CLIを使用したSVMのNTFSファイルセキュリティ、NTFS監査ポリシー、ストレージレベルのアクセス保護の管理

ONTAP 9

NetApp
February 12, 2026

目次

CLIを使用したSVMのNTFSファイル セキュリティ、NTFS監査ポリシー、ストレージレベルのアクセス保護の管理

SMB NTFSファイルセキュリティ、NTFS監査ポリシー、Storage-Level Access Guardを管理するためのONTAPコマンド

CLIを使用して、Storage Virtual Machine（SVM）のNTFSファイル セキュリティ、NTFS監査ポリシー、ストレージレベルのアクセス保護を管理できます。

NTFSファイル セキュリティと監査ポリシーは、SMBクライアントから、またはCLIを使用して管理できます。ただし、CLIを使用してファイル セキュリティと監査ポリシーを設定する場合、リモート クライアントを使用せずにファイル セキュリティを管理できます。CLIを使用すると、多数のファイルやフォルダに対してセキュリティを適用する場合でも1つのコマンドで実行できるため、作業時間を大幅に短縮できます。

ONTAPがSVMボリュームに提供するもう1つのセキュリティ レイヤであるストレージレベルのアクセス保護を設定できます。ストレージレベルのアクセス保護は、すべてのNASプロトコルからストレージレベルのアクセス保護が適用されるストレージ オブジェクトへのアクセスに適用されます。

ストレージレベルのアクセス保護はONTAP CLIからのみ設定および管理できます。ストレージレベルのアクセス保護設定をSMBクライアントから管理することはできません。さらに、NFSやSMBクライアントからファイルまたはディレクトリのセキュリティ設定を表示した場合、ストレージレベルのアクセス保護のセキュリティは表示されません。システム（WindowsまたはUNIX）管理者であっても、ストレージレベルのアクセス保護セキュリティをクライアントから取り消すことはできません。そのため、ストレージレベルのアクセス保護は、ストレージ管理者が独立して設定および管理できるセキュリティ レイヤをデータ アクセスに追加で提供します。

ストレージレベルのアクセス保護ではNTFSのアクセス権のみがサポートされます。ただし、ストレージレベルのアクセス保護が適用されているボリューム上のデータへのNFS経由のアクセスに対しても、そのボリュームを所有するSVM上のWindowsユーザにUNIXユーザがマッピングされている場合は、ONTAPでセキュリティ チェックを実行できます。

NTFSセキュリティ形式のボリューム

NTFSセキュリティ形式のボリュームおよびqtreeに含まれるすべてのファイルとフォルダには、NTFS対応のセキュリティが適用されます。 `vserver security file-directory`コマンドファミリを使用して、NTFSセキュリティ形式のボリュームに以下の種類のセキュリティを実装できます：

- ボリュームに含まれるファイルやフォルダに対するファイル権限と監査ポリシー
- ボリュームに対するストレージレベルのアクセス保護セキュリティ

mixedセキュリティ形式のボリューム

混合セキュリティ形式のボリュームおよびqtreeには、UNIX対応セキュリティが適用され、UNIXファイル権限（モードビットまたはNFSv4.x ACLとNFSv4.x監査ポリシーのいずれか）を使用するファイルとフォルダ、およびNTFS対応セキュリティが適用され、NTFSファイル権限と監査ポリシーを使用するファイルとフォルダ

が含まれる場合があります。 `vserver security file-directory`コマンドファミリーを使用して、混合セキュリティ形式のデータに以下の種類のセキュリティを適用できます：

- mixed形式のボリュームやqtreeでのNTFS対応のセキュリティ形式のファイルおよびフォルダに対するファイル権限と監査ポリシー
- NTFS対応またはUNIX対応のセキュリティ形式のボリュームに対するストレージレベルのアクセス保護

UNIXセキュリティ形式のボリューム

UNIXセキュリティ形式のボリュームとqtreeには、UNIX対応セキュリティ（モードビットまたはNFSv4.x ACL）が設定されたファイルとフォルダが含まれます。 `vserver security file-directory`コマンドファミリを使用してUNIXセキュリティ形式のボリュームにセキュリティを実装する場合は、以下の点に留意してください：

- `vserver security file-directory`コマンド ファミリは、UNIXセキュリティ形式のボリュームおよびqtree上のUNIXファイル セキュリティおよび監査ポリシーの管理には使用できません。
- `vserver security file-directory`コマンド ファミリを使用して、ターゲット ボリュームを持つ SVM に CIFS サーバが含まれている場合、UNIX セキュリティ形式のボリュームにストレージ レベルのアクセス ガードを設定できます。

関連情報

- ファイルのセキュリティと監査ポリシーの表示について学習する
- サーバーに NTFS セキュリティ記述子を作成する
- ファイルとフォルダに監査ポリシーを設定および適用するためのコマンド
- 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

SMBファイルとフォルダのセキュリティを設定するためのONTAPコマンド

リモート クライアントを介さずにファイルとフォルダーのセキュリティをローカルで適用および管理できるため、多数のファイルやフォルダーに一括してセキュリティを設定するのにかかる時間を大幅に短縮できます。

次のユースケースでは、CLI を使用してファイルとフォルダーのセキュリティを設定すると便利です：

- ホームディレクトリ内のファイルストレージなど、大規模なエンタープライズ環境でのファイルのストレージ
- データの移行
- Windowsドメインの変更
- NTFS ファイルシステム全体にわたるファイルセキュリティと監査ポリシーの標準化

ONTAPコマンドを使用してSMBファイルとフォルダのセキュリティを設定する際の制限について学習します

ファイルおよびフォルダのセキュリティ設定でCLIを使用する際には、一定の制限事項を

知っておく必要があります。

- `vserver security file-directory`コマンド ファミリはNFSv4 ACLの設定をサポートしていません。

  NTFSのセキュリティ記述子はNTFSファイルとNTFSフォルダにのみ適用できます。

セキュリティ記述子を使用して **ONTAP SMB** ファイルおよびフォルダのセキュリティを適用する

セキュリティ記述子には、ユーザがファイルやフォルダに対して実行できる操作、およびユーザがファイルやフォルダにアクセスするときに監査される内容を決定するアクセス制御リストが含まれます。

- 権限

  権限はオブジェクトの所有者によって許可または拒否され、オブジェクト（ユーザ、グループ、またはコンピュータ オブジェクト）が指定されたファイルまたはフォルダに対して実行できる操作を決定します。

- セキュリティ記述子

  セキュリティ記述子は、ファイルまたはフォルダに関連付けられた権限を定義するセキュリティ情報を含むデータ構造です。

- アクセス制御リスト（**ACL**）

  アクセス制御リストは、セキュリティ記述子内に含まれるリストです。セキュリティ記述子が適用されるファイルまたはフォルダに対してユーザ、グループ、またはコンピュータ オブジェクトが実行できる操作に関する情報が含まれます。セキュリティ記述子には、次の2種類のACLを含めることができます。

  - 任意アクセス制御リスト（DACL）
  - システム アクセス制御リスト（SACL）

- 任意アクセス制御リスト（**DACL**）

  DACLには、ユーザ、グループ、およびコンピュータ オブジェクトのSIDリストと、ファイルまたはフォルダに対する操作アクセスの許可または拒否設定が含まれています。DACLには、0個以上のアクセス制御エントリ（ACE）が含まれます。

- システム アクセス制御リスト（**SACL**）

  SACLには、成功または失敗した監査イベントがログに記録されるユーザ、グループ、およびコンピュータ オブジェクトのSIDリストが含まれます。SACLには、0個以上のアクセス制御エントリ（ACE）が含まれます。

- **Access Control Entries**（**ACE**）

  ACEは、DACLまたはSACL内の個々のエントリです。

  - DACL アクセス制御エントリは、特定のユーザー、グループ、またはコンピューター オブジェクトに対して許可または拒否されるアクセス権を指定します。

- SACL アクセス制御エントリは、特定のユーザー、グループ、またはコンピューター オブジェクトによって実行された指定されたアクションを監査するときにログに記録する成功イベントまたは失敗イベントを指定します。

- 権限の継承

  権限の継承とは、セキュリティ記述子で定義された権限が親オブジェクトからオブジェクトにどのように伝播されるかを表します。継承可能な権限のみが子オブジェクトに継承されます。親オブジェクトの権限を設定する際に、「`Apply to `this-folder sub-folders、および files`」を使用して、フォルダ、サブフォルダ、およびファイルに権限を継承するかどうかを指定できます。

関連情報

- "SMBおよびNFS監査とセキュリティトレース"
- ファイルとフォルダに監査ポリシーを設定および適用するためのコマンド

ONTAP SVMディザスタリカバリデスティネーションでローカルSMBユーザまたはグループを使用するファイルディレクトリポリシーの適用について説明します

ファイルとディレクトリのポリシー設定がセキュリティ記述子、DACL、SACLエントリのいずれかでローカル ユーザまたはグループを使用する場合、ID破棄設定のStorage Virtual Machine（SVM）ディザスタ リカバリ デスティネーションでファイルとディレクトリのポリシーを適用する前に注意すべきいくつかのガイドラインがあります。

ソース クラスタ上のソース SVM がソース SVM からデスティネーション クラスタ上のデスティネーション SVM にデータと設定をレプリケートする SVM のディザスタ リカバリ設定を構成できます。

次の 2 種類の SVM ディザスタ リカバリのいずれかを設定できます。

- IDの保持

  この構成では、SVM と CIFS サーバのアイデンティティが保持されます。

- ID を破棄しました

  この設定では、SVMとCIFSサーバのIDは保持されません。このシナリオでは、デスティネーション SVM上のSVMとCIFSサーバの名前は、ソース SVM上のSVMとCIFSサーバの名前と異なります。

ID破棄設定のガイドライン

ID破棄設定において、ローカルユーザ、グループ、および権限設定を含むSVMソースの場合、ローカルドメイン名（ローカルCIFSサーバ名）をSVMデスティネーションのCIFSサーバ名と一致するように変更する必要があります。たとえば、ソースSVM名が「vs1」、CIFSサーバ名が「CIFS1」、デスティネーションSVM名が「vs1_dst」、CIFSサーバ名が「CIFS1_DST」の場合、「CIFS1\user1」というローカルユーザのローカルドメイン名は、デスティネーションSVM上で自動的に「CIFS1_DST\user1」に変更されます：

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1          CIFS1\Administrator                     Built-in
administrator account
vs1          CIFS1\user1              -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1_dst      CIFS1_DST\Administrator                 Built-in
administrator account
vs1_dst      CIFS1_DST\user1          -              -
```

ローカル ユーザおよびグループ データベースではローカル ユーザ名とグループ名が自動的に変更されますが、ファイル ディレクトリ ポリシー設定（`vserver security file-directory`コマンド ファミリを使用してCLIで設定されるポリシー）ではローカル ユーザ名またはグループ名は自動的に変更されません。

たとえば、「`vs1`」の場合、 `-account`パラメータが「`CIFS1\user1`」に設定されたDACLエントリを設定した場合、デスティネーションSVMの設定はデスティネーションのCIFSサーバ名を反映するように自動的に変更されません。

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

`vserver security file-directory modify`コマンドを使用して、CIFSサーバ名をデスティネーションCIFSサーバ名に手動で変更する必要があります。

アカウント パラメータを含むファイル ディレクトリ ポリシー設定コンポーネント

ローカル ユーザーまたはグループを含めることができるパラメーター設定を使用できるファイル ディレクトリ ポリシー構成コンポーネントは 3 つあります：

- セキュリティ記述子

  オプションで、セキュリティ記述子の所有者と、その所有者のプライマリ グループを指定できます。セキュリティ記述子で所有者およびプライマリ グループのエントリにローカル ユーザまたはグループが使用されている場合は、アカウント名にデスティネーション SVMを使用するようにセキュリティ記述子を変更する必要があります。 `vserver security file-directory ntfs modify`コマンドを使用して、アカウント名に必要な変更を加えることができます。

- DACLエントリ

  各 DACL エントリはアカウントに関連付ける必要があります。ローカル ユーザまたはグループ アカウントを使用する DACL は、デスティネーション SVM 名を使用するように変更する必要があります。既存の DACL エントリのアカウント名を変更することはできないため、ローカル ユーザまたはグループを含む DACL エントリをセキュリティ記述子から削除し、修正したデスティネーション アカウント名で新しい DACL エントリを作成し、これらの新しい DACL エントリを適切なセキュリティ記述子に関連付ける必要があります。

- SACLエントリ

  各 SACL エントリはアカウントに関連付ける必要があります。ローカル ユーザまたはグループ アカウントを使用する SACL は、デスティネーション SVM 名を使用するように変更する必要があります。既存の SACL エントリのアカウント名を変更することはできないため、ローカル ユーザまたはグループを含む SACL エントリをセキュリティ記述子から削除し、修正されたデスティネーション アカウント名で新しい SACL エントリを作成し、これらの新しい SACL エントリを適切なセキュリティ記述子に関連付ける必要があります。

ポリシーを適用する前に、ファイル ディレクトリ ポリシー構成で使用されるローカル ユーザーまたはグループに必要な変更を加える必要があります。変更を行わないと、適用ジョブは失敗します。

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および適用

ONTAP SMBサーバにNTFSセキュリティ記述子を作成する

NTFSセキュリティ記述子（ファイル セキュリティ ポリシー）の作成は、Storage Virtual Machine（SVM）内のファイルとフォルダにNTFSアクセス制御リスト（ACL）を設定して適用するための最初のステップです。ポリシー タスクで、セキュリティ記述子をファイルまたはフォルダのパスに関連付けることができます。

タスク概要

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、または混在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が作成されると、そのセキュリティ記述子に4つの随意アクセス制御リスト（DACL）アクセス制御エントリ（ACE）が追加されます。4つのデフォルトのACEは次のとおりです：

オブジェクト	アクセス タイプ	権限	権限の適用先
BUILTIN\Administrators	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
BUILTIN\Users	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
CREATOR OWNER	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 パラメータを使用して、セキュリティ記述子の構成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

ストレージレベルのアクセス保護では、オプションパラメータの値は無視されます。詳細については、"ONTAPコマンド リファレンス"をご覧ください。

ONTAP SMBサーバ上のNTFSセキュリティ記述子にNTFS DACLアクセス制御エントリを追加する

NTFSセキュリティ記述子にDACL（随意アクセス制御リスト）アクセス制御エントリ（ACE）を追加することは、ファイルまたはフォルダにNTFS ACLを設定および適用するための2番目のステップです。各エントリは、アクセスを許可または拒否するオブジェクトを識別し、ACEで定義されたファイルまたはフォルダに対してオブジェクトが実行できる操作と実行できない操作を定義します。

タスク概要

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

`_
account`パラメータで指定されたアカウントに対して許可または拒否する権限を指定することで、必要に応じてDACLエントリをカスタマイズできます。権限を指定するには、相互に排他的な3つの方法があります：

- 権限
- 高度な権利
- Raw 権限（advanced-privilege）

DACL エントリの権限を指定しない場合は、デフォルトで権限が `Full Control`に設定されます。

継承を適用する方法を指定して、必要に応じて DACL エントリをカスタマイズできます。

ストレージレベルのアクセス保護では、オプションパラメータの値は無視されます。この手順で説明されているコマンドの詳細については、"ONTAPコマンド リファレンス"を参照してください。

手順

1. セキュリティ記述子に DACL エントリを追加します `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

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

2. DACL エントリが正しいことを確認します：`vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

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

   ```
                   Vserver: vs1
   Security Descriptor Name: sd1
             Allow or Deny: deny
       Account Name or SID: DOMAIN\joe
             Access Rights: full-control
     Advanced Access Rights: -
                  Apply To: this-folder
             Access Rights: full-control
   ```

`vserver security file-directory ntfs dacl`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+security+file-directory+ntfs+dacl["ONTAPコマンド リファレンス"^]をご覧ください。

ONTAP SMBセキュリティ ポリシーを作成する

SVMのファイル セキュリティ ポリシーの作成は、ファイルまたはフォルダにACLを設定および適用するための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、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。セキュリティ ポリシーには後からタスクを追加できます。

タスク概要

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またはフォルダのパスと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を各SVM（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）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
```

ONTAP SMB セキュリティ ポリシーにタスクを追加する

ポリシー タスクを作成してセキュリティ ポリシーに追加することは、SVM 内のファイルまたはフォルダに ACL を設定して適用するための 4 番目の手順です。ポリシー タスクを作成すると、そのタスクをセキュリティ ポリシーに関連付けます。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。

タスク概要

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、セキュリティ ポリシーによって NTFS または混合セキュリティのファイルまたはフォルダ（または Storage-Level Access Guard を設定している場合はボリューム オブジェクト）に対して実行できる単一の操作を指します。

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とフォルダにセキュリティ記述子を適用するタスクを指定するために使用されます。ファイルおよびディレクトリタスクを通じて適用されたACLは、SMBクライアントまたはONTAP CLIを使用して管理できます。

- Storage-Level Access Guard 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セキュリティ記述子を適用するタスクを指定するために使用されます。ストレージレベルのアクセス保護タスクを通じて適用されたACLは、ONTAP CLIを通じてのみ管理できます。

タスクには、ファイル（またはフォルダ）またはファイルセット（またはフォルダ）のセキュリティ設定の定義が含まれます。ポリシー内の各タスクは、パスによって一意に識別されます。1つのポリシー内では、パスごとに1つのタスクのみを設定できます。ポリシー内に重複するタスクエントリを設定することはできません。

ポリシーにタスクを追加するためのガイドライン：

- ポリシーごとに最大 10,000 件のタスク エントリが可能です。
- 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、ファイル / ディレクトリ タスクとStorage-Level Access Guardタスクの両方を含むポリシーを設定することはできません。ポリシーには、すべてのStorage-Level Access Guardタスク、またはすべてのファイル / ディレクトリ タスクのいずれかを含める必要があります。

- Storage-Level Access Guard は、アクセス許可を制限するために使用されます。

  追加のアクセス権限を与えることはありません。

セキュリティ ポリシーにタスクを追加するときは、次の 4 つの必須パラメータを指定する必要があります：

- SVM名
- ポリシー名
- パス
- パスに関連付けるセキュリティ記述子

次のオプション パラメータを使用して、セキュリティ記述子の構成をカスタマイズできます：

- セキュリティ タイプ
- 伝播モード
- インデックス位置
- アクセス制御の種類

ストレージレベルのアクセス保護では、オプションパラメータの値は無視されます。この手順で説明されているコマンドの詳細については、"ONTAPコマンド リファレンス"を参照してください。

手順

1. 関連付けられたセキュリティ記述子を持つ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 `-access-control`パラメータのデフォルト値です。ファイルおよびディレクトリ アクセス タスクを構成する際にアクセス制御の種類を指定することはオプションです。

   ```
   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 タスクの構成を確認します： `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
   ```

   `vserver security file-directory policy task`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+security+file-directory+policy+task["ONTAPコマンド リファレンス"^]をご覧ください。

ONTAP SMB セキュリティ ポリシーを適用する

ファイル セキュリティ ポリシーを SVM に適用することは、NTFS ACL を作成してファイルまたはフォルダに適用する最後の手順です。

タスク概要

セキュリティ ポリシーに定義されているセキュリティ設定を、FlexVol（NTFSまたはmixedセキュリティ形式）内の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は上書きされます。セキュリティ ポリシーと関連するDACLを適用すると、既存のDACLは上書きされます。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 ポリシーを確認してください。

手順

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`

   ポリシーを適用する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
   ```

ONTAP SMBセキュリティ ポリシー ジョブを監視する

ストレージ仮想マシン（SVM）にセキュリティ ポリシーを適用する際、セキュリティ ポリシー ジョブを監視することでタスク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場合に役立ちます。また、多数のファイルやフォルダに一括でセキュリティを適用する、実行時間が長いジョブがある場合にも役立ちます。

タスク概要

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、 `-instance` パラメータを使用する必要があります。

手順

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
   ```

ONTAP SMBファイルのセキュリティを確認する

ファイルセキュリティ設定を検証して、セキュリティポリシーを適用したStorage Virtual Machine（SVM）上のファイルまたはフォルダに必要な設定がされているかどうかを確認できます。

タスク概要

データが格納されているSVMの名前と、セキュリティ設定を確認するファイルおよびフォルダへのパスを指定する必要があります。オプションの `-expand-mask`パラメータを使用すると、セキュリティ設定の詳細情報を表示できます。

手順

1. ファイルとフォルダのセキュリティ設定を表示： `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

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

CLIを使用したNTFSファイルおよびフォルダに対する監査ポリシーの設定および適用

NTFS ファイルとフォルダに SMB 監査ポリシーを設定して適用するための ONTAP コマンド

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、SACLをセキュリティ記述子に追加します。次に、セキュリティ ポリシーを作成してポリシー タスクを追加します。その後、Storage Virtual Machine（SVM）にセキュリティ ポリシーを適用します。

タスク概要

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 ジョブを監視して、適用した監査ポリシーの設定を確認することができます。

監査ポリシーと関連するSACLを適用すると、既存のDACLは上書きされます。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 ポリシーを確認してください。

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
- コマンドを使用してSMBファイルとフォルダのセキュリティを設定する際の制限について学習します
- セキュリティ記述子を使用してファイルとフォルダのセキュリティを適用する
- "SMBおよびNFS監査とセキュリティトレース"
- サーバーに NTFS セキュリティ記述子を作成する

ONTAP SMBサーバにNTFSセキュリティ記述子を作成する

NTFSセキュリティ記述子監査ポリシーの作成は、SVM内のファイルとフォルダにNTFSアクセス制御リスト（ACL）を設定および適用するための最初のステップです。ポリシー タスクで、セキュリティ記述子をファイルまたはフォルダのパスに関連付けます。

タスク概要

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、または混在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が作成されると、そのセキュリティ記述子に4つの随意アクセス制御リスト（DACL）アクセス制御エントリ（ACE）が追加されます。4つのデフォルトのACEは次のとおりです：

オブジェクト	アクセス タイプ	権限	権限の適用先
BUILTIN\Administrators	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
BUILTIN\Users	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
CREATOR OWNER	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 パラメータを使用して、セキュリティ記述子の構成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

ストレージレベルのアクセス保護では、オプションパラメータの値は無視されます。この手順で説明されているコマンドの詳細については、"ONTAPコマンド リファレンス"を参照してください。

手順

1. 高度な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構成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. 上級権限レベルの場合は、管理者権限レベルに戻ります： `set -privilege admin`

ONTAP SMBサーバ上のNTFSセキュリティ記述子にNTFS SACLアクセス制御エントリを追加する

SVM内のファイルまたはフォルダに対するNTFS監査ポリシーを作成するための2番目のステップは、NTFSセキュリティ記述子に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）を追加することです。各エントリは、監査対象となるユーザーまたはグループを識別します。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。

タスク概要

セキュリティ記述子の SACL に 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、そのDACLに新しいACEが追加されます。

`-
account`パラメータで指定され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することで、SACL エントリを設定できます。権限を指定するには、互いに排他的な 3 つの方法があります：

- 権限
- 高度な権利
- Raw 権限（advanced-privilege）

SACL エントリの権限を指定しない場合、デフォルト設定は `Full Control`になります。

`apply to`パラメータを使用して継承の適用方法を指定することにより、必要に応じてSACLエントリをカスタマイズできます。このパラメータを指定しない場合は、デフォルトでこの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. セキュリティ記述子に SACL エントリを追加します `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
   ```

ONTAP SMBセキュリティ ポリシーを作成する

ストレージ仮想マシン（SVM）の監査ポリシーの作成は、ファイルまたはフォルダ

にACLを設定および適用するための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、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。セキュリティ ポリシーには後からタスクを追加できます。

タスク概要

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またはフォルダのパスと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混在セキュリティ形式のボリュームを含む各Storage Virtual Machine（SVM）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
   ```

ONTAP SMB セキュリティ ポリシーにタスクを追加する

ポリシー タスクを作成してセキュリティ ポリシーに追加することは、SVM 内のファイルまたはフォルダに ACL を設定して適用するための 4 番目の手順です。ポリシー タスクを作成すると、そのタスクをセキュリティ ポリシーに関連付けます。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。

タスク概要

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、セキュリティ ポリシーによって NTFS または混合セキュリティのファイルまたはフォルダ（または Storage-Level Access Guard を設定している場合はボリューム オブジェクト）に対して実行できる単一の操作を指します。

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とフォルダにセキュリティ記述子を適用するタスクを指定するために使用されます。ファイルおよびディレクトリタスクを通じて適用されたACLは、SMBクライアントまたはONTAP CLIを使用して管理できます。

- Storage-Level Access Guard 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セキュリティ記述子を適用するタスクを指定するために使用されます。ストレージレベルのアクセス保護タスクを通じて適用されたACLは、ONTAP CLI

を通じてのみ管理できます。

タスクには、ファイル（またはフォルダ）またはファイルセット（またはフォルダ）のセキュリティ設定の定義が含まれます。ポリシー内の各タスクは、パスによって一意に識別されます。1つのポリシー内では、パスごとに1つのタスクのみを設定できます。ポリシー内に重複するタスクエントリを設定することはできません。

ポリシーにタスクを追加するためのガイドライン：

- ポリシーごとに最大 10,000 件のタスク エントリが可能です。
- 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、ファイル / ディレクトリ タスクとStorage-Level Access Guardタスクの両方を含むポリシーを設定することはできません。ポリシーには、すべてのStorage-Level Access Guardタスク、またはすべてのファイル / ディレクトリ タスクのいずれかを含める必要があります。

- Storage-Level Access Guard は、アクセス許可を制限するために使用されます。

  追加のアクセス権限を与えることはありません。

次のオプション パラメータを使用して、セキュリティ記述子の構成をカスタマイズできます：

- セキュリティ タイプ
- 伝播モード
- インデックス位置
- アクセス制御の種類

ストレージレベルのアクセス保護では、オプションパラメータの値は無視されます。この手順で説明されているコマンドの詳細については、"ONTAPコマンド リファレンス"を参照してください。

手順

1. 関連付けられたセキュリティ記述子を持つ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 `-access-control`パラメータのデフォルト値です。ファイルおよびディレクトリ アクセス タスクを構成する際にアクセス制御の種類を指定することはオプションです。

   ```
   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 タスクの構成を確認します： `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
```

```
`vserver security file-directory policy task`
の詳細については、link:https://docs.netapp.com/us-en/ontap-
cli/search.html?q=vserver+security+file-
directory+policy+task["ONTAPコマンド リファレンス"^]をご覧ください。
```

ONTAP SMB セキュリティ ポリシーを適用する

監査ポリシーを SVM に適用することは、NTFS ACL を作成してファイルまたはフォルダに適用する最後の手順です。

タスク概要

セキュリティ ポリシーに定義されているセキュリティ設定を、FlexVol（NTFSまたはmixedセキュリティ形式）内の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は上書きされます。セキュリティ ポリシーと関連するDACLを適用すると、既存のDACLは上書きされます。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 ポリシーを確認してください。

手順

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
   ```

   ポリシーを適用する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
   ```

ONTAP SMBセキュリティ ポリシー ジョブを監視する

ストレージ仮想マシン（SVM）にセキュリティ ポリシーを適用する際、セキュリティ ポリシー ジョブを監視することでタスク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場合に役立ちます。また、多数のファイルやフォルダに一括でセキュリティを適用する、実行時間が長いジョブがある場合にも役立ちます。

タスク概要

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、 `-instance` パラメータを使用する必要があります。

手順

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
   ```

ONTAP SMB監査ポリシーを確認する

監査ポリシーを検証して、セキュリティポリシーを適用したStorage Virtual Machine（SVM）上のファイルまたはフォルダに必要な監査セキュリティ設定があることを確認できます。

タスク概要

`vserver security file-directory show`コマンドを使用して監査ポリシー情報を表示します。ファイルまたはフォルダの監査ポリシー情報を表示するデータが格納されているSVMの名前とデータへのパスを指定する必要があります。

手順

1. 監査ポリシー設定を表示： `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情報を表示します。このパスには、SUCCESS と SUCCESS/FAIL の両方の SACL 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
```

ONTAP SMBセキュリティポリシージョブの管理について学習します

セキュリティポリシージョブが存在する場合、特定の状況下では、そのセキュリティポリシーやそのポリシーに割り当てられたタスクを変更できません。セキュリティポリシーの変更が成功するように、どのような条件で変更できるか、または変更できないかを理解しておく必要があります。ポリシーの変更には、ポリシーに割り当てられたタスクの追加、削除、または変更、およびポリシー自体の削除または変更が含まれます。

セキュリティ ポリシーのジョブが存在し、そのジョブが次の状態にある場合は、セキュリティ ポリシーまたはそのポリシーに割り当てられたタスクを変更することはできません：

- ジョブは実行中または進行中です。
- ジョブは一時停止されています。
- ジョブは再開され、実行状態になります。
- ジョブが別のノードへのフェイルオーバーを待機している場合。

次の状況では、セキュリティ ポリシーのジョブが存在する場合、そのセキュリティ ポリシーまたはそのポリ

シーに割り当てられたタスクを正常に変更できます：

- ポリシー ジョブが停止されました。
- ポリシージョブは正常に終了しました。

SMBサーバー上のNTFSセキュリティ記述子を管理するためのONTAPコマンド

セキュリティ記述子を管理するための専用のONTAPコマンドがあります。セキュリティ記述子に関する情報を作成、変更、削除、表示できます。

状況	使用するコマンド
NTFSセキュリティ記述子を作成する	`vserver security file-directory ntfs create`
既存のNTFSセキュリティ記述子を変更する	`vserver security file-directory ntfs modify`
既存の NTFS セキュリティ記述子に関する情報を表示する	`vserver security file-directory ntfs show`
NTFSセキュリティ記述子を削除する	`vserver security file-directory ntfs delete`

`vserver security file-directory ntfs`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+security+file-directory+ntfs["ONTAPコマンドリファレンス"^]をご覧ください。

SMBサーバ上のNTFS DACLアクセス制御エントリを管理するためのONTAPコマンド

DACL アクセス制御エントリ（ACE）を管理するための ONTAP 専用コマンドがあります。NTFS DACL にはいつでも ACE を追加できます。また、DACL 内の ACE に関する情報を変更、削除、表示することで、既存の NTFS DACL を管理することもできます。

状況	使用するコマンド
ACEを作成し、NTFS DACLに追加する	`vserver security file-directory ntfs dacl add`

状況	使用するコマンド
NTFS DACL 内の既存の ACE を変更する	`vserver security file-directory ntfs dacl modify`
NTFS DACL 内の既存の ACE に関する情報を表示する	`vserver security file-directory ntfs dacl show`
NTFS DACLから既存のACEを削除する	`vserver security file-directory ntfs dacl remove`

`vserver security file-directory ntfs dacl`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+security+file-directory+ntfs+dacl["ONTAPコマンドリファレンス"^]をご覧ください。

SMBサーバ上のNTFS SACLアクセス制御エントリを管理するためのONTAPコマンド

SACL アクセス制御エントリ（ACE）を管理するための ONTAP 専用コマンドがあります。NTFS SACL にはいつでも ACE を追加できます。また、SACL 内の ACE に関する情報を変更、削除、表示することで、既存の NTFS SACL を管理することもできます。

状況	使用するコマンド
ACEを作成し、NTFS SACLに追加する	`vserver security file-directory ntfs sacl add`
NTFS SACLの既存のACEを変更する	`vserver security file-directory ntfs sacl modify`
NTFS SACL内の既存のACEに関する情報を表示する	`vserver security file-directory ntfs sacl show`
NTFS SACLから既存のACEを削除する	`vserver security file-directory ntfs sacl remove`

`vserver security file-directory ntfs sacl`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+security+file-directory+ntfs+sacl["ONTAPコマンドリファレンス"^]をご覧ください。

SMBセキュリティポリシーを管理するためのONTAPコマンド

セキュリティポリシーを管理するための特定のONTAPコマンドがあります。ポリシーに関する情報を表示したり、ポリシーを削除したりできます。セキュリティポリシーを変更することはできません。

状況	使用するコマンド
セキュリティポリシーを作成する	`vserver security file-directory policy create`
セキュリティポリシーに関する情報を表示する	`vserver security file-directory policy show`
セキュリティポリシーを削除する	`vserver security file-directory policy delete`

`vserver security file-directory policy`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+security+file-directory+policy["ONTAPコマンドリファレンス"^]をご覧ください。

ONTAPのSMBセキュリティポリシータスクを管理するためのコマンド

ONTAPには、セキュリティ ポリシー タスクの追加、変更、削除、および関連する情報の表示を行うためのコマンドが用意されています。

状況	使用するコマンド
セキュリティポリシータスクを追加する	`vserver security file-directory policy task add`
セキュリティポリシータスクの変更	`vserver security file-directory policy task modify`
セキュリティ ポリシー タスクに関する情報を表示する	`vserver security file-directory policy task show`
セキュリティ ポリシー タスクを削除する	`vserver security file-directory policy task remove`

`vserver security file-directory policy task`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+security+file-directory+policy+task["ONTAPコマンドリファレンス"^]をご覧ください。

SMBセキュリティポリシージョブを管理するためのONTAPコマンド

セキュリティ ポリシー ジョブの一時停止、再開、停止、および情報表示を行うための ONTAP コマンドがあります。

状況	使用するコマンド
セキュリティ ポリシー ジョブを一時停止する	`vserver security file-directory job pause -vserver vserver_name -id integer`
セキュリティポリシージョブを再開する	`vserver security file-directory job resume -vserver vserver_name -id integer`
セキュリティ ポリシー ジョブに関する情報を表示する	`vserver security file-directory job show -vserver vserver_name` このコマンドを使用してジョブのジョブ ID を判別できます。
セキュリティポリシージョブを停止する	`vserver security file-directory job stop -vserver vserver_name -id integer`

`vserver security file-directory job`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+security+file-directory+job["ONTAPコマンドリファレンス"^]をご覧ください。

著作権に関する情報

商標に関する情報