



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.....	1
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.....	1
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.....	2
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.....	6

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せん。

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	<code>vserver security file-directory show -vserver vserver_name -path path</code>
詳細なリストとして	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

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
```

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。