ファイルおよびディレクトリに適用されている監査ポリシーに関する情報の表示

ONTAP 9

NetApp
February 12, 2026

目次

ファイルおよびディレクトリに適用されている監査ポリシーに関する情報の表示

Windows のセキュリティ タブにアクセスして ONTAP 監査ポリシー情報を表示

Windowsの[プロパティ]ウィンドウにある[セキュリティ]タブを使用して、ファイルやディレクトリに適用されている監査ポリシーに関する情報を表示できます。これはWindowsサーバ上に存在するデータを利用する場合と同じ方法であり、ユーザは使い慣れたものと同じGUIインターフェイスを使用できます。

タスク概要

ファイルやディレクトリに適用されている監査ポリシーに関する情報を表示すると、指定したファイルやフォルダに適切なシステム アクセス制御リスト（SACL）が設定されていることを確認できます。

NTFSファイルおよびフォルダに適用されているSACLに関する情報を表示するには、Windowsホストで以下の手順を実行します。

手順

1. エクスプローラの ツール メニューから、ネットワーク ドライブの割り当て を選択します。
2. ネットワーク ドライブの割り当て ダイアログ ボックスを完了します：
   a. *ドライブ*文字を選択します。
   b. フォルダ ボックスに、監査するデータと共有の名前の両方を保持する共有を含むStorage Virtual Machine（SVM）のIPアドレスまたはSMBサーバー名を入力します。

      SMB サーバー名が「`SMB_SERVER`」で、共有名が「`share1`」の場合は、 `\\SMB_SERVER\share1` と入力する必要があります。

      SMBサーバ名の代わりに、SMBサーバのデータ インターフェイスのIPアドレスを指定することもできます。

   c. *完了*をクリックします。

   選択したドライブがマウントされて使用可能な状態となり、共有内に格納されているファイルやフォルダがWindowsエクスプローラ ウィンドウに表示されます。
3. 監査情報を表示するファイルまたはディレクトリを選択します。
4. ファイルまたはディレクトリを右クリックし、*プロパティ*を選択します。
5. *セキュリティ*タブを選択します。
6. *Advanced*をクリックします。
7. *監査*タブを選択します。
8. *続行*をクリックします。

監査ボックスが開きます。*監査エントリ*ボックスには、SACLが適用されているユーザーとグループの概要が表示されます。

9. 監査エントリ ボックスで、SACL エントリを表示するユーザーまたはグループを選択します。
10. *編集*をクリックします。

    <object>ボックスの監査エントリが開きます。

11. アクセス ボックスで、選択したオブジェクトに適用されている現在の SACL を表示します。
12. **[**キャンセル**]** をクリックして、**<object>** の監査エントリ ボックスを閉じます。
13. *キャンセル*をクリックして*監査*ボックスを閉じます。

ONTAP 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

セキュリティ形式と有効なセキュリティ形式、適用されているアクセス権、システム アクセス制御リストに関する情報など、FlexVolのNTFS監査ポリシーに関する情報を表示できます。この情報を使用して、セキュリティ設定の検証や、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

ファイルやディレクトリに適用されている監査ポリシーに関する情報を表示すると、指定したファイルやフォルダに適切なシステム アクセス制御リスト（SACL）が設定されていることを確認できます。

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
```

ワイルドカード文字を使用して、ONTAPファイルのセキュリティと監査ポリシーに関する情報を表示します。

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、その下のすべてのファイルとディレクトリの情報が表示されます。

「*」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（" "）で囲んで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
```

著作権に関する情報

商標に関する情報