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を表示します

ONTAP 9

NetApp
April 24, 2024

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を表示します

Windows のセキュリティタブを使用して、監査ポリシーに関する情報を表示します

Windows のプロパティウィンドウのセキュリティタブを使用して、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を表示できます。これは Windows サーバ上に存在するデータの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。

このタスクについて

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 ホストで次の手順を実行します。

手順

1. Windows Explorer の * ツール * メニューから、 * ネットワークドライブのマップ * 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に入力します。
   a. ドライブ文字を選択します。
   b. [フォルダ]ボックスに、監査するデータが格納されている共有を含むStorage Virtual Machine（SVM）のIPアドレスまたはSMBサーバ名と、共有の名前を入力します。

      SMBサーバ名が「smb_server」で、共有の名前が「share1」の場合は、と入力します `\\SMB_SERVER\share1`。

      > 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になり、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. 「 * 詳細設定 * 」をクリックします。
7. [監査 *] タブを選択します。
8. [* Continue （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（ Edit ）] をクリックします。

    [< オブジェクト > の監査エントリ] ボックスが開きます。

11. [* アクセス * （ * Access * ）] 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、 [* 監査エントリ for < オブジェクト >*] 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。

CLI を使用して、 FlexVol 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。

このタスクについて

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、および監査情報を表示するファイルまたはフォルダのパスを指定する必要があります。出力は要約形式または詳細なリストで表示できます。

- 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 には、 UNIX ファイル権限、モードビットまたは NFSv4 ACL 、および NTFS ファイル権限を使用する一部のファイルおよびディレクトリを含めることができます。

- 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。
- 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 の有効なセキュリティ形式が UNIX であっても、 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 パスの出力には、通常の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を表示する場合、UNIX 関連の出力フィールドには表示専用の UNIX ファイル権限情報が格納されます。

  ファイルアクセス権の決定時、 NTFS セキュリティ形式のファイルおよびフォルダでは、 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、モードビットのアクセス権のみ（ 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。

ステップ

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

表示する情報	入力するコマンド
要約形式で表示されます	`vserver security file-directory show -vserver vserver_name -path path`
詳細なリストとして	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

例

次の例は、パスの監査ポリシーの情報を表示します `/corp` （SVM vs1）。パスで NTFS 対応のセキュリティが有効になっています。NTFS セキュリティ記述子には、 SUCCESS および SUCCESS/FAIL SACL エントリの両方が含まれています。

```
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、パスの監査ポリシーの情報を表示します `/datavol1` （SVM vs1）。このパスには、標準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保護の SACL の両方が格納されています。

```
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
```

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する方法

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および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、すべてのファイルおよびディレクトリの情報を表示する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、パス全体を二重引用符（ "" ）で囲む必要があります。

例

次のコマンドにワイルドカード文字を指定すると、パス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が表示されます `/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)
```

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

```
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
```