使用SMB管理檔案存取

ONTAP 9

NetApp
June 19, 2024

目錄

使用SMB管理檔案存取

使用本機使用者和群組進行驗證和授權

如何使用本機使用者和群組ONTAP

本機使用者與群組概念

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

- 本機使用者

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

  使用者帳戶有多種用途：

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

- 本機群組

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

  群組有多種用途：

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

- 本機網域

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

- 安全性識別碼（**SID**）

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

- * NTLM驗證*

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

- 叢集複寫資料庫（**RDB**）

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

建立本機使用者和本機群組的理由

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

您可以基於下列理由建立一或多個本機使用者帳戶：

- 您的SMB伺服器位於工作群組中、網域使用者無法使用。

  工作群組組組態需要本機使用者。

- 如果網域控制器無法使用、您希望能夠驗證並登入SMB伺服器。

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

- 您想要指派_使用者權限管理_權限給本機使用者。

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

您可以基於下列理由建立一或多個本機群組：

- 您的SMB伺服器位於工作群組中、而且網域群組無法使用。

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

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

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

相關資訊

本機使用者驗證的運作方式

支援的權限清單

本機使用者驗證的運作方式

本機使用者必須先建立已驗證的工作階段、才能存取CIFS伺服器上的資料。

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

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

- 網域部分相符

在要求存取資料時提供本機使用者認證的使用者、會在CIFS伺服器本機驗證。

- 網域部分不符

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

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

- 未指定網域部分

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

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

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

相關資訊

啟用或停用本機使用者驗證

如何建構使用者存取權杖

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

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

- 本機使用者登入

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

- 網域使用者登入

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

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

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

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

在包含本機群組的**SVM**上使用**SnapMirror**的準則

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

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

刪除**CIFS**伺服器時、本機使用者和群組會發生什麼事

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

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

CIFS伺服器管理狀態不會影響本機使用者或群組的可見度。

如何將**Microsoft**管理主控台與本機使用者和群組搭配使用

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

還原準則

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

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

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

什麼是本機權限

支援的權限清單

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

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

權限名稱	預設安全性設定	說明
SeTcbPrivilege	無	做為作業系統的一部分
SeBackupPrivilege	BUILTIN\Administrators、BUILTIN\Backup Operators	備份檔案和目錄、覆寫任何ACL
SeRestorePrivilege	BUILTIN\Administrators、BUILTIN\Backup Operators	還原檔案和目錄、覆寫任何ACL、將任何有效的使用者或群組SID設為檔案擁有者
SeTakeOwnershipPrivilege	BUILTIN\Administrators	取得檔案或其他物件的擁有權
SeSecurityPrivilege	BUILTIN\Administrators	管理稽核 這包括檢視、卸載及清除安全性記錄。
SeChangeNotifyPrivilege	BUILTIN\Administrators、BUILTIN\Backup Operators、BUILTIN\Power Users、BUILTIN\Users、 Everyone	略過周遊檢查 具有此權限的使用者不需要具有周遊（x）權限、即可周遊資料夾、符號連結或交叉路口。

相關資訊

- 指派本機權限
- 設定略過周遊檢查

指派權限

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

- 您可以將一組權限指派給所建立的群組。

  接著、您可以將擁有該使用者所擁有權限的使用者新增至群組。

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

相關資訊

- 新增權限給本機或網域使用者或群組
- 移除本機或網域使用者或群組的權限
- 重設本機或網域使用者和群組的權限

- 設定略過周遊檢查

使用**BUILTIN**群組和本機系統管理員帳戶的準則

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

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

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

- 沒有本機來賓帳戶。

相關資訊

預先定義的BUILTIN群組和預設權限

本機使用者密碼需求

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

密碼必須符合下列條件：

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

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

相關資訊

啟用或停用本機SMB使用者所需的密碼複雜度

顯示有關CIFS伺服器安全性設定的資訊

變更本機使用者帳戶密碼

預先定義的**BUILTIN**群組和預設權限

您可以將本機使用者或網域使用者的成員資格指派給ONTAP 由供應的一組預先定義

的BUILTIN群組。預先定義的群組已指派預先定義的權限。

下表說明預先定義的群組：

預先定義的**BUILTIN**群組	預設權限
`BUILTIN\Administrators`RID 544 第一次建立時、即為本機 `Administrator` 帳戶（ RID 為 500 ）會自動成為此群組的成員。當儲存虛擬機器（ SVM ）加入網域時 `domain\Domain Admins` 群組即會新增至群組。如果 SVM 離開網域、則為 `domain\Domain Admins` 群組即會從群組中移除。	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Power Users`RID 547 第一次建立時、此群組沒有任何成員。此群組成員具有下列特性： • 可建立及管理本機使用者和群組。 • 無法將自己或任何其他物件新增至 `BUILTIN\Administrators` 群組：	`SeChangeNotifyPrivilege`
`BUILTIN\Backup Operators`RID 551. 第一次建立時、此群組沒有任何成員。如果是以備份目的開啟檔案或資料夾、則此群組的成員可以覆寫其讀取和寫入權限。	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Users`RID 545 第一次建立時、此群組沒有任何成員（隱含的除外） `Authenticated Users` 特殊群組）。當 SVM 加入網域時 `domain\Domain Users` 群組隨即新增至此群組。如果 SVM 離開網域、則為 `domain\Domain Users` 群組已從此群組中移除。	`SeChangeNotifyPrivilege`
`Everyone`SID S-1-1-0 此群組包括所有使用者、包括來賓（但非匿名使用者）。這是暗示的群組、具有暗示的成員資格。	`SeChangeNotifyPrivilege`

相關資訊

使用BUILTIN群組和本機系統管理員帳戶的準則

支援的權限清單

設定略過周遊檢查

啟用或停用本機使用者和群組功能

啟用或停用本機使用者和群組功能總覽

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

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

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

相關資訊

修改本機使用者帳戶

修改本機群組

新增權限給本機或網域使用者或群組

啟用或停用本機使用者和群組

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

關於這項工作

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

步驟

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

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

3. 返回管理權限層級： `set -privilege admin`

範例

下列範例可在SVM VS1上啟用本機使用者和群組功能：

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

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

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

相關資訊

啟用或停用本機使用者驗證

啟用或停用本機使用者帳戶

啟用或停用本機使用者驗證

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

開始之前

必須在CIFS伺服器上啟用本機使用者和群組功能。

關於這項工作

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

步驟

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

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

3. 返回管理權限層級： `set -privilege admin`

範例

下列範例可在SVM VS1上啟用本機使用者驗證：

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

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

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

相關資訊

本機使用者驗證的運作方式

啟用或停用本機使用者和群組

管理本機使用者帳戶

修改本機使用者帳戶

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

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

範例

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

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

啟用或停用本機使用者帳戶

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

關於這項工作

您可以修改使用者帳戶來啟用本機使用者。

步驟

1. 執行適當的行動：

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

變更本機使用者帳戶密碼

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

步驟

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

範例

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

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

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

相關資訊

啟用或停用本機SMB使用者所需的密碼複雜度

顯示有關CIFS伺服器安全性設定的資訊

顯示本機使用者的相關資訊

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

關於這項工作

永遠不會顯示使用者密碼的相關資訊。

步驟

1. 執行下列其中一項動作：

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

您可以在執行命令時選擇其他選用參數。如需詳細資訊、請參閱手冊頁。

範例

下列範例顯示SVM VS1上所有本機使用者的相關資訊：

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

顯示本機使用者群組成員資格的相關資訊

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

關於這項工作

您可以自訂命令、僅顯示您要查看的資訊。

步驟

1. 執行下列其中一項動作：

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

範例

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

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

刪除本機使用者帳戶

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

關於這項工作

刪除本機使用者時、請謹記下列事項：

- 檔案系統不會變更。

  不會調整參照此使用者之檔案和目錄上的Windows安全性描述元。

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

步驟

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

範例

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

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


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

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

管理本機群組

修改本機群組

您可以變更現有本機群組的說明、或重新命名群組、以修改現有的本機群組。

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

如果您想要...	使用命令...
重新命名本機群組	`vserver cifs users-and-groups local-group rename -vserver vserver_name -group-name group_name -new-group-name new_group_name`

範例

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

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

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

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

顯示本機群組的相關資訊

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

步驟

1. 執行下列其中一項動作：

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

您可以在執行此命令時選擇其他選用參數。如需詳細資訊、請參閱手冊頁。

範例

下列範例顯示SVM VS1上所有本機群組的相關資訊：

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

管理本機群組成員資格

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

關於這項工作

新增成員至本機群組的準則：

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

從本機群組移除成員的準則：

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

步驟

1. 新增或移除群組中的成員。

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

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

以下範例將本機使用者「'Smb_server\sue」和網域群組「'AD_DOM\DOM_DOM_eng'」新增至SVM VS1上的本機群組「'Smb_server\engin'」：

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

以下範例將SVM VS1上本機群組「'Smb_server\sue」和「'smb_server\james'」中的本機使用者移除：

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

相關資訊

顯示本機群組成員的相關資訊

顯示本機群組成員的相關資訊

您可以顯示叢集或指定儲存虛擬機器（SVM）上所設定之本機群組的所有成員清單。在疑難排解檔案存取問題或使用者權限（權限）問題時、此資訊很有用。

步驟

1. 執行下列其中一項動作：

如果您想要顯示有關...的資訊	輸入命令...
叢集上所有本機群組的成員	`vserver cifs users-and-groups local-group show-members`
SVM上所有本機群組的成員	`vserver cifs users-and-groups local-group show-members -vserver` *`vserver_name`*

範例

下列範例顯示SVM VS1上所有本機群組成員的相關資訊：

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                    Members
--------- --------------------------- ----------------------
vs1       BUILTIN\Administrators       CIFS_SERVER\Administrator
                                       AD_DOMAIN\Domain Admins
                                       AD_DOMAIN\dom_grp1
          BUILTIN\Users                AD_DOMAIN\Domain Users
                                       AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering      CIFS_SERVER\james
```

刪除本機群組

如果不再需要本機群組來判斷與該SVM相關之資料的存取權限、或不再需要將SVM使用者權限（權限）指派給群組成員、您可以從儲存虛擬機器（SVM）中刪除該群組。

關於這項工作

刪除本機群組時、請謹記下列事項：

- 檔案系統不會變更。

  不會調整參照此群組之檔案和目錄上的Windows安全性描述元。

- 如果群組不存在、則會傳回錯誤。
- 無法刪除特殊的_Everyon__群組。
- 無法刪除內建群組、例如_BUILTIN\Administrators__BUILTIN\Users_。

步驟

1. 在 SVM 上顯示本機群組清單、藉此判斷您要刪除的本機群組名稱： `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. 刪除本機群組： `vserver cifs users-and-groups local-group delete -vserver` *`vserver_name`* `-group-name` *`group_name`*
3. 確認群組已刪除： `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

範例

下列範例會刪除與SVM VS1相關聯的本機群組「'CIFs_Server\sales'」：

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

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

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

更新本機資料庫中的網域使用者和群組名稱

您可以將網域使用者和群組新增至CIFS伺服器的本機群組。這些網域物件會在叢集的本機資料庫中登錄。如果重新命名網域物件、則必須手動更新本機資料庫。

關於這項工作

您必須指定要更新網域名稱的儲存虛擬機器（SVM）名稱。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 執行適當的行動：

如果您想要更新網域使用者和群組、以及...	使用此命令...
顯示已成功更新且無法更新的網域使用者和群組	`vserver cifs users-and-groups update-names -vserver` *vserver_name*
顯示成功更新的網域使用者和群組	`vserver cifs users-and-groups update-names -vserver` *vserver_name* `-display -failed-only false`

如果您想要更新網域使用者和群組、以及...	使用此命令...
僅顯示無法更新的網域使用者和群組	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true`
隱藏更新的所有狀態資訊	`vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true`

3. 返回管理權限層級： `set -privilege admin`

範例

下列範例會更新與儲存虛擬機器（SVM、先前稱為Vserver）VS1相關聯的網域使用者和群組名稱。對於上一次更新、需要更新的是一條相依的名稱鏈：

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

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-12345
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654322-23456
   Domain:            EXAMPLE2
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-123456
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user3
   Updated Name:      dom_user4
   Status:            Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                      to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

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

管理本機權限

新增權限給本機或網域使用者或群組

您可以新增權限來管理本機或網域使用者或群組的使用者權限。新增的權限會覆寫指派給任何這些物件的預設權限。這可讓您自訂使用者或群組擁有的權限、進而增強安全性。

開始之前

要新增權限的本機或網域使用者或群組必須已經存在。

關於這項工作

新增權限至物件會覆寫該使用者或群組的預設權限。新增權限並不會移除先前新增的權限。

新增權限給本機或網域使用者或群組時、必須謹記下列事項：

- 您可以新增一或多個權限。
- 將權限新增至網域使用者或群組時ONTAP 、可能會聯絡網域控制器來驗證網域使用者或群組。

  如果無法聯絡網域控制器、則指令可能會失敗ONTAP 。

步驟

1. 新增一或多個權限至本機或網域使用者或群組： `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. 確認所需權限已套用至物件： `vserver cifs users-and-groups privilege show -vserver _vserver_name_ -user-or-group-name _name_`

範例

以下範例將「'eTcbprivre'」和「'eTakeOwnershipprivatef'」權限新增至儲存虛擬機器（SVM、先前稱為Vserver）VS1上的使用者「'CIFs_Server\sue'」：

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege
```

移除本機或網域使用者或群組的權限

您可以移除權限、來管理本機或網域使用者或群組的使用者權限。這可讓您自訂使用者和群組擁有的最大權限、進而增強安全性。

開始之前

將從中移除權限的本機或網域使用者或群組必須已經存在。

關於這項工作

在移除本機或網域使用者或群組的權限時、您必須謹記下列事項：

- 您可以移除一或多個權限。
- 當移除網域使用者或群組的權限時、ONTAP 可能會聯絡網域控制器來驗證網域使用者或群組。

  如果無法聯絡網域控制器、則指令可能會失敗ONTAP 。

步驟

1. 移除本機或網域使用者或群組的一或多個權限： `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. 確認已從物件中移除所需的權限： `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

範例

下列範例移除儲存虛擬機器（SVM、前身為Vserver）VS1上使用者「'CIFs_Server\sue」的「'eTcbprivre'」和「'eTakeOwnershipprivatef'」權限：

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- -------------------
vs1       CIFS_SERVER\sue      -
```

重設本機或網域使用者和群組的權限

您可以重設本機或網域使用者和群組的權限。當您已修改本機或網域使用者或群組的權限、而且不再需要或需要這些修改時、此功能就很有用。

關於這項工作

重設本機或網域使用者或群組的權限、會移除該物件的任何權限項目。

步驟

1. 重設本機或網域使用者或群組的權限： `vserver cifs users-and-groups privilege reset-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

2. 確認物件上的權限已重設： `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

範例

下列範例會重設儲存虛擬機器（SVM、先前稱為Vserver）VS1上使用者「'CIFs_Server\sue」的權限。根據預設、一般使用者沒有與其帳戶相關的權限：

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

下列範例會重設群組「'BUILTIN\管理員'」的權限、有效移除權限項目：

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name       Privileges
--------- ----------------------- -------------------
vs1       BUILTIN\Administrators   SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

顯示權限置換的相關資訊

您可以顯示指派給網域或本機使用者帳戶或群組的自訂權限相關資訊。此資訊可協助您判斷是否套用所需的使用者權限。

步驟

1. 執行下列其中一項動作：

如果您想要顯示有關...的資訊	輸入此命令...
儲存虛擬機器（SVM）上所有網域和本機使用者和群組的自訂權限	`vserver cifs users-and-groups privilege show -vserver vserver_name`
自訂SVM上特定網域或本機使用者和群組的權限	`vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

您可以在執行此命令時選擇其他選用參數。如需詳細資訊、請參閱手冊頁。

範例

下列命令會顯示明確與SVM VS1的本機或網域使用者和群組相關聯的所有權限：

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name     Privileges
---------- ---------------------  ---------------
vs1        BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                   SeRestorePrivilege
vs1        CIFS_SERVER\sue         SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

設定略過周遊檢查

設定略過周遊檢查總覽

「略過周遊檢查」是一項使用者權限（也稱為_priv榮幸_）、可決定使用者是否可以周遊檔案路徑中的所有目錄、即使使用者對周遊目錄沒有權限。您應該瞭解允許或禁止略過周遊檢查時會發生什麼情況、以及如何為儲存虛擬機器（SVM）上的使用者設定略過周遊檢查。

允許或禁止略過周遊檢查時會發生什麼事

- 如果允許、當使用者嘗試存取檔案時ONTAP 、當決定是否授予或拒絕存取檔案時、不會檢查中繼目錄的周遊權限。
- 如果不允許、ONTAP 則此功能會檢查檔案路徑中所有目錄的周遊（執行）權限。

  如果任何中繼目錄沒有「'X'」（周遊權限）、ONTAP 則無法存取檔案。

設定略過周遊檢查

您可以使用ONTAP CLI或使用此使用者權限設定Active Directory群組原則、來設定略過周遊檢查。

。 `SeChangeNotifyPrivilege` 權限可控制是否允許使用者略過周遊檢查。

- 將它新增至SVM上的本機SMB使用者或群組、或新增至網域使用者或群組、可進行略過周遊檢查。
- 從SVM上的本機SMB使用者或群組或網域使用者或群組中移除此功能、將不允許略過周遊檢查。

根據預設、SVM上的下列BUILTIN群組有權略過周遊檢查：

- `BUILTIN\Administrators`
- `BUILTIN\Power Users`
- `BUILTIN\Backup Operators`
- `BUILTIN\Users`
- `Everyone`

如果您不想讓其中一個群組的成員略過周遊檢查、則必須從群組中移除此權限。

使用CLI在SVM上設定本機SMB使用者和群組的略過周遊檢查時、必須謹記下列事項：

- 如果您想要允許自訂本機或網域群組的成員略過周遊檢查，則必須新增 `SeChangeNotifyPrivilege` 權限給該群組。
- 如果您想要允許個別本機或網域使用者略過周遊檢查，而該使用者不是具有該權限的群組成員，則可以新增 `SeChangeNotifyPrivilege` 該使用者帳戶的權限。
- 您可以移除來停用本機或網域使用者或群組的略過周遊檢查 `SeChangeNotifyPrivilege` 隨時享有特權。

> 若要停用特定本機或網域使用者或群組的略過傳輸檢查、您也必須移除 `SeChangeNotifyPrivilege` 的權限 `Everyone` 群組：

相關資訊

允許使用者或群組略過目錄周遊檢查

不允許使用者或群組繞過目錄周遊檢查

設定磁碟區上SMB檔案名稱轉譯的字元對應

建立SMB共用存取控制清單

使用儲存層級存取保護來保護檔案存取安全

支援的權限清單

新增權限給本機或網域使用者或群組

允許使用者或群組略過目錄周遊檢查

如果您希望使用者能夠周遊檔案路徑中的所有目錄、即使使用者對周遊目錄沒有權限、您也可以新增 `SeChangeNotifyPrivilege` 本機 SMB 使用者或儲存虛擬機器上群組的權限（ SVM ）。根據預設、使用者可以略過目錄周遊檢查。

開始之前

- SVM上必須有SMB伺服器。
- 必須啟用本機使用者和群組SMB伺服器選項。
- 本機或網域使用者或群組 `SeChangeNotifyPrivilege` 新增權限必須已存在。

關於這項工作

將權限新增至網域使用者或群組時ONTAP 、可能會聯絡網域控制器來驗證網域使用者或群組。如果無法聯絡網域控制器、則指令可能會失敗ONTAP 。

步驟

1. 新增以啟用略過周遊檢查 `SeChangeNotifyPrivilege` 本機或網域使用者或群組的權限： `vserver cifs users-and-groups privilege add-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

   的值 `-user-or-group-name` 參數是本機使用者或群組、或是網域使用者或群組。

2. 確認指定的使用者或群組已啟用略過周遊檢查： `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

範例

下列命令可讓屬於 “example\eng” 群組的使用者透過新增來略過目錄周遊檢查 `SeChangeNotifyPrivilege` 群組的權限：

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege
```

相關資訊

禁止使用者或群組繞過目錄周遊檢查

不允許使用者或群組繞過目錄周遊檢查

如果您不希望使用者周遊檔案路徑中的所有目錄、因為使用者對周遊目錄沒有權限、您可以移除 `SeChangeNotifyPrivilege` 本機 SMB 使用者或儲存虛擬機器上群組的權限（ SVM ）。

開始之前

將從中移除權限的本機或網域使用者或群組必須已經存在。

關於這項工作

當移除網域使用者或群組的權限時、ONTAP 可能會聯絡網域控制器來驗證網域使用者或群組。如果無法聯絡網域控制器、則指令可能會失敗ONTAP 。

步驟

1. 不允許略過周遊檢查： `vserver cifs users-and-groups privilege remove-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

   命令會移除 `SeChangeNotifyPrivilege` 本機或網域使用者或群組的權限、您可以使用的值來指定 `-user-or-group-name name` 參數。

2. 確認指定的使用者或群組已停用略過周遊檢查： `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

範例

下列命令會禁止屬於「'example\eng'」群組的使用者略過目錄周遊檢查：

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ----------------------
vs1       EXAMPLE\eng          SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ----------------------
vs1       EXAMPLE\eng          -
```

相關資訊

允許使用者或群組略過目錄周遊檢查

顯示檔案安全性和稽核原則的相關資訊

顯示檔案安全性與稽核原則總覽的相關資訊

您可以在儲存虛擬機器（SVM）上的磁碟區內、顯示有關檔案與目錄安全性的資訊。您可以顯示FlexVol 有關在功能區上稽核原則的資訊。如果已設定、您可以在FlexVol 下列項目上顯示儲存層級存取保護和動態存取控制安全性設定的相關資訊：

顯示檔案安全性的相關資訊

您可以使用FlexVol 下列安全性樣式、顯示套用至Volume和qtree（適用於哪些人）中所含資料的檔案安全性相關資訊：

- NTFS
- UNIX

- 混合

顯示稽核原則的相關資訊

您可以透過FlexVol 下列NAS傳輸協定、顯示稽核原則的相關資訊、以稽核在支援功能上執行的存取事件：

- SMB（所有版本）
- NFSv4.x

顯示儲存層級存取保護（**slag**）安全性的相關資訊

儲存層級的存取保護安全功能可套用FlexVol 至下列安全樣式的物件：

- NTFS
- 混合
- UNIX（如果CIFS伺服器是在包含該磁碟區的SVM上設定）

顯示動態存取控制（**DAC**）安全性的相關資訊

動態存取控制安全功能FlexVol 可套用至包含下列安全樣式的物件：

- NTFS
- 混合（如果物件具有NTFS有效安全性）

相關資訊

使用儲存層級存取保護來保護檔案存取安全

顯示儲存層級存取保護的相關資訊

顯示**NTFS**安全型磁碟區上檔案安全性的相關資訊

您可以在NTFS安全型磁碟區上顯示檔案與目錄安全性的相關資訊、包括安全型態與有效的安全性樣式、套用的權限、以及DOS屬性的相關資訊。您可以使用結果來驗證安全性組態、或疑難排解檔案存取問題。

關於這項工作

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

- 由於NTFS安全型磁碟區和qtree在決定檔案存取權限時僅使用NTFS檔案權限、而Windows使用者和群組、因此UNIX相關的輸出欄位會包含僅供顯示的UNIX檔案權限資訊。
- 將顯示具有NTFS安全性的檔案和資料夾的ACL輸出。
- 由於儲存層級的存取保護安全性可在磁碟區根目錄或qtree上設定、因此設定儲存層級存取保護的磁碟區或qtree路徑輸出可能會同時顯示一般檔案ACL和儲存層級的存取保護ACL。
- 如果已針對指定的檔案或目錄路徑設定動態存取控制、則輸出也會顯示動態存取控制ACE的相關資訊。

步驟

1. 以所需的詳細資料層級顯示檔案和目錄安全性設定：

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

範例

下列範例顯示有關路徑的安全性資訊 `/vol4` 在 SVM VS1 中：

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                                Vserver: vs1
                              File Path: /vol4
                      File Inode Number: 64
                         Security Style: ntfs
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                         Unix Mode Bits: 777
                 Unix Mode Bits in Text: rwxrwxrwx
                                   ACLs: NTFS Security Descriptor
                                         Control:0x8004
                                         Owner:BUILTIN\Administrators
                                         Group:BUILTIN\Administrators
                                         DACL - ACEs
                                         ALLOW-Everyone-0x1f01ff
                                         ALLOW-Everyone-0x10000000-
OI|CI|IO
```

以下範例顯示有關路徑的安全性資訊、並提供有關路徑的擴充遮罩 `/data/engineering` 在 SVM VS1 中：

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true

                Vserver: vs1
              File Path: /data/engineering
```

```
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
          Unix User Id: 0
         Unix Group Id: 0
        Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
Generic Execute
```

```
                           ...0 .... .... .... .... .... .... .... =
Generic All
                           .... ...0 .... .... .... .... .... .... =
System Security
                           .... .... ...1 .... .... .... .... .... =
Synchronize
                           .... .... .... 1... .... .... .... .... =
Write Owner
                           .... .... .... .1.. .... .... .... .... =
Write DAC
                           .... .... .... ..1. .... .... .... .... =
Read Control
                           .... .... .... ...1 .... .... .... .... =
Delete
                           .... .... .... .... .... ...1 .... .... =
Write Attributes
                           .... .... .... .... .... .... 1... .... =
Read Attributes
                           .... .... .... .... .... .... .1.. .... =
Delete Child
                           .... .... .... .... .... .... ..1. .... =
Execute
                           .... .... .... .... .... .... ...1 .... =
Write EA
                           .... .... .... .... .... .... .... 1... =
Read EA
                           .... .... .... .... .... .... .... .1.. =
Append
                           .... .... .... .... .... .... .... ..1. =
Write
                           .... .... .... .... .... .... .... ...1 =
Read

                         ALLOW-Everyone-0x10000000-OI|CI|IO
                           0... .... .... .... .... .... .... .... =
Generic Read
                           .0.. .... .... .... .... .... .... .... =
Generic Write
                           ..0. .... .... .... .... .... .... .... =
Generic Execute
                           ...1 .... .... .... .... .... .... .... =
Generic All
                           .... ...0 .... .... .... .... .... .... =
System Security
                           .... .... ...0 .... .... .... .... .... =
Synchronize
```

```
                                .... .... .... 0... .... .... .... .... =
Write Owner
                                .... .... .... .0.. .... .... .... .... =
Write DAC
                                .... .... .... ..0. .... .... .... .... =
Read Control
                                .... .... .... ...0 .... .... .... .... =
Delete
                                .... .... .... .... .... ...0 .... .... =
Write Attributes
                                .... .... .... .... .... .... 0... .... =
Read Attributes
                                .... .... .... .... .... .... .0.. .... =
Delete Child
                                .... .... .... .... .... .... ..0. .... =
Execute
                                .... .... .... .... .... .... ...0 .... =
Write EA
                                .... .... .... .... .... .... .... 0... =
Read EA
                                .... .... .... .... .... .... .... .0.. =
Append
                                .... .... .... .... .... .... .... ..0. =
Write
                                .... .... .... .... .... .... .... ...0 =
Read
```

以下範例顯示具有路徑之磁碟區的安全性資訊、包括儲存層級 Access Guard 安全性資訊 `/datavol1` 在 SVM VS1 中：

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

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


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

相關資訊

在混合式安全型磁碟區上顯示檔案安全性的相關資訊

顯示UNIX安全型磁碟區上的檔案安全資訊

顯示混合式安全型磁碟區的檔案安全資訊

您可以在混合式安全型磁碟區上顯示檔案與目錄安全性的相關資訊、包括安全型態與有效的安全性樣式、套用的權限、以及UNIX擁有者與群組的相關資訊。您可以使用結果來驗證安全性組態、或疑難排解檔案存取問題。

關於這項工作

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

- 混合式安全型磁碟區和qtree可包含使用UNIX檔案權限的部分檔案和資料夾、包括模式位元或NFSv4 ACL、以及使用NTFS檔案權限的部分檔案和目錄。
- 混合式安全型磁碟區的最上層可能具有UNIX或NTFS的有效安全性。
- ACL輸出只會針對具有NTFS或NFSv4安全性的檔案和資料夾顯示。

  對於使用UNIX安全性的檔案和目錄、如果只套用模式位元權限（無NFSv4 ACL）、則此欄位為空白。
- ACL輸出中的擁有者和群組輸出欄位僅適用於NTFS安全性描述元。
- 因為即使Volume root或qtree的有效安全樣式為UNIX、也可以在混合式安全型Volume或qtree上設定儲存層級的存取保護安全性、 已設定儲存層級存取保護的Volume或qtree路徑輸出、可能會同時顯示UNIX檔案權限和儲存層級存取保護ACL。
- 如果在命令中輸入的路徑是使用NTFS有效安全性的資料、則當動態存取控制是針對指定的檔案或目錄路徑設定時、輸出也會顯示動態存取控制ACE的相關資訊。

步驟

1. 以所需的詳細資料層級顯示檔案和目錄安全性設定：

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

範例

下列範例顯示有關路徑的安全性資訊 `/projects` 在 SVM VS1 中以擴充遮罩形式呈現。這種混合式安全型路徑具有UNIX有效的安全性。

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

                Vserver: vs1
              File Path: /projects
      File Inode Number: 78
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

下列範例顯示有關路徑的安全性資訊 `/data` 在 SVM VS1 中。這種混合式安全型路徑具有NTFS有效安全性。

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

                                Vserver: vs1
                              File Path: /data
                      File Inode Number: 544
                         Security Style: mixed
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                         Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                            ALLOW-Everyone-0x1f01ff
                                            ALLOW-Everyone-0x10000000-
OI|CI|IO
```

以下範例顯示路徑中有關 Volume 的安全性資訊 `/datavol5` 在 SVM VS1 中。這種混合式安全型磁碟區的最上層具有UNIX有效的安全性。Volume具有儲存層級的存取保護安全性。

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

相關資訊

在NTFS安全型磁碟區上顯示檔案安全性的相關資訊

顯示UNIX安全型磁碟區上的檔案安全資訊

顯示**UNIX**安全型磁碟區上的檔案安全資訊

您可以顯示UNIX安全型磁碟區上的檔案與目錄安全性相關資訊、包括安全性樣式與有效的安全性樣式、套用的權限、以及UNIX擁有者與群組的相關資訊。您可以使用結果來驗證安

全性組態、或疑難排解檔案存取問題。

關於這項工作

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

- UNIX安全型磁碟區和qtree在決定檔案存取權限時、只會使用UNIX檔案權限（模式位元或NFSv4 ACL）。
- ACL輸出只會針對具有NFSv4安全性的檔案和資料夾顯示。

  對於使用UNIX安全性的檔案和目錄、如果只套用模式位元權限（無NFSv4 ACL）、則此欄位為空白。

- 如果使用NFSv4安全性描述元、則不會套用ACL輸出中的擁有者和群組輸出欄位。

  它們只對NTFS安全描述元有意義。

- 由於如果在 SVM 上設定 CIFS 伺服器、則 UNIX 磁碟區或 qtree 上支援儲存層級存取保護安全性、因此輸出可能包含適用於中指定之磁碟區或 qtree 的儲存層級存取保護安全性相關資訊 `-path` 參數。

步驟

1. 以所需的詳細資料層級顯示檔案和目錄安全性設定：

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

範例

下列範例顯示有關路徑的安全性資訊 `/home` 在 SVM VS1 中：

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 1
                         Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

下列範例顯示有關路徑的安全性資訊 `/home` 在 SVM VS1 的擴充遮罩形式中：

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: 0x10
                    ...0 .... .... .... = Offline
                    .... ..0. .... .... = Sparse
                    .... .... 0... .... = Normal
                    .... .... ..0. .... = Archive
                    .... .... ...1 .... = Directory
                    .... .... .... .0.. = System
                    .... .... .... ..0. = Hidden
                    .... .... .... ...0 = Read Only
                           Unix User Id: 0
                          Unix Group Id: 1
                         Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

相關資訊

[在NTFS安全型磁碟區上顯示檔案安全性的相關資訊]

[在混合式安全型磁碟區上顯示檔案安全性的相關資訊]

使用**FlexVol CLI**在整個過程中顯示有關**NTFS**稽核原則的資訊

您可以在FlexVol 功能區上顯示NTFS稽核原則的相關資訊、包括安全樣式和有效的安全樣式、套用的權限、以及系統存取控制清單的相關資訊。您可以使用結果來驗證安全性組態或疑難排解稽核問題。

關於這項工作

您必須提供儲存虛擬機器（SVM）的名稱、以及要顯示其稽核資訊的檔案或資料夾路徑。您可以以摘要形式或詳細清單來顯示輸出。

- NTFS安全型磁碟區和qtree僅使用NTFS系統存取控制清單（SACL）來執行稽核原則。
- 在具有NTFS有效安全性的混合式安全型磁碟區中、檔案和資料夾可以套用NTFS稽核原則。

  混合式安全型磁碟區和qtree可包含使用UNIX檔案權限的部分檔案和目錄、包括模式位元或NFSv4 ACL、以及使用NTFS檔案權限的部分檔案和目錄。

- 混合式安全型磁碟區的最上層可能具有UNIX或NTFS有效安全性、而且可能包含或不包含NTFS SACL。
- 因為即使Volume root或qtree的有效安全樣式為UNIX、也可以在混合式安全型Volume或qtree上設定儲存層級的存取保護安全性、 已設定儲存層級存取保護的Volume或qtree路徑輸出、可能會同時顯示一般檔案和資料夾NFSv4 SACL、以及儲存層級存取保護NTFS SACL。
- 如果在命令中輸入的路徑是使用NTFS有效安全性的資料、則輸出也會顯示動態存取控制ACE的相關資訊（如果已針對指定的檔案或目錄路徑設定動態存取控制）。
- 在顯示具有NTFS有效安全性的檔案和資料夾的安全性資訊時、UNIX相關的輸出欄位會包含僅供顯示的UNIX檔案權限資訊。

  NTFS安全型檔案和資料夾在決定檔案存取權限時、僅使用NTFS檔案權限、Windows使用者和群組。

- ACL輸出只會針對具有NTFS或NFSv4安全性的檔案和資料夾顯示。

  對於使用UNIX安全性的檔案和資料夾而言、此欄位為空白、只套用模式位元權限（無NFSv4 ACL）。

- ACL輸出中的擁有者和群組輸出欄位僅適用於NTFS安全性描述元。

步驟

1. 以所需的詳細資料層級顯示檔案和目錄稽核原則設定：

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

範例

下列範例顯示路徑的稽核原則資訊 `/corp` 在 SVM VS1 中。路徑具有NTFS有效安全性。NTFS安全性描述元包含成功和成功/失敗SACL項目。

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

下列範例顯示路徑的稽核原則資訊 `/datavol1` 在 SVM VS1 中。路徑包含一般檔案和資料夾SACL、以及儲存層級存取保護SACL。

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

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

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

使用**FlexVol CLI**顯示有關**NFSv4**稽核原則的資訊

您可以FlexVol 使用ONTAP CLI在S什麼 磁碟區上顯示NFSv4稽核原則的相關資訊、包括安全樣式和有效的安全樣式、套用的權限、以及系統存取控制清單（SACL）的相關資訊。

您可以使用結果來驗證安全性組態或疑難排解稽核問題。

關於這項工作

您必須提供儲存虛擬機器（SVM）的名稱、以及要顯示其稽核資訊的檔案或目錄路徑。您可以以摘要形式或詳細清單來顯示輸出。

- UNIX安全型磁碟區和qtree僅使用NFSv4 SACL來執行稽核原則。
- 混合式安全型磁碟區中的檔案和目錄、若為UNIX安全型態、則可套用NFSv4稽核原則。

  混合式安全型磁碟區和qtree可包含使用UNIX檔案權限的部分檔案和目錄、包括模式位元或NFSv4 ACL、以及使用NTFS檔案權限的部分檔案和目錄。

- 混合式安全型磁碟區的最上層可能具有UNIX或NTFS的有效安全性、而且可能包含或不包含NFSv4 SACL。
- ACL輸出只會針對具有NTFS或NFSv4安全性的檔案和資料夾顯示。

  對於使用UNIX安全性的檔案和資料夾而言、此欄位為空白、只套用模式位元權限（無NFSv4 ACL）。

- ACL輸出中的擁有者和群組輸出欄位僅適用於NTFS安全性描述元。
- 因為即使Volume root或qtree的有效安全樣式為UNIX、也可以在混合式安全型Volume或qtree上設定儲存層級的存取保護安全性、 已設定儲存層級存取保護的Volume或qtree路徑輸出、可能會同時顯示一般NFSv4檔案和目錄SACL、以及儲存層級存取保護NTFS SACL。
- 由於如果在 SVM 上設定 CIFS 伺服器、則 UNIX 磁碟區或 qtree 上支援儲存層級存取保護安全性、因此輸出可能包含適用於中指定之磁碟區或 qtree 的儲存層級存取保護安全性相關資訊 `-path` 參數。

步驟

1. 以所需的詳細資料層級顯示檔案和目錄安全性設定：

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

範例

下列範例顯示有關路徑的安全性資訊 `/lab` 在 SVM VS1 中。此UNIX安全型路徑具有NFSv4 SACL。

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

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

顯示檔案安全性與稽核原則相關資訊的方法

您可以使用萬用字元（*）來顯示特定路徑或根磁碟區下所有檔案和目錄的檔案安全性和稽核原則相關資訊。

萬用字元（）可做為指定目錄路徑的最後一個子元件、您可以在該子元件下方顯示所有檔案和目錄的資訊。如果您想要顯示名為「」的特定檔案或目錄資訊、則必須在雙引號（「'」）內提供完整路徑。

範例

下列含有萬用字元的命令會顯示路徑下方所有檔案和目錄的相關資訊 `/1/` SVM VS1 ：

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

下列命令會顯示路徑下名為「*」的檔案資訊 `/vol1/a` SVM VS1 的路徑會以雙引號（""）括住。

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                 Vserver: vs1
               File Path: "/vol1/a/*"
          Security Style: mixed
         Effective Style: unix
          DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
            Unix User Id: 1002
           Unix Group Id: 65533
          Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

使用CLI管理SVM上的NTFS檔案安全性、NTFS稽核原則及儲存層級存取保護

使用CLI總覽管理SVM上的NTFS檔案安全性、NTFS稽核原則及儲存層級存取保護

您可以使用CLI管理儲存虛擬機器（SVM）上的NTFS檔案安全性、NTFS稽核原則及儲存層級存取保護。

您可以從SMB用戶端或使用CLI來管理NTFS檔案安全性和稽核原則。不過、使用CLI來設定檔案安全性和稽核原則、就不需要使用遠端用戶端來管理檔案安全性。使用CLI可大幅縮短使用單一命令在許多檔案和資料夾上套用安全性所需的時間。

您可以設定儲存層級的存取防護、ONTAP 這是由SVM Volume套用的另一層安全防護。儲存層級存取保護適用於從所有NAS傳輸協定存取至套用儲存層級存取保護的儲存物件。

儲存層級的存取保護只能從ONTAP 整套CLI進行設定和管理。您無法從SMB用戶端管理儲存層級的存取保護設定。此外、如果您從NFS或SMB用戶端檢視檔案或目錄上的安全性設定、就不會看到儲存層級的存取保護安全性。即使是系統（Windows或UNIX）管理員、也無法從用戶端撤銷儲存層級的存取保護安全性。因此、儲存層級的存取保護功能可為資料存取提供額外的安全層級、並由儲存管理員獨立設定及管理。

即使儲存層級存取保護僅支援NTFS存取權限、ONTAP 但如果UNIX使用者對應至擁有該磁碟區的SVM上的Windows使用者、則可在套用Storage層級存取保護的磁碟區上執行安全性檢查、以透過NFS存取資料。

NTFS安全型磁碟區

NTFS安全型磁碟區和qtree中包含的所有檔案和資料夾都具有NTFS有效安全性。您可以使用 `vserver security file-directory` 命令系列可在 NTFS 安全樣式磁碟區上實作下列類型的安全性：

- 磁碟區中所含檔案和資料夾的檔案權限和稽核原則
- 磁碟區上的儲存層級存取保護安全性

混合式安全型磁碟區

混合式安全型磁碟區和qtree可包含一些具有UNIX有效安全性的檔案和資料夾、並使用UNIX檔案權限、包括模式位元或NFSv4.x ACL和NFSv4.x稽核原則、以及某些具有NTFS有效安全性、並使用NTFS檔案權限和稽核原則的檔案和資料夾。您可以使用 `vserver security file-directory` 命令系列可將下列類型的安全性套用至混合式安全型資料：

- 在混合磁碟區或qtree中、使用NTFS有效安全型態的檔案和資料夾的檔案權限和稽核原則
- 儲存層級的存取保護功能、可用於NTFS和UNIX有效的安全型態磁碟區

UNIX 安全型磁碟區

UNIX安全型磁碟區和qtree包含具有UNIX有效安全性的檔案和資料夾（模式位元或NFSv4.x ACL）。如果您想要使用、請務必謹記下列事項 `vserver security file-directory` 在 UNIX 安全型磁碟區上實作安全功能的命令系列：

- 。 `vserver security file-directory` 命令系列無法用於管理 UNIX 安全性樣式磁碟區和 qtree 上的 UNIX 檔案安全性和稽核原則。
- 您可以使用 `vserver security file-directory` 命令系列可在 UNIX 安全性型磁碟區上設定儲存層級存取保護、前提是目標磁碟區的 SVM 包含 CIFS 伺服器。

相關資訊

顯示檔案安全性和稽核原則的相關資訊

使用CLI在NTFS檔案和資料夾上設定及套用檔案安全性

使用CLI設定稽核原則並套用至NTFS檔案和資料夾

使用儲存層級存取保護來保護檔案存取安全

使用**CLI**設定檔案和資料夾安全性的使用案例

由於您可以在本機套用及管理檔案與資料夾安全性、而無需遠端用戶端介入、因此您可以大幅縮短設定大量檔案或資料夾的大量安全性所需的時間。

在下列使用案例中、您可以使用CLI設定檔案和資料夾的安全性：

- 在大型企業環境中儲存檔案、例如在主目錄中儲存檔案
- 資料移轉
- Windows網域變更
- 跨NTFS檔案系統的檔案安全性與稽核原則標準化

使用**CLI**設定檔案和資料夾安全性時的限制

使用CLI設定檔案和資料夾安全性時、您必須注意特定限制。

- 。 `vserver security file-directory` Command Family 不支援設定 NFSv4 ACL 。

  您只能將NTFS安全性描述元套用至NTFS檔案和資料夾。

如何使用安全性描述元來套用檔案和資料夾安全性

安全性描述元包含存取控制清單、可決定使用者可對檔案和資料夾執行的動作、以及使用者存取檔案和資料夾時所稽核的項目。

- 權限

  物件擁有者允許或拒絕權限、並決定物件（使用者、群組或電腦物件）可對指定的檔案或資料夾執行哪些動作。

- 安全性描述元

  安全性描述元是包含安全性資訊的資料結構、可定義與檔案或資料夾相關的權限。

- 存取控制清單（**ACL**）

  存取控制清單是安全性描述元中所包含的清單、其中包含使用者、群組或電腦物件可在套用安全性描述元的檔案或資料夾上執行哪些動作的相關資訊。安全性描述元可包含下列兩種ACL：

  - 判別存取控制清單（DACL）
  - 系統存取控制清單（SACL）

- 任意存取控制清單（**DACL**）

  DACL包含使用者、群組和電腦物件的「小島嶼」清單、這些使用者、群組和電腦物件均可存取或拒絕存取檔案或資料夾上的動作。DACL包含零個以上的存取控制項目（ACE）。

- 系統存取控制清單（**SACL**）

  SACL包含已記錄成功或失敗稽核事件之使用者、群組及電腦物件的「小島嶼」清單。SACL包含零個以上的存取控制項目（ACE）。

- 存取控制項目（**ACE**）

  ACE是DACL或SACL中的個別項目：

- DACL存取控制項目會指定特定使用者、群組或電腦物件所允許或拒絕的存取權限。
- SACL存取控制項目會指定在稽核特定使用者、群組或電腦物件執行的指定動作時、要記錄的成功或失敗事件。

- 權限繼承

  權限繼承說明如何將安全性描述元中定義的權限、從父物件傳播到物件。子物件只會繼承可繼承的權限。在父物件上設定權限時、您可以決定資料夾、子資料夾和檔案是否可以使用「套用至」來繼承它們 `this-folder`、 `sub-folders`和「檔案」。

相關資訊

"SMB與NFS稽核與安全性追蹤"

使用CLI設定及套用稽核原則至NTFS檔案和資料夾

套用在**SVM**災難恢復目的地上使用本機使用者或群組的檔案目錄原則準則

如果您的檔案目錄原則組態在安全性描述元、DACL或SACL項目中使用本機使用者或群組、則在ID捨棄組態中的儲存虛擬機器（SVM）災難恢復目的地上套用檔案目錄原則之前、必須謹記一些準則。

您可以為SVM設定災難恢復組態、讓來源叢集上的來源SVM將資料和組態從來源SVM複寫到目的地叢集上的目的地SVM。

您可以設定兩種SVM災難恢復類型之一：

- 身分識別保留

  有了這項組態、SVM和CIFS伺服器的身分識別就會保留下來。

- 身分識別已捨棄

  使用此組態時、SVM和CIFS伺服器的身分識別將不會保留。在此案例中、目的地SVM上的SVM和CIFS伺服器名稱與來源SVM上的SVM和CIFS伺服器名稱不同。

身分識別捨棄組態的準則

在身分識別捨棄組態中、對於包含本機使用者、群組和權限組態的SVM來源、必須變更本機網域名稱（本機CIFS伺服器名稱）、以符合SVM目的地上的CIFS伺服器名稱。例如、如果來源SVM名稱為「'VS1'」、CIFS伺服器名稱為「'CIFS1'」、目的地SVM名稱為「'VS1_DST'」、CIFS伺服器名稱為「'CIFS1_DST'」、則本機使用者的本機網域名稱會自動變更為「CIFS1\user1'上的Cdst_Dst：」

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1          CIFS1\Administrator                     Built-in
administrator account
vs1          CIFS1\user1              -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1_dst      CIFS1_DST\Administrator                 Built-in
administrator account
vs1_dst      CIFS1_DST\user1          -              -
```

雖然本機使用者和群組資料庫中的本機使用者和群組名稱會自動變更、但檔案目錄原則組態中的本機使用者或群組名稱不會自動變更（使用在 CLI 上設定的原則） `vserver security file-directory` Command Family ）。

例如、如果您已設定 DACL 項目、其中會顯示「 'VS1' 」 `-account` 參數設為「 'CIFS1\user1' 」、目的地 SVM 上的設定不會自動變更、以反映目的地的 CIFS 伺服器名稱。

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

您必須使用 `vserver security file-directory modify` 手動將 CIFS 伺服器名稱變更為目的地 CIFS 伺服器名稱的命令。

包含帳戶參數的檔案目錄原則組態元件

有三個檔案目錄原則組態元件可以使用參數設定、這些設定可以包含本機使用者或群組：

- 安全性描述元

  您可以選擇性地指定安全性描述元的擁有者和安全性描述元擁有者的主要群組。如果安全性描述元使用本機使用者或群組做為擁有者和主要群組項目、則必須修改安全性描述元、才能在帳戶名稱中使用目的地SVM。您可以使用 `vserver security file-directory ntfs modify` 命令以對帳戶名稱進行任何必要的變更。

- DACL項目

  每個DACL項目都必須與一個帳戶相關聯。您必須修改任何使用本機使用者或群組帳戶的DACL、才能使用目的地SVM名稱。由於您無法修改現有DACL項目的帳戶名稱、因此您必須從安全性描述元中移除任何具有本機使用者或群組的DACL項目、以修正的目的地帳戶名稱建立新的DACL項目、並將這些新的DACL項目與適當的安全性描述元建立關聯。

- SACL 項目

  每個SACL項目都必須與帳戶建立關聯。您必須修改任何使用本機使用者或群組帳戶的SACL、才能使用目的地SVM名稱。由於您無法修改現有SACL項目的帳戶名稱、因此您必須從安全性描述元中移除具有本機使用者或群組的任何SACL項目、以修正的目的地帳戶名稱建立新的SACL項目、並將這些新的SACL項目與適當的安全性描述元建立關聯。

套用原則之前、您必須對檔案目錄原則組態中使用的本機使用者或群組進行任何必要的變更、否則套用工作會失敗。

使用**CLI**在**NTFS**檔案和資料夾上設定及套用檔案安全性

建立**NTFS**安全性描述元

建立NTFS安全性描述元（檔案安全性原則）是設定NTFS存取控制清單（ACL）並套用至儲存虛擬機器（SVM）內的檔案和資料夾的第一步。您可以將安全性描述元與原則工作中的檔案或資料夾路徑建立關聯。

關於這項工作

您可以針對位於NTFS安全型磁碟區內的檔案和資料夾、或是位於混合式安全型磁碟區上的檔案和資料夾、建立NTFS安全性描述元。

根據預設、建立安全性描述元時、會將四個判別存取控制清單（DACL）存取控制項目（ACE）新增至該安全性描述元。四個預設的ACE如下所示：

物件	存取類型	存取權限	權限的套用位置
內建\系統管理員	允許	完全控制	此資料夾、子資料夾、檔案

物件	存取類型	存取權限	權限的套用位置
內建\使用者	允許	完全控制	此資料夾、子資料夾、檔案
建立者擁有者	允許	完全控制	此資料夾、子資料夾、檔案
NT AUTHORITY\系統	允許	完全控制	此資料夾、子資料夾、檔案

您可以使用下列選用參數來自訂安全性描述元組態：

- 安全性描述元的擁有者
- 擁有者的主要群組
- 原始控制旗標

儲存層級存取保護會忽略任何選用參數的值。如需詳細資訊、請參閱手冊頁。

將 **NTFS DACL** 存取控制項目新增至 **NTFS** 安全性描述元

將DACL（判別存取控制清單）存取控制項目（ACE）新增至NTFS安全性描述元、是設定及套用NTFS ACL至檔案或資料夾的第二步驟。每個項目都會識別允許或拒絕存取的物件、並定義物件可以或無法對ACE中定義的檔案或資料夾執行的操作。

關於這項工作

您可以將一或多個 ACE 新增至安全性描述元的 DACL 。

如果安全性描述元包含具有現有 ACE 的 DACL 、則命令會將新的 ACE 新增至 DACL 。如果安全性描述元不包含DACL、則命令會建立DACL並新增新的ACE。

您可以選擇自訂 DACL 項目、方法是指定要允許或拒絕中指定之帳戶的權限 `-account` 參數。有三種互不相容的方法可以指定權限：

- 權利
- 進階權限
- 原始權限（進階權限）

如果您未指定 DACL 項目的權限、則預設會將權限設定為 `Full Control`。

您可以指定如何套用繼承、以選擇性地自訂DACL項目。

儲存層級存取保護會忽略任何選用參數的值。如需詳細資訊、請參閱手冊頁。

步驟

1. 將 DACL 項目新增至安全性描述元： `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account`

```
name_or_SIDoptional_parameters

vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
-account domain\joe -rights full-control -apply-to this-folder -vserver vs1
```

2. 驗證 DACL 項目是否正確：`vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
-access-type deny -account domain\joe
```

```
                Vserver: vs1
      Security Descriptor Name: sd1
                Allow or Deny: deny
           Account Name or SID: DOMAIN\joe
                 Access Rights: full-control
        Advanced Access Rights: -
                     Apply To: this-folder
                 Access Rights: full-control
```

建立安全性原則

為SVM建立檔案安全性原則、是設定及套用ACL至檔案或資料夾的第三個步驟。原則可做為各種工作的容器、其中每項工作都是可套用至檔案或資料夾的單一項目。您可以稍後將工作新增至安全性原則。

關於這項工作

您新增至安全性原則的工作包含NTFS安全性描述元與檔案或資料夾路徑之間的關聯。因此、您應該將安全性原則與每個SVM建立關聯（包含NTFS安全型磁碟區或混合式安全型磁碟區）。

步驟

1. 建立安全性原則：`vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

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

2. 驗證安全性原則：`vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
  ------------     --------------
      vs1              policy1
```

新增工作至安全性原則

建立原則工作並將其新增至安全性原則、是設定及套用ACL至SVM中的檔案或資料夾的第四個步驟。當您建立原則工作時、會將工作與安全性原則建立關聯。您可以將一或多個工作項目新增至安全性原則。

關於這項工作

安全性原則是工作的容器。工作指的是單一作業、可透過安全性原則對具有NTFS或混合式安全性的檔案或資料夾（或是在設定儲存層級存取保護時、對磁碟區物件執行）。

工作有兩種類型：

- 檔案與目錄工作

  用於指定將安全性描述元套用至指定檔案和資料夾的工作。透過檔案和目錄工作所套用的ACL、可透過SMB用戶端或ONTAP CLI進行管理。

- 儲存層級的存取保護工作

  用於指定將儲存層級存取保護安全性描述元套用至指定磁碟區的工作。透過儲存層級存取保護工作套用的ACL只能透過ONTAP CLI進行管理。

工作包含檔案（或資料夾）或一組檔案（或資料夾）的安全性組態定義。原則中的每項工作都會以路徑唯一識別。在單一原則中、每個路徑只能有一項工作。原則不能有重複的工作項目。

新增工作至原則的準則：

- 每個原則最多可有10、000個工作項目。
- 原則可以包含一或多個工作。

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

- 儲存層級的存取保護用於限制權限。

  它永遠不會提供額外的存取權限。

將工作新增至安全性原則時、您必須指定下列四個必要參數：

- SVM名稱
- 原則名稱
- 路徑
- 與路徑相關聯的安全性描述元

您可以使用下列選用參數來自訂安全性描述元組態：

- 安全類型
- 傳播模式

- 索引位置
- 存取控制類型

儲存層級存取保護會忽略任何選用參數的值。如需詳細資訊、請參閱手冊頁。

步驟

1. 將具有相關安全性描述元的工作新增至安全性原則： `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` 為的預設值 `-access-control` 參數。設定檔案和目錄存取工作時、可選擇指定存取控制類型。

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
   ```

2. 驗證原則工作組態： `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

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

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

套用安全性原則

將檔案安全性原則套用到SVM是建立NTFS ACL並套用到檔案或資料夾的最後步驟。

關於這項工作

您可以將安全性原則中定義的安全性設定套用至FlexVol 駐留在各處的NTFS檔案和資料夾（NTFS或混合式安全樣式）。

> 套用稽核原則和相關的SACL時、會覆寫任何現有的DACL。套用安全性原則及其相關的DACL時、會覆寫任何現有的DACL。您應該在建立及套用新的安全性原則之前、先檢閱現有的安全性原則。

步驟

1. 套用安全性原則： `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

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

   原則套用工作已排程、並傳回工作ID。

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

監控安全性原則工作

將安全性原則套用至儲存虛擬機器（SVM）時、您可以監控安全性原則工作、以監控工作進度。如果您想要確定安全性原則的應用是否成功、這項功能就很有幫助。如果您的工作執行時間很長、而您要將大量安全性套用到大量的檔案和資料夾、這也很有幫助。

關於這項工作

若要顯示安全性原則工作的詳細資訊、您應該使用 `-instance` 參數。

步驟

1. 監控安全性原則工作： `vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

驗證套用的檔案安全性

您可以驗證檔案安全性設定、確認您套用安全性原則的儲存虛擬機器（SVM）上的檔案或資料夾具有所需的設定。

關於這項工作

您必須提供SVM名稱、其中包含資料、以及您要驗證安全性設定之檔案和資料夾的路徑。您可以使用選用的 `-expand-mask` 顯示安全性設定詳細資訊的參數。

步驟

1. 顯示檔案和資料夾安全性設定： `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

   `vserver security file-directory show -vserver vs1 -path /data/engineering -expand-mask true`

```
         Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
```

```
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...0 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
```

```
System Security
                                .... .... ...0 .... .... .... .... .... =
Synchronize
                                .... .... .... 0... .... .... .... .... =
Write Owner
                                .... .... .... .0.. .... .... .... .... =
Write DAC
                                .... .... .... ..0. .... .... .... .... =
Read Control
                                .... .... .... ...0 .... .... .... .... =
Delete
                                .... .... .... .... .... ...0 .... .... =
Write Attributes
                                .... .... .... .... .... .... 0... .... =
Read Attributes
                                .... .... .... .... .... .... .0.. .... =
Delete Child
                                .... .... .... .... .... .... ..0. .... =
Execute
                                .... .... .... .... .... .... ...0 .... =
Write EA
                                .... .... .... .... .... .... .... 0... =
Read EA
                                .... .... .... .... .... .... .... .0.. =
Append
                                .... .... .... .... .... .... .... ..0. =
Write
                                .... .... .... .... .... .... .... ...0 =
Read
```

使用**CLI**總覽設定稽核原則並套用至**NTFS**檔案和資料夾

使用ONTAP CLI時、您必須執行幾個步驟、才能將稽核原則套用至NTFS檔案和資料夾。首先、您要建立NTFS安全性描述元、然後將SACL新增至安全性描述元。接下來您要建立安全性原則並新增原則工作。然後將安全性原則套用至儲存虛擬機器（SVM）。

關於這項工作

套用安全性原則之後、您可以監控安全性原則工作、然後驗證套用的稽核原則設定。

套用稽核原則和相關的SACL時、會覆寫任何現有的DACL。您應該在建立及套用新的安全性原則之前、先檢閱現有的安全性原則。

相關資訊

使用儲存層級存取保護來保護檔案存取安全

使用CLI設定檔案和資料夾安全性時的限制

如何使用安全性描述元來套用檔案和資料夾安全性

"SMB與NFS稽核與安全性追蹤"

使用CLI在NTFS檔案和資料夾上設定及套用檔案安全性

建立**NTFS**安全性描述元

建立NTFS安全性描述元稽核原則是設定NTFS存取控制清單（ACL）並套用至位於SVM內的檔案和資料夾的第一步。您將在原則工作中、將安全性描述元與檔案或資料夾路徑建立關聯。

關於這項工作

您可以針對位於NTFS安全型磁碟區內的檔案和資料夾、或是位於混合式安全型磁碟區上的檔案和資料夾、建立NTFS安全性描述元。

根據預設、建立安全性描述元時、會將四個判別存取控制清單（DACL）存取控制項目（ACE）新增至該安全性描述元。四個預設的ACE如下所示：

物件	存取類型	存取權限	權限的套用位置
內建\系統管理員	允許	完全控制	此資料夾、子資料夾、檔案
內建\使用者	允許	完全控制	此資料夾、子資料夾、檔案
建立者擁有者	允許	完全控制	此資料夾、子資料夾、檔案
NT AUTHORITY\系統	允許	完全控制	此資料夾、子資料夾、檔案

您可以使用下列選用參數來自訂安全性描述元組態：

- 安全性描述元的擁有者
- 擁有者的主要群組
- 原始控制旗標

儲存層級存取保護會忽略任何選用參數的值。如需詳細資訊、請參閱手冊頁。

步驟

1. 如果您要使用進階參數、請將權限等級設為進階： `set -privilege advanced`
2. 建立安全性描述元： `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

```
vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner
DOMAIN\joe
```

3. 驗證安全描述元組態是否正確： `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

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

```
                                    Vserver: vs1
                          Security Descriptor Name: sd1
                    Owner of the Security Descriptor: DOMAIN\joe
```

4. 如果您處於進階權限層級、請返回管理權限層級： `set -privilege admin`

將**NTFS SACL**存取控制項目新增至**NTFS**安全性描述元

將SACL（系統存取控制清單）存取控制項目（ACE）新增至NTFS安全性描述元、是在SVM中為檔案或資料夾建立NTFS稽核原則的第二步驟。每個項目都會識別您要稽核的使用者或群組。SACL項目會定義您要稽核成功或失敗的存取嘗試。

關於這項工作

您可以將一個或多個ACE新增至安全性描述元的SACL。

如果安全性描述元包含具有現有ACE的SACL、則命令會將新的ACE新增至SACL。如果安全性描述元未包含SACL、則命令會建立SACL並將新的ACE新增至其中。

您可以指定要稽核中所指定帳戶成功或失敗事件的權限、以設定 SACL 項目 `-account` 參數。有三種互不相容的方法可以指定權限：

- 權利
- 進階權限
- 原始權限（進階權限）

如果您未指定 SACL 項目的權限、則預設設定為 `Full Control`。

您可以選擇自訂 SACL 項目、方法是指定如何使用套用繼承 `apply to` 參數。如果您未指定此參數、預設值為將此SACL項目套用至此資料夾、子資料夾及檔案。

步驟

1. 將 SACL 項目新增至安全性描述元： `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

```
vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type
failure -account domain\joe -rights full-control -apply-to this-folder
-vserver vs1
```

2. 驗證 SACL 項目是否正確： `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

   `vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1 -access-type deny -account domain\joe`

```
                                Vserver: vs1
                    Security Descriptor Name: sd1
          Access type for Specified Access Rights: failure
                        Account Name or SID: DOMAIN\joe
                              Access Rights: full-control
                     Advanced Access Rights: -
                                   Apply To: this-folder
                              Access Rights: full-control
```

建立安全性原則

建立儲存虛擬機器（SVM）的稽核原則、是設定及套用ACL至檔案或資料夾的第三個步驟。原則可做為各種工作的容器、其中每項工作都是可套用至檔案或資料夾的單一項目。您可以稍後將工作新增至安全性原則。

關於這項工作

您新增至安全性原則的工作包含NTFS安全性描述元與檔案或資料夾路徑之間的關聯。因此、您應該將安全性原則與每個儲存虛擬機器（SVM）（包含NTFS安全型磁碟區或混合式安全型磁碟區）建立關聯。

步驟

1. 建立安全性原則： `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

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

2. 驗證安全性原則： `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver           Policy Name
  ------------     --------------
      vs1              policy1
```

新增工作至安全性原則

建立原則工作並將其新增至安全性原則、是設定及套用ACL至SVM中的檔案或資料夾的第四個步驟。當您建立原則工作時、會將工作與安全性原則建立關聯。您可以將一或多個工

作項目新增至安全性原則。

關於這項工作

安全性原則是工作的容器。工作指的是單一作業、可透過安全性原則對具有NTFS或混合式安全性的檔案或資料夾（或是在設定儲存層級存取保護時、對磁碟區物件執行）。

工作有兩種類型：

- 檔案與目錄工作

  用於指定將安全性描述元套用至指定檔案和資料夾的工作。透過檔案和目錄工作所套用的ACL、可透過SMB用戶端或ONTAP CLI進行管理。

- 儲存層級的存取保護工作

  用於指定將儲存層級存取保護安全性描述元套用至指定磁碟區的工作。透過儲存層級存取保護工作套用的ACL只能透過ONTAP CLI進行管理。

工作包含檔案（或資料夾）或一組檔案（或資料夾）的安全性組態定義。原則中的每項工作都會以路徑唯一識別。在單一原則中、每個路徑只能有一項工作。原則不能有重複的工作項目。

新增工作至原則的準則：

- 每個原則最多可有10、000個工作項目。
- 原則可以包含一或多個工作。

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

- 儲存層級的存取保護用於限制權限。

  它永遠不會提供額外的存取權限。

您可以使用下列選用參數來自訂安全性描述元組態：

- 安全類型
- 傳播模式
- 索引位置
- 存取控制類型

儲存層級存取保護會忽略任何選用參數的值。如需詳細資訊、請參閱手冊頁。

步驟

1. 將具有相關安全性描述元的工作新增至安全性原則： `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` 為的預設值 `-access-control` 參數。設定檔案和目錄存取工作時、可選擇指定存取控制類型。

```
vserver security file-directory policy task add -vserver vs1 -policy-name
policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
-index-num 1 -access-control file-directory
```

2. 驗證原則工作組態：`vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

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

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   -----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

套用安全性原則

將稽核原則套用到SVM是建立NTFS ACL並套用到檔案或資料夾的最後一步。

關於這項工作

您可以將安全性原則中定義的安全性設定套用至FlexVol 駐留在各處的NTFS檔案和資料夾（NTFS或混合式安全樣式）。

> 套用稽核原則和相關的SACL時、會覆寫任何現有的DACL。套用安全性原則及其相關的DACL時、會覆寫任何現有的DACL。您應該在建立及套用新的安全性原則之前、先檢閱現有的安全性原則。

步驟

1. 套用安全性原則：`vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

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

   原則套用工作已排程、並傳回工作ID。

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

監控安全性原則工作

將安全性原則套用至儲存虛擬機器（SVM）時、您可以監控安全性原則工作、以監控工作進度。如果您想要確定安全性原則的應用是否成功、這項功能就很有幫助。如果您的工作執行時間很長、而您要將大量安全性套用到大量的檔案和資料夾、這也很有幫助。

關於這項工作

若要顯示安全性原則工作的詳細資訊、您應該使用 `-instance` 參數。

步驟

1. 監控安全性原則工作： `vserver security file-directory job show -vserver vserver_name`

   ```
   vserver security file-directory job show -vserver vs1
   ```

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

驗證套用的稽核原則

您可以驗證稽核原則、確認您套用安全性原則的儲存虛擬機器（SVM）上的檔案或資料夾具有所需的稽核安全性設定。

關於這項工作

您可以使用 `vserver security file-directory show` 顯示稽核原則資訊的命令。您必須提供SVM名稱、其中包含您要顯示其檔案或資料夾稽核原則資訊的資料、以及其路徑。

步驟

1. 顯示稽核原則設定： `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

範例

下列命令會顯示套用至SVM VS1路徑「/corp」的稽核原則資訊。這條路徑既成功、也套用成功/失敗的SACL項目：

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

                Vserver: vs1
              File Path: /corp
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

管理安全性原則工作時的考量

如果存在安全性原則工作、在某些情況下、您將無法修改該安全性原則或指派給該原則的工作。您應該瞭解可以修改或無法修改安全性原則的條件、以便成功修改原則。原則的修改包括新增、移除或修改指派給原則的工作、以及刪除或修改原則。

如果該原則的工作存在、且該工作處於下列狀態、則您無法修改安全性原則或指派給該原則的工作：

- 工作正在執行或進行中。
- 工作已暫停。
- 工作會恢復並處於執行中狀態。
- 如果工作正在等待容錯移轉到另一個節點。

在下列情況下、如果安全性原則有工作存在、您可以成功修改該安全性原則或指派給該原則的工作：

- 原則工作已停止。
- 原則工作已成功完成。

用於管理**NTFS**安全描述元的命令

管理安全性描述元時、會ONTAP 有特定的指令檔。您可以建立、修改、刪除及顯示安全性描述元的相關資訊。

如果您想要...	使用此命令...
建立NTFS安全性描述元	`vserver security file-directory ntfs create`
修改現有的NTFS安全性描述元	`vserver security file-directory ntfs modify`
顯示現有NTFS安全性描述元的相關資訊	`vserver security file-directory ntfs show`
刪除NTFS安全性描述元	`vserver security file-directory ntfs delete`

請參閱的手冊頁 `vserver security file-directory ntfs` 命令以取得更多資訊。

用於管理**NTFS DACL**存取控制項目的命令

管理ONTAP DACL存取控制項目（ACE）時、會有特定的功能不完整的指令。您可以隨時將ACE新增至NTFS DACL。您也可以在DACL中修改、刪除及顯示有關ACE的資訊、來管理現有的NTFS DACL。

如果您想要...	使用此命令...
建立ACE並將其新增至NTFS DACL	`vserver security file-directory ntfs dacl add`
修改NTFS DACL中的現有ACE	`vserver security file-directory ntfs dacl modify`
顯示NTFS DACL中現有ACE的相關資訊	`vserver security file-directory ntfs dacl show`
從NTFS DACL移除現有的ACE	`vserver security file-directory ntfs dacl remove`

請參閱的手冊頁 `vserver security file-directory ntfs dacl` 命令以取得更多資訊。

管理 **NTFS SACL** 存取控制項目的命令

管理ONTAP SACL存取控制項目（ACE）時、會有特定的功能不完整的命令。您可以隨時

將ACE新增至NTFS SACL。您也可以在SACL中修改、刪除及顯示有關ACE的資訊、來管理現有的NTFS SACL。

如果您想要...	使用此命令...
建立ACE並將其新增至NTFS SACL	`vserver security file-directory ntfs sacl add`
修改NTFS SACL中的現有ACE	`vserver security file-directory ntfs sacl modify`
顯示NTFS SACL中現有ACE的相關資訊	`vserver security file-directory ntfs sacl show`
從NTFS SACL移除現有的ACE	`vserver security file-directory ntfs sacl remove`

請參閱的手冊頁 `vserver security file-directory ntfs sacl` 命令以取得更多資訊。

管理安全性原則的命令

管理安全性原則時、會ONTAP 有特定的指令檔。您可以顯示原則的相關資訊、也可以刪除原則。您無法修改安全性原則。

如果您想要...	使用此命令...
建立安全性原則	`vserver security file-directory policy create`
顯示安全性原則的相關資訊	`vserver security file-directory policy show`
刪除安全性原則	`vserver security file-directory policy delete`

請參閱的手冊頁 `vserver security file-directory policy` 命令以取得更多資訊。

用於管理安全性原則工作的命令

有一些用來新增、修改、移除及顯示安全性原則工作相關資訊的指令。ONTAP

如果您想要...	使用此命令...
新增安全性原則工作	`vserver security file-directory policy task add`

如果您想要...	使用此命令...
修改安全性原則工作	`vserver security file-directory policy task modify`
顯示安全性原則工作的相關資訊	`vserver security file-directory policy task show`
移除安全性原則工作	`vserver security file-directory policy task remove`

請參閱的手冊頁 `vserver security file-directory policy task` 命令以取得更多資訊。

用於管理安全性原則工作的命令

有一些用來暫停、恢復、停止及顯示安全性原則工作資訊的指令。ONTAP

如果您想要...	使用此命令...
暫停安全性原則工作	`vserver security file-directory job pause -vserver vserver_name -id integer`
恢復安全原則工作	`vserver security file-directory job resume -vserver vserver_name -id integer`
顯示安全性原則工作的相關資訊	`vserver security file-directory job show -vserver vserver_name` 您可以使用此命令來判斷工作的工作 ID 。
停止安全性原則工作	`vserver security file-directory job stop -vserver vserver_name -id integer`

請參閱的手冊頁 `vserver security file-directory job` 命令以取得更多資訊。

設定SMB共用的中繼資料快取

SMB中繼資料快取的運作方式

中繼資料快取可讓SMB 1.0用戶端上的檔案屬性快取、更快存取檔案和資料夾屬性。您可以啟用或停用每個共用區的屬性快取。如果啟用中繼資料快取、您也可以設定快取項目的即時時間。如果用戶端透過SMB 2.x或SMB 3.0連線至共用區、則不需要設定中繼資料快取。

啟用時、SMB中繼資料快取會在有限的時間內儲存路徑和檔案屬性資料。這可為具有一般工作負載的SMB 1.0用戶端提升SMB效能。

對於某些工作、SMB會建立大量的流量、包括多個相同的路徑和檔案中繼資料查詢。您可以使用SMB中繼資料快取來從快取擷取資訊、藉此減少備援查詢的數量、並改善SMB 1.0用戶端的效能。

雖然不太可能、但中繼資料快取可能會將過時的資訊提供給SMB 1.0用戶端。如果您的環境負擔不起這項風險、則不應啟用此功能。

啟用SMB中繼資料快取

您可以啟用SMB中繼資料快取、以改善SMB 1.0用戶端的SMB效能。根據預設、SMB中繼資料快取會停用。

步驟

1. 執行所需的動作：

如果您想要...	輸入命令...
建立共用時啟用SMB中繼資料快取	`vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties attributecache`
在現有共用區上啟用SMB中繼資料快取	`vserver cifs share properties add -vserver` *`vserver_name`* `-share-name` *`share_name`* `-share-properties attributecache`

相關資訊

設定SMB中繼資料快取項目的生命週期

新增或移除現有SMB共用區上的共用內容

設定SMB中繼資料快取項目的生命週期

您可以設定SMB中繼資料快取項目的生命週期、以最佳化環境中的SMB中繼資料快取效能。預設值為 10 秒。

開始之前

您必須啟用SMB中繼資料快取功能。如果未啟用SMB中繼資料快取、則不會使用SMB快取TTL設定。

步驟

1. 執行所需的動作：

如果您想要在下列情況下設定**SMB**中繼資料快取項目的生命週期...	輸入命令...
建立共用區	`vserver cifs share -create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-attribute-cache-ttl [integerh][integerm][integers]`
修改現有的共用區	`vserver cifs share -modify -vserver` *`vserver_name`* `-share-name` *`share_name`* `-attribute-cache-ttl [integerh][integerm][integers]`

您可以在建立或修改共用時指定其他共用組態選項和屬性。如需詳細資訊、請參閱手冊頁。

管理檔案鎖定

關於在傳輸協定之間鎖定檔案

檔案鎖定是用戶端應用程式用來防止使用者存取先前由其他使用者開啟的檔案的方法。如何鎖定檔案取決於用戶端的傳輸協定。ONTAP

如果用戶端是NFS用戶端、則鎖定為建議事項；如果用戶端是SMB用戶端、則鎖定為必要項目。

由於NFS與SMB檔案鎖定之間的差異、NFS用戶端可能無法存取先前由SMB應用程式開啟的檔案。

當NFS用戶端嘗試存取SMB應用程式鎖定的檔案時、會發生下列情況：

- 在混合或 NTFS 磁碟區中、檔案處理作業、例如 `rm`、 `rmdir`和 `mv` 可能導致 NFS 應用程式失敗。
- SMB拒絕讀取和拒絕寫入開啟模式會分別拒絕NFS讀取和寫入作業。
- 當檔案的寫入範圍遭專屬SMB bytelock鎖定時、NFS寫入作業會失敗。
- 取消連結
  - 對於 NTFS 檔案系統、支援 SMB 和 CIFS 刪除作業。

    檔案將在上次關閉後移除。
  - 不支援 NFS 取消連結作業。

    不支援此功能、因為需要 NTFS 和 SMB 的語言、而且 NFS 不支援上次的「刪除 - 關閉」作業。
  - 對於 UNIX 檔案系統、支援取消連結作業。

    支援此功能、因為需要 NFS 和 UNIX 的語言。
- 重新命名
  - 對於 NTFS 檔案系統、如果目的地檔案是從 SMB 或 CIFS 開啟、則可以重新命名目的地檔案。

- 不支援 NFS 重新命名。

  不支援此功能、因為需要 NTFS 和 SMB 的語言。

在UNIX安全型磁碟區中、NFS取消連結和重新命名作業會忽略SMB鎖定狀態、並允許存取檔案。UNIX安全型磁碟區上的所有其他NFS作業都會遵守SMB鎖定狀態。

如何處理唯讀位元ONTAP

唯讀位元是逐一檔案設定、以反映檔案是可寫入（停用）或唯讀（啟用）。

使用Windows的SMB用戶端可以設定每個檔案的唯讀位元。NFS用戶端不會設定每個檔案的唯讀位元、因為NFS用戶端沒有任何使用每個檔案唯讀位元的傳輸協定作業。

當使用Windows的SMB用戶端建立檔案時、可以在檔案上設定唯讀位元。ONTAP在NFS用戶端和SMB用戶端之間共用檔案時、也可以設定唯讀位元。ONTAP有些軟體在NFS用戶端和SMB用戶端使用時、需要啟用唯讀位元。

為了在NFS用戶端和SMB用戶端之間共用的檔案上保留適當的讀取和寫入權限、它會根據下列規則來處理唯讀位元：ONTAP

- NFS會將任何啟用唯讀位元的檔案視為未啟用寫入權限位元。
- 如果NFS用戶端停用所有寫入權限位元、且至少有一個位元先前已啟用、ONTAP 則會啟用該檔案的唯讀位元。
- 如果NFS用戶端啟用任何寫入權限位元、ONTAP 則無法使用該檔案的唯讀位元。
- 如果已啟用檔案的唯讀位元、且NFS用戶端嘗試探索檔案的權限、則檔案的權限位元不會傳送至NFS用戶端；ONTAP 而是將權限位元傳送至NFS用戶端、並遮罩寫入權限位元。
- 如果已啟用檔案的唯讀位元、且SMB用戶端停用唯讀位元、ONTAP 則會啟用檔案的擁有者寫入權限位元。
- 啟用唯讀位元的檔案只能由root寫入。

> 檔案權限的變更會立即在SMB用戶端上生效、但如果NFS用戶端啟用屬性快取、則可能不會立即在NFS用戶端上生效。

在處理共用路徑元件上的鎖定時、此功能與Windows有何ONTAP 不同

不像Windows、ONTAP 在檔案開啟時、不會鎖定開啟檔案路徑的每個元件。此行為也會影響SMB共用路徑。

由於無法鎖定路徑的每個元件、因此可以重新命名開啟檔案或共用區上方的路徑元件、這可能會對某些應用程式造成問題、也可能導致SMB組態中的共用路徑無效。ONTAP這可能導致無法存取共用區。

為了避免重新命名路徑元件所造成的問題、您可以套用安全性設定、防止使用者或應用程式重新命名重要目錄。

顯示鎖定的相關資訊

您可以顯示目前檔案鎖定的相關資訊、包括鎖定的類型、鎖定狀態、位元組範圍鎖定、共用鎖定模式、委派鎖定及投機鎖定的詳細資料、以及鎖定是以耐久或持續的控點開啟。

關於這項工作

無法針對透過NFSv4或NFSv4.1建立的鎖定顯示用戶端IP位址。

依預設、命令會顯示所有鎖定的相關資訊。您可以使用命令參數來顯示特定儲存虛擬機器（SVM）的鎖定資訊、或是根據其他條件篩選命令的輸出。

。 `vserver locks show` 命令會顯示四種鎖定類型的相關資訊：

- 位元組範圍鎖定、僅鎖定部分檔案。
- 共用鎖定、可鎖定開啟的檔案。
- 投機鎖定、可控制SMB上的用戶端快取。
- 委派：透過NFSv4.x控制用戶端快取

藉由指定選用參數、您可以決定每種鎖定類型的重要資訊。如需詳細資訊、請參閱命令的手冊頁。

步驟

1. 使用顯示鎖定的相關資訊 `vserver locks show` 命令。

範例

以下範例顯示具有路徑之檔案上 NFSv4 鎖定的摘要資訊 `/vol1/file1`。共享鎖定存取模式為WRITE拒絕_nONE、且鎖定是以寫入委派授予的：

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                         delegation  -
               Delegation Type: write
```

以下範例顯示有關 SMB 鎖定的詳細 oplock 和共享鎖定資訊、這些資訊位於具有路徑的檔案上 `/data2/data2_2/intro.pptx`。對於IP位址為10.3.1.3的用戶端、檔案上會以寫入拒絕的共用鎖定存取模式授予可持久使用的控制代碼。批次oplock層級的租賃oplock已授予：

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

                    Vserver: vs1
                     Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
             Lock Protocol: cifs
```

```
                 Lock Type: share-level
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                   Vserver: vs1
                    Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/test.pptx
                 Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
             Lock Protocol: cifs
                 Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

中斷鎖定

當檔案鎖定阻礙用戶端存取檔案時、您可以顯示目前保留的鎖定資訊、然後中斷特定鎖定。您可能需要中斷鎖定的案例包括偵錯應用程式。

關於這項工作

。 `vserver locks break` 命令只能在進階權限層級及更高層級使用。命令的手冊頁包含詳細資訊。

步驟

1. 若要尋找打破鎖定所需的資訊、請使用 `vserver locks show` 命令。

   命令的手冊頁包含詳細資訊。

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

如果您要指定...來中斷鎖定	輸入命令...
SVM名稱、Volume名稱、LIF名稱及檔案路徑	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
鎖定ID	`vserver locks break -lockid UUID`

4. 返回管理權限層級： `set -privilege admin`

監控SMB活動

顯示SMB工作階段資訊

您可以顯示已建立SMB工作階段的相關資訊、包括SMB連線和工作階段ID、以及使用工作階段之工作站的IP位址。您可以顯示工作階段SMB傳輸協定版本的相關資訊、以及持續可用的保護層級、協助您識別工作階段是否支援不中斷營運。

關於這項工作

您可以在SVM上以摘要形式顯示所有工作階段的資訊。不過、在許多情況下、傳回的輸出量很大。您可以指定選用參數、自訂輸出中顯示的資訊：

- 您可以使用選用的 `-fields` 參數顯示有關所選欄位的輸出。

  您可以輸入 `-fields ?` 決定您可以使用哪些欄位。

- 您可以使用 `-instance` 顯示已建立 SMB 工作階段的詳細資訊的參數。
- 您可以使用 `-fields` 參數或 `-instance` 參數可以單獨使用、也可以搭配其他選用參數使用。

步驟

1. 執行下列其中一項動作：

如果您要顯示**SMB**工作階段資訊...	輸入下列命令...
以摘要形式顯示SVM上的所有工作階段	`vserver cifs session show -vserver vserver_name`
在指定的連線ID上	`vserver cifs session show -vserver vserver_name -connection-id integer`
從指定的工作站IP位址	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
在指定的LIF IP位址上	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
在指定的節點上	`vserver cifs session show -vserver vserver_name -node {node_name
local}`	從指定的Windows使用者
`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`	使用指定的驗證機制
`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1	NTLMv2
Kerberos	Anonymous}`
使用指定的傳輸協定版本	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1
SMB2	SMB2_1
SMB3	SMB3_1}`  [NOTE] ==== 持續可用的保護功能和SMB多通道功能僅適用於SMB 3.0及更新版本的工作階段。若要在所有合格的工作階段中檢視其狀態、您應該指定此參數、並將值設為 `SMB3` 或更新版本。 ====
提供特定等級的持續可用保護	`vserver cifs session show -vserver vserver_name -continuously-available {No

如果您要顯示**SMB**工作階段資訊...	輸入下列命令...
Yes	Partial}`  [NOTE] ==== 如果持續可用的狀態為 `Partial`這表示工作階段至少包含一個開啟的持續可用檔案、但工作階段有一些檔案無法以持續可用的保護開啟。您可以使用 `vserver cifs sessions file show` 命令來判斷已建立工作階段上的哪些檔案未以持續可用的保護開啟。 ====
具有指定的SMB簽署工作階段狀態	`vserver cifs session show -vserver vserver_name -is-session-signed {true

範例

下列命令會顯示SVM VS1上從IP位址為10.1.1的工作站所建立之工作階段的工作階段資訊：

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open          Idle
ID         ID      Workstation      Windows User    Files         Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281 1       10.1.1.1         DOMAIN\joe          2          23s
```

下列命令會顯示SVM VS1具有持續可用保護之工作階段的詳細工作階段資訊。連線是使用網域帳戶建立的。

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: Yes
          Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

下列命令會顯示SVM VS1上使用SMB 3.0和SMB多通道之工作階段的工作階段資訊。在此範例中、使用者使用LIF IP位址從具有SMB 3.0功能的用戶端連線到此共用區、因此驗證機制預設為NTLMv2。連線必須使用Kerberos驗證、才能以持續可用的保護進行連線。

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

相關資訊

顯示開啟SMB檔案的相關資訊

顯示開啟**SMB**檔案的相關資訊

您可以顯示開啟SMB檔案的相關資訊、包括SMB連線和工作階段ID、託管磁碟區、共用名稱和共用路徑。您可以顯示檔案持續可用保護層級的相關資訊、這有助於判斷開啟的檔案是否處於支援不中斷營運的狀態。

關於這項工作

您可以在已建立的SMB工作階段中顯示開啟檔案的相關資訊。當您需要判斷SMB工作階段中特定檔案的SMB工作階段資訊時、所顯示的資訊非常有用。

例如、如果您有 SMB 工作階段、其中某些開啟的檔案會以持續可用的保護開啟、有些則無法以持續可用的保護開啟（的值） `-continuously-available` 欄位輸入 `vserver cifs session show` 命令輸出為 `Partial`）、您可以使用此命令來判斷哪些檔案無法持續使用。

您可以使用、以摘要形式顯示已建立的儲存虛擬機器（ SVM ） SMB 工作階段上所有開啟檔案的資訊 `vserver cifs session file show` 不含任何選用參數的命令。

不過、在許多情況下、傳回的輸出量很大。您可以指定選用參數、自訂輸出中顯示的資訊。如果您只想檢視開啟檔案的一小部分資訊、這項功能就很有幫助。

- 您可以使用選用的 `-fields` 參數、可在您選擇的欄位上顯示輸出。

  您可以單獨使用此參數、也可以搭配其他選用參數一起使用。

- 您可以使用 `-instance` 顯示開啟 SMB 檔案的詳細資訊的參數。

  您可以單獨使用此參數、也可以搭配其他選用參數一起使用。

步驟

1. 執行下列其中一項動作：

如果您要顯示開啟的**SMB**檔案...	輸入下列命令...
在SVM上以摘要形式顯示	`vserver cifs session file show -vserver vserver_name`
在指定的節點上	`vserver cifs session file show -vserver vserver_name -node {node_name`
local}`	在指定的檔案ID上
`vserver cifs session file show -vserver vserver_name -file-id integer`	在指定的SMB連線ID上
`vserver cifs session file show -vserver vserver_name -connection-id integer`	在指定的SMB工作階段ID上
`vserver cifs session file show -vserver vserver_name -session-id integer`	在指定的託管Aggregate上
`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`	在指定的磁碟區上
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	在指定的SMB共用區上
`vserver cifs session file show -vserver vserver_name -share share_name`	在指定的SMB路徑上
`vserver cifs session file show -vserver vserver_name -path path`	提供指定等級的持續可用保護

如果您要顯示開啟的**SMB**檔案…	輸入下列命令…
`vserver cifs session file show -vserver vserver_name -continuously-available {No	Yes}`  [NOTE] ==== 如果持續可用的狀態為 `No`這表示這些開啟的檔案無法不中斷地從接管和恢復恢復。在高可用度關係中、他們也無法從合作夥伴之間的一般Aggregate重新配置中恢復。 ====
指定的重新連線狀態	`vserver cifs session file show -vserver vserver_name -reconnected {No

您可以使用其他選用參數來精簡輸出結果。如需詳細資訊、請參閱手冊頁。

範例

下列範例顯示SVM VS1上開啟檔案的相關資訊：

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

下列範例顯示SVM VS1上開啟檔案ID為82的SMB檔案的詳細資訊：

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
             CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

相關資訊

顯示SMB工作階段資訊

判斷可用的統計資料物件和計數器

在取得CIFS、SMB、稽核和BranchCache雜湊統計資料的相關資訊及監控效能之前、您必須先知道哪些物件和計數器可供您取得資料。

步驟

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

如果您想要判斷...	輸入...
可用的物件	`statistics catalog object show`
可用的特定物件	`statistics catalog object show object object_name`
可用的計數器	`statistics catalog counter show object object_name`

請參閱手冊頁、以取得可用物件和計數器的詳細資訊。

3. 返回管理權限層級： `set -privilege admin`

範例

下列命令會顯示與叢集中CIFS和SMB存取相關之所選統計物件的說明、如進階權限層級所示：

```
cluster1::> set -privilege advanced

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

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

下列命令會顯示的一些計數器相關資訊 `cifs` 進階權限層級的物件：

> 此範例不會顯示的所有可用計數器 `cifs` 物件；輸出被截斷。

```
cluster1::> set -privilege advanced

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

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
--------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                                vserver_1:10.72.205.179
    instance_uuid                                       2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

相關資訊

顯示統計資料

顯示統計資料

您可以顯示各種統計資料、包括CIFS和SMB、稽核和BranchCache雜湊的統計資料、以監控效能並診斷問題。

開始之前

您必須使用收集資料樣本 `statistics start` 和 `statistics stop` 顯示物件相關資訊之前的命令。

步驟

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

如果您要顯示下列項目的統計資料...	輸入...
SMB的所有版本	`statistics show -object cifs`
SMB 1.0	`statistics show -object smb1`
SMB 2.x和SMB 3.0	`statistics show -object smb2`
節點的CIFS子系統	`statistics show -object nblade_cifs`
多重傳輸協定稽核	`statistics show -object audit_ng`
BranchCache雜湊服務	`statistics show -object hashd`
動態DNS	`statistics show -object ddns_update`

   如需詳細資訊、請參閱每個命令的手冊頁。

3. 返回管理權限層級： `set -privilege admin`

相關資訊

判斷可用的統計資料物件和計數器

監控SMB簽署的工作階段統計資料

顯示BranchCache統計資料

使用統計資料來監控自動節點參照活動

"Microsoft Hyper-V和SQL Server的SMB組態"

"效能監控設定"