CLIを使用した監査ポリシーの設定とNTFSファイルおよびフォルダへの適用

ONTAP 9

NetApp
December 20, 2024

目次

CLIを使用した監査ポリシーの設定とNTFSファイルおよびフォルダへの適用

CLIの概要を使用したNTFSファイルおよびフォルダへの監査ポリシーの設定と適用

ONTAP CLIを使用してNTFSファイルおよびフォルダに監査ポリシーを適用するには、いくつかの手順を実行する必要があります。まず、NTFSセキュリティ記述子を作成し、そのセキュリティ記述子にSACLを追加します。次に、セキュリティポリシーを作成し、ポリシータスクを追加します。その後、そのセキュリティポリシーをStorage Virtual Machine（SVM）に適用します。

タスクの内容

セキュリティポリシーを適用したら、セキュリティポリシージョブを監視し、適用した監査ポリシーの設定を確認できます。

監査ポリシーと関連するSACLを適用すると、既存のDACLが上書きされます。新しいセキュリティポリシーを作成して適用する前に、既存のセキュリティポリシーを確認する必要があります。

関連情報

ストレージレベルのアクセス保護を使用したファイルアクセスの保護

CLIを使用してファイルおよびフォルダのセキュリティを設定する場合の制限事項

セキュリティ記述子を使用したファイルおよびフォルダのセキュリティの適用方法

"SMBおよびNFSの監査とセキュリティトレース"

CLIを使用したNTFSファイルおよびフォルダに対するファイルセキュリティの設定と適用

NTFSセキュリティ記述子を作成します。

NTFS セキュリティ記述子監査ポリシーの作成は、 SVM 内のファイルやフォルダの NTFS Access Control List （ ACL ；アクセス制御リスト）を設定および適用するための最初のステップです。このセキュリティ記述子をポリシータスクでファイルパスまたはフォルダパスに関連付けます。

タスクの内容

NTFS セキュリティ形式のボリューム内に存在するファイルやフォルダ、または mixed セキュリティ形式のボリューム上に存在するファイルやフォルダに対して、 NTFS セキュリティ記述子を作成できます。

デフォルトでは、セキュリティ記述子を作成すると、 Discretionary Access Control List （ DACL ；随意アクセス制御リスト）の 4 つの Access Control Entry （ ACE ；アクセス制御エントリ）がそのセキュリティ記述子に追加されます。4つのデフォルトACEは次のとおりです。

オブジェクト	アクセスタイプ	アクセス権	権限の適用先
組み込み\管理者	許可	フルコントロール	このフォルダ、サブフォルダ、ファイル
組み込み\ユーザ	許可	フルコントロール	このフォルダ、サブフォルダ、ファイル
作成者所有者	許可	フルコントロール	このフォルダ、サブフォルダ、ファイル
NT AUTHORITY\SYSTEM	許可	フルコントロール	このフォルダ、サブフォルダ、ファイル

次のオプションのパラメータを使用して、セキュリティ記述子の設定をカスタマイズできます。

- セキュリティ記述子の所有者
- 所有者のプライマリグループ
- raw 制御フラグ

オプションのパラメータの値はストレージレベルのアクセス保護では無視されます。詳細については、マニュアルページを参照してください。

手順

1. advancedパラメータを使用する場合は、権限レベルをadvancedに設定します。 `set -privilege advanced`
2. セキュリティ記述子を作成します。 `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

   ```
   vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe
   ```

3. セキュリティ記述子の設定が正しいことを確認します。 `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

   ```
   vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
   ```

   ```
                                   Vserver: vs1
                         Security Descriptor Name: sd1
                    Owner of the Security Descriptor: DOMAIN\joe
   ```

4. advanced権限レベルの場合は、admin権限レベルに戻ります。 `set -privilege admin`

NTFSセキュリティ記述子へのNTFS SACLアクセス制御エントリの追加

NTFS セキュリティ記述子への SACL （システムアクセス制御リスト）アクセス制御エントリ（ ACE ）の追加は、 SVM 内のファイルやフォルダに対する NTFS 監査ポリシーを作成する 2 番目のステップです。エントリごとに、監査するユーザまたはグループを指定します。SACL エントリは、成功したアクセス試行と失敗したアクセス試行のどちらを監査するかを定義します。

タスクの内容

セキュリティ記述子のSACLには1つ以上のACEを追加できます。

セキュリティ記述子に含まれるSACLに既存のACEがある場合は、新しいACEがSACLに追加されます。セキュリティ記述子にSACLが含まれていない場合は、SACLが作成されて新しいACEが追加されます。

SACLエントリを設定するには、パラメータで指定したアカウントの成功イベントまたは失敗イベントについて監査する権限を指定し `-account`ます。権限を指定する場合、次の 3 つの相互に排他的な方法があります。

- 権限
- 詳細な権限
- raw 権限（ advanced 権限）

SACLエントリの権限を指定しない場合のデフォルト設定はです `Full Control`。

必要に応じて、パラメータで継承を適用する方法を指定して、SACLエントリをカスタマイズでき `apply to`ます。このパラメータを指定しない場合、デフォルトでは、この SACL エントリがこのフォルダ、サブフォルダ、およびファイルに適用されます。

手順

1. SACLエントリをセキュリティ記述子に追加します。 `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type
   failure -account domain\joe -rights full-control -apply-to this-folder
   -vserver vs1
   ```

2. SACLエントリが正しいことを確認します。 `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

```
                                Vserver: vs1
                    Security Descriptor Name: sd1
Access type for Specified Access Rights: failure
                        Account Name or SID: DOMAIN\joe
                              Access Rights: full-control
                     Advanced Access Rights: -
                                   Apply To: this-folder
                              Access Rights: full-control
```

セキュリティポリシーを作成する

Storage Virtual Machine （ SVM ）の監査ポリシーの作成は、ファイルまたはフォルダに対して ACL を設定および適用する 3 番目のステップです。ポリシーは、さまざまなタスクのコンテナとして機能します。各タスクは、ファイルまたはフォルダに適用できる単一のエントリです。あとで、このセキュリティポリシーにタスクを追加できます。

タスクの内容

セキュリティポリシーに追加するタスクには、 NTFS セキュリティ記述子とファイルパスまたはフォルダパスとの間の関連付けが含まれます。そのため、セキュリティポリシーは、NTFSセキュリティ形式のボリュームまたはmixedセキュリティ形式のボリュームを含むStorage Virtual Machine（SVM）ごとに関連付ける必要があります。

手順

1. セキュリティポリシーを作成します。 `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. セキュリティポリシーを確認します。 `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver           Policy Name
 ------------      --------------
     vs1               policy1
```

セキュリティポリシーにタスクを追加する

ACL を設定し、 SVM 内のファイルやフォルダへ適用する 4 番目のステップでは、ポリシータスクを作成してセキュリティポリシーに追加します。ポリシータスクを作成するときに、セキュリティポリシーとタスクを関連付けます。セキュリティポリシーには、 1 つ以上のタスクエントリを追加できます。

タスクの内容

セキュリティポリシーはタスクのコンテナです。タスクとは、 NTFS または mixed セキュリティが設定されたファイルまたはフォルダ（ストレージレベルのアクセス保護を設定する場合はボリュームオブジェクト）へのセキュリティポリシーによって実行できる単一の処理を指します。

タスクには次の2種類があります。

- ファイルとディレクトリのタスク

  指定されたファイルやフォルダにセキュリティ記述子を適用するタスクの指定に使用します。ファイルとディレクトリのタスクによって適用される ACL は、 SMB クライアントまたは ONTAP CLI で管理できます。

- ストレージレベルのアクセス保護タスク

  指定されたボリュームにストレージレベルのアクセス保護のセキュリティ記述子を適用するタスクの指定に使用します。ストレージレベルのアクセス保護タスクで適用される ACL は ONTAP CLI からのみ管理できます。

タスクには、ファイル（またはフォルダ）やファイルセット（またはフォルダセット）のセキュリティ構成の定義が含まれています。ポリシー内のすべてのタスクは、一意のパスによって識別されます。1 つのポリシー内の 1 つのパスに含められるのは 1 つのタスクだけです。ポリシーに重複するタスクエントリを含めることはできません。

ポリシーへのタスクの追加に関するガイドラインを次に示します。

- ポリシーあたりのタスクエントリは最大 10 、 000 個です。
- ポリシーには 1 つ以上のタスクを含めることができます。

  ポリシーには複数のタスクを含めることができますが、ポリシーにファイルとディレクトリのタスクとストレージレベルのアクセス保護タスクの両方を含めることはできません。ポリシーに含めるタスクは、すべてストレージレベルのアクセス保護タスクにするか、すべてファイルとディレクトリのタスクにする必要があります。

- ストレージレベルのアクセス保護は、権限の制限に使用します。

  アクセス権限は付与されません。

次のオプションのパラメータを使用して、セキュリティ記述子の設定をカスタマイズできます。

- セキュリティタイプ
- プロパゲーションモード
- インデックス位置
- アクセス制御の種類

オプションのパラメータの値はストレージレベルのアクセス保護では無視されます。詳細については、マニュアルページを参照してください。

手順

1. セキュリティ記述子が関連付けられているタスクをセキュリティポリシーに追加します。 `vserver`

```
security file-directory policy task add -vserver vserver_name -policy-name
policy_name -path path -ntfs-sd SD_nameoptional_parameters
```

`file-directory`は、パラメータのデフォルト値 `-access-control`です。ファイルとディレクトリのアクセスタスクを設定する場合、アクセス制御の種類の指定は任意です。

```
vserver security file-directory policy task add -vserver vs1 -policy-name
policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
-index-num 1 -access-control file-directory
```

2. ポリシータスクの設定を確認します。 `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

```
vserver security file-directory policy task show
```

```
Vserver: vs1
Policy: policy1

Index    File/Folder    Access           Security   NTFS       NTFS
Security
         Path           Control          Type       Mode
Descriptor Name
-----    --------       -----------      --------   ------
----------------
1        /home/dir1     file-directory   ntfs       propagate  sd2
```

セキュリティポリシーを適用する

SVMへの監査ポリシーの適用は、ファイルまたはフォルダに対してNTFS ACLを作成および適用する最後のステップです。

タスクの内容

セキュリティポリシーで定義されたセキュリティ設定を、FlexVolボリューム（NTFSまたはmixedセキュリティ形式）内に存在するNTFSファイルおよびフォルダに適用できます。

> 監査ポリシーと関連するSACLを適用すると、既存のDACLが上書きされます。セキュリティポリシーとそれに関連付けられたDACLが適用されると、既存のDACLはすべて上書きされます。新しいセキュリティポリシーを作成して適用する前に、既存のセキュリティポリシーを確認する必要があります。

ステップ

1. セキュリティポリシーを適用します。 `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

ポリシー適用ジョブがスケジュールされ、ジョブIDが返されます。

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
53322" command to view the status of the operation
```

セキュリティポリシージョブを監視する

Storage Virtual Machine （ SVM ）にセキュリティポリシーを適用する場合、セキュリティポリシージョブを監視してその進行状況を監視できます。これは、セキュリティポリシーの適用が成功したかどうかを確認するのに役立ちます。また、多数のファイルやフォルダに一括してセキュリティ設定を適用するような長時間のジョブを実行する場合にも、この方法が便利です。

タスクの内容

セキュリティポリシージョブに関する詳細情報を表示するには、パラメータを使用し `-instance`ます。

ステップ

1. セキュリティポリシージョブを監視します。 `vserver security file-directory job show -vserver vserver_name`

```
vserver security file-directory job show -vserver vs1
```

```
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
53322  Fsecurity Apply      vs1        node1          Success
       Description: File Directory Security Apply Job
```

適用された監査ポリシーの確認

Storage Virtual Machine （ SVM ）のファイルやフォルダにセキュリティポリシーを適用した場合に、それらの監査セキュリティの設定が意図したとおりになっているかを確認するには、監査ポリシーを確認します。

タスクの内容

監査ポリシーの情報を表示するには、コマンドを使用し `vserver security file-directory show`ます。データが格納されている SVM の名前、およびファイルまたはフォルダの監査ポリシーの情報を表示するデータのパスを指定する必要があります。

ステップ

1. 監査ポリシーの設定を表示します。 `vserver security file-directory show -vserver vserver_name -path path`

例

次のコマンドは、 SVM vs1 のパス「 `/corp` 」に適用されている監査ポリシーの情報を表示します。このパスには、 SUCCESS と SUCCESS/FAIL SACL の両方のエントリが適用されています。

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

                Vserver: vs1
              File Path: /corp
         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
```

著作権に関する情報

商標に関する情報