使用本機使用者和群組進行驗證和授權
ONTAP 9

NetApp
April 24, 2024

目錄

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」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

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`

如果您希望本機使用者和群組...	輸入命令...
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。

如果您想要...	輸入命令...
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。
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。
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`
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
```