使用 CLI 管理 SMB

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/zh-tw/ontap/smb-admin/index.html on February 12, 2026. Always check docs.netapp.com for the latest.

目錄

使用 CLI 管理 SMB

瞭解 ONTAP SMB

SMB傳輸協定可使用的支援資料檔存取功能。ONTAP您可以啟用CIFS伺服器、建立共用及啟用Microsoft服務。

SMB（伺服器訊息區塊）是指通用網際網路檔案系統（CIFS）傳輸協定的現代語言。您仍會在ONTAP VMware的指令行介面（CLI）和OnCommand VMware的管理工具中看到_CIFS_。

SMB伺服器支援

瞭解 ONTAP SMB 伺服器支援

您可以在儲存虛擬機器（SVM）上啟用和設定SMB伺服器、讓SMB用戶端存取叢集上的檔案。

- 叢集中的每個資料SVM只能繫結到一個Active Directory網域。
- 資料SVM不需要繫結至同一個網域。
- 多個SVM可以綁定到同一個網域。

您必須先設定用來提供資料的SVM和LIF、才能建立SMB伺服器。如果您的資料網路不平坦、您可能還需要設定IPspace、廣播網域和子網路。

相關資訊

"網路管理"

修改伺服器

"系統管理"

支援的 ONTAP SMB 版本與功能

伺服器訊息區（SMB）是Microsoft Windows用戶端和伺服器所使用的遠端檔案共用傳輸協定。支援所有 SMB 版本。您應該確認ONTAP 支援您環境中所需的用戶端和功能的功能。

有關哪些SMB用戶端和網域控制器ONTAP 支援的最新資訊、請參閱「互通性對照表工具」。

ONTAP SMB 伺服器預設會啟用 SMB 2.0 及更新版本，並可視需要啟用或停用。SMB 1.0 可視需要啟用或停用。

SMB 1.0和2.0連線至網域控制器的預設設定也取決於ONTAP 版本。如"指令參考資料ONTAP"需詳細 `vserver cifs security modify`資訊，請參閱。對於現有CIFS伺服器執行SMB 1.0的環境、您應該盡快移轉至較新的SMB版本、以準備增強安全性與法規遵循。如需詳細資訊、請聯絡您的NetApp代表。

下表顯示每個SMB版本支援哪些SMB功能。部分SMB功能預設為啟用、有些則需要額外的組態。

此功能：	需要啟用：	*支援上述**SMB**版本*的支援功能**ONTAP**	
		3.0	3.1.1
舊版SMB 1.0功能		x	x
耐用的握把		x	x
複雜作業		x	x
非同步作業		x	x
增加讀寫緩衝區大小		x	x
提升擴充性		x	x
SMB簽署	x	x	x
替代資料串流（ADS）檔案格式	x	x	x
大型MTU（預設為ONTAP以支援功能更新為開頭）	x	x	x
租賃oplocks		x	x
持續可用的共用	x	x	x
持續處理		x	x
見證人		x	x
SMB加密：AES-128與CCM	x	x	x
橫向擴充（CA共用區要求）		x	x
透明的容錯移轉		x	x
SMB多通道（從ONTAP NetApp 9.4開始）	x	x	x

此功能：	需要啟用：	*支援上述SMB版本*的支援功能ONTAP	
預先驗證完整性			x
叢集用戶端容錯移轉v.2（CCFv2）			x
SMB 加密： AES-128/GCM	x		x

相關資訊

了解如何使用 ONTAP 簽章來增強網路安全

設定伺服器最低身份驗證安全級別

在SMB伺服器上設定必要的SMB加密、以便透過SMB傳輸資料

"NetApp互通性"

ONTAP SMB 中不支援的 Windows 功能

在您的網路中使用CIFS之前、您必須注意ONTAP 到某些不支援的Windows功能。

不支援下列Windows功能：ONTAP

- 加密檔案系統（EFS）
- 在變更日誌中記錄NT檔案系統（NTFS）事件
- Microsoft檔案複寫服務（FRS）
- Microsoft Windows索引服務
- 透過階層式儲存管理（HSM）進行遠端儲存
- 從Windows用戶端進行配額管理
- Windows配額語義
- LMHOSTS.檔案
- NTFS原生壓縮

在 ONTAP SMB VM 上設定 NIS 或 LDAP 名稱服務

透過SMB存取、即使存取NTFS安全型磁碟區中的資料、也會一律執行與UNIX使用者的使用者對應。如果您將Windows使用者對應至儲存在NIS或LDAP目錄存放區中的對應UNIX使用者、或是使用LDAP進行名稱對應、則應該在SMB設定期間設定這些名稱服務。

開始之前

您必須自訂名稱服務資料庫組態、以符合您的名稱服務基礎架構。

關於這項工作

SVM會使用名稱服務ns-交換器資料庫來決定查詢指定名稱服務資料庫來源的順序。ns 交換器來源可以是、 `nis`或 `ldap`的任意組合 `files`。針對Groups資料庫、ONTAP Ses庫 會嘗試從所有已設定的來源取得群組成員資格、然後使用整合的群組成員資格資訊進行存取檢查。如果其中一個來源在取得UNIX群組資訊時無法使用、ONTAP 則無法取得完整的UNIX認證、後續的存取檢查可能會失敗。因此、您必須一律在ns交換器設定中、檢查是否已針對群組資料庫設定所有的ns交換器來源。

預設是讓 SMB 伺服器將所有 Windows 使用者對應至儲存在本機中的預設 UNIX 使用者 `passwd` 資料庫。如果您想要使用預設組態、則可選擇設定NIS或LDAP UNIX使用者與群組名稱服務或LDAP使用者對應、以供SMB存取。

步驟

1. 如果UNIX使用者、群組及netgroup資訊是由NIS名稱服務管理、請設定NIS名稱服務：

   a. 使用判斷名稱服務的目前順序 `vserver services name-service ns-switch show` 命令。

      在此範例中、這三個資料庫 (`group`、 `passwd`和 `netgroup`） `nis` 因為名稱服務來源僅在使用中 `files` 做為來源。

      ```
      vserver services name-service ns-switch show -vserver vs1
      ```

      ```
                                                   Source
      Vserver         Database       Enabled       Order
      --------------- ------------   ---------     ---------
      vs1             hosts          true          dns,
                                                   files
      vs1             group          true          files
      vs1             passwd         true          files
      vs1             netgroup       true          files
      vs1             namemap        true          files
      ```

      您必須新增 `nis` 的來源 `group` 和 `passwd` 資料庫、或是選擇性的 `netgroup` 資料庫。

   b. 使用調整名稱服務 nS-switch 資料庫的順序 `vserver services name-service ns-switch modify` 命令。

      為獲得最佳效能、除非您計畫在SVM上設定名稱服務、否則不應將名稱服務新增至名稱服務資料庫。

      如果您修改多個名稱服務資料庫的組態、則必須針對每個要修改的名稱服務資料庫分別執行命令。

      在此範例中、 `nis` 和 `files` 設定為的來源 `group` 和 `passwd` 資料庫、依此順序。其餘的名稱服務資料庫則維持不變。

      ```
      vserver services name-service ns-switch modify -vserver vs1 -database group
      -sources nis,files vserver services name-service ns-switch modify -vserver
      vs1 -database passwd -sources nis,files
      ```

   c. 使用確認名稱服務的順序正確無誤 `vserver services name-service ns-switch show` 命令。

```
vserver services name-service ns-switch show -vserver vs1
```

```
                                                Source
Vserver         Database       Enabled          Order
--------------- ------------   ---------        ---------
vs1             hosts          true             dns,
                                                files
vs1             group          true             nis,
                                                files
vs1             passwd         true             nis,
                                                files
vs1             netgroup       true             files
vs1             namemap        true             files
```

d. 建立 NIS 名稱服務組態：
`vserver services name-service nis-domain create -vserver <vserver_name> -domain <NIS_domain_name> -servers <NIS_server_IPaddress>,…`

```
vserver services name-service nis-domain create -vserver vs1 -domain example.com -servers 10.0.0.60
```

> 領域 `-nis-servers`取代了領域 `-servers` 。此欄位可以採用 NIS 伺服器的主機名稱或 IP 位址。

e. 確認 NIS 名稱服務已正確設定： `vserver services name-service nis-domain show vserver <vserver_name>`

```
vserver services name-service nis-domain show vserver vs1
```

```
Vserver         Domain                Server
--------------- --------------------- ---------------
vs1             example.com           10.0.0.60
```

2. 如果UNIX使用者、群組及netgroup資訊或名稱對應是由LDAP名稱服務管理、請使用所在的資訊來設定LDAP名稱服務 "NFS管理"。

瞭解 ONTAP SMB 名稱服務交換器組態

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

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

資料庫類型

此表格會針對下列每一種資料庫類型儲存個別的名稱服務清單：

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

以下範例顯示 SVM 的名稱服務交換器組態 `svm_1`：

```
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。

管理SMB伺服器

修改 ONTAP SMB 伺服器

您可以使用將 SMB 伺服器從工作群組移至 Active Directory 網域、從工作群組移至其他工作群組、或從 Active Directory 網域移至工作群組 `vserver cifs modify` 命令。

關於這項工作

您也可以修改SMB伺服器的其他屬性、例如SMB伺服器名稱和管理狀態。如"指令參考資料ONTAP"需詳細`vserver cifs modify`資訊，請參閱。

選擇

- 將SMB伺服器從工作群組移至Active Directory網域：

a. 將 SMB 伺服器的管理狀態設為 down。

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

b. 將SMB伺服器從工作群組移至Active Directory網域： `vsserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`*

```
Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
```

若要為 SMB 伺服器建立 Active Directory 機器帳戶、您必須提供具有足夠權限的 Windows 帳戶名稱和密碼、以便將電腦新增至 `ou=`*`example`* `ou` 中的容器 *`example`*.com 網域。

從ONTAP 功能更新9.7開始、AD管理員可以提供Keytab檔案的URI、作為提供權限Windows帳戶名稱和密碼的替代方案。當您收到 URI 時、請將其加入 `-keytab-uri` 參數 `vserver cifs` 命令。

- 將SMB伺服器從工作群組移至其他工作群組：

a. 將 SMB 伺服器的管理狀態設為 down。

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

b. 修改 SMB 伺服器的工作群組： `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`new_workgroup_name`*

```
Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
```

- 將SMB伺服器從Active Directory網域移至工作群組：

a. 將 SMB 伺服器的管理狀態設為 down。

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

b. 將 SMB 伺服器從 Active Directory 網域移至工作群組： `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`workgroup_name`*

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```

若要進入工作群組模式、系統必須停用所有網域型功能、並自動移除其組態、包括持續可用的共用、陰影複製及AES。不過、網域設定的共用ACL（例如「EXAMPLE.COM\userName"」）無法正常運作、ONTAP 但無法由支援部門移除。命令完成後、請使用外部工具儘快移除這些共用ACL。如果啟用AES、系統可能會要求您提供具有足夠權限的Windows帳戶名稱和密碼、以便在「example.com」網域中停用該帳戶。

- 使用的適當參數修改其他屬性 `vserver cifs modify` 命令。

使用選項自訂**SMB**伺服器

可用的 **ONTAP SMB** 伺服器選項

在考量如何自訂SMB伺服器時、瞭解可用的選項很有用。雖然有些選項適用於SMB伺服器的一般用途、但有幾個選項可用來啟用和設定特定的SMB功能。SMB 伺服器選項由控制 `vserver cifs options modify` 選項。

下列清單指定可在管理權限層級使用的SMB伺服器選項：

- 設定**SMB**工作階段逾時值

  設定此選項可讓您指定SMB工作階段中斷連線之前的閒置時間秒數。閒置工作階段是指使用者在用戶端上沒有開啟任何檔案或目錄的工作階段。預設值為 900 秒。

- 設定預設的**UNIX**使用者

  設定此選項可讓您指定SMB伺服器使用的預設UNIX使用者。自動建立名為「'pcuser'」的預設使用者（UID為65534）、建立名為「'pcuser'」的群組（gid為65534）、並將預設使用者新增至「'pcuser'」群組。ONTAP當您建立SMB伺服器時ONTAP 、支援將「'pcuser'」自動設定為預設UNIX使用者。

- 設定來賓**UNIX**使用者

  設定此選項可讓您指定從不受信任網域登入的使用者所對應的UNIX使用者名稱、如此可讓來自不受信任網域的使用者連線至SMB伺服器。根據預設、此選項並未設定（沒有預設值）；因此、預設值是不允許來自不受信任網域的使用者連線至SMB伺服器。

- *啟用或停用模式位元*的讀取授與執行

  啟用或停用此選項可讓您指定是否允許SMB用戶端以UNIX模式位元執行可執行檔、即使未設定UNIX執行檔位元、也能存取這些位元。此選項預設為停用。

- 啟用或停用從**NFS**用戶端刪除唯讀檔案的功能

  啟用或停用此選項可決定是否允許NFS用戶端刪除具有唯讀屬性集的檔案或資料夾。NTFS刪除語義不允許在設定唯讀屬性時刪除檔案或資料夾。UNIX刪除語義會忽略唯讀位元、改用父目錄權限來判斷是否可以刪除檔案或資料夾。預設設定為 `disabled`，從而產生 NTFS 刪除義。

- 設定**Windows**網際網路名稱服務伺服器位址

  設定此選項可讓您將Windows網際網路名稱服務（WINS）伺服器位址清單指定為以逗號分隔的清單。您必須指定IPV4位址。不支援IPv6位址。沒有預設值。

下列清單指定可在進階權限層級使用的SMB伺服器選項：

- 授予**CIFS**使用者**UNIX**群組權限

  設定此選項可決定是否可以將不是檔案擁有者的傳入CIFS使用者授予群組權限。如果 CIFS 使用者不是 UNIX 安全樣式檔案的擁有者、則此參數會設為 `true`，則會授予該檔案的群組權限。如果 CIFS 使用者不是 UNIX 安全樣式檔案的擁有者、則此參數會設為 `false`，然後，正常的 UNIX 規則適用於授予檔案權限。此參數適用於權限設為的 UNIX 安全性樣式檔案 `mode bits` 且不適用於 NTFS 或 NFSv4 安全模式的檔案。預設設定為 `false`。

- 啟用或停用**SMB 1.0**

  SMB 1.0在SVM上預設為停用、而SVM是在ONTAP SVM上建立SMB伺服器、以供使用。

  > ⓘ 從功能9.3開始ONTAP 、ONTAP 根據預設、針對以功能9.3建立的新SMB伺服器、會停用SMB 1.0。您應該盡快移轉至較新的SMB版本、以準備增強安全性和法規遵循。如需詳細資訊、請聯絡您的NetApp代表。

- *啟用或停用SMB 2.x *

  SMB 2.0是支援LIF容錯移轉的最小SMB版本。如果停用SMB 2.x、ONTAP 則無法使用支援功能的功能也會自動停用SMB 3.x

  SMB 2.0僅在SVM上受支援。此選項在SVM上預設為啟用

- * 啟用或停用 SMB 3.0*

  SMB 3.0是支援持續可用共用的最小SMB版本。Windows Server 2012和Windows 8是支援SMB 3.0的最低Windows版本。

  SMB 3.0 僅支援 SVM 。此選項在SVM上預設為啟用

- * 啟用或停用 SMB 3.1*

  Windows 10是唯一支援SMB 3.1的Windows版本。

  SMB 3.1 僅支援 SVM 。此選項在SVM上預設為啟用

- 啟用或停用**ODX**複本卸載

  支援ODX複本卸載的Windows用戶端會自動使用ODX複本卸載。此選項預設為啟用。

- 啟用或停用**ODX**複本卸載的直接複製機制

  當Windows用戶端嘗試以一種模式開啟複本的來源檔案時、直接複製機制可提高複本卸載作業的效能、避免在複本進行期間變更檔案。根據預設、直接複製機制會啟用。

- 啟用或停用自動節點參照

  使用自動節點參照時、SMB伺服器會自動將用戶端參照到本機資料LIF、並將其指向裝載透過所要求共用區存取資料的節點。

- *啟用或停用SMB*的匯出原則

  此選項預設為停用。

- 啟用或停用使用連接點做為重新分析點

  如果啟用此選項、SMB伺服器會將連接點公開給SMB用戶端做為重新分析點。此選項僅適用於SMB 2.x或SMB 3.0連線。此選項預設為啟用。

  此選項僅在SVM上受支援。此選項在SVM上預設為啟用

- 設定每個**TCP**連線同時執行的最大作業數

  預設值為 255 。

- 啟用或停用本機**Windows**使用者和群組功能

  此選項預設為啟用。

- 啟用或停用本機**Windows**使用者驗證

  此選項預設為啟用。

- 啟用或停用**VSS**陰影複製功能

  利用陰影複製功能、對使用Hyper-V over SMB解決方案儲存的資料執行遠端備份。ONTAP

  此選項僅在SVM上受支援、僅在Hyper-V over SMB組態上受支援。此選項在SVM上預設為啟用

- 設定陰影複製目錄深度

  設定此選項可讓您定義在使用陰影複製功能時建立陰影複製的目錄深度上限。

  此選項僅在SVM上受支援、僅在Hyper-V over SMB組態上受支援。此選項在SVM上預設為啟用

- 啟用或停用名稱對應的多網域搜尋功能

  如果啟用、當UNIX使用者透過在Windows使用者名稱的網域部分（例如*\Joe）中使用萬用字元（*）對應至Windows網域使用者時ONTAP 、將會在所有具有雙向信任的網域中搜尋指定使用者。主網域是包含SMB伺服器電腦帳戶的網域。

  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。如果啟用此選項且已設定偏好的清單、則會使用偏好的清單來執行多網域名稱對應搜尋。

  預設為啟用多網域名稱對應搜尋。

- 設定檔案系統區段大小

  設定此選項可讓您設定以位元組為單位的檔案系統區段大小、ONTAP 以便向SMB用戶端回報。此選項有兩個有效值： `4096` 和 `512`。預設值為 `4096`。您可能需要將此值設為 `512` 如果 Windows 應用程式僅支援 512 位元組的扇區大小。

- 啟用或停用動態存取控制

啟用此選項可讓您使用動態存取控制（DAC）來保護SMB伺服器上的物件、包括使用稽核來登入中央存取原則、以及使用群組原則物件來實作中央存取原則。此選項預設為停用。

此選項僅在SVM上受支援。

- 設定未驗證工作階段的存取限制（限制匿名）

  設定此選項可決定未驗證工作階段的存取限制。這些限制適用於匿名使用者。根據預設、匿名使用者沒有存取限制。

- 在具有**UNIX**有效安全性的磁碟區上啟用或停用**NTFS ACL**的呈現（**UNIX**安全型磁碟區或具有**UNIX**有效安全性的混合式安全型磁碟區）

  啟用或停用此選項可決定如何向SMB用戶端呈現具有UNIX安全性之檔案和資料夾的檔案安全性。如果啟用ONTAP 此功能、則使用NTFS ACL將具有UNIX安全性的磁碟區中的檔案和資料夾、顯示為具有NTFS檔案安全性。如果停用ONTAP 、則在不提供檔案安全性的情況下、將UNIX安全性的磁碟區顯示為FAT磁碟區。根據預設、磁碟區會以NTFS ACL的NTFS檔案安全性呈現。

- 啟用或停用**SMB**假開放功能

  啟用此功能可最佳化ONTAP 當查詢檔案和目錄的屬性資訊時、如何執行開放和關閉要求、進而改善SMB 2.x和SMB 3.0的效能。依預設、SMB假開放功能已啟用。此選項僅適用於使用SMB 2.x或更新版本的連線。

- 啟用或停用**UNIX**擴充功能

  啟用此選項可在SMB伺服器上啟用UNIX擴充功能。UNIX擴充功能可透過SMB傳輸協定顯示POSIX / UNIX類型的安全性。此選項預設為停用。

  如果您的環境中有UNIX型SMB用戶端（例如Mac OSX用戶端）、則應該啟用UNIX擴充功能。啟用UNIX擴充功能可讓SMB伺服器透過SMB將Posix / UNIX安全資訊傳輸到UNIX用戶端、然後將安全資訊轉譯為POSIX / UNIX安全性。

- 啟用或停用對簡短名稱搜尋的支援

  啟用此選項可讓SMB伺服器針對簡短名稱執行搜尋。啟用此選項的搜尋查詢會嘗試比對8.3檔名和長檔名。此參數的預設值為 `false`。

- *啟用或停用對自動通告DFS*功能的支援

  啟用或停用此選項可決定SMB伺服器是否自動向連線至共用的SMB 2.x和SMB 3.0用戶端通告DFS功能。在實作SMB存取的符號連結時、使用DFS轉介。ONTAP如果啟用、則無論是否啟用符號連結存取、SMB伺服器一律會通告DFS功能。如果停用、SMB伺服器只會在用戶端連線至啟用符號連結存取的共用時、才會通告「DFS功能」。

- 設定**SMB**點數上限

  從 ONTAP 9.4 開始、設定 `-max-credits` 選項可讓您在用戶端和伺服器執行 SMB 版本 2 或更新版本時、限制 SMB 連線上要授予的點數數量。預設值為 128 。

- *啟用或停用SMB多通道*支援

  啟用 `-is-multichannel-enabled` ONTAP 9.4 及更新版本中的選項可讓 SMB 伺服器在叢集及其用戶端上部署適當的 NIC 時、為單一 SMB 工作階段建立多個連線。這樣做可改善處理量和容錯能力。此參數的預

設值為 `false`。

啟用SMB多通道時、您也可以指定下列參數：

- 每個多通道工作階段允許的最大連線數。此參數的預設值為 32 。
- 每個多通道工作階段所通告的網路介面數量上限。此參數的預設值為 256 。

設定 ONTAP SMB 伺服器選項

您可以在儲存虛擬機器（SVM）上建立SMB伺服器之後、隨時設定SMB伺服器選項。

步驟

1. 執行所需的動作：

如果您要設定SMB伺服器選項...	輸入命令...
管理員權限等級	`vserver cifs options modify -vserver` *`vserver_name options`*
進階權限層級	a. `set -privilege advanced` b. `vserver cifs options modify -vserver` *`vserver_name options`* c. `set -privilege admin`

如"指令參考資料ONTAP"需瞭解及設定 SMB 伺服器選項的詳細 `vserver cifs options modify`資訊，請參閱。

設定 ONTAP SMB 使用者的「授與 UNIX 群組」權限

即使傳入的SMB使用者不是檔案的擁有者、您也可以設定此選項、以授予群組存取檔案或目錄的權限。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 視需要設定授予UNIX群組權限：

如果您想要	輸入命令
即使使用者不是檔案的擁有者、也能存取檔案或目錄、以取得群組權限	`vserver cifs options modify -grant-unix-group-perms-to-others true`
即使使用者不是檔案的擁有者、也請停用檔案或目錄的存取權、以取得群組權限	`vserver cifs options modify -grant-unix-group-perms-to-others false`

3. 確認選項設定為所需的值： `vserver cifs options show -fields grant-unix-group-perms-to-others`

4. 返回管理權限層級： `set -privilege admin`

為匿名使用者設定 **ONTAP SMB** 存取限制

根據預設、匿名、未驗證的使用者（也稱為_null使用者_）可以存取網路上的特定資訊。您可以使用SMB伺服器選項來設定匿名使用者的存取限制。

關於這項工作

。 `-restrict-anonymous` SMB 伺服器選項對應於 `RestrictAnonymous` Windows 中的登錄項目。

匿名使用者可以從網路上的Windows主機列出或列舉特定類型的系統資訊、包括使用者名稱和詳細資料、帳戶原則和共用名稱。您可以指定下列三種存取限制設定之一來控制匿名使用者的存取：

價值	說明
`no-restriction` （預設）	不指定匿名使用者的存取限制。
`no-enumeration`	指定僅限匿名使用者進行列舉。
`no-access`	指定匿名使用者的存取受到限制。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 設定限制匿名設定： `vserver cifs options modify -vserver vserver_name -restrict -anonymous {no-restriction|no-enumeration|no-access}`
3. 確認選項設定為所需的值： `vserver cifs options show -vserver vserver_name`
4. 返回管理權限層級： `set -privilege admin`

相關資訊

可用的伺服器選項

管理如何向**SMB**用戶端提供**UNIX**安全型資料的檔案安全性

瞭解如何將 **ONTAP** 檔案安全性呈現給 **SMB** 用戶端，以取得 **UNIX** 安全性型資料

您可以啟用或停用將NTFS ACL呈現給SMB用戶端的功能、來選擇如何向SMB用戶端展示UNIX安全型資料的檔案安全性。每項設定都有優點、您應該瞭解如何選擇最適合您業務需求的設定。

根據預設、ONTAP 將UNIX安全型磁碟區上的UNIX權限以NTFS ACL形式呈現給SMB用戶端。有些情況需要這樣做、包括：

- 您想要使用「Windows內容」方塊中的「安全性」索引標籤來檢視及編輯UNIX權限。

  如果UNIX系統不允許此作業、您就無法從Windows用戶端修改權限。例如、您無法變更您不擁有的檔案所有權、因為UNIX系統不允許此作業。此限制可防止SMB用戶端略過在檔案和資料夾上設定的UNIX權限。

- 使用者使用某些Windows應用程式（例如Microsoft Office）來編輯及儲存UNIX安全型磁碟區上的檔案、ONTAP 而在這些應用程式中、當執行儲存作業時、必須保留UNIX權限。
- 您環境中有些Windows應用程式預期會讀取其所使用檔案的NTFS ACL。

在某些情況下、您可能會想要停用將UNIX權限呈現為NTFS ACL的功能。如果停用此功能、ONTAP 則將UNIX安全型磁碟區顯示為SMB用戶端的FAT磁碟區。您可能會想要將UNIX安全型磁碟區以FAT磁碟區的形式呈現給SMB用戶端的具體理由如下：

- 您只能在UNIX用戶端上使用掛載來變更UNIX權限。

  當SMB用戶端上對應UNIX安全型磁碟區時、「安全性」索引標籤將無法使用。對應的磁碟機似乎是以不具檔案權限的檔案系統格式化。

- 您正在使用SMB上的應用程式、在存取的檔案和資料夾上設定NTFS ACL、如果資料位於UNIX安全型磁碟區、則這些應用程式可能會失敗。

  如果ONTAP 將磁碟區報告為「FAT」、應用程式就不會嘗試變更ACL。

相關資訊

- 在FlexVol 功能區上設定安全樣式
- 在qtree上設定安全性樣式

設定 **NTFS ACL** 呈現給 **ONTAP SMB** 用戶端以取得 **UNIX** 安全性型資料

您可以針對UNIX安全型資料（UNIX安全型磁碟區和混合式安全型磁碟區、以及UNIX有效安全性）、啟用或停用將NTFS ACL呈現給SMB用戶端的功能。

關於這項工作

如果啟用此選項、ONTAP 則將具有有效UNIX安全樣式的磁碟區上的檔案和資料夾、呈現給SMB用戶端、如同使用NTFS ACL。如果停用此選項、磁碟區會以FAT磁碟區的形式呈現給SMB用戶端。預設為向SMB用戶端顯示NTFS ACL。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 設定 UNIX NTFS ACL 選項設定： `vserver cifs options modify -vserver vserver_name -is-unix-nt-acl-enabled {true|false}`
3. 確認選項設定為所需的值： `vserver cifs options show -vserver vserver_name`
4. 返回管理權限層級： `set -privilege admin`

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。

管理**SMB**伺服器安全性設定

瞭解如何處理 **ONTAP SMB** 用戶端驗證

使用者必須先由SMB伺服器所屬的網域驗證、才能建立SMB連線來存取SVM上所含的資料。SMB伺服器支援兩種驗證方法：Kerberos和NTLM（位在NTLMv1或NTLMv2之間）。Kerberos是用於驗證網域使用者的預設方法。

Kerberos驗證

建立驗證的SMB工作階段時、支援Kerberos驗證。ONTAP

Kerberos是Active Directory的主要驗證服務。Kerberos伺服器或Kerberos金鑰發佈中心（Kdc）服務會在Active Directory中儲存及擷取安全性原則的相關資訊。與NTLM模式不同的是、Active Directory用戶端若想要與另一部電腦（例如SMB伺服器）建立工作階段、請直接聯絡Kdc以取得其工作階段認證。

NTLM 驗證

以密碼為基礎、根據使用者專屬密碼的共享知識、使用挑戰回應傳輸協定來完成NTLM用戶端驗證。

如果使用者使用本機 Windows 使用者帳戶建立 SMB 連線、則驗證作業會由 SMB 伺服器使用 NTLMv2 在本機完成。

瞭解 **ONTAP SVM** 災難恢復組態的 **SMB** 伺服器安全性設定

建立 SVM 之前、請先將其設定為災難恢復目的地、但不會保留身分識別（ `-identity -preserve` 選項設定為 `false` 在 SnapMirror 組態中）、您應該知道如何在目的地 SVM 上管理 SMB 伺服器安全性設定。

- 非預設的SMB伺服器安全性設定不會複寫到目的地。

  當您在目的地SVM上建立SMB伺服器時、所有SMB伺服器安全性設定都會設為預設值。當SVM災難恢復目的地初始化、更新或重新同步時、來源上的SMB伺服器安全性設定不會複寫到目的地。

- 您必須手動設定非預設的SMB伺服器安全性設定。

  如果您在來源SVM上設定了非預設的SMB伺服器安全性設定、則必須在目的地SVM變成讀寫（SnapMirror關係中斷之後）之後、在目的地上手動設定這些相同的設定。

顯示 **ONTAP SMB** 伺服器安全性設定的相關資訊

您可以在儲存虛擬機器（SVM）上顯示SMB伺服器安全性設定的相關資訊。您可以使用此資訊來驗證安全性設定是否正確。

關於這項工作

顯示的安全性設定可以是該物件的預設值、也可以是透過ONTAP 使用列舉CLI或使用Active Directory群組原則物件（GPO）設定的非預設值。

請勿使用 `vserver cifs security show` 工作群組模式中 SMB 伺服器的命令、因為某些選項無效。

步驟

1. 執行下列其中一項動作：

如果您想要顯示有關...的資訊	輸入命令...
指定SVM上的所有安全性設定	`vserver cifs security show -vserver` *`vserver_name`*
SVM上的特定安全性設定或設定	`vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]` 您可以輸入 `-fields ?` 決定您可以使用哪些欄位。

範例

下列範例顯示SVM VS1的所有安全性設定：

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                          Kerberos Clock Skew:        5 minutes
                          Kerberos Ticket Age:        10 hours
                         Kerberos Renewal Age:        7 days
                         Kerberos KDC Timeout:        3 seconds
                          Is Signing Required:        false
               Is Password Complexity Required:        true
          Use start_tls For AD LDAP connection:        false
                     Is AES Encryption Enabled:        false
                        LM Compatibility Level:        lm-ntlm-ntlmv2-krb
                    Is SMB Encryption Required:        false
                       Client Session Security:        none
              SMB1 Enabled for DC Connections:        false
              SMB2 Enabled for DC Connections:        system-default
LDAP Referral Enabled For AD LDAP connections:        false
             Use LDAPS for AD LDAP connection:        false
    Encryption is required for DC Connections:        false
 AES session key enabled for NetLogon channel:        false
  Try Channel Binding For AD LDAP Connections:        false
```

請注意、顯示的設定取決於執行ONTAP 中的版本。

以下範例顯示SVM VS1的Kerberos時鐘偏移：

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew

            vserver kerberos-clock-skew
            ------- -------------------
            vs1     5
```

相關資訊

顯示有關GPO組態的資訊

為本機 **SMB** 使用者設定 **ONTAP** 密碼複雜度

所需的密碼複雜度可為儲存虛擬機器（SVM）上的本機SMB使用者提供更高的安全性。預設會啟用所需的密碼複雜度功能。您可以隨時停用並重新啟用。

開始之前

必須在CIFS伺服器上啟用本機使用者、本機群組和本機使用者驗證。

關於這項工作

請勿在工作群組模式中使用 `vserver cifs security modify` CIFS 伺服器的命令，因為某些選項無效。

步驟

1. 執行下列其中一項動作：

如果您想讓本機SMB使用者的密碼複雜度達到所需...	輸入命令...
已啟用	`vserver cifs security modify -vserver vserver_name -is-password-complexity -required true`
已停用	`vserver cifs security modify -vserver vserver_name -is-password-complexity -required false`

2. 驗證所需密碼複雜度的安全性設定： `vserver cifs security show -vserver vserver_name`

範例

以下範例顯示、SVM VS1的本機SMB使用者已啟用必要的密碼複雜度：

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
------- -------------------------------
vs1     true
```

相關資訊

- 顯示有關伺服器安全設定的信息
- 了解本地用戶和群組
- 本機使用者密碼需求
- 變更本機使用者帳戶密碼

修改 **ONTAP SMB** 伺服器 **Kerberos** 安全性設定

您可以修改某些CIFS伺服器Kerberos安全性設定、包括允許的Kerberos時鐘偏移時間上限、Kerberos票證壽命、以及票證續約天數上限。

關於這項工作

使用修改 CIFS 伺服器 Kerberos 設定 `vserver cifs security modify` 命令只會修改您使用指定的單一儲存虛擬機器（ SVM ）上的設定 `-vserver` 參數。您可以使用Active Directory群組原則物件（GPO）、集中管理屬於同一個Active Directory網域之叢集上所有SVM的Kerberos安全性設定。

步驟

1. 執行下列一或多項動作：

如果您想要…	輸入…
指定允許的 Kerberos 時鐘偏差時間上限（以分鐘為單位（ 9.13.1 及更新版本）或秒（ 9.12.1 或更新版本）。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-clock-skew` *`integer_in_minutes`* 預設設定為5分鐘。
以小時為單位指定Kerberos票證壽命。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-ticket-age integer_in_hours` 預設設定為10小時。
指定通知單續約天數上限。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-renew-age` *`integer_in_days`* 預設設定為7天。
指定KDC上的通訊端逾時、之後所有KDC都會標示為無法連線。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-kdc-timeout` *`integer_in_seconds`* 預設設定為3秒。

2. 驗證Kerberos安全性設定：

   `vserver cifs security show -vserver` *`vserver_name`*

範例

下列範例對Kerberos安全性進行下列變更：「Kerberos時鐘偏移」設為3分鐘、而SVM VS1的「Kerberos票證時間」設為8小時：

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                    Kerberos Clock Skew:                    3 minutes
                    Kerberos Ticket Age:                    8 hours
                  Kerberos Renewal Age:                     7 days
                  Kerberos KDC Timeout:                     3 seconds
                    Is Signing Required:                false
        Is Password Complexity Required:                 true
   Use start_tls For AD LDAP connection:                false
              Is AES Encryption Enabled:                false
                 LM Compatibility Level:  lm-ntlm-ntlmv2-krb
             Is SMB Encryption Required:                false
```

相關資訊

"顯示有關伺服器安全設定的信息"

"支援的GPO"

"將群組原則物件套用至CIFS伺服器"

設定 **ONTAP SMB** 伺服器的最低驗證安全層級

您可以在SMB伺服器上設定SMB伺服器的最低安全性層級（也稱為_LMCompatibilityLevel）、以符合SMB用戶端存取的企業安全性需求。最低安全層級是SMB伺服器從SMB用戶端接受的安全性權杖最低層級。

關於這項工作

- 工作群組模式中的SMB伺服器僅支援NTLM驗證。不支援Kerberos驗證。
- LMCompatibilityLevel僅適用於SMB用戶端驗證、不適用於管理驗證。

您可以將最低驗證安全性層級設為四種支援的安全性層級之一。

價值	說明
`lm-ntlm-ntlmv2-krb` （預設）	儲存虛擬機器（SVM）接受LM、NTLM、NTLMv2及Kerberos驗證安全性。
`ntlm-ntlmv2-krb`	SVM接受NTLM、NTLMv2及Kerberos驗證安全性。SVM拒絕LM驗證。

價值	說明
`ntlmv2-krb`	SVM接受NTLMv2和Kerberos驗證安全性。SVM拒絕LM和NTLM驗證。
`krb`	SVM僅接受Kerberos驗證安全性。SVM會拒絕LM、NTLM及NTLMv2驗證。

步驟

1. 設定最低驗證安全層級： `vserver cifs security modify -vserver vserver_name -lm -compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. 驗證驗證安全性層級是否設為所需層級： `vserver cifs security show -vserver vserver_name`

相關資訊

為基於 Kerberos 的通訊配置 AES 加密

使用 **AES** 加密，為 **Kerberos** 型通訊設定強大的 **ONTAP SMB** 安全性

為了以Kerberos為基礎的通訊提供最強大的安全性、您可以在SMB伺服器上啟用AES-256和AES-128加密。根據預設、當您在SVM上建立SMB伺服器時、會停用進階加密標準（AES）加密。您必須讓IT能夠充分利用AES加密所提供的強大安全性。

SMB的Kerberos相關通訊是在SVM上建立SMB伺服器期間、以及SMB工作階段設定階段期間使用。SMB伺服器支援下列Kerberos通訊加密類型：

- AES 256
- AES 128
- 第
- RC4-HMAC

如果您想要使用最高的安全性加密類型進行Kerberos通訊、您應該在SVM上啟用AES加密來進行Kerberos通訊。

建立SMB伺服器時、網域控制器會在Active Directory中建立電腦帳戶。此時、Kdc會得知特定機器帳戶的加密功能。之後、會選取特定的加密類型來加密用戶端在驗證期間向伺服器顯示的服務票證。

從ONTAP 《支援資料》9.12.1開始、您可以指定要向Active Directory（AD）kdc通告的加密類型。您可以使用`-advertised-enc-types`選項來啟用建議的加密類型，也可以使用它來停用較弱的加密類型。瞭解如何"為基於 Kerberos 的通訊配置 AES 加密"。

SMB 3.0提供Intel AES新指令（Intel AES NI）、可改善AES演算法、並以支援的處理器系列產品加速資料加密。從SMB 3.3.1開始、AES-120-GCM取代AES-120-CCMs做為SMB加密所使用的雜湊演算法。

相關資訊

修改伺服器安全設定

為 **ONTAP SMB Kerberos** 型通訊設定 **AES** 加密

若要利用以 Kerberos 為基礎的通訊所提供的最強大安全性、您應該在 SMB 伺服器上使用 AES-256 和 AES-128 加密。從 ONTAP 9.13.1 開始、預設會啟用 AES 加密。 如果您不希望SMB伺服器選取AES加密類型、以便與Active Directory（AD）kdc進行Kerberos型通訊、您可以停用AES加密。

是否預設啟用 AES 加密、以及您是否可以選擇指定加密類型、取決於您的 ONTAP 版本。

版本**ONTAP**	**AES** 加密已啟用 **...**	您可以指定加密類型嗎？
9.13.1 及更新版本	依預設	是的
9.12.1	手動	是的
9.11.1 及更早版本	手動	否

從ONTAP 功能支援的9.12.1開始、AES加密會使用啟用和停用 `-advertised-enc-types` 選項、可讓您指定通告給AD Kdc的加密類型。預設設定為 `rc4` 和 `des`，但當指定AES類型時，將會啟用AES加密。您也可以使用選項來明確停用較弱的RC4和DES加密類型。在 ONTAP 9.11.1 及更早版本中、您必須使用 `-is-aes-encryption-enabled` 啟用和停用AES加密的選項、無法指定加密類型。

為了增強安全性、儲存虛擬機器（SVM）會在每次修改AES安全性選項時、變更AD中的機器帳戶密碼。變更密碼可能需要包含機器帳戶的組織單位（OU）的系統管理AD認證。

如果 SVM 設定為災難恢復目的地、而該目的地不會保留身分識別（ `-identity-preserve` 選項設定為 `false` 在 SnapMirror 組態中）、非預設 SMB 伺服器安全性設定不會複寫到目的地。如果您已在來源 SVM 上啟用 AES 加密、則必須手動啟用。

範例 **1.** 步驟

更新版本**ONTAP**

1. 執行下列其中一項動作：

如果您希望**Kerberos**通訊的**AES**加密類型…	輸入命令…
已啟用	`vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256`
已停用	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

附註： The `-is-aes-encryption-enabled` 選項在ONTAP 更新版本中已過時、可能會在更新版本中移除。

2. 確認已視需要啟用或停用AES加密： `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

範例

以下範例可為 SVM VS1 上的 SMB 伺服器啟用 AES 加密類型：

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs1      aes-128,aes-256
```

下列範例可為SVM VS2上的SMB伺服器啟用AES加密類型。系統會提示系統管理員輸入包含SMB伺服器之OU的管理AD認證。

```
cluster1::> vserver cifs security modify -vserver vs2 -advertised-enc
-types aes-128,aes-256

Info: In order to enable SMB AES encryption, the password for the SMB
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs2      aes-128,aes-256
```

更新版本**ONTAP**

1. 執行下列其中一項動作：

如果您希望**Kerberos**通訊的**AES**加密類型...	輸入命令...
已啟用	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled true`
已停用	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false`

2. 確認已視需要啟用或停用AES加密： `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

   ◦ `is-aes-encryption-enabled` 欄位隨即顯示 `true` 如果已啟用 AES 加密、且 `false` 如果已停用。

範例

以下範例可為 SVM VS1 上的 SMB 伺服器啟用 AES 加密類型：

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs1      true
```

下列範例可為SVM VS2上的SMB伺服器啟用AES加密類型。系統會提示系統管理員輸入包含SMB伺服器之OU的管理AD認證。

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs2      true
```

相關資訊

"網域使用者無法使用網域通道登入叢集"

使用SMB簽署來強化網路安全性

瞭解如何使用 ONTAP SMB 簽署來增強網路安全性

SMB簽章有助於確保SMB伺服器與用戶端之間的網路流量不會受到影響、並可防止重播攻擊。根據預設ONTAP 、若用戶端要求、支援SMB簽署。或者、儲存管理員可以將SMB伺服器設定為需要SMB簽署。

除了CIFS伺服器SMB簽署安全性設定之外、Windows用戶端上的兩個SMB簽署原則也會控制用戶端與CIFS伺服器之間的通訊數位簽署。您可以設定符合業務需求的設定。

用戶端SMB原則是透過Windows本機安全性原則設定來控制、這些設定是使用Microsoft管理主控台（MMC）或Active Directory GPO來設定。如需用戶端SMB簽署與安全性問題的詳細資訊、請參閱Microsoft Windows文件。

以下是Microsoft用戶端上兩種SMB簽署原則的說明：

- `Microsoft network client: Digitally sign communications (if server agrees)`

  此設定可控制是否啟用用戶端的SMB簽署功能。預設為啟用。當用戶端停用此設定時、與CIFS伺服器的用戶端通訊取決於CIFS伺服器上的SMB簽署設定。

- `Microsoft network client: Digitally sign communications (always)`

  此設定可控制用戶端是否需要SMB簽署才能與伺服器通訊。預設為停用。當用戶端上停用此設定時、 SMB簽署行為會根據的原則設定而定 `Microsoft network client: Digitally sign communications (if server agrees)` 以及 CIFS 伺服器上的設定。

> ⓘ 如果您的環境包含設定為需要SMB簽署的Windows用戶端、則必須在CIFS伺服器上啟用SMB簽署。如果您沒有、CIFS伺服器就無法將資料提供給這些系統。

用戶端和CIFS伺服器SMB簽署設定的有效結果取決於SMB工作階段是使用SMB 1.0或SMB 2.x或更新版本。

下表摘要說明當工作階段使用SMB 1.0時的有效SMB簽署行為：

用戶端	**ONTAP** -不需要簽署	**ONTAP** -需要簽署
簽署已停用且不需要	未簽署	已簽署
簽署已啟用且不需要	未簽署	已簽署
簽署已停用且必要	已簽署	已簽署
簽署已啟用且必要	已簽署	已簽署

> ⓘ 舊版Windows SMB 1用戶端和部分非Windows SMB 1用戶端若在用戶端上停用簽署、但CIFS伺服器上需要簽署、則可能無法連線。

下表摘要說明當工作階段使用SMB 2.x或SMB 3.0時的有效SMB簽署行為：

> ⓘ 對於SMB 2.x和SMB 3.0用戶端、一律會啟用SMB簽署。無法停用。

用戶端	**ONTAP** -不需要簽署	**ONTAP** -需要簽署
不需要簽署	未簽署	已簽署
需要簽署	已簽署	已簽署

下表摘要說明預設的Microsoft用戶端和伺服器SMB簽署行為：

傳輸協定	雜湊演算法	可啟用/停用	可能需要/不需要	用戶端預設值	伺服器預設值	**DC**預設值
SMB 1.0	md5	是的	是的	已啟用（非必要）	已停用（非必要）	必要
SMB 2.x	HMAC SHA-256	否	是的	不需要	不需要	必要
SMB 3.0	AES-CMAC：	否	是的	不需要	不需要	必要

Microsoft 不再建議使用 `Digitally sign communications (if client agrees)` 或 `Digitally sign communications (if server agrees)` 群組原則設定。Microsoft 也不再建議使用 `EnableSecuritySignature` 登錄設定。這些選項只會影響 SMB 1 行為、可由取代 `Digitally sign communications (always)` 群組原則設定或 `RequireSecuritySignature` 登錄設定。您也可以從 Microsoft 部落格取得更多資訊。 The SMB 簽署基礎知識（涵蓋 SMB1 和 SMB2 ）

瞭解 **ONTAP SMB** 簽署對效能的影響

當SMB工作階段使用SMB簽署時、所有往返Windows用戶端的SMB通訊都會受到效能影響、這會影響用戶端和伺服器（亦即、叢集上執行SVM的節點包含SMB伺服器）。

效能影響顯示用戶端和伺服器的CPU使用量增加、不過網路流量並未改變。

效能影響的程度取決於ONTAP 您所執行的版本的VMware®。從推出全新的加密卸載演算法、即可在ONTAP 簽署的SMB流量中提供更好的效能。啟用SMB簽署時、預設會啟用SMB簽署卸載。

增強的SMB簽署效能需要AES-NI卸載功能。請參閱Hardware Universe 《支援資料》（HWU）、確認您的平台是否支援AES-NI卸載。

如果您能夠使用支援速度更快的 GCM 演算法的 SMB 版本 3.11 、也可以進一步改善效能。

視您的網路ONTAP 、支援的版本為VMware、SMB版本及SVM實作而定、SMB簽署的效能影響可能會有很大差異；您只能在網路環境中進行測試來驗證。

如果伺服器上已啟用SMB簽署、則大部分的Windows用戶端會依預設協調SMB簽署。如果您的部分Windows用戶端需要SMB保護、而且SMB簽章造成效能問題、您可以在任何不需要保護以防止重播攻擊的Windows用戶端上停用SMB簽署。如需在Windows用戶端上停用SMB簽署的相關資訊、請參閱Microsoft Windows文件。

ONTAP SMB 簽署組態建議

您可以設定SMB用戶端與CIFS伺服器之間的SMB簽署行為、以符合您的安全需求。您在CIFS伺服器上設定SMB簽署時所選擇的設定、取決於您的安全需求。

您可以在用戶端或CIFS伺服器上設定SMB簽署。設定SMB簽署時、請考慮下列建議：

如果...	建議...
您想要提高用戶端與伺服器之間通訊的安全性	啟用、讓用戶端需要 SMB 簽署 `Require Option (Sign always)` 用戶端上的安全性設定。
您希望所有SMB流量都簽署到特定的儲存虛擬機器（SVM）	設定安全性設定以要求SMB簽署、使CIFS伺服器上的SMB簽署成為必要項目。

如需設定Windows用戶端安全性設定的詳細資訊、請參閱Microsoft文件。

瞭解多重資料生命的 ONTAP SMB 簽署組態

如果您在SMB伺服器上啟用或停用必要的SMB簽署、您應該瞭解SVM多重資料生命量組態的準則。

設定SMB伺服器時、可能會設定多個資料生命量。如果是、則 DNS 伺服器包含多個 `A` 記錄 CIFS 伺服器的項目、所有項目都使用相同的 SMB 伺服器主機名稱、但每個項目都有唯一的 IP 位址。例如、已設定兩個資料生命期的 SMB 伺服器可能具有下列 DNS `A` 記錄項目：

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

正常情況是、變更必要的SMB簽署設定後、只有來自用戶端的新連線會受到SMB簽署設定的變更影響。不過、這種行為有例外。在某種情況下、用戶端與共用有現有的連線、而用戶端會在變更設定之後、建立新的連線至同一個共用區、同時維持原始連線。在這種情況下、新的和現有的SMB連線都會採用新的SMB簽署要求。

請考慮下列範例：

1. Client1 連接到共享區、而不需要使用路徑簽署 SMB `O:\`。
2. 儲存管理員會修改SMB伺服器組態、以要求SMB簽署。
3. Client1 會使用路徑連線到具有必要 SMB 簽署的同一個共用區 `S:\` （同時使用路徑維持連線 `O:\`）。
4. 結果是在存取兩者的資料時、會使用 SMB 簽署 `O:\` 和 `S:\` 磁碟機。

為傳入的 SMB 流量設定 ONTAP 簽署

您可以啟用必要的SMB簽署、強制要求用戶端簽署SMB訊息。如果啟用ONTAP 、僅當SMB訊息具有有效的簽名時、才會接受該訊息。如果您想要允許SMB簽署、但不需要SMB簽署、可以停用必要的SMB簽署。

關於這項工作

預設會停用必要的SMB簽署。您可以隨時啟用或停用所需的SMB簽署。

在下列情況下、預設不會停用SMB簽署：

1. 啟用必要的SMB簽署、叢集將還原為ONTAP 不支援SMB簽署的版本。
2. 叢集隨後會升級至ONTAP 支援SMB簽署的版本的支援。

   在這種情況下、原本設定在支援版本ONTAP 的支援版本上的SMB簽署組態會透過還原及後續升級來保留。

當您設定儲存虛擬機器（ SVM ）災難恢復關係時、您為選取的值 `-identity-preserve` 的選項 `snapmirror create` 命令可決定在目的地 SVM 中複寫的組態詳細資料。

如果您設定 `-identity-preserve` 選項 `true` （ ID-preserve ）、 SMB 簽署安全性設定會複寫到目的地。

如果您設定 `-identity-preserve` 選項 `false` （非 ID-preserve ）、 SMB 簽署安全性設定不會複寫到目的地。在此情況下、目的地上的CIFS伺服器安全性設定會設為預設值。如果您已在來源SVM上啟用必要的SMB簽署、則必須在目的地SVM上手動啟用必要的SMB簽署。

步驟

1. 執行下列其中一項動作：

如果您想要**SMB**簽署...	輸入命令...
已啟用	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required true`
已停用	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required false`

2. 判斷中的值是否已啟用或停用必要的 SMB 簽署 `Is Signing Required` 下列命令輸出中的欄位設定為所需的值： `vserver cifs security show -vserver` *`vserver_name`* `-fields is-signing-required`

範例

下列範例可為SVM VS1啟用必要的SMB簽署：

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required
true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
required
vserver  is-signing-required
-------- --------------------
vs1      true
```

對加密設定的變更會對新連線生效。現有連線不受影響。

相關資訊

- "SnapMirror建立"

判斷 **ONTAP SMB** 工作階段是否已簽署

您可以在CIFS伺服器上顯示連線SMB工作階段的相關資訊。您可以使用此資訊來判斷SMB工作階段是否已簽署。這有助於判斷SMB用戶端工作階段是否與所需的安全性設定連線。

步驟

1. 執行下列其中一項動作：

如果您想要顯示有關...的資訊	輸入命令...
指定儲存虛擬機器（SVM）上的所有簽署工作階段	`vserver cifs session show -vserver vserver_name -is-session-signed true`
在SVM上具有特定工作階段ID的已簽署工作階段詳細資料	`vserver cifs session show -vserver vserver_name -session-id integer -instance`

範例

下列命令會顯示SVM VS1上已簽署工作階段的相關工作階段資訊。預設的摘要輸出不會顯示「Is Session Signed」（已簽署的工作階段）輸出欄位：

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:    node1
Vserver: vs1
Connection Session                                      Open          Idle
ID         ID      Workstation      Windows User     Files         Time
---------- ------- ---------------- ------------- ------- ------------
3151272279 1       10.1.1.1         DOMAIN\joe           2          23s
```

下列命令會在工作階段ID為2的SMB工作階段上顯示詳細的工作階段資訊、包括工作階段是否已簽署：

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

相關資訊

監控SMB簽署的工作階段統計資料

監控 **ONTAP SMB** 簽署的工作階段統計資料

您可以監控SMB工作階段統計資料、並判斷哪些已建立的工作階段已簽署、哪些尚未簽署。

關於這項工作

。 `statistics` 進階權限層級的命令提供 `signed_sessions` 可用來監控已簽署 SMB 工作階段數量的計數器。。 `signed_sessions` 下列統計資料物件可使用計數器：

- `cifs` 可讓您監控所有 SMB 工作階段的 SMB 簽署。
- `smb1` 可讓您監控 SMB 1.0 工作階段的 SMB 簽署。
- `smb2` 可讓您監控 SMB 2.x 和 SMB 3.0 工作階段的 SMB 簽署。

  的輸出中包含 SMB 3.0 統計資料 `smb2` 物件：

如果您想要比較已簽署工作階段的數目與工作階段總數、您可以比較的輸出 `signed_sessions` 以的輸出進行計數 `established_sessions` 計數器。

您必須先開始收集統計資料樣本、才能檢視結果資料。如果不停止資料收集、您可以檢視範例中的資料。停止資料收集可提供固定的範例。不停止資料收集可讓您取得更新的資料、以便與先前的查詢進行比較。這項比較可協

助您識別趨勢。

步驟

1. 將權限等級設為進階：
   `set -privilege advanced`
2. 開始資料收集：+ `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]`

   如果您未指定 `-sample-id` 參數、命令會為您產生範例識別碼、並將此範例定義為 CLI 工作階段的預設範例。的價值 `-sample-id` 為文字字串。如果您在相同的CLI工作階段中執行此命令、但未指定 `-sample-id` 參數時、命令會覆寫先前的預設範例。

   您可以選擇性地指定要收集統計資料的節點。如果您未指定節點、範例會收集叢集中所有節點的統計資料。

   如"指令參考資料ONTAP"需詳細 `statistics start`資訊，請參閱。
3. 使用 `statistics stop` 停止收集樣本資料的命令。

   詳細了解 `statistics stop`在"指令參考資料ONTAP" 。
4. 檢視SMB簽署統計資料：

如果您要檢視下列項目的資訊...	輸入...
已簽署的工作階段	`show -sample-id sample_ID -counter signed_sessions
node_name [-node *node_name*]`	已簽署的工作階段和已建立的工作階段
`show -sample-id *sample_ID* -counter signed_sessions	established_sessions

   如果您只想顯示單一節點的資訊、請指定選用項目 `-node` 參數。

   如"指令參考資料ONTAP"需詳細 `statistics show`資訊，請參閱。
5. 返回管理權限層級：
   `set -privilege admin`

範例

以下範例說明如何監控儲存虛擬機器（SVM）VS1上的SMB 2.x和SMB 3.0簽署統計資料。

下列命令會移至進階權限層級：

```
cluster1::> set -privilege advanced

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

下列命令會啟動新範例的資料收集：

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

下列命令會停止範例的資料收集：

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

下列命令會顯示已簽署的SMB工作階段、以及範例中各節點所建立的SMB工作階段：

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|established_sessions|node_name

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- ------------------------
    established_sessions                                            0
    node_name                                                   node1
    signed_sessions                                                 0
    established_sessions                                            1
    node_name                                                   node2
    signed_sessions                                                 1
    established_sessions                                            0
    node_name                                                   node3
    signed_sessions                                                 0
    established_sessions                                            0
    node_name                                                   node4
    signed_sessions                                                 0
```

以下命令顯示節點2的簽署SMB工作階段：

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|node_name -node node2

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- ------------------------
    node_name                                                   node2
    signed_sessions                                                 1
```

下列命令會移回管理權限層級：

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

相關資訊

- 判斷SMB工作階段是否已簽署
- "效能監控與管理總覽"

在**SMB**伺服器上設定必要的**SMB**加密、以便透過**SMB**傳輸資料

瞭解 **ONTAP SMB** 加密

SMB加密可在SMB伺服器上啟用或停用SMB資料傳輸功能、是一項安全性增強功能。您也可以透過共用內容設定、逐一設定所需的SMB加密設定。

根據預設、當您在儲存虛擬機器（ SVM ）上建立 SMB 伺服器時、 SMB 加密會停用。您必須讓IT能夠充分利用SMB加密所提供的增強安全性。

若要建立加密的SMB工作階段、SMB用戶端必須支援SMB加密。從Windows Server 2012和Windows 8開始的Windows用戶端支援SMB加密。

SVM上的SMB加密可透過兩種設定加以控制：

- SMB 伺服器安全選項、可在 SVM 上啟用功能
- SMB 共用屬性，可依每個共用區設定 SMB 加密設定

您可以決定是否需要加密才能存取SVM上的所有資料、或是需要SMB加密才能存取所選共用區中的資料。SVM層級的設定會取代共用層級的設定。

有效的SMB加密組態取決於兩項設定的組合、如下表所述：

啟用**SMB**伺服器**SMB**加密	共用加密資料設定已啟用	伺服器端加密行為
是的	錯	SVM中的所有共用都啟用伺服器層級加密。有了這項組態、整個SMB工作階段就會進行加密。
是的	是的	無論共用層級加密為何、SVM中的所有共用都會啟用伺服器層級加密。有了這項組態、整個SMB工作階段就會進行加密。
錯	是的	特定共用區已啟用共用層級加密。使用此組態、即可從樹狀結構連線進行加密。
錯	錯	未啟用加密。

不支援加密的 SMB 用戶端無法連線至需要加密的 SMB 伺服器或共用區。

對加密設定的變更會對新連線生效。現有連線不受影響。

瞭解 **ONTAP SMB** 加密對效能的影響

當SMB工作階段使用SMB加密時、所有往返Windows用戶端的SMB通訊都會受到效能影響、影響用戶端和伺服器（亦即叢集上執行SVM的節點、其中包含SMB伺服器）。

效能影響顯示用戶端和伺服器的CPU使用量增加、不過網路流量並未改變。

效能影響的程度取決於ONTAP 您所執行的版本的VMware®。從推出全新的加密卸載演算法、即可在ONTAP 加密的SMB流量中提供更好的效能。啟用SMB加密時、預設會啟用SMB加密卸載。

增強的SMB加密效能需要AES-NI卸載功能。請參閱Hardware Universe 《支援資料》（HWU）、確認您的平台是否支援AES-NI卸載。

如果您能夠使用支援速度更快的 GCM 演算法的 SMB 版本 3.11 、也可以進一步改善效能。

視您的網路ONTAP 、支援的版本為VMware、SMB版本及SVM實作而定、SMB加密的效能影響可能會有很大差異、您只能在網路環境中進行測試來驗證。

SMB加密在SMB伺服器上預設為停用。您只能在需要加密的SMB共用區或SMB伺服器上啟用SMB加密。藉由SMB加密、ONTAP 支援進一步處理解密要求、並加密每個要求的回應。因此、只有在必要時才應啟用SMB加密。

啟用或停用傳入流量的 **ONTAP SMB** 加密

如果您想為傳入的SMB流量要求SMB加密、可以在CIFS伺服器或共用層級啟用SMB加密。根據預設、不需要SMB加密。

關於這項工作

您可以在CIFS伺服器上啟用SMB加密、此功能適用於CIFS伺服器上的所有共用。如果您不希望CIFS伺服器上的所有共用都需要SMB加密、或是想要針對每個共用區的傳入SMB流量啟用必要的SMB加密、可以停用CIFS伺服器上所需的SMB加密。

當您設定儲存虛擬機器（ SVM ）災難恢復關係時、您為選取的值 `-identity-preserve` 的選項 `snapmirror create` 命令可決定在目的地 SVM 中複寫的組態詳細資料。

如果您設定 `-identity-preserve` 選項 `true` （ ID-preserve ）、 SMB 加密安全性設定會複寫到目的地。

如果您設定 `-identity-preserve` 選項 `false` （非 ID-preserve ）、 SMB 加密安全性設定不會複寫到目的地。在此情況下、目的地上的CIFS伺服器安全性設定會設為預設值。如果您已在來源SVM上啟用SMB加密、則必須在目的地上手動啟用CIFS伺服器SMB加密。

步驟

1. 執行下列其中一項動作：

如果您想要**CIFS**伺服器上傳入**SMB**流量的**SMB**加密功能**...**	輸入命令**...**
已啟用	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required true`

如果您想要**CIFS**伺服器上傳入**SMB**流量的**SMB**加密功能...	輸入命令...
已停用	`vserver cifs security modify -vserver vserver_name -is-smb-encryption -required false`

2. 確認 CIFS 伺服器上所需的 SMB 加密已視需要啟用或停用： `vserver cifs security show -vserver vserver_name -fields is-smb-encryption-required`

   。 `is-smb-encryption-required` 欄位隨即顯示 `true` 如果需要、會在 CIFS 伺服器和上啟用 SMB 加密 `false` 如果已停用。

範例

下列範例為SVM VS1上的CIFS伺服器啟用必要的SMB加密功能：

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- --------------------------
vs1      true
```

相關資訊

- "SnapMirror建立"

判斷用戶端是否使用加密的 **ONTAP SMB** 工作階段連線

您可以顯示連線SMB工作階段的相關資訊、以判斷用戶端是否使用加密的SMB連線。這有助於判斷SMB用戶端工作階段是否與所需的安全性設定連線。

關於這項工作

SMB用戶端工作階段可以有三種加密層級之一：

- `unencrypted`

  SMB工作階段未加密。未設定儲存虛擬機器（SVM）層級或共用層級的加密。

- `partially-encrypted`

  當樹狀結構連線發生時、會啟動加密。已設定共用層級加密。未啟用SVM層級的加密。

- `encrypted`

  SMB工作階段已完全加密。已啟用SVM層級的加密。共用層級加密可能已啟用、也可能未啟用。SVM層級

的加密設定會取代共用層級的加密設定。

步驟

1. 執行下列其中一項動作：

如果您想要顯示有關...的資訊	輸入命令...
針對指定SVM上的工作階段、具有指定加密設定的工作階段	`vserver cifs session show -vserver *vserver_name* {unencrypted
partially-encrypted	encrypted} -instance`
指定SVM上特定工作階段ID的加密設定	`vserver cifs session show -vserver *vserver_name* -session-id *integer* -instance`

範例

下列命令會在工作階段ID為2的SMB工作階段上顯示詳細的工作階段資訊、包括加密設定：

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                          Node: node1
                       Vserver: vs1
                    Session ID: 2
                 Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                   Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

監控 **ONTAP SMB** 加密統計資料

您可以監控SMB加密統計資料、並判斷哪些已建立的工作階段和共用連線已加密、哪些尚未加密。

關於這項工作

。 `statistics` 進階權限層級的命令會提供下列計數器、您可以使用這些計數器來監控加密的 SMB 工作階段數目及共用連線：

計數器名稱	說明
`encrypted_sessions`	提供加密的SMB 3.0工作階段數量
`encrypted_share_connections`	提供樹狀結構連線所在的加密共用數
`rejected_unencrypted_sessions`	提供因缺乏用戶端加密功能而遭拒的工作階段設定數
`rejected_unencrypted_shares`	提供因缺乏用戶端加密功能而遭拒的共用對應數目

這些計數器可與下列統計資料物件一起使用：

- `cifs` 可讓您監控所有 SMB 3.0 工作階段的 SMB 加密。

  的輸出中包含 SMB 3.0 統計資料 `cifs` 物件： 如果您想要比較加密工作階段的數目與工作階段總數、可以比較的輸出 `encrypted_sessions` 以的輸出進行計數 `established_sessions` 計數器。

  如果您要比較加密共用連線的數目與共用連線的總數、可以比較的輸出 `encrypted_share_connections` 以的輸出進行計數 `connected_shares` 計數器。

- `rejected_unencrypted_sessions` 提供嘗試建立 SMB 工作階段的次數、該工作階段需要從不支援 SMB 加密的用戶端進行加密。
- `rejected_unencrypted_shares` 提供嘗試連線至 SMB 共用的次數、該共用需要來自不支援 SMB 加密的用戶端進行加密。

您必須先開始收集統計資料樣本、才能檢視結果資料。如果不停止資料收集、您可以檢視範例中的資料。停止資料收集可提供固定的範例。不停止資料收集可讓您取得更新的資料、以便與先前的查詢進行比較。這項比較可協助您識別趨勢。

步驟

1. 將權限等級設為進階：
   `set -privilege advanced`
2. 開始資料收集：+ `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   如果您未指定 `-sample-id` 參數、命令會為您產生範例識別碼、並將此範例定義為 CLI 工作階段的預設範例。的價值 `-sample-id` 為文字字串。如果您在相同的CLI工作階段中執行此命令、但未指定 `-sample-id` 參數時、命令會覆寫先前的預設範例。

   您可以選擇性地指定要收集統計資料的節點。如果您未指定節點、範例會收集叢集中所有節點的統計資料。

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

3. 使用 `statistics stop` 停止收集樣本資料的命令。

詳細了解 `statistics stop`在"指令參考資料ONTAP" 。

4. 檢視SMB加密統計資料：

如果您要檢視下列項目的資訊...	輸入...
加密工作階段	`show -sample-id *sample_ID* -counter encrypted_sessions
node_name [-node *node_name*]`	加密的工作階段和已建立的工作階段
`show -sample-id *sample_ID* -counter encrypted_sessions	established_sessions
node_name [-node *node_name*]`	加密的共用連線
`show -sample-id *sample_ID* -counter encrypted_share_connections	*node_name* [-node *node_name*]`
加密的共用連線和連線共用	`show -sample-id *sample_ID* -counter encrypted_share_connections
connected_shares	*node_name* [-node *node_name*]`
拒絕未加密的工作階段	`show -sample-id *sample_ID* -counter rejected_unencrypted_sessions
node_name [-node *node_name*]`	拒絕未加密的共用連線
`show -sample-id *sample_ID* -counter rejected_unencrypted_share	*node_name* [-node *node_name*]`

如果您只想顯示單一節點的資訊、請指定選用項目 `-node` 參數。

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

5. 返回管理權限層級：
`set -privilege admin`

範例

以下範例說明如何監控儲存虛擬機器（SVM）VS1上的SMB 3.0加密統計資料。

下列命令會移至進階權限層級：

```
cluster1::> set -privilege advanced

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

下列命令會啟動新範例的資料收集：

```
cluster1::*> statistics start -object cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

下列命令會停止該範例的資料收集：

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

下列命令顯示節點從範例中所建立的加密SMB工作階段和已建立的SMB工作階段：

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2

    Counter                                 Value
    ----------------------------  ----------------------
    established_sessions                       1
    encrypted_sessions                         1

2 entries were displayed
```

下列命令顯示節點從範例中拒絕的未加密SMB工作階段數目：

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2

    Counter                                     Value
    --------------------------------    ----------------------
    rejected_unencrypted_sessions                 1

1 entry was displayed.
```

下列命令顯示範例中節點所連線的SMB共用數和加密的SMB共用數：

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

    Counter                                     Value
    --------------------------------    ----------------------
    connected_shares                              2
    encrypted_share_connections                   1

2 entries were displayed.
```

下列命令顯示節點從範例中拒絕的未加密SMB共用連線數目：

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

    Counter                                     Value
    --------------------------------    ----------------------
    rejected_unencrypted_shares                   1

1 entry was displayed.
```

相關資訊

- 確定伺服器上可用的統計資料、物件和計數器
- "效能監控與管理總覽"

安全的**LDAP**工作階段通訊

瞭解 **ONTAP SMB LDAP** 簽署與封裝

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CIFS伺服器安全性設定、以對應於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`。

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

在 **ONTAP SMB** 伺服器上啟用 **LDAP** 簽署和密封

CIFS伺服器必須先修改CIFS伺服器安全性設定、才能使用簽署和密封功能與Active Directory LDAP伺服器進行安全通訊。

開始之前

您必須洽詢AD伺服器管理員、以判斷適當的安全性組態值。

步驟

1. 設定 CIFS 伺服器安全性設定、以啟用 Active Directory LDAP 伺服器的簽署和密封流量： `vserver cifs security modify -vserver` *`vserver_name`* `-session-security-for-ad-ldap`

`{none|sign|seal}`

您可以啟用簽署 (`sign`、資料完整性）、簽署及密封 (`seal`**或兩者皆非** `none`、無簽署或密封）。預設值為 `none`。

2. 確認 LDAP 簽署與密封安全設定已正確設定：`vserver cifs security show -vserver vserver_name`

> 如果 SVM 使用相同的 LDAP 伺服器來查詢名稱對應或其他 UNIX 資訊、例如使用者、群組和網路群組、則必須使用啟用對應的設定 `-session-security` 的選項 `vserver services name-service ldap client modify` 命令。

設定**LDAP over TLS**

匯出 **ONTAP SMB SVM** 的自我簽署根 **CA** 憑證

若要使用LDAP over SSL/TLS來保護Active Directory通訊安全、您必須先將Active Directory憑證服務的自我簽署根CA憑證複本匯出至憑證檔案、然後將其轉換成Ascii文字檔。這個文字檔是ONTAP 由SITALL用來在儲存虛擬機器（SVM）上安裝憑證。

開始之前

Active Directory憑證服務必須已針對CIFS伺服器所屬的網域進行安裝和設定。如需安裝及設定Active Director憑證服務的相關資訊、請參閱Microsoft TechNet程式庫。

"Microsoft TechNet程式庫：technet.microsoft.com"

步驟

1. 取得中網域控制站的根 CA 憑證 `.pem` 文字格式。

   "Microsoft TechNet程式庫：technet.microsoft.com"

完成後

在SVM上安裝憑證。

相關資訊

"Microsoft TechNet程式庫"

在 **ONTAP SMB SVM** 上安裝自我簽署的根 **CA** 憑證

如果在連結至LDAP伺服器時需要使用TLS進行LDAP驗證、您必須先在SVM上安裝自我簽署的根CA憑證。

關於這項工作

ONTAP 中所有使用 TLS 通訊的應用程式，都可以使用線上憑證狀態傳輸協定（ OCSP ）來檢查數位憑證狀態。如果在TLS上為LDAP啟用OCSP、則撤銷的憑證會遭到拒絕、連線也會失敗。

步驟

1. 安裝自我簽署的根CA憑證：

a. 開始安裝憑證： `security certificate install -vserver vserver_name -type server-ca`

   主控台輸出會顯示下列訊息： `Please enter Certificate: Press <Enter> when done`

b. 開啟憑證 `.pem` 使用文字編輯器檔案、複製憑證、包括開頭的行 `-----BEGIN CERTIFICATE-----` 並以結束 `-----END CERTIFICATE-----`，然後在命令提示字元之後貼上憑證。

c. 確認已正確顯示憑證。

d. 按Enter完成安裝。

2. 確認已安裝憑證： `security certificate show -vserver vserver_name`

相關資訊

- "安全性憑證安裝"
- "安全證書展示"

在 **ONTAP SMB** 伺服器上啟用 **LDAP over TLS**

您的SMB伺服器必須先修改SMB伺服器安全性設定、才能使用TLS與Active Directory LDAP伺服器進行安全通訊。

從ONTAP 《支援範圍》9.10.1開始、Active Directory（AD）和名稱服務LDAP連線預設都支援LDAP通道繫結。僅當啟用Start-TLS或LDAPS並將工作階段安全性設定為簽署或密封時、才能嘗試透過LDAP連線進行通道繫結。ONTAP若要停用或重新啟用與 AD 伺服器的 LDAP 通道繫結、請使用 `-try-channel-binding-for-ad-ldap` 參數 `vserver cifs security modify` 命令。

若要深入瞭解、請參閱：

- "了解適用於 ONTAP NFS SVM 的 LDAP"
- "2020 LDAP通道繫結和LDAP簽署要求、適用於Windows"。

步驟

1. 設定 SMB 伺服器安全性設定、以允許與 Active Directory LDAP 伺服器進行安全的 LDAP 通訊： `vserver cifs security modify -vserver vserver_name -use-start-tls-for-ad-ldap true`
2. 確認 LDAP over TLS 安全性設定已設定為 `true`： `vserver cifs security show -vserver vserver_name`

> 如果 SVM 使用相同的 LDAP 伺服器來查詢名稱對應或其他 UNIX 資訊（例如使用者、群組和網路群組）、則您也必須修改 `-use-start-tls` 選項：使用 `vserver services name-service ldap client modify` 命令。

設定 **ONTAP SMB** 多通道以獲得效能和備援

從支援支援支援的9.4開始ONTAP 、您可以設定SMB多通道、ONTAP 在單一SMB工作階段中、在支援的情況下提供多個連接功能。這樣做可改善處理量和容錯能力。

開始之前

只有當用戶端在SMB 3.0或更新版本上進行交涉時、才能使用SMB多通道功能。根據預設、SMB 3.0及更新版本會在ONTAP 支援SMB的伺服器上啟用。

關於這項工作

如果ONTAP 在故障叢集上識別出適當的組態、SMB用戶端會自動偵測並使用多個網路連線。

SMB工作階段中的同時連線數目取決於您已部署的NIC：

- *用戶端和ONTAP 叢集上的1G NIC *

  用戶端每個NIC建立一個連線、並將工作階段連結至所有連線。

- *用戶端與ONTAP 支援叢集*上的10G與更大容量NIC

  用戶端每個NIC最多可建立四個連線、並將工作階段連結至所有連線。用戶端可在多個10G和更大容量的NIC上建立連線。

您也可以修改下列參數（進階權限）：

- `-max-connections-per-session`

  每個多通道工作階段允許的最大連線數。預設為32個連線。

  如果您想要啟用比預設值更多的連線、則必須對用戶端組態進行類似的調整、也就是預設的32個連線。

- `-max-lifs-per-session`

  每個多通道工作階段所通告的網路介面數量上限。預設為256個網路介面。

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 在SMB伺服器上啟用SMB多通道：

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. 驗證ONTAP 此功能是否回報SMB多通道工作階段：

```
vserver cifs session show
```

4. 返回管理權限層級：

```
set -privilege admin
```

範例

下列範例顯示所有SMB工作階段的相關資訊、顯示單一工作階段的多個連線：

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User          Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

下列範例顯示使用工作階段ID 1之SMB工作階段的詳細資訊：

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                            Node: node1
                      Session ID: 1
                  Connection IDs: 138683,138684,138685
                Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                 Connected Time: 5s
                      Idle Time: 5s
                Protocol Version: SMB3
        Continuously Available: No
             Is Session Signed: false
                  NetBIOS Name: -
```

在SMB伺服器上設定預設的Windows使用者對UNIX使用者對應

設定預設的 ONTAP SMB UNIX 使用者

您可以將預設UNIX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和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、則不應設定預設的UNIX使用者。

關於這項工作

根據預設、預設UNIX使用者的名稱為「'pcuser'」、這表示預設會啟用使用者對應至預設UNIX使用者的功能。您可以指定其他名稱作為預設UNIX使用者。您指定的名稱必須存在於為儲存虛擬機器（SVM）設定的名稱服務資料庫中。如果此選項設為null字串、則無人能以UNIX預設使用者的身分存取CIFS伺服器。也就是、每位使用者必須在密碼資料庫中擁有帳戶、才能存取CIFS伺服器。

使用者若要使用預設UNIX使用者帳戶連線至CIFS伺服器、必須符合下列先決條件：

- 使用者已通過驗證。
- 使用者位於CIFS伺服器的本機Windows使用者資料庫、CIFS伺服器的主網域或信任的網域（如果CIFS伺服器上已啟用多網域名稱對應搜尋）中。
- 使用者名稱未明確對應至null字串。

步驟

1. 設定預設UNIX使用者：

如果您想...	輸入...
使用預設的UNIX使用者「'pcuser'」	`vserver cifs options modify -default -unix-user pcuser`
使用另一個UNIX使用者帳戶做為預設使用者	`vserver cifs options modify -default -unix-user user_name`
停用預設UNIX使用者	`vserver cifs options modify -default -unix-user ""`

```
vserver cifs options modify -default-unix-user pcuser
```

2. 確認預設UNIX使用者已正確設定：`vserver cifs options show -vserver vserver_name`

   在下列範例中、SVM VS1上的預設UNIX使用者和來賓UNIX使用者均設定為使用UNIX使用者「'pcuser'」：

   ```
   vserver cifs options show -vserver vs1
   ```

   ```
   Vserver: vs1

     Client Session Timeout : 900
     Default Unix Group     : -
     Default Unix User      : pcuser
     Guest Unix User        : pcuser
     Read Grants Exec       : disabled
     Read Only Delete       : disabled
     WINS Servers           : -
   ```

設定來賓 **ONTAP SMB UNIX** 使用者

設定來賓UNIX使用者選項表示從不受信任網域登入的使用者會對應到來賓UNIX使用者、並可連線到CIFS伺服器。或者、如果您想要驗證來自不受信任網域的使用者、則不應該設定來賓UNIX使用者。預設值是不允許來自不受信任網域的使用者連線至CIFS伺服器（未設定來賓UNIX帳戶）。

關於這項工作

設定來賓UNIX帳戶時、請謹記下列事項：

- 如果CIFS伺服器無法針對主網域或信任的網域或本機資料庫的網域控制器驗證使用者、且已啟用此選項、則CIFS伺服器會將使用者視為來賓使用者、並將使用者對應至指定的UNIX使用者。
- 如果此選項設為null字串、則停用來賓UNIX使用者。
- 您必須建立UNIX使用者、才能在其中一個儲存虛擬機器（SVM）名稱服務資料庫中做為來賓UNIX使用者。

- 以訪客使用者身分登入的使用者會自動成為CIFS伺服器上BUILTIN\訪 客群組的成員。
- 「homdirs-public」選項僅適用於已驗證的使用者。以來賓使用者身分登入的使用者沒有主目錄、因此無法存取其他使用者的主目錄。

步驟

1. 執行下列其中一項動作：

如果您想要...	輸入...
設定來賓UNIX使用者	`vserver cifs options modify -guest -unix-user` *`unix_name`*
停用來賓UNIX使用者	`vserver cifs options modify -guest -unix-user ""`

```
vserver cifs options modify -guest-unix-user pcuser
```

2. 確認來賓 UNIX 使用者已正確設定： `vserver cifs options show -vserver` *`vserver_name`*

   在下列範例中、SVM VS1上的預設UNIX使用者和來賓UNIX使用者均設定為使用UNIX使用者「'pcuser'」：

   ```
   vserver cifs options show -vserver vs1
   ```

   ```
   Vserver: vs1

     Client Session Timeout : 900
     Default Unix Group     : -
     Default Unix User      : pcuser
     Guest Unix User        : pcuser
     Read Grants Exec       : disabled
     Read Only Delete       : disabled
     WINS Servers           : -
   ```

將系統管理員群組對應至 **ONTAP SMB** 根目錄

如果您的環境中只有CIFS用戶端、且儲存虛擬機器（SVM）設定為多重傳輸協定儲存系統、則您必須擁有至少一個具有root權限的Windows帳戶、才能存取SVM上的檔案； 否則、您將無法管理SVM、因為您沒有足夠的使用者權限。

關於這項工作

如果您的儲存系統設定為僅 NTFS ， `/etc`則目錄會有檔案層級的 ACL ，讓系統管理員群組能夠存取 ONTAP 組態檔案。

步驟

1. 將權限層級設為進階： `set -privilege advanced`

2. 設定CIFS伺服器選項、將系統管理員群組適當對應至root：

如果您想要...	然後...
將系統管理員群組成員對應至root	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled true` 即使您沒有、系統管理員群組中的所有帳戶都會視為 root `/etc/usermap.cfg` 將帳戶對應至根目錄的項目。如果您使用屬於系統管理員群組的帳戶來建立檔案、則當您從UNIX用戶端檢視檔案時、檔案將由root擁有。
停用將系統管理員群組成員對應至root	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled false` 系統管理員群組中的帳戶不再對應至根目錄。您只能明確地將單一使用者對應至root。

3. 確認選項設定為所需的值： `vserver cifs options show -vserver` *`vserver_name`*
4. 返回管理權限層級： `set -privilege admin`

顯示透過 **ONTAP SMB** 工作階段連線的使用者類型資訊

您可以顯示透過SMB工作階段連線的使用者類型資訊。這有助於確保只有適當類型的使用者透過儲存虛擬機器（SVM）上的SMB工作階段進行連線。

關於這項工作

下列類型的使用者可透過SMB工作階段連線：

- `local-user`

  已驗證為本機CIFS使用者

- `domain-user`

  驗證為網域使用者（可從CIFS伺服器的主網域或信任的網域）

- `guest-user`

  驗證為來賓使用者

- `anonymous-user`

  驗證為匿名或null使用者

步驟

1. 判斷透過 SMB 工作階段連線的使用者類型： `vserver cifs session show -vserver` *`vserver_name`* `-windows-user` *`windows_user_name`* `-fields windows-user,address,lif-address,user-type`

如果您要顯示已建立工作階段的使用者類型資訊...	輸入下列命令...
適用於具有指定使用者類型的所有工作階段	`vserver cifs session show -vserver *vserver_name* -user-type {local-user
domain-user	guest-user
anonymous-user}`	適用於特定使用者

範例

下列命令會顯示使用者「eubs\user1'」在SVM VS1上建立之工作階段的使用者類型工作階段資訊：

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node      vserver session-id connection-id lif-address  address
windows-user         user-type
--------- ------- ---------- ------------- ------------ -------------
-------------------- -----------
pub1node1 pub1    1          3439441860    10.0.0.1     10.1.1.1
IEPUBS\user1         domain-user
```

ONTAP 命令選項可限制過度的 Windows 用戶端資源使用量

的選項 `vserver cifs options modify` 命令可讓您控制 Windows 用戶端的資源使用量。如果有任何用戶端超出資源使用量的正常範圍、例如開啟的檔案數量異常多、開啟的工作階段或變更通知要求、則這項功能會很有幫助。

的下列選項 `vserver cifs options modify` 已新增命令以控制 Windows 用戶端資源使用量。如果超過這些選項的最大值、則會拒絕要求、並傳送EMS訊息。當達到這些選項設定上限的80%時、也會傳送EMS警告訊息。

- `-max-opens-same-file-per-tree`

  每個CIFS樹狀結構在同一個檔案上開啟的最大數目

- `-max-same-user-sessions-per-connection`

  每個連線的相同使用者所開啟的工作階段數目上限

- `-max-same-tree-connect-per-session`

  每個工作階段在相同共用區上連線的樹狀結構數目上限

- `-max-watches-set-per-tree`

  每個樹狀結構建立的監視數目上限（也稱為「變更通知」）

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

從ONTAP Sf9.4開始、執行SMB第2版或更新版本的伺服器可以限制用戶端在SMB連線上傳送至伺服器的未處理要求數（*SMB*點數）。SMB信用管理是由用戶端啟動、由伺服器控制。

可在 SMB 連線上授予的未處理要求數目上限是由控制 `-max-credits` 選項。此選項的預設值為128。

利用傳統和租賃**oplock**來提升用戶端效能

瞭解如何利用傳統和租賃資源來改善 **ONTAP SMB** 用戶端效能

傳統oplocks（投機鎖定）和租用oplock可在某些檔案共用案例中、讓SMB用戶端執行預先讀取、回寫及鎖定資訊的用戶端快取。然後用戶端可以讀取或寫入檔案、而不會定期提醒伺服器需要存取相關檔案。如此可減少網路流量、進而提升效能。

租賃oplock是SMB 2.1傳輸協定及更新版本所提供的一種強化型oplock形式。租賃oplock可讓用戶端在自有的多個SMB之間取得及保留用戶端快取狀態。

oplocks有兩種控制方式：

- 透過共用屬性、使用 `vserver cifs share create` 建立共用時的命令、或 `vserver share properties` 建立後的命令。
- 使用 qtree 屬性 `volume qtree create` qtree 建立時的命令、或 `volume qtree oplock` 建立後的命令。

瞭解在使用 **oplocks** 時寫入 **ONTAP SMB** 快取資料遺失考量

在某些情況下、如果某個處理程序在檔案上有獨家oplock、而第二個處理程序嘗試開啟該檔案、則第一個處理程序必須使快取的資料失效、並清除寫入和鎖定。然後用戶端必須放棄oplock並存取檔案。如果在此排清期間發生網路故障、快取的寫入資料可能會遺失。

- 資料遺失的可能性

  任何具有寫入快取資料的應用程式、都可能在下列情況下遺失該資料：

  - 連線是使用SMB 1.0進行。
  - 檔案上有獨家oplock。
  - 系統會要求中斷oplock或關閉檔案。
  - 在清空寫入快取的過程中、網路或目標系統會產生錯誤。
- 錯誤處理和寫入完成

  快取本身沒有任何錯誤處理、應用程式也有。當應用程式寫入快取時、寫入作業一律會完成。如果快取反過來又透過網路寫入目標系統、則必須假設寫入作業已完成、因為如果寫入作業未完成、資料就會遺失。

建立 **ONTAP SMB** 共用時，請啟用或停用 **oplocks**

oplocks可讓用戶端在本機上鎖定檔案和快取內容、進而提升檔案作業的效能。在儲存虛擬

機器（SVM）上的SMB共用上啟用oplocks。在某些情況下、您可能會想要停用oplocks。您可以逐一啟用或停用oplocks。

關於這項工作

如果在包含共用區的磁碟區上啟用oplock、但該共用區的oplock共用內容已停用、則該共用區的oplocks會停用。停用共用上的oplocks優先於Volume oplock設定。停用共用區上的oplocks會停用投機和租用oplock。

除了使用以逗號分隔的清單來指定oplock共用屬性之外、您也可以指定其他共用屬性。您也可以指定其他共用參數。

步驟

1. 執行適用的行動：

如果您想要...	然後...
在共用建立期間、在共用區上啟用oplocks	輸入下列命令： `vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share -properties [oplocks,...]` 如果您希望共用只有預設的共用內容、即 `oplocks`、`browsable`和 `changenotify` 啟用時、您不需要指定 `-share-properties` 建立 SMB 共用時的參數。如果您想要使用預設以外的任何共用內容組合、則必須指定 `-share-properties` 參數、以及用於該共用的共用內容清單。
在共用建立期間停用共用區上的oplocks	輸入下列命令： `vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]` 停用 oplocks 時、您必須在建立共用時指定共用內容清單、但不應指定 `oplocks` 屬性。

相關資訊

啟用或停用現有SMB共用區上的oplocks

監控oplock狀態

ONTAP 命令，用於在 **SMB** 磁碟區和 **qtree** 上啟用或停用 **oplocks**

oplocks可讓用戶端在本機上鎖定檔案和快取內容、進而提升檔案作業的效能。您需要知道

在磁碟區或qtree上啟用或停用oplocks的命令。您也必須知道何時可以在磁碟區和qtree上啟用或停用oplocks。

- 預設會在磁碟區上啟用oplocks。
- 您無法在建立Volume時停用oplocks。
- 您可以隨時在現有磁碟區上為SVM啟用或停用oplock。
- 您可以在qtree上為SVM啟用oplocks。

  oplock模式設定是qtree ID 0的屬性、即所有磁碟區的預設qtree。如果您在建立qtree時未指定oplock設定、qtree會繼承父Volume的oplock設定、此設定預設為啟用。不過、如果您在新qtree上指定oplock設定、則其優先於Volume上的oplock設定。

如果您想要...	使用此命令...
在磁碟區或qtree上啟用oplocks	`volume qtree oplocks` 使用 `-oplock-mode` 參數設為 `enable`
停用磁碟區或qtree上的oplocks	`volume qtree oplocks` 使用 `-oplock-mode` 參數設為 `disable`

相關資訊

監控oplock狀態

啟用或停用現有 **ONTAP SMB** 共用上的 **oplocks**

預設會在儲存虛擬機器（SVM）上的SMB共用上啟用oplocks。在某些情況下、您可能想要停用oplocks；或者、如果您先前已停用共用區上的oplocks、則可能需要重新啟用oplocks。

關於這項工作

如果在包含共用區的磁碟區上啟用oplock、但該共用區的oplock共用內容已停用、則該共用區的oplocks會停用。停用共用區上的oplocks優先於在磁碟區上啟用oplocks。停用共用區上的oplocks、停用機會和租用oplock。您可以隨時在現有共用區上啟用或停用oplocks。

步驟

1. 執行適用的行動：

如果您想要...	然後...
修改現有的共用區、在共用區上啟用oplocks	輸入下列命令：`vserver cifs share properties add -vserver vserver_name -share-name share_name -share -properties oplocks` 您可以使用以逗號分隔的清單來指定要新增的其他共用屬性。 新增的內容會附加到現有的共用內容清單中。您先前指定的任何共用內容都會維持有效。
透過修改現有的共用區來停用共用區上的oplocks	輸入下列命令：`vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties oplocks` 您可以使用以逗號分隔的清單來指定要移除的其他共用屬性。 您移除的共用內容會從現有的共用內容清單中刪除、不過您先前設定的共用內容若未移除、則仍會維持有效。

範例

下列命令可在儲存虛擬機器（SVM、先前稱為Vserver）VS1上、針對名為「Engineering」的共用區啟用oplocks：

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      oplocks
                                  browsable
                                  changenotify
                                  showsnapshot
```

下列命令會停用SVM VS1上名為「Engineering」的共用區oplocks：

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      browsable
                                  changenotify
                                  showsnapshot
```

相關資訊

- 建立SMB共用時啟用或停用oplocks
- 監控oplock狀態
- 新增或刪除現有共享的共享屬性

監控 **ONTAP SMB oplock** 狀態

您可以監控及顯示oplock狀態的相關資訊。您可以使用此資訊來判斷哪些檔案有oplock、oplock層級和oplock狀態層級、以及是否使用oplock租賃。您也可以決定手動中斷鎖定的相關資訊。

關於這項工作

您可以在摘要表單或詳細清單表單中顯示所有oplock的相關資訊。您也可以使用選用參數來顯示現有鎖定的較小子集相關資訊。例如、您可以指定輸出只傳回指定用戶端IP位址或指定路徑的鎖定。

您可以顯示下列關於傳統和租賃oplock的資訊：

- 建立oplock的SVM、節點、Volume和LIF
- 鎖定UUID
- 使用oplock的用戶端IP位址
- 建立oplock的路徑
- 鎖定傳輸協定（SMB）和類型（oplock）
- 鎖定狀態
- oplock層級
- 連線狀態和SMB到期時間
- 開放群組ID（如果已授予租賃oplock）

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

步驟

1. 使用顯示 oplock 狀態 `vserver locks show` 命令。

範例

下列命令會顯示所有鎖定的預設資訊。所顯示檔案上的 oplock 會授予 `read-batch` Oplock 層級：

```
cluster1::> vserver locks show

Vserver: vs0
Volume   Object Path        LIF         Protocol  Lock Type   Client
-------- ------------------ ----------- --------- ----------- ----------
vol1     /vol1/notes.txt    node1_data1
                                        cifs      share-level 192.168.1.5
         Sharelock Mode: read_write-deny_delete
                                                  op-lock     192.168.1.5
         Oplock Level: read-batch
```

下列範例顯示有關鎖定路徑檔案的詳細資訊 `/data2/data2_2/intro.pptx`。在檔案上授予租用 oplock `batch` Oplock 層級至 IP 位址為的用戶端 `10.3.1.3`：

> 顯示詳細資訊時、命令會針對oplock和共享鎖定資訊提供個別輸出。此範例僅顯示oplock區段的輸出。

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

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

相關資訊

建立SMB共用時啟用或停用oplocks

啟用或停用現有SMB共用區上的oplocks

用於在 SMB 捲和 qtree 上啟用或停用 oplock 的命令

將群組原則物件套用至**SMB**伺服器

瞭解如何將群組原則物件套用至 **ONTAP SMB** 伺服器

您的SMB伺服器支援群組原則物件（GPO）、這是一套稱為「群組原則屬性」的規則、適用於Active Directory環境中的電腦。您可以使用GPO集中管理屬於同一個Active Directory網域之叢集上所有儲存虛擬機器（SVM）的設定。

在SMB伺ONTAP 服器上啟用GPO時、將LDAP查詢傳送至Active Directory伺服器、要求取得GPO資訊。如果您的SMB伺服器適用GPO定義、Active Directory伺服器會傳回下列GPO資訊：

- GPO 名稱
- 目前的GPO版本
- GPO定義的位置
- GPO原則集的UUID清單（通用唯一識別碼）

相關資訊

- 了解伺服器的檔案存取安全性
- "SMB與NFS稽核與安全性追蹤"

瞭解支援的 **ONTAP SMB GPO**

雖然並非所有的群組原則物件（GPO）都適用於CIFS型儲存虛擬機器（SVM）、但SVM可以辨識及處理相關的GPO集。

SVM目前支援下列GPO：

- 進階稽核原則組態設定：

  物件存取：集中存取原則接移

  指定要稽核中央存取原則（CAP）接移的事件類型、包括下列設定：

  - 請勿稽核
  - 僅稽核成功事件
  - 僅稽核失敗事件
  - 稽核成功與失敗事件

  > 如果三個稽核選項中有任何一個已設定（僅稽核成功事件、僅稽核失敗事件、同時稽核成功和失敗事件）ONTAP 、則會同時稽核成功和失敗事件。

  使用設定 `Audit Central Access Policy Staging` 的設定 `Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO ：

  > 若要使用進階稽核原則組態GPO設定、您必須在要套用這些設定的CIFS型SVM上設定稽核。如果未在SVM上設定稽核、則不會套用及捨棄GPO設定。

- 登錄設定：

  - 啟用CIFS的SVM的群組原則重新整理時間間隔

    使用設定 `Registry` GPO ：

  - 群組原則重新整理隨機偏移

    使用設定 `Registry` GPO ：

  - BranchCache的雜湊發佈

BranchCache GPO的雜湊發佈會對應到BranchCache作業模式。支援下列三種操作模式：

- 每個共用區
- All共享區
- 已停用 使用設定 `Registry` GPO ：

◦ 支援BranchCache的雜湊版本

支援下列三種雜湊版本設定：

- BranchCache第1版
- BranchCache 版本 2
- BranchCache 第 1 版和第 2 版 使用設定 `Registry` GPO ：

> 若要使用BranchCache GPO設定、必須在您要套用這些設定的CIFS型SVM上設定BranchCache。如果未在SVM上設定BranchCache、則不會套用GPO設定、也會捨棄。

- 安全性設定

◦ 稽核原則與事件記錄

- 稽核登入事件

指定要稽核的登入事件類型、包括下列設定：

- 請勿稽核
- 僅稽核成功事件
- 稽核失敗事件
- 稽核成功與失敗事件 使用設定 `Audit logon events` 的設定 `Local Policies/Audit Policy` GPO ：

> 如果三個稽核選項中有任何一個已設定（僅稽核成功事件、僅稽核失敗事件、同時稽核成功和失敗事件）ONTAP 、則會同時稽核成功和失敗事件。

- 稽核物件存取

指定要稽核的物件存取類型、包括下列設定：

- 請勿稽核
- 僅稽核成功事件
- 稽核失敗事件
- 稽核成功與失敗事件 使用設定 `Audit object access` 的設定 `Local Policies/Audit Policy` GPO ：

> 如果三個稽核選項中有任何一個已設定（僅稽核成功事件、僅稽核失敗事件、同時稽核成功和失敗事件）ONTAP 、則會同時稽核成功和失敗事件。

- 記錄保留方法

  指定稽核記錄保留方法、包括下列設定：

  - 當記錄檔大小超過最大記錄檔大小時、請覆寫事件記錄
  - 不要覆寫事件記錄（手動清除記錄） 使用設定 `Retention method for security log` 的設定 `Event Log` GPO ：

- 最大記錄大小

  指定稽核記錄的最大大小。

  使用設定 `Maximum security log size` 的設定 `Event Log` GPO ：

  若要使用稽核原則和事件記錄GPO設定、您必須在要套用這些設定的CIFS型SVM上設定稽核。如果未在SVM上設定稽核、則不會套用及捨棄GPO設定。

◦ 檔案系統安全性

指定透過GPO套用檔案安全性的檔案或目錄清單。

使用設定 `File System` GPO ：

設定檔案系統安全性GPO的磁碟區路徑必須存在於SVM中。

◦ Kerberos原則

- 最大時鐘偏移

  指定電腦時鐘同步的最大容許值（以分鐘為單位）。

  使用設定 `Maximum tolerance for computer clock synchronization` 的設定 `Account Policies/Kerberos Policy` GPO ：

- 票證最長使用期限

  指定使用者票證的最長壽命（以小時為單位）。

  使用設定 `Maximum lifetime for user ticket` 的設定 `Account Policies/Kerberos Policy` GPO ：

- 票證續約期限上限

  指定使用者票證續約的最長壽命（以天為單位）。

使用設定 `Maximum lifetime for user ticket renewal` 的設定 `Account Policies/Kerberos Policy` GPO ：

◦ 使用者權限指派（權限）

- 取得擁有權

指定有權取得任何安全物件所有權的使用者和群組清單。

使用設定 `Take ownership of files or other objects` 的設定 `Local Policies/User Rights Assignment` GPO ：

- 安全性權限

  指定使用者和群組清單、這些使用者和群組可指定個別資源（例如檔案、資料夾和Active Directory物件）物件存取的稽核選項。

  使用設定 `Manage auditing and security log` 的設定 `Local Policies/User Rights Assignment` GPO ：

- 變更通知權限（略過周遊檢查）

  指定可遍歷目錄樹狀結構的使用者和群組清單、即使使用者和群組對周遊目錄可能沒有權限。

使用者必須擁有相同的權限、才能接收檔案和目錄變更通知。使用設定 `Bypass traverse checking` 的設定 `Local Policies/User Rights Assignment` GPO ：

- 登錄值

  - 需要簽署設定

    指定是否啟用或停用必要的SMB簽署。

  使用設定 `Microsoft network server: Digitally sign communications (always)` 的設定 `Security Options` GPO ：

- 限制匿名

  指定匿名使用者的限制、並包含下列三項GPO設定：

  - 無列舉安全性客戶經理（SAM）帳戶：

    此安全性設定可決定授與哪些其他權限給電腦的匿名連線。此選項會顯示為 `no-enumeration` 在 ONTAP 中（如果已啓用）。

    使用設定 `Network access: Do not allow anonymous enumeration of SAM accounts` 的設定 `Local Policies/Security Options` GPO ：

  - 未列舉SAM帳戶和共用

    此安全性設定可決定是否允許SAM帳戶和共用的匿名列舉。此選項會顯示為 `no-enumeration` 在 ONTAP 中（如果已啓用）。

    使用設定 `Network access: Do not allow anonymous enumeration of SAM accounts and shares` 的設定 `Local Policies/Security Options` GPO ：

  - 限制匿名存取共用和具名管道

    此安全性設定會限制匿名存取共用和管道。此選項會顯示為 `no-access` 在 ONTAP 中（如果已啓用）。

使用設定 `Network access: Restrict anonymous access to Named Pipes and Shares` 的設定 `Local Policies/Security Options` GPO ：

顯示已定義和已套用群組原則的相關資訊時、會顯示 `Resultant restriction for anonymous user` 「輸出」欄位提供三個限制匿名 GPO 設定的結果限制相關資訊。可能的結果限制如下：

- `no-access`

  匿名使用者無法存取指定的共用和具名管道、也無法使用SAM帳戶和共用的列舉。如果出現這種情況、就會出現這種限制 `Network access: Restrict anonymous access to Named Pipes and Shares` 已啟用 GPO 。

- `no-enumeration`

  匿名使用者可以存取指定的共用和具名管道、但無法使用SAM帳戶和共用的列舉。如果符合下列兩項條件、就會看到這項限制：

  - 。 `Network access: Restrict anonymous access to Named Pipes and Shares` GPO 已停用。
  - 或是 `Network access: Do not allow anonymous enumeration of SAM accounts` 或 `Network access: Do not allow anonymous enumeration of SAM accounts and shares` 已啟用 GPO 。

- `no-restriction`

  匿名使用者擁有完整存取權、可以使用列舉功能。如果符合下列兩項條件、就會看到這項限制：

  - 。 `Network access: Restrict anonymous access to Named Pipes and Shares` GPO 已停用。
  - 兩者皆是 `Network access: Do not allow anonymous enumeration of SAM accounts` 和 `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPO 已停用。

    - 受限群組

      您可以設定受限群組、集中管理內建或使用者定義群組的成員資格。透過群組原則套用受限群組時、CIFS伺服器本機群組的成員資格會自動設定為符合套用群組原則中定義的成員資格清單設定。

使用設定 `Restricted Groups` GPO ：

- 集中存取原則設定

  指定集中存取原則清單。集中存取原則及相關的集中存取原則規則、決定SVM上多個檔案的存取權限。

相關資訊

- 在伺服器上啟用或停用 GPO 支援
- 了解伺服器的檔案存取安全性
- "SMB與NFS稽核與安全性追蹤"

- 修改伺服器安全設定
- 了解如何使用 BranchCache 在分公司快取共享內容
- 了解如何使用 ONTAP 簽章來增強網路安全
- 了解如何配置繞過遍歷檢查
- 設定匿名使用者的存取限制

ONTAP SMB 伺服器對 GPO 的需求

若要在SMB伺服器上使用群組原則物件（GPO）、您的系統必須符合多項需求。

- SMB必須在叢集上獲得授權。SMB 授權隨附於"ONTAP One"。如果您沒有 ONTAP One 且未安裝授權、請聯絡您的銷售代表。
- SMB伺服器必須設定並加入Windows Active Directory網域。
- SMB伺服器管理狀態必須為開啟。
- 必須設定GPO並套用至包含SMB伺服器電腦物件的Windows Active Directory組織單位（OU）。
- 必須在SMB伺服器上啟用GPO支援。

在 ONTAP SMB 伺服器上啟用或停用 GPO 支援

您可以在CIFS伺服器上啟用或停用群組原則物件（GPO）支援。如果您在CIFS伺服器上啟用GPO支援、則會將群組原則上定義的適用GPO（套用至包含CIFS伺服器電腦物件之組織單位（OU）的原則）套用至CIFS伺服器。

關於這項工作

無法在CIFS伺服器上以工作群組模式啟用GPO。

步驟

1. 執行下列其中一項動作：

如果您想要...	輸入命令...
啟用GPO	`vserver cifs group-policy modify -vserver vserver_name -status enabled`
停用GPO	`vserver cifs group-policy modify -vserver vserver_name -status disabled`

2. 確認 GPO 支援處於所需的狀態：`vserver cifs group-policy show -vserver +vserver_name_`

   工作群組模式中CIFS伺服器的群組原則狀態顯示為「停用」。

範例

下列範例可在儲存虛擬機器（SVM）VS1上啟用GPO支援：

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

            Vserver: vs1
Group Policy Status: enabled
```

相關資訊

了解受支援的 GPO

GPO 的伺服器要求

了解如何在 SMB 伺服器上更新 GPO

手動更新 SMB 伺服器上的 GPO 設定

顯示有關GPO組態的資訊

如何在 **SMB** 伺服器上更新 **GPO**

瞭解如何更新 **ONTAP SMB** 伺服器上的 **GPO**

根據預設ONTAP 、每90分鐘擷取並套用群組原則物件（GPO）變更一次。安全性設定每16小時重新整理一次。如果您想在ONTAP 更新GPO之前先套用新的GPO原則設定、然後再自動更新、您可以在CIFS伺服器上使用ONTAP flexto命令觸發手動更新。

- 根據預設、所有的GPO都會視需要每90分鐘進行一次驗證和更新。

  此時間間隔可設定、並可使用設定 `Refresh interval` 和 `Random offset` GPO 設定。

  可查詢Active Directory以取得變更GPO的資訊。ONTAP如果Active Directory中記錄的GPO版本號碼高於CIFS伺服器、ONTAP 則會擷取並套用新的GPO。如果版本號碼相同、則CIFS伺服器上的GPO不會更新。

- 安全性設定GPO每16小時重新整理一次。

  無論這些GPO是否已變更、均可每16小時擷取並套用安全性設定GPO。ONTAP

  > ⓘ 目前ONTAP 版本的16小時預設值無法變更。這是Windows用戶端的預設設定。

- 所有的GPO都可以使用ONTAP flexflexfcommand手動更新。

  此命令模擬 Windows `gpupdate.exe`/force 命令。

相關資訊

手動更新 SMB 伺服器上的 GPO 設定

手動更新 ONTAP SMB 伺服器上的 GPO 設定

如果您想要立即更新CIFS伺服器上的群組原則物件（GPO）設定、您可以手動更新這些設定。您只能更新變更的設定、或是強制更新所有設定、包括先前套用但尚未變更的設定。

步驟

1. 執行適當的行動：

如果您想要更新...	輸入命令...
變更GPO設定	`vserver cifs group-policy update -vserver vserver_name`
所有GPO設定	`vserver cifs group-policy update -vserver vserver_name -force-reapply -all-settings true`

相關資訊

了解如何在 SMB 伺服器上更新 GPO

顯示 ONTAP SMB GPO 組態的相關資訊

您可以顯示Active Directory中定義的群組原則物件（GPO）組態資訊、以及應用於CIFS伺服器的GPO組態資訊。

關於這項工作

您可以顯示CIFS伺服器所屬網域Active Directory中定義的所有GPO組態資訊、或只顯示套用至CIFS伺服器之GPO組態的相關資訊。

步驟

1. 執行下列其中一項動作、以顯示有關GPO組態的資訊：

如果您要顯示所有群組原則組態的相關資訊...	輸入命令...
在Active Directory中定義	`vserver cifs group-policy show-defined -vserver vserver_name`
套用至CIFS型儲存虛擬機器（SVM）	`vserver cifs group-policy show-applied -vserver vserver_name`

範例

下列範例顯示在Active Directory中定義的GPO組態、其中CIFS啟用的SVM名稱為VS1屬於：

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1
```

```
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 : version1
  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
      Status: enabled
```

```
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for Mode BranchCache: per-share
      Hash Version Support for BranchCache: version1
  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
```

下列範例顯示套用至CIFS型SVM VS1的GPO組態：

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

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
```

相關資訊

在伺服器上啟用或停用 GPO 支援

顯示 **ONTAP SMB** 受限群組 **GPO** 的相關資訊

您可以顯示Active Directory中定義為群組原則物件（GPO）且套用至CIFS伺服器的受限群組詳細資訊。

關於這項工作

依預設、會顯示下列資訊：

- 群組原則名稱
- 群組原則版本
- 連結

  指定群組原則的設定層級。可能的輸出值包括：

  - `Local` 在 ONTAP 中設定群組原則時
  - `Site` 在網域控制站的站台層級設定群組原則時
  - `Domain` 當群組原則是在網域控制站的網域層級設定時
  - `OrganizationalUnit` 當群組原則在網域控制站的組織單位（ OU ）層級上設定時
  - `RSOP` 針對衍生自各個層級所定義之所有群組原則的結果原則集
- 受限群組名稱
- 屬於受限群組且不屬於受限群組的使用者和群組
- 新增受限群組的群組清單

  群組可以是此處所列群組以外的群組成員。

步驟

1. 執行下列其中一項動作、顯示所有受限群組GPO的相關資訊：

如果您要顯示所有受限群組**GPO**的相關資訊**...**	輸入命令**...**
在Active Directory中定義	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
套用至CIFS伺服器	`vserver cifs group-policy restricted-group show-applied -vserver vserver_name`

範例

下列範例顯示在Active Directory網域中定義的受限群組GPO相關資訊、其中CIFS啟用的SVM名稱為VS1屬於該網域：

```
cluster1::> vserver cifs group-policy restricted-group show-defined
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
            MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
            MemberOf: EXAMPLE\group9
```

下列範例顯示套用至CIFS型SVM VS1之受限群組GPO的相關資訊：

```
cluster1::> vserver cifs group-policy restricted-group show-applied
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
            MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
            MemberOf: EXAMPLE\group9
```

相關資訊

顯示有關GPO組態的資訊

顯示 **ONTAP SMB** 中央存取原則的相關資訊

您可以顯示Active Directory中定義的中央存取原則詳細資訊。您也可以顯示透過群組原則物件（GPO）套用至CIFS伺服器的中央存取原則相關資訊。

關於這項工作

依預設、會顯示下列資訊：

- SVM名稱
- 中央存取原則的名稱
- SID
- 說明
- 建立時間
- 修改時間
- 成員規則

工作群組模式中的CIFS伺服器不會顯示、因為它們不支援GPO。

步驟

1. 執行下列其中一項動作、以顯示有關中央存取原則的資訊：

如果您想要顯示所有集中存取原則的相關資訊...	輸入命令...
在Active Directory中定義	`vserver cifs group-policy central-access-policy show-defined -vserver` *vserver_name*
套用至CIFS伺服器	`vserver cifs group-policy central-access-policy show-applied -vserver` *vserver_name*

範例

下列範例顯示Active Directory中定義的所有集中存取原則資訊：

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver  Name                 SID
-------- --------------------
----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

下列範例顯示套用至叢集上儲存虛擬機器（SVM）的所有集中存取原則資訊：

```
cluster1::> vserver cifs group-policy central-access-policy show-applied

Vserver    Name                   SID
-------- --------------------
----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

相關資訊

- 了解伺服器的檔案存取安全性

- 顯示有關GPO組態的資訊
- 顯示有關集中存取原則規則的資訊

顯示 **ONTAP SMB** 中央存取原則規則的相關資訊

您可以顯示與Active Directory中定義的中央存取原則相關聯的中央存取原則規則詳細資訊。您也可以透過集中存取原則GPO（群組原則物件）、顯示套用至CIFS伺服器的中央存取原則規則相關資訊。

關於這項工作

您可以顯示已定義及已套用之集中存取原則規則的詳細資訊。依預設、會顯示下列資訊：

- Vserver名稱
- 中央存取規則的名稱
- 說明
- 建立時間
- 修改時間
- 目前權限
- 建議的權限
- 目標資源

如果您要顯示與集中存取原則相關的所有集中存取原則規則資訊...	輸入命令...
在Active Directory中定義	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
套用至CIFS伺服器	`vserver cifs group-policy central-access-rule show-applied -vserver vserver_name`

範例

下列範例顯示Active Directory中定義之中央存取原則相關的所有中央存取原則規則資訊：

```
cluster1::> vserver cifs group-policy central-access-rule show-defined

Vserver     Name
----------- --------------------
vs1         r1
              Description: rule #1
            Creation Time: Tue Oct 22 09:33:48 2013
        Modification Time: Tue Oct 22 09:33:48 2013
       Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
      Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1         r2
              Description: rule #2
            Creation Time: Tue Oct 22 10:27:57 2013
        Modification Time: Tue Oct 22 10:27:57 2013
       Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
      Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

下列範例顯示與套用至叢集上儲存虛擬機器（SVM）的集中存取原則相關的所有集中存取原則規則資訊：

```
cluster1::> vserver cifs group-policy central-access-rule show-applied

Vserver     Name
----------- --------------------
vs1         r1
              Description: rule #1
            Creation Time: Tue Oct 22 09:33:48 2013
        Modification Time: Tue Oct 22 09:33:48 2013
       Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
      Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1         r2
              Description: rule #2
            Creation Time: Tue Oct 22 10:27:57 2013
        Modification Time: Tue Oct 22 10:27:57 2013
       Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
      Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

相關資訊

- 了解伺服器的檔案存取安全性
- 顯示有關GPO組態的資訊
- 顯示有關集中存取原則的資訊

用於管理 SMB 伺服器電腦帳戶密碼的 ONTAP 命令

您需要知道變更、重設及停用密碼、以及設定自動更新排程的命令。您也可以在 SMB 伺服器上設定排程、以自動更新排程。

如果您想要...	使用此命令...
當 ONTAP 與 AD 服務同步時，請變更網域帳戶密碼	`vserver cifs domain password change`
當 ONTAP 未與 AD 服務同步時，請重設網域帳戶密碼	`vserver cifs domain password reset`
設定SMB伺服器以自動變更電腦帳戶密碼	`vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true`
停用SMB伺服器上的自動電腦帳戶密碼變更	`vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false`

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

管理網域控制器連線

顯示 ONTAP SMB 探索伺服器的相關資訊

您可以顯示CIFS伺服器上探索到的LDAP伺服器和網域控制器相關資訊。

步驟

1. 若要顯示與探索到的伺服器相關的資訊、請輸入下列命令： `vserver cifs domain discovered-servers show`

範例

下列範例顯示SVM VS1探索到的伺服器：

```
cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address     Status
--------------- -------- ---------- ----------- -------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4        OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5        OK
example.com     MS-DC    adequate   DC-1        1.1.3.4        OK
example.com     MS-DC    adequate   DC-2        1.1.3.5        OK
```

相關資訊

- 重設並重新探索伺服器
- 停止或啟動伺服器

重設及重新探索 ONTAP SMB 伺服器

重設及重新探索CIFS伺服器上的伺服器、可讓CIFS伺服器捨棄有關LDAP伺服器和網域控制器的儲存資訊。在捨棄伺服器資訊之後、CIFS伺服器會重新取得這些外部伺服器的目前資訊。當連線的伺服器沒有適當回應時、此功能很有用。

步驟

1. 輸入下列命令： `vserver cifs domain discovered-servers reset-servers -vserver` *`vserver_name`*
2. 顯示新重新探索到的伺服器相關資訊： `vserver cifs domain discovered-servers show -vserver` *`vserver_name`*

範例

下列範例可重設及重新探索儲存虛擬機器（SVM、先前稱為Vserver）VS1的伺服器：

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver
vs1

cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

相關資訊

- 顯示探索到的伺服器相關資訊
- 停止或啟動伺服器

管理 ONTAP SMB 網域控制站探索

從ONTAP 功能更新9.3開始、您可以修改探索網域控制器（DC）的預設程序。如此一來、您就能將探索範圍限制在網站或偏好的DC資源池中、進而提升效能、端視環境而定。

關於這項工作

根據預設、動態探索程序會探索所有可用的DC、包括任何慣用的DC、本機站台中的所有DC、以及所有遠端DC。此組態可能會導致驗證延遲、以及在特定環境中存取共用區。如果您已經決定要使用的DC資源池、或是遠端DC不足或無法存取、您可以變更探索方法。

在 ONTAP 9.3 及更新版本中 `discovery-mode` 的參數 `cifs domain discovered-servers` 命令可讓您選取下列其中一個探索選項：

- 探索網域中的所有DC。
- 只會探索本機站台中的DC。
  - `default-site` SMB 伺服器的參數可定義為使用此模式搭配未指派給站台和服務中站台的生命。
- 未執行伺服器探索、SMB伺服器組態僅取決於偏好的DC。

  若要使用此模式、您必須先定義SMB伺服器的慣用DC。

開始之前

您必須處於進階權限層級。

步驟

1. 指定所需的探索選項： `vserver cifs domain discovered-servers discovery-mode modify -vserver` *`vserver_name`* `-mode {all|site|none}`

   的選項 `mode` 參數：

   - `all`

     探索所有可用的DC（預設）。

   - `site`

     將DC探索限制在您的站台上。

   - `none`

     僅使用偏好的DC、而不執行探索。

新增偏好的 **ONTAP SMB** 網域控制站

透過DNS自動探索網域控制器。ONTAP或者、您可以將一個或多個網域控制器新增至特定網域的慣用網域控制器清單。

關於這項工作

如果指定網域的慣用網域控制器清單已經存在、則新清單會與現有清單合併。

步驟

1. 若要新增至偏好的網域控制站清單、請輸入下列命令：
   `vserver cifs domain preferred-dc add -vserver` *`vserver_name`* `-domain` *`domain_name`* `-preferred-dc IP_address, …+`

`-vserver vserver_name` 指定儲存虛擬機器（ SVM ）名稱。

`-domain domain_name` 指定指定網域控制站所屬之網域的完整 Active Directory 名稱。

`-preferred-dc IP_address`、 ... 依喜好設定順序，指定慣用網域控制站的一或多個 IP 位址，以逗號分隔的清單形式顯示。

範例

下列命令會將網域控制器172.17.102.25和172.17.102.24新增至SVM VS1上的SMB伺服器用來管理cifs.lab.example.com網域外部存取的慣用網域控制器清單。

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

相關資訊

管理慣用網域控制器的命令

用於管理偏好的 **SMB** 網域控制站的 **ONTAP** 命令

您需要知道用於新增、顯示及移除慣用網域控制器的命令。

如果您想要...	使用此命令...
新增慣用的網域控制器	`vserver cifs domain preferred-dc add`
顯示慣用的網域控制器	`vserver cifs domain preferred-dc show`
移除慣用的網域控制器	`vserver cifs domain preferred-dc remove`

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

相關資訊

新增慣用的網域控制器

啟用與 **ONTAP SMB** 網域控制站的加密連線

從ONTAP 功能表9.8開始、您可以指定要加密網域控制器的連線。

關於這項工作

ONTAP 需要加密網域控制站（ DC ）通訊 `-encryption-required-for-dc-connection` 選項設定為 `true`；預設值為 `false`。設定此選項時、只有SMb3傳輸協定會用於ONTAP-DC連線、因為只有SMb3才支援加密。

當需要加密的 DC 通訊時、 `-smb2-enabled-for-dc-connections` 選項會被忽略、因為 ONTAP 只會交涉 SMB3 連線。如果DC不支援SMB3和加密、ONTAP 則無法與之連線。

步驟

1. 啟用與 DC 的加密通訊： `vserver cifs security modify -vserver *svm_name* -encryption -required-for-dc-connection true`

使用null工作階段來存取非Kerberos環境中的儲存設備

使用 **ONTAP SMB null** 工作階段來存取非 **Kerberos** 環境中的儲存設備

null工作階段存取可提供網路資源（例如儲存系統資料）的權限、以及在本機系統下執行的用戶端型服務的權限。當用戶端程序使用「系統」帳戶存取網路資源時、就會發生null工作階段。null工作階段組態是專為非Kerberos驗證而設計。

瞭解 **ONTAP SMB** 儲存系統如何提供 **Null** 工作階段存取

由於null工作階段共用不需要驗證、因此需要null工作階段存取的用戶端必須在儲存系統上對應其IP位址。

根據預設、未對應的null工作階段用戶端可以存取某些ONTAP 功能不全的系統服務、例如共用列舉、但它們受到限制、無法存取任何儲存系統資料。

> ONTAP 支援使用選項的 Windows RestrictAnonymous 登錄設定值 `-restrict-anonymous`。這可讓您控制未對應的null使用者檢視或存取系統資源的程度。例如、您可以停用共用列舉並存取IPC$共用區（隱藏的命名管道共用區）。深入瞭解 `vserver cifs options modify`及 `vserver cifs options show `–restrict-anonymous`中的選項"指令參考資料ONTAP"。

除非另有設定、否則執行本機處理程序的用戶端透過null工作階段要求存取儲存系統、只是不受限制群組的成員、例如「'ee任何人'」。若要限制對所選儲存系統資源的null工作階段存取、您可能需要建立一個所有null工作階段用戶端所屬的群組；建立此群組可讓您限制儲存系統存取、並設定專屬於null工作階段用戶端的儲存系統資源權限。

ONTAP 在中提供對應語法 `vserver name-mapping` 命令集可指定允許使用 null 使用者工作階段存取儲存系統資源的用戶端 IP 位址。為null使用者建立群組之後、您可以針對僅適用於null工作階段的儲存系統資源和資源權限、指定存取限制。null使用者被識別為匿名登入。null使用者無法存取任何主目錄。

從對應IP位址存取儲存系統的任何null使用者、都會被授予對應的使用者權限。請考量適當的預防措施、以防止未獲授權存取與null使用者對應的儲存系統。為獲得最大保護、請將儲存系統和所有需要null使用者儲存系統存取的用戶端放在獨立的網路上、以避免IP位址「欺詐」的可能性。

相關資訊

設定匿名使用者的存取限制

授予 **null** 使用者存取 **ONTAP SMB** 檔案系統共用的權限

您可以指派一個群組供null工作階段用戶端使用、並記錄null工作階段用戶端的IP位址、以便新增至儲存系統允許使用null工作階段存取資料的用戶端清單、藉此允許null工作階段用戶端存取儲存系統資源。

步驟

1. 使用 `vserver name-mapping create` 命令，將 null 使用者對應至任何有效的 Windows 使用者，並提供 IP 辨識符號。

下列命令會將null使用者對應至具有有效主機名稱google.com的user1：

```
vserver name-mapping create -direction win-unix  -position 1 -pattern
"ANONYMOUS LOGON" -replacement user1 - hostname google.com
```

下列命令會將null使用者對應至具有有效IP位址10.238.2.54/32的user1：

```
vserver name-mapping create -direction win-unix  -position 2 -pattern
"ANONYMOUS LOGON" -replacement user1 -address 10.238.2.54/32
```

2. 使用 `vserver name-mapping show` 確認名稱對應的命令。

```
vserver name-mapping show

Vserver:   vs1
Direction: win-unix
Position Hostname         IP Address/Mask
-------- --------         ----------------
1       -                 10.72.40.83/32      Pattern: anonymous logon
                                          Replacement: user1
```

3. 使用 `vserver cifs options modify –win-name-for-null-user` 命令將 Windows 成員資格指派給 null 使用者。

此選項僅適用於具有null使用者有效名稱對應的情況。

```
vserver cifs options modify -win-name-for-null-user user1
```

4. 使用 `vserver cifs options show` 用於確認 null 使用者與 Windows 使用者或群組之間對應的命令。

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```

管理SMB伺服器的NetBios別名

瞭解如何管理 **ONTAP SMB** 伺服器的 **NetBios** 別名

NetBios別名是SMB伺服器的替代名稱、SMB用戶端可在連線至SMB伺服器時使用。當您

將其他檔案伺服器的資料整合到SMB伺服器、並希望SMB伺服器回應原始檔案伺服器的名稱時、設定SMB伺服器的NetBios別名很有用。

您可以在建立SMB伺服器時或建立SMB伺服器之後的任何時間、指定一個NetBios別名清單。您可以隨時從清單中新增或移除NetBios別名。您可以使用NetBios別名清單中的任何名稱連線至SMB伺服器。

相關資訊

顯示有關TCP連線上的NetBios資訊

將 **NetBios** 別名清單新增至 **ONTAP SMB** 伺服器

如果您希望SMB用戶端使用別名連線到SMB伺服器、您可以建立一份NetBios別名清單、或是將NetBios別名新增到現有的NetBios別名清單。

關於這項工作

- NetBios別名長度最多可為15個字元。
- 您最多可以在SMB伺服器上設定200個NetBios別名。
- 不允許使用下列字元：

  @ # * （） = + [ ] | ； ： " 、 < > \ / ？

步驟

1. 新增 NetBIOS 別名：
   `vserver cifs add-netbios-aliases -vserver vserver_name -netbios-aliases NetBIOS_alias,…`

   ```
   vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases
   alias_1,alias_2,alias_3
   ```

   - 您可以使用以逗號分隔的清單來指定一或多個NetBios別名。
   - 指定的NetBios別名會新增至現有清單。
   - 如果清單目前空白、則會建立新的NetBios別名清單。
2. 確認已正確新增 NetBIOS 別名：`vserver cifs show -vserver vserver_name -display -netbios-aliases`

   ```
   vserver cifs show -vserver vs1 -display-netbios-aliases
   ```

   ```
   Vserver: vs1

            Server Name: CIFS_SERVER
            NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
   ```

相關資訊

- 從 SMB 伺服器清單中刪除 NetBIOS 別名

- 顯示 SMB 伺服器的 NetBIOS 別名列表

從 **ONTAP SMB** 伺服器清單中移除 **NetBIOS** 別名

如果您不需要CIFS伺服器的特定NetBios別名、可以從清單中移除這些NetBios別名。您也可以從清單中移除所有的NetBios別名。

關於這項工作

您可以使用以逗號分隔的清單來移除多個NetBios別名。您可以透過指定來移除 CIFS 伺服器上的所有 NetBIOS 別名 - 做為的值 `-netbios-aliases` 參數。

步驟

1. 執行下列其中一項動作：

如果您要移除...	輸入...
清單中的特定NetBios別名	`vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios -aliases _NetBIOS_alias_,...`
清單中的所有NetBios別名	`vserver cifs remove-netbios-aliases -vserver vserver_name -netbios-aliases -`

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
```

2. 確認已移除指定的 NetBIOS 別名：`vserver cifs show -vserver vserver_name -display -netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_2, ALIAS_3
```

顯示 **ONTAP SMB** 伺服器的 **NetBios** 別名清單

您可以顯示NetBios別名清單。當您想要判斷SMB用戶端可連線至CIFS伺服器的名稱清單時、這項功能很實用。

步驟

1. 執行下列其中一項動作：

如果您想要顯示有關...的資訊	輸入...
CIFS伺服器的NetBios別名	`vserver cifs show -display-netbios -aliases`
詳細CIFS伺服器資訊的一部分是NetBios別名清單	`vserver cifs show -instance`

下列範例顯示CIFS伺服器的NetBios別名相關資訊：

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

下列範例顯示詳細CIFS伺服器資訊的一部分是NetBios別名清單：

```
vserver cifs show -instance
```

```
                                        Vserver: vs1
                      CIFS Server NetBIOS Name: CIFS_SERVER
                  NetBIOS Domain/Workgroup Name: EXAMPLE
                    Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                         Authentication Style: domain
              CIFS Server Administrative Status: up
                        CIFS Server Description:
                        List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

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

相關資訊

- 向伺服器新增 NetBIOS 別名列表
- 管理伺服器的命令

判斷 **ONTAP SMB** 用戶端是否使用 **NetBIOS** 別名連線

您可以判斷SMB用戶端是否使用NetBios別名進行連線、如果是、則會使用哪個NetBios別名進行連線。這在疑難排解連線問題時很有用。

關於這項工作

您必須使用 `-instance` 顯示與 SMB 連線相關聯的 NetBIOS 別名（如果有）的參數。如果使用 CIFS 伺服器名

稱或 IP 位址建立 SMB 連線、則會輸出 `NetBIOS Name` 欄位為 - （連字號）。

步驟

1. 執行所需的動作：

如果您要顯示下列項目的**NetBios**資訊...	輸入...
SMB 連線	`vserver cifs session show -instance`
使用指定的NetBios別名的連線：	`vserver cifs session show -instance -netbios-name` *`netbios_name`*

下列範例顯示使用工作階段ID 1建立SMB連線所用的NetBios別名資訊：

```
vserver cifs session show -session-id 1 -instance
```

```
                          Node: node1
                       Vserver: vs1
                    Session ID: 1
                 Connection ID: 127834
 Incoming Data LIF IP Address: 10.1.1.25
                   Workstation: 10.2.2.50
     Authentication Mechanism: NTLMv2
                 Windows User: EXAMPLE\user1
                    UNIX User: user1
                  Open Shares: 2
                   Open Files: 2
                   Open Other: 0
                Connected Time: 1d 1h 10m 5s
                     Idle Time: 22s
            Protocol Version: SMB3
       Continuously Available: No
            Is Session Signed: true
        User Authenticated as: domain-user
                  NetBIOS Name: ALIAS1
        SMB Encryption Status: Unencrypted
```

管理各種**SMB**伺服器工作

停止或啟動 **ONTAP SMB** 伺服器

您可以停止SVM上的CIFS伺服器、這在使用者無法透過SMB共用存取資料時、在執行工作時很有用。您可以啟動CIFS伺服器來重新啟動SMB存取。停止CIFS伺服器之後、您也可以修改儲存虛擬機器（SVM）上允許的傳輸協定。

步驟

1. 執行下列其中一項動作：

如果您想要...	輸入命令...
停止CIFS伺服器	`vserver cifs stop -vserver *vserver_name* [-foreground {true
false}]`	啟動CIFS伺服器
`vserver cifs start -vserver *vserver_name* [-foreground {true	false}]`

`-foreground` 指定命令應在前景或背景執行。如果您未輸入此參數、則會將其設為 `true`，命令將在前臺執行。

2. 使用驗證 CIFS 伺服器管理狀態是否正確 `vserver cifs show` 命令。

範例

下列命令會在SVM VS1上啟動CIFS伺服器：

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: VS1
                    NetBIOS Domain/Workgroup Name: DOMAIN
                      Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
```

相關資訊

- 顯示探索到的伺服器相關資訊
- 重設並重新探索伺服器

將 **ONTAP SMB** 伺服器移至不同的 **OU**

除非您指定不同的OU、否則CIFS伺服器建立程序會在設定期間使用預設的組織單位（OU）CN=電腦。您可以在設定後將CIFS伺服器移至不同的OU。

步驟

1. 在Windows伺服器上、開啟「* Active Directory使用者與電腦*」樹狀結構。
2. 找出儲存虛擬機器（SVM）的Active Directory物件。

3. 在物件上按一下滑鼠右鍵、然後選取*移動*。
4. 選取您要與SVM建立關聯的OU

結果

SVM物件會放置在選取的OU中。

在移動 **ONTAP SMB** 伺服器之前，請先修改動態 **DNS** 網域

如果您想要Active Directory整合式DNS伺服器在將SMB伺服器移至其他網域時、在DNS中動態登錄SMB伺服器的DNS記錄、則必須先修改儲存虛擬機器（SVM）上的動態DNS（DDNS）、才能移動SMB伺服器。

開始之前

必須在SVM上修改DNS名稱服務、才能使用DNS網域、其中包含將包含SMB伺服器電腦帳戶之新網域的服務位置記錄。如果您使用的是安全的DDNS、則必須使用Active Directory整合的DNS名稱伺服器。

關於這項工作

雖然DDNS（如果在SVM上設定）會自動將資料LIF的DNS記錄新增至新網域、但原始網域的DNS記錄不會自動從原始DNS伺服器刪除。您必須手動刪除。

若要在移動SMB伺服器之前完成DDNS修改、請參閱下列主題：

"設定動態DNS服務"

將 **ONTAP SMB SVM** 加入 **Active Directory** 網域

您可以使用修改網域、將儲存虛擬機器（ SVM ）加入 Active Directory 網域、而無需刪除現有的 SMB 伺服器 `vserver cifs modify` 命令。您可以重新加入目前的網域、或加入新的網域。

開始之前

- SVM必須已有DNS組態。
- SVM的DNS組態必須能夠為目標網域提供服務。

  DNS伺服器必須包含網域LDAP和網域控制器伺服器的服務位置記錄（SRV),

關於這項工作

- CIFS 伺服器的管理狀態必須設為 `down`，才能繼續 Active Directory 網域修改。
- 如果命令成功完成，管理狀態會自動設定為 `up`。如"指令參考資料ONTAP"需詳細 `up`資訊，請參閱。
- 加入網域時、此命令可能需要幾分鐘的時間才能完成。

步驟

1. 將 SVM 加入 CIFS 伺服器網域： `vserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`* `-status-admin down`

   如"指令參考資料ONTAP"需詳細 `vserver cifs modify`資訊，請參閱。如果您需要重新設定新網域的 DNS ，

請在中深入瞭解 `vserver dns modify`"指令參考資料ONTAP"。

若要為 SMB 伺服器建立 Active Directory 機器帳戶、您必須提供具有足夠權限的 Windows 帳戶名稱和密碼、以便將電腦新增至 `ou= example ou` 中的容器 *example*.com 網域。

從ONTAP 功能更新9.7開始、AD管理員可以提供Keytab檔案的URI、作為提供權限Windows帳戶名稱和密碼的替代方案。當您收到 URI 時、請將其加入 `-keytab-uri` 參數 `vserver cifs` 命令。

2. 確認 CIFS 伺服器位於所需的 Active Directory 網域： `vserver cifs show`

範例

在下列範例中、SVM VS1上的SMB伺服器「'CIFSSERVER1'」會使用Keytab驗證加入example.com網域：

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab

cluster1::> vserver cifs show

          Server       Status       Domain/Workgroup  Authentication
Vserver   Name         Admin        Name              Style
--------- -----------  ---------    ----------------  --------------
vs1       CIFSSERVER1  up           EXAMPLE           domain
```

顯示 **ONTAP SMB NetBios over TCP** 連線的相關資訊

您可以顯示有關TCP上的NetBios（NBT）連線的資訊。這在疑難排解與NetBios相關的問題時很有用。

步驟

1. 使用 `vserver cifs nbtstat` 顯示關於 TCP 連線上的 NetBIOS 資訊的命令。

> 不支援透過IPv6提供的NetBios名稱服務（NBNS）。

範例

以下範例顯示「'cluster1'」的NetBios名稱服務資訊：

```
cluster1::> vserver cifs nbtstat

          Vserver: vs1
          Node:    cluster1-01
          Interfaces:
                   10.10.10.32
                   10.10.10.33
         Servers:
                   17.17.1.2  (active  )
         NBT Scope:
                  [ ]
         NBT Mode:
                  [h]
         NBT Name    NetBIOS Suffix   State   Time Left   Type
         ----------- ---------------  ------- ---------   -----
         CLUSTER_1   00               wins    57
         CLUSTER_1   20               wins    57

         Vserver: vs1
         Node:    cluster1-02
         Interfaces:
                 10.10.10.35
         Servers:
                 17.17.1.2  (active  )
         CLUSTER_1           00               wins          58
         CLUSTER_1           20               wins          58
         4 entries were displayed.
```

用於管理 **SMB** 伺服器的 **ONTAP** 命令

您需要知道建立、顯示、修改、停止、啟動、 和刪除SMB伺服器。也有命令可重設和重新探索伺服器、變更或重設機器帳戶密碼、排程機器帳戶密碼變更、以及新增或移除NetBios別名。

如果您想要...	使用此命令...
建立 SMB 伺服器	`vserver cifs create`
顯示SMB伺服器的相關資訊	`vserver cifs show`
修改 SMB 伺服器	`vserver cifs modify`
將SMB伺服器移至其他網域	`vserver cifs modify`

停止SMB伺服器	`vserver cifs stop`
啟動SMB伺服器	`vserver cifs start`
刪除 SMB 伺服器	`vserver cifs delete`
重設並重新探索SMB伺服器的伺服器	`vserver cifs domain discovered-servers reset-servers`
變更SMB伺服器的機器帳戶密碼	`vserver cifs domain password change`
重設SMB伺服器的機器帳戶密碼	`vserver cifs domain password change`
排程SMB伺服器機器帳戶的自動密碼變更	`vserver cifs domain password schedule modify`
新增SMB伺服器的NetBios別名	`vserver cifs add-netbios-aliases`
移除SMB伺服器的NetBios別名	`vserver cifs remove-netbios-aliases`

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

相關資訊

"刪除 SMB 伺服器時、本機使用者和群組會發生什麼情況"

啟用 **ONTAP SMB NetBios** 名稱服務

從ONTAP 功能更新開始、預設會停用NetBios名稱服務（NBNS、有時稱為Windows網際網路名稱服務或WINS）。先前、不論網路上是否啟用了WINS、均會傳送名稱登錄廣播給啟用CIFS的儲存虛擬機器（SVM）。若要將此類廣播限制在需要NBNS的組態、您必須針對新的CIFS伺服器明確啟用NBNS。

開始之前

- 如果您已經使用NBNS並升級ONTAP 至版本S9、則不需要完成此工作。NBNS將繼續如以往一樣運作。
- 透過udp（連接埠137）啟用NBNS。
- 不支援透過IPv6的NBNS。

步驟

1. 將權限層級設為進階。

```
set -privilege advanced
```

2. 在CIFS伺服器上啟用NBNS。

```
vserver cifs options  modify -vserver <vserver name> -is-nbns-enabled
true
```

3. 返回管理權限層級。

```
set -privilege admin
```

使用IPv6進行SMB存取和SMB服務

瞭解 ONTAP 的 IPv6 SMB 需求

在SMB伺ONTAP 服器上使用IPv6之前、您必須先知道哪些版本的支援哪些版本的支援、以及授權需求為何。

不含授權需求ONTAP

取得SMB授權時、IPv6不需要特殊授權。SMB 授權隨附於"ONTAP One"。如果您沒有 ONTAP One 且未安裝授權、請聯絡您的銷售代表。

SMB傳輸協定版本需求

- 對於SVM、ONTAP 支援所有SMB傳輸協定版本上的IPv6。

> 不支援透過IPv6提供的NetBios名稱服務（NBNS）。

瞭解支援 ONTAP SMB 存取和 CIFS 服務的 IPv6

如果您想要在CIFS伺服器上使用IPv6、您必須瞭解ONTAP 如何支援使用IPv6進行SMB存取、以及使用網路通訊來進行CIFS服務。

Windows用戶端與伺服器支援

支援支援IPv6的Windows伺服器和用戶端。ONTAP以下說明Microsoft Windows用戶端和伺服器IPv6支援：

- Windows 7、Windows 8、Windows Server 2008、Windows Server 2012及更新版本均支援IPv6用於SMB檔案共用及Active Directory服務、包括DNS、LDAP、CLDAP及Kerberos服務。

  如果設定IPv6位址、Windows 7和Windows Server 2008及更新版本預設會使用IPv6來執行Active Directory服務。支援透過IPv6連線進行的NTLM和Kerberos驗證。

  支援的所有Windows用戶端ONTAP 都可以使用IPv6位址連線至SMB共用區。

如需 Windows 用戶端 ONTAP 支援的最新資訊、請參閱 "互通性對照表"。

> IPv6不支援NT網域。

額外的**CIFS**服務支援

除了IPv6支援SMB檔案共用和Active Directory服務之外、ONTAP 支援下列項目的功能還包括：

- 用戶端服務、包括離線資料夾、漫遊設定檔、資料夾重新導向及舊版
- 伺服器端服務、包括動態主目錄（主目錄功能）、symlink和Widgelinks、BranchCache、ODX複本卸載、自動節點參照、 和舊版
- 檔案存取管理服務、包括使用Windows本機使用者和群組進行存取控制和權限管理、使用CLI設定檔案權限和稽核原則、安全追蹤、檔案鎖定管理、以及監控SMB活動
- NAS多重傳輸協定稽核
- FPolicy
- 持續可用的共享區、見證傳輸協定及遠端VSS（搭配SMB上的Hyper-V組態使用）

名稱服務與驗證服務支援

IPv6支援與下列名稱服務的通訊：

- 網域控制器
- DNS伺服器
- LDAP 伺服器
- Kdc伺服器
- NIS 伺服器

瞭解 **ONTAP SMB** 伺服器如何使用 **IPv6** 連線至外部伺服器

若要建立符合需求的組態、您必須瞭解CIFS伺服器在連線至外部伺服器時如何使用IPv6。

- 來源位址選擇

  如果嘗試連線至外部伺服器、則選取的來源位址必須與目的地位址的類型相同。例如、如果連線至IPv6位址、則託管CIFS伺服器的儲存虛擬機器（SVM）必須具有IPv6位址的資料LIF或管理LIF、才能作為來源位址。同樣地、如果連線至IPV4位址、SVM必須具有資料LIF或管理LIF、且該資料具有可作為來源位址的IPV4位址。

- 對於使用DNS動態探索的伺服器、伺服器探索的執行方式如下：
  - 如果叢集上停用IPv6、則只會探索到IPv6伺服器位址。
  - 如果叢集上已啟用IPv6、則會同時探索IPv4和IPv6伺服器位址。視位址所屬伺服器的適用性、以及IPv6或IPv4資料或管理生命期的可用度而定、可能會使用這兩種類型。 動態伺服器探索可用於探索網域控制器及其相關服務、例如LSA、NETLOGON、Kerberos及LDAP。
- DNS伺服器連線能力

  SVM在連線至DNS伺服器時是否使用IPv6、取決於DNS名稱服務組態。如果DNS服務設定為使用IPv6位址、則會使用IPv6建立連線。如果需要、DNS名稱服務組態可以使用IPV4位址、讓DNS伺服器的連線繼續使用IPV4位址。設定DNS名稱服務時、可以指定同時使用的IPv6位址和IPv6位址。

- LDAP 伺服器連線

SVM在連線至LDAP伺服器時是否使用IPv6、取決於LDAP用戶端組態。如果LDAP用戶端設定為使用IPv6位址、則會使用IPv6建立連線。如果需要、LDAP用戶端組態可以使用IPv4位址、以便連線至LDAP伺服器、繼續使用IPv4位址。設定LDAP用戶端組態時、可指定IPv6位址的組合。

LDAP用戶端組態用於設定LDAP以供UNIX使用者、群組及netgroup名稱服務使用。

- NIS 伺服器連線

  SVM 連線至 NIS 伺服器時是否使用 IPv6 、取決於 NIS 名稱服務組態。如果 NIS 服務設定為使用 IPv6 位址、則會使用 IPv6 進行連線。如果需要、NIS名稱服務組態可以使用IPv4位址、以便連線至NIS伺服器時、繼續使用IPv4位址。設定NIS名稱服務時、可指定IPv6位址的組合。

  NIS名稱服務用於儲存及管理UNIX使用者、群組、netgroup及主機名稱物件。

相關資訊

- 為伺服器啟用 IPv6
- 監控並顯示有關 IPv6 會話的信息

啟用 **ONTAP SMB** 伺服器的 **IPv6**

在叢集設定期間、不會啟用IPv6網路。叢集管理員必須在完成叢集設定之後啟用IPv6、才能將IPv6用於SMB。當叢集管理員啟用IPv6時、會為整個叢集啟用IPv6。

步驟

1. 啟用 IPv6 ： `network options ipv6 modify -enabled true`

   IPv6已啟用。可設定用於SMB存取的IPv6資料生命量。

相關資訊

- 監控並顯示有關 IPv6 會話的信息
- "使用 System Manager 視覺化網路"
- "在叢集上啟用 IPv6"
- "網路選項IPv6修改"

瞭解如何停用 **ONTAP SMB** 伺服器的 **IPv6**

即使使用網路選項在叢集上啟用IPv6、您仍無法使用相同的命令來停用SMB的IPv6。而ONTAP 當叢集管理員停用叢集上最後啟用IPv6的介面時、則會停用IPv6。您應該與叢集管理員溝通、瞭解如何管理啟用IPv6的介面。

相關資訊

- "使用系統管理員視覺化 ONTAP 網路"

監控及顯示 **IPv6 ONTAP SMB** 工作階段的相關資訊

您可以監控及顯示使用IPv6網路連線的SMB工作階段相關資訊。此資訊可用於判斷哪些用戶端使用IPv6連線、以及其他有關IPv6 SMB工作階段的實用資訊。

步驟

1. 執行所需的動作：

如果您想要判斷...	輸入命令...
儲存虛擬機器（SVM）的SMB工作階段會使用IPv6連線	`vserver cifs session show -vserver vserver_name -instance`
IPv6用於透過指定LIF位址進行SMB工作階段	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address -instance` *LIF_IP_address* 為資料 LIF 的 IPv6 位址。

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`
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*`

> ℹ `-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`

如果您想要多網域名稱對應搜尋...	輸入命令...
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>`

如果您想要使用...來設定**ACL**	輸入命令...
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」。
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。

功能	註解
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`
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
```

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

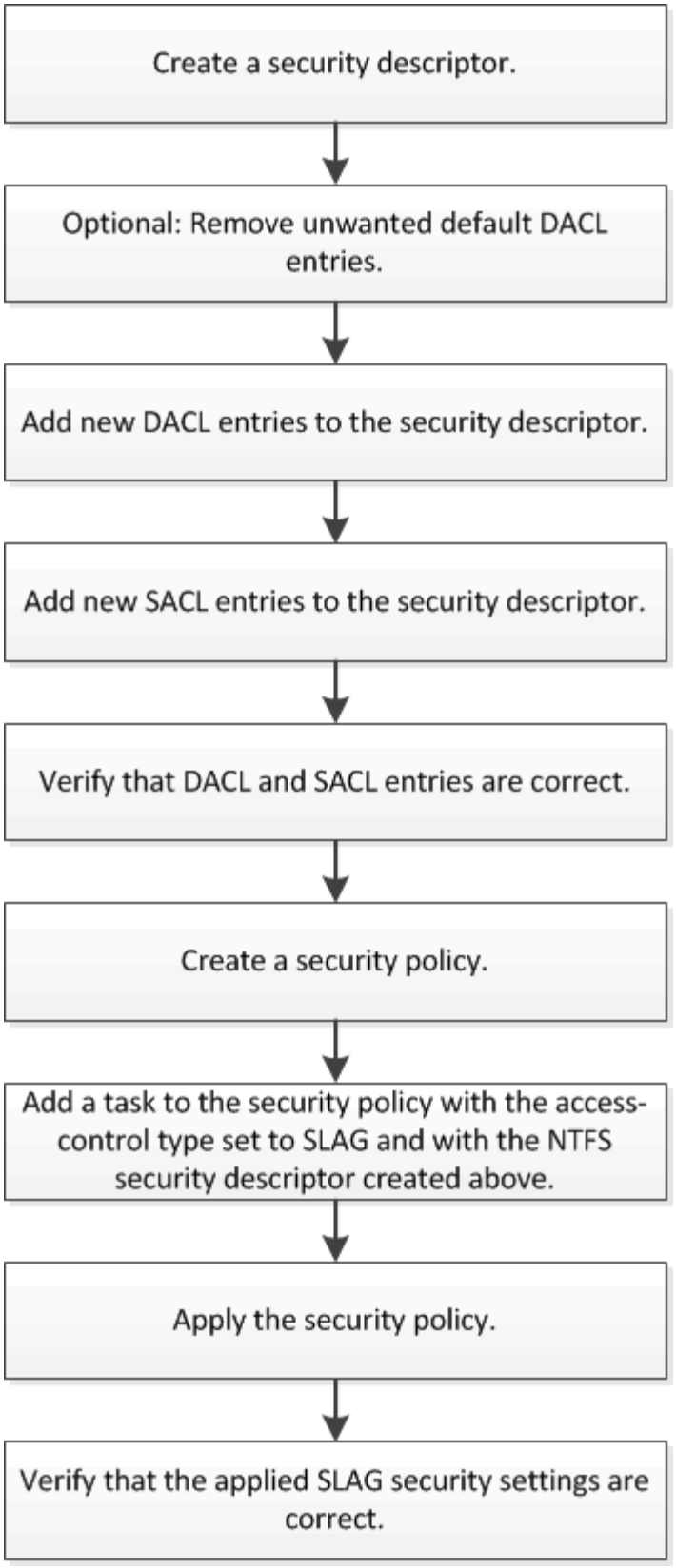
儲存層級的存取保護功能可在儲存層級提供額外的安全性、從用戶端看不到；因此、任何使用者或系統管理員都無法從其桌面撤銷。在某些使用案例中、在儲存層級控制存取的能力是有益的。

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（**AFFS**）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
```

使用SMB管理檔案存取

使用本機使用者和群組進行驗證和授權

如何使用本機使用者和群組ONTAP

了解本機 ONTAP SMB 使用者和群組

您應該先知道哪些是本機使用者和群組、以及這些使用者和群組的一些基本資訊、然後再決定是否要在環境中設定及使用本機使用者和群組。

- 本機使用者

  具有唯一安全性識別碼（SID）的使用者帳戶、只有在建立該帳戶的儲存虛擬機器（SVM）上才具有可見度。本機使用者帳戶具有一組屬性、包括使用者名稱和SID。本機使用者帳戶會使用NTLM驗證、在CIFS伺服器上進行本機驗證。

  使用者帳戶有多種用途：

  - 用於授予_使用者權限管理_權限給使用者。
  - 用於控制SVM擁有之檔案和資料夾資源的共用層級和檔案層級存取。

- 本機群組

具有唯一SID的群組只能在建立該群組的SVM上看到。群組包含一組成員。成員可以是本機使用者、網域使用者、網域群組和網域機器帳戶。可以建立、修改或刪除群組。

群組有多種用途：

- 用於授予_使用者權限管理_權限給其成員。
- 用於控制SVM擁有之檔案和資料夾資源的共用層級和檔案層級存取。

- 本機網域

  具有本機範圍的網域、受SVM限制。本機網域名稱為CIFS伺服器名稱。本機使用者和群組包含在本機網域內。

- 安全性識別碼（**SID**）

  SID是可識別Windows型安全性主體的可變長度數值。例如、一般的SID格式如下：s-1-5-21-3136354847-3130905135-2517279418-123456。

- * NTLM驗證*

  一種Microsoft Windows安全性方法、用於驗證CIFS伺服器上的使用者。

- 叢集複寫資料庫（**RDB**）

  叢集中每個節點上都有執行個體的複寫資料庫。本機使用者和群組物件會儲存在RDB中。

建立本機 **ONTAP SMB** 使用者和本機群組的原因

在您的儲存虛擬機器（SVM）上建立本機使用者和本機群組的理由有好幾種。例如、如果網域控制器（DC）無法使用、您可能想要使用本機群組來指派權限、或SMB伺服器位於工作群組中、您可以使用本機使用者帳戶來存取SMB伺服器。

您可以基於下列理由建立一或多個本機使用者帳戶：

- 您的SMB伺服器位於工作群組中、網域使用者無法使用。

  工作群組組組態需要本機使用者。

- 如果網域控制器無法使用、您希望能夠驗證並登入SMB伺服器。

  本機使用者可以在網域控制器當機或網路問題使SMB伺服器無法連絡網域控制器時、使用NTLM驗證來驗證SMB伺服器。

- 您想要指派_使用者權限管理_權限給本機使用者。

  _使用者權限管理_是SMB伺服器管理員控制使用者和群組在SVM上擁有哪些權限的能力。您可以將權限指派給使用者帳戶、或是將使用者設為具有這些權限的本機群組成員、藉此指派權限給使用者。

您可以基於下列理由建立一或多個本機群組：

- 您的SMB伺服器位於工作群組中、而且網域群組無法使用。

工作群組組組態不需要本機群組、但這些群組對於管理本機工作群組使用者的存取權限非常有用。

- 您想要使用本機群組來控制檔案和資料夾資源的存取、以進行共用和檔案存取控制。
- 您想要使用自訂的_使用者權限管理_權限來建立本機群組。

  某些內建使用者群組具有預先定義的權限。若要指派一組自訂的權限、您可以建立本機群組、並將必要的權限指派給該群組。然後您可以將本機使用者、網域使用者和網域群組新增至本機群組。

相關資訊

- 了解本地用戶身份驗證
- 支援的權限清單

了解本機 **ONTAP SMB** 使用者身份驗證

本機使用者必須先建立已驗證的工作階段、才能存取CIFS伺服器上的資料。

由於SMB是以工作階段為基礎、因此在第一次設定工作階段時、只要確定一次使用者身分即可。CIFS伺服器在驗證本機使用者時、會使用以NTLM為基礎的驗證。支援「位在位在位在位在位在位」的「位在位

在三種使用案例下使用本機驗證。ONTAP每個使用案例取決於使用者名稱的網域部分（使用網域\使用者格式）是否符合CIFS伺服器的本機網域名稱（CIFS伺服器名稱）：

- 網域部分相符

  在要求存取資料時提供本機使用者認證的使用者、會在CIFS伺服器本機驗證。

- 網域部分不符

  嘗試在CIFS伺服器所屬網域中的網域控制器上使用NTLM驗證。ONTAP如果驗證成功、登入即告完成。如果驗證失敗、接下來的情況取決於驗證失敗的原因。

  例如、如果使用者存在於Active Directory中、但密碼無效或過期、ONTAP 則無法嘗試在CIFS伺服器上使用對應的本機使用者帳戶。而是驗證失敗。有些情況ONTAP 下、即使有CIFS伺服器上的對應本機帳戶存在、也會使用該帳戶進行驗證、即使這些NetBios網域名稱不相符。例如、如果存在相符的網域帳戶、但該帳戶已停用、ONTAP 則會使用CIFS伺服器上對應的本機帳戶進行驗證。

- 未指定網域部分

  以本機使用者身分先嘗試驗證。ONTAP如果本機使用者驗證失敗、ONTAP 則由CIFS伺服器所屬網域中的網域控制器來驗證使用者。

成功完成本機或網域使用者驗證後ONTAP 、將會建構完整的使用者存取權杖、並將本機群組成員資格和權限納入考量。

如需本機使用者的NTLM驗證詳細資訊、請參閱Microsoft Windows文件。

相關資訊

在伺服器上啟用或停用本機使用者身份驗證

了解 **ONTAP SMB** 使用者存取權令牌

當使用者對應共用時、會建立已驗證的SMB工作階段、並建構使用者存取權杖、其中包含使用者、使用者群組成員資格和累積權限、以及對應的UNIX使用者的相關資訊。

除非停用此功能、否則本機使用者和群組資訊也會新增至使用者存取權杖。存取權杖的建構方式取決於登入是針對本機使用者還是Active Directory網域使用者：

- 本機使用者登入

  雖然本機使用者可以是不同本機群組的成員、但本機群組不能是其他本機群組的成員。本機使用者存取權杖是由指派給特定本機使用者所屬群組的所有權限聯合所組成。

- 網域使用者登入

  當網域使用者登入時ONTAP 、即可取得使用者存取權杖、其中包含使用者所屬之所有網域群組的使用者ID和SID。使用網域使用者存取權杖的聯合、搭配使用者網域群組的本機成員資格（若有）所提供的存取權杖、以及指派給網域使用者或其任何網域群組成員資格的任何直接權限。ONTAP

對於本機和網域使用者登入、也會針對使用者存取權杖設定主要群組RID。預設 RID 為 `Domain Users` （ RID 513 ）。您無法變更預設值。

Windows對UNIX和UNIX對Windows名稱對應程序、對本機和網域帳戶都遵循相同的規則。

> 從UNIX使用者到本機帳戶並無暗示的自動對應。如果需要、則必須使用現有的名稱對應命令來指定明確的對應規則。

了解如何在包含本機群組的 **ONTAP SMB SVM** 上使用 **SnapMirror**

在包含本機群組的SVM所擁有的磁碟區上設定SnapMirror時、您應該瞭解相關準則。

您無法使用應用到SnapMirror複寫到另一個SVM之檔案、目錄或共用的ACE中的本機群組。如果您使用SnapMirror功能在另一個SVM上建立磁碟區的DR鏡像、而該磁碟區有一個用於本機群組的ACE、則該ACE在鏡射上無效。如果將資料複寫到不同的SVM、資料就會有效地跨入不同的本機網域。授予本機使用者和群組的權限僅在最初建立的SVM範圍內有效。

了解刪除 **ONTAP SMB** 伺服器對使用者和群組的影響

預設的本機使用者和群組集是在建立CIFS伺服器時建立、並與託管CIFS伺服器的儲存虛擬機器（SVM）建立關聯。SVM管理員可以隨時建立本機使用者和群組。刪除CIFS伺服器時、您必須瞭解本機使用者和群組的情況。

本機使用者和群組與SVM相關聯、因此在刪除CIFS伺服器時、不會因為安全考量而刪除它們。雖然在刪除CIFS伺服器時不會刪除本機使用者和群組、但它們會隱藏起來。在SVM上重新建立CIFS伺服器之前、您無法檢視或管理本機使用者和群組。

> CIFS伺服器管理狀態不會影響本機使用者或群組的可見度。

了解如何將 **Microsoft** 管理主控台與本機 **ONTAP SMB** 使用者和群組結合使用

您可以從Microsoft管理主控台檢視本機使用者和群組的相關資訊。有了這個版本ONTAP的功能、您就無法從Microsoft管理主控台為本機使用者和群組執行其他管理工作。

了解如何恢復 **ONTAP SMB** 叢集

如果您計畫將叢集還原至ONTAP 不支援本機使用者和群組的支援版本、以及本機使用者和群組用於管理檔案存取或使用者權限、則必須注意某些考量。

- 基於安全考量、當ONTAP 將設定的本機使用者、群組和權限資訊還原至不支援本機使用者和群組功能的版本時、不會刪除這些資訊。
- 還原至ONTAP 舊版的主要版本時ONTAP 、在驗證和認證建立期間、不使用本地使用者和群組。
- 本機使用者和群組不會從檔案和資料夾ACL中移除。
- 由於授予本機使用者或群組權限、因此會拒絕視存取權限而定的檔案存取要求。

  若要允許存取、您必須重新設定檔案權限、以根據網域物件而非本機使用者和群組物件來允許存取。

什麼是本機權限

受支援的 **ONTAP SMB** 權限列表

支援的權限已預先定義。ONTAP某些預先定義的本機群組預設會新增其中一些權限。您也可以從預先定義的群組新增或移除權限、或建立新的本機使用者或群組、並新增權限至您所建立的群組、或新增至現有的網域使用者和群組。

下表列出儲存虛擬機器（SVM）上支援的權限、並提供具有指派權限的BUILTIN群組清單：

權限名稱	預設安全性設定	說明
`SeTcbPrivilege`	無	做為作業系統的一部分
`SeBackupPrivilege`	`BUILTIN\Administrators`、`BUILTIN\Backup Operators`	備份檔案和目錄、覆寫任何ACL
`SeRestorePrivilege`	`BUILTIN\Administrators`、`BUILTIN\Backup Operators`	還原檔案和目錄、覆寫任何ACL、將任何有效的使用者或群組SID設為檔案擁有者
`SeTakeOwnershipPrivilege`	`BUILTIN\Administrators`	取得檔案或其他物件的擁有權
`SeSecurityPrivilege`	`BUILTIN\Administrators`	管理稽核 這包括檢視、卸載及清除安全性記錄。

權限名稱	預設安全性設定	說明
SeChangeNotifyPrivilege	BUILTIN\Administrators、BUILTIN\Backup Operators、BUILTIN\Power Users、BUILTIN\Users、Everyone	略過周遊檢查 具有此權限的使用者不需要具有周遊（x）權限、即可周遊資料夾、符號連結或交叉路口。

相關資訊

- 了解如何分配權限
- 了解如何配置繞過遍歷檢查

了解如何指派 **ONTAP SMB** 權限

您可以直接將權限指派給本機使用者或網域使用者。或者、您也可以將使用者指派給本機群組、其指派的權限與您希望這些使用者擁有的功能相符。

- 您可以將一組權限指派給所建立的群組。

  接著、您可以將擁有該使用者所擁有權限的使用者新增至群組。

- 您也可以將本機使用者和網域使用者指派給預先定義的群組、這些群組的預設權限與您要授予這些使用者的權限相符。

相關資訊

- 新增權限給本機或網域使用者或群組
- 移除本機或網域使用者或群組的權限
- 重設本機或網域使用者和群組的權限
- 了解如何配置繞過遍歷檢查

了解 **ONTAP SMB** 伺服器上的 **BUILTIN** 群組和本機管理員帳戶

當您使用BUILTIN群組和本機系統管理員帳戶時、請謹記以下幾項準則。例如、您可以重新命名本機系統管理員帳戶、但無法刪除此帳戶。

- 系統管理員帳戶可以重新命名、但無法刪除。
- 系統管理員帳戶無法從BUILTIN\Administrator群組中移除。
- 可以重新命名內建群組、但無法刪除。

  在重新命名BUILTIN群組之後、可以使用已知名稱建立另一個本機物件、但會指派新的RID給該物件。

- 沒有本機來賓帳戶。

相關資訊

預先定義的BUILTIN群組和預設權限

本地 ONTAP SMB 使用者密碼要求

根據預設、本機使用者密碼必須符合複雜度要求。密碼複雜度需求與Microsoft Windows本地安全策略_中定義的要求類似。

密碼必須符合下列條件：

- 長度必須至少六個字元
- 不得包含使用者帳戶名稱
- 必須包含下列四種類別中至少三種的字元：
  - 英文大寫字元（A到Z）
  - 英文小寫字元（a到z）
  - 基礎10位數（0到9）
  - 特殊字元：

```
~ ! @ # $ % {caret} & * _ - + = ` \ | ( ) [ ] : ; " ' < > , . ? /
```

相關資訊

- 設定本地用戶的密碼複雜度
- 顯示有關伺服器安全設定的信息
- 變更本機使用者帳戶密碼

預先定義的 BUILTIN 群組和預設 ONTAP SMB 權限

您可以將本機使用者或網域使用者的成員資格指派給ONTAP 由供應的一組預先定義的BUILTIN群組。預先定義的群組已指派預先定義的權限。

下表說明預先定義的群組：

預先定義的BUILTIN群組	預設權限
`BUILTIN\Administrators`RID 544 第一次建立時、即為本機 `Administrator` 帳戶（ RID 為 500 ）會自動成為此群組的成員。當儲存虛擬機器（ SVM ）加入網域時 `domain\Domain Admins` 群組即會新增至群組。如果 SVM 離開網域、則為 `domain\Domain Admins` 群組即會從群組中移除。	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`

預先定義的**BUILTIN**群組	預設權限
`BUILTIN\Power Users`RID 547 第一次建立時、此群組沒有任何成員。此群組成員具有下列特性： • 可建立及管理本機使用者和群組。 • 無法將自己或任何其他物件新增至 `BUILTIN\Administrators` 群組：	`SeChangeNotifyPrivilege`
`BUILTIN\Backup Operators`RID 551. 第一次建立時、此群組沒有任何成員。如果是以備份目的開啟檔案或資料夾、則此群組的成員可以覆寫其讀取和寫入權限。	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Users`RID 545 第一次建立時、此群組沒有任何成員（隱含的除外）`Authenticated Users` 特殊群組）。當 SVM 加入網域時 `domain\Domain Users` 群組隨即新增至此群組。如果 SVM 離開網域、則為 `domain\Domain Users` 群組已從此群組中移除。	`SeChangeNotifyPrivilege`
`Everyone`SID S-1-1-0 此群組包括所有使用者、包括來賓（但非匿名使用者）。這是暗示的群組、具有暗示的成員資格。	`SeChangeNotifyPrivilege`

相關資訊

- 了解伺服器上的 BUILTIN 群組和本機管理員帳戶
- 支援的權限清單
- 了解如何配置繞過遍歷檢查

啟用或停用本機使用者和群組功能

了解本機 **ONTAP SMB** 使用者和群組功能

您必須先啟用本機使用者和群組功能、才能使用本機使用者和群組來存取NTFS安全型資料。此外、如果您想要使用本機使用者進行SMB驗證、則必須啟用本機使用者驗證功能。

預設會啟用本機使用者和群組功能和本機使用者驗證。如果未啟用這些功能、您必須先啟用這些功能、才能設定及使用本機使用者和群組。您可以隨時停用本機使用者和群組功能。

除了明確停用本機使用者和群組功能之外、ONTAP 如果叢集中的任何節點還原ONTAP 為不支援此功能的版本、則無法使用本地使用者和群組功能。本機使用者和群組功能只有在叢集中的所有節點都執行ONTAP 支援的版本支援之前、才會啟用。

相關資訊

- 修改本機使用者帳戶
- 修改本機群組
- 新增權限給本機或網域使用者或群組

在 **ONTAP SMB** 伺服器上啟用或停用本機使用者和群組

您可以在儲存虛擬機器（SVM）上啟用或停用本機使用者和群組進行SMB存取。預設會啟用本機使用者和群組功能。

關於這項工作

您可以在設定SMB共用區和NTFS檔案權限時使用本機使用者和群組、也可以在建立SMB連線時選用本機使用者進行驗證。若要使用本機使用者進行驗證、您也必須啟用本機使用者和群組驗證選項。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 執行下列其中一項動作：

如果您希望本機使用者和群組...	輸入命令...
已啟用	`vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled true`
已停用	`vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled false`

3. 返回管理權限層級： `set -privilege admin`

範例

下列範例可在SVM VS1上啟用本機使用者和群組功能：

```
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-local-users-and
-groups-enabled true

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

相關資訊

- 在伺服器上啟用或停用本機使用者身份驗證
- 啟用或停用本機使用者帳戶

在 **ONTAP SMB** 伺服器上啟用或停用本機使用者身份驗證

您可以在儲存虛擬機器（SVM）上啟用或停用SMB存取的本機使用者驗證。預設為允許本機使用者驗證、這在SVM無法連絡網域控制器或您選擇不使用網域層級存取控制時非常有用。

開始之前

必須在CIFS伺服器上啟用本機使用者和群組功能。

關於這項工作

您可以隨時啟用或停用本機使用者驗證。如果您想要在建立SMB連線時使用本機使用者進行驗證、也必須啟用CIFS伺服器的本機使用者和群組選項。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 執行下列其中一項動作：

如果您希望本機驗證...	輸入命令...
已啟用	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled true`
已停用	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled false`

3. 返回管理權限層級： `set -privilege admin`

範例

下列範例可在SVM VS1上啟用本機使用者驗證：

```
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-local-auth
-enabled true

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

相關資訊

- 了解本地用戶身份驗證
- 啟用或停用伺服器上的本機使用者和群組

管理本機使用者帳戶

修改本機 **ONTAP SMB** 使用者帳戶

如果您想要變更現有使用者的完整名稱或說明、以及要啟用或停用使用者帳戶、您可以修改本機使用者帳戶。如果使用者名稱遭入侵、或是為了管理目的而需要變更名稱、您也可以重新命名本機使用者帳戶。

如果您想要...	輸入命令...
修改本機使用者的全名	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-full-name text` 如果全名包含空格、則必須以雙引號括住。
修改本機使用者的說明	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-description text` 如果描述包含空格、則必須以雙引號括住。
啟用或停用本機使用者帳戶	`vserver cifs users-and-groups local-user modify -vserver` *vserver_name* -user-name *user_name* -is-account-disabled {true
false}`	重新命名本機使用者帳戶

範例

下列範例將儲存虛擬機器（SVM、先前稱為Vserver）VS1上的本機使用者「'CIFs_Server\sue」重新命名為「'CIFS伺服器\ sue新'」：

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

啟用或停用本機 **ONTAP SMB** 使用者帳戶

如果您希望使用者能夠透過SMB連線存取儲存虛擬機器（SVM）中所含的資料、請啟用本機使用者帳戶。如果您不想讓本機使用者帳戶透過SMB存取SVM資料、也可以停用該使用者帳戶。

關於這項工作

您可以修改使用者帳戶來啟用本機使用者。

步驟

1. 執行適當的行動：

如果您想要...	輸入命令...
啟用使用者帳戶	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account -disabled false`
停用使用者帳戶	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account -disabled true`

變更本機 **ONTAP SMB** 使用者帳戶密碼

您可以變更本機使用者的帳戶密碼。如果使用者的密碼遭入侵或使用者忘記密碼、這項功能就很有用。

步驟

1. 請執行適當的動作來變更密碼： `vserver cifs users-and-groups local-user set-password -vserver vserver_name -user-name user_name`

範例

下列範例設定與儲存虛擬機器（SVM、先前稱為Vserver）VS1相關之本機使用者「'CIFS/Server\sue」的密碼：

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

相關資訊

設定本地用戶的密碼複雜度

顯示有關伺服器安全設定的信息

顯示有關 **ONTAP SMB** 本地用戶的信息

您可以在摘要表單中顯示所有本機使用者的清單。如果您想要判斷特定使用者的帳戶設定、可以顯示該使用者的詳細帳戶資訊、以及多位使用者的帳戶資訊。此資訊可協助您判斷是否需要修改使用者的設定、以及疑難排解驗證或檔案存取問題。

關於這項工作

永遠不會顯示使用者密碼的相關資訊。

步驟

1. 執行下列其中一項動作：

如果您想要...	輸入命令...
顯示儲存虛擬機器（SVM）上所有使用者的相關資訊	`vserver cifs users-and-groups local-user show -vserver vserver_name`
顯示使用者的詳細帳戶資訊	`vserver cifs users-and-groups local-user show -instance -vserver vserver_name -user-name user_name`

您可以在執行命令時選擇其他選用參數。如"指令參考資料ONTAP"需詳細 `vserver cifs`資訊，請參閱。

範例

下列範例顯示SVM VS1上所有本機使用者的相關資訊：

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name     Description
-------- ---------------------------- ------------- -------------
vs1      CIFS_SERVER\Administrator    James Smith   Built-in administrator
account
vs1      CIFS_SERVER\sue              Sue   Jones
```

顯示有關本機使用者的 **ONTAP SMB** 群組成員身分的信息

您可以顯示本機使用者所屬的本機群組資訊。您可以使用此資訊來判斷使用者對檔案和資料夾的存取權限。此資訊有助於判斷使用者對檔案和資料夾的存取權限、或是疑難排解檔案存取問題。

關於這項工作

您可以自訂命令、僅顯示您要查看的資訊。

步驟

1. 執行下列其中一項動作：

如果您想要...	輸入命令...
顯示指定本機使用者的本機使用者成員資格資訊	`vserver cifs users-and-groups local-user show-membership -user-name user_name`
顯示本機使用者所屬本機群組的本機使用者成員資格資訊	`vserver cifs users-and-groups local-user show-membership -membership group_name`

如果您想要...	輸入命令...
顯示與指定儲存虛擬機器（SVM）相關聯之本機使用者的使用者成員資格資訊	`vserver cifs users-and-groups local-user show-membership -vserver` *vserver_name*
顯示指定SVM上所有本機使用者的詳細資訊	`vserver cifs users-and-groups local-user show-membership -instance -vserver` *vserver_name*

範例

以下範例顯示SVM VS1上所有本機使用者的成員資格資訊；使用者「CIFS伺服器管理員」是「BUILTIN\Administrators」群組的成員、而「CIFS伺服器\ sue」是「CIFS伺服器\ g1`」群組的成員：

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver    User Name                     Membership
---------- ----------------------------- ------------------------
vs1        CIFS_SERVER\Administrator     BUILTIN\Administrators
           CIFS_SERVER\sue               CIFS_SERVER\g1
```

刪除本機 **ONTAP SMB** 使用者帳戶

如果不再需要本機SMB驗證CIFS伺服器、或決定SVM所含資料的存取權限、您可以從儲存虛擬機器（SVM）刪除本機使用者帳戶。

關於這項工作

刪除本機使用者時、請謹記下列事項：

- 檔案系統不會變更。

  不會調整參照此使用者之檔案和目錄上的Windows安全性描述元。

- 所有對本機使用者的參照都會從成員資格和權限資料庫中移除。
- 標準且知名的使用者（例如Administrator）無法刪除。

步驟

1. 決定您要刪除的本機使用者帳戶名稱： `vserver cifs users-and-groups local-user show -vserver` *vserver_name*
2. 刪除本機使用者： `vserver cifs users-and-groups local-user delete -vserver` *vserver_name* `-user-name` *username_name*
3. 確認已刪除使用者帳戶： `vserver cifs users-and-groups local-user show -vserver` *vserver_name*

範例

下列範例會刪除與SVM VS1相關聯的本機使用者「'CIFS/Server\sue」：

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name      Description
-------- ---------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator    James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue              Sue   Jones


cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                    Full Name      Description
-------- ---------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator    James Smith    Built-in administrator
account
```

管理本機群組

修改本地 **ONTAP SMB** 群組

您可以變更現有本機群組的說明、或重新命名群組、以修改現有的本機群組。

如果您想要...	使用命令...
修改本機群組說明	`vserver cifs users-and-groups local-group modify -vserver` *vserver_name* `-group-name` *group_name* `-description text` 如果描述包含空格、則必須以雙引號括住。
重新命名本機群組	`vserver cifs users-and-groups local-group rename -vserver` *vserver_name* `-group-name` *group_name* `-new-group-name` *new_group_name*

範例

下列範例將本機群組「'CIFs_Server\Engineering」重新命名為「'CIFs_Server\Engineering _new'」：

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

下列範例修改本機群組「'CIFs_Server\Engineering」的說明：

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

顯示有關 **ONTAP SMB** 本機群組的信息

您可以顯示在叢集或指定儲存虛擬機器（SVM）上設定的所有本機群組清單。此資訊在疑難排解SVM上所含資料的檔案存取問題或SVM上的使用者權限（權限）問題時非常實用。

步驟

1. 執行下列其中一項動作：

如果您想要有關...的資訊	輸入命令...
叢集上的所有本機群組	`vserver cifs users-and-groups local-group show`
SVM上的所有本機群組	`vserver cifs users-and-groups local-group show -vserver` *`vserver_name`*

您可以在執行此命令時選擇其他選用參數。如"指令參考資料ONTAP"需詳細 `vserver cifs`資訊，請參閱。

範例

下列範例顯示SVM VS1上所有本機群組的相關資訊：

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                   Description
-------- ---------------------------- ----------------------------
vs1      BUILTIN\Administrators       Built-in Administrators group
vs1      BUILTIN\Backup Operators     Backup Operators group
vs1      BUILTIN\Power Users          Restricted administrative privileges
vs1      BUILTIN\Users                All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

管理本機 **ONTAP SMB** 群組成員資格

您可以新增及移除本機或網域使用者、或新增及移除網域群組、來管理本機群組成員資格。如果您想要根據群組中的存取控制來控制資料存取、或是想要使用者擁有與該群組相關的權限、這很有用。

關於這項工作

新增成員至本機群組的準則：

- 您無法將使用者新增至特殊的_Everyon__群組。

- 您必須先存在本機群組、才能將使用者新增至該群組。
- 使用者必須存在、才能將使用者新增至本機群組。
- 您無法將本機群組新增至其他本機群組。
- 若要將網域使用者或群組新增至本機群組、Data ONTAP 則必須能夠將名稱解析為SID。

從本機群組移除成員的準則：

- 您無法從特殊的_Everyon__群組中移除成員。
- 您要從中移除成員的群組必須存在。
- 必須能夠將您要從群組移除的成員名稱解析為對應的SID。ONTAP

步驟

1. 新增或移除群組中的成員。

如果您想要...	然後使用命令...
新增成員至群組	`vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` 您可以指定要新增至指定本機群組的本機使用者、網域使用者或網域群組的以逗號分隔的清單。
從群組中移除成員	`vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` 您可以指定要從指定本機群組中移除的本機使用者、網域使用者或網域群組的以逗號分隔的清單。

以下範例將本機使用者「'Smb_server\sue」和網域群組「'AD_DOM\DOM_DOM_eng'」新增至SVM VS1上的本機群組「'Smb_server\engin'」：

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

以下範例將SVM VS1上本機群組「'Smb_server\sue」和「'smb_server\james'」中的本機使用者移除：

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

相關資訊

顯示本機群組成員的相關資訊

顯示有關本機群組成員的 ONTAP SMB 信息

您可以顯示叢集或指定儲存虛擬機器（SVM）上所設定之本機群組的所有成員清單。在疑難排解檔案存取問題或使用者權限（權限）問題時、此資訊很有用。

步驟

1. 執行下列其中一項動作：

如果您想要顯示有關...的資訊	輸入命令...
叢集上所有本機群組的成員	`vserver cifs users-and-groups local-group show-members`
SVM上所有本機群組的成員	`vserver cifs users-and-groups local-group show-members -vserver` *`vserver_name`*

範例

下列範例顯示SVM VS1上所有本機群組成員的相關資訊：

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                    Members
--------- ----------------------------- ------------------------
vs1       BUILTIN\Administrators        CIFS_SERVER\Administrator
                                        AD_DOMAIN\Domain Admins
                                        AD_DOMAIN\dom_grp1
          BUILTIN\Users                 AD_DOMAIN\Domain Users
                                        AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering       CIFS_SERVER\james
```

刪除本機 ONTAP SMB 群組

如果不再需要本機群組來判斷與該SVM相關之資料的存取權限、或不再需要將SVM使用者權限（權限）指派給群組成員、您可以從儲存虛擬機器（SVM）中刪除該群組。

關於這項工作

刪除本機群組時、請謹記下列事項：

- 檔案系統不會變更。

  不會調整參照此群組之檔案和目錄上的Windows安全性描述元。

- 如果群組不存在、則會傳回錯誤。

- 無法刪除特殊的_Everyon__群組。
- 無法刪除內建群組、例如_BUILTIN\Administrators__BUILTIN\Users_。

步驟

1. 在 SVM 上顯示本機群組清單、藉此判斷您要刪除的本機群組名稱：`vserver cifs users-and-groups local-group show -vserver vserver_name`
2. 刪除本機群組：`vserver cifs users-and-groups local-group delete -vserver` *`vserver_name`* `-group-name` *`group_name`*
3. 確認群組已刪除：`vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

範例

下列範例會刪除與SVM VS1相關聯的本機群組「'CIFs_Server\sales'」：

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- --------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- --------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
```

更新本機資料庫中的 **ONTAP SMB** 網域使用者和群組名稱

您可以將網域使用者和群組新增至CIFS伺服器的本機群組。這些網域物件會在叢集的本機資料庫中登錄。如果重新命名網域物件、則必須手動更新本機資料庫。

關於這項工作

您必須指定要更新網域名稱的儲存虛擬機器（SVM）名稱。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 執行適當的行動：

如果您想要更新網域使用者和群組、以及...	使用此命令...
顯示已成功更新且無法更新的網域使用者和群組	`vserver cifs users-and-groups update-names -vserver vserver_name`
顯示成功更新的網域使用者和群組	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false`
僅顯示無法更新的網域使用者和群組	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true`
隱藏更新的所有狀態資訊	`vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true`

3. 返回管理權限層級： `set -privilege admin`

範例

下列範例會更新與儲存虛擬機器（SVM、先前稱為Vserver）VS1相關聯的網域使用者和群組名稱。對於上一次更新、需要更新的是一條相依的名稱鏈：

```
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 users-and-groups update-names -vserver vs1

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-12345
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654322-23456
   Domain:            EXAMPLE2
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-123456
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user3
   Updated Name:      dom_user4
   Status:            Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                      to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

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

管理本機權限

向 **ONTAP SMB** 本機或網域使用者或群組新增權限

您可以新增權限來管理本機或網域使用者或群組的使用者權限。新增的權限會覆寫指派給任何這些物件的預設權限。這可讓您自訂使用者或群組擁有的權限、進而增強安全性。

開始之前

要新增權限的本機或網域使用者或群組必須已經存在。

關於這項工作

新增權限至物件會覆寫該使用者或群組的預設權限。新增權限並不會移除先前新增的權限。

新增權限給本機或網域使用者或群組時、必須謹記下列事項：

- 您可以新增一或多個權限。
- 將權限新增至網域使用者或群組時ONTAP 、可能會聯絡網域控制器來驗證網域使用者或群組。

  如果無法聯絡網域控制器、則指令可能會失敗ONTAP 。

步驟

1. 新增一或多個權限至本機或網域使用者或群組： `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. 確認所需權限已套用至物件： `vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *name*`

範例

以下範例將「'eTcbprivre'」和「'eTakeOwnershipprivatef'」權限新增至儲存虛擬機器（SVM、先前稱為Vserver）VS1上的使用者「'CIFs_Server\sue'」：

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege
```

刪除 **ONTAP SMB** 本機或網域使用者或群組的權限

您可以移除權限、來管理本機或網域使用者或群組的使用者權限。這可讓您自訂使用者和群組擁有的最大權限、進而增強安全性。

開始之前

將從中移除權限的本機或網域使用者或群組必須已經存在。

關於這項工作

在移除本機或網域使用者或群組的權限時、您必須謹記下列事項：

- 您可以移除一或多個權限。
- 當移除網域使用者或群組的權限時、ONTAP 可能會聯絡網域控制器來驗證網域使用者或群組。

  如果無法聯絡網域控制器、則指令可能會失敗ONTAP 。

步驟

1. 移除本機或網域使用者或群組的一或多個權限： `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. 確認已從物件中移除所需的權限： `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

範例

下列範例移除儲存虛擬機器（SVM、前身為Vserver）VS1上使用者「'CIFs_Server\sue」的「'eTcbprivre'」和「'eTakeOwnershipprivatef'」權限：

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- -------------------
vs1       CIFS_SERVER\sue       -
```

重設 **ONTAP SMB** 本機或網域使用者和群組的權限

您可以重設本機或網域使用者和群組的權限。當您已修改本機或網域使用者或群組的權限、而且不再需要或需要這些修改時、此功能就很有用。

關於這項工作

重設本機或網域使用者或群組的權限、會移除該物件的任何權限項目。

步驟

1. 重設本機或網域使用者或群組的權限： `vserver cifs users-and-groups privilege reset-privilege -vserver vserver_name -user-or-group-name name`

2. 確認物件上的權限已重設： `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

範例

下列範例會重設儲存虛擬機器（SVM、先前稱為Vserver）VS1上使用者「'CIFs_Server\sue」的權限。根據預設、一般使用者沒有與其帳戶相關的權限：

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

下列範例會重設群組「'BUILTIN\管理員'」的權限、有效移除權限項目：

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name       Privileges
--------- ----------------------- -------------------
vs1       BUILTIN\Administrators   SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

顯示有關 **ONTAP SMB** 權限覆蓋的信息

您可以顯示指派給網域或本機使用者帳戶或群組的自訂權限相關資訊。此資訊可協助您判斷是否套用所需的使用者權限。

步驟

1. 執行下列其中一項動作：

如果您想要顯示有關...的資訊	輸入此命令...
儲存虛擬機器（SVM）上所有網域和本機使用者和群組的自訂權限	`vserver cifs users-and-groups privilege show -vserver vserver_name`
自訂SVM上特定網域或本機使用者和群組的權限	`vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

您可以在執行此命令時選擇其他選用參數。如"指令參考資料ONTAP"需詳細 `vserver cifs users-and-groups privilege show`資訊，請參閱。

範例

下列命令會顯示明確與SVM VS1的本機或網域使用者和群組相關聯的所有權限：

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name     Privileges
---------  --------------------   ---------------
vs1        BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                   SeRestorePrivilege
vs1        CIFS_SERVER\sue         SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

設定略過周遊檢查

了解如何設定 **ONTAP SMB** 繞過遍歷檢查

「略過周遊檢查」是一項使用者權限（也稱為_priv榮幸_）、可決定使用者是否可以周遊檔案路徑中的所有目錄、即使使用者對周遊目錄沒有權限。您應該瞭解允許或禁止略過周遊檢查時會發生什麼情況、以及如何為儲存虛擬機器（SVM）上的使用者設定略過周遊檢查。

允許或禁止略過周遊檢查時會發生什麼事

- 如果允許、當使用者嘗試存取檔案時ONTAP 、當決定是否授予或拒絕存取檔案時、不會檢查中繼目錄的周遊權限。
- 如果不允許、ONTAP 則此功能會檢查檔案路徑中所有目錄的周遊（執行）權限。

  如果任何中繼目錄沒有「'X'」（周遊權限）、ONTAP 則無法存取檔案。

設定略過周遊檢查

您可以使用ONTAP CLI或使用此使用者權限設定Active Directory群組原則、來設定略過周遊檢查。

。 `SeChangeNotifyPrivilege` 權限可控制是否允許使用者略過周遊檢查。

- 將它新增至SVM上的本機SMB使用者或群組、或新增至網域使用者或群組、可進行略過周遊檢查。
- 從SVM上的本機SMB使用者或群組或網域使用者或群組中移除此功能、將不允許略過周遊檢查。

根據預設、SVM上的下列BUILTIN群組有權略過周遊檢查：

- `BUILTIN\Administrators`
- `BUILTIN\Power Users`
- `BUILTIN\Backup Operators`
- `BUILTIN\Users`
- `Everyone`

如果您不想讓其中一個群組的成員略過周遊檢查、則必須從群組中移除此權限。

使用CLI在SVM上設定本機SMB使用者和群組的略過周遊檢查時、必須謹記下列事項：

- 如果您想要允許自訂本機或網域群組的成員略過周遊檢查，則必須新增 `SeChangeNotifyPrivilege` 權限給該群組。
- 如果您想要允許個別本機或網域使用者略過周遊檢查，而該使用者不是具有該權限的群組成員，則可以新增 `SeChangeNotifyPrivilege` 該使用者帳戶的權限。
- 您可以移除來停用本機或網域使用者或群組的略過周遊檢查 `SeChangeNotifyPrivilege` 隨時享有特權。

> 若要停用特定本機或網域使用者或群組的略過傳輸檢查、您也必須移除 `SeChangeNotifyPrivilege` 的權限 `Everyone` 群組：

相關資訊

- 允許使用者或群組略過目錄周遊檢查
- 不允許使用者或群組繞過目錄周遊檢查
- 配置卷上的檔案名稱轉換的字元映射
- 建立共用存取控制列表
- 使用儲存層級存取保護來保護檔案存取安全
- 支援的權限清單
- 新增權限給本機或網域使用者或群組

允許使用者或群組繞過 ONTAP SMB 目錄遍歷檢查

如果您希望使用者能夠周遊檔案路徑中的所有目錄、即使使用者對周遊目錄沒有權限、您也可以新增 `SeChangeNotifyPrivilege` 本機 SMB 使用者或儲存虛擬機器上群組的權限（ SVM ）。根據預設、使用者可以略過目錄周遊檢查。

開始之前

- SVM上必須有SMB伺服器。
- 必須啟用本機使用者和群組SMB伺服器選項。

- 本機或網域使用者或群組 `SeChangeNotifyPrivilege` 新增權限必須已存在。

關於這項工作

將權限新增至網域使用者或群組時ONTAP 、可能會聯絡網域控制器來驗證網域使用者或群組。如果無法聯絡網域控制器、則指令可能會失敗ONTAP 。

步驟

1. 新增以啟用略過周遊檢查 `SeChangeNotifyPrivilege` 本機或網域使用者或群組的權限： `vserver cifs users-and-groups privilege add-privilege -vserver vserver_name -user-or -group-name name -privileges SeChangeNotifyPrivilege`

   的值 `-user-or-group-name` 參數是本機使用者或群組、或是網域使用者或群組。

2. 確認指定的使用者或群組已啟用略過周遊檢查： `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

範例

下列命令可讓屬於 “example\eng” 群組的使用者透過新增來略過目錄周遊檢查 `SeChangeNotifyPrivilege` 群組的權限：

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege
```

相關資訊

不允許使用者或群組繞過目錄周遊檢查

禁止使用者或群組繞過 **ONTAP SMB** 目錄遍歷檢查

如果您不希望使用者周遊檔案路徑中的所有目錄、因為使用者對周遊目錄沒有權限、您可以移除 `SeChangeNotifyPrivilege` 本機 SMB 使用者或儲存虛擬機器上群組的權限（ SVM ）。

開始之前

將從中移除權限的本機或網域使用者或群組必須已經存在。

關於這項工作

當移除網域使用者或群組的權限時、ONTAP 可能會聯絡網域控制器來驗證網域使用者或群組。如果無法聯絡網域控制器、則指令可能會失敗ONTAP 。

步驟

1. 不允許略過周遊檢查： `vserver cifs users-and-groups privilege remove-privilege -vserver vserver_name -user-or-group-name name -privileges`

`SeChangeNotifyPrivilege`

命令會移除 `SeChangeNotifyPrivilege` 本機或網域使用者或群組的權限、您可以使用的值來指定 `-user-or-group-name` *name* 參數。

2. 確認指定的使用者或群組已停用略過周遊檢查： `vserver cifs users-and-groups privilege show -vserver` *vserver_name* `-user-or-group-name` *name*

範例

下列命令會禁止屬於「'example\eng'」群組的使用者略過目錄周遊檢查：

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ----------------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ----------------------
vs1       EXAMPLE\eng           -
```

相關資訊

允許使用者或群組略過目錄周遊檢查

顯示檔案安全性和稽核原則的相關資訊

了解如何查看 ONTAP SMB 檔案安全和稽核策略

您可以在儲存虛擬機器（SVM）上的磁碟區內、顯示有關檔案與目錄安全性的資訊。您可以顯示FlexVol 有關在功能區上稽核原則的資訊。如果已設定、您可以在FlexVol 下列項目上顯示儲存層級存取保護和動態存取控制安全性設定的相關資訊：

顯示檔案安全性的相關資訊

您可以使用FlexVol 下列安全性樣式、顯示套用至Volume和qtree（適用於哪些人）中所含資料的檔案安全性相關資訊：

- NTFS
- UNIX
- 混合

顯示稽核原則的相關資訊

您可以透過FlexVol 下列NAS傳輸協定、顯示稽核原則的相關資訊、以稽核在支援功能上執行的存取事件：

- SMB（所有版本）
- NFSv4.x

顯示儲存層級存取保護（**slag**）安全性的相關資訊

儲存層級的存取保護安全功能可套用FlexVol 至下列安全樣式的物件：

- NTFS
- 混合
- UNIX（如果CIFS伺服器是在包含該磁碟區的SVM上設定）

顯示動態存取控制（**DAC**）安全性的相關資訊

動態存取控制安全功能FlexVol 可套用至包含下列安全樣式的物件：

- NTFS
- 混合（如果物件具有NTFS有效安全性）

相關資訊

- 了解如何使用儲存級別存取防護來保護文件存取
- 顯示有關伺服器上儲存層級存取防護的信息

顯示有關 **NTFS** 安全模式磁碟區上的 **ONTAP SMB** 檔案安全性的信息

您可以在NTFS安全型磁碟區上顯示檔案與目錄安全性的相關資訊、包括安全型態與有效的安全性樣式、套用的權限、以及DOS屬性的相關資訊。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。

- 由於NTFS安全型磁碟區和qtree在決定檔案存取權限時僅使用NTFS檔案權限、而Windows使用者和群組、因此UNIX相關的輸出欄位會包含僅供顯示的UNIX檔案權限資訊。
- 將顯示具有NTFS安全性的檔案和資料夾的ACL輸出。
- 由於儲存層級的存取保護安全性可在磁碟區根目錄或qtree上設定、因此設定儲存層級存取保護的磁碟區或qtree路徑輸出可能會同時顯示一般檔案ACL和儲存層級的存取保護ACL。
- 如果已針對指定的檔案或目錄路徑設定動態存取控制、則輸出也會顯示動態存取控制ACE的相關資訊。

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`

範例

下列範例顯示有關路徑的安全性資訊 `/vol4` 在 SVM VS1 中：

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                                Vserver: vs1
                              File Path: /vol4
                      File Inode Number: 64
                         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
```

以下範例顯示有關路徑的安全性資訊、並提供有關路徑的擴充遮罩 `/data/engineering` 在 SVM VS1 中：

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true

               Vserver: vs1
             File Path: /data/engineering
     File Inode Number: 5544
        Security Style: ntfs
```

```
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
          Unix User Id: 0
         Unix Group Id: 0
        Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
Generic Execute
                             ...0 .... .... .... .... .... .... .... =
Generic All
```

```
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
Write Owner
```

```
                                .... .... .... .0.. .... .... .... .... =
Write DAC
                                .... .... .... ..0. .... .... .... .... =
Read Control
                                .... .... .... ...0 .... .... .... .... =
Delete
                                .... .... .... .... .... ...0 .... .... =
Write Attributes
                                .... .... .... .... .... .... 0... .... =
Read Attributes
                                .... .... .... .... .... .... .0.. .... =
Delete Child
                                .... .... .... .... .... .... ..0. .... =
Execute
                                .... .... .... .... .... .... ...0 .... =
Write EA
                                .... .... .... .... .... .... .... 0... =
Read EA
                                .... .... .... .... .... .... .... .0.. =
Append
                                .... .... .... .... .... .... .... ..0. =
Write
                                .... .... .... .... .... .... .... ...0 =
Read
```

以下範例顯示具有路徑之磁碟區的安全性資訊、包括儲存層級 Access Guard 安全性資訊 `/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
```

相關資訊

- 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

您可以在混合式安全型磁碟區上顯示檔案與目錄安全性的相關資訊、包括安全型態與有效的安全性樣式、套用的權限、以及UNIX擁有者與群組的相關資訊。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。

- 混合式安全型磁碟區和qtree可包含使用UNIX檔案權限的部分檔案和資料夾、包括模式位元或NFSv4 ACL、以及使用NTFS檔案權限的部分檔案和目錄。
- 混合式安全型磁碟區的最上層可能具有UNIX或NTFS的有效安全性。
- ACL輸出只會針對具有NTFS或NFSv4安全性的檔案和資料夾顯示。

  對於使用UNIX安全性的檔案和目錄、如果只套用模式位元權限（無NFSv4 ACL）、則此欄位為空白。
- ACL輸出中的擁有者和群組輸出欄位僅適用於NTFS安全性描述元。
- 因為即使Volume root或qtree的有效安全樣式為UNIX、也可以在混合式安全型Volume或qtree上設定儲存層級的存取保護安全性、 已設定儲存層級存取保護的Volume或qtree路徑輸出、可能會同時顯示UNIX檔案權限和儲存層級存取保護ACL。
- 如果在命令中輸入的路徑是使用NTFS有效安全性的資料、則當動態存取控制是針對指定的檔案或目錄路徑設定時、輸出也會顯示動態存取控制ACE的相關資訊。

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`

範例

下列範例顯示有關路徑的安全性資訊 `/projects` 在 SVM VS1 中以擴充遮罩形式呈現。這種混合式安全型路徑具有UNIX有效的安全性。

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

                Vserver: vs1
              File Path: /projects
      File Inode Number: 78
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

下列範例顯示有關路徑的安全性資訊 `/data` 在 SVM VS1 中。這種混合式安全型路徑具有NTFS有效安全性。

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

                                Vserver: vs1
                              File Path: /data
                      File Inode Number: 544
                         Security Style: mixed
                        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
```

以下範例顯示路徑中有關 Volume 的安全性資訊 `/datavol5` 在 SVM VS1 中。這種混合式安全型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
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
```

相關資訊

- 顯示NTFS安全型磁碟區上的檔案安全資訊
- 顯示UNIX安全型磁碟區上的檔案安全資訊

顯示有關 **UNIX** 安全模式磁碟區上的 **ONTAP SMB** 檔案安全性的信息

您可以顯示UNIX安全型磁碟區上的檔案與目錄安全性相關資訊、包括安全性樣式與有效的安全性樣式、套用的權限、以及UNIX擁有者與群組的相關資訊。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目錄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。

- UNIX安全型磁碟區和qtree在決定檔案存取權限時、只會使用UNIX檔案權限（模式位元或NFSv4 ACL）。
- ACL輸出只會針對具有NFSv4安全性的檔案和資料夾顯示。

  對於使用UNIX安全性的檔案和目錄、如果只套用模式位元權限（無NFSv4 ACL）、則此欄位為空白。

- 如果使用NFSv4安全性描述元、則不會套用ACL輸出中的擁有者和群組輸出欄位。

  它們只對NTFS安全描述元有意義。

- 由於如果在 SVM 上設定 CIFS 伺服器、則 UNIX 磁碟區或 qtree 上支援儲存層級存取保護安全性、因此輸出可能包含適用於中指定之磁碟區或 qtree 的儲存層級存取保護安全性相關資訊 `-path` 參數。

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`

範例

下列範例顯示有關路徑的安全性資訊 `/home` 在 SVM VS1 中：

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 1
                          Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                 ACLs: -
```

下列範例顯示有關路徑的安全性資訊 `/home` 在 SVM VS1 的擴充遮罩形式中：

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: 0x10
                    ...0 .... .... .... = Offline
                    .... ..0. .... .... = Sparse
                    .... .... 0... .... = Normal
                    .... .... ..0. .... = Archive
                    .... .... ...1 .... = Directory
                    .... .... .... .0.. = System
                    .... .... .... ..0. = Hidden
                    .... .... .... ...0 = Read Only
                          Unix User Id: 0
                         Unix Group Id: 1
                         Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                 ACLs: -
```

相關資訊

- 顯示有關安全類型捲上的文件安全性的信息
- 顯示混合式安全型磁碟區的檔案安全資訊

ONTAP 指令用於顯示有關 **SMB FlexVol** 磁碟區上的 **NTFS** 稽核策略的信息

您可以在FlexVol 功能區上顯示NTFS稽核原則的相關資訊、包括安全樣式和有效的安全樣式、套用的權限、以及系統存取控制清單的相關資訊。您可以使用結果來驗證安全性組態或疑難排解稽核問題。

關於這項工作

您必須提供儲存虛擬機器（SVM）的名稱、以及要顯示其稽核資訊的檔案或資料夾路徑。您可以以摘要形式或詳細清單來顯示輸出。

- NTFS安全型磁碟區和qtree僅使用NTFS系統存取控制清單（SACL）來執行稽核原則。
- 在具有NTFS有效安全性的混合式安全型磁碟區中、檔案和資料夾可以套用NTFS稽核原則。

  混合式安全型磁碟區和qtree可包含使用UNIX檔案權限的部分檔案和目錄、包括模式位元或NFSv4 ACL、以及使用NTFS檔案權限的部分檔案和目錄。
- 混合式安全型磁碟區的最上層可能具有UNIX或NTFS有效安全性、而且可能包含或不包含NTFS SACL。
- 因為即使Volume root或qtree的有效安全樣式為UNIX、也可以在混合式安全型Volume或qtree上設定儲存層級的存取保護安全性、 已設定儲存層級存取保護的Volume或qtree路徑輸出、可能會同時顯示一般檔案和資料夾NFSv4 SACL、以及儲存層級存取保護NTFS SACL。
- 如果在命令中輸入的路徑是使用NTFS有效安全性的資料、則輸出也會顯示動態存取控制ACE的相關資訊（如果已針對指定的檔案或目錄路徑設定動態存取控制）。
- 在顯示具有NTFS有效安全性的檔案和資料夾的安全性資訊時、UNIX相關的輸出欄位會包含僅供顯示的UNIX檔案權限資訊。

  NTFS安全型檔案和資料夾在決定檔案存取權限時、僅使用NTFS檔案權限、Windows使用者和群組。
- ACL輸出只會針對具有NTFS或NFSv4安全性的檔案和資料夾顯示。

  對於使用UNIX安全性的檔案和資料夾而言、此欄位為空白、只套用模式位元權限（無NFSv4 ACL）。
- ACL輸出中的擁有者和群組輸出欄位僅適用於NTFS安全性描述元。

步驟

1. 以所需的詳細資料層級顯示檔案和目錄稽核原則設定：

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`
詳細清單	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

範例

下列範例顯示路徑的稽核原則資訊 `/corp` 在 SVM VS1 中。路徑具有NTFS有效安全性。NTFS安全性描述元包含成功和成功/失敗SACL項目。

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         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:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

下列範例顯示路徑的稽核原則資訊 `/datavol1` 在 SVM VS1 中。路徑包含一般檔案和資料夾SACL、以及儲存層級存取保護SACL。

```
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:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         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
```

ONTAP 指令用於顯示有關 **SMB FlexVol** 磁碟區上的 **NFSv4** 稽核策略的信息

您可以FlexVol 使用ONTAP CLI在S什麼 磁碟區上顯示NFSv4稽核原則的相關資訊、包括安全樣式和有效的安全樣式、套用的權限、以及系統存取控制清單（SACL）的相關資訊。

您可以使用結果來驗證安全性組態或疑難排解稽核問題。

關於這項工作

您必須提供儲存虛擬機器（SVM）的名稱、以及要顯示其稽核資訊的檔案或目錄路徑。您可以以摘要形式或詳細清單來顯示輸出。

- UNIX安全型磁碟區和qtree僅使用NFSv4 SACL來執行稽核原則。
- 混合式安全型磁碟區中的檔案和目錄、若為UNIX安全型態、則可套用NFSv4稽核原則。

  混合式安全型磁碟區和qtree可包含使用UNIX檔案權限的部分檔案和目錄、包括模式位元或NFSv4 ACL、以及使用NTFS檔案權限的部分檔案和目錄。

- 混合式安全型磁碟區的最上層可能具有UNIX或NTFS的有效安全性、而且可能包含或不包含NFSv4 SACL。
- ACL輸出只會針對具有NTFS或NFSv4安全性的檔案和資料夾顯示。

  對於使用UNIX安全性的檔案和資料夾而言、此欄位為空白、只套用模式位元權限（無NFSv4 ACL）。

- ACL輸出中的擁有者和群組輸出欄位僅適用於NTFS安全性描述元。
- 因為即使Volume root或qtree的有效安全樣式為UNIX、也可以在混合式安全型Volume或qtree上設定儲存層級的存取保護安全性、 已設定儲存層級存取保護的Volume或qtree路徑輸出、可能會同時顯示一般NFSv4檔案和目錄SACL、以及儲存層級存取保護NTFS SACL。
- 由於如果在 SVM 上設定 CIFS 伺服器、則 UNIX 磁碟區或 qtree 上支援儲存層級存取保護安全性、因此輸出可能包含適用於中指定之磁碟區或 qtree 的儲存層級存取保護安全性相關資訊 `-path` 參數。

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`

範例

下列範例顯示有關路徑的安全性資訊 `/lab` 在 SVM VS1 中。此UNIX安全型路徑具有NFSv4 SACL。

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

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

了解如何顯示 **ONTAP SMB** 文件安全和審計策略信息

您可以使用萬用字元（*）來顯示特定路徑或根磁碟區下所有檔案和目錄的檔案安全性和稽核原則相關資訊。

萬用字元（）可做為指定目錄路徑的最後一個子元件、您可以在該子元件下方顯示所有檔案和目錄的資訊。如果您想要顯示名為「」的特定檔案或目錄資訊、則必須在雙引號（「'」）內提供完整路徑。

範例

下列含有萬用字元的命令會顯示路徑下方所有檔案和目錄的相關資訊 `/1/` SVM VS1 ：

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
            Security Style: mixed
           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:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
            Security Style: mixed
           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:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

下列命令會顯示路徑下名為「*」的檔案資訊 `/vol1/a` SVM VS1 的路徑會以雙引號（""）括住。

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                Vserver: vs1
              File Path: "/vol1/a/*"
      Security Style: mixed
     Effective Style: unix
      DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
         Unix User Id: 1002
        Unix Group Id: 65533
       Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                  ACLs: NFSV4 Security Descriptor
                        Control:0x8014
                        SACL - ACEs
                          AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                        DACL - ACEs
                          ALLOW-EVERYONE@-0x1f00a9-FI|DI
                          ALLOW-OWNER@-0x1f01ff-FI|DI
                          ALLOW-GROUP@-0x1200a9-IG
```

使用**CLI**管理**SVM**上的**NTFS**檔案安全性、**NTFS**稽核原則及儲存層級存取保護

用於管理 **SMB NTFS** 檔案安全、**NTFS** 稽核原則和儲存層級存取防護的 **ONTAP** 命令

您可以使用CLI管理儲存虛擬機器（SVM）上的NTFS檔案安全性、NTFS稽核原則及儲存層級存取保護。

您可以從SMB用戶端或使用CLI來管理NTFS檔案安全性和稽核原則。不過、使用CLI來設定檔案安全性和稽核原則、就不需要使用遠端用戶端來管理檔案安全性。使用CLI可大幅縮短使用單一命令在許多檔案和資料夾上套用安全性所需的時間。

您可以設定儲存層級的存取防護、ONTAP 這是由SVM Volume套用的另一層安全防護。儲存層級存取保護適用於從所有NAS傳輸協定存取至套用儲存層級存取保護的儲存物件。

儲存層級的存取保護只能從ONTAP 整套CLI進行設定和管理。您無法從SMB用戶端管理儲存層級的存取保護設定。此外、如果您從NFS或SMB用戶端檢視檔案或目錄上的安全性設定、就不會看到儲存層級的存取保護安全性。即使是系統（Windows或UNIX）管理員、也無法從用戶端撤銷儲存層級的存取保護安全性。因此、儲存層級的存取保護功能可為資料存取提供額外的安全層級、並由儲存管理員獨立設定及管理。

> 即使儲存層級存取保護僅支援NTFS存取權限、ONTAP 但如果UNIX使用者對應至擁有該磁碟區的SVM上的Windows使用者、則可在套用Storage層級存取保護的磁碟區上執行安全性檢查、以透過NFS存取資料。

NTFS安全型磁碟區

NTFS安全型磁碟區和qtree中包含的所有檔案和資料夾都具有NTFS有效安全性。您可以使用 `vserver security file-directory` 命令系列可在 NTFS 安全樣式磁碟區上實作下列類型的安全性：

- 磁碟區中所含檔案和資料夾的檔案權限和稽核原則
- 磁碟區上的儲存層級存取保護安全性

混合式安全型磁碟區

混合式安全型磁碟區和qtree可包含一些具有UNIX有效安全性的檔案和資料夾、並使用UNIX檔案權限、包括模式位元或NFSv4.x ACL和NFSv4.x稽核原則、以及某些具有NTFS有效安全性、並使用NTFS檔案權限和稽核原則的檔案和資料夾。您可以使用 `vserver security file-directory` 命令系列可將下列類型的安全性套用至混合式安全型資料：

- 在混合磁碟區或qtree中、使用NTFS有效安全型態的檔案和資料夾的檔案權限和稽核原則
- 儲存層級的存取保護功能、可用於NTFS和UNIX有效的安全型態磁碟區

UNIX 安全型磁碟區

UNIX安全型磁碟區和qtree包含具有UNIX有效安全性的檔案和資料夾（模式位元或NFSv4.x ACL）。如果您想要使用、請務必謹記下列事項 `vserver security file-directory` 在 UNIX 安全型磁碟區上實作安全功能的命令系列：

- 。 `vserver security file-directory` 命令系列無法用於管理 UNIX 安全性樣式磁碟區和 qtree 上的 UNIX 檔案安全性和稽核原則。
- 您可以使用 `vserver security file-directory` 命令系列可在 UNIX 安全性型磁碟區上設定儲存層級存取保護、前提是目標磁碟區的 SVM 包含 CIFS 伺服器。

相關資訊

- 了解如何查看文件安全和審核策略
- 在伺服器上建立 NTFS 安全描述符
- 配置和應用審核策略到檔案和資料夾的命令
- 了解如何使用儲存級別存取防護來保護文件存取

用於設定 **SMB** 檔案和資料夾安全性的 **ONTAP** 命令

由於您可以在本機套用及管理檔案與資料夾安全性、而無需遠端用戶端介入、因此您可以大幅縮短設定大量檔案或資料夾的大量安全性所需的時間。

在下列使用案例中、您可以使用CLI設定檔案和資料夾的安全性：

- 在大型企業環境中儲存檔案、例如在主目錄中儲存檔案
- 資料移轉
- Windows網域變更
- 跨NTFS檔案系統的檔案安全性與稽核原則標準化

了解使用 **ONTAP** 命令設定 **SMB** 檔案和資料夾安全性時的限制

使用CLI設定檔案和資料夾安全性時、您必須注意特定限制。

- 。 `vserver security file-directory` Command Family 不支援設定 NFSv4 ACL 。

  您只能將NTFS安全性描述元套用至NTFS檔案和資料夾。

使用安全描述符應用 **ONTAP SMB** 檔案和資料夾安全性

安全性描述元包含存取控制清單、可決定使用者可對檔案和資料夾執行的動作、以及使用者存取檔案和資料夾時所稽核的項目。

- 權限

  物件擁有者允許或拒絕權限、並決定物件（使用者、群組或電腦物件）可對指定的檔案或資料夾執行哪些動作。

- 安全性描述元

  安全性描述元是包含安全性資訊的資料結構、可定義與檔案或資料夾相關的權限。

- 存取控制清單（**ACL**）

  存取控制清單是安全性描述元中所包含的清單、其中包含使用者、群組或電腦物件可在套用安全性描述元的檔案或資料夾上執行哪些動作的相關資訊。安全性描述元可包含下列兩種ACL：

  - 判別存取控制清單（DACL）
  - 系統存取控制清單（SACL）

- 任意存取控制清單（**DACL**）

  DACL包含使用者、群組和電腦物件的「小島嶼」清單、這些使用者、群組和電腦物件均可存取或拒絕存取檔案或資料夾上的動作。DACL包含零個以上的存取控制項目（ACE）。

- 系統存取控制清單（**SACL**）

  SACL包含已記錄成功或失敗稽核事件之使用者、群組及電腦物件的「小島嶼」清單。SACL包含零個以上的存取控制項目（ACE）。

- 存取控制項目（**ACE**）

  ACE是DACL或SACL中的個別項目：

  - DACL存取控制項目會指定特定使用者、群組或電腦物件所允許或拒絕的存取權限。
  - SACL存取控制項目會指定在稽核特定使用者、群組或電腦物件執行的指定動作時、要記錄的成功或失敗事件。

- 權限繼承

  權限繼承說明如何將安全性描述元中定義的權限、從父物件傳播到物件。子物件只會繼承可繼承的權限。在父物件上設定權限時、您可以決定資料夾、子資料夾和檔案是否可以使用「套用至」來繼承它們 `this-`

`folder`、`sub-folders`和「檔案」。

相關資訊

- "SMB與NFS稽核與安全性追蹤"
- 配置和應用審核策略到檔案和資料夾的命令

了解如何在 **ONTAP SVM** 災難復原目標上套用使用本機 **SMB** 使用者或群組的檔案目錄策略

如果您的檔案目錄原則組態在安全性描述元、DACL或SACL項目中使用本機使用者或群組、則在ID捨棄組態中的儲存虛擬機器（SVM）災難恢復目的地上套用檔案目錄原則之前、必須謹記一些準則。

您可以為SVM設定災難恢復組態、讓來源叢集上的來源SVM將資料和組態從來源SVM複寫到目的地叢集上的目的地SVM。

您可以設定兩種SVM災難恢復類型之一：

- 身分識別保留

  有了這項組態、SVM和CIFS伺服器的身分識別就會保留下來。

- 身分識別已捨棄

  使用此組態時、SVM和CIFS伺服器的身分識別將不會保留。在此案例中、目的地SVM上的SVM和CIFS伺服器名稱與來源SVM上的SVM和CIFS伺服器名稱不同。

身分識別捨棄組態的準則

在身分識別捨棄組態中、對於包含本機使用者、群組和權限組態的SVM來源、必須變更本機網域名稱（本機CIFS伺服器名稱）、以符合SVM目的地上的CIFS伺服器名稱。例如、如果來源SVM名稱為「'VS1'」、CIFS伺服器名稱為「'CIFS1'」、目的地SVM名稱為「'VS1_DST'」、CIFS伺服器名稱為「'CIFS1_DST'」、則本機使用者的本機網域名稱會自動變更為「CIFS1\user1'上的Cdst_Dst：」

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1          CIFS1\Administrator                     Built-in
administrator account
vs1          CIFS1\user1              -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1_dst      CIFS1_DST\Administrator                 Built-in
administrator account
vs1_dst      CIFS1_DST\user1          -              -
```

雖然本機使用者和群組資料庫中的本機使用者和群組名稱會自動變更、但檔案目錄原則組態中的本機使用者或群組名稱不會自動變更（使用在 CLI 上設定的原則） `vserver security file-directory` Command Family ）。

例如、如果您已設定 DACL 項目、其中會顯示「 'VS1' 」 `-account` 參數設為「 'CIFS1\user1' 」、目的地 SVM 上的設定不會自動變更、以反映目的地的 CIFS 伺服器名稱。

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

您必須使用 `vserver security file-directory modify` 手動將 CIFS 伺服器名稱變更為目的地 CIFS 伺服器名稱的命令。

包含帳戶參數的檔案目錄原則組態元件

有三個檔案目錄原則組態元件可以使用參數設定、這些設定可以包含本機使用者或群組：

- 安全性描述元

  您可以選擇性地指定安全性描述元的擁有者和安全性描述元擁有者的主要群組。如果安全性描述元使用本機使用者或群組做為擁有者和主要群組項目、則必須修改安全性描述元、才能在帳戶名稱中使用目的地SVM。您可以使用 `vserver security file-directory ntfs modify` 命令以對帳戶名稱進行任何必要的變更。

- DACL項目

  每個DACL項目都必須與一個帳戶相關聯。您必須修改任何使用本機使用者或群組帳戶的DACL、才能使用目的地SVM名稱。由於您無法修改現有DACL項目的帳戶名稱、因此您必須從安全性描述元中移除任何具有本機使用者或群組的DACL項目、以修正的目的地帳戶名稱建立新的DACL項目、並將這些新的DACL項目與適當的安全性描述元建立關聯。

- SACL 項目

  每個SACL項目都必須與帳戶建立關聯。您必須修改任何使用本機使用者或群組帳戶的SACL、才能使用目的地SVM名稱。由於您無法修改現有SACL項目的帳戶名稱、因此您必須從安全性描述元中移除具有本機使用者或群組的任何SACL項目、以修正的目的地帳戶名稱建立新的SACL項目、並將這些新的SACL項目與適當的安全性描述元建立關聯。

套用原則之前、您必須對檔案目錄原則組態中使用的本機使用者或群組進行任何必要的變更、否則套用工作會失敗。

使用**CLI**在**NTFS**檔案和資料夾上設定及套用檔案安全性

在 **ONTAP SMB** 伺服器上建立 **NTFS** 安全性描述符

建立NTFS安全性描述元（檔案安全性原則）是設定NTFS存取控制清單（ACL）並套用至儲存虛擬機器（SVM）內的檔案和資料夾的第一步。您可以將安全性描述元與原則工作中的檔案或資料夾路徑建立關聯。

關於這項工作

您可以針對位於NTFS安全型磁碟區內的檔案和資料夾、或是位於混合式安全型磁碟區上的檔案和資料夾、建立NTFS安全性描述元。

根據預設、建立安全性描述元時、會將四個判別存取控制清單（DACL）存取控制項目（ACE）新增至該安全性描述元。四個預設的ACE如下所示：

物件	存取類型	存取權限	權限的套用位置
內建\系統管理員	允許	完全控制	此資料夾、子資料夾、檔案

物件	存取類型	存取權限	權限的套用位置
內建\使用者	允許	完全控制	此資料夾、子資料夾、檔案
建立者擁有者	允許	完全控制	此資料夾、子資料夾、檔案
NT AUTHORITY\系統	允許	完全控制	此資料夾、子資料夾、檔案

您可以使用下列選用參數來自訂安全性描述元組態：

- 安全性描述元的擁有者
- 擁有者的主要群組
- 原始控制旗標

儲存層級存取保護會忽略任何選用參數的值。如需詳細資訊，請參閱 "指令參考資料ONTAP"。

將 **NTFS DACL** 存取控制項目新增至 **ONTAP SMB** 伺服器上的 **NTFS** 安全性描述符

將DACL（判別存取控制清單）存取控制項目（ACE）新增至NTFS安全性描述元、是設定及套用NTFS ACL至檔案或資料夾的第二步驟。每個項目都會識別允許或拒絕存取的物件、並定義物件可以或無法對ACE中定義的檔案或資料夾執行的操作。

關於這項工作

您可以將一或多個 ACE 新增至安全性描述元的 DACL 。

如果安全性描述元包含具有現有 ACE 的 DACL 、則命令會將新的 ACE 新增至 DACL 。如果安全性描述元不包含DACL、則命令會建立DACL並新增新的ACE。

您可以選擇自訂 DACL 項目、方法是指定要允許或拒絕中指定之帳戶的權限 `-account` 參數。有三種互不相容的方法可以指定權限：

- 權利
- 進階權限
- 原始權限（進階權限）

如果您未指定 DACL 項目的權限、則預設會將權限設定為 `Full Control`。

您可以指定如何套用繼承、以選擇性地自訂DACL項目。

儲存層級存取保護會忽略任何選用參數的值。如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

步驟

1. 將 DACL 項目新增至安全性描述元： `vserver security file-directory ntfs dacl add`

```
-vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account
name_or_SIDoptional_parameters

vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
-account domain\joe -rights full-control -apply-to this-folder -vserver vs1
```

2. 驗證 DACL 項目是否正確：`vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
-access-type deny -account domain\joe
```

```
                Vserver: vs1
Security Descriptor Name: sd1
           Allow or Deny: deny
     Account Name or SID: DOMAIN\joe
           Access Rights: full-control
  Advanced Access Rights: -
                Apply To: this-folder
           Access Rights: full-control
```

如"指令參考資料ONTAP"需詳細 `vserver security file-directory ntfs dacl`資訊，請參閱。

建立 ONTAP SMB 安全性策略

為SVM建立檔案安全性原則、是設定及套用ACL至檔案或資料夾的第三個步驟。原則可做為各種工作的容器、其中每項工作都是可套用至檔案或資料夾的單一項目。您可以稍後將工作新增至安全性原則。

關於這項工作

您新增至安全性原則的工作包含NTFS安全性描述元與檔案或資料夾路徑之間的關聯。因此、您應該將安全性原則與每個SVM建立關聯（包含NTFS安全型磁碟區或混合式安全型磁碟區）。

步驟

1. 建立安全性原則：`vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

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

2. 驗證安全性原則：`vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
  ------------     --------------
      vs1              policy1
```

建立原則工作並將其新增至安全性原則、是設定及套用ACL至SVM中的檔案或資料夾的第四個步驟。當您建立原則工作時、會將工作與安全性原則建立關聯。您可以將一或多個工作項目新增至安全性原則。

關於這項工作

安全性原則是工作的容器。工作指的是單一作業、可透過安全性原則對具有NTFS或混合式安全性的檔案或資料夾（或是在設定儲存層級存取保護時、對磁碟區物件執行）。

工作有兩種類型：

- 檔案與目錄工作

  用於指定將安全性描述元套用至指定檔案和資料夾的工作。透過檔案和目錄工作所套用的ACL、可透過SMB用戶端或ONTAP CLI進行管理。

- 儲存層級的存取保護工作

  用於指定將儲存層級存取保護安全性描述元套用至指定磁碟區的工作。透過儲存層級存取保護工作套用的ACL只能透過ONTAP CLI進行管理。

工作包含檔案（或資料夾）或一組檔案（或資料夾）的安全性組態定義。原則中的每項工作都會以路徑唯一識別。在單一原則中、每個路徑只能有一項工作。原則不能有重複的工作項目。

新增工作至原則的準則：

- 每個原則最多可有10、000個工作項目。
- 原則可以包含一或多個工作。

  即使原則可以包含多項工作、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。

- 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。

將工作新增至安全性原則時、您必須指定下列四個必要參數：

- SVM名稱
- 原則名稱
- 路徑
- 與路徑相關聯的安全性描述元

您可以使用下列選用參數來自訂安全性描述元組態：

- 安全類型
- 傳播模式

- 索引位置
- 存取控制類型

儲存層級存取保護會忽略任何選用參數的值。如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

步驟

1. 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 -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` 為的預設值 `-access-control` 參數。設定檔案和目錄存取工作時、可選擇指定存取控制類型。

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
   ```

2. 驗證原則工作組態： `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

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

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access            Security   NTFS        NTFS
   Security
            Path           Control           Type       Mode
   Descriptor Name
   -----    --------       -----------       --------   ------
   ----------------
   1        /home/dir1     file-directory    ntfs       propagate   sd2
   ```

如"指令參考資料ONTAP"需詳細 `vserver security file-directory policy task`資訊，請參閱。

應用 **ONTAP SMB** 安全性策略

將檔案安全性原則套用到SVM是建立NTFS ACL並套用到檔案或資料夾的最後步驟。

關於這項工作

您可以將安全性原則中定義的安全性設定套用至FlexVol 駐留在各處的NTFS檔案和資料夾（NTFS或混合式安全樣式）。

套用稽核原則和相關的SACL時、會覆寫任何現有的DACL。套用安全性原則及其相關的DACL時、會覆寫任何現有的DACL。您應該在建立及套用新的安全性原則之前、先檢閱現有的安全性原則。

步驟

1. 套用安全性原則： `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

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

   原則套用工作已排程、並傳回工作ID。

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id 53322" command to view the status of the operation
   ```

監控 ONTAP SMB 安全性策略作業

將安全性原則套用至儲存虛擬機器（SVM）時、您可以監控安全性原則工作、以監控工作進度。如果您想要確定安全性原則的應用是否成功、這項功能就很有幫助。如果您的工作執行時間很長、而您要將大量安全性套用到大量的檔案和資料夾、這也很有幫助。

關於這項工作

若要顯示安全性原則工作的詳細資訊、您應該使用 `-instance` 參數。

步驟

1. 監控安全性原則工作： `vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

驗證 ONTAP SMB 檔案安全性

您可以驗證檔案安全性設定、確認您套用安全性原則的儲存虛擬機器（SVM）上的檔案或資料夾具有所需的設定。

關於這項工作

您必須提供SVM名稱、其中包含資料、以及您要驗證安全性設定之檔案和資料夾的路徑。您可以使用選用的 `-expand-mask` 顯示安全性設定詳細資訊的參數。

步驟

1. 顯示檔案和資料夾安全性設定： `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

   `vserver security file-directory show -vserver vs1 -path /data/engineering`

```
-expand-mask true
```

```
         Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
          Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
```

```
                           .0.. .... .... .... .... .... .... .... =
Generic Write
                           ..0. .... .... .... .... .... .... .... =
Generic Execute
                           ...0 .... .... .... .... .... .... .... =
Generic All
                           .... ...0 .... .... .... .... .... .... =
System Security
                           .... .... ...1 .... .... .... .... .... =
Synchronize
                           .... .... .... 1... .... .... .... .... =
Write Owner
                           .... .... .... .1.. .... .... .... .... =
Write DAC
                           .... .... .... ..1. .... .... .... .... =
Read Control
                           .... .... .... ...1 .... .... .... .... =
Delete
                           .... .... .... .... .... ...1 .... .... =
Write Attributes
                           .... .... .... .... .... .... 1... .... =
Read Attributes
                           .... .... .... .... .... .... .1.. .... =
Delete Child
                           .... .... .... .... .... .... ..1. .... =
Execute
                           .... .... .... .... .... .... ...1 .... =
Write EA
                           .... .... .... .... .... .... .... 1... =
Read EA
                           .... .... .... .... .... .... .... .1.. =
Append
                           .... .... .... .... .... .... .... ..1. =
Write
                           .... .... .... .... .... .... .... ...1 =
Read

                         ALLOW-Everyone-0x10000000-OI|CI|IO
                           0... .... .... .... .... .... .... .... =
Generic Read
                           .0.. .... .... .... .... .... .... .... =
Generic Write
                           ..0. .... .... .... .... .... .... .... =
Generic Execute
                           ...1 .... .... .... .... .... .... .... =
Generic All
```

```
                                .... ...0 .... .... .... .... .... .... =
System Security
                                .... .... ...0 .... .... .... .... .... =
Synchronize
                                .... .... .... 0... .... .... .... .... =
Write Owner
                                .... .... .... .0.. .... .... .... .... =
Write DAC
                                .... .... .... ..0. .... .... .... .... =
Read Control
                                .... .... .... ...0 .... .... .... .... =
Delete
                                .... .... .... .... .... ...0 .... .... =
Write Attributes
                                .... .... .... .... .... .... 0... .... =
Read Attributes
                                .... .... .... .... .... .... .0.. .... =
Delete Child
                                .... .... .... .... .... .... ..0. .... =
Execute
                                .... .... .... .... .... .... ...0 .... =
Write EA
                                .... .... .... .... .... .... .... 0... =
Read EA
                                .... .... .... .... .... .... .... .0.. =
Append
                                .... .... .... .... .... .... .... ..0. =
Write
                                .... .... .... .... .... .... .... ...0 =
Read
```

使用**CLI**設定稽核原則並套用至**NTFS**檔案和資料夾

用於設定 **SMB** 稽核策略並將其套用至 **NTFS** 檔案和資料夾的 **ONTAP** 命令

使用ONTAP CLI時、您必須執行幾個步驟、才能將稽核原則套用至NTFS檔案和資料夾。首先、您要建立NTFS安全性描述元、然後將SACL新增至安全性描述元。接下來您要建立安全性原則並新增原則工作。然後將安全性原則套用至儲存虛擬機器（SVM）。

關於這項工作

套用安全性原則之後、您可以監控安全性原則工作、然後驗證套用的稽核原則設定。

套用稽核原則和相關的SACL時、會覆寫任何現有的DACL。您應該在建立及套用新的安全性原則之前、先檢閱現有的安全性原則。

相關資訊

- 了解如何使用儲存級別存取防護來保護文件存取
- 了解使用命令設定 SMB 檔案和資料夾安全性時的限制
- 使用安全描述符來應用檔案和資料夾安全性
- "SMB與NFS稽核與安全性追蹤"
- 在伺服器上建立 NTFS 安全描述符

在 **ONTAP SMB** 伺服器上建立 **NTFS** 安全性描述符

建立NTFS安全性描述元稽核原則是設定NTFS存取控制清單（ACL）並套用至位於SVM內的檔案和資料夾的第一步。您將在原則工作中、將安全性描述元與檔案或資料夾路徑建立關聯。

關於這項工作

您可以針對位於NTFS安全型磁碟區內的檔案和資料夾、或是位於混合式安全型磁碟區上的檔案和資料夾、建立NTFS安全性描述元。

根據預設、建立安全性描述元時、會將四個判別存取控制清單（DACL）存取控制項目（ACE）新增至該安全性描述元。四個預設的ACE如下所示：

物件	存取類型	存取權限	權限的套用位置
內建\系統管理員	允許	完全控制	此資料夾、子資料夾、檔案
內建\使用者	允許	完全控制	此資料夾、子資料夾、檔案
建立者擁有者	允許	完全控制	此資料夾、子資料夾、檔案
NT AUTHORITY\系統	允許	完全控制	此資料夾、子資料夾、檔案

您可以使用下列選用參數來自訂安全性描述元組態：

- 安全性描述元的擁有者
- 擁有者的主要群組
- 原始控制旗標

儲存層級存取保護會忽略任何選用參數的值。如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

步驟

1. 如果您要使用進階參數、請將權限等級設為進階： `set -privilege advanced`
2. 建立安全性描述元： `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

```
vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner
DOMAIN\joe
```

3. 驗證安全描述元組態是否正確： `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

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

```
                                    Vserver: vs1
                          Security Descriptor Name: sd1
                    Owner of the Security Descriptor: DOMAIN\joe
```

4. 如果您處於進階權限層級、請返回管理權限層級： `set -privilege admin`

將 **NTFS SACL** 存取控制項目新增至 **ONTAP SMB** 伺服器上的 **NTFS** 安全性描述符

將SACL（系統存取控制清單）存取控制項目（ACE）新增至NTFS安全性描述元、是在SVM中為檔案或資料夾建立NTFS稽核原則的第二步驟。每個項目都會識別您要稽核的使用者或群組。SACL項目會定義您要稽核成功或失敗的存取嘗試。

關於這項工作

您可以將一個或多個ACE新增至安全性描述元的SACL。

如果安全性描述元包含具有現有ACE的SACL、則命令會將新的ACE新增至SACL。如果安全性描述元未包含SACL、則命令會建立SACL並將新的ACE新增至其中。

您可以指定要稽核中所指定帳戶成功或失敗事件的權限、以設定 SACL 項目 `-account` 參數。有三種互不相容的方法可以指定權限：

- 權利
- 進階權限
- 原始權限（進階權限）

如果您未指定 SACL 項目的權限、則預設設定為 `Full Control`。

您可以選擇自訂 SACL 項目、方法是指定如何使用套用繼承 `apply to` 參數。如果您未指定此參數、預設值為將此SACL項目套用至此資料夾、子資料夾及檔案。

步驟

1. 將 SACL 項目新增至安全性描述元： `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

```
vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type
failure -account domain\joe -rights full-control -apply-to this-folder
-vserver vs1
```

2. 驗證 SACL 項目是否正確：`vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

   `vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1 -access-type deny -account domain\joe`

```
                                Vserver: vs1
                    Security Descriptor Name: sd1
         Access type for Specified Access Rights: failure
                         Account Name or SID: DOMAIN\joe
                               Access Rights: full-control
                      Advanced Access Rights: -
                                    Apply To: this-folder
                               Access Rights: full-control
```

建立 **ONTAP SMB** 安全性策略

建立儲存虛擬機器（SVM）的稽核原則、是設定及套用ACL至檔案或資料夾的第三個步驟。原則可做為各種工作的容器、其中每項工作都是可套用至檔案或資料夾的單一項目。您可以稍後將工作新增至安全性原則。

關於這項工作

您新增至安全性原則的工作包含NTFS安全性描述元與檔案或資料夾路徑之間的關聯。因此、您應該將安全性原則與每個儲存虛擬機器（SVM）（包含NTFS安全型磁碟區或混合式安全型磁碟區）建立關聯。

步驟

1. 建立安全性原則：`vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

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

2. 驗證安全性原則：`vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver           Policy Name
  ------------      --------------
      vs1               policy1
```

將任務新增至 **ONTAP SMB** 安全性原則

建立原則工作並將其新增至安全性原則、是設定及套用ACL至SVM中的檔案或資料夾的第四個步驟。當您建立原則工作時、會將工作與安全性原則建立關聯。您可以將一或多個工作項目新增至安全性原則。

關於這項工作

安全性原則是工作的容器。工作指的是單一作業、可透過安全性原則對具有NTFS或混合式安全性的檔案或資料夾（或是在設定儲存層級存取保護時、對磁碟區物件執行）。

工作有兩種類型：

- 檔案與目錄工作

  用於指定將安全性描述元套用至指定檔案和資料夾的工作。透過檔案和目錄工作所套用的ACL、可透過SMB用戶端或ONTAP CLI進行管理。

- 儲存層級的存取保護工作

  用於指定將儲存層級存取保護安全性描述元套用至指定磁碟區的工作。透過儲存層級存取保護工作套用的ACL只能透過ONTAP CLI進行管理。

工作包含檔案（或資料夾）或一組檔案（或資料夾）的安全性組態定義。原則中的每項工作都會以路徑唯一識別。在單一原則中、每個路徑只能有一項工作。原則不能有重複的工作項目。

新增工作至原則的準則：

- 每個原則最多可有10、000個工作項目。
- 原則可以包含一或多個工作。

  即使原則可以包含多項工作、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。

- 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。

您可以使用下列選用參數來自訂安全性描述元組態：

- 安全類型
- 傳播模式
- 索引位置
- 存取控制類型

儲存層級存取保護會忽略任何選用參數的值。如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

步驟

1. 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 -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` 為的預設值 `-access-control` 參數。設定檔案和目錄存取工作時、可選擇指定存取控制類型。

```
vserver security file-directory policy task add -vserver vs1 -policy-name
policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
-index-num 1 -access-control file-directory
```

2. 驗證原則工作組態： `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

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

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

如"指令參考資料ONTAP"需詳細 `vserver security file-directory policy task`資訊，請參閱。

應用 **ONTAP SMB** 安全性策略

將稽核原則套用到SVM是建立NTFS ACL並套用到檔案或資料夾的最後一步。

關於這項工作

您可以將安全性原則中定義的安全性設定套用至FlexVol 駐留在各處的NTFS檔案和資料夾（NTFS或混合式安全樣式）。

> 套用稽核原則和相關的SACL時、會覆寫任何現有的DACL。套用安全性原則及其相關的DACL時、會覆寫任何現有的DACL。您應該在建立及套用新的安全性原則之前、先檢閱現有的安全性原則。

步驟

1. 套用安全性原則： `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

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

   原則套用工作已排程、並傳回工作ID。

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

監控 ONTAP SMB 安全性策略作業

將安全性原則套用至儲存虛擬機器（SVM）時、您可以監控安全性原則工作、以監控工作進度。如果您想要確定安全性原則的應用是否成功、這項功能就很有幫助。如果您的工作執行時間很長、而您要將大量安全性套用到大量的檔案和資料夾、這也很有幫助。

關於這項工作

若要顯示安全性原則工作的詳細資訊、您應該使用 `-instance` 參數。

步驟

1. 監控安全性原則工作： `vserver security file-directory job show -vserver vserver_name`

   ```
   vserver security file-directory job show -vserver vs1
   ```

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

驗證 ONTAP SMB 稽核策略

您可以驗證稽核原則、確認您套用安全性原則的儲存虛擬機器（SVM）上的檔案或資料夾具有所需的稽核安全性設定。

關於這項工作

您可以使用 `vserver security file-directory show` 顯示稽核原則資訊的命令。您必須提供SVM名稱、其中包含您要顯示其檔案或資料夾稽核原則資訊的資料、以及其路徑。

步驟

1. 顯示稽核原則設定： `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

範例

下列命令會顯示套用至SVM VS1路徑「/corp」的稽核原則資訊。這條路徑既成功、也套用成功/失敗的SACL項目：

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

                Vserver: vs1
              File Path: /corp
         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:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

了解如何管理 **ONTAP SMB** 安全性策略作業

如果存在安全性原則工作、在某些情況下、您將無法修改該安全性原則或指派給該原則的工作。您應該瞭解可以修改或無法修改安全性原則的條件、以便成功修改原則。原則的修改包括新增、移除或修改指派給原則的工作、以及刪除或修改原則。

如果該原則的工作存在、且該工作處於下列狀態、則您無法修改安全性原則或指派給該原則的工作：

- 工作正在執行或進行中。
- 工作已暫停。
- 工作會恢復並處於執行中狀態。
- 如果工作正在等待容錯移轉到另一個節點。

在下列情況下、如果安全性原則有工作存在、您可以成功修改該安全性原則或指派給該原則的工作：

- 原則工作已停止。
- 原則工作已成功完成。

用於管理 **SMB** 伺服器上的 **NTFS** 安全描述符的 **ONTAP** 命令

管理安全性描述元時、會ONTAP 有特定的指令檔。您可以建立、修改、刪除及顯示安全性描述元的相關資訊。

如果您想要...	使用此命令...
建立NTFS安全性描述元	`vserver security file-directory ntfs create`
修改現有的NTFS安全性描述元	`vserver security file-directory ntfs modify`
顯示現有NTFS安全性描述元的相關資訊	`vserver security file-directory ntfs show`
刪除NTFS安全性描述元	`vserver security file-directory ntfs delete`

如"指令參考資料ONTAP"需詳細 `vserver security file-directory ntfs`資訊，請參閱。

用於管理 **SMB** 伺服器上的 **NTFS DACL** 存取控制項目的 **ONTAP** 命令

管理ONTAP DACL存取控制項目（ACE）時、會有特定的功能不完整的指令。您可以隨時將ACE新增至NTFS DACL。您也可以在DACL中修改、刪除及顯示有關ACE的資訊、來管理現有的NTFS DACL。

如果您想要...	使用此命令...
建立ACE並將其新增至NTFS DACL	`vserver security file-directory ntfs dacl add`
修改NTFS DACL中的現有ACE	`vserver security file-directory ntfs dacl modify`
顯示NTFS DACL中現有ACE的相關資訊	`vserver security file-directory ntfs dacl show`
從NTFS DACL移除現有的ACE	`vserver security file-directory ntfs dacl remove`

如"指令參考資料ONTAP"需詳細 `vserver security file-directory ntfs dacl`資訊，請參閱。

用於管理 **SMB** 伺服器上的 **NTFS SACL** 存取控制項目的 **ONTAP** 命令

管理ONTAP SACL存取控制項目（ACE）時、會有特定的功能不完整的命令。您可以隨時

將ACE新增至NTFS SACL。您也可以在SACL中修改、刪除及顯示有關ACE的資訊、來管理現有的NTFS SACL。

如果您想要...	使用此命令...
建立ACE並將其新增至NTFS SACL	`vserver security file-directory ntfs sacl add`
修改NTFS SACL中的現有ACE	`vserver security file-directory ntfs sacl modify`
顯示NTFS SACL中現有ACE的相關資訊	`vserver security file-directory ntfs sacl show`
從NTFS SACL移除現有的ACE	`vserver security file-directory ntfs sacl remove`

如"指令參考資料ONTAP"需詳細 `vserver security file-directory ntfs sacl`資訊，請參閱。

用於管理 **SMB** 安全性原則的 **ONTAP** 命令

管理安全性原則時、會ONTAP 有特定的指令檔。您可以顯示原則的相關資訊、也可以刪除原則。您無法修改安全性原則。

如果您想要...	使用此命令...
建立安全性原則	`vserver security file-directory policy create`
顯示安全性原則的相關資訊	`vserver security file-directory policy show`
刪除安全性原則	`vserver security file-directory policy delete`

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

用於管理 **SMB** 安全性原則任務的 **ONTAP** 命令

有一些用來新增、修改、移除及顯示安全性原則工作相關資訊的指令。ONTAP

如果您想要...	使用此命令...
新增安全性原則工作	`vserver security file-directory policy task add`

如果您想要...	使用此命令...
修改安全性原則工作	`vserver security file-directory policy task modify`
顯示安全性原則工作的相關資訊	`vserver security file-directory policy task show`
移除安全性原則工作	`vserver security file-directory policy task remove`

如"指令參考資料ONTAP"需詳細 `vserver security file-directory policy task`資訊，請參閱。

用於管理 **SMB** 安全性原則作業的 **ONTAP** 指令

有一些用來暫停、恢復、停止及顯示安全性原則工作資訊的指令。ONTAP

如果您想要...	使用此命令...
暫停安全性原則工作	`vserver security file-directory job pause -vserver vserver_name -id integer`
恢復安全原則工作	`vserver security file-directory job resume -vserver vserver_name -id integer`
顯示安全性原則工作的相關資訊	`vserver security file-directory job show -vserver vserver_name` 您可以使用此命令來判斷工作的工作 ID 。
停止安全性原則工作	`vserver security file-directory job stop -vserver vserver_name -id integer`

如"指令參考資料ONTAP"需詳細 `vserver security file-directory job`資訊，請參閱。

設定SMB共用的中繼資料快取

了解 **ONTAP SMB** 元資料緩存

中繼資料快取可讓SMB 1.0用戶端上的檔案屬性快取、更快存取檔案和資料夾屬性。您可以啟用或停用每個共用區的屬性快取。如果啟用中繼資料快取、您也可以設定快取項目的即時時間。如果用戶端透過SMB 2.x或SMB 3.0連線至共用區、則不需要設定中繼資料快取。

啟用時、SMB中繼資料快取會在有限的時間內儲存路徑和檔案屬性資料。這可為具有一般工作負載的SMB 1.0用戶端提升SMB效能。

對於某些工作、SMB會建立大量的流量、包括多個相同的路徑和檔案中繼資料查詢。您可以使用SMB中繼資料

快取來從快取擷取資訊、藉此減少備援查詢的數量、並改善SMB 1.0用戶端的效能。

> 雖然不太可能、但中繼資料快取可能會將過時的資訊提供給SMB 1.0用戶端。如果您的環境負擔不起這項風險、則不應啟用此功能。

啟用 **ONTAP SMB** 元資料緩存

您可以啟用SMB中繼資料快取、以改善SMB 1.0用戶端的SMB效能。根據預設、SMB中繼資料快取會停用。

步驟

1. 執行所需的動作：

如果您想要...	輸入命令...
建立共用時啟用SMB中繼資料快取	`vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties attributecache`
在現有共用區上啟用SMB中繼資料快取	`vserver cifs share properties add -vserver` *`vserver_name`* `-share-name` *`share_name`* `-share-properties attributecache`

相關資訊

- 配置元資料快取條目的生存期
- 新增或刪除現有共享的共享屬性

配置 **ONTAP SMB** 元資料快取條目的生命週期

您可以設定SMB中繼資料快取項目的生命週期、以最佳化環境中的SMB中繼資料快取效能。預設值為 10 秒。

開始之前

您必須啟用SMB中繼資料快取功能。如果未啟用SMB中繼資料快取、則不會使用SMB快取TTL設定。

步驟

1. 執行所需的動作：

如果您想要在下列情況下設定**SMB**中繼資料快取項目的生命週期...	輸入命令...
建立共用區	`vserver cifs share -create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-attribute-cache-ttl [integerh][integerm][integers]`
修改現有的共用區	`vserver cifs share -modify -vserver` *`vserver_name`* `-share-name` *`share_name`* `-attribute-cache-ttl [integerh][integerm][integers]`

您可以在建立或修改共用時指定其他共用組態選項和屬性。如"指令參考資料ONTAP"需詳細 `vserver cifs share`資訊，請參閱。

管理檔案鎖定

了解協定之間的 **ONTAP SMB** 檔案鎖定

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

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

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

當NFS用戶端嘗試存取SMB應用程式鎖定的檔案時、會發生下列情況：

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

    檔案將在上次關閉後移除。
  - 不支援 NFS 取消連結作業。

    不支援此功能、因為需要 NTFS 和 SMB 的語言、而且 NFS 不支援上次的「刪除 - 關閉」作業。
  - 對於 UNIX 檔案系統、支援取消連結作業。

    支援此功能、因為需要 NFS 和 UNIX 的語言。
- 重新命名
  - 對於 NTFS 檔案系統、如果目的地檔案是從 SMB 或 CIFS 開啟、則可以重新命名目的地檔案。

- 不支援 NFS 重新命名。

  不支援此功能、因為需要 NTFS 和 SMB 的語言。

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

了解 **ONTAP SMB** 唯讀位

唯讀位元是逐一檔案設定、以反映檔案是可寫入（停用）或唯讀（啟用）。

使用Windows的SMB用戶端可以設定每個檔案的唯讀位元。NFS用戶端不會設定每個檔案的唯讀位元、因為NFS用戶端沒有任何使用每個檔案唯讀位元的傳輸協定作業。

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

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

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

唯讀位元以下列方式與 ACL 和 Unix 模式位元互動：

當檔案設定了唯讀位元：

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

當檔案未設定唯讀位元：

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

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

ONTAP 在處理共用路徑元件上的鎖定時，與 **Windows** 有何不同

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

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

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

顯示有關 **ONTAP SMB** 鎖的信息

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

關於這項工作

無法針對透過NFSv4或NFSv4.1建立的鎖定顯示用戶端IP位址。

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

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

- 位元組範圍鎖定、僅鎖定部分檔案。
- 共用鎖定、可鎖定開啟的檔案。
- 投機鎖定、可控制SMB上的用戶端快取。
- 委派：透過NFSv4.x控制用戶端快取

藉由指定選用參數、您可以決定每種鎖定類型的重要資訊。如"指令參考資料ONTAP"需詳細 `vserver locks show`資訊，請參閱。

步驟

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

範例

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

```
cluster1::> vserver locks show

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

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

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

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
              Lock Protocol: cifs
                  Lock Type: share-level
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                    Vserver: vs1
                     Volume: data2_2
```

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

打破 **ONTAP SMB** 鎖

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

關於這項工作

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

步驟

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

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

2. 將權限層級設為進階： `set -privilege advanced`
3. 執行下列其中一項動作：

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

如果您要指定...來中斷鎖定	輸入命令...
鎖定ID	`vserver locks break -lockid UUID`

4. 返回管理權限層級： `set -privilege admin`

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

監控SMB活動

顯示 ONTAP SMB 會話訊息

您可以顯示已建立SMB工作階段的相關資訊、包括SMB連線和工作階段ID、以及使用工作階段之工作站的IP位址。您可以顯示工作階段SMB傳輸協定版本的相關資訊、以及持續可用的保護層級、協助您識別工作階段是否支援不中斷營運。

關於這項工作

您可以在SVM上以摘要形式顯示所有工作階段的資訊。不過、在許多情況下、傳回的輸出量很大。您可以指定選用參數、自訂輸出中顯示的資訊：

- 您可以使用選用的 `-fields` 參數顯示有關所選欄位的輸出。

  您可以輸入 `-fields ?` 決定您可以使用哪些欄位。

- 您可以使用 `-instance` 顯示已建立 SMB 工作階段的詳細資訊的參數。
- 您可以使用 `-fields` 參數或 `-instance` 參數可以單獨使用、也可以搭配其他選用參數使用。

步驟

1. 執行下列其中一項動作：

如果您要顯示SMB工作階段資訊...	輸入下列命令...
以摘要形式顯示SVM上的所有工作階段	`vserver cifs session show -vserver vserver_name`
在指定的連線ID上	`vserver cifs session show -vserver vserver_name -connection-id integer`
從指定的工作站IP位址	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
在指定的LIF IP位址上	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`

如果您要顯示**SMB**工作階段資訊...	輸入下列命令...
在指定的節點上	`vserver cifs session show -vserver vserver_name -node {node_name
local}`	從指定的Windows使用者
`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`	使用指定的驗證機制
`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1	NTLMv2
Kerberos	Anonymous}`
使用指定的傳輸協定版本	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1
SMB2	SMB2_1
SMB3	SMB3_1}`  [NOTE] ==== 持續可用的保護功能和SMB多通道功能僅適用於SMB 3.0及更新版本的工作階段。若要在所有合格的工作階段中檢視其狀態、您應該指定此參數、並將值設為 `SMB3` 或更新版本。 ====
提供特定等級的持續可用保護	`vserver cifs session show -vserver vserver_name -continuously-available {No
Yes	Partial}`  [NOTE] ==== 如果持續可用的狀態為 `Partial`這表示工作階段至少包含一個開啟的持續可用檔案、但工作階段有一些檔案無法以持續可用的保護開啟。您可以使用 `vserver cifs sessions file show` 命令來判斷已建立工作階段上的哪些檔案未以持續可用的保護開啟。 ====
具有指定的SMB簽署工作階段狀態	`vserver cifs session show -vserver vserver_name -is-session-signed {true

範例

下列命令會顯示SVM VS1上從IP位址為10.1.1的工作站所建立之工作階段的工作階段資訊：

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

下列命令會顯示SVM VS1具有持續可用保護之工作階段的詳細工作階段資訊。連線是使用網域帳戶建立的。

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                      Node: node1
                   Vserver: vs1
                Session ID: 1
              Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
             Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

下列命令會顯示SVM VS1上使用SMB 3.0和SMB多通道之工作階段的工作階段資訊。在此範例中、使用者使用LIF IP位址從具有SMB 3.0功能的用戶端連線到此共用區、因此驗證機制預設為NTLMv2。連線必須使用Kerberos驗證、才能以持續可用的保護進行連線。

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

相關資訊

顯示開啟SMB檔案的相關資訊

顯示有關開啟的 **ONTAP SMB** 檔案的信息

您可以顯示開啟SMB檔案的相關資訊、包括SMB連線和工作階段ID、託管磁碟區、共用名稱和共用路徑。您可以顯示檔案持續可用保護層級的相關資訊、這有助於判斷開啟的檔案是否處於支援不中斷營運的狀態。

關於這項工作

您可以在已建立的SMB工作階段中顯示開啟檔案的相關資訊。當您需要判斷SMB工作階段中特定檔案的SMB工作階段資訊時、所顯示的資訊非常有用。

例如、如果您有 SMB 工作階段、其中某些開啟的檔案會以持續可用的保護開啟、有些則無法以持續可用的保護開啟（的值） `-continuously-available` 欄位輸入 `vserver cifs session show` 命令輸出為 `Partial`）、您可以使用此命令來判斷哪些檔案無法持續使用。

您可以使用、以摘要形式顯示已建立的儲存虛擬機器（ SVM ） SMB 工作階段上所有開啟檔案的資訊 `vserver cifs session file show` 不含任何選用參數的命令。

不過、在許多情況下、傳回的輸出量很大。您可以指定選用參數、自訂輸出中顯示的資訊。如果您只想檢視開啟檔案的一小部分資訊、這項功能就很有幫助。

- 您可以使用選用的 `-fields` 參數、可在您選擇的欄位上顯示輸出。

  您可以單獨使用此參數、也可以搭配其他選用參數一起使用。

- 您可以使用 `-instance` 顯示開啟 SMB 檔案的詳細資訊的參數。

  您可以單獨使用此參數、也可以搭配其他選用參數一起使用。

步驟

1. 執行下列其中一項動作：

如果您要顯示開啟的**SMB**檔案...	輸入下列命令...
在SVM上以摘要形式顯示	`vserver cifs session file show -vserver vserver_name`
在指定的節點上	`vserver cifs session file show -vserver vserver_name -node {node_name
local}`	在指定的檔案ID上
`vserver cifs session file show -vserver vserver_name -file-id integer`	在指定的SMB連線ID上
`vserver cifs session file show -vserver vserver_name -connection-id integer`	在指定的SMB工作階段ID上
`vserver cifs session file show -vserver vserver_name -session-id integer`	在指定的託管Aggregate上
`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`	在指定的磁碟區上
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	在指定的SMB共用區上
`vserver cifs session file show -vserver vserver_name -share share_name`	在指定的SMB路徑上
`vserver cifs session file show -vserver vserver_name -path path`	提供指定等級的持續可用保護

如果您要顯示開啟的**SMB**檔案...	輸入下列命令...
`vserver cifs session file show -vserver vserver_name -continuously-available {No	Yes}`  [NOTE] ==== 如果持續可用的狀態為 `No`這表示這些開啟的檔案無法不中斷地從接管和恢復恢復。在高可用度關係中、他們也無法從合作夥伴之間的一般Aggregate重新配置中恢復。 ====
指定的重新連線狀態	`vserver cifs session file show -vserver vserver_name -reconnected {No

您可以使用其他選用參數來精簡輸出結果。如"指令參考資料ONTAP"需詳細 `vserver cifs session file show` 資訊，請參閱。

範例

下列範例顯示SVM VS1上開啟檔案的相關資訊：

```
cluster1::> vserver cifs session file show -vserver vs1
Node:        node1
Vserver:     vs1
Connection: 3151274158
Session:     1
File     File       Open Hosting               Continuously
ID       Type       Mode Volume     Share      Available
-------- ---------- ---- ---------- ---------- ------------
41       Regular    r    data       data       Yes
Path: \mytest.rtf
```

下列範例顯示SVM VS1上開啟檔案ID為82的SMB檔案的詳細資訊：

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
            CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

相關資訊

顯示會話訊息

確定 ONTAP SMB 伺服器上可用的統計資料、物件和計數器

在取得CIFS、SMB、稽核和BranchCache雜湊統計資料的相關資訊及監控效能之前、您必須先知道哪些物件和計數器可供您取得資料。

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：

如果您想要判斷...	輸入...
可用的物件	`statistics catalog object show`
可用的特定物件	`statistics catalog object show -object object_name`
可用的計數器	`statistics catalog counter show -object object_name`

   如需詳細資訊 `statistics catalog object show`，包括可使用的物件和計數器"指令參考資料ONTAP"，請參閱。

3. 返回管理權限層級： `set -privilege admin`

範例

下列命令會顯示與叢集中CIFS和SMB存取相關之所選統計物件的說明、如進階權限層級所示：

```
cluster1::> set -privilege advanced

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

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

下列命令會顯示的一些計數器相關資訊 `cifs` 進階權限層級的物件：

此範例不會顯示的所有可用計數器 `cifs` 物件；輸出被截斷。

```
cluster1::> set -privilege advanced

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

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
-----------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                                vserver_1:10.72.205.179
    instance_uuid                                       2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

相關資訊

- 顯示統計資料

- "統計目錄計數器顯示對象"
- "統計開始"

顯示 **ONTAP SMB** 統計資料

您可以顯示各種統計資料、包括CIFS和SMB、稽核和BranchCache雜湊的統計資料、以監控效能並診斷問題。

開始之前

您必須使用收集資料樣本 `statistics start` 和 `statistics stop` 顯示物件相關資訊之前的命令。

詳細了解 `statistics start`和 `statistics stop`在"指令參考資料ONTAP" 。

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：

如果您要顯示下列項目的統計資料...	輸入...
SMB的所有版本	`statistics show -object cifs`
SMB 1.0	`statistics show -object smb1`
SMB 2.x和SMB 3.0	`statistics show -object smb2`
節點的CIFS子系統	`statistics show -object nblade_cifs`
多重傳輸協定稽核	`statistics show -object audit_ng`
BranchCache雜湊服務	`statistics show -object hashd`
動態DNS	`statistics show -object ddns_update`

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

3. 返回管理權限層級： `set -privilege admin`

相關資訊

- 確定伺服器上可用的統計資料、物件和計數器
- 監控SMB簽署的工作階段統計資料
- 顯示BranchCache統計資料
- 使用統計資料來監控自動節點參照活動
- "Microsoft Hyper-V和SQL Server的SMB組態"

- "效能監控設定"

部署SMB用戶端型服務

使用離線檔案來允許快取檔案以供離線使用

了解如何使用離線檔案來允許快取 **ONTAP SMB** 檔案以供離線使用

支援Microsoft離線檔案功能（或用戶端快取）、可在本機主機上快取檔案以供離線使用。ONTAP即使使用者與網路中斷連線、仍可使用離線檔案功能繼續處理檔案。

您可以指定Windows使用者文件和程式是自動快取到共用區、還是必須手動選取檔案以供快取。預設會針對新共用啟用手動快取。離線使用的檔案會同步處理至Windows用戶端的本機磁碟。當連線至特定儲存系統共用區的網路連線恢復時、就會發生同步。

由於離線檔案和資料夾的存取權限與儲存在CIFS伺服器上的檔案和資料夾版本相同、因此使用者必須對儲存在CIFS伺服器上的檔案和資料夾擁有足夠的權限、才能對離線檔案和資料夾執行動作。

當使用者和網路上的其他人變更同一個檔案時、使用者可以將檔案的本機版本儲存到網路、保留其他版本、或同時儲存兩者。如果使用者同時保留這兩個版本、則會在本機儲存含有本機使用者變更的新檔案、而快取的檔案會被保存在CIFS伺服器上的檔案版本變更所覆寫。

您可以使用共用組態設定、逐一設定離線檔案。您可以在建立或修改共用時、從四個離線資料夾組態中選擇一個：

- 無快取

  停用共用區的用戶端快取。檔案和資料夾不會自動在本機用戶端上快取、而且使用者無法選擇在本機快取檔案或資料夾。

- 手動快取

  可手動選取要快取至共用區的檔案。這是預設設定。根據預設、不會在本機用戶端上快取任何檔案或資料夾。使用者可以選擇要在本機快取以供離線使用的檔案和資料夾。

- 自動文件快取

  可讓使用者文件自動快取至共用區。只有存取的檔案和資料夾才會在本機快取。

- 自動程式快取

  可讓程式和使用者文件自動快取至共用區。只有存取的檔案、資料夾和程式才會在本機快取。此外、此設定可讓用戶端執行本機快取的可執行檔、即使連線到網路也沒問題。

如需在Windows伺服器和用戶端上設定離線檔案的詳細資訊、請參閱Microsoft TechNet資源庫。

相關資訊

- 使用漫遊設定檔、將使用者設定檔集中儲存在與SVM相關的CIFS伺服器上
- 了解如何使用資料夾重新導向在伺服器上儲存數據

- 了解如何使用 BranchCache 在分公司快取共享內容
- "Microsoft TechNet程式庫：technet.microsoft.com/en-us/library/"

了解使用離線 **ONTAP SMB** 檔案的要求

在CIFS伺服器上使用Microsoft離線檔案功能之前、您必須先知道ONTAP 哪些版本的支援功能、以及哪些Windows用戶端支援該功能。

版本需求**ONTAP**

發行支援離線檔案。ONTAP

SMB傳輸協定版本需求

對於儲存虛擬機器（SVM）、ONTAP 支援所有SMB版本上的離線檔案。

Windows用戶端需求

Windows用戶端必須支援離線檔案。

如需哪些Windows用戶端支援離線檔案功能的最新資訊、請參閱互通性對照表。

"mysupport.netapp.com/matrix"

部署離線 **ONTAP SMB** 檔案的指南

當您在具有的主目錄共用上部署離線檔案時、需要瞭解一些重要準則 `showsnapshot` 在主目錄上共用屬性集。

如果 `showsnapshot`共用內容是在已設定離線檔案的主目錄共用上設定， `Windows` 用戶端會快取使用者主目錄資料夾下的所有快照 `~snapshot`。

如果下列其中一項為真，則 Windows 用戶端會快取主目錄下的所有快照：

- 使用者可從用戶端離線使用主目錄。

  的內容 `~snapshot` 主目錄中的資料夾會隨附並可供離線使用。

- 使用者可設定資料夾重新導向以重新導向等資料夾 `My Documents` 位於 CIFS 伺服器共用上主目錄的根目錄。

  某些Windows用戶端可能會自動讓重新導向的資料夾離線使用。如果資料夾重新導向至主目錄的根目錄、則會重新導向 `~snapshot` 資料夾包含在快取的離線內容中。

> 應避免將資料夾包含在離線檔案中的離線檔案部署 `~snapshot`。資料夾中的快照 `~snapshot`包含磁碟區上 ONTAP 建立快照的所有資料。因此，建立資料夾的離線複本 `~snapshot`會消耗用戶端上的大量本機儲存空間，在離線檔案同步期間消耗網路頻寬，並增加同步離線檔案所需的時間。

用於設定離線 **SMB** 檔案支援的 **ONTAP** 命令

您可以在ONTAP 建立SMB共用時、或隨時修改現有的SMB共用時、指定四個離線檔案設定之一、使用支援的還原CLI來設定離線檔案。手動離線檔案支援為預設設定。

關於這項工作

設定離線檔案支援時、您可以選擇下列四種離線檔案設定之一：

設定	說明
`none`	不允許Windows用戶端快取此共用區上的任何檔案。
`manual`	可讓Windows用戶端上的使用者手動選取要快取的檔案。
`documents`	允許Windows用戶端快取使用者用於離線存取的使用者文件。
`programs`	允許Windows用戶端快取使用者用於離線存取的程式。即使共用可用、用戶端仍可在離線模式下使用快取的程式檔案。

您只能選擇一個離線檔案設定。如果您修改現有SMB共用區上的離線檔案設定、新的離線檔案設定會取代原始設定。其他現有的SMB共用組態設定和共用內容不會移除或取代。它們會一直有效、直到明確移除或變更為止。

步驟

1. 執行適當的行動：

如果您要設定離線檔案於...	輸入命令...
新的SMB共用區	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none
manual	documents
programs}`	現有的SMB共用區
`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none	manual
documents	programs}`

2. 確認 SMB 共用組態正確無誤：`vserver cifs share show -vserver vserver_name -share -name share_name -instance`

範例

下列命令會建立名為「 data1 」的 SMB 共用、並將離線檔案設為 `documents`：

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                Share Properties: oplocks
                                  browsable
                                  changenotify
              Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                   Share Comment: Offline files
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: documents
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

下列命令會將離線檔案設定變更為、以修改名為「 data1 」的現有 SMB 共用 `manual` 以及新增檔案和目錄模式建立遮罩的值：

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
          CIFS Server NetBIOS Name: VS1
                             Path: /data1
                  Share Properties: oplocks
                                    browsable
                                    changenotify
                Symlink Properties: enable
           File Mode Creation Mask: 644
      Directory Mode Creation Mask: 777
                   Share Comment: Offline files
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

相關資訊

新增或刪除現有共享的共享屬性

使用電腦管理 **MMC** 設定 **ONTAP SMB** 共享上的離線文件支持

如果您想要允許使用者在本機快取檔案以供離線使用、您可以使用電腦管理MMC（Microsoft管理主控台）來設定離線檔案支援。

步驟

1. 若要在Windows伺服器上開啟MMC、請在Windows檔案總管中、以滑鼠右鍵按一下本機電腦的圖示、然後選取*管理*。
2. 在左側面板上、選取*電腦管理*。
3. 選取*「行動*」>*「連線到另一台電腦*」。

   「選取電腦」對話方塊隨即出現。

4. 輸入CIFS伺服器名稱、或按一下*瀏覽*以尋找CIFS伺服器。

   如果CIFS伺服器名稱與儲存虛擬機器（SVM）主機名稱相同、請輸入SVM名稱。如果CIFS伺服器名稱與SVM主機名稱不同、請輸入CIFS伺服器名稱。

5. 按一下「確定」。
6. 在主控台樹狀目錄中、按一下「系統工具」>「共用資料夾」。
7. 按一下*共享*。
8. 在結果窗格中、以滑鼠右鍵按一下共用區。
9. 按一下*「內容」*。

   顯示所選共用的內容。

10. 在*一般*索引標籤中、按一下*離線設定*。

    「離線設定」對話方塊隨即出現。

11. 視需要設定離線可用度選項。
12. 按一下「確定」。

使用漫遊設定檔、將使用者設定檔集中儲存在與**SVM**相關的**SMB**伺服器上

了解如何使用漫遊設定檔集中儲存 **ONTAP SMB** 使用者設定檔

支援將Windows漫遊設定檔儲存在與儲存虛擬機器（SVM）相關聯的CIFS伺服器上。ONTAP設定使用者漫遊設定檔可為使用者帶來許多優勢、例如無論使用者登入的位置為何、自動提供資源可用度。漫遊設定檔也能簡化使用者設定檔的管理。

漫遊使用者設定檔具有下列優點：

- 自動資源可用度

  當使用者登入網路上執行Windows 8、Windows 7、Windows 2000或Windows XP的任何電腦時、就會自動使用該使用者的唯一設定檔。使用者不需要在網路上使用的每部電腦上建立設定檔。

- 簡化電腦更換作業

  由於使用者的所有設定檔資訊都是在網路上個別維護、因此使用者的設定檔可以輕鬆下載到新的替換電腦上。當使用者第一次登入新電腦時、使用者設定檔的伺服器複本會複製到新電腦。

相關資訊

- 了解如何使用離線檔案來快取檔案以供離線使用
- 了解如何使用資料夾重新導向在伺服器上儲存數據

了解使用漫遊 **ONTAP SMB** 設定檔的要求

在您將Microsoft的漫遊設定檔搭配CIFS伺服器使用之前、您必須先知道ONTAP 哪些版本的支援功能、以及哪些Windows用戶端支援此功能。

版本需求**ONTAP**

支援漫遊設定檔。ONTAP

SMB傳輸協定版本需求

對於儲存虛擬機器（SVM）、ONTAP 支援所有SMB版本上的漫遊設定檔。

Windows用戶端需求

在使用者使用漫遊設定檔之前、Windows用戶端必須支援此功能。

如需哪些Windows用戶端支援漫遊設定檔的最新資訊、請參閱互通性對照表。

"NetApp 互通性對照表工具"

透過 Active Directory 使用者和電腦 MMC 設定漫遊 ONTAP SMB 設定檔

如果您想要在使用者登入網路上的任何電腦時、自動讓使用者的設定檔可供使用、您可以透過Active Directory使用者和電腦MMC嵌入式管理單元來設定漫遊設定檔。如果您在 Windows Server 上設定漫遊設定檔、則可以使用 Active Directory 管理中心。

步驟

1. 在 Windows 伺服器上、開啟 Active Directory 使用者和電腦 MMC （或 Windows 伺服器上的 Active Directory 管理中心）。
2. 找出您要設定漫遊設定檔的使用者。
3. 在使用者上按一下滑鼠右鍵、然後按一下「內容」。
4. 在 * 設定檔 * 索引標籤上、輸入您要儲存使用者漫遊設定檔之共用的設定檔路徑、然後輸入 `%username%`。

   例如、設定檔路徑可能如下： `\\vs1.example.com\profiles\%username%`。使用者第一次登入時、 `%username%` 以使用者名稱取代。

   > 在路徑中 `\\vs1.example.com\profiles\%username%`、 `profiles` 是儲存虛擬機器（ SVM ） VS1 上具有「 Everyone 完全控制」權限的共用名稱。

5. 按一下「確定」。

使用資料夾重新導向將資料儲存在SMB伺服器上

了解如何使用資料夾重新導向在 ONTAP SMB 伺服器上儲存數據

支援Microsoft資料夾重新導向、可讓使用者或系統管理員將本機資料夾路徑重新導向至CIFS伺服器上的位置。ONTAP即使資料儲存在SMB共用區、重新導向的資料夾仍會顯示為儲存在本機Windows用戶端上。

資料夾重新導向主要是針對已部署主目錄、且想要維持與現有主目錄環境相容性的組織。

- `Documents`、 `Desktop`和 `Start Menu` 是您可以重新導向的資料夾範例。
- 使用者可以從Windows用戶端重新導向資料夾。
- 系統管理員可以在Active Directory中設定GPO、集中設定及管理資料夾重新導向。
- 如果系統管理員已設定漫遊設定檔、資料夾重新導向可讓系統管理員將使用者資料與設定檔資料分開。

- 系統管理員可以同時使用資料夾重新導向和離線檔案、將本機資料夾的資料儲存區重新導向至CIFS伺服器、同時允許使用者在本機快取內容。

相關資訊

- 了解如何使用離線檔案來快取檔案以供離線使用
- 使用漫遊設定檔、將使用者設定檔集中儲存在與SVM相關的CIFS伺服器上

了解使用 ONTAP SMB 資料夾重新導向的要求

在您將Microsoft的資料夾重新導向用於CIFS伺服器之前、您必須先知道ONTAP 哪些版本的支援功能、以及哪些Windows用戶端支援此功能。

版本需求ONTAP

支援Microsoft資料夾重新導向。ONTAP

SMB傳輸協定版本需求

對於儲存虛擬機器（SVM）、ONTAP 支援Microsoft在所有SMB版本上的資料夾重新導向。

Windows用戶端需求

在使用者使用Microsoft的資料夾重新導向之前、Windows用戶端必須支援此功能。

如需哪些Windows用戶端支援資料夾重新導向的最新資訊、請參閱互通性對照表。

"mysupport.netapp.com/matrix"

使用 Windows 屬性配置 ONTAP SMB 資料夾重新導向

您可以使用Windows內容視窗來設定資料夾重新導向。使用此方法的優點是Windows使用者可以設定資料夾重新導向、而無需SVM管理員的協助。

步驟

1. 在Windows檔案總管中、以滑鼠右鍵按一下您要重新導向至網路共用的資料夾。
2. 按一下*「內容」*。

   顯示所選共用的內容。

3. 在*捷徑*索引標籤中、按一下*目標*、然後指定您要重新導向所選資料夾的網路位置路徑。

   例如、如果您要將資料夾重新導向至 `data` 對應至之主目錄中的資料夾 `Q:\`、請指定 `Q:\data` 成為目標。

4. 按一下「確定」。

   如需設定離線資料夾的詳細資訊、請參閱Microsoft TechNet資源庫。

相關資訊

"Microsoft TechNet程式庫：technet.microsoft.com/en-us/library/"

了解如何使用 **SMB 2.x** 從 **Windows** 用戶端存取 **ONTAP ~snapshot** 目錄

您使用 SMB 2.x 從 Windows 用戶端存取目錄的方法與 SMB 1.0 使用的方法 `~snapshot` 不同。使用 SMB 2.x 連線成功存取儲存在快照中的資料時，您必須瞭解如何存取 `~snapshot`目錄。

SVM 管理員可控制 Windows 用戶端上的使用者是否可以檢視及存取 `~snapshot` 啟用或停用、即可在共用上建立目錄 `showsnapshot` 使用 vserver CIFS 共用內容系列中的命令來共用內容。

> `showsnapshot`停用共用內容時，使用 `SMB 2.x` 的 `Windows` 用戶端上的使用者無法檢視 `~snapshot`目錄，也無法存取目錄中的快照，即使手動輸入目錄路徑或目錄中的特定快照 `~snapshot`也 `~snapshot`一樣。

當 `showsnapshot` 共用內容已啟用、使用 SMB 2.x 的 Windows 用戶端上的使用者仍無法檢視 `~snapshot` 目錄位於共享區的根目錄、或位於共享區根目錄下的任何交會或目錄內。不過、連線至共用之後、使用者就可以存取隱藏的 `~snapshot` 手動附加目錄 `\~snapshot` 至共用路徑的結尾。隱藏的 `~snapshot` 目錄可從兩個入口點存取：

- 位於共用區的根目錄
- 在共享空間的每個交會點

隱藏的 `~snapshot` 無法從共享區內的非連接子目錄存取目錄。

範例

使用下列範例所示的組態、 Windows 用戶端上有 SMB 2.x 連線至「 'eng' 」共用的使用者可以存取 `~snapshot` 手動附加目錄 `\~snapshot` 到共享區根目錄和路徑中每個連接點的共享路徑。隱藏的 `~snapshot` 目錄可從下列三個路徑存取：

- `\\vs1\eng\~snapshot`
- `\\vs1\eng\projects1\~snapshot`
- `\\vs1\eng\projects2\~snapshot`

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume       junction-path
------- ------------ ----------------------------------------
vs1     vs1_root      /
vs1     vs1_vol1      /eng
vs1     vs1_vol2      /eng/projects1
vs1     vs1_vol3      /eng/projects2

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

使用舊版還原檔案和資料夾

了解如何使用先前的版本還原 **ONTAP SMB** 檔案和資料夾

使用 Microsoft 舊版的功能適用於支援某種形式的快照並啟用快照的檔案系統。Snapshot技術是ONTAP 不可或缺的一部分。使用者可以使用 Microsoft 舊版功能，從 Windows 用戶端的快照中復原檔案和資料夾。

舊版功能可讓使用者瀏覽快照或從快照還原資料，而無需儲存管理員介入。無法設定舊版。此功能一律啟用。如果儲存管理員已在共用上提供快照，則使用者可以使用舊版來執行下列工作：

- 恢復意外刪除的檔案。
- 從意外覆寫檔案中恢復。
- 在工作時比較檔案版本。

儲存在快照中的資料是唯讀的。使用者必須將檔案複本儲存到其他位置、才能對檔案進行任何變更。快照會定期刪除；因此，如果使用者想要無限期保留舊版檔案，則需要建立舊版檔案的複本。

使用 **Microsoft** 早期版本的 **ONTAP SMB** 需求

在您將舊版CIFS伺服器搭配使用之前、您必須先知道ONTAP 哪些版本的支援哪些版本的支援、以及哪些Windows用戶端支援哪些版本。您也需要知道快照設定需求。

版本需求**ONTAP**

支援舊版。

SMB傳輸協定版本需求

對於儲存虛擬機器（SVM）、ONTAP 支援所有SMB版本上的舊版。

Windows用戶端需求

使用者必須先支援此功能，才能使用舊版存取快照中的資料。

如需哪些Windows用戶端支援舊版的最新資訊、請參閱互通性對照表。

"NetApp 互通性對照表工具"

快照設定需求

若要使用舊版存取快照中的資料，啟用的快照原則必須與包含資料的磁碟區相關聯，用戶端必須能夠存取快照資料，而且快照必須存在。

使用 **Windows Previous Versions** 標籤檢視和管理 **ONTAP SMB** 快照數據

Windows 用戶端機器上的使用者可以使用 Windows 內容視窗上的舊版索引標籤來還原快照中儲存的資料，而不需要儲存虛擬機器（ SVM ）管理員介入。

關於這項工作

如果管理員已在包含共享區的磁碟區上啟用快照，且管理員將共用區設定為顯示快照，則您只能使用「舊版」索引標籤來檢視和管理儲存在 SVM 上資料快照中的資料。

步驟

1. 在Windows檔案總管中、顯示儲存在CIFS伺服器上之資料對應磁碟機的內容。
2. 以滑鼠右鍵按一下您要檢視或管理其快照的對應網路磁碟機中的檔案或資料夾。
3. 按一下*「內容」*。

   隨即顯示所選檔案或資料夾的內容。

4. 按一下*舊版*索引標籤。

   所選檔案或資料夾的可用快照清單會顯示在資料夾版本：方塊中。列出的快照會以快照名稱首碼和建立時間戳記來識別。

5. 在「資料夾版本：」方塊中、以滑鼠右鍵按一下您要管理的檔案或資料夾複本。
6. 執行適當的行動：

如果您想要...	請執行下列動作...
檢視該快照的資料	按一下「開啟」。
從該快照建立資料複本	按一下 * 複本 * 。

   快照中的資料是唯讀的。如果您想要修改「舊版」索引標籤中所列的檔案和資料夾、則必須將您要修改的檔案和資料夾複本儲存到可寫入的位置、並對複本進行修改。

7. 管理完快照資料後，按一下 * 確定 * ，關閉 * 內容 * 對話方塊。

   如需使用 [舊版] 索引標籤檢視及管理快照資料的詳細資訊，請參閱 Microsoft TechNet Library 。

相關資訊

"Microsoft TechNet程式庫：technet.microsoft.com/en-us/library/"

確定 ONTAP SMB 快照是否可供先前版本使用

只有在已啟用的快照原則套用至包含共用的磁碟區，且磁碟區組態允許存取快照時，才能從「舊版」索引標籤檢視快照。判斷快照可用度有助於協助使用者存取舊版。

步驟

1. 判斷共用資料所在的磁碟區是否已啟用自動快照，以及用戶端是否可存取快照目錄： `volume show -vserver vserver-name -volume volume-name -fields vserver,volume,snapdir-access,snapshot-policy,snapshot-count`

   輸出會顯示與磁碟區相關的快照原則，是否啟用用戶端快照目錄存取，以及可用快照的數量。

2. 判斷是否已啟用相關的快照原則： `volume snapshot policy show -policy policy-name`
3. 列出可用的快照： `volume snapshot show -volume volume_name`

   如需設定及管理快照原則和快照排程的詳細資訊，請參閱"資料保護"。

範例

以下範例顯示與名為「 data1 」的磁碟區相關的快照原則資訊，該磁碟區包含「 data1 」上的共用資料和可用快照。

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-------- ------ -------------- --------------- --------------
vs1      data1  true           default         10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1
                   Number of Is
Policy Name        Schedules Enabled Comment
------------------ --------- ------- ---------------------------------
default                   3 true    Default policy with hourly, daily &
weekly schedules.
    Schedule         Count     Prefix                  SnapMirror Label
    ---------------- -----     ----------------------- -------------------
    hourly               6     hourly                  -
    daily                2     daily                   daily
    weekly               2     weekly                  weekly

cluster1::> volume snapshot show -volume data1
                                                                 ---Blocks---
Vserver  Volume  Snapshot                  State        Size Total% Used%
-------- ------- ------------------------- -------- -------- ------ -----
vs1      data1
                 weekly.2012-12-16_0015    valid       408KB     0%    1%
                 daily.2012-12-22_0010     valid       420KB     0%    1%
                 daily.2012-12-23_0010     valid       192KB     0%    0%
                 weekly.2012-12-23_0015    valid       360KB     0%    1%
                 hourly.2012-12-23_1405    valid       196KB     0%    0%
                 hourly.2012-12-23_1505    valid       196KB     0%    0%
                 hourly.2012-12-23_1605    valid       212KB     0%    0%
                 hourly.2012-12-23_1705    valid       136KB     0%    0%
                 hourly.2012-12-23_1805    valid       200KB     0%    0%
                 hourly.2012-12-23_1905    valid       184KB     0%    0%
```

相關資訊

- 建立快照配置以啟用先前版本的訪問
- "資料保護"

建立 ONTAP SMB 快照配置以啟用先前版本的訪問

只要啟用用戶端對快照的存取權，且快照存在，舊版功能就永遠可用。如果您的快照組態不符合這些需求，您可以建立一個快照組態，

步驟

1. 如果包含您要允許舊版存取之共用區的磁碟區沒有相關聯的快照原則，請將快照原則與磁碟區建立關聯，然後使用命令加以啟用 `volume modify`。

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

2. 使用命令將選項設定為 `true`，以 `-snap-dir`啟用快照的存取 `volume modify`。

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

3. 使用和 `volume snapshot policy show`命令確認已啟用快照原則，且已啟用快照目錄的存取 `volume show`。

   深入瞭解 `volume show`及 `volume snapshot policy show` "指令參考資料ONTAP"。

   如需設定及管理快照原則和快照排程的詳細資訊，請參閱"資料保護"。

相關資訊

"資料保護"

了解如何還原包含 **ONTAP SMB** 連線點的先前版本目錄

使用舊版還原包含連接點的資料夾時、請務必謹記某些準則。

使用舊版還原具有子資料夾的子資料夾時、還原可能會因為而失敗 `Access Denied` 錯誤。

您可以使用來判斷您嘗試還原的資料夾是否包含連接 `vol show` 命令 `-parent` 選項。您也可以使用 `vserver security trace` 建立檔案與資料夾存取問題詳細記錄的命令。

相關資訊

在NAS命名空間中建立及管理資料磁碟區

部署SMB伺服器型服務

管理主目錄

了解如何在 **ONTAP SMB** 伺服器上啟用動態主目錄

利用支援支援的主目錄、您可以根據連線的使用者及一組變數、設定對應至不同目錄的SMB共用區。ONTAP您可以使用幾個主目錄參數來設定一個共用區、以定義使用者在入口點（共享區）和主目錄（SVM上的目錄）之間的關係、而非為每個使用者建立個別的共用區。

以訪客使用者身分登入的使用者沒有主目錄、也無法存取其他使用者的主目錄。有四個變數可決定使用者如何對應至目錄：

- 共享名稱

  這是您建立的共用名稱、使用者可連線至該共用。您必須設定此共用的主目錄屬性。

共用名稱可以使用下列動態名稱：

- `%w` （使用者的 Windows 使用者名稱）
- `%d` （使用者的 Windows 網域名稱）
- `%u` （使用者對應的 UNIX 使用者名稱） 若要讓共用名稱在所有主目錄中都是唯一的、共用名稱必須包含/`%w` 或 `%u` 變動。共用名稱可以同時包含 `%d` 和/`%w` 變數（例如、 `%d/%w`）、或共享區名稱可以包含靜態部分和可變部分（例如 hom_ ）/`%w`）。

- 共享路徑

  這是由共用定義的相對路徑、因此會與其中一個共用名稱相關聯、並附加到每個搜尋路徑、以從SVM根目錄產生使用者的完整主目錄路徑。它可以是靜態的（例如、 `home`）、動態（例如、 `%w`）、或兩者的組合（例如、 `eng/%w`）。

- 搜尋路徑

  這是從SVM根目錄開始的一組絕對路徑、您可以指定這些路徑來引導ONTAP 針對主目錄進行搜尋。您可以使用命令來指定一或多個搜尋路徑 `vserver cifs home-directory search-path add`。如果您指定多個搜尋路徑、ONTAP 則在找到有效路徑之前、將會依照指定的順序嘗試這些路徑。如"指令參考資料ONTAP"需詳細 `vserver cifs home-directory search-path add`資訊，請參閱。

- 目錄

  這是您為使用者建立的使用者主目錄。目錄名稱通常是使用者的名稱。您必須在搜尋路徑所定義的其中一個目錄中建立主目錄。

舉例來說、請考慮下列設定：

- 使用者：John Smith
- 使用者網域：Acme
- 使用者名稱：jsmith
- SVM名稱：VS1
- 主目錄共用名稱 #1 ： hom_ `%w` - 共享路徑： `%w`
- 主目錄共用名稱 #2 ： `%w` - 共享路徑： `%d/%w`
- 搜尋路徑 #1 ： `/vol0home/home`
- 搜尋路徑 #2 ： `/vol1home/home`
- 搜尋路徑 #3 ： `/vol2home/home`
- 主目錄： `/vol1home/home/jsmith`

案例 1 ：使用者連線至 `\\vs1\home_jsmith`。這會比對第一個主目錄共用名稱、並產生相對路徑 `jsmith`。ONTAP 現在會搜尋名為的目錄 `jsmith` 依序檢查每個搜尋路徑：

- `/vol0home/home/jsmith` 不存在；請繼續搜尋路徑 #2 。
- `/vol1home/home/jsmith` 存在；因此不會核取搜尋路徑 #3 ；使用者現在已連線至其主目錄。

案例 2 ：使用者連線至 `\\vs1\jsmith`。這會比對第二個主目錄共用名稱、並產生相對路徑 `acme/jsmith`

。ONTAP 現在會搜尋名為的目錄 acme/jsmith 依序檢查每個搜尋路徑：

- /vol0home/home/acme/jsmith 不存在；請繼續搜尋路徑 #2 。
- /vol1home/home/acme/jsmith 不存在；請繼續搜尋路徑 #3 。
- /vol2home/home/acme/jsmith 不存在；主目錄不存在；因此連線失敗。

主目錄共用

新增 **ONTAP SMB** 主目錄共享

如果您想要使用SMB主目錄功能、則必須將至少一個共用新增至共用內容中包含的主目錄內容。

關於這項工作

您可以在使用建立共用時建立主目錄共用 vserver cifs share create 命令、或者您可以隨時使用將現有共用變更為主目錄共用 vserver cifs share modify 命令。

若要建立主目錄共用、您必須包含 homedirectory 中的值 -share-properties 建立或修改共用時的選項。您可以使用使用者連線至其主目錄時動態擴充的變數來指定共用名稱和共用路徑。您可以在路徑中使用的可用變數有 %w、 %d`和 `%u，分別對應於 Windows 使用者名稱、網域及對應的 UNIX 使用者名稱。

步驟

1. 新增主目錄共用：
   vserver cifs share create -vserver *vserver_name* -share-name *share_name* -path *path* -share-properties homedirectory[,…]

   -vserver vserver 指定要新增搜尋路徑的 CIFS 儲存虛擬機器（ SVM ）。

   -share-name *share-name* 指定主目錄共用名稱。

   除了包含其中一個必要的變數之外、如果共用名稱包含其中一個文字字串 %w、 %u`或 `%d，您必須在文字字串前面加上 % （百分比）字元，以防止 ONTAP 將文字字串視為變數（例如， %%w）。

   - 共用名稱必須包含 %w 或 %u 變動。
   - 共用名稱也可以包含 %d 變數（例如、 %d/%w）或共享區名稱中的靜態部分（例如 home1_/%w）。
   - 如果系統管理員使用該共用區來連線至其他使用者的主目錄、或是允許使用者連線至其他使用者的主目錄、則動態共用名稱模式的前面必須有一個字首符號（~）。

     。 vserver cifs home-directory modify 用於透過設定來啟用此存取 -is-home-dirs -access-for-admin-enabled 選項 true）或設定進階選項 -is-home-dirs-access-for -public-enabled 至 true。

   -path path 指定主目錄的相對路徑。

-share-properties homedirectory[,…] 指定該共用的共用內容。您必須指定 homedirectory 價值。您可以使用以逗號分隔的清單來指定其他共用屬性。

1. 使用確認您已成功新增主目錄共用 vserver cifs share show 命令。

範例

下列命令會建立名為的主目錄共用 `%w`。。 `oplocks`、 `browsable`和 `changenotify` 除了設定之外、還會設定共用內容 `homedirectory` 共用屬性。

此範例不會顯示SVM上所有共用的輸出。輸出被截短。

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory

vs1::> vserver cifs share show -vserver vs1
Vserver    Share    Path          Properties     Comment  ACL
---------- -------- ------------ -------------- -------- -----------
vs1        %w       %w           oplocks        -        Everyone / Full
Control
                                 browsable
                                 changenotify
                                 homedirectory
```

相關資訊

- 新增主目錄搜尋路徑
- 在伺服器上使用自動節點引用的要求和指南
- 管理使用者主目錄的可訪問性

了解主目錄共享的唯一 **ONTAP SMB** 使用者名稱要求

使用建立主目錄共用時、請務必指定唯一的使用者名稱 `%w` （ Windows 使用者名稱）或 `%u` （ UNIX 使用者名稱）可動態產生共用的變數。共用名稱會對應至您的使用者名稱。

靜態共用區名稱和使用者名稱相同時、可能會發生兩個問題：

- 當使用者使用列出叢集上的共用時 `net view` 命令會顯示兩個具有相同使用者名稱的共用。
- 當使用者連線至該共用名稱時、該使用者一律會連線至靜態共用區、而且無法以相同名稱存取主目錄共用區。

例如、有一個名稱為「管理員」的共用區、您有一個「管理員」Windows使用者名稱。如果您建立主目錄共用並連線至該共用區、就會連線至「管理員」靜態共用區、而非「管理員」主目錄共用區。

您可以依照下列任一步驟、以重複的共用名稱來解決此問題：

- 重新命名靜態共用、使其不再與使用者的主目錄共用發生衝突。
- 為使用者提供新的使用者名稱、使其不再與靜態共用名稱衝突。
- 建立 CIFS 主目錄共用時、請使用靜態名稱、例如「 'home' 」、而非使用 `%w` 避免與共用名稱衝突的參數。

主目錄共用名稱必須包含 %w 或 %u 動態變數。您應該瞭ONTAP 解現有靜態主目錄共用名稱在升級至更新需求的版本的版本時、會發生什麼變化。

如果您的主目錄組態包含靜態共用名稱、而且您升級到ONTAP 了某個版本、靜態主目錄共用名稱將不會變更、而且仍然有效。但是、您無法建立任何不包含的新主目錄共用 %w 或 %u 變動。

使用者的主目錄共用名稱必須包含其中一個變數、才能確保主目錄組態中的每個共用名稱都是唯一的。如果需要、您可以將靜態主目錄共用名稱變更為包含其中一種的名稱 %w 或 %u 變動。

新增 **ONTAP SMB** 主目錄搜尋路徑

如果您想要使用ONTAP 支援功能的SMB主目錄、您必須至少新增一個主目錄搜尋路徑。

關於這項工作

您可以使用新增主目錄搜尋路徑 vserver cifs home-directory search-path add 命令。

。 vserver cifs home-directory search-path add 命令會檢查中指定的路徑 -path 命令執行期間的選項。如果指定的路徑不存在、命令會產生訊息、提示您是否要繼續。您可以自行選擇 y 或 n。如果您選擇 y 若要繼續、 ONTAP 會建立搜尋路徑。不過、您必須先建立目錄結構、才能在主目錄組態中使用搜尋路徑。如果您選擇不繼續、則命令會失敗；不會建立搜尋路徑。接著您可以建立路徑目錄結構、然後重新執行 vserver cifs home-directory search-path add 命令。

步驟

1. 新增主目錄搜尋路徑： vserver cifs home-directory search-path add -vserver vserver -path path
2. 請確認您已使用成功新增搜尋路徑 vserver cifs home-directory search-path show 命令。

範例

下列範例新增路徑 /home1 移至 SVM VS1 上的主目錄組態。

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

vs1::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

下列範例會嘗試新增路徑 /home2 移至 SVM VS1 上的主目錄組態。路徑不存在。您可以選擇不繼續。

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home2
Warning: The specified path "/home2" does not exist in the namespace
         belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

相關資訊

新增主目錄共享

使用 %w 和 %d 變數建立 ONTAP SMB 主目錄配置

您可以使用建立主目錄組態 `%w` 和 `%d` 變數。然後使用者可以使用動態建立的共用區連線到他們的主共用區。

步驟

1. 建立 qtree 以包含使用者的主目錄： `volume qtree create -vserver vserver_name -qtree -path qtree_path`
2. 驗證 qtree 是否使用正確的安全樣式： `volume qtree show`
3. 如果 qtree 未使用所需的安全樣式、請使用變更安全樣式 `volume qtree security` 命令。
4. 新增主目錄共用： `vserver cifs share create -vserver vserver -share-name %w -path %d/%w -share-properties homedirectory\[,...\]`

   `-vserver vserver` 指定要新增搜尋路徑的 CIFS 儲存虛擬機器（ SVM ）。

   `-share-name %w` 指定主目錄共用名稱。當每位使用者連線至其主目錄時、系統會動態建立共用名稱。ONTAP共用名稱的格式為_windows_user_name_。

   `-path %d/%w` 指定主目錄的相對路徑。當每個使用者連線至其主目錄時、會動態建立相對路徑、其格式為_domain/windows_user_name_。

   `-share-properties homedirectory[,…]+` 指定該共用的共用內容。您必須指定 `homedirectory` 價值。您可以使用以逗號分隔的清單來指定其他共用屬性。

5. 使用確認共用具有所需的組態 `vserver cifs share show` 命令。
6. 新增主目錄搜尋路徑： `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver` *`vserver-name`* 指定要在其中新增搜尋路徑的啟用 CIFS 的 SVM 。

   `-path` *`path`* 指定搜尋路徑的絕對目錄路徑。

7. 請確認您已使用成功新增搜尋路徑 `vserver cifs home-directory search-path show` 命令。
8. 對於擁有主目錄的使用者、請在qtree或指定包含主目錄的磁碟區中建立對應的目錄。

   例如、如果您使用的路徑建立 qtree `/vol/vol1/users` 而您要建立目錄的使用者名稱是 mydomain\user1 、您可以建立具有下列路徑的目錄： `/vol/vol1/users/mydomain/user1`。

如果您在上建立一個名為「 'home1' 」的 Volume `/home1`，您可以使用以下路徑建立目錄：`/home1/mydomain/user1`。

9. 確認使用者可以透過對應磁碟機或使用UNC路徑連線、成功連線至主共用區。

   例如、如果使用者 mydomain\user1 想要連線到步驟 8 中建立的 SVM VS1 目錄、則 user1 會使用 UNC 路徑連線 `\\vs1\user1`。

範例

下列範例中的命令會以下列設定建立主目錄組態：

- 共享區名稱為%W.
- 相對主目錄路徑為%d/%w
- 用於包含主目錄的搜尋路徑、 `/home1`，是設定為 NTFS 安全性樣式的磁碟區。
- 組態是在SVM VS1上建立。

當使用者從Windows主機存取其主目錄時、您可以使用此類型的主目錄組態。當使用者從Windows和UNIX主機存取其主目錄時、您也可以使用此類組態、而檔案系統管理員則使用Windows型使用者和群組來控制對檔案系統的存取。

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %w

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %d/%w
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

相關資訊

- 使用%u變數設定主目錄
- 了解其他主目錄配置
- 顯示有關使用者主目錄路徑的信息

使用 %u 變數設定 ONTAP SMB 主目錄

您可以建立主目錄組態、在其中使用指定共用名稱 `%w` 變數、但您使用 `%u` 可指定主目錄共用的相對路徑的變數。然後使用者可以使用使用Windows使用者名稱所建立的動態共用來連線到他們的主共用區、而不需要知道主目錄的實際名稱或路徑。

步驟

1. 建立 qtree 以包含使用者的主目錄： `volume qtree create -vserver vserver_name -qtree`

`-path qtree_path`

2. 驗證 qtree 是否使用正確的安全樣式： `volume qtree show`
3. 如果 qtree 未使用所需的安全樣式、請使用變更安全樣式 `volume qtree security` 命令。
4. 新增主目錄共用： `vserver cifs share create -vserver vserver -share-name %w -path %u -share-properties homedirectory ,...]`

   `-vserver vserver` 指定要新增搜尋路徑的 CIFS 儲存虛擬機器（ SVM ）。

   `-share-name %w` 指定主目錄共用名稱。當每個使用者連線至其主目錄時、就會動態建立共用名稱、格式為_windows_user_name_。

   您也可以使用 `%u` 的變數 `-share-name` 選項。這會建立使用對應UNIX使用者名稱的相對共用路徑。

   `-path %u` 指定主目錄的相對路徑。當每個使用者連線至其主目錄時、會動態建立相對路徑、其格式為_Mapped_UNIX/user_name_。

   此選項的值也可以包含靜態元素。例如、 `eng/%u`。

   `-share-properties homedirectory\[,...\]` 指定該共用的共用內容。您必須指定 `homedirectory` 價值。您可以使用以逗號分隔的清單來指定其他共用屬性。

5. 使用確認共用具有所需的組態 `vserver cifs share show` 命令。
6. 新增主目錄搜尋路徑： `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver vserver` 指定要在其中新增搜尋路徑的啟用 CIFS 的 SVM 。

   `-path path` 指定搜尋路徑的絕對目錄路徑。

7. 請確認您已使用成功新增搜尋路徑 `vserver cifs home-directory search-path show` 命令。
8. 如果 UNIX 使用者不存在、請使用建立 UNIX 使用者 `vserver services unix-user create` 命令。

   對應Windows使用者名稱的UNIX使用者名稱必須存在、才能對應使用者。

9. 使用下列命令建立 Windows 使用者與 UNIX 使用者的名稱對應： `vserver name-mapping create -vserver vserver_name -direction win-unix -priority integer -pattern windows_user_name -replacement unix_user_name`

   如果已存在將Windows使用者對應至UNIX使用者的名稱對應、則不必執行對應步驟。

   Windows使用者名稱會對應至對應的UNIX使用者名稱。當Windows使用者連線至其主目錄共用時、他們會連線至動態建立的主目錄、其中共用名稱對應於Windows使用者名稱、但不知道該目錄名稱對應於UNIX使用者名稱。

10. 對於擁有主目錄的使用者、請在qtree或指定包含主目錄的磁碟區中建立對應的目錄。

例如、如果您使用的路徑建立 qtree `/vol/vol1/users` 而您要建立其目錄的使用者對應 UNIX 使用者名稱是「 unixuser1 」、則您可以建立具有下列路徑的目錄： `/vol/vol1/users/unixuser1`。

如果您在上建立一個名為「 'home1' 」的 Volume `/home1`，您可以使用以下路徑建立目錄：`/home1/unixuser1`。

11. 確認使用者可以透過對應磁碟機或使用UNC路徑連線、成功連線至主共用區。

例如、如果使用者 mydomain\user1 對應至 UNIX 使用者 unixuser1 、並想要連線至步驟 10 中建立的 SVM VS1 目錄、則 user1 會使用 UNC 路徑進行連線 `\\vs1\user1`。

範例

下列範例中的命令會以下列設定建立主目錄組態：

- 共享區名稱為%W.
- 相對主目錄路徑為%u
- 用於包含主目錄的搜尋路徑、 `/home1`，是設定為 UNIX 安全樣式的 Volume 。
- 組態是在SVM VS1上建立。

當使用者從Windows主機或Windows和UNIX主機存取其主目錄時、您可以使用此類型的主目錄組態、而檔案系統管理員則使用UNIX使用者和群組來控制檔案系統的存取。

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %u

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %u
              Share Properties: oplocks
                                browsable
                                changenotify
                                homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show -vserver vs1
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1

cluster::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1

cluster::> vserver name-mapping show -pattern user1
Vserver        Direction Position
-------------- --------- --------
vs1            win-unix  5        Pattern: user1
                                Replacement: unixuser1
```

相關資訊

- 使用 %w 和 %d 變數建立主目錄配置
- 了解其他主目錄配置
- 顯示有關使用者主目錄路徑的信息

了解其他 **ONTAP SMB** 主目錄配置

您可以使用建立其他主目錄組態 %w、 %d`和 `%u 變數、可讓您自訂主目錄組態以滿足您的需求。

您可以使用共用名稱和搜尋路徑中的變數和靜態字串組合、來建立許多主目錄組態。下表提供一些範例、說明如何建立不同的主目錄組態：

建立時間的路徑 /vol1/user 包含主目錄 ...	共用命令...
建立共用路徑 \\vs1\~win_username 將使用者導向 /vol1/user/win_username	`vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory`
建立共用路徑 \\vs1\win_username 將使用者導向 /vol1/user/domain/win_username	`vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory`
建立共用路徑 \\vs1\win_username 將使用者導向 /vol1/user/unix_username	`vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory`
建立共用路徑 \\vs1\unix_username 將使用者導向 /vol1/user/unix_username	`vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory`

用於管理 **SMB** 搜尋路徑的 **ONTAP** 命令

針對ONTAP SMB主目錄組態、有特定的支援功能可用來管理搜尋路徑。例如、您可以使用命令來新增、移除及顯示搜尋路徑的相關資訊。還有一個命令可用來變更搜尋路徑順序。

如果您想要...	使用此命令...
新增搜尋路徑	`vserver cifs home-directory search-path add`
顯示搜尋路徑	`vserver cifs home-directory search-path show`
變更搜尋路徑順序	`vserver cifs home-directory search-path reorder`

如果您想要...	使用此命令...
移除搜尋路徑	`vserver cifs home-directory search-path remove`

如"指令參考資料ONTAP"需詳細 `vserver cifs home-directory search-path`資訊，請參閱。

顯示有關 ONTAP SMB 使用者主目錄路徑的信息

您可以在儲存虛擬機器（SVM）上顯示SMB使用者的主目錄路徑、如果您已設定多個CIFS主目錄路徑、而且想要查看哪個路徑包含使用者的主目錄、就可以使用該路徑。

步驟

1. 使用顯示主目錄路徑 `vserver cifs home-directory show-user` 命令。

```
vserver cifs home-directory show-user -vserver vs1 -username user1
```

```
Vserver      User                 Home Dir Path
-----------  -------------------  ----------------------
vs1          user1                /home/user1
```

相關資訊

管理使用者主目錄的可訪問性

管理 ONTAP SMB 使用者主目錄的可存取性

根據預設、使用者的主目錄只能由該使用者存取。如果共用區的動態名稱前面有一個波狀符號（｛cilde｝）、您可以啟用或停用Windows系統管理員或任何其他使用者對使用者主目錄的存取（公共存取）。

開始之前

儲存虛擬機器（SVM）上的主目錄共用必須以動態共用名稱進行設定、並在名稱前面加上一個波狀符號（｛波狀符號｝）。下列案例說明共用命名需求：

主目錄共用名稱	連線至共用區的命令範例
{tilde} %d {tilde} %w	`net use * \\IPaddress\~domain~user/u:credentials`
{tilde} %w	`net use * \\IPaddress\~user/u:credentials`
{tilde} abc {tilde} %w	`net use * \\IPaddress\abc~user/u:credentials`

步驟

1. 執行適當的行動：

如果您要啟用或停用存取使用者主目錄的權限、以便...	輸入下列項目...
Windows系統管理員	`vserver cifs home-directory modify -vserver vserver_name -is-home-dirs -access-for-admin-enabled {true|false}` 預設值為 `true`。
任何使用者（公共存取）	a. 將權限等級設為進階：`set -privilege advanced` b. 啟用或停用存取：`vserver cifs home-directory modify -vserver vserver_name -is-home-dirs -access-for-public-enabled {true`

下列範例可讓使用者的主目錄公開存取：

```
set -privilege advanced
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public
-enabled true
set -privilege admin
```

相關資訊

顯示有關使用者主目錄路徑的信息

設定SMB用戶端存取UNIX符號連結

了解如何提供 **ONTAP SMB** 用戶端對 **UNIX** 符號連結的訪問

符號連結是在UNIX環境中建立的檔案、其中包含對其他檔案或目錄的參照。如果用戶端存取符號連結、用戶端會重新導向至符號連結所指的目標檔案或目錄。支援相對和絕對符號連結、包括連結（與本機檔案系統外部目標的絕對連結）ONTAP 。

支援SMB用戶端追蹤SVM上設定的UNIX符號連結。ONTAP此功能為選用功能、您可以使用在每個共享區的基礎上進行設定 `-symlink-properties` 的選項 `vserver cifs share create` 命令、並提供下列其中一項設定：

- 已啟用讀寫存取權
- 啟用唯讀存取
- 隱藏SMB用戶端的符號連結來停用
- 停用時無法存取SMB用戶端的符號連結

如果您在共用區上啟用符號連結、則相對符號連結無需進一步設定即可運作。

如果您在共用區上啟用符號連結、絕對符號連結將無法立即運作。您必須先在符號連結的UNIX路徑與目的地SMB路徑之間建立對應。建立絕對符號連結對應時、您可以指定它是本機連結或_widelink_；widelinks可以是其他儲存裝置上檔案系統的連結、也可以是連結、連結到同ONTAP 一個支援相同效能的系統上、分別裝載於不

同SVM中的檔案系統。建立wideink時、必須包含用戶端要追蹤的資訊、也就是建立重新分析點、讓用戶端探索目錄交會點。如果您在本機共用區以外建立檔案或目錄的絕對符號連結、但將「局部」設為「本機」、ONTAP則不允許存取目標。

> 如果用戶端嘗試刪除本機符號連結（絕對或相對）、則只會刪除符號連結、而不會刪除目標檔案或目錄。但是、如果用戶端嘗試刪除widelink、可能會刪除實際的目標檔案或是welink參照的目錄。由於用戶端可以明確開啟SVM外部的目標檔案或目錄、並將其刪除、所以無法控制此功能。ONTAP

- 重新分析點與**ONTAP** 不支援檔案系統服務

  _重新 分析點_是NTFS檔案系統物件、可選擇性地與檔案一起儲存在磁碟區上。重新分析點可讓SMB用戶端在使用NTFS樣式磁碟區時、接收增強或延伸的檔案系統服務。重新分析點由標準標記組成、可識別重新分析點的類型、以及SMB用戶端可擷取的重新分析點內容、以供用戶端進一步處理。在可用於延伸檔案系統功能的物件類型中、ONTAP 使用重新分析點標籤來實作NTFS符號連結和目錄交會點的支援。無法瞭解重新分析點內容的SMB用戶端只要忽略它、而不提供重新分析點可能啟用的延伸檔案系統服務。

- 目錄交會點與**ONTAP** 符號連結的支援

  目錄交會點是檔案系統目錄結構中的位置、可用來參照儲存檔案的替代位置、無論是在不同路徑（符號連結）或是個別儲存設備（widelinks）上。支援SMB的伺服器將目錄交會點以重新分析點的形式提供給Windows用戶端、讓有能力的用戶端在經過目錄交會點時、能夠從無法修復的點內容。ONTAP ONTAP因此、他們可以瀏覽並連線到不同的路徑或儲存裝置、就像它們是同一個檔案系統的一部分。

- *使用重新分析點選項*來啟用wideink支援

  此 `-is-use-junctions-as-reparse-points-enabled`選項在 ONTAP 9 中預設為啟用。由於並非所有 SMB 用戶端都支援 Widelink，因此啟用該資訊的選項可根據每個協定版本進行設定。這允許管理員同時適應受支援和不受支援的 SMB 用戶端。您必須啟用該選項 `-widelink-as-reparse-point-versions`對於使用寬連結存取共享的每個用戶端協定；預設值為 SMB1。

相關資訊

- "Windows 備份應用程式和 Unix 風格的符號連結"
- "Microsoft文件：重新分析點"

為 **ONTAP SMB** 存取配置 **UNIX** 符號連結時的限制

在設定UNIX符號連結進行SMB存取時、您必須注意特定限制。

限制	說明
45	使用CIFS伺服器名稱的FQDN時、可以指定的CIFS伺服器名稱長度上限。 您也可以將CIFS伺服器名稱指定為僅限15個字元的NetBios名稱。
80	共用名稱的最大長度。

限制	說明
256	在建立符號連結或修改現有符號連結的 UNIX 路徑時、您可以指定的 UNIX 路徑長度上限。 UNIX 路徑必須以「」開頭/`" (slash) and end with a “/” 。開頭和結尾的斜槓都會算作256個字元限制的一部分。
256	當您建立符號連結或修改現有符號連結的 CIFS 路徑時、可以指定的 CIFS 路徑長度上限。 CIFS 路徑必須以「」開頭/`" (slash) and end with a “/” 。開頭和結尾的斜槓都會算作256個字元限制的一部分。

相關資訊

為共享建立符號連結映射

控制 **ONTAP SMB** 伺服器上的自動 **DFS** 廣告

CIFS伺服器選項可控制連線至共用時、如何向SMB用戶端通告DFS功能。由於當用戶端透過SMB存取符號連結時、使用的是DFS轉介、因此您應該瞭解停用或啟用此選項時會有什麼影響。ONTAP

CIFS伺服器選項可決定CIFS伺服器是否自動向SMB用戶端通告其具備的DFS功能。根據預設、此選項會啟用、而且CIFS伺服器一律會向SMB用戶端通告它具有DFS-功能（即使連線至停用符號連結存取權的共用區）。如果您想要CIFS伺服器只在連接到已啟用符號連結存取權限的共用時、才向用戶端通告它具有DFS-功能、您可以停用此選項。

您應該注意停用此選項時會發生什麼情況：

- 符號連結的共用組態不變。
- 如果共用參數設定為允許符號連結存取（讀寫存取或唯讀存取）、則CIFS伺服器會將DFS功能通告給連線至該共用的用戶端。

  用戶端連線和符號連結存取不中斷地繼續進行。

- 如果共用參數設定為不允許符號連結存取（停用存取或如果共用參數值為null）、則CIFS伺服器不會向連線至該共用的用戶端通告DFS功能。

  由於用戶端已快取CIFS伺服器可支援的資訊、而且不再廣告、因此在停用CIFS伺服器選項之後、連線至停用符號連結存取的共用區的用戶端、可能無法存取這些共用區。停用此選項之後、您可能需要重新開機連線至這些共用的用戶端、以便清除快取的資訊。

這些變更不適用於SMB 1.0連線。

在 **ONTAP SMB** 共用上設定 **UNIX** 符號連結支持

您可以在建立SMB共用時或隨時修改現有SMB共用時、指定符號連結共用屬性設定、以設定SMB共用上的UNIX符號連結支援。UNIX符號連結支援預設為啟用。您也可以停用共用區上的UNIX符號連結支援。

關於這項工作

設定SMB共用的UNIX符號連結支援時、您可以選擇下列其中一項設定：

設定	說明
`enable` （已過時 * ）	指定啟用符號連結以進行讀寫存取。
`read_only` （已過時 * ）	指定啟用symlink進行唯讀存取。此設定不適用於無線連結。Wielink存取永遠是讀寫的。
`hide` （已過時 * ）	指定SMB用戶端無法看到symlink。
`no-strict-security`	指定用戶端在共用邊界之外追蹤symlink。
`symlinks`	指定在本機啟用symlink以進行讀寫存取。即使使用 CIFS 選項、也不會產生 DFS 通告 `is-advertise-dfs-enabled` 設為 `true`。這是預設設定。
`symlinks-and-widelinks`	指定本機symlink和widelinks以進行讀寫存取。即使使用 CIFS 選項、也會同時為本機 symlink 和 wedelinks 產生 DFS 通告 `is-advertise-dfs-enabled` 設為 `false`。
`disable`	指定停用symlink和widelinks。即使使用 CIFS 選項、也不會產生 DFS 通告 `is-advertise-dfs-enabled` 設為 `true`。
"" （ null 、未設定）	停用共用區上的符號連結。
- （未設定）	停用共用區上的符號連結。

*啟用_、隱藏_和唯讀_參數已過時、未來發行ONTAP 版的更新版可能會移除。

步驟

1. 設定或停用符號連結支援：

如果是...	輸入...
新的SMB共用區	`+vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink -properties {enable
hide	read-only
""	-
symlinks	symlinks-and-widelinks

如果是...	輸入...
disable},...]+`	現有的SMB共用區
`+vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable	hide
read-only	""
-	symlinks
symlinks-and-widelinks	disable},...]+`

2. 確認 SMB 共用組態正確無誤： `vserver cifs share show -vserver vserver_name -share -name share_name -instance`

範例

下列命令會建立名為「 data1 」的 SMB 共用、並將 UNIX 符號連結組態設定為 `enable` ：

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                Share Properties: oplocks
                                  browsable
                                  changenotify
              Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                   Share Comment: -
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

相關資訊

為共享建立符號連結映射

為 ONTAP SMB 共用建立符號連結映射

您可以建立SMB共用的UNIX符號連結對應。您可以建立相對符號連結、以參照檔案或資料夾與其父資料夾的相對位置、也可以建立絕對符號連結、以使用絕對路徑來參照檔案或資料夾。

關於這項工作

如果您使用SMB 2.x、就無法從Mac OS X用戶端存取Widgelinks當使用者嘗試從Mac OS X用戶端使用wideinks連線至共用時、嘗試會失敗。不過、如果您使用SMB 1、則可以將wideinks與Mac OS X用戶端搭配使用。

步驟

1. 若要建立 SMB 共用的符號連結對應： `vserver cifs symlink create -vserver virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-directory {true|false}]`

   `-vserver virtual_server_name` 指定儲存虛擬機器（ SVM ）名稱。

   `-unix-path path` 指定 UNIX 路徑。UNIX 路徑必須以斜線開頭 (/）、且必須以斜線結尾 (/）。

   `-share-name share_name` 指定要對應的 SMB 共用名稱。

   `-cifs-path path` 指定 CIFS 路徑。CIFS 路徑必須以斜線開頭 (/）、且必須以斜線結尾 (/）。

   `-cifs-server server_name` 指定 CIFS 伺服器名稱。CIFS伺服器名稱可以指定為DNS名稱（例如mynetwork.cifs.server.com）、IP位址或NetBios名稱。您可以使用來判斷 NetBIOS 名稱 `vserver cifs show` 命令。如果未指定此選用參數、預設值為本機CIFS伺服器的NetBios名稱。

   `-locality local|free|widelink}` 指定要建立本機連結、免費連結或寬符號連結。本機符號連結會對應至本機SMB共用區。免費的符號連結可以對應到本機SMB伺服器上的任何位置。廣泛的符號連結會對應到網路上的任何SMB共用區。如果您未指定此選用參數、則預設值為 `local`。

   `-home-directory true false}` 指定目標共用是否為主目錄。即使此參數為選用參數、您仍必須將此參數設為 `true` 當目標共用設定為主目錄時。預設值為 `false`。

範例

下列命令會在名為VS1的SVM上建立符號連結對應。它有 UNIX 路徑 `/src/`、 SMB 共享名稱「 'SOURCE' 」、 CIFS 路徑 `/mycompany/source/`和 CIFS 伺服器 IP 位址 123.123.123.123 、這是一種有線連結。

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

相關資訊

在共享上配置 UNIX 符號連結支持

用於管理 **SMB** 符號連結映射的 **ONTAP** 命令

有特定ONTAP 的功能可用來管理符號連結對應。

如果您想要...	使用此命令...
建立符號連結對應	`vserver cifs symlink create`
顯示符號連結對應的相關資訊	`vserver cifs symlink show`
修改符號連結對應	`vserver cifs symlink modify`
刪除符號連結對應	`vserver cifs symlink delete`

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

ONTAP SMB 伺服器上的 **Windows** 備份應用程式和 **Unix** 樣式符號鏈接

當在 Windows 上執行的備份應用程式遇到 Unix 樣式的符號連結（ symlink ）時、會追蹤連結並備份資料。從 ONTAP 9.15.1 開始、您可以選擇備份 symlinks 而非資料。ONTAP FlexGroup Volume 和 FlexVols 完全支援此功能。

總覽

在您變更 ONTAP 在 Windows 備份作業期間處理符號連結的方式之前、您應該先熟悉這些優點、主要概念和組態選項。

效益

當此功能停用或無法使用時、系統會周遊每個 symlink 、並備份其連結的資料。因此、有時可能會備份不必要的資料、在某些情況下、應用程式可能會在迴圈中結束。備份 symlinks 可避免這些問題。由於 symlink 檔案與大多數情況下的資料相比非常小、因此備份所需的時間較短。由於 IO 作業減少、叢集的整體效能也可以改善。

Windows 伺服器環境

此功能支援在 Windows 上執行的備份應用程式。使用前、您應該先瞭解環境的相關技術層面。

延伸屬性

Windows 支援延伸屬性（ EA ）、這些屬性共同構成與檔案相關的額外中繼資料（選擇性）。這些屬性由多種應用程式使用、例如 Windows Subsystem for Linux 、如所述 "WSL 的檔案權限"。從 ONTAP 讀取資料時、應用程式可以要求每個檔案的延伸屬性。

啟用此功能時、會在延伸屬性中傳回符號連結。因此、備份應用程式必須提供用於儲存中繼資料的標準 EA 支援。部分 Windows 公用程式支援並保留延伸屬性。不過、如果備份軟體不支援備份及還原延伸屬性、則不會保留與每個檔案相關的中繼資料、也無法正確處理符號連結。

Windows 組態

在 Microsoft Windows 伺服器上執行的備份應用程式可獲得特殊權限、讓它們略過一般檔案安全性。這通常是透過將應用程式新增至 Backup Operators 群組來完成。應用程式接著可視需要備份及還原檔案、並執行其他相關

的系統作業。備份應用程式使用的 SMB 傳輸協定有細微的變更、 ONTAP 可以在讀取和寫入資料時偵測到這些變更。

需求

symlink 備份功能有多項需求、包括：

- 您的叢集正在執行 ONTAP 9.15.1 或更新版本。
- 已獲授特殊備份權限的 Windows 備份應用程式。
- 備份應用程式也必須支援延伸屬性、並在備份作業期間要求這些屬性。
- ONTAP symlink 備份功能已針對適用的資料 SVM 啟用。

組態選項

除了 ONTAP CLI 之外、您也可以使用 REST API 來管理此功能。如需詳細資訊、請參閱 "ONTAP REST API 與自動化的新功能" 。決定 ONTAP 處理 Unix 型符號連結的方式的組態、必須針對每個 SVM 分別執行。

啟用 **ONTAP** 中的 **symlink** 備份功能

已使用 ONTAP 9.15.1 將組態選項導入現有的 CLI 命令。您可以使用此選項來啟用或停用 Unix 樣式的 symlink 處理。

開始之前

查看基本 [需求]。此外：

- 能夠將 CLI 權限提升至進階層級。
- 判斷您要修改的資料 SVM 。SVM `vs1` 用於範例命令。

步驟

1. 設定進階權限等級。

```
set privilege advanced
```

2. 啟用 symlink 檔案備份。

```
vserver cifs options modify -vserver vs1 -is-backup-symlink-enabled true
```

使用**BranchCache**快取分公司的**SMB**共用內容

了解如何使用 **BranchCache** 在分公司快取 **ONTAP SMB** 共享內容

Microsoft開發了BranchCache、以便在要求用戶端的本機電腦上快取內容。實施BranchCache可降低廣域網路（WAN）的使用率、並在分公司使用者使用SMB存取儲存在儲存虛擬機器（SVM）上的內容時、提供更佳的存取回應時間。ONTAP

如果您設定了BranchCache、Windows BranchCache用戶端會先從SVM擷取內容、然後快取分公司電腦上的內容。如果分公司中另一個啟用了BranchCache的用戶端要求相同的內容、SVM會先驗證並授權要求的使用者。然後SVM會判斷快取內容是否仍為最新狀態、如果是、則會傳送有關快取內容的用戶端中繼資料。然後用戶端會使用中繼資料、直接從本機快取擷取內容。

相關資訊

了解如何使用離線檔案來快取檔案以供離線使用

要求與準則

了解 **ONTAP SMB BranchCache** 版本支持

您應該知道ONTAP 哪些版本的BranchCache支援哪些版本。

支援BranchCache 1和增強的BranchCache 2：ONTAP

- 在SMB伺服器上為儲存虛擬機器（SVM）設定BranchCache時、您可以啟用BranchCache 1、BranchCache 2或所有版本。

  根據預設、所有版本都會啟用。

- 如果只啟用了BranchCache 2、遠端辦公室Windows用戶端機器必須支援BranchCache 2。

  只有SMB 3.0或更新版本的用戶端支援BranchCache 2。

如需更多關於BranchCache版本的資訊，請參閱Microsoft TechNet程式庫。

相關資訊

"Microsoft TechNet程式庫：technet.microsoft.com/en-us/library/"

了解 **ONTAP SMB** 網路協定支援要求

您必須瞭解實作ONTAP 《Sing Sof BranchCache》（英文）的網路傳輸協定需求。

您可以ONTAP 使用SMB 2.1或更新版本、在使用SMB 2.1或更新版本的IPv4和IPv6網路上實作「S21：快取」功能。

參與BranchCache實作的所有CIFS伺服器和分公司機器、都必須啟用SMB 2.1或更新的傳輸協定。SMB 2.1具有允許用戶端參與BranchCache環境的傳輸協定延伸功能。這是支援BranchCache的最低SMB傳輸協定版本。SMB 2.1支援版本BranchCache第1版。

如果您要使用BranchCache第2版、SMB 3.0是支援的最低版本。參與BranchCache 2實作的所有CIFS伺服器和分公司機器、都必須啟用SMB 3.0或更新版本。

如果您的遠端辦公室中有部分用戶端僅支援SMB 2.1、而部分用戶端支援SMB 3.0、您可以在CIFS伺服器上實作一項BranchCache組態、以同時在BranchCache 1和BranchCache 2上提供快取支援。

雖然Microsoft BranchCache功能同時支援使用HTTP / HTTPS和SMB傳輸協定做為檔案存取傳輸協定、ONTAP 但支援使用SMB。

了解 **ONTAP SMB** 和 **Windows** 主機版本需求

在設定BranchCache之前、Windows主機和分公司必須符合特定的版本需求。ONTAP

在設定BranchCache之前、您必須確保ONTAP 叢集和參與的分公司用戶端上的版本支援SMB 2.1或更新版本、並支援BranchCache功能。如果您設定「主控快取」模式、也必須確保您使用支援的主機作為快取伺服器。

下列ONTAP 版本的支援包含BranchCache 1和Windows主機：

- 內容伺服器：儲存虛擬機器（SVM）ONTAP 、含
- 快取伺服器：Windows Server 2008 R2或Windows Server 2012或更新版本
- 對等端點或用戶端：Windows 7 Enterprise、Windows 7 Ultimate、Windows 8、Windows Server 2008 R2或Windows Server 2012或更新版本

下列ONTAP 版本的支援及Windows主機均支援BranchCache 2：

- 內容伺服器：SVM with ONTAP SfSIf
- 快取伺服器：Windows Server 2012或更新版本
- 對等端點或用戶端：Windows 8或Windows Server 2012或更新版本

了解 **ONTAP SMB** 使 **BranchCache** 哈希無效的原因

規劃ONTAP 您的BranchCache組態時、瞭解為什麼不驗證雜湊會有幫助。它可協助您決定應該設定哪種操作模式、並協助您選擇要啟用的共用區。

必須管理BranchCache雜湊、才能確保雜湊有效。ONTAP如果雜湊無效、ONTAP 則在下次要求內容時、如果仍然啟用了BranchCache、則無法驗證雜湊並計算新雜湊。

由於下列原因、導致雜湊失效：ONTAP

- 伺服器金鑰已修改。

  如果伺服器金鑰已修改、ONTAP 則無法驗證雜湊存放區中的所有雜湊。

- 由於已達到BranchCache雜湊存放區的最大大小、因此會從快取中清除雜湊。

  這是可調整的參數、可加以修改以符合您的業務需求。

- 檔案會透過SMB或NFS存取進行修改。
- 已計算雜湊的檔案會使用還原 `snap restore` 命令。
- 包含已啟用 BranchCache 之 SMB 共用的磁碟區會使用還原 `snap restore` 命令。

了解如何選擇 **ONTAP SMB** 雜湊儲存位置

設定BranchCache時、您可以選擇要儲存雜湊的位置、以及雜湊存放區的大小。瞭解在選擇雜湊存放區位置和大小時的準則、有助於在啟用CIFS的SVM上規劃您的BranchCache組態。

- 您應該在允許更新atime的磁碟區上找到雜湊存放區。

  雜湊檔案的存取時間是用來將經常存取的檔案保留在雜湊存放區中。如果停用atime更新、建立時間就會用於此用途。最好使用atime來追蹤經常使用的檔案。

- 您無法將雜湊儲存在唯讀檔案系統上、例如SnapMirror目的地和SnapLock SnapMirror Volume。
- 如果達到雜湊存放區的最大大小、則會清除舊雜湊、以便留出新雜湊的空間。

  您可以增加雜湊存放區的最大大小、以減少從快取排清的雜湊量。

- 如果您儲存雜湊的磁碟區無法使用或已滿、或是叢集內通訊發生問題、導致無法擷取雜湊資訊、則無法使用BranchCache服務。

  磁碟區可能無法使用、因為它離線、或是儲存管理員為雜湊存放區指定新位置。

  這不會造成檔案存取問題。如果存取雜湊存放區受到阻礙、ONTAP 則將Microsoft定義的錯誤傳回給用戶端、這會導致用戶端使用一般SMB讀取要求來要求檔案。

相關資訊

- 在伺服器上設定 BranchCache
- 修改共享上的 BranchCache 配置

了解 **ONTAP SMB BranchCache** 建議

在您設定BranchCache之前、在決定要啟用什麼SMB共用區的時候、您應該謹記一些建議。

在決定要使用哪種操作模式、以及要啟用BranchCache的SMB共用區時、請謹記下列建議：

- 當要遠端快取的資料經常變更時、會降低BranchCache的優點。
- 對於包含檔案內容的共用區而言、具有很大的好處、這些檔案內容可由多個遠端辦公室用戶端重複使用、或是由單一遠端使用者重複存取的檔案內容。
- 請考慮為唯讀內容啟用快取，例如快照和 SnapMirror 目的地中的資料。

設定**BranchCache**

了解 **ONTAP SMB BranchCache** 配置

您可以在SMB伺服器上使用ONTAP flexf命令 來設定BranchCache。若要實作BranchCache、您也必須在要快取內容的分公司設定用戶端、以及選擇性地設定裝載的快取伺服器。

如果您將BranchCache設定為依共用區啟用快取、則必須在要提供BranchCache快取服務的SMB共用區上啟用BranchCache。

配置 **ONTAP SMB BranchCache** 的要求

在滿足某些先決條件之後、您可以設定BranchCache。

在為SVM設定CIFS伺服器上的BranchCache之前、必須符合下列需求：

- 叢集中的所有節點都必須安裝此程式。ONTAP
- CIFS 必須獲得授權、而且必須設定 SMB 伺服器。SMB 授權隨附於"ONTAP One"。如果您沒有 ONTAP One 且未安裝授權、請聯絡您的銷售代表。
- 必須設定IPv4或IPv6網路連線。
- 對於BranchCache 1、必須啟用SMB 2.1或更新版本。
- 對於BranchCache 2、必須啟用SMB 3.0、且遠端Windows用戶端必須支援BranchCache 2。

在 **ONTAP SMB** 伺服器上設定 **BranchCache**

您可以設定在每個共用區基礎上提供BranchCache服務。或者、您也可以設定在所有SMB共用區上自動啟用快取。

關於這項工作

您可以在SVM上設定BranchCache。

- 如果您想要針對CIFS伺服器上所有SMB共用區內的所有內容提供快取服務、可以建立All共享區的BranchCache組態。
- 如果您想要針對CIFS伺服器上所選SMB共用區內的內容提供快取服務、可以建立每個共用區的BranchCache組態。

在設定BranchCache時、您必須指定下列參數：

必要參數	說明
*SVM*名稱	以每個SVM為基礎來設定BranchCache。您必須指定要在哪些CIFS型SVM上設定BranchCache服務。
散列存放區路徑	BranchCache雜湊儲存在SVM磁碟區的一般檔案中。您必須指定ONTAP 要將雜湊資料儲存在其中的現有目錄路徑。您必須將BranchCache雜湊路徑設定為可讀寫。不允許使用唯讀路徑，例如快照目錄。您可以將雜湊資料儲存在包含其他資料的磁碟區中、也可以建立獨立的磁碟區來儲存雜湊資料。 如果SVM是SVM災難恢復來源、則雜湊路徑無法位於根磁碟區上。這是因為根磁碟區並未複寫到災難恢復目的地。 雜湊路徑可以包含空白和任何有效的檔案名稱字元。

您可以選擇性地指定下列參數：

選用參數	說明
支援的版本	支援BranchCache 1和2。ONTAP您可以啟用版本1、版本2或兩者。預設為啟用這兩個版本。

選用參數	說明
雜湊存放區的最大大小_	您可以指定雜湊資料存放區的大小。如果雜湊資料超過此值、ONTAP 則用更新的雜湊來刪除舊的雜湊。雜湊存放區的預設大小為1 GB。如果未以過度積極的方式捨棄雜湊、則會使BranchCache的效能更有效率。如果您判斷雜湊存放區已滿而經常捨棄雜湊、可以修改BranchCache組態來增加雜湊存放區大小。
伺服器金鑰	您可以指定一個伺服器機碼，讓BranchCache服務用來防止用戶端模擬BranchCache伺服器。如果未指定伺服器金鑰、則會在建立BranchCache組態時隨機產生一個金鑰。您可以將伺服器金鑰設定為特定值、以便在多個伺服器為相同檔案提供BranchCache資料時、用戶端可以使用相同伺服器金鑰來自任何伺服器的雜湊。如果伺服器金鑰包含任何空格、則必須以引號括住伺服器金鑰。
操作模式	預設是以每個共用為基礎來啟用BranchCache。 • 若要建立 BranchCache 組態，讓您以每個共用為基礎啟用 BranchCache ，您可以指定此選用參數，也可以指定 `per-share`。 • 若要在所有共用上自動啟用 BranchCache 、您必須將作業模式設定為 `all-shares`。

步驟

1. 視需要啟用SMB 2.1和3.0：
   a. 將權限層級設為進階： `set -privilege advanced`
   b. 檢查設定的 SVM SMB 設定、判斷是否已啟用所有必要的 SMB 版本： `vserver cifs options show -vserver vserver_name`
   c. 如有必要、請啟用 SMB 2.1 ： `vserver cifs options modify -vserver vserver_name -smb2-enabled true`

      命令可同時啟用SMB 2.0和SMB 2.1。

   d. 如有必要、請啟用 SMB 3.0 ： `vserver cifs options modify -vserver vserver_name -smb3-enabled true`
   e. 返回管理權限層級： `set -privilege admin`
2. 設定 BranchCache ： `vserver cifs branchcache create -vserver vserver_name -hash-store-path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all] [-server-key text] -operating-mode {per-share|all-shares}`

   指定的雜湊儲存路徑必須存在、而且必須位於SVM管理的磁碟區上。路徑也必須位於可讀寫磁碟區上。如果路徑為唯讀或不存在、則命令會失敗。

如果您想在其他SVM BranchCache組態中使用相同的伺服器機碼、請記錄您輸入的伺服器機碼值。當您顯示有關BranchCache組態的資訊時、不會顯示伺服器機碼。

3. 驗證 BranchCache 組態是否正確： `vserver cifs branchcache show -vserver vserver_name`

範例

下列命令可驗證是否同時啟用SMB 2.1和3.0、並設定BranchCache在SVM VS1的所有SMB共用區上自動啟用快取：

```
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 show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true


cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: all_shares
```

下列命令可驗證是否同時啟用SMB 2.1和3.0、設定在SVM VS1上啟用每個共用區的快取、並驗證BranchCache組態：

```
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 show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

相關資訊

- 了解 BranchCache 版本支持
- 了解如何在遠端辦公室配置 BranchCache
- 建立啟用BranchCache的SMB共用區
- 在現有共享上啟用 BranchCache
- 修改共享上的 BranchCache 配置
- 了解如何停用共用上的 BranchCache
- 刪除共享上的 BranchCache 配置

了解如何在 **ONTAP SMB** 中的遠端辦公室設定 **BranchCache**

在SMB伺服器上設定了BranchCache之後、您必須在用戶端電腦上安裝及設定BranchCache、並選擇性地在遠端辦公室的快取伺服器上進行設定。Microsoft提供在遠端辦公室設定BranchCache的說明。

Microsoft BranchCache網站上有設定分公司用戶端的指示、以及選用快取伺服器以使用BranchCache的指示。

"Microsoft BranchCache文件：新功能"

設定啟用了**BranchCache**的**SMB**共用區

了解如何設定啟用 **BranchCache** 的 **ONTAP SMB** 共享

在SMB伺服器和分公司設定了BranchCache之後、您可以在SMB共用區上啟用內含您要允許分公司用戶端快取內容的BranchCache。

您可以在SMB伺服器上的所有SMB共用區上啟用「BranchCache快取」、或是以每個共用區為基礎來啟用「BranchCache快取」。

- 如果您以每共用區為基礎來啟用BranchCache、您可以在建立共用區或修改現有共用區時啟用BranchCache。

  如果您啟用現有SMB共用區的快取、ONTAP 只要您在該共用區上啟用了「BranchCache」、就會立即開始運算雜湊、並將中繼資料傳送給要求內容的用戶端。

- 如果隨後在該共用區上啟用了BranchCache、則任何與共用區有SMB連線的用戶端都不會獲得BranchCache支援。

  此版本可在SMB工作階段設定時、針對共用區通告BranchCache支援。ONTAP啟用了BranchCache之後、已建立工作階段的用戶端必須中斷連線並重新連線、才能使用此共用區的快取內容。

> ⓘ 如果SMB共用區上的BranchCache後來停用、ONTAP 則停止傳送中繼資料給要求的用戶端。需要資料的用戶端會直接從內容伺服器（SMB伺服器）擷取資料。

建立啟用 **BranchCache** 的 **ONTAP SMB** 共享

您可以在建立共用時、透過設定在 SMB 共用上啟用 BranchCache `branchcache` 共用屬性。

關於這項工作

- 如果在SMB共用區上啟用了BranchCache、則共用區必須將離線檔案組態設定為手動快取。

  這是您建立共用時的預設設定。

- 您也可以在建立啟用了BranchCache的共用時指定其他選用的共用參數。
- 您可以設定 `branchcache` 即使在儲存虛擬機器（ SVM ）上未設定和啟用 BranchCache 、也會在共用上顯示內容。

  不過、如果您想要共用區提供快取內容、則必須在SVM上設定及啟用BranchCache。

- 因為使用時並未套用預設共用屬性至共用 `-share-properties` 參數、除了、您還必須指定要套用至共用的所有其他共用屬性 `branchcache` 使用以逗號分隔的清單來共用屬性。
- 如"指令參考資料ONTAP"需詳細 `vserver cifs share create`資訊，請參閱。

步驟

1. 建立啟用 BranchCache 的 SMB 共用區：

`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties branchcache[,…]`

2. 使用確認 SMB 共用上的 BranchCache 共用屬性已設定 `vserver cifs share show` 命令。

範例

下列命令會建立一個已啟用 BranchCache 的 SMB 共用，名稱為「 dATA 」，路徑為 `/data` 在 SVM VS1 上。根據預設，離線檔案設定為 `manual`：

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path
/data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
                      Vserver: vs1
                        Share: data
     CIFS Server NetBIOS Name: VS1
                         Path: /data
            Share Properties: branchcache
                              oplocks
                              browsable
                              changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: data
                Offline Files: manual
Vscan File-Operations Profile: standard
```

相關資訊

在單一共用上停用 BranchCache

在現有 **ONTAP SMB** 共用上啟用 **BranchCache**

您可以新增、在現有的 SMB 共用上啟用 BranchCache `branchcache` 將屬性共用至現有的共用屬性清單。

關於這項工作

- 如果在SMB共用區上啟用了BranchCache、則共用區必須將離線檔案組態設定為手動快取。

  如果現有共用的離線檔案設定未設定為手動快取、您必須修改共用區來設定。

- 您可以設定 `branchcache` 即使在儲存虛擬機器（ SVM ）上未設定和啟用 BranchCache 、也會在共用上顯示內容。

不過、如果您想要共用區提供快取內容、則必須在SVM上設定及啟用BranchCache。

- 當您新增時 `branchcache` 共用屬性、現有的共用設定和共用屬性都會保留。

  會將BranchCache共用屬性新增至現有的共用屬性清單。如"指令參考資料ONTAP"需詳細 `vserver cifs share properties add`資訊，請參閱。

步驟

1. 如有必要、請設定離線檔案共用設定以手動快取：
   a. 使用來判斷離線檔案共用設定 `vserver cifs share show` 命令。
   b. 如果未將離線檔案共用設定設為手動、請將其變更為所需的值： `vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual`
2. 在現有的 SMB 共用上啟用 BranchCache ： `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`
3. 確認已在 SMB 共用上設定 BranchCache 共用屬性： `vserver cifs share show -vserver vserver_name -share-name share_name`

範例

下列命令會在路徑為的現有 SMB 共用「 'data2 」上啟用 BranchCache `/data2` 在 SVM VS1 上：

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              showsnapshot
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties add  -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              showsnapshot
                              changenotify
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

相關資訊

- 新增或刪除現有共享的共享屬性
- 在單一共用上停用 BranchCache

管理及監控**BranchCache**組態

修改 **ONTAP SMB** 共用上的 **BranchCache** 配置

您可以修改SVM上的BranchCache服務組態、包括變更雜湊存放區目錄路徑、雜湊存放區最大目錄大小、作業模式、以及支援哪些版本的BranchCache。您也可以增加包含雜湊存放區的磁碟區大小。

步驟

1. 執行適當的行動：

如果您想要...	輸入下列項目...
修改雜湊存放區目錄大小	`vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB
MB	GB
TB	PB]}`
增加包含雜湊存放區的磁碟區大小	`volume size -vserver vserver_name -volume volume_name -new-size new_size[k
m	g
t]` 如果包含雜湊儲存區的磁碟區已滿、您可能可以增加磁碟區的大小。您可以將新的Volume大小指定為數字、然後再指定單位。 深入瞭解 "管理FlexVol 功能"	修改雜湊存放區目錄路徑
`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true	false}` 如果SVM是SVM災難恢復來源、則雜湊路徑無法位於根磁碟區上。這是因為根磁碟區並未複寫到災難恢復目的地。  BranchCache雜湊路徑可以包含空白和任何有效的檔案名稱字元。  如果您修改雜湊路徑、 `-flush-hashes` 是必要參數、可指定 ONTAP 是否要清除原始雜湊儲存位置的雜湊。您可以為設定下列值 `-flush-hashes` 參數：  如果您指定 **`true`**， **ONTAP** 會刪除原始位置的雜湊，並在啟用 **BranchCache** 的用戶端提出新要求時，在新位置建立新的雜湊。 如果您指定 `false`，則不會清除雜湊。 + 在這種情況下、您可以選擇稍後再重複使用現有的雜湊、方法是將雜湊存放區路徑變更回原始位置。

如果您想要...	輸入下列項目...
變更操作模式	`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share
all-shares	disable}` 修改操作模式時、請注意下列事項： 設定**SMB**工作階段時、會針對共用區通告**BranchCache**支援**ONTAP** 。 啟用了BranchCache之後、已建立工作階段的用戶端必須中斷連線並重新連線、才能使用此共用區的快取內容。
變更支援的BranchCache版本	`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable
v2-enable	enable-all}`

2. 使用驗證組態變更 `vserver cifs branchcache show` 命令。

顯示有關 **ONTAP SMB** 共享上的 **BranchCache** 配置的信息

您可以在儲存虛擬機器（SVM）上顯示有關BranchCache組態的資訊、這些資訊可在驗證組態或在修改組態之前判斷目前設定時使用。

步驟

1. 執行下列其中一項動作：

如果您要顯示...	輸入此命令...
關於所有SVM上的BranchCache組態的摘要資訊	`vserver cifs branchcache show`
有關特定SVM組態的詳細資訊	`vserver cifs branchcache show -vserver` *`vserver_name`*

範例

下列範例顯示SVM VS1上的BranchCache組態相關資訊：

```
cluster1::> vserver cifs branchcache show -vserver vs1

                                    Vserver: vs1
            Supported BranchCache Versions: enable_all
                       Path to Hash Store: /hash_data
            Maximum Size of the Hash Store: 20GB
  Encryption Key Used to Secure the Hashes: -
          CIFS BranchCache Operating Modes: per_share
```

變更 **ONTAP SMB BranchCache** 伺服器金鑰

您可以修改儲存虛擬機器（SVM）上的BranchCache組態、並指定不同的伺服器金鑰、藉此變更BranchCache伺服器金鑰。

關於這項工作

您可以將伺服器金鑰設定為特定值、以便在多個伺服器為相同檔案提供BranchCache資料時、用戶端可以使用相同伺服器金鑰來自任何伺服器的雜湊。

變更伺服器金鑰時、您也必須清除雜湊快取。在清除雜湊之後、ONTAP 當啟用了BranchCache的用戶端發出新要求時、會建立新的雜湊。

步驟

1. 使用下列命令變更伺服器金鑰： `vserver cifs branchcache modify -vserver vserver_name -server-key text -flush-hashes true`

   設定新的伺服器金鑰時、您也必須指定 `-flush-hashes` 並將值設為 `true`。

2. 使用驗證 BranchCache 組態是否正確 `vserver cifs branchcache show` 命令。

範例

下列範例設定新的伺服器金鑰、其中包含空格並清除SVM VS1上的雜湊快取：

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

相關資訊

在指定的 **ONTAP SMB** 路徑上預先計算 **BranchCache** 哈希

您可以將BranchCache服務設定為預先計算單一檔案、目錄或目錄結構中所有檔案的雜湊。如果您想要在關閉非尖峰時段內、針對啟用了BranchCache的共用區中的資料運算雜湊、這項功能就很有幫助。

關於這項工作

如果您想在顯示雜湊統計資料之前收集資料範例、則必須使用 `statistics start` 和選用 `statistics stop` 命令。

- 您必須指定要預先計算雜湊的儲存虛擬機器（SVM）和路徑。
- 您也必須指定是否要以循環方式計算雜湊。
- 如果您想要以遞迴方式計算雜湊、則BranchCache服務會在指定路徑下遍歷整個目錄樹狀結構、並針對每個符合條件的物件來計算雜湊。

  詳細了解 `statistics start`和 `statistics stop`在"指令參考資料ONTAP" 。

步驟

1. 視需要預先運算雜湊：

如果您想要預先計算雜湊...	輸入命令...
單一檔案或目錄	`vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false`
以循環方式處理目錄結構中的所有檔案	`vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true`

2. 使用驗證正在計算雜湊 `statistics` 命令：

   a. 顯示的統計資料 `hashd` 所需 SVM 執行個體上的物件： `statistics show -object hashd -instance vserver_name`

   b. 重複執行命令、確認所建立的雜湊數量增加。

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

範例

下列範例會在路徑上建立雜湊 `/data` 以及 SVM VS1 上所有包含的檔案和子目錄：

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       85
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       92
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -
```

相關資訊

- "效能監控設定"

從 ONTAP SMB SVM BranchCache 哈希存儲中刷新哈希

您可以清除儲存虛擬機器（SVM）上的BranchCache雜湊存放區中的所有快取雜湊。如果您已變更分公司的BranchCache組態、這項功能就很有用。例如、如果您最近將快取模式從分散式快取重新設定為託管式快取模式、就會想要清除雜湊存放區。

關於這項工作

在清除雜湊之後、ONTAP 當啟用了BranchCache的用戶端發出新要求時、會建立新的雜湊。

步驟

1. 清除 BranchCache 雜湊存放區的雜湊： `vserver cifs branchcache hash-flush -vserver` *`vserver_name`*

   ```
   vserver cifs branchcache hash-flush -vserver vs1
   ```

顯示 ONTAP SMB BranchCache 統計訊息

您可以顯示BranchCache統計資料、以識別快取效能的表現、判斷您的組態是否提供快取內容給用戶端、並判斷是否刪除雜湊檔案、以留出空間來儲存較新的雜湊資料。

關於這項工作

。 `hashd` 統計資料物件包含提供有關 BranchCache 雜湊統計資訊的計數器。。 `cifs` 統計資料物件包含提供與 BranchCache 相關活動之統計資訊的計數器。您可以在進階權限層級收集及顯示這些物件的相關資訊。

步驟

1. 將權限層級設為進階： `set -privilege advanced`

   ```
   cluster1::> set -privilege advanced

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

2. 使用顯示與 BranchCache 相關的計數器 `statistics catalog counter show` 命令。

   ```
   cluster1::*> statistics catalog counter show -object hashd

   Object: hashd
       Counter                     Description
       --------------------------
   ----------------------------------------------
       branchcache_hash_created    Number of times a request to generate
                                   BranchCache hash for a file succeeded.
       branchcache_hash_files_replaced
                                   Number of times a BranchCache hash file
   ```

```
was
                                deleted to make room for more recent
hash
                                data. This happens if the hash store
size is
                                exceeded.
    branchcache_hash_rejected   Number of times a request to generate
                                BranchCache hash data failed.
    branchcache_hash_store_bytes
                                Total number of bytes used to store hash
data.
    branchcache_hash_store_size Total space used to store BranchCache
hash
                                data for the Vserver.
    instance_name               Instance Name
    instance_uuid               Instance UUID
    node_name                   System node name
    node_uuid                   System node id
9 entries were displayed.

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
-------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    avg_junction_depth          Average number of junctions crossed by
SMB
                                and SMB2 path-based commands
    branchcache_hash_fetch_fail Total number of times a request to fetch
hash
                                data failed. These are failures when
                                attempting to read existing hash data.
It
                                does not include attempts to fetch hash
data
                                that has not yet been generated.
    branchcache_hash_fetch_ok   Total number of times a request to fetch
hash
```

```
                                    data succeeded.
    branchcache_hash_sent_bytes Total number of bytes sent to clients
                                    requesting hashes.
    branchcache_missing_hash_bytes
                                    Total number of bytes of data that had
to be
                                    read by the client because the hash for
that
                                    content was not available on the server.
    ....Output truncated....
```

如"指令參考資料ONTAP"需詳細 `statistics catalog counter show`資訊，請參閱。

3. 使用收集與 BranchCache 相關的統計資料 `statistics start` 和 `statistics stop` 命令。

```
cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11
```

詳細了解 `statistics start`和 `statistics stop`在"指令參考資料ONTAP" 。

4. 使用顯示收集的 BranchCache 統計資料 `statistics show` 命令。

```
cluster1::*> statistics show -object cifs -counter
branchcache_hash_sent_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0

cluster1::*> statistics show -object cifs -counter
branchcache_missing_hash_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
```

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

5. 返回管理權限層級： `set -privilege admin`

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

相關資訊

- 顯示統計資料
- "效能監控設定"
- "統計開始"
- "統計停止"

了解 ONTAP SMB 對 BranchCache 群組原則物件的支持

支援BranchCache群組原則物件（GPO）、可集中管理某些BranchCache組態參數。ONTAP有兩個GPO用於BranchCache：「BranchCache GPO的雜湊發佈」和「BranchCache GPO的雜湊版本支援」。

- *《BranchCache GPO*雜湊》發佈

  BranchCache GPO 的雜湊發佈會對應到 `-operating-mode` 參數。當發生GPO更新時、此值會套用至群組原則所套用之組織單位（OU）內的儲存虛擬機器（SVM）物件。

- *支援BranchCache GPO *的雜湊版本

  BranchCache GPO 的雜湊版本支援對應到 `-versions` 參數。當發生GPO更新時、此值會套用至群組原則套用至的組織單位內所包含的SVM物件。

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 ONTAP SMB BranchCache 群組原則物件的信息

您可以顯示有關CIFS伺服器的群組原則物件（GPO）組態資訊、以判斷是否為CIFS伺服器所屬的網域定義了BranchCache GPO、如果是、允許的設定為何。您也可以決定是否將BranchCache GPO設定套用至CIFS伺服器。

關於這項工作

即使在CIFS伺服器所屬的網域中定義了GPO設定、但不一定會套用至包含CIFS型儲存虛擬機器（SVM）的組織單位（OU）。套用的GPO設定是套用至CIFS型SVM的所有已定義GPO的子集。透過GPO套用的BranchCache設定會覆寫透過CLI套用的設定。

步驟

1. 使用顯示 Active Directory 網域的已定義 BranchCache GPO 設定 `vserver cifs group-policy show-defined` 命令。

   此範例不會顯示命令的所有可用輸出欄位。輸出被截短。

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

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: version1
  [...]

    GPO Name: Resultant Set of Policy
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for Mode BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]
```

2. 使用顯示套用至 CIFS 伺服器的 BranchCache GPO 設定 `vserver cifs group-policy show-applied` 命令。」

此範例不會顯示命令的所有可用輸出欄位。輸出被截短。

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

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: version1
  [...]

    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: version1
 [...]
```

相關資訊

- 在伺服器上啟用或停用 GPO 支援
- "Vserver CIFS群組原則顯示定義"
- "已套用Vserver CIFS群組原則"

停用**SMB**共用區上的**BranchCache**

了解如何在 **ONTAP SMB** 共用上停用 **BranchCache**

如果您不想在某些SMB共用區上提供BranchCache快取服務、但稍後可能想要在這些共用區上提供快取服務、可以逐一停用BranchCache。如果您已將BranchCache設定為在所有共用區上提供快取功能、但想要暫時停用所有快取服務、您可以修改BranchCache組態、以停止在所有共用區上自動快取。

如果SMB共用區上的BranchCache在第一次啟用後即停用、ONTAP 則停止傳送中繼資料給要求的用戶端。需要

資料的用戶端會直接從內容伺服器（儲存虛擬機器（SVM）上的CIFS伺服器）擷取資料。

相關資訊

了解如何設定啟用 BranchCache 的共享

在單一 ONTAP SMB 共用上停用 BranchCache

如果您不想在先前提供快取內容的某些共用區上提供快取服務、可以停用現有SMB共用區上的BranchCache。

步驟

1. 輸入下列命令： `vserver cifs share properties remove -vserver vserver_name -share -name share_name -share-properties branchcache`

   會移除BranchCache共用內容。其他已套用的共用內容仍會維持有效。

範例

下列命令會在名為「data2」的現有SMB共用區上停用BranchCache：

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

如果您的BranchCache組態自動啟用每個儲存虛擬機器（SVM）上所有SMB共用區的快取、您可以修改BranchCache組態、停止自動快取所有SMB共用區的內容。

關於這項工作

若要停止在所有SMB共用區上自動快取、請將「BranchCache」作業模式變更為「每個共用快取」。

步驟

1. 設定 BranchCache 以停止所有 SMB 共用上的自動快取： `vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
2. 驗證 BranchCache 組態是否正確： `vserver cifs branchcache show -vserver vserver_name`

範例

下列命令會變更儲存虛擬機器（SVM、先前稱為Vserver）VS1上的BranchCache組態、以停止所有SMB共用區上的自動快取：

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

停用或啟用**SVM**上的**BranchCache**

了解在 **ONTAP SMB** 伺服器上停用或重新啟用 **BranchCache** 時會發生什麼情況

如果您先前已設定了BranchCache、但不想讓分公司用戶端使用快取內容、可以停用CIFS伺服器上的快取功能。您必須知道停用BranchCache時會發生什麼情況。

停用BranchCache時ONTAP 、無法再計算雜湊或將中繼資料傳送至要求的用戶端。不過、檔案存取不會中斷。其後、啟用BranchCache的用戶端要求中繼資料資訊以供其存取內容時ONTAP 、會以Microsoft定義的錯誤回應、導致用戶端傳送第二個要求、要求提供實際內容。為了回應內容要求、CIFS伺服器會傳送儲存在儲存虛擬機器（SVM）上的實際內容。

在CIFS伺服器上停用了BranchCache之後、SMB共用區不會通告BranchCache功能。若要存取新SMB連線上的資料、用戶端會進行一般讀取SMB要求。

您可以隨時在CIFS伺服器上重新啟用BranchCache。

- 由於停用BranchCache時並未刪除雜湊存放區、ONTAP 所以只要所要求的雜湊仍然有效、即可在重新啟

用BranchCache後、在回覆雜湊要求時使用儲存的雜湊。

- 在停用BranchCache期間，任何已建立SMB連線至啟用了BranchCache的共用區的用戶端，如果隨後重新啟用了BranchCache，則不會取得BranchCache支援。

  這是因為ONTAP 在設定SMB工作階段時、會針對共用區通告BranchCache支援。在停用了BranchCache的情況下、建立已啟用BranchCache之共用區工作階段的用戶端、必須中斷連線並重新連線、才能使用此共用區的快取內容。

> 如果您不想在CIFS伺服器上停用BranchCache之後儲存雜湊存放區、可以手動刪除它。如果重新啟用了BranchCache、您必須確定雜湊存放區目錄存在。重新啟用BranchCache之後、啟用BranchCache的共用區會通告BranchCache功能。支援BranchCache的用戶端在提出新要求時、會建立新的雜湊。ONTAP

在 **ONTAP SMB** 共用上停用或啟用 **BranchCache**

您可以將 BranchCache 作業模式變更為、以停用儲存虛擬機器（ SVM ）上的 BranchCache `disabled`。您可以隨時啟用BranchCache、只要將作業模式變更為每個共用區提供BranchCache服務、或自動為所有共用區提供。

步驟

1. 執行適當的命令：

如果您想要...	然後輸入下列內容...
停用BranchCache	`vserver cifs branchcache modify -vserver vserver_name -operating-mode disable`
啟用每個共用區的BranchCache	`vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
啟用所有共用區的BranchCache	`vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares`

2. 確認已使用所需的設定來設定 BranchCache 作業模式： `vserver cifs branchcache show -vserver vserver_name`

範例

下列範例停用SVM VS1上的BranchCache：

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: disable
```

刪除**SVM**上的**BranchCache**組態

了解刪除 **ONTAP SMB** 共用上的 **BranchCache** 配置時會發生什麼

如果您先前已設定了BranchCache、但不想讓儲存虛擬機器（SVM）繼續提供快取內容、可以刪除CIFS伺服器上的BranchCache組態。您必須知道刪除組態時會發生什麼事。

當您刪除組態時、ONTAP S什麼 會從叢集移除該SVM的組態資訊、然後停止BranchCache服務。您可以選擇ONTAP 是否應刪除SVM上的雜湊存放區。

刪除BranchCache組態不會中斷啟用BranchCache的用戶端存取。其後、啟用BranchCache的用戶端要求現有SMB連線上已快取內容的中繼資料資訊時ONTAP 、由於Microsoft定義的錯誤、導致用戶端傳送第二個要求、要求提供實際內容。為了回應內容要求、CIFS伺服器會傳送儲存在SVM上的實際內容

在刪除BranchCache組態之後、SMB共用區不會通告BranchCache功能。若要存取先前未使用新SMB連線快取的內容、用戶端會進行一般讀取SMB要求。

刪除 **ONTAP SMB** 共用上的 **BranchCache** 配置

您用於刪除儲存虛擬機器（SVM）上的BranchCache服務的命令、會因您要刪除或保留現有雜湊而有所不同。

步驟

1. 執行適當的命令：

如果您想要...	然後輸入下列內容...
刪除BranchCache組態並刪除現有的雜湊	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes true`
刪除BranchCache組態、但保留現有的雜湊	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes false`

範例

下列範例會刪除SVM VS1上的BranchCache組態、並刪除所有現有的雜湊：

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes
true
```

了解恢復時 **ONTAP SMB BranchCache** 會發生什麼情況

請務必瞭解ONTAP 當您將不支援BranchCache的版本還原為版本時、會發生什麼情況。

- 當您回復ONTAP 到不支援BranchCache的版本時、SMB共用區不會向啟用BranchCache的用戶端通告BranchCache功能、因此用戶端不會要求雜湊資訊。

  而是使用一般SMB讀取要求來要求實際內容。為了回應內容要求、 SMB 伺服器會傳送儲存虛擬機器（ SVM ）上儲存的實際內容。

- 當主控雜湊存放區的節點還原至不支援BranchCache的版本時、儲存管理員需要使用還原期間列印的命令、手動還原BranchCache組態。

  此命令會刪除BranchCache組態和雜湊。

  還原完成後、儲存管理員可視需要手動刪除包含雜湊存放區的目錄。

相關資訊

刪除共享上的 BranchCache 配置

提升**Microsoft**遠端複製效能

了解 **ONTAP SMB** 伺服器上的 **Microsoft** 遠端複製效能改進

Microsoft卸載資料傳輸（ODX）也稱為_copy offload_、可在相容的儲存裝置內或之間直接傳輸資料、而無需透過主機電腦傳輸資料。

支援適用於SMB與SAN傳輸協定的ODX。ONTAP來源可以是CIFS伺服器或LUN、目的地可以是CIFS伺服器或LUN。

在非ODX檔案傳輸中、資料會從來源讀取、並透過網路傳輸到用戶端電腦。用戶端電腦會透過網路將資料傳輸回目的地。總而言之、用戶端電腦會從來源讀取資料、然後寫入目的地。使用ODX檔案傳輸時、資料會直接從來源複製到目的地。

由於ODX卸載複本是直接在來源與目的地儲存設備之間執行、因此效能優勢顯著。實現的效能效益包括加快來源與目的地之間的複製時間、降低用戶端上的資源使用率（CPU、記憶體）、以及降低網路I/O頻寬使用率。

對於SMB環境、此功能只有在用戶端和儲存伺服器均支援SMB 3.0和ODX功能時才能使用。對於SAN環境、此功能僅在用戶端和儲存伺服器均支援ODX功能時才可使用。支援ODX並自動且透明地啟用ODX的用戶端電腦、可在移動或複製檔案時使用卸載檔案傳輸。無論您是透過Windows檔案總管拖放檔案、還是使用命令列檔案複製命令、或是用戶端應用程式啟動檔案複製要求、都會使用ODX。

相關資訊

- 了解如何透過使用自動定位提供自動節點推薦來提高客戶端回應時間
- "Microsoft Hyper-V和SQL Server的SMB組態"

了解 **ONTAP SMB** 伺服器上的 **ODX**

ODX複本卸載使用權杖型機制、在啟用ODX的CIFS伺服器內或之間讀取和寫入資料。CIFS伺服器不會透過主機路由傳送資料、而是傳送代表資料的小Token給用戶端。ODX用戶端會將該權杖呈現給目的地伺服器、然後再將該權杖所代表的資料從來源傳輸到目的地。

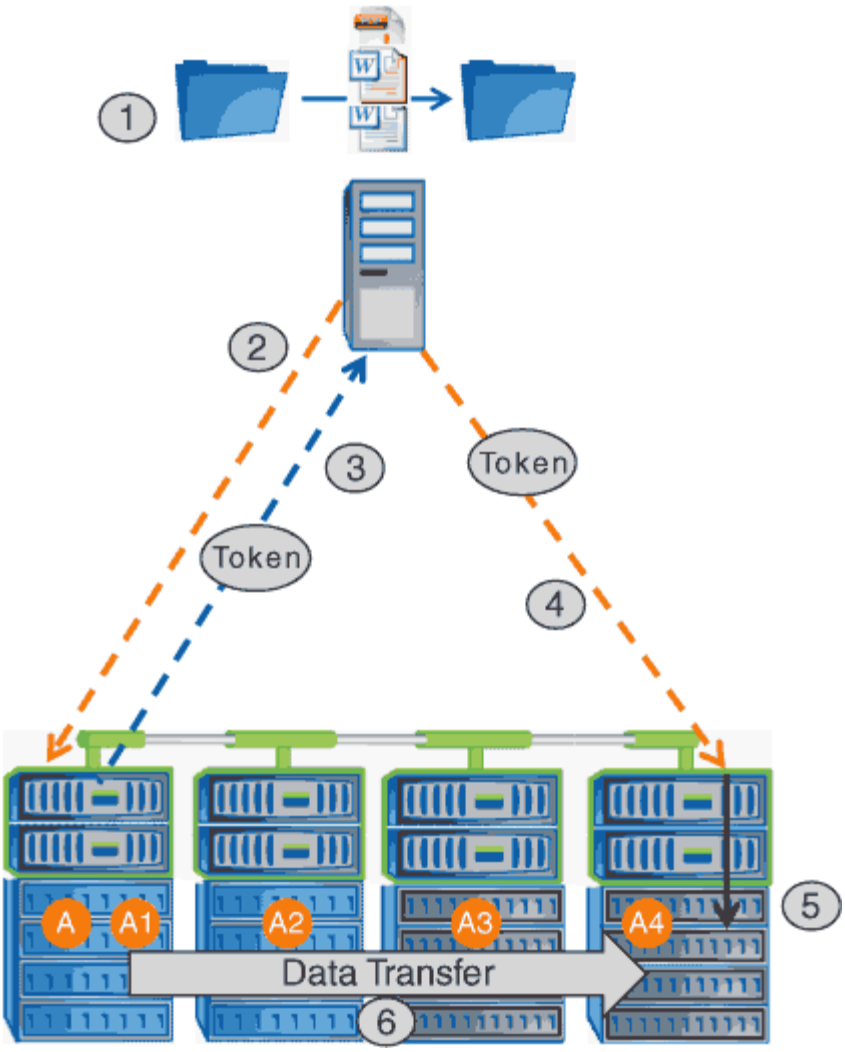
當ODX用戶端得知CIFS伺服器具備ODX功能時、它會開啟來源檔案、並從CIFS伺服器要求權杖。開啟目的地檔案之後、用戶端會使用權杖指示伺服器將資料直接從來源複製到目的地。

> 來源與目的地可以位於相同的儲存虛擬機器（SVM）或不同的SVM上、視複製作業的範圍而定。

此權杖可做為資料的時間點表示。例如、當您在儲存位置之間複製資料時、代表資料區段的權杖會傳回要求的用戶端、用戶端會將該用戶端複製到目的地、因此不需要透過用戶端複製基礎資料。

支援代表8 MB資料的權杖。ONTAP使用多個權杖執行大於8 MB的ODX複本、每個權杖代表8 MB的資料。

下圖說明ODX複製作業的相關步驟：



1. 使用者可以使用Windows檔案總管、命令列介面、或是虛擬機器移轉的一部分、或是應用程式啟動檔案複本或移動、來複製或移動檔案。
2. 具備ODX功能的用戶端會自動將此傳輸要求轉譯為ODX要求。

   傳送至CIFS伺服器的ODX要求包含權杖要求。
3. 如果在CIFS伺服器上啟用ODX、而且連線是透過SMB 3.0、則CIFS伺服器會產生權杖、這是資料在來源上的邏輯表示。
4. 用戶端會收到代表資料的權杖、並隨寫入要求一起傳送至目的地CIFS伺服器。

   這是唯一透過網路從來源複製到用戶端、然後從用戶端複製到目的地的資料。
5. 權杖會傳送至儲存子系統。
6. SVM會在內部執行複本或移動。

   如果複製或移動的檔案大於8 MB、則需要多個權杖才能執行複本。視需要執行步驟2至6以完成複本。

如果ODX卸載複本發生故障、複本或移動作業會回復為複本或移動作業的傳統讀取和寫入。同樣地、如果目的地CIFS伺服器不支援ODX或ODX已停用、則複製或移動作業會回溯到複製或移動作業的傳統讀取和寫入。

在 **ONTAP SMB** 伺服器上使用 **ODX** 的要求

在您使用ODX卸載儲存虛擬機器（SVM）的複本之前、您必須先瞭解某些需求。

版本需求**ONTAP**

發行版支援ODX進行複本卸載。ONTAP

SMB版本需求

- 支援ODX搭配SMB 3.0及更新版本。ONTAP
- 必須在CIFS伺服器上啟用SMB 3.0、才能啟用ODX：
  - 如果尚未啟用ODX、啟用ODX也會啟用SMB 3.0。
  - 停用SMB 3.0也會停用ODX。

Windows伺服器與用戶端需求

在使用ODX卸載複本之前、Windows用戶端必須支援此功能。

- "NetApp 互通性對照表"包含支援的 Windows 用戶端的最新資訊。

Volume需求

- 來源磁碟區至少必須為1.25 GB。
- 如果您使用壓縮磁碟區、壓縮類型必須是可調適的、而且只支援8K大小的壓縮群組。

  不支援次要壓縮類型。

在 **ONTAP SMB** 伺服器上使用 **ODX** 的指南

在使用ODX進行複本卸載之前、您必須先瞭解準則。例如、您需要知道可以使用ODX的磁碟區類型、而且需要瞭解叢集內和叢集間ODX的考量。

Volume準則

- 您無法使用ODX進行下列Volume組態的複本卸載：
  - 來源Volume大小低於1.25 GB

    磁碟區大小必須大於或等於1.25 GB、才能使用ODX。
  - 唯讀磁碟區

    ODX不適用於位於負載共享鏡像或SnapMirror或SnapVault 目的地Volume中的檔案和資料夾。
  - 如果來源Volume未進行重複資料刪除
- ODX複本僅支援叢集內複本。

  您無法使用ODX將檔案或資料夾複製到其他叢集中的磁碟區。

其他準則

- 在SMB環境中、若要使用ODX進行複本卸載、檔案必須大於或等於256 KB。

  較小的檔案會使用傳統的複製作業來傳輸。

- ODX複製卸載會在複製程序中使用重複資料刪除技術。

  如果您不想在複製或移動資料時於SVM磁碟區上執行重複資料刪除、則應停用該SVM上的ODX複本卸載。

- 執行資料傳輸的應用程式必須寫入以支援ODX。

  支援ODX的應用程式作業包括：

  - Hyper-V 管理作業，例如建立及轉換虛擬硬碟（ VHD ），管理快照，以及在虛擬機器之間複製檔案
  - Windows檔案總管作業
  - Windows PowerShell複製命令
  - Windows命令提示字元複製命令

    Windows命令提示字元的Robocopy支援ODX。

    應用程式必須在支援ODX的Windows伺服器或用戶端上執行。

  +
  如需Windows伺服器和用戶端上支援的ODX應用程式的詳細資訊、請參閱Microsoft TechNet程式庫。

相關資訊

"Microsoft TechNet程式庫：technet.microsoft.com/en-us/library/"

ONTAP SMB 伺服器上 **ODX** 的用例

您應該瞭解在SVM上使用ODX的使用案例、以便判斷ODX在何種情況下可為您提供效能優勢。

支援ODX的Windows伺服器和用戶端使用複本卸載做為在遠端伺服器上複製資料的預設方法。如果Windows伺服器或用戶端不支援ODX、或ODX複本卸載在任何時間點都失敗、則複本或移動作業會回溯到複本或移動作業的傳統讀取和寫入。

下列使用案例支援使用ODX複本和移動：

- Volume內

  來源與目的地檔案或LUN位於同一個磁碟區內。

- 磁碟區間、相同節點、相同SVM

  來源與目的地檔案或LUN位於同一個節點上的不同磁碟區。資料歸同一個SVM所有。

- 磁碟區間、不同節點、相同SVM

來源與目的地檔案或LUN位於不同節點上的不同磁碟區。資料歸同一個SVM所有。

- SVM之間、相同節點

  來源與目的地檔案或LUN位於同一個節點上的不同磁碟區。資料由不同的SVM擁有。

- SVM之間、不同節點

  來源與目的地檔案或LUN位於不同節點上的不同磁碟區。資料由不同的SVM擁有。

- 叢集間

  來源和目的地LUN位於不同的磁碟區、位於不同的叢集節點上。這僅適用於SAN、不適用於CIFS。

還有一些特殊使用案例：

- 藉由ONTAP 採用流通不整的ODX技術、您可以使用ODX在SMB共享區與FC或iSCSI附加虛擬磁碟機之間複製檔案。

  您可以使用Windows檔案總管、Windows CLI或PowerShell、Hyper-V或其他支援ODX的應用程式、使用ODX複製卸載功能在SMB共用區和連線LUN之間順暢地複製或移動檔案、前提是SMB共用區和LUN位於同一個叢集上。

- Hyper-V針對ODX複製卸載提供了一些額外的使用案例：

  - 您可以使用ODX複本卸載傳遞搭配Hyper-V、在虛擬硬碟（VHD）檔案內或之間複製資料、或在同一個叢集內的對應SMB共用區和連接的iSCSI LUN之間複製資料。

    如此一來、從客體作業系統的複本就能傳遞到基礎儲存設備。

  - 建立固定大小的VHD時、ODX會使用已知的零權杖、以零初始化磁碟。
  - 如果來源與目的地儲存設備位於同一個叢集、則ODX複本卸載可用於虛擬機器儲存移轉。

> ⓘ 若要利用ODX複本卸載傳遞與Hyper-V的使用案例、來賓作業系統必須支援ODX、而來賓作業系統的磁碟必須是支援ODX的儲存設備（SMB或SAN）所支援的SCSI磁碟。客體作業系統上的IDE磁碟不支援ODX傳遞。

在 **ONTAP SMB** 伺服器上啟用或停用 **ODX**

您可以在儲存虛擬機器（SVM）上啟用或停用ODX。預設為啟用支援ODX複本卸載（若同時啟用SMB 3.0）。

開始之前

必須啟用SMB 3.0。

關於這項工作

如果您停用SMB 3.0、ONTAP 則不支援SMB ODX。如果您重新啟用SMB 3.0、則必須手動重新啟用SMB ODX。

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**ODX**複本卸載...	輸入命令...
已啟用	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled true`
已停用	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled false`

3. 返回管理權限層級： `set -privilege admin`

範例

下列範例可在SVM VS1上啟用ODX複製卸載：

```
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 -copy-offload
-enabled true

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

相關資訊

可用的伺服器選項

透過自動定位提供SMB自動節點參照、縮短用戶端回應時間

了解如何透過使用自動定位提供 **ONTAP SMB** 自動節點引用來縮短客戶端回應時間

「自動定位」使用SMB自動節點參照來提升儲存虛擬機器（SVM）上的SMB用戶端效能。自動節點參照會自動將要求的用戶端重新導向至裝載資料所在磁碟區之節點SVM上的LIF、進而改善用戶端回應時間。

當SMB用戶端連線至裝載於SVM上的SMB共用時、它可能會使用不擁有所要求資料的節點上的LIF進行連線。用戶端所連接的節點會使用叢集網路存取其他節點所擁有的資料。如果SMB連線使用位於包含所要求資料之節點上的LIF、用戶端就能獲得更快的回應時間：

- 提供此功能的方法是使用Microsoft Dfs轉介來通知SMB用戶端命名空間中所要求的檔案或資料夾位於其他位置。ONTAP

當節點判斷包含資料的節點上是否有任一SVM LIF時、就會進行參照。

- 支援自動節點參照、可用於IPV4和IPv6 LIF IP位址。
- 參照是根據用戶端所連線之共用區根的位置而進行。
- 參照發生在SMB交涉期間。

參照會在建立連線之前進行。將SMB用戶端指向目標節點之後ONTAP 、就會建立連線、然後用戶端從該點透過參照的LIF路徑存取資料。這可讓用戶端更快存取資料、避免額外的叢集通訊。

> 如果共享區跨越多個交會點、而部分交會則是包含在其他節點上的磁碟區、則共用區內的資料會分散在多個節點上。由於支援從本機介面轉介至共享區根目錄、因此、必須使用叢集網路來擷取這些非本機磁碟區內的資料。ONTAP ONTAP 有了這種命名空間架構、自動節點參照可能無法提供顯著的效能效益。

如果託管資料的節點沒有可用的LIF、ONTAP 則使用用戶端選擇的LIF來建立連線。在SMB用戶端開啟檔案之後、它會繼續透過相同的參照連線來存取檔案。

如果CIFS伺服器因故無法進行轉介、則不會中斷SMB服務。建立SMB連線時、會如同未啟用自動節點參照。

相關資訊

提升Microsoft遠端複製效能

在 **ONTAP SMB** 伺服器上使用自動節點引用的要求和準則

在您使用SMB自動節點參照（也稱為_autosocure_）之前、您必須先瞭解某些需求、包括ONTAP 哪些版本的支援功能。您也必須瞭解支援的SMB傳輸協定版本及其他特定準則。

版本與授權要求**ONTAP**

- 叢集中的所有節點都必須執行ONTAP 支援自動節點參照的版本的支援功能。
- 必須在SMB共用區上啟用Widgelinks、才能使用自動定位功能。
- CIFS必須獲得授權、且SVM上必須有SMB伺服器。SMB 授權隨附於"ONTAP One"。如果您沒有 ONTAP One 且未安裝授權、請聯絡您的銷售代表。

SMB傳輸協定版本需求

- 對於SVM、ONTAP 此功能支援在所有SMB版本上自動轉介節點。

SMB用戶端需求

支援的所有Microsoft用戶端ONTAP 均支援SMB自動節點轉介。

互通性對照表包含Windows用戶ONTAP 端所支援的最新資訊。

"NetApp 互通性對照表工具"

資料**LIF**需求

如果您想要使用資料LIF做為SMB用戶端的潛在參照、則必須同時啟用NFS和CIFS來建立資料生命期。

如果目標節點包含僅針對NFS傳輸協定啟用或僅針對SMB傳輸協定啟用的資料LIF、則自動節點參照可能無法運作。

如果不符合此要求、資料存取將不受影響。SMB用戶端會使用用戶端用來連線至SVM的原始LIF來對應共用區。

建立參照**SMB**連線時的**NTLM**驗證需求

必須允許在包含CIFS伺服器的網域和包含要使用自動節點參照之用戶端的網域上進行NTLM驗證。

進行轉介時、SMB伺服器會將IP位址指向Windows用戶端。由於使用IP位址進行連線時會使用NTLM驗證、因此不會針對參照的連線執行Kerberos驗證。

發生這種情況的原因是 Windows 用戶端無法建立 Kerberos 所使用的服務主體名稱（屬於表單 `service/NetBIOS name` 和 `service/FQDN`）、這表示用戶端無法向服務要求 Kerberos 票證。

使用主目錄功能自動節點參照的準則

當共用區設定為啟用主目錄共用屬性時、可以針對主目錄組態設定一或多個主目錄搜尋路徑。搜尋路徑可指向包含SVM磁碟區的每個節點上所包含的磁碟區。用戶端會接收參照、如果有作用中的本機資料LIF可用、則會透過主使用者主目錄的本機參照LIF連線。

當SMB 1.0用戶端存取啟用自動節點參照的動態主目錄時、有一些準則。這是因為SMB 1.0用戶端需要在驗證之前自動進行節點參照、SMB伺服器才有使用者名稱。不過、如果下列陳述屬實、SMB主目錄存取功能可在SMB 1.0用戶端正常運作：

- SMB主目錄設定為使用簡單名稱、例如「`%w'（Windows使用者名稱）」或「%u」（對應的UNIX使用者名稱）、而非網域名稱樣式名稱、例如「`%d\%w」（網域名稱\使用者名稱）。
- 建立主目錄共用時、CIFS主目錄共用名稱會設定變數（「'%w'」或「'%u'」）、而非靜態名稱、例如「'home'」。

對於SMB 2.x和SMB 3.0用戶端、使用自動節點參照來存取主目錄時、沒有特別的準則。

在**CIFS**伺服器上停用自動節點參照的準則（含現有參照連線）

如果您在啟用此選項之後停用自動節點參照、則目前連線至參照LIF的用戶端會保留參照的連線。由於支援使用DFS轉介做為SMB自動節點轉介的機制、因此在停用此選項之後、用戶端甚至可以重新連線到參照的LIF、直到用戶端的快取DFS參照 逾時為止。ONTAP即使還原ONTAP 至不支援自動節點參照的版本、也一樣。用戶端會繼續使用參照、直到來自用戶端快取的Dfs參照逾時為止。

Autolocation會使用SMB自動節點參照、將用戶端轉介至擁有SVM資料磁碟區的節點上的LIF、藉此提高SMB用戶端效能。當SMB用戶端連線至裝載於SVM上的SMB共用時、它可能會使用不擁有所要求資料的節點上的LIF來連線、並使用叢集互連網路來擷取資料。如果SMB連線使用位於包含所要求資料之節點上的LIF、用戶端就能獲得更快的回應時間。

提供此功能的方法是使用Microsoft分散式檔案系統（Dfs）轉介來通知SMB用戶端命名空間中所要求的檔案或資料夾位於其他位置。ONTAP當節點判斷包含資料的節點上有SVM LIF時、就會進行參照。參照是根據用戶端所連線之共用區根的位置而進行。

參照發生在SMB交涉期間。參照會在建立連線之前進行。將SMB用戶端指向目標節點之後ONTAP 、就會建立連

線、然後用戶端從該點透過參照的LIF路徑存取資料。這可讓用戶端更快存取資料、避免額外的叢集通訊。

在**Mac OS**用戶端上使用自動節點參照的準則

Mac OS X用戶端不支援SMB自動節點轉介、即使Mac OS支援Microsoft的分散式檔案系統（DFs）。Windows用戶端在連線至SMB共用區之前、會先提出一個Dfs參照要求。提供資料LIF的參照、可在裝載所要求資料的同一個節點上找到、進而改善用戶端回應時間。ONTAP雖然Mac OS支援DFS,Mac OS用戶端在此領域的行為與Windows用戶端並不完全相同。

相關資訊

- 了解如何在伺服器上啟用動態主目錄
- "網路管理"
- "NetApp 互通性對照表工具"

支援 **ONTAP SMB** 自動節點引用

在啟用SMB自動節點參照之前、您應該注意某些ONTAP 功能不支援參照。

- 下列類型的磁碟區不支援SMB自動節點參照：
  - 負載共用鏡像的唯讀成員
  - 資料保護鏡射的目的地Volume
- 節點參照不會隨著LIF移動而移動。

  如果用戶端使用SMB 2.x或SMB 3.0連線上的參照連線、而資料LIF在不中斷營運的情況下移動、即使LIF不再是資料的本機連線、用戶端仍會繼續使用相同的參照連線。

- 節點參照不會隨著磁碟區移動而移動。

  如果用戶端透過任何SMB連線使用參照連線、而發生磁碟區移動、則即使磁碟區不再與資料LIF位於同一個節點、用戶端仍會繼續使用相同的參照連線。

啟用或停用 **ONTAP SMB** 自動節點引用

您可以啟用SMB自動節點參照、以提升SMB用戶端存取效能。如果您不想ONTAP 讓使用者向SMB用戶端轉介資料、可以停用自動節點轉介。

開始之前

CIFS伺服器必須設定並在儲存虛擬機器（SVM）上執行。

關於這項工作

SMB自動節點參照功能預設為停用。您可以視需要在每個SVM上啟用或停用此功能。

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. 視需要啟用或停用SMB自動節點參照：

如果您想要SMB自動節點參照...	輸入下列命令...
已啟用	`vserver cifs options modify -vserver vserver_name -is-referral-enabled true`
已停用	`vserver cifs options modify -vserver vserver_name -is-referral-enabled false`

選項設定會對新的SMB工作階段生效。具有現有連線的用戶端只能在現有快取逾時過期時使用節點參照。

3. 切換至管理員權限層級： `set -privilege admin`

相關資訊

可用的伺服器選項

使用統計資料監控 **ONTAP SMB** 自動節點參考活動

若要判斷要參照多少 SMB 連線、您可以使用監控自動節點參照活動 `statistics` 命令。透過監控轉介、您可以判斷自動轉介在裝載共用的節點上尋找連線的程度、以及是否應重新分配資料生命量、以提供對CIFS伺服器上共用區的更佳本機存取。

關於這項工作

。 `cifs` 物件在進階權限層級提供數個計數器、可在監控 SMB 自動節點參照時提供協助：

- `node_referral_issued`

  在用戶端使用與共用根節點不同的節點所主控的LIF連線之後、已向共用根節點發出參照的用戶端數目。

- `node_referral_local`

  使用裝載共用根目錄之同一個節點所裝載之LIF進行連線的用戶端數目。本機存取通常可提供最佳效能。

- `node_referral_not_possible`

  使用與共用根節點不同的節點所裝載的LIF進行連線之後、尚未向裝載共用根目錄的節點發出轉介的用戶端數目。這是因為找不到共用根節點的作用中資料LIF。

- `node_referral_remote`

  使用裝載於共享根目錄之節點不同之節點的LIF所連線的用戶端數目。遠端存取可能導致效能降低。

您可以在儲存虛擬機器（SVM）上收集及檢視特定時間段（範例）的資料、以監控自動節點參照統計資料。如果不停止資料收集、您可以檢視範例中的資料。停止資料收集可提供固定的範例。不停止資料收集可讓您取得更新的資料、以便與先前的查詢進行比較。這項比較可協助您識別效能趨勢。

評估及使用您從收集到的資訊 `statistics` 命令、您應該瞭解用戶端在環境中的發佈。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 使用檢視自動節點參照統計資料 `statistics` 命令。

   此範例透過收集和檢視取樣期間的資料來檢視自動節點參照統計資料：

   a. 開始收藏： `statistics start -object cifs -instance vs1 -sample-id sample1`

   ```
   Statistics collection is being started for Sample-id: sample1
   ```

   b. 等待所需的收集時間到。

   c. 停止集合： `statistics stop -sample-id sample1`

   ```
   Statistics collection is being stopped for Sample-id: sample1
   ```

   詳細了解 `statistics start`和 `statistics stop`在"指令參考資料ONTAP" 。

   d. 檢視自動節點參照統計資料： `statistics show -sample-id sample1 -counter` **`node`**

   ```
   Object: cifs
   Instance: vs1
   Start-time: 2/4/2013 19:27:02
   End-time: 2/4/2013 19:30:11
   Cluster: cluster1

       Counter                                     Value
       --------------------------- ----------------------------
       node_name                                   node1
       node_referral_issued                            0
       node_referral_local                             1
       node_referral_not_possible                      2
       node_referral_remote                            2
       ...

       node_name                                   node2
       node_referral_issued                            2
       node_referral_local                             1
       node_referral_not_possible                      0
       node_referral_remote                            2
       ...
   ```

   輸出會顯示所有參與SVM VS1的節點計數器。為了清楚起見、範例中僅提供與自動節點參照統計資料相關的輸出欄位。

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

3. 返回管理權限層級： `set -privilege admin`

相關資訊

- 顯示統計資料
- "效能監控設定"

使用 **Windows** 用戶端監控用戶端 **ONTAP SMB** 自動節點參考訊息

若要從用戶端的角度判斷要進行哪些轉介、您可以使用 Windows `dfsutil.exe` 公用程式：

Windows 7 及更新版本用戶端隨附的遠端伺服器管理工具（ RSAT ）套件包含 `dfsutil.exe` 公用程式：使用此公用程式、您可以顯示參照快取內容的相關資訊、以及檢視用戶端目前所使用之每個參照的相關資訊。您也可以使用公用程式清除用戶端的參照快取。如需詳細資訊、請參閱Microsoft TechNet程式庫。

相關資訊

"Microsoft TechNet程式庫：technet.microsoft.com/en-us/library/"

利用存取型列舉、為共享區提供資料夾安全性

透過基於存取的枚舉在共用上提供 **ONTAP SMB** 資料夾安全性

在SMB共用區上啟用存取型列舉（ABE）時、沒有權限存取共用區中所含資料夾或檔案的使用者（無論是透過個別或群組權限限制）、不會看到其環境中顯示的共用資源、不過共用區本身仍為可見。

傳統共用內容可讓您指定哪些使用者（個別或群組）有權檢視或修改共用區中包含的檔案或資料夾。不過、這些資料夾不允許您控制共用區內的資料夾或檔案是否可供無權存取的使用者查看。如果共用區中的這些資料夾或檔案名稱描述敏感資訊、例如客戶名稱或開發中的產品、可能會造成問題。

存取型列舉（ABE）可延伸共用內容、以包括共用區內的檔案與資料夾列舉。因此、Abe可讓您根據使用者存取權限、篩選共用區內的檔案和資料夾顯示。也就是所有使用者都能看到共用區本身、但共用區內的檔案和資料夾可能會顯示給指定使用者、或是隱藏給指定使用者。除了保護工作環境中的敏感資訊、ABE還能讓您簡化大型目錄結構的顯示、讓不需要存取完整內容的使用者受益。例如、共用區本身對所有使用者都是可見的、但共用區內的檔案和資料夾可能會顯示或隱藏。

深入瞭解 "使用SMB/CIFS存取型列舉時的效能影響"。

在 **ONTAP SMB** 共用上啟用或停用基於存取的枚舉

您可以在SMB共用區上啟用或停用存取型列舉（ABE）、以允許或防止使用者看到他們無權存取的共用資源。

關於這項工作

依預設、ABE為停用狀態。

步驟

1. 執行下列其中一項動作：

如果您想要...	輸入命令...
在新共用區上啟用ABE	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share -properties access-based-enumeration`建立 SMB 共用時，您可以指定其他選用的共用設定和其他共用內容。如"指令參考資料ONTAP"需詳細 `vserver cifs share create`資訊，請參閱。
在現有共用區上啟用ABE	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` 保留現有的共用內容。ABE共用屬性會新增至現有的共用屬性清單。
停用現有共用區上的ABE	`vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` 其他共用內容將會保留。只有ABE共用內容會從共用內容清單中移除。

2. 使用確認共用組態正確無誤 `vserver cifs share show` 命令。

範例

以下範例建立名為「銷售」的 ABE SMB 共用、路徑為 `/sales` 在 SVM VS1 上。共用即會建立於 `access-based-enumeration` 做為共享內容：

```
cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path
/sales  -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

                      Vserver: vs1
                        Share: sales
     CIFS Server NetBIOS Name: VS1
                         Path: /sales
             Share Properties: access-based-enumeration
                               oplocks
                               browsable
                               changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

下列範例新增 `access-based-enumeration` 將內容共用至名為「 data2 」的 SMB 共用區：

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
------- ---------- ------------------------------------------------------
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration
```

相關資訊

新增或刪除現有共享的共享屬性

在 **ONTAP SMB** 共用上啟用或停用 **Windows** 用戶端的基於存取的枚舉

您可以從Windows用戶端啟用或停用SMB共用上的存取型列舉（ABE）、讓您無需連線至CIFS伺服器即可設定此共用設定。

。 `abecmd` Windows Server 和 Windows 用戶端的新版本不提供公用程式。它是Windows Server 2008的一部分。Windows Server 2008支援服務已於2020年1月14日終止。

步驟

1. 從支援 ABE 的 Windows 用戶端輸入下列命令： `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

   如需更多關於的資訊、請參閱 `abecmd` 命令、請參閱 Windows 用戶端文件。

NFS和SMB檔案及目錄命名相依性

了解 ONTAP NFS 和 SMB 檔案和目錄命名依賴關係

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

作業系統和檔案共用傳輸協定決定下列事項：

- 檔案名稱可使用的字元
- 檔案名稱的大小寫敏感度

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

了解 ONTAP SMB 檔案或目錄名稱的有效字符

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

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

多協定環境中 ONTAP SMB 檔案和目錄名稱的大小寫敏感性

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

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

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

- 在 SMB 用戶端上、您會看到 `testdir` 和 `TESTDI~1`。
- ONTAP 會建立 `TESTDI~1` 用於區分兩個目錄的目錄名稱。

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

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

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

> 如果您已使用vserver CIFS字元對應命令啟用或修改字元對應、則通常不區分大小寫的Windows查詢會變成區分大小寫。

了解如何建立 **ONTAP SMB** 檔案和目錄名稱

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

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

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

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

- 如果是檔案、則會將副檔名縮短為三個字元。

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

了解 **ONTAP SMB** 多位元組檔案、目錄和 **qtree** 名稱

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

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

您必須以下列其中一種方式建立新的Volume：

- 設定音量 `-language` 選項明確： `volume create -language utf8mb4 {…}`
- 繼承 Volume `-language` SVM 中的選項、此選項已針對選項建立或修改： `vserver [create|modify] -language utf8mb4 {…}``volume create {…}`
- 在 ONTAP 9.6 及更早版本中、您無法修改現有的 Volume 以支援 utf8mb4 ；您必須建立新的 utf8mb4 就緒磁碟區、然後使用用戶端型複本工具移轉資料。

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

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

- 從 ONTAP 9.8 開始、您可以使用 `[-language <Language code>]` 將 Volume 語言從 *.UTF-8 變更為 utf8mb4 的參數。若要變更 Volume 的語言、請聯絡 "NetApp支援"。

> ⓘ 目前不支援使用4位元組utf-8字元的LUN名稱。

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

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

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

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

從ONTAP 功能表9開始、qtree名稱中允許使用統一碼字元。

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

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

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

為磁碟區上的 **ONTAP SMB** 檔案名稱轉換設定字元映射

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

則將無效。

關於這項工作

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

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

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

您可以依Volume設定字元對應。

在磁碟區上設定字元對應時、必須謹記下列事項：

- 字元對應不會套用至交叉點。

  您必須明確設定每個交會Volume的字元對應。

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

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

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

步驟

1. 設定字元對應：+

`vserver cifs character-mapping create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-mapping` *`mapping_text`*`, …` +

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

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

- 來源對應+

下表顯示來源對應的允許UNICODE字元集：

+

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

- 目標對應

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

範例

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

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

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

相關資訊

了解如何在命名空間中建立和管理資料卷

用於管理 SMB 檔案名稱轉換的字元對映的 ONTAP 命令

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

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

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

相關資訊

配置卷上的檔案名稱轉換的字元映射

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

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

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

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

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

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

商標資訊

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