ファイル セキュリティと監査ポリシーに関する情報の表示

ONTAP 9

NetApp
February 12, 2026

目次

ファイル セキュリティと監査ポリシーに関する情報の表示 1
ONTAP SMBファイルセキュリティと監査ポリシーの表示について学習します 1
ファイル セキュリティに関する情報の表示 1
監査ポリシーに関する情報の表示 1
ストレージレベルのアクセス保護（SLAG）セキュリティに関する情報の表示 1
ダイナミック アクセス制御（DAC）セキュリティに関する情報の表示 1
ONTAP SMBファイルセキュリティに関する情報を NTFSセキュリティ形式のボリューム上に表示します 2
混合セキュリティ形式のボリューム上のONTAP SMBファイルセキュリティに関する情報を表示します 8
UNIXセキュリティ形式のボリューム上のONTAP SMBファイルセキュリティに関する情報を表示します 11
SMB FlexVol ボリューム上の NTFS 監査ポリシーに関する情報を表示する ONTAP コマンド 14
SMB FlexVol ボリューム上の NFSv4 監査ポリシーに関する情報を表示する ONTAP コマンド 17
ONTAP SMBファイルのセキュリティと監査ポリシー情報を表示する方法を学びます 18

ファイル セキュリティと監査ポリシーに関する情報の表示

ONTAP SMBファイルセキュリティと監査ポリシーの表示について学習します

Storage Virtual Machine（SVM）のボリューム内に格納されたファイルとディレクトリのファイル セキュリティに関する情報を表示できます。FlexVolの監査ポリシーに関する情報を表示できます。設定されている場合、FlexVolのストレージレベルのアクセス保護およびダイナミック アクセス制御セキュリティの設定に関する情報を表示できます。

ファイル セキュリティに関する情報の表示

次のセキュリティ形式のボリュームと（FlexVolの）qtreeに格納されたデータに適用されているファイル セキュリティに関する情報を表示できます。

- NTFS
- UNIX
- 混合

監査ポリシーに関する情報の表示

次のNASプロトコルを介したFlexVolのアクセス イベントを監査する監査ポリシーに関する情報を表示できます。

- SMB（すべてのバージョン）
- NFSv4.x

ストレージレベルのアクセス保護（SLAG）セキュリティに関する情報の表示

ストレージレベルのアクセス保護セキュリティは、次のセキュリティ形式のFlexVolおよびqtreeオブジェクトに適用できます。

- NTFS
- 混合
- UNIX（ボリュームが含まれるSVMでCIFSサーバが設定されている場合）

ダイナミック アクセス制御（DAC）セキュリティに関する情報の表示

ダイナミック アクセス制御セキュリティは、次のセキュリティ形式のFlexVol内のオブジェクトに適用できます。

- NTFS
- Mixed（オブジェクトにNTFS対応のセキュリティが設定されている場合）

関連情報

- Storage-Level Access Guard を使用した安全なファイルアクセスについて学習します
- サーバ上の Storage-Level Access Guard に関する情報を表示する

ONTAP SMBファイルセキュリティに関する情報をNTFSセキュリティ形式のボリューム上に表示します

セキュリティ形式と有効なセキュリティ形式、適用されている権限、DOS属性に関する情報など、NTFSセキュリティ形式のボリューム上にあるファイルやディレクトリのセキュリティに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、ファイル アクセスに関する問題のトラブルシューティングを行うことができます。

タスク概要

Storage Virtual Machine（SVM）の名前、およびファイルまたはフォルダのセキュリティ情報を表示するデータのパスを入力する必要があります。出力には要約または詳細な一覧を表示できます。

- NTFSセキュリティ形式のボリュームとqtreeでは、NTFSファイル権限およびWindowsのユーザとグループのみを使用してファイルのアクセス権を判断するため、UNIX関連の出力フィールドのUNIXファイル権限情報は表示のみです。
- ACL出力は、NTFSセキュリティが適用されたファイルとフォルダについて表示されます。
- ストレージレベルのアクセス保護セキュリティは、ボリュームのルートまたはqtreeで設定できるので、ストレージレベルのアクセス保護が設定されているボリュームまたはqtreeパスの出力には、通常のファイルACLとストレージレベルのアクセス保護ACLの両方が表示されることがあります。
- そのファイルまたはディレクトリ パスにダイナミック アクセス制御が設定されていれば、ダイナミック アクセス制御ACEに関する情報も出力に表示されます。

手順

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

情報を表示する場合...	入力するコマンド
要約形式	`vserver security file-directory show -vserver vserver_name -path path`
詳細	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

例

次の例では、SVM vs1 内のパス `/vol4`に関するセキュリティ情報を表示します：

```
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
```

次の例では、SVM vs1 内のパス `/data/engineering`に関する拡張マスク付きのセキュリティ情報を表示します：

```
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
```

次の例では、SVM vs1 内のパス `/datavol1`を持つボリュームのセキュリティ情報（ストレージレベルのアクセス ガードのセキュリティ情報を含む）を表示します：

```
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
```

関連情報

- mixedセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示
- UNIXセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示

混合セキュリティ形式のボリューム上のONTAP SMBファイルセキュリティに関する情報を表示します

セキュリティ形式と有効なセキュリティ形式、適用されている権限、UNIXの所有者とグループに関する情報など、mixedセキュリティ形式のボリューム上にあるファイルやディレクトリのセキュリティに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、ファイル アクセスに関する問題のトラブルシューティングを行うことができます。

タスク概要

Storage Virtual Machine（SVM）の名前、およびファイルまたはフォルダのセキュリティ情報を表示するデータのパスを入力する必要があります。出力には要約または詳細な一覧を表示できます。

- mixedセキュリティ形式のボリュームおよびqtreeは、UNIXファイル権限（モード ビットまたはNFSv4 ACL）を使用するファイルおよびフォルダと、NTFSファイル権限を使用するファイルおよびディレクトリを格納できます。
- mixedセキュリティ形式のボリュームの最上位には、UNIX対応のセキュリティまたはNTFS対応のセキュリティを設定できます。
- ACL出力は、NTFSまたはNFSv4セキュリティが適用されたファイルとフォルダについてのみ表示されます。

  このフィールドは、モード ビットの権限のみ（NFSv4 ACLはなし）が適用されているUNIXセキュリティ形式のファイルおよびディレクトリでは空になります。

- ACL出力の所有者とグループの出力フィールドは、NTFSセキュリティ記述子の場合にのみ適用されます。
- ストレージレベルのアクセス保護セキュリティは、たとえボリュームのルートまたはqtreeの有効なセキュリティ形式がUNIXでも、mixedセキュリティ形式のボリュームまたはqtreeで設定できるので、ストレージレベルのアクセス保護が設定されているボリュームまたはqtreeパスの出力には、UNIXファイル権限とストレージレベルのアクセス保護ACLの両方が表示されることがあります。
- コマンドで入力したパスが、NTFS対応のセキュリティを使用するデータへのパスである場合、そのファイルまたはディレクトリ パスにダイナミック アクセス制御が設定されていれば、ダイナミック アクセス制御ACEに関する情報も出力に表示されます。

手順

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

情報を表示する場合...	入力するコマンド
要約形式	`vserver security file-directory show -vserver vserver_name -path path`
詳細	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

例

次の例は、SVM vs1 内のパス `/projects`に関するセキュリティ情報を拡張マスク形式で表示します。この混合セキュリティ形式のパスは、UNIX 対応のセキュリティを備えています。

```
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: -
```

次の例は、SVM vs1 内のパス `/data`のセキュリティ情報を表示します。この混合セキュリティ形式のパスには、NTFS 対応のセキュリティが適用されます。

```
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
```

次の例は、SVM vs1のパス `/datavol5`にあるボリュームのセキュリティ情報を表示します。この混合セキュリティ形式のボリュームの最上位レベルには、UNIX対応のセキュリティが設定されています。このボリュームには、ストレージレベルのアクセス保護セキュリティが設定されています。

```
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
```

関連情報

- NTFSセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示
- UNIXセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示

UNIXセキュリティ形式のボリューム上のONTAP SMBファイル セキュリティに関する情報を表示します

セキュリティ形式と有効なセキュリティ形式、適用されている権限、UNIXの所有者とグ

ループに関する情報など、UNIXセキュリティ形式のボリューム上にあるファイルやディレクトリのセキュリティに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、ファイル アクセスに関する問題のトラブルシューティングを行うことができます。

タスク概要

Storage Virtual Machine（SVM）の名前、およびファイルまたはディレクトリのセキュリティ情報を表示するデータのパスを入力する必要があります。出力には要約または詳細な一覧を表示できます。

- ファイル権限の決定時、UNIXセキュリティ形式のボリュームおよびqtreeでは、UNIXファイル権限（モード ビットまたはNFSv4 ACL）のみが使用されます。
- ACL出力は、NFSv4セキュリティが適用されたファイルとフォルダについてのみ表示されます。

  このフィールドは、モード ビットの権限のみ（NFSv4 ACLはなし）が適用されているUNIXセキュリティ形式のファイルおよびディレクトリでは空になります。

- ACL出力の所有者とグループの出力フィールドは、NFSv4セキュリティ記述子には該当しません。

  これらのフィールドが意味があるのは、NTFSセキュリティ記述子の場合のみです。

- SVM に CIFS サーバが設定されている場合、UNIX ボリュームまたは qtree でストレージ レベルのアクセス ガード セキュリティがサポートされるため、出力には、 `-path`パラメータで指定されたボリュームまたは qtree に適用されたストレージ レベルのアクセス ガード セキュリティに関する情報が含まれることがあります。

手順

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

情報を表示する場合...	入力するコマンド
要約形式	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
詳細	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

例

次の例では、SVM vs1 内のパス `/home`に関するセキュリティ情報を表示します：

```
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: -
```

次の例では、SVM vs1 内のパス `/home`に関するセキュリティ情報を拡張マスク形式で表示します：

```
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: -
```

関連情報

- セキュリティ形式のボリューム上のファイルセキュリティに関する情報を表示します
- mixedセキュリティ形式のボリュームのファイル セキュリティに関する情報の表示

SMB FlexVol ボリューム上の NTFS 監査ポリシーに関する情報を表示する ONTAP コマンド

FlexVolボリューム上のNTFS監査ポリシーに関する情報（セキュリティ スタイルと有効なセキュリティ スタイル、適用されている権限、システム アクセス制御リストに関する情報など）を表示できます。この結果を使用して、セキュリティ構成の検証や監査に関する問題のトラブルシューティングを行うことができます。

タスク概要

Storage Virtual Machine（SVM）の名前と、監査情報を表示するファイルまたはディレクトリへのパスを指定する必要があります。出力には要約または詳細な一覧を表示できます。

- NTFSセキュリティ形式のボリュームおよびqtreeでは、NTFSのシステム アクセス制御リスト（SACL）のみが監査ポリシーに使用されます。
- NTFS対応のセキュリティが有効なmixedセキュリティ形式のボリューム内のファイルおよびフォルダには、NTFS監査ポリシーを適用できます。

  mixedセキュリティ形式のボリュームおよびqtreeは、UNIXファイル権限（モード ビットまたはNFSv4 ACL）を使用するファイルおよびディレクトリと、NTFSファイル権限を使用するファイルおよびディレクトリを格納できます。

- mixedセキュリティ形式のボリュームの最上位では、UNIXまたはNTFS対応のセキュリティを有効にすることができ、そこにはNTFS SACLが格納されている場合も、格納されていない場合もあります。
- mixedセキュリティ形式のボリュームまたはqtreeでは、ボリュームのルートまたはqtreeの有効なセキュリティ形式がUNIXであっても、ストレージレベルのアクセス保護セキュリティを設定できるため、ストレージレベルのアクセス保護が設定されているボリュームまたはqtreeの出力には、標準ファイルおよびフォルダのNFSv4 SACLとストレージレベルのアクセス保護のNTFS SACLの両方が表示される場合があります。
- コマンドで入力したパスが、NTFS対応のセキュリティを使用するデータへのパスである場合、そのファイルまたはディレクトリ パスにダイナミック アクセス制御が設定されていれば、ダイナミック アクセス制御ACEに関する情報も出力に表示されます。
- NTFS対応のセキュリティが有効なファイルおよびフォルダに関するセキュリティ情報の表示時には、UNIX関連の出力フィールドに表示専用のUNIXファイル アクセス権情報が格納されます。

  ファイル アクセス権の決定時には、NTFSセキュリティ形式のファイルおよびフォルダで、NTFSファイル アクセス権とWindowsユーザおよびグループのみが使用されます。

- ACL出力は、NTFSまたはNFSv4セキュリティが適用されたファイルとフォルダについてのみ表示されます。

  このフィールドは、モード ビットの権限のみ（NFSv4 ACLはなし）が適用されているUNIXセキュリティ形式のファイルおよびフォルダでは空になります。

- ACL出力の所有者とグループの出力フィールドは、NTFSセキュリティ記述子の場合にのみ適用されます。

手順

1. ファイルおよびディレクトリ監査ポリシー設定を適切な詳細レベルで表示します。

情報を表示する場合...	入力するコマンド
要約形式	`vserver security file-directory show -vserver vserver_name -path path`
詳細な一覧	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

例

次の例は、SVM vs1 内のパス `/corp`の監査ポリシー情報を表示します。パスには NTFS 有効セキュリティが設定されています。NTFS セキュリティ記述子には、SUCCESS と SUCCESS/FAIL の両方の SACL エントリが含まれています。

```
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
```

次の例は、SVM vs1 内のパス `/datavol1`の監査ポリシー情報を表示します。パスには、通常のファイルおよびフォルダの SACL と、ストレージレベルのアクセスガード SACL の両方が含まれています。

```
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
```

SMB FlexVol ボリューム上の NFSv4 監査ポリシーに関する情報を表示する ONTAP コマンド

ONTAP CLIを使用して、FlexVolボリューム上のNFSv4監査ポリシーに関する情報（セキュリティ形式と有効なセキュリティ形式、適用されている権限、システム アクセス制御リスト（SACL）に関する情報など）を表示できます。これらの結果を使用して、セキュリティ設定の検証や監査の問題のトラブルシューティングを行うことができます。

タスク概要

ストレージ仮想マシン（SVM）の名前と、監査情報を表示するファイルまたはディレクトリへのパスを指定する必要があります。出力は、概要形式または詳細リスト形式で表示できます。

- UNIX セキュリティ形式のボリュームと qtree は、監査ポリシーに NFSv4 SACL のみを使用します。
- UNIX セキュリティ スタイルの混合セキュリティ スタイル ボリューム内のファイルとディレクトリには、NFSv4 監査ポリシーを適用できます。

  mixedセキュリティ形式のボリュームおよびqtreeは、UNIXファイル権限（モード ビットまたはNFSv4 ACL）を使用するファイルおよびディレクトリと、NTFSファイル権限を使用するファイルおよびディレクトリを格納できます。

- 混合セキュリティ形式のボリュームの最上位レベルには、UNIX または NTFS の有効なセキュリティを設定でき、NFSv4 SACL が含まれる場合と含まれない場合があります。
- ACL出力は、NTFSまたはNFSv4セキュリティが適用されたファイルとフォルダについてのみ表示されます。

  このフィールドは、モード ビットの権限のみ（NFSv4 ACLはなし）が適用されているUNIXセキュリティ形式のファイルおよびフォルダでは空になります。

- ACL出力の所有者とグループの出力フィールドは、NTFSセキュリティ記述子の場合にのみ適用されます。
- ストレージ レベルのアクセス ガード セキュリティは、ボリューム ルートまたは qtree の有効なセキュリティ スタイルが UNIX であっても、混合セキュリティ スタイルのボリュームまたは qtree に設定できるため、ストレージ レベルのアクセス ガードが設定されているボリュームまたは qtree パスの出力には、通常の NFSv4 ファイルおよびディレクトリの SACL と、ストレージ レベルのアクセス ガードの NTFS SACL の両方が表示される場合があります。
- SVM に CIFS サーバが設定されている場合、UNIX ボリュームまたは qtree でストレージ レベルのアクセス ガード セキュリティがサポートされるため、出力には、 `-path`パラメータで指定されたボリュームまたは qtree に適用されたストレージ レベルのアクセス ガード セキュリティに関する情報が含まれることがあります。

手順

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

情報を表示する場合...	入力するコマンド
要約形式	`vserver security file-directory show -vserver vserver_name -path path`

情報を表示する場合...	入力するコマンド
詳細	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

例

次の例は、SVM vs1 内のパス `/lab`に関するセキュリティ情報を表示します。この UNIX セキュリティ形式のパスには、NFSv4 SACL があります。

```
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
```

ONTAP SMBファイルのセキュリティと監査ポリシー情報を表示する方法を学びます

ワイルドカード文字（*）を使用すると、特定のパスまたはルート ボリュームの下にあるすべてのファイルとディレクトリのファイル セキュリティと監査ポリシーに関する情報を表示できます。

ワイルドカード文字（）は、特定のディレクトリ パスの最後のサブコンポーネントとして使用でき、そのパス配下のすべてのファイルとディレクトリの情報を表示できます。「」という名前の特定のファイルまたはディレクトリの情報を表示する場合は、二重引用符（"``"）内に完全なパスを指定する必要があります。

例

ワイルドカード文字を使用した次のコマンドは、SVM vs1 のパス `/1/`の下にあるすべてのファイルとディレクトリに関する情報を表示します：

```
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)
```

次のコマンドは、SVM vs1のパス `/vol1/a`下にある「*」という名前のファイルの情報を表示します。パスは二重引用符（" "）で囲まれています。

```
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
```