顯示檔案安全性和稽核原則的相關資訊 ONTAP 9

NetApp
February 12, 2026

目錄

顯示檔案安全性和稽核原則的相關資訊

了解如何查看 ONTAP SMB 檔案安全和稽核策略

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

顯示檔案安全性的相關資訊

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

- NTFS
- UNIX
- 混合

顯示稽核原則的相關資訊

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

- SMB（所有版本）
- NFSv4.x

顯示儲存層級存取保護（slag）安全性的相關資訊

儲存層級的存取保護安全功能可套用FlexVol 至下列安全樣式的物件：

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

顯示動態存取控制（DAC）安全性的相關資訊

動態存取控制安全功能FlexVol 可套用至包含下列安全樣式的物件：

- NTFS
- 混合（如果物件具有NTFS有效安全性）

相關資訊

- 了解如何使用儲存級別存取防護來保護文件存取
- 顯示有關伺服器上儲存層級存取防護的信息

顯示有關 NTFS 安全模式磁碟區上的 ONTAP SMB 檔案安全性的信息

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

關於這項工作

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

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

步驟

1. 以所需的詳細資料層級顯示檔案和目錄安全性設定：

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

範例

下列範例顯示有關路徑的安全性資訊 `/vol4` 在 SVM VS1 中：

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

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

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

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

               Vserver: vs1
             File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
```

```
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

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

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
Generic Execute
                             ...0 .... .... .... .... .... .... .... =
Generic All
                             .... ...0 .... .... .... .... .... .... =
System Security
                             .... .... ...1 .... .... .... .... .... =
Synchronize
                             .... .... .... 1... .... .... .... .... =
Write Owner
                             .... .... .... .1.. .... .... .... .... =
Write DAC
                             .... .... .... ..1. .... .... .... .... =
Read Control
                             .... .... .... ...1 .... .... .... .... =
Delete
```

```
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
Write Owner
                              .... .... .... .0.. .... .... .... .... =
Write DAC
                              .... .... .... ..0. .... .... .... .... =
Read Control
                              .... .... .... ...0 .... .... .... .... =
Delete
                              .... .... .... .... .... ...0 .... .... =
Write Attributes
                              .... .... .... .... .... .... 0... .... =
Read Attributes
                              .... .... .... .... .... .... .0.. .... =
Delete Child
```

```
                                .... .... .... .... .... .... ..0. .... =
Execute
                                .... .... .... .... .... .... ...0 .... =
Write EA
                                .... .... .... .... .... .... .... 0... =
Read EA
                                .... .... .... .... .... .... .... .0.. =
Append
                                .... .... .... .... .... .... .... ..0. =
Write
                                .... .... .... .... .... .... .... ...0 =
Read
```

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

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

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


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

相關資訊

- 顯示混合式安全型磁碟區的檔案安全資訊
- 顯示UNIX安全型磁碟區上的檔案安全資訊

顯示有關混合安全模式磁碟區上的 ONTAP SMB 檔案安全性的信息

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

關於這項工作

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

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

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

步驟

1. 以所需的詳細資料層級顯示檔案和目錄安全性設定：

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

範例

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

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

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

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

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

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

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

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

相關資訊

- 顯示NTFS安全型磁碟區上的檔案安全資訊
- 顯示UNIX安全型磁碟區上的檔案安全資訊

顯示有關 UNIX 安全模式磁碟區上的 ONTAP SMB 檔案安全性的信息

您可以顯示UNIX安全型磁碟區上的檔案與目錄安全性相關資訊、包括安全性樣式與有效的

安全性樣式、套用的權限、以及UNIX擁有者與群組的相關資訊。您可以使用結果來驗證安全性組態、或疑難排解檔案存取問題。

關於這項工作

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

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

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

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

  它們只對NTFS安全描述元有意義。

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

步驟

1. 以所需的詳細資料層級顯示檔案和目錄安全性設定：

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

範例

下列範例顯示有關路徑的安全性資訊 `/home` 在 SVM VS1 中：

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

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

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

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

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

相關資訊

- 顯示有關安全類型捲上的文件安全性的信息
- 顯示混合式安全型磁碟區的檔案安全資訊

ONTAP 指令用於顯示有關 SMB FlexVol 磁碟區上的 NTFS 稽核策略的信息

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

關於這項工作

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

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

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

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

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

- ACL輸出只會針對具有NTFS或NFSv4安全性的檔案和資料夾顯示。

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

- ACL輸出中的擁有者和群組輸出欄位僅適用於NTFS安全性描述元。

步驟

1. 以所需的詳細資料層級顯示檔案和目錄稽核原則設定：

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

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

範例

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

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

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

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

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

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

ONTAP 指令用於顯示有關 SMB FlexVol 磁碟區上的 NFSv4 稽核策略的信息

您可以FlexVol 使用ONTAP CLI在S什麼 磁碟區上顯示NFSv4稽核原則的相關資訊、包括安全樣式和有效的安全樣式、套用的權限、以及系統存取控制清單（SACL）的相關資訊。您可以使用結果來驗證安全性組態或疑難排解稽核問題。

關於這項工作

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

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

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

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

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

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

步驟

1. 以所需的詳細資料層級顯示檔案和目錄安全性設定：

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

範例

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

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

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

了解如何顯示 ONTAP SMB 文件安全和審計策略信息

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

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

範例

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

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

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

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

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

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

版權資訊

商標資訊