管理SMB伺服器

ONTAP 9

NetApp
April 24, 2024

目錄

管理SMB伺服器

修改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。如需詳細資料、請參閱手冊頁。

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**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`

   如需設定 SMB 伺服器選項的詳細資訊、請參閱的手冊頁 `vserver cifs options modify` 命令。

設定授予**SMB**使用者**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`

設定匿名使用者的存取限制

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SMB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

管理如何向**SMB**用戶端提供檔案安全性、以利**UNIX**安全型態的資料總覽

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

啟用或停用**NTFS ACL**的**UNIX**安全型資料呈現

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`

如何保留**UNIX**權限**ONTAP**

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

使用**Windows**安全性索引標籤管理**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

如何處理SMB用戶端驗證ONTAP

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。

SVM災難恢復組態中SMB伺服器安全性設定的準則

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

啟用或停用本機SMB使用者所需的密碼複雜度

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
>
> 您不得使用 `vserver cifs security modify` 工作群組模式中的 CIFS 伺服器命令、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CIFS伺服器安全性設定的資訊

使用本機使用者和群組進行驗證和授權

本機使用者密碼需求

變更本機使用者帳戶密碼

修改CIFS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CIFS伺服器安全性設定的資訊"

"支援的GPO"

"將群組原則物件套用至CIFS伺服器"

設定SMB伺服器的最低驗證安全性層級

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。
`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

啟用或停用AES加密以進行Kerberos型通訊

使用AES加密來設定Kerberos通訊的強大安全性

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` 可啟用建議加密類型的選項、您也可以使用此選項來停用較弱的加密類型。瞭解操作方法 "啟用和停用Kerberos型通訊的加密類型"。

> 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CIFS伺服器Kerberos安全性設定

啟用或停用**Kerberos**型通訊的**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
```

使用**SMB**簽署來強化網路安全性

使用**SMB**簽署來強化網路安全性總覽

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。

SMB簽署原則如何影響與**CIFS**伺服器的通訊

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

用戶端	**ONTAP** -不需要簽署	**ONTAP** -需要簽署
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 ）

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。

設定**SMB**簽署的建議

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。

設定多個資料生命量時的**SMB**簽署準則

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。

啟用或停用傳入**SMB**流量所需的**SMB**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。

判斷**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**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。
3. 使用 `statistics stop` 停止收集樣本資料的命令。
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。

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

SMB加密總覽

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。

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**SMB**流量所需的**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
```

判斷用戶端是否使用加密的**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**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。

3. 使用 statistics stop 停止收集樣本資料的命令。
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。

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

判斷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

LDAP簽署與密封概念

從ONTAP 功能支援功能支援功能支援功能支援功能、從功能支援功能支援功能升級至功能性管理功能。您必須在儲存虛擬機器（SVM）上設定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**CIFS**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

匯出自我簽署根CA憑證的複本

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

啟用LDAP over TLS時、ONTAP SVM上的SVM上的SfyLDAP用戶端不支援ONTAP 使用版本為9.0和9.1的撤銷憑證。

從ONTAP 功能支援的9.2開始、ONTAP 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*`

在伺服器上啟用**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：

- "LDAP 概述"
- "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SMB多通道以獲得效能與備援

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` *`options`*
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**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root

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

但是、如果您的儲存系統設定為僅 NTFS 、則會設定為 `/etc` 目錄具有檔案層級的 ACL 、可讓系統管理員群組存取 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
```

命令選項可限制過多的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」）

如需預設限制、請參閱手冊頁、並顯示目前的組態。

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

利用傳統和租賃oplock總覽來改善用戶端效能

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。

使用**oplocks**時、請將快取資料遺失的考量寫入

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**SMB**共用時啟用或停用**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

在磁碟區和qtree上啟用或停用oplock的命令

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SMB共用區上的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。

如果您想要...	然後...
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

監控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）

請參閱 `vserver oplocks show` 手冊頁、以取得每個參數的詳細說明。

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

在磁碟區和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

將群組原則物件套用至SMB伺服器總覽

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

使用動態存取控制（DAC）保護檔案存取

"SMB與NFS稽核與安全性追蹤"

支援的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CIFS伺服器上啟用或停用GPO支援

使用動態存取控制（DAC）保護檔案存取

"SMB與NFS稽核與安全性追蹤"

修改CIFS伺服器Kerberos安全性設定

使用BranchCache快取分公司的SMB共用內容

使用SMB簽署來強化網路安全性

設定略過周遊檢查

設定匿名使用者的存取限制

搭配SMB伺服器使用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。隨附 SMB 授權 "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CIFS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

支援的GPO

在CIFS伺服器上使用GPO的需求

如何在CIFS伺服器上更新GPO

手動更新CIFS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

如何在**CIFS**伺服器總覽中更新**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CIFS伺服器上的GPO設定

手動更新CIFS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

如何在CIFS伺服器上更新GPO

顯示有關GPO組態的資訊

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CIFS伺服器上啟用或停用GPO支援

顯示受限群組GPO的詳細資訊

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`

如果您要顯示所有受限群組GPO的相關資訊...	輸入命令...
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

顯示有關集中存取原則的資訊

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

使用動態存取控制（DAC）保護檔案存取

顯示有關GPO組態的資訊

顯示中央存取原則規則的相關資訊

顯示有關集中存取原則規則的資訊

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

使用動態存取控制（DAC）保護檔案存取

顯示有關GPO組態的資訊

顯示中央存取原則的相關資訊

用於管理SMB伺服器電腦帳戶密碼的命令

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...
變更或重設網域帳戶密碼、您就知道密碼	`vserver cifs domain password change`
重設網域帳戶密碼、但您不知道密碼	`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`

如需詳細資訊、請參閱每個命令的手冊頁。

管理網域控制器連線

顯示探索到的伺服器相關資訊

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

重新設定及重新探索伺服器

停止或啟動CIFS伺服器

重設並重新探索伺服器

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

顯示已探索伺服器的相關資訊

停止或啟動CIFS伺服器

管理網域控制器探索

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。

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。

新增慣用的網域控制器

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

管理慣用網域控制器的命令

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`

如需詳細資訊、請參閱每個命令的手冊頁。

相關資訊

新增慣用的網域控制器

啟用與網域控制器的SMB2連線

從ONTAP 推出支援支援功能的支援功能支援使用SMB 2.0版連線至網域控制器。如果您已在網域控制器上停用SMB 1.0、就必須這麼做。從功能9.2開始ONTAP 、預設會啟用SMB2。

關於這項工作

。 `smb2-enabled-for-dc-connections` 命令選項會針對您所使用的 ONTAP 版本啟用系統預設值。系統預設ONTAP 值為支援SMB 1.0、而SMB 2.0則停用。系統預設ONTAP 為適用於SMB 1.0的系統預設值為啟用、並啟用SMB 2.0。如果網域控制器一開始無法協調SMB 2.0、則會使用SMB 1.0。

SMB 1.0可從ONTAP 功能區停用至網域控制器。在支援功能9.1中ONTAP 、如果SMB 1.0已停用、則必須啟用SMB 2.0才能與網域控制器通訊。

深入瞭解：

- "正在驗證啟用的SMB版本"。
- "支援的SMB版本與功能"。

> 如果 `-smb1-enabled-for-dc-connections` 設為 `false` 而 `-smb1-enabled` 設為 `true`，ONTAP 拒絕 SMB 1.0 連線做為用戶端，但會繼續接受傳入 SMB 1.0 連線做為伺服器。

步驟

1. 變更 SMB 安全性設定之前、請先確認已啟用哪些 SMB 版本： `vserver cifs security show`
2. 向下捲動清單以查看SMB版本。
3. 使用執行適當的命令 `smb2-enabled-for-dc-connections` 選項。

如果您想要SMB2為...	輸入命令...
已啟用	`vserver cifs security modify -vserver` *`vserver_name`* `-smb2-enabled-for-dc -connections true`

如果您想要SMB2為...	輸入命令...
已停用	`vserver cifs security modify -vserver` *`vserver_name`* `-smb2-enabled-for-dc -connections false`

啟用對網域控制器的加密連線

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null工作階段存取非Kerberos環境中的儲存設備總覽

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。

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 Windows RestrictAnonymous 登錄設定值與 `-restrict-anonymous` 選項。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）。。 `vserver cifs options modify` 和 `vserver cifs options show` 手冊頁提供有關的更多資訊 `-restrict-anonymous` 選項。

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使用者檔案系統共用的存取權

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

管理SMB伺服器的NetBios別名總覽

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

新增一組NetBios別名至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NetBios別名清單中移除NetBios別名

顯示CIFS伺服器上的NetBios別名清單

從NetBios別名清單中移除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**CIFS**伺服器上的**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
```

如需命令的詳細資訊、請參閱手冊頁。

相關資訊

新增一組NetBios別名至CIFS伺服器

管理CIFS伺服器的命令

判斷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CIFS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

顯示已探索伺服器的相關資訊

重新設定及重新探索伺服器

將**CIFS**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**SMB**伺服器之前、請先修改**SVM**上的動態**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定為「主動」、才能繼續修改Active Directory網域。
- 如果命令成功完成、系統管理狀態會自動設為「up」。
- 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`

   如需詳細資訊、請參閱的手冊頁 `vserver cifs modify` 命令。如果您需要重新設定新網域的 DNS 、請參閱的手冊頁 `vserver dns modify` 命令。

   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
```

顯示有關TCP連線上的NetBios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.
```

管理 SMB 伺服器的命令

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`

如需詳細資訊、請參閱每個命令的手冊頁。

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

使用IPv6的需求

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。隨附 SMB 授權 "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）。

支援使用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

CIFS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

啟用SMB的IPv6（僅限叢集管理員）

監控及顯示IPv6 SMB工作階段的相關資訊

啟用**SMB**的**IPv6**（僅限叢集管理員）

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`

   如需在叢集上啟用IPv6及設定IPv6 LIF的詳細資訊、請參閱網路管理指南_。

   IPv6已啟用。可設定用於SMB存取的IPv6資料生命量。

相關資訊

監控及顯示IPv6 SMB工作階段的相關資訊

"網路管理"

停用**SMB**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。

如需在叢集上停用IPv6的詳細資訊、請參閱網路管理指南_。

相關資訊

"網路管理"

監控及顯示IPv6 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。