# 显示有关文件安全性和审核策略的信息

ONTAP 9

NetApp
April 24, 2024

# 目录

# 显示有关文件安全性和审核策略的信息

## 显示有关文件安全性和审核策略概述的信息

您可以显示 Storage Virtual Machine （ SVM ） 上卷中包含的文件和目录的文件安全信息。您可以显示有关 FlexVol 卷上审核策略的信息。如果已配置，则可以显示有关 FlexVol 卷上存储级别访问防护和动态访问控制安全设置的信息。

### 显示有关文件安全性的信息

您可以使用以下安全模式显示应用于卷和 qtree （对于 FlexVol 卷）中数据的文件安全性信息：

- NTFS
- "unix"
- 混合

### 显示有关审核策略的信息

您可以通过以下 NAS 协议显示有关审核 FlexVol 卷上访问事件的审核策略的信息：

- SMB （所有版本）
- NFSv4.x

### 显示有关存储级别访问防护（ **SLAG** ）安全性的信息

可以使用以下安全模式对 FlexVol 卷和 qtree 对象应用存储级别访问防护安全性：

- NTFS
- 混合
- UNIX （如果在包含此卷的 SVM 上配置了 CIFS 服务器）

### 显示有关动态访问控制（ **DAC** ）安全性的信息

可以使用以下安全模式对 FlexVol 卷中的对象应用动态访问控制安全性：

- NTFS
- 混合（如果对象具有 NTFS 有效安全性）

相关信息

使用存储级别访问防护保护文件访问安全

显示有关存储级别访问防护的信息

# 显示 NTFS 安全模式卷上的文件安全性信息

您可以显示 NTFS 安全模式卷上的文件和目录安全性信息，包括安全模式和有效安全模式是什么，应用了哪些权限以及有关 DOS 属性的信息。您可以使用结果验证安全配置或对文件访问问题进行故障排除。

关于此任务

您必须提供 Storage Virtual Machine （ SVM ）的名称以及要显示其文件或文件夹安全信息的数据的路径。您可以摘要形式或详细列表形式显示输出。

- 由于 NTFS 安全模式卷和 qtree 在确定文件访问权限时仅使用 NTFS 文件权限以及 Windows 用户和组，因此与 UNIX 相关的输出字段包含仅显示的 UNIX 文件权限信息。
- 对于采用 NTFS 安全模式的文件和文件夹，将显示 ACL 输出。
- 由于可以在卷根或 qtree 上配置存储级别访问防护安全性，因此配置了存储级别访问防护的卷或 qtree 路径的输出可能会同时显示常规文件 ACL 和存储级别访问防护 ACL 。
- 如果为给定文件或目录路径配置了动态访问控制，则输出还会显示有关动态访问控制 ACE 的信息。

步骤

1. 使用所需的详细信息级别显示文件和目录安全设置：

| 要显示信息的项 | 输入以下命令 ... |
|---|---|
| 摘要形式 | `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* |
| 扩展了详细信息 | `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true` |

示例

以下示例显示路径的安全信息 `/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
```

以下示例显示了路径的安全信息以及展开的掩码 `/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
```

以下示例显示路径为的卷的安全信息、包括存储级别访问防护安全信息 `/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
```

相关信息

显示混合安全模式卷上的文件安全性信息

显示 UNIX 安全模式卷上的文件安全性信息

# 显示混合安全模式卷上的文件安全性信息

## 您可以显示混合安全模式卷上的文件和目录安全性信息，包括安全模式和有效安全模式是什么，应用了哪些权限以及有关 UNIX 所有者和组的信息。您可以使用结果验证安全配置或对文件访问问题进行故障排除。

关于此任务

您必须提供 Storage Virtual Machine （ SVM ）的名称以及要显示其文件或文件夹安全信息的数据的路径。您可以摘要形式或详细列表形式显示输出。

- 混合安全模式卷和 qtree 可以包含一些使用 UNIX 文件权限的文件和文件夹，模式位或 NFSv4 ACL ，以及一些使用 NTFS 文件权限的文件和目录。
- 混合安全模式卷的顶层可以具有 UNIX 或 NTFS 有效安全性。
- 只有采用 NTFS 或 NFSv4 安全模式的文件和文件夹才会显示 ACL 输出。

  对于使用 UNIX 安全性且仅应用模式位权限（无 NFSv4 ACL ）的文件和目录，此字段为空。

- ACL 输出中的所有者和组输出字段仅适用于 NTFS 安全描述符。
- 由于即使卷根或 qtree 的有效安全模式为 UNIX ，也可以在混合安全模式卷或 qtree 上配置存储级别访问防护安全性， 配置了存储级别访问防护的卷或 qtree 路径的输出可能会同时显示 UNIX 文件权限和存储级别访问防护 ACL 。
- 如果在命令中输入的路径指向具有 NTFS 有效安全性的数据，则如果为给定文件或目录路径配置了动态访问控制，则输出还会显示有关动态访问控制 ACE 的信息。

步骤

1. 使用所需的详细信息级别显示文件和目录安全设置：

| 要显示信息的项 | 输入以下命令 ... |
| --- | --- |
| 摘要形式 | `vserver security file-directory show -vserver vserver_name -path path` |
| 扩展了详细信息 | `vserver security file-directory show -vserver vserver_name -path path -expand-mask true` |

示例

以下示例显示路径的安全信息 `/projects` 在SVM VS1中、以扩展掩码形式显示。此混合安全模式路径具有 UNIX 有效安全性。

```
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: -
```

以下示例显示路径的安全信息 `/data` 在SVM VS1中。此混合安全模式路径具有 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
```

以下示例显示路径上卷的安全信息 `/datavol5` 在SVM VS1中。此混合安全模式卷的顶层具有 UNIX 有效安全性。此卷具有存储级别访问防护安全性。

```
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
```

相关信息

显示NTFS安全模式卷上的文件安全性信息

显示 UNIX 安全模式卷上的文件安全性信息

# 显示有关 UNIX 安全模式卷上的文件安全性的信息

您可以显示 UNIX 安全模式卷上的文件和目录安全性信息，包括安全模式和有效安全模式

是什么，应用了哪些权限以及有关 UNIX 所有者和组的信息。您可以使用结果验证安全配置或对文件访问问题进行故障排除。

关于此任务

您必须提供 Storage Virtual Machine （ SVM ）的名称以及要显示其文件或目录安全信息的数据的路径。您可以摘要形式或详细列表形式显示输出。

- 在确定文件访问权限时， UNIX 安全模式卷和 qtree 仅使用 UNIX 文件权限，模式位或 NFSv4 ACL 。
- 只有具有 NFSv4 安全性的文件和文件夹才会显示 ACL 输出。

  对于使用 UNIX 安全性且仅应用模式位权限（无 NFSv4 ACL ）的文件和目录，此字段为空。

- 对于 NFSv4 安全描述符， ACL 输出中的所有者和组输出字段不适用。

  它们仅对 NTFS 安全描述符有意义。

- 由于如果在SVM上配置了CIFS服务器、则UNIX卷或qtree支持存储级别访问防护安全性、因此输出可能包含应用于中指定的卷或qtree的存储级别访问防护安全性的信息 `-path` 参数。

步骤

1. 使用所需的详细信息级别显示文件和目录安全设置：

| 要显示信息的项 | 输入以下命令 ... |
| --- | --- |
| 摘要形式 | `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* |
| 扩展了详细信息 | `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true` |

示例

以下示例显示路径的安全信息 `/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: -
```

以下示例显示路径的安全信息 `/home` 在扩展掩码形式的SVM VS1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: -
```

相关信息

显示NTFS安全模式卷上的文件安全性信息

显示混合安全模式卷上的文件安全性信息

# 使用命令行界面显示有关 FlexVol 卷上 NTFS 审核策略的信息

您可以显示有关 FlexVol 卷上的 NTFS 审核策略的信息，包括什么是安全模式和有效安全模式，应用了哪些权限以及有关系统访问控制列表的信息。您可以使用结果验证安全配置或对审核问题进行故障排除。

关于此任务

您必须提供 Storage Virtual Machine （ SVM ）的名称以及要显示其审核信息的文件或文件夹的路径。您可以摘要形式或详细列表形式显示输出。

- 对于审核策略， NTFS 安全模式卷和 qtree 仅使用 NTFS 系统访问控制列表（ SACL ）。
- 具有 NTFS 有效安全性的混合安全模式卷中的文件和文件夹可以应用 NTFS 审核策略。

  混合安全模式卷和 qtree 可以包含一些使用 UNIX 文件权限的文件和目录，模式位或 NFSv4 ACL ，以及一些使用 NTFS 文件权限的文件和目录。

- 混合安全模式卷的顶层可以具有 UNIX 或 NTFS 有效安全性，并且可能包含也可能不包含 NTFS SACL 。
- 由于即使卷根或 qtree 的有效安全模式为 UNIX ，也可以在混合安全模式卷或 qtree 上配置存储级别访问防护安全性， 配置了存储级别访问防护的卷或 qtree 路径的输出可能会同时显示常规文件和文件夹 NFSv4 SACL 以及存储级别访问防护 NTFS SACL 。
- 如果在命令中输入的路径指向采用 NTFS 有效安全模式的数据，则如果为给定文件或目录路径配置了动态访问控制，则输出还会显示有关动态访问控制 ACE 的信息。
- 显示有关具有 NTFS 有效安全性的文件和文件夹的安全信息时，与 UNIX 相关的输出字段包含仅显示的 UNIX 文件权限信息。

  在确定文件访问权限时， NTFS 安全模式文件和文件夹仅使用 NTFS 文件权限以及 Windows 用户和组。

- 只有采用 NTFS 或 NFSv4 安全模式的文件和文件夹才会显示 ACL 输出。

  对于使用 UNIX 安全性且仅应用模式位权限（无 NFSv4 ACL ）的文件和文件夹，此字段为空。

- ACL 输出中的所有者和组输出字段仅适用于 NTFS 安全描述符。

步骤

1. 显示具有所需详细级别的文件和目录审核策略设置：

| 要显示信息的项 | 输入以下命令 ... |
| --- | --- |
| 摘要形式 | `vserver security file-directory show -vserver vserver_name -path path` |

| 要显示信息的项 | 输入以下命令 ... |
| --- | --- |
| 作为详细列表 | `vserver security file-directory show -vserver vserver_name -path path -expand-mask true` |

示例

以下示例显示了路径的审核策略信息 `/corp` 在SVM VS1中。此路径具有 NTFS 有效安全性。NTFS 安全描述符包含成功和成功 / 失败 SACL 条目。

```
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
```

以下示例显示了路径的审核策略信息 `/datavol1` 在SVM VS1中。此路径包含常规文件和文件夹 SACL 以及存储级别访问防护 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
```

## 使用命令行界面显示有关 **FlexVol** 卷上 **NFSv4** 审核策略的信息

您可以使用 ONTAP 命令行界面显示有关 FlexVol 卷上 NFSv4 审核策略的信息，包括什么

是安全模式和有效安全模式，应用了哪些权限以及有关系统访问控制列表（SACL）的信息。您可以使用结果验证安全配置或对审核问题进行故障排除。

关于此任务

您必须提供 Storage Virtual Machine （SVM）的名称以及要显示其审核信息的文件或目录的路径。您可以摘要形式或详细列表形式显示输出。

- UNIX 安全模式卷和 qtree 仅对审核策略使用 NFSv4 SACL 。
- 混合安全模式卷中采用 UNIX 安全模式的文件和目录可以应用 NFSv4 审核策略。

  混合安全模式卷和 qtree 可以包含一些使用 UNIX 文件权限的文件和目录，模式位或 NFSv4 ACL ，以及一些使用 NTFS 文件权限的文件和目录。

- 混合安全模式卷的顶层可以具有 UNIX 或 NTFS 有效安全性，并且可能包含也可能不包含 NFSv4 SACL 。
- 只有采用 NTFS 或 NFSv4 安全模式的文件和文件夹才会显示 ACL 输出。

  对于使用 UNIX 安全性且仅应用模式位权限（无 NFSv4 ACL ）的文件和文件夹，此字段为空。

- ACL 输出中的所有者和组输出字段仅适用于 NTFS 安全描述符。
- 由于即使卷根或 qtree 的有效安全模式为 UNIX ，也可以在混合安全模式卷或 qtree 上配置存储级别访问防护安全性， 配置了存储级别访问防护的卷或 qtree 路径的输出可能会同时显示常规 NFSv4 文件和目录 SACL 以及存储级别访问防护 NTFS SACL 。
- 由于如果在SVM上配置了CIFS服务器、则UNIX卷或qtree支持存储级别访问防护安全性、因此输出可能包含应用于中指定的卷或qtree的存储级别访问防护安全性的信息 `-path` 参数。

步骤

1. 使用所需的详细信息级别显示文件和目录安全设置：

| 要显示信息的项 | 输入以下命令 ... |
| --- | --- |
| 摘要形式 | `vserver security file-directory show -vserver vserver_name -path path` |
| 扩展了详细信息 | `vserver security file-directory show -vserver vserver_name -path path -expand-mask true` |

示例

以下示例显示路径的安全信息 `/lab` 在SVM VS1中。此 UNIX 安全模式路径具有 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
```

# 显示有关文件安全性和审核策略信息的方式

## 您可以使用通配符（*）显示有关给定路径或根卷下所有文件和目录的文件安全和审核策略的信息。

通配符（*）可用作给定目录路径的最后一个子组件，在该路径下，您希望显示所有文件和目录的信息。如果要显示名为 "` *` " 的特定文件或目录的信息，则需要在双引号（"`` "）中提供完整路径。

示例

以下带有通配符的命令显示路径下所有文件和目录的信息 `/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)
```

以下命令显示路径下名为"*"的文件的信息 `/vol1/a` SVM VS1。路径用双引号括起来（""）。

```
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
```