用資源可共用具名管道、這些管道對於程式之間的通訊非常重要。IPC$共用區用於遠端管理電腦、以及檢視電腦的共用資源。您無法變更IPC$共用區的共用設定、共用內容或ACL。您也無法重新命名或刪除IPC$共用區。

- admin$共享區（ONTAP 僅限用作更新版本的版本）

  > 從功能支援的9.8開始ONTAP 、系統將不再預設建立admin$共用區。

  admin$共用區是在遠端管理SVM期間使用。此資源的路徑永遠是SVM根目錄的路徑。您無法變更admin$共用區的共用設定、共用內容或ACL。您也無法重新命名或刪除admin$共用區。

使用**c$**預設共用的方式

c$共用區是叢集或SVM管理員可用來存取及管理SVM根磁碟區的管理共用區。

以下是c$共用區的特性：

- 此共用區的路徑永遠是SVM根磁碟區的路徑、無法修改。
- c$共用區的預設ACL為「管理員/完全控制」。

  此使用者為BUILTIN\Administrator。根據預設、BUILTIN\Administrator可以對應至共用區、並在對應的根目錄中檢視、建立、修改或刪除檔案和資料夾。管理此目錄中的檔案和資料夾時、請務必謹慎。

- 您可以變更c$共用區的ACL。
- 您可以變更c$共用設定及共用內容。
- 您無法刪除c$共用區。
- SVM系統管理員可以跨越命名空間連接點、從對應的c$共用區存取SVM命名空間的其餘部分。
- 您可以使用Microsoft管理主控台存取c$共用區。

相關資訊

使用 Windows 安全性標籤設定進階檔案權限

瞭解 **ONTAP SMB** 共享命名要求

在SMB伺服器ONTAP 上建立SMB共用時、請務必記住「不共享區」的命名要求。

共享的名稱命名慣例ONTAP 與Windows相同、並包含下列需求：

- SMB伺服器的每個共用區名稱必須是唯一的。
- 共用名稱不區分大小寫。
- 共享區名稱長度上限為80個字元。
- 支援統一碼共用名稱。
- 以$字元結尾的共用名稱為隱藏共用。
- 對於更新版本的版本、系統會自動在每部CIFS伺服器上建立管理共用區管理$、IPC$和c$、並保留共用名稱ONTAP 。從零件9.8開始ONTAP 、系統不再自動建立admin$共用區。
- 建立共用時、您無法使用共用名稱ONTAP_admin$。
- 支援含有空格的共用名稱：
  - 您不能使用空格作為共用名稱的第一個字元或最後一個字元。
  - 您必須以引號括住包含空格的共用名稱。

    單引號被視為共享區名稱的一部分、無法用來取代引號。

- 當您命名SMB共用時、支援下列特殊字元：

```
! @ # $ % & ' _ - . ~ ( ) { }
```

- 當您命名SMB共用時、不支援下列特殊字元：

```
** [ ] " / \ : ; | < > , ? * =
```

瞭解在多重傳輸協定環境中建立共用時， **ONTAP SMB** 目錄區分大小寫的需求

如果您在SVM中建立共用區、使用8.3命名配置來區分只有不同名稱大小寫的目錄名稱、則必須在共用路徑中使用8.3名稱、以確保用戶端連線至所需的目錄路徑。

在下列範例中、Linux用戶端上建立了兩個名為「'testdir'」和「'TESTDIR'」的目錄。包含目錄的磁碟區的交會路徑為 `/home`。第一個輸出來自Linux用戶端、第二個輸出來自SMB用戶端。

```
 ls -l
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:24 TESTDIR
```

```
dir

 Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

建立第二個目錄的共用時、您必須在共用路徑中使用8.3名稱。在此範例中、第一個目錄的共用路徑為 `/home/testdir` 而第二個目錄的共用路徑則是 `/home/TESTDI~1`。

使用SMB共用內容

瞭解如何使用 **ONTAP SMB** 共用內容

您可以自訂SMB共用的內容。

可用的共用內容如下：

共用內容	說明
`oplocks`	此內容會指定共用區使用投機性鎖定、也稱為用戶端快取。
`browsable`	此內容可讓Windows用戶端瀏覽共用區。
`showsnapshot`	此內容指定用戶端可以檢視及周遊快照。
`changenotify`	此內容指定共用區支援變更通知要求。對於SVM上的共用、這是預設的初始屬性。
`attributecache`	此屬性可讓SMB共用區上的檔案屬性快取、以提供更快速的屬性存取。預設為停用屬性快取。只有當用戶端透過SMB 1.0連線至共用時、才應啟用此屬性。如果用戶端透過SMB 2.x或SMB 3.0連線至共用區、則此共用內容不適用。
`continuously-available`	此內容可讓支援此功能的SMB用戶端持續開啟檔案。以這種方式開啟的檔案可避免發生中斷事件、例如容錯移轉和還原。
`branchcache`	此內容指定共用區可讓用戶端要求此共用區內檔案的BranchCache雜湊。只有在CIFS BranchCache組態中指定「每個共用區」作為作業模式時、此選項才有用。

共用內容	說明
`access-based-enumeration`	此內容指定在此共用區上啟用_Access Based Enumeration_（ABE）。根據個別使用者的存取權限、使用者可以看到經過Abe篩選的共用資料夾、因此無法顯示使用者無權存取的資料夾或其他共用資源。
`namespace-caching`	此內容指定連線至此共用區的SMB用戶端可快取CIFS伺服器傳回的目錄列舉結果、以提供更好的效能。根據預設、SMB 1用戶端不會快取目錄列舉結果。由於SMB 2和SMB 3用戶端預設會快取目錄列舉結果、因此指定此共用內容只能為SMB 1用戶端連線提供效能優勢。
`encrypt-data`	此內容指定存取此共用時必須使用SMB加密。存取SMB資料時不支援加密的SMB用戶端將無法存取此共用區。

新增或移除現有 **ONTAP SMB** 共用上的共用內容

您可以新增或移除共用內容、來自訂現有的SMB共用區。如果您想要變更共用組態以符合環境中不斷變化的需求、這項功能就很有用。

開始之前

您要修改其內容的共用區必須存在。

關於這項工作

新增共用內容的準則：

- 您可以使用以逗號分隔的清單來新增一或多個共用屬性。
- 您先前指定的任何共用內容都會維持有效。

  新增的內容會附加到現有的共用內容清單中。
- 如果您為已套用至共用區的共用屬性指定新值、則新指定的值會取代原始值。
- 您無法使用移除共用內容 `vserver cifs share properties add` 命令。

  您可以使用 `vserver cifs share properties remove` 移除共用內容的命令。

移除共用內容的準則：

- 您可以使用以逗號分隔的清單來移除一或多個共用屬性。
- 您先前已指定但未移除的任何共用內容都會維持有效。

步驟

1. 輸入適當的命令：

如果您想要...	輸入命令...
新增共用內容	`vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`
移除共用內容	`vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`

2. 確認共用內容設定： `vserver cifs share show -vserver vserver_name -share-name share_name`

範例

下列命令會新增 `showsnapshot` 在 SVM VS1 上、將屬性共用至名為「 shahre1 」的共享區：

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share1  /share1   oplocks      -          Everyone / Full
Control
                             browsable
                             changenotify
                             showsnapshot
```

下列命令會移除 `browsable` 在 SVM VS1 上共享名爲 "shahre2" 的共享區的屬性：

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share2  /share2   oplocks      -          Everyone / Full
Control
                             changenotify
```

相關資訊

管理共享的命令

使用強制群組共用設定來最佳化 **ONTAP SMB** 使用者存取

當您以ONTAP UNIX有效的安全性從Sflexity命令列建立共用區到資料時、可以指定該共用區中SMB使用者所建立的所有檔案都屬於同一個群組（稱為_force-group）、該群組必須是UNIX群組資料庫中預先定義的群組。使用強制群組可讓屬於不同群組的SMB使用者更容易存取檔案。

只有當共用位於UNIX或混合qtree中時、才需要指定強制群組。不需要為NTFS磁碟區或qtree中的共用設定強制群組、因為這些共用中的檔案存取權是由Windows權限而非UNIX GID決定。

如果已為共用區指定強制群組、則下列項目將成為該共用區的真實情況：

- 存取此共用區的強制群組中的SMB使用者會暫時變更為強制群組的GID。

  此項GID可讓他們存取此共用區中的檔案、這些檔案無法以主要的GID或UID正常存取。

- 無論檔案擁有者的主要Gid為何、SMB使用者在此共用區中建立的所有檔案都屬於同一個強制群組。

當SMB使用者嘗試存取NFS所建立的檔案時、SMB使用者的主要GID會決定存取權限。

強制群組不會影響NFS使用者存取此共用區中檔案的方式。NFS所建立的檔案會從檔案擁有者處取得Gid。存取權限的判斷取決於嘗試存取檔案的NFS使用者的UID和主要GID。

使用強制群組可讓屬於不同群組的SMB使用者更容易存取檔案。例如、如果您想要建立共用區來儲存公司的網頁、並將寫入權限授予工程與行銷部門的使用者、您可以建立共用區、並授予名為「webGroup1」的群組寫入權限。由於使用強制群組、因此此共用區中SMB使用者所建立的所有檔案均歸「webgroup 1」群組所有。此外、使用者在存取共用時、也會自動指派「webgroup 1」群組的GID。因此、所有使用者都可以寫入此共用區、而不需要管理工程與行銷部門使用者的存取權限。

相關資訊

使用強制群組共享設定建立共享

使用強制群組共用設定建立 **ONTAP SMB** 共用

如果您想讓SMB使用者存取具有UNIX檔案安全性的磁碟區或qtree上的資料、ONTAP 將其視為屬於同一個UNIX群組、您可以使用強制群組共用設定來建立SMB共用區。

步驟

1. 建立 SMB 共用區： `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path path -force-group-for-create` *`UNIX_group_name`*

   如果是 UNC 路徑 (`\\servername\sharename\filepath`）共享區中包含超過 256 個字元（不包括初始「`\\`」）、「Windows 內容」方塊中的「 * 安全性 * 」標籤將無法使用。這是Windows用戶端問題、而非ONTAP 功能不均的問題。為避免此問題、請勿使用超過256個字元的UNC路徑建立共用。

   如果您想要在建立共用之後移除強制群組、可以隨時修改共用區、並指定空字串（ "" ）作為的值 `-force-group-for-create` 參數。如果您透過修改共用區來移除強制群組、則此共用區的所有現有連線仍會將先前設定的強制群組設為主要的Gid。

範例

下列命令會建立「網頁」共用、可在中的網路上存取 `/corp/companyinfo` SMB 使用者建立的所有檔案都指派給 webgroup1 群組的目錄：

```
vserver cifs share create -vserver vs1 -share-name webpages -path
/corp/companyinfo -force-group-for-create webgroup1
```

相關資訊

使用強制群組共享設定優化用戶訪問

使用 MMC 檢視 ONTAP SMB 共用的相關資訊

您可以檢視SVM上SMB共用的相關資訊、並使用Microsoft管理主控台（MMC）執行部分管理工作。您必須先將MMC連線至SVM、才能檢視共用區。

關於這項工作

您可以使用MMC在SVM內的共用上執行下列工作：

- 檢視共享區
- 檢視作用中工作階段
- 檢視開啟的檔案
- 列舉系統中的工作階段、檔案和樹狀結構連線清單
- 關閉系統中開啟的檔案
- 關閉開啟的工作階段
- 建立/管理共用

> 上述功能所顯示的檢視是節點專屬的、而非叢集專屬的。因此、當您使用MMC連線至SMB伺服器主機名稱（即cifs01.domain.local）時、系統會根據您設定DNS的方式、將您路由至叢集內的單一LIF。

MMC ONTAP 不支援下列功能以利執行下列功能：

- 建立新的本機使用者/群組
- 管理/檢視現有的本機使用者/群組
- 檢視事件或效能記錄
- 儲存設備
- 服務與應用程式

在不支援該作業的情況下、您可能會遇到問題 `remote procedure call failed` 錯誤。

"常見問題集：搭配ONTAP 使用Windows MMC搭配使用"

步驟

1. 若要在任何Windows伺服器上開啟「電腦管理」MMC、請在*「控制台」中選取「系統管理工具」*「電腦管理」。

2. 選取*「行動*」>*「連線到另一台電腦*」。

   「選取電腦」對話方塊隨即出現。

3. 鍵入儲存系統的名稱、或按一下*瀏覽*以找出儲存系統。
4. 按一下「確定」。

   MMC會連線至SVM。

5. 在導覽窗格中、按一下*「共享資料夾」>「共享資料夾」*。

   SVM上的共用清單會顯示在右顯示窗格中。

6. 若要顯示共用區的共用內容、請按兩下該共用區、以開啟「內容」對話方塊。
7. 如果無法使用MMC連線至儲存系統、您可以在儲存系統上使用下列其中一個命令、將使用者新增至BUILTIN\Administrators群組或BUILTIN\Power Users群組：

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

用於管理 **SMB** 共用的 **ONTAP** 命令

您可以使用 `vserver cifs share` 和 `vserver cifs share properties` 管理 SMB 共用的命令。

如果您想要...	使用此命令...
建立SMB共用區	`vserver cifs share create`
顯示SMB共用區	`vserver cifs share show`
修改SMB共用區	`vserver cifs share modify`
刪除SMB共用區	`vserver cifs share delete`
新增共用內容至現有的共用區	`vserver cifs share properties add`
從現有共用區移除共用內容	`vserver cifs share properties remove`
顯示共用內容的相關資訊	`vserver cifs share properties show`

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

使用SMB共用ACL來保護檔案存取安全

瞭解如何管理 ONTAP SMB 共用層級 ACL

您可以變更共用層級的ACL、讓使用者擁有更多或更少的共用存取權限。您可以使用Windows使用者和群組或UNIX使用者和群組來設定共用層級ACL。

根據預設，共用層級 ACL 可完全控制名為 Everyone 的標準群組。ACL 中的完全控制權表示網域和所有信任網域中的所有使用者都能完整存取共用區。您可以使用 Windows 用戶端上的 Microsoft 管理主控台 (MMC) 或 ONTAP 命令列來控制共用級 ACL 的存取等級。"建立共用存取控制列表"。

當您使用MMC時、適用下列準則：

- 指定的使用者和群組名稱必須是Windows名稱。
- 您只能指定Windows權限。

當您使用ONTAP flexfuse命令列時、適用下列準則：

- 指定的使用者和群組名稱可以是Windows名稱或UNIX名稱。

  如果在建立或修改ACL時未指定使用者和群組類型、則預設類型為Windows使用者和群組。

- 您只能指定Windows權限。

建立 ONTAP SMB 共用存取控制清單

建立SMB共用區的存取控制清單（ACL）來設定共用權限、可讓您控制使用者和群組對共用區的存取層級。

關於這項工作

您可以使用本機或網域Windows使用者或群組名稱、或UNIX使用者或群組名稱來設定共用層級ACL。

建立新 ACL 之前、您應該先刪除預設的共用 ACL `Everyone / Full Control`，這會帶來安全風險。

在工作群組模式中、本機網域名稱是SMB伺服器名稱。

步驟

1. 刪除預設的共用 ACL:`vserver CIFS 共用存取控制刪除 -vserver <vserver_name> -share <share_name> -user-or -group Everyone`
2. 設定新ACL：

如果您想要使用...來設定**ACL**	輸入命令...
Windows使用者	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\user_name> -permission <access_right>`
Windows群組	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\group_name> -permission <access_right>`
UNIX使用者	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-user> -user-or-group <UNIX_user_name> -permission <access_right>`
UNIX群組	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-group> -user-or-group <UNIX_group_name> -permission <access_right>`

3. 使用驗證套用至共用的 ACL 是否正確 `vserver cifs share access-control show` 命令。

範例

下列命令提供 `Change` 在「vs1.example.com」「SVM：

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com
                Share       User/Group              User/Group  Access
Vserver         Name        Name                    Type
Permission
--------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\Sales Team     windows     Change
```

下列命令會授予 `Read`「工程」 UNIX 群組在「 vs2.example.com 」 SVM 上「 eng 」共用區的權限：

```
cluster1::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com
                Share       User/Group               User/Group  Access
Vserver         Name        Name                     Type
Permission
--------------- ----------- -------------------      -----------
-----------
vs2.example.com  c$          BUILTIN\Administrators   windows
Full_Control
vs2.example.com  eng         engineering              unix-group  Read
```

下列命令會授予 `Change`本機 Windows 群組「 Tiger Team 」的權限、並授予 `Full_Control`本機 Windows 使用者「 Sue Chang 」在「 VS1 」 SVM 上的「 datavol5 」共用區的權限：

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    Tiger Team         windows     Change
vs1            datavol5    Sue Chang          windows     Full_Control
```

用於管理 **SMB** 共用存取控制清單的 **ONTAP** 命令

您需要知道管理SMB存取控制清單（ACL）的命令、包括建立、顯示、修改及刪除這些清單。

如果您想要...	使用此命令...
建立新的 ACL	`vserver cifs share access-control create`
顯示ACL	`vserver cifs share access-control show`
修改ACL	`vserver cifs share access-control modify`
刪除ACL	`vserver cifs share access-control delete`

使用檔案權限來保護檔案存取安全

使用 **ONTAP SMB SVM** 的 **Windows** 安全性標籤配置進階 **NTFS** 檔案權限

您可以使用「Windows內容」視窗中的「* Windows安全性*」索引標籤、設定檔案和資料夾的標準NTFS檔案權限。

開始之前

執行此工作的系統管理員必須擁有足夠的NTFS權限、才能變更所選物件的權限。

關於這項工作

在Windows主機上設定NTFS檔案權限的方法是將項目新增至NTFS安全性描述元相關聯的NTFS判別存取控制清單（DACL）。然後將安全性描述元套用至NTFS檔案和目錄。這些工作會由Windows GUI自動處理。

步驟

1. 從Windows檔案總管的*工具*功能表中、選取*對應網路磁碟機*。
2. 完成*對應網路磁碟機*對話方塊：

   a. 選取*磁碟機*字母。

   b. 在「資料夾」方塊中、輸入CIFS伺服器名稱、其中包含您要套用權限的資料及共用名稱。

      如果您的 CIFS 伺服器名稱為「 CIFS 伺服器」、且您的共用名稱為「 shahre1 」、則應輸入 `\\CIFS_SERVER\share1`。

      您可以指定CIFS伺服器的資料介面IP位址、而非CIFS伺服器名稱。

   c. 單擊*完成*。

   您選取的磁碟機會掛載、並在Windows檔案總管視窗中顯示共用區中包含的檔案和資料夾、做好準備。

3. 選取您要設定NTFS檔案權限的檔案或目錄。
4. 以滑鼠右鍵按一下檔案或目錄、然後選取*內容*。
5. 選取*安全性*索引標籤。

   「安全性」標籤會顯示已設定NTFS權限的使用者和群組清單。「權限」方塊會針對每個選取的使用者或群組、顯示有效的「允許」和「拒絕」權限清單。

6. 按一下*進階*。

   「Windows內容」視窗會顯示指派給使用者和群組之現有檔案權限的相關資訊。

7. 按一下*變更權限*。

   「權限」視窗隨即開啟。

8. 執行所需的動作：

如果您想要...	請執行下列動作...
設定新使用者或群組的進階NTFS權限	a. 按一下「 * 新增 * 」。 b. 在*輸入要選取的物件名稱*方塊中、輸入您要新增的使用者或群組名稱。 c. 按一下「確定」。

如果您想要...	請執行下列動作...
變更使用者或群組的進階NTFS權限	a. 在「權限項目：」方塊中、選取您要變更其進階權限的使用者或群組。 b. 按一下 * 編輯 * 。
移除使用者或群組的進階NTFS權限	a. 在「權限項目：」方塊中、選取您要移除的使用者或群組。 b. 按一下「移除」。 c. 跳至步驟13。

如果您要在新使用者或群組上新增進階NTFS權限、或是變更現有使用者或群組的NTFS進階權限、就會開啟「<Object>的權限項目」方塊。

9. 在「套用至」方塊中、選取您要套用此NTFS檔案權限項目的方式。

   如果您要在單一檔案上設定NTFS檔案權限、則「套用至」方塊不會作用。「套用至」設定預設為*僅此物件*。

10. 在「權限」方塊中、針對您要在此物件上設定的進階權限、選取「允許」或「拒絕」方塊。

    - 若要允許指定的存取權、請選取*允許*方塊。
    - 若要不允許指定的存取、請選取* Deny（拒絕）*方塊。 您可以設定下列進階權限的權限：
    - 完全控制

      如果您選擇此進階權限、則會自動選擇所有其他進階權限（允許或拒絕權限）。

    - 周遊資料夾/執行檔案
    - 列出資料夾/讀取資料
    - 讀取屬性
    - 讀取延伸屬性
    - 建立檔案/寫入資料
    - 建立資料夾/附加資料
    - 寫入屬性
    - 寫入延伸屬性
    - 刪除子資料夾與檔案
    - 刪除
    - 讀取權限
    - 變更權限
    - 取得所有權

    如果任何進階權限方塊無法選取、這是因為權限是從父物件繼承而來。

11. 如果您希望此物件的子資料夾和檔案繼承這些權限、請選取「僅將這些權限套用至此容器內的物件和（或）容器*」方塊。
12. 按一下「確定」。
13. 完成新增、移除或編輯NTFS權限之後、請指定此物件的繼承設定：
    - 選取「包含此物件父項的可繼承權限」方塊。

      這是預設值。
    - 選取「使用此物件的可繼承權限來取代所有子物件權限」方塊。

      如果您要在單一檔案上設定NTFS檔案權限、則此設定不會出現在「權限」方塊中。

      > 選取此設定時請務必謹慎。此設定會移除所有子物件上的所有現有權限、並以此物件的權限設定取代這些權限。您可能不小心移除不想移除的權限。在混合式安全型磁碟區或qtree中設定權限時尤其重要。如果子物件具有UNIX有效的安全樣式、將NTFS權限傳播到這些子物件會ONTAP 導致將這些物件從UNIX安全樣式變更為NTFS安全樣式、而這些子物件上的所有UNIX權限都會以NTFS權限取代。
    - 選取兩個方塊。
    - 請選取兩個方塊。
14. 按一下「確定」以關閉「權限」方塊。
15. 按一下「確定」以關閉「進階安全性設定**<Object>**」方塊。

    如需如何設定進階NTFS權限的詳細資訊、請參閱Windows文件。

相關資訊

- 在伺服器上建立 NTFS 安全描述符
- 顯示NTFS安全型磁碟區上的檔案安全資訊
- 顯示混合式安全型磁碟區的檔案安全資訊
- 顯示UNIX安全型磁碟區上的檔案安全資訊

用於 **SMB NTFS** 檔案權限的 **ONTAP** 命令

您可以使用ONTAP CLI在檔案和目錄上設定NTFS檔案權限。這可讓您設定NTFS檔案權限、而不需要使用Windows用戶端上的SMB共用區連線至資料。

您可以將項目新增至與NTFS安全性描述元相關聯的NTFS判別存取控制清單（DACL）、以設定NTFS檔案權限。然後將安全性描述元套用至NTFS檔案和目錄。

您只能使用命令列設定NTFS檔案權限。您無法使用CLI來設定NFSv4 ACL。

步驟

1. 建立NTFS安全性描述元。

   ```
   vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
   ```

```
ntfs_security_descriptor_name -owner owner_name -group primary_group_name
-control-flags-raw raw_control_flags
```

2. 將DACL新增至NTFS安全性描述元。

```
vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
-rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
{this-folder|sub-folders|files}
```

3. 建立檔案/目錄安全性原則。

```
vserver security file-directory policy create -vserver svm_name -policy-name
policy_name
```

了解透過 **ONTAP SMB** 伺服器存取檔案時提供存取控制的 **UNIX** 檔案權限

一個包含以下三種類型的安全型態之一：NTFS、UNIX或混合式。FlexVol無論安全風格為何、您都可以透過SMB存取資料、不過需要適當的UNIX檔案權限、才能以UNIX有效的安全性存取資料。

當透過SMB存取資料時、在判斷使用者是否有權執行要求的動作時、會使用數種存取控制：

- 匯出權限

  設定SMB存取的匯出權限為選用項目。

- 共用權限
- 檔案權限

  下列類型的檔案權限可能會套用至使用者想要執行動作的資料：

  - NTFS
  - UNIX NFSv4 ACL
  - UNIX模式位元

對於已設定NFSv4 ACL或UNIX模式位元的資料、會使用UNIX樣式權限來決定資料的檔案存取權限。SVM管理員需要設定適當的檔案權限、以確保使用者擁有執行所需動作的權限。

混合式安全型磁碟區中的資料可能具有NTFS或UNIX有效的安全風格。如果資料具有UNIX有效的安全樣式、則在決定資料的檔案存取權限時、會使用NFSv4權限或UNIX模式位元。

使用動態存取控制（**DAC**）保護檔案存取

了解 **ONTAP SMB** 伺服器的 **DAC** 檔案存取安全性

您可以使用動態存取控制、並在Active Directory中建立集中存取原則、並透過套用的群組原則物件（GPO）將其套用至SVM上的檔案和資料夾、以確保存取安全。您可以將稽核設

定為使用集中式存取原則暫存事件、以便在套用變更之前查看中央存取原則的影響。

CIFS認證新增功能

在動態存取控制之前、CIFS認證會包含安全主體（使用者）的身分識別和Windows群組成員資格。有了動態存取控制、憑證中還會新增三種類型的資訊：裝置身分識別、裝置宣告及使用者宣告：

- 裝置識別

  使用者身分識別資訊的類比、但使用者登入裝置的身分識別和群組成員資格除外。

- 裝置聲明

  關於裝置安全主體的說法。例如、裝置宣告可能是特定OU的成員。

- 使用者聲明

  關於使用者安全性主體的說法。例如、使用者聲稱其AD帳戶可能是特定OU的成員。

集中存取原則

檔案的集中存取原則可讓組織集中部署及管理授權原則、這些原則包括使用者群組、使用者宣告、裝置宣告及資源內容的條件式運算式。

例如、若要存取高商業影響資料、使用者必須是全職員工、而且只能從受管理裝置存取資料。集中存取原則是在Active Directory中定義、並透過GPO機制散佈到檔案伺服器。

使用進階稽核進行集中式存取原則登臺

中央存取原則可以是「年齡」、在這種情況下、會在檔案存取檢查期間以「假設」的方式進行評估。原則生效時會發生的結果、以及與目前設定的不同之處、會記錄為稽核事件。如此一來、系統管理員就能在實際執行原則之前、先使用稽核事件記錄來研究存取原則變更的影響。評估存取原則變更的影響之後、即可透過GPO將原則部署至所需的SVM。

相關資訊

- 了解受支援的 GPO
- 了解如何將群組原則物件套用至 SMB 伺服器
- 在伺服器上啟用或停用 GPO 支援
- 顯示有關GPO組態的資訊
- 顯示有關集中存取原則的資訊
- 顯示有關集中存取原則規則的資訊
- 配置中央存取策略以保護伺服器上的數據
- 顯示有關伺服器安全的信息
- "SMB與NFS稽核與安全性追蹤"

ONTAP SMB 伺服器支援的 DAC 功能

如果您想要在CIFS伺服器上使用動態存取控制（DAC）、您需要瞭解ONTAP 如何在Active Directory環境中支援動態存取控制功能。

支援動態存取控制

在CIFS伺服器上啟用動態存取控制時、支援下列功能：ONTAP

功能	註解
宣告進入檔案系統	聲稱是簡單的名稱和值配對、說明使用者的一些真實情況。使用者認證包含宣告資訊、檔案上的安全性描述元可以執行包含宣告檢查的存取檢查。如此可讓系統管理員更精細地控制哪些人可以存取檔案。
檔案存取檢查的條件式運算式	修改檔案的安全性參數時、使用者可以將任意複雜的條件運算式新增至檔案的安全性描述元。條件運算式可以包含宣告檢查。
透過集中存取原則集中控制檔案存取	集中存取原則是一種儲存在Active Directory中的ACL、可標記為檔案。只有在磁碟上的安全性描述元和標記的集中存取原則都允許存取時、才會授予檔案存取權。這可讓系統管理員控制從中央位置（AD）存取檔案的權限、而不需要修改磁碟上的安全性描述元。
集中存取原則接移	藉由「老舊」變更中央存取原則、並在稽核報告中看到變更的影響、來增加在不影響實際檔案存取的情況下嘗試安全性變更的能力。
支援使用ONTAP CLI顯示有關中央存取原則安全性的資訊	延伸 `vserver security file-directory show` 顯示已套用集中存取原則的相關資訊。
包括集中存取原則的安全性追蹤	延伸 `vserver security trace` 命令系列可顯示包含已套用集中存取原則相關資訊的結果。

不支援動態存取控制

在CIFS伺服器上啟用動態存取控制時、不支援下列功能：ONTAP

功能	註解
NTFS檔案系統物件的自動分類	這是ONTAP Windows檔案分類基礎架構的副檔名、不受支援。
進階稽核、不包括集中存取原則接移	進階稽核僅支援集中存取原則移位。

了解如何將 DAC 和中央存取原則與 ONTAP SMB 伺服器結合使用

使用動態存取控制（DAC）和集中存取原則來保護CIFS伺服器上的檔案和資料夾安全時、必須謹記某些考量事項。

如果原則規則套用至網域\系統管理員使用者、則**NFS**存取權限可能會被拒絕

在某些情況下、如果將集中存取原則安全性套用至root使用者嘗試存取的資料、則可能會拒絕NFS存取root。當集中存取原則包含套用至網域\系統管理員的規則、且根帳戶對應至網域\系統管理員帳戶時、就會發生此問題。

您應該將規則套用至具有管理權限的群組、例如網域\系統管理員群組、而非套用規則至網域\系統管理員使用者。如此一來、您就可以將root對應到網域\系統管理員帳戶、而不受root影響。

在**Active Directory**中找不到所套用的集中存取原則時、**CIFS**伺服器的**BUILTIN\Administrator**群組可存取資源

CIFS伺服器中包含的資源可能會套用集中存取原則、但如果CIFS伺服器使用集中存取原則的SID嘗試從Active Directory擷取資訊、則該SID與Active Directory中任何現有的集中存取原則SID都不相符。在此情況下、CIFS伺服器會套用該資源的本機預設還原原則。

本機預設還原原則可讓CIFS伺服器的BUILTIN\Administrator群組存取該資源。

為 ONTAP SMB 伺服器啟用或停用 DAC

預設會停用可讓您使用動態存取控制（DAC）來保護CIFS伺服器上物件的選項。如果您想要在CIFS伺服器上使用動態存取控制、則必須啟用此選項。如果您稍後決定不想使用動態存取控制來保護儲存在CIFS伺服器上的物件、可以停用此選項。

您可以在 Microsoft TechNet Library 中找到有關如何在 Active Directory 上設定動態存取控制的資訊。

"Microsoft TechNet：動態存取控制案例總覽"

關於這項工作

啟用動態存取控制後、檔案系統就能包含具有動態存取控制相關項目的ACL。如果停用動態存取控制、則會忽略目前的動態存取控制項目、不允許新的項目。

此選項僅適用於進階權限層級。

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：

如果您想要動態存取控制...	輸入命令...
已啟用	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled true`
已停用	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled false`

3. 返回系統管理員權限等級： `set -privilege admin`

相關資訊

配置中央存取策略以保護伺服器上的數據

當 ONTAP SMB 伺服器上停用 DAC 時，管理包含 DAC ACE 的 ACL

如果您的資源已將ACL套用至動態存取控制ACE、而且您在儲存虛擬機器（SVM）上停用了動態存取控制、則必須先移除動態存取控制ACE、才能管理該資源上的非動態存取控制ACE。

關於這項工作

停用動態存取控制之後、除非您移除現有的動態存取控制ACE、否則無法移除現有的非動態存取控制ACE或新增非動態存取控制ACE。

您可以使用一般用來管理ACL的工具來執行這些步驟。

步驟

1. 判斷要將哪些動態存取控制ACE套用至資源。
2. 從資源移除動態存取控制ACE。
3. 視需要從資源中新增或移除非動態存取控制ACE。

設定中央存取策略以保護 ONTAP SMB 伺服器上的數據

您必須採取幾個步驟、才能使用集中存取原則來保護CIFS伺服器上的資料存取安全、包括在CIFS伺服器上啟用動態存取控制（DAC）、在Active Directory中設定集中存取原則、將集中存取原則套用至含GPO的Active Directory容器、 並在CIFS伺服器上啟用GPO。

開始之前

- Active Directory必須設定為使用集中存取原則。
- 您必須對Active Directory網域控制器擁有足夠的存取權限、才能建立集中存取原則、以及建立GPO並套用至包含CIFS伺服器的容器。
- 您必須對儲存虛擬機器（SVM）擁有足夠的管理存取權限、才能執行必要的命令。

關於這項工作

集中存取原則會定義並套用至Active Directory上的群組原則物件（GPO）。您可以在 Microsoft TechNet Library 中找到有關如何在 Active Directory 上設定集中存取原則的資訊。

"Microsoft TechNet：集中存取原則案例"

步驟

1. 如果 SVM 尚未使用啟用動態存取控制、請在 SVM 上啟用動態存取控制 `vserver cifs options modify` 命令。

   ```
   vserver cifs options modify -vserver vs1 -is-dac-enabled true
   ```

2. 如果尚未使用啟用群組原則物件（ GPO ）、請在 CIFS 伺服器上啟用這些物件 `vserver cifs group-policy modify` 命令。

   ```
   vserver cifs group-policy modify -vserver vs1 -status enabled
   ```

3. 在Active Directory上建立集中存取規則和集中存取原則。
4. 建立群組原則物件（GPO）、在Active Directory上部署集中存取原則。
5. 將GPO套用至CIFS伺服器電腦帳戶所在的容器。
6. 使用手動更新套用至 CIFS 伺服器的 GPO `vserver cifs group-policy update` 命令。

   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. 使用確認 GPO 中央存取原則已套用至 CIFS 伺服器上的資源 `vserver cifs group-policy show-applied` 命令。

   下列範例顯示預設網域原則有兩個套用至CIFS伺服器的集中存取原則：

   ```
   vserver cifs group-policy show-applied
   ```

   ```
   Vserver: vs1
   ----------------------------
       GPO Name: Default Domain Policy
          Level: Domain
         Status: enabled
     Advanced Audit Settings:
         Object Access:
             Central Access Policy Staging: failure
     Registry Settings:
         Refresh Time Interval: 22
         Refresh Random Offset: 8
         Hash Publication Mode for BranchCache: per-share
         Hash Version Support for BranchCache: all-versions
     Security Settings:
         Event Audit and Event Log:
             Audit Logon Events: none
             Audit Object Access: success
             Log Retention Method: overwrite-as-needed
             Max Log Size: 16384
         File Security:
             /vol1/home
             /vol1/dir1
         Kerberos:
             Max Clock Skew: 5
             Max Ticket Age: 10
             Max Renew Age:  7
         Privilege Rights:
   ```

```
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
```

```
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
2 entries were displayed.
```

相關資訊

- 了解如何將群組原則物件套用至 SMB 伺服器
- 顯示有關GPO組態的資訊
- 顯示有關集中存取原則的資訊
- 顯示有關集中存取原則規則的資訊
- 啟用或停用伺服器的 DAC

顯示有關 **ONTAP SMB** 伺服器的 **DAC** 安全性的信息

您可以顯示NTFS磁碟區上的動態存取控制（DAC）安全性資訊、以及在混合式安全型磁碟區上具有NTFS有效安全性的資料。這包括有關條件式ACE、資源ACE和集中存取原則ACE的資訊。您可以使用結果來驗證安全性組態、或疑難排解檔案存取問題。

關於這項工作

您必須提供儲存虛擬機器（SVM）的名稱、以及您要顯示其檔案或資料夾安全性資訊的資料路徑。您可以以摘要形式或詳細清單來顯示輸出。

步驟

1. 以所需的詳細資料層級顯示檔案和目錄安全性設定：

如果您想要顯示資訊...	輸入下列命令...
以摘要形式提供	`vserver security file-directory show -vserver vserver_name -path path`
更詳細的資料	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

如果您想要顯示資訊...	輸入下列命令...
其中輸出會顯示群組和使用者的SID	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
關於將十六進位位元遮罩轉譯為文字格式之檔案和目錄的檔案和目錄安全性	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

範例

下列範例顯示有關路徑的動態存取控制安全性資訊 `/vol1` 在 SVM VS1 中：

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                           Vserver: vs1
                         File Path: /vol1
                File Inode Number: 112
                   Security Style: mixed
                  Effective Style: ntfs
                   DOS Attributes: 10
           DOS Attributes in Text: ----D---
           Expanded Dos Attribute: -
                     Unix User Id: 0
                    Unix Group Id: 1
                   Unix Mode Bits: 777
           Unix Mode Bits in Text: rwxrwxrwx
                             ACLs: NTFS Security Descriptor
                                   Control:0xbf14
                                   Owner:CIFS1\Administrator
                                   Group:CIFS1\Domain Admins
                                   SACL - ACEs
                                      ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                      RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                      POLICY ID-All resources - No Write-
0x0-OI|CI
                                   DACL - ACEs
                                      ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                      ALLOW-Everyone-0x1f01ff-OI|CI
                                      ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)
```

相關資訊

- 顯示有關GPO組態的資訊
- 顯示有關集中存取原則的資訊
- 顯示有關集中存取原則規則的資訊

ONTAP SMB 伺服器上 DAC 的復原註意事項

您應該瞭解還原ONTAP 至不支援動態存取控制（DAC）的版本時會發生什麼事、以及還原之前和之後必須執行的動作。

如果您想要將叢集還原成ONTAP 不支援動態存取控制的版本、且已在一或多個儲存虛擬機器（SVM）上啟用動態存取控制、則必須先執行下列動作、才能還原：

- 您必須停用叢集上所有已啟用動態存取控制的SVM。
- 您必須修改包含的叢集上的任何稽核組態 `cap-staging` 僅使用的事件類型 `file-op` 事件類型。

您必須瞭解動態存取控制ACE的檔案和資料夾、並採取行動：

- 如果叢集還原、則不會移除現有的動態存取控制ACE；不過、檔案存取檢查會忽略這些ACE。
- 由於還原後會忽略動態存取控制ACE、因此使用動態存取控制ACE的檔案存取權會有所變更。

  這可能會允許使用者存取先前無法存取的檔案、或無法存取先前可能存取的檔案。

- 您應該將非動態存取控制ACE套用至受影響的檔案、以還原其先前的安全層級。

  這可以在還原之前或還原完成後立即完成。

> 由於還原後會忽略動態存取控制ACE、因此在將非動態存取控制ACE套用至受影響的檔案時、不需要將其移除。不過、如果需要、您可以手動移除。

使用匯出原則保護 SMB 存取安全

了解如何將匯出策略與 ONTAP SMB 存取權結合使用

如果SMB伺服器上已啟用SMB存取的匯出原則、則會在控制SMB用戶端對SVM磁碟區的存取時使用匯出原則。若要存取資料、您可以建立允許SMB存取的匯出原則、然後將原則與包含SMB共用的磁碟區建立關聯。

匯出原則會套用一或多個規則、指定允許哪些用戶端存取資料、以及哪些驗證傳輸協定支援唯讀和讀寫存取。您可以設定匯出原則、允許透過SMB存取所有用戶端、用戶端子網路或特定用戶端、並在決定資料的唯讀和讀寫存取時、允許使用Kerberos驗證、NTLM驗證或Kerberos和NTLM驗證進行驗證。

在處理所有套用至匯出原則的匯出規則之後ONTAP 、即可判斷用戶端是否已獲授予存取權限、以及授予何種存取層級。匯出規則適用於用戶端機器、而非Windows使用者和群組。匯出規則不會取代Windows使用者和群組型驗證與授權。匯出規則除了提供共用和檔案存取權限之外、還提供另一層存取安全性。

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

- 為SVM的每個Volume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。
- 將相同的匯出原則指派給SVM的多個磁碟區、以獲得相同的用戶端存取控制權、而無需為每個磁碟區建立新的匯出原則。

每個SVM至少有一個稱為「預設」的匯出原則、不含任何規則。您無法刪除此匯出原則、但可以重新命名或修改它。SVM上的每個Volume預設都與預設匯出原則相關聯。如果在SVM上停用SMB存取的匯出原則、「預設」匯出原則對SMB存取沒有影響。

您可以設定規則來提供NFS和SMB主機的存取權、並將該規則與匯出原則建立關聯、然後再與包含NFS和SMB主機所需存取之資料的磁碟區建立關聯。或者、如果有些磁碟區只有SMB用戶端需要存取、您可以設定匯出原

則、其中的規則僅允許使用SMB傳輸協定存取、而且只使用Kerberos或NTLM（或兩者）進行唯讀和寫入存取驗證。然後、匯出原則會與僅需要SMB存取的磁碟區建立關聯。

如果啟用SMB的匯出原則、且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。如果用戶端不符合磁碟區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。即使共用和檔案權限不允許存取、也會發生這種情況。這表示您必須將匯出原則設定為在包含SMB共用的磁碟區上、至少允許下列項目：

- 允許存取所有用戶端或適當的用戶端子集
- 允許透過SMB存取
- 使用Kerberos或NTLM驗證（或兩者）、允許適當的唯讀和寫入存取

深入瞭解 "設定及管理匯出原則"。

了解 ONTAP SMB 匯出規則

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。

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。

限製或允許透過 **SMB** 進行存取的 **ONTAP** 導出策略規則範例

這些範例說明如何在啟用SMB存取匯出原則的SVM上、建立限制或允許存取SMB的匯出原則規則。

SMB存取的匯出原則預設為停用。只有在啟用SMB存取的匯出原則時、才需要設定限制或允許透過SMB存取的匯出原則規則。

僅適用於**SMB**存取的匯出規則

下列命令會在名為「'VS1'」的SVM上建立具有下列組態的匯出規則：

- 原則名稱：if1
- 索引編號：1.
- 用戶端比對：僅比對網路192.168.1.0/24上的用戶端
- 傳輸協定：僅啟用SMB存取
- 唯讀存取：使用NTLM或Kerberos驗證的用戶端

- 讀寫存取：使用Kerberos驗證的用戶端

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

SMB與NFS存取的匯出規則

下列命令會在SVM上建立具有下列組態的「」VS1「匯出規則：

- 原則名稱：ifsnfs1
- 索引編號： 2.
- 用戶端配對：符合所有用戶端
- 傳輸協定：SMB與NFS存取
- 唯讀存取：存取所有用戶端
- 讀寫存取：使用Kerberos（NFS和SMB）或NTLM驗證（SMB）的用戶端
- UNIX使用者ID 0對應（零）：對應至使用者ID 65534（通常對應至使用者名稱nobnobody）
- SUID和SGID存取：允許

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule
any -rwrule krb5,ntlm -anon 65534 -allow-suid true
```

僅使用**NTLM**匯出**SMB**存取規則

下列命令會在名為「'VS1'」的SVM上建立具有下列組態的匯出規則：

- 原則名稱：ntlm1
- 索引編號：1.
- 用戶端配對：符合所有用戶端
- 傳輸協定：僅啟用SMB存取
- 唯讀存取：僅限使用NTLM的用戶端
- 讀寫存取：僅限使用NTLM的用戶端

如果您將唯讀選項或讀寫選項設定為僅限NTL-存取、則必須在用戶端比對選項中使用IP位址型項目。否則、您就會收到 `access denied` 錯誤。這是因為ONTAP 使用主機名稱檢查用戶端存取權限時、使用Kerberos服務主要名稱（SPN-）。NTLM驗證不支援SPN-Name。

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

啟用或停用 **ONTAP** 匯出策略以進行 **SMB** 訪問

您可以在儲存虛擬機器（SVM）上啟用或停用SMB存取的匯出原則。您可以選擇使用匯出原則來控制SMB對資源的存取。

開始之前

以下是啟用SMB匯出原則的需求：

- 在您為該用戶端建立匯出規則之前，用戶端必須在 DNS 中有「 PTR 」記錄。
- 如果 SVM 提供對 NFS 用戶端的存取，而您要用於 NFS 存取的主機名稱與 CIFS 伺服器名稱不同，則需要額外的一組主機名稱「 A 」和「 PTR 」記錄。

關於這項工作

在SVM上設定新的CIFS伺服器時、預設會停用SMB存取的匯出原則。如果您想要根據驗證傳輸協定或用戶端IP位址或主機名稱來控制存取、可以啟用SMB存取的匯出原則。您可以隨時啟用或停用SMB存取的匯出原則。

> 在啟用 NFS 的 SVM 中啟用 CIFS/SMB 的匯出原則，可讓 Linux 用戶端使用 `showmount -e` SVM 上的命令，檢視所有 SMB 磁碟區的交會路徑及相關的匯出原則規則。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 啟用或停用匯出原則：
   - 啟用匯出原則： `vserver cifs options modify -vserver vserver_name -is -exportpolicy-enabled true`
   - 停用匯出原則： `vserver cifs options modify -vserver vserver_name -is -exportpolicy-enabled false`
3. 返回管理權限層級： `set -privilege admin`

範例

下列範例可讓您使用匯出原則來控制SMB用戶端對SVM VS1上資源的存取：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

使用儲存層級存取保護來保護檔案存取安全

了解如何使用儲存層級存取防護來保護 **ONTAP SMB** 檔案存取

除了使用原生檔案層級來保護存取安全、以及匯出及共用安全性、您也可以設定儲存層級的存取保護、ONTAP 這是由流通量層級的第三層安全防護。儲存層級存取保護適用於從所有NAS傳輸協定存取套用到儲存物件的存取。

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

儲存層級存取保護行為

- 儲存層級的存取保護適用於儲存物件中的所有檔案或目錄。

  由於某個Volume中的所有檔案或目錄都受限於儲存層級的存取保護設定、因此不需要透過傳播進行繼承。

- 您可以設定儲存層級的存取保護、使其僅套用至檔案、僅套用至目錄、或同時套用至磁碟區內的檔案和目錄。
  - 檔案與目錄安全性

    適用於儲存物件內的每個目錄和檔案。這是預設設定。

  - 檔案安全性

    適用於儲存物件內的每個檔案。套用此安全性不會影響目錄的存取或稽核。

  - 目錄安全性

    適用於儲存物件內的每個目錄。套用此安全性不會影響檔案的存取或稽核。

- 儲存層級的存取保護用於限制權限。

  它永遠不會提供額外的存取權限。

- 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。

  它會套用至儲存物件層級、並儲存在用於判斷有效權限的中繼資料中。

- 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安全性。

  它的設計僅供儲存管理員修改。

- 您可以將儲存層級的存取保護套用至NTFS或混合式安全型態的磁碟區。
- 只要包含該磁碟區的SVM已設定CIFS伺服器、您就可以將儲存層級的存取保護套用至具有UNIX安全樣式的磁碟區。
- 當磁碟區掛載於磁碟區交會路徑下、且該路徑上有儲存層級存取保護、則不會將其傳播至其下掛載的磁碟區。
- 儲存層級的存取保護安全性描述元會透過SnapMirror資料複寫和SVM複寫來複寫。
- 病毒掃描程式有特殊的分配。

  即使儲存層級的存取保護拒絕存取物件、這些伺服器仍可享有特殊存取權限來篩選檔案和目錄。

- 如果因為儲存層級存取保護而拒絕存取、則不會傳送FPolicy通知。

存取檢查順序

檔案或目錄的存取權取決於匯出或共用權限、在磁碟區上設定的儲存層級存取保護權限、以及套用至檔案和/或目錄的原生檔案權限的組合效應。評估所有層級的安全性、以判斷檔案或目錄具有哪些有效權限。安全性存取檢查的執行順序如下：

1. SMB共用區或NFS匯出層級權限
2. 儲存層級存取保護
3. NTFS檔案/資料夾存取控制清單（ACL）、NFSv4 ACL或UNIX模式位元

使用儲存層級存取保護的使用案例

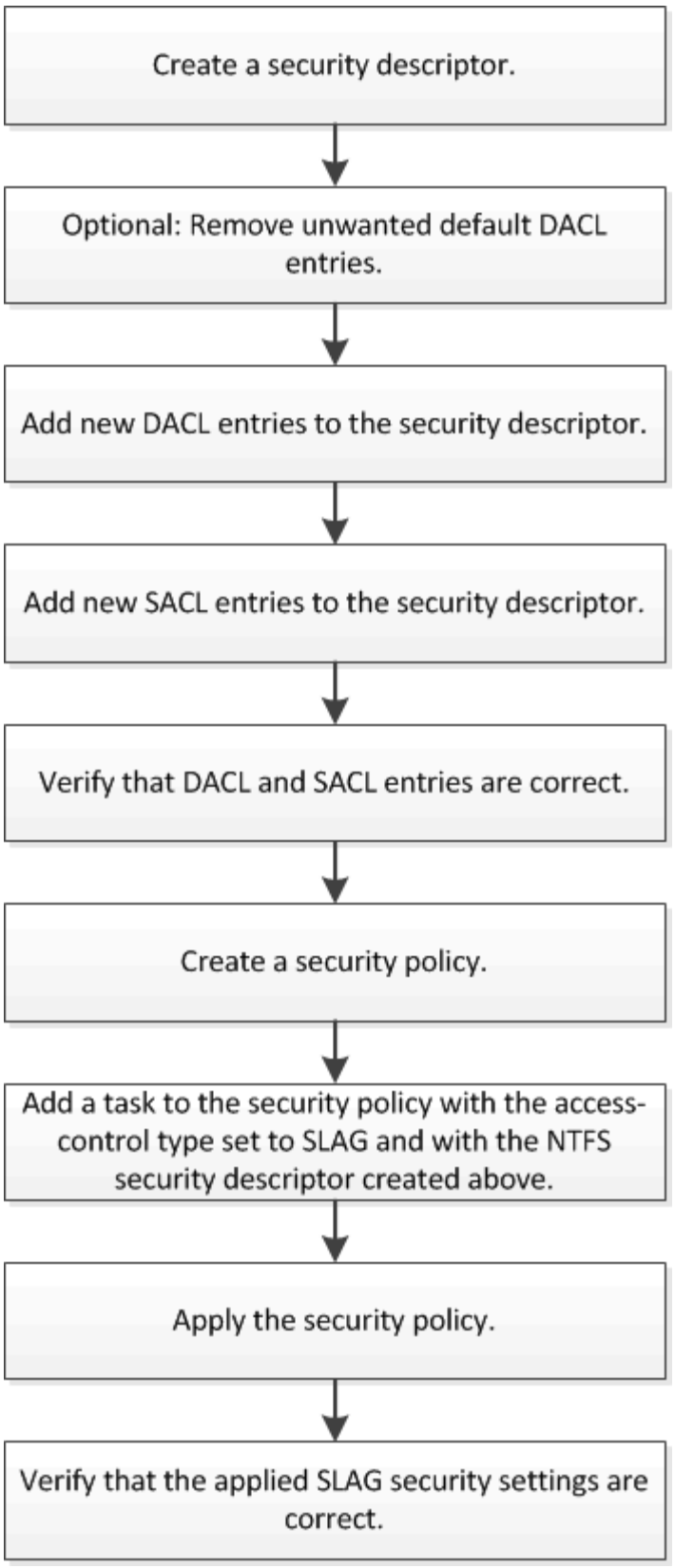
儲存層級的存取保護功能可在儲存層級提供額外的安全性、從用戶端看不到；因此、任何使用者或系統管理員都無法從其桌面撤銷。在某些使用案例中、在儲存層級控制存取的能力是有益的。

此功能的一般使用案例包括下列案例：

- 透過稽核及控制所有使用者在儲存層級的存取、來保護智慧財產
- 金融服務公司（包括銀行和交易集團）的儲存設備
- 為個別部門提供具有獨立檔案儲存設備的政府服務
- 大學保護所有學生檔案

ONTAP SMB 伺服器上儲存層級存取防護的設定工作流程

設定儲存層級存取保護（slag）的工作流程使用相同ONTAP 的CLI命令來設定NTFS檔案權限和稽核原則。您可以在指定的儲存虛擬機器（SVM）磁碟區上設定slag、而非在指定的目標上設定檔案和目錄存取。



相關資訊

在伺服器上配置儲存級別存取防護

在 ONTAP SMB 伺服器上設定儲存層級存取防護

在Volume或qtree上設定儲存層級存取保護時、您需要遵循許多步驟。儲存層級的存取保護可提供在儲存層級設定的存取安全性層級。它提供的安全性適用於從所有NAS傳輸協定到套用它的儲存物件的所有存取。

步驟

1. 使用建立安全性描述元 `vserver security file-directory ntfs create` 命令。

   `vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1 vserver security file-directory ntfs show -vserver vs1`

```
Vserver: vs1

   NTFS Security    Owner Name
   Descriptor Name
   ------------     --------------
   sd1              -
```

   安全性描述元會以下列四個預設DACL存取控制項目（ACE）建立：

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    BUILTIN\Administrators
                     allow    full-control   this-folder, sub-folders,
files
    BUILTIN\Users    allow    full-control   this-folder, sub-folders,
files
    CREATOR OWNER    allow    full-control   this-folder, sub-folders,
files
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

   如果您不想在設定儲存層級存取保護時使用預設項目、可以在建立及新增自己的ACE至安全性描述元之前將其移除。

2. 從安全性描述元中移除任何您不想設定儲存層級存取保護安全性的預設DACL ACE：

   a. 使用移除任何不想要的 DACL ACE `vserver security file-directory ntfs dacl remove` 命令。

在此範例中、安全性描述元中會移除三個預設的DACL ACE：BUILTIN\Administrator、BUILTIN\Users和Creator Owners。

```
vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
-access-type allow -account builtin\users vserver security file-directory
ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
builtin\administrators vserver security file-directory ntfs dacl remove
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
```

b. 請使用確認您不想用於儲存層級存取保護安全性的 DACL ACE 已從安全性描述元中移除 `vserver security file-directory ntfs dacl show` 命令。

在此範例中、命令的輸出會驗證安全性描述元中是否已移除三個預設的DACL ACE、只留下NT AUTORITY\SYSTEM預設的DACL ACE項目：

```
vserver security file-directory ntfs dacl show -vserver vs1
```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

3. 使用將一或多個 DACL 項目新增至安全性描述元 `vserver security file-directory ntfs dacl add` 命令。

在此範例中、安全性描述元中會新增兩個DACL ACE：

```
vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
-access-type allow -account example\engineering -rights full-control -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs dacl add
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
-rights read -apply-to this-folder,sub-folders,files
```

4. 使用將一或多個 SACL 項目新增至安全性描述元 `vserver security file-directory ntfs sacl add` 命令。

在此範例中、兩個 SACL ACE 會新增至安全性描述元：

```
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
-access-type failure -account "example\Domain Users" -rights read -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. 使用確認 DACL 和 SACL ACE 已正確設定 `vserver security file-directory ntfs dacl show`

和 `vserver security file-directory ntfs sacl show` 命令。

在此範例中、下列命令會顯示安全性描述元「'shd1」的DACL項目資訊：

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    EXAMPLE\Domain Users
                     allow    read           this-folder, sub-folders,
files
    EXAMPLE\engineering
                     allow    full-control   this-folder, sub-folders,
files
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

在此範例中、下列命令會顯示安全性描述元「'shd1'」的SACL項目相關資訊：

```
vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    EXAMPLE\Domain Users
                     failure  read           this-folder, sub-folders,
files
    EXAMPLE\engineering
                     success  full-control   this-folder, sub-folders,
files
```

6. 使用建立安全性原則 `vserver security file-directory policy create` 命令。

以下範例建立名為「policy1'」的原則：

```
vserver security file-directory policy create -vserver vs1 -policy-name
policy1
```

7. 使用確認原則已正確設定 `vserver security file-directory policy show` 命令。

   ```
   vserver security file-directory policy show
   ```

   ```
      Vserver          Policy Name
      ------------     --------------
      vs1              policy1
   ```

8. 使用將具有相關安全性描述元的工作新增至安全性原則 `vserver security file-directory policy task add` 命令 `-access-control` 參數設為 `slag`。

   即使原則可以包含多個儲存層級的存取保護工作、您也無法將原則設定為同時包含檔案目錄和儲存層級的存取保護工作。原則必須包含所有儲存層級的存取保護工作或所有檔案目錄工作。

   在此範例中、工作會新增至名為「policy1」的原則、該原則會指派給安全性描述元「shD1」。它會指派給 `/datavol1` 存取控制類型設為「 lag 」的路徑。

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode
   propagate -ntfs-sd sd1
   ```

9. 使用確認工作已正確設定 `vserver security file-directory policy task show` 命令。

   ```
   vserver security file-directory policy task show -vserver vs1 -policy-name
   policy1
   ```

   ```
    Vserver: vs1
     Policy: policy1

      Index  File/Folder  Access           Security  NTFS       NTFS
   Security
             Path         Control          Type      Mode       Descriptor
   Name
      -----  -----------  ---------------  --------  ----------
   ---------------
      1      /datavol1    slag             ntfs      propagate  sd1
   ```

10. 使用套用儲存層級存取保護安全性原則 `vserver security file-directory apply` 命令。

    ```
    vserver security file-directory apply -vserver vs1 -policy-name policy1
    ```

    已排程要套用安全性原則的工作。

11. 使用驗證套用的儲存層級存取保護安全性設定是否正確 `vserver security file-directory show` 命令。

    在此範例中、命令的輸出顯示儲存層級存取保護安全性已套用至 NTFS 磁碟區 `/datavol1`。即使預設

的DACL允許「所有人」完全控制、儲存層級的存取保護安全性仍會限制（及稽核）存取儲存層級存取保護設定中定義的群組。

```
vserver security file-directory show -vserver vs1 -path /datavol1
```

```
                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

相關資訊

- 用於管理 NTFS 檔案安全、NTFS 審核原則和儲存層級存取防護的命令
- 伺服器上儲存層級存取防護的設定工作流程

- 顯示有關伺服器上儲存層級存取防護的信息
- 刪除伺服器上的儲存層級存取保護

ONTAP SMB 伺服器上的有效 SLAG 矩陣

您可以在磁碟區或qtree或兩者上設定slag。根據slog對照表、您可以定義哪些Volume或qtree是適用的slog組態、以符合表格中所列的各種情境。

	在美國的主動轉向系統中使用大量的	快照中的 **Volume slag**	在美國的美國美國美國戰地服務團（**AFF S**）中使用**qtree**	在快照中使用 **qtree slig**
存取檔案系統（AFs）中的Volume存取	是的	否	不適用	不適用
快照中的 Volume 存取	是的	否	不適用	不適用
在主動轉向服務器中存取qtree（當qtree中有slog時）	否	否	是的	否
在主動轉向服務器中存取qtree（當qtree中不存在slog時）	是的	否	否	否
在快照中存取 qtree（當 qtree AFS 中存在 slag 時）	否	否	是的	否
qtree 存取快照（當 qtree AFS 中不存在 slag 時）	是的	否	否	否

顯示有關 ONTAP SMB 伺服器上的儲存層級存取防護的信息

儲存層級的存取保護是套用在磁碟區或qtree上的第三層安全保護。無法使用Windows內容視窗檢視儲存層級的存取保護設定。您必須使用ONTAP VMware CLI來檢視儲存層級存取保護安全性的相關資訊、以便用來驗證組態或疑難排解檔案存取問題。

關於這項工作

您必須提供儲存虛擬機器（SVM）的名稱、以及要顯示其儲存層級存取保護安全性資訊的磁碟區或qtree路徑。您可以以摘要形式或詳細清單來顯示輸出。

步驟

1. 顯示儲存層級的存取保護安全設定、並提供所需的詳細資料：

如果您想要顯示資訊...	輸入下列命令...
以摘要形式提供	`vserver security file-directory show -vserver vserver_name -path path`
更詳細的資料	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

範例

以下範例顯示 NTFS 安全性樣式磁碟區的儲存層級存取保護安全性資訊及路徑 `/datavol1` 在 SVM VS1 中：

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

以下範例顯示儲存層級存取保護在路徑上的混合式安全樣式磁碟區相關資訊 `/datavol5` 在 SVM VS1 中。此磁碟區的最上層具有UNIX有效的安全性。Volume具有儲存層級的存取保護安全性。

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

刪除 **ONTAP SMB** 伺服器上的儲存層級存取保護

如果您不想再在儲存層級設定存取安全性、可以移除磁碟區或qtree上的儲存層級存取保護。移除儲存層級的存取保護不會修改或移除一般NTFS檔案和目錄安全性。

步驟

1. 使用確認磁碟區或 qtree 已設定儲存層級存取保護 `vserver security file-directory show` 命令。

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

                         Storage-Level Access Guard security
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

2. 使用移除儲存層級存取保護 `vserver security file-directory remove-slag` 命令。

   ```
   vserver security file-directory remove-slag -vserver vs1 -path /datavol2
   ```

3. 使用確認儲存層級存取保護已從 Volume 或 qtree 移除 `vserver security file-directory show` 命令。

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
               Vserver: vs1
             File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```