CLIを使用して、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します。

ONTAP 9

NetApp
December 20, 2024

目次

CLIを使用して、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します。

CLIの概要を使用して、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します。

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と、リモートクライアントを使用してファイルセキュリティを管理する必要がなくなります。CLIを使用すると、1つのコマンドで多数のファイルやフォルダにセキュリティを適用する時間を大幅に短縮できます。

ONTAPがSVMボリュームに適用するもう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または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個別に設定および管理できる、データアクセスのセキュリティレイヤを強化します。

ストレージレベルのアクセス保護ではNTFSのアクセス権限のみがサポートされますが、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経由のアクセスについては、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に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やqtreeに格納されているファイルやフォルダでは、すべてNTFS対応のセキュリティが有効になります。コマンドファミリーを使用すると、NTFSセキュリティ形式のボリュームに次の種類のセキュリティを実装でき `vserver security file-directory`ます。

- ボリュームに含まれるファイルと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

mixedセキュリティ形式のボリュームやqtreeには、UNIX対応のセキュリティが有効で、UNIXファイル権限（モードビットまたはNFSv4.x ACL）とNFSv4.x監査ポリシーを使用するファイルやフォルダ、およびNTFS対応のセキュリティが有効でNTFSファイル権限と監査ポリシーを使用するファイルやフォルダを格納できま

す。コマンドファミリーを使用すると、mixedセキュリティ形式のデータに次の種類のセキュリティを適用でき `vserver security file-directory`ます。

- mixed形式のボリュームまたはqtreeにおける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およびqtreeには、UNIX対応のセキュリティ（モードビットまたはNFSv4.x ACL）が設定されたファイルおよびフォルダが格納されます。コマンドファミリーを使用して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、次の点に注意する必要があり `vserver security file-directory`ます。

- UNIXセキュリティ形式のボリュームおよびqtreeでは、 `vserver security file-directory`コマンドファミリーを使用してUNIXファイルセキュリティおよび監査ポリシーを管理することはできません。
- ターゲットボリュームを含むSVMにCIFSサーバが含まれている場合は、コマンドファミリーを使用して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保護を設定できます `vserver security file-directory`。

関連情報

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

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

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

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を使用したファイルおよびフォルダのセキュリティ設定のユースケース

ファイルおよびフォルダのセキュリティは、リモートクライアントを使用せずにローカルで適用および管理できるため、多数のファイルまたはフォルダに対して一括でセキュリティを設定する場合に比べて大幅に時間を短縮できます。

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と効果的な状況として、次のようなユースケースがあります。

- 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のファイルの格納
- データの移行
- Windowsドメインの変更
- NTFS ファイルシステムのファイルセキュリティと監査ポリシーの標準化

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

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は、一定の制限事項に注意する必要があります。

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

  NTFSセキュリティ記述子は、NTFSファイルおよび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たファイルおよびフォルダのセキュリティの適用方法

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、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。

  - Discretionary Access Control List （ DACL ；随意アクセス制御リスト）
  - システムアクセスセイギョリスト SACL

- * 随意アクセス制御リスト（ DACL ） *

  DACLには、ファイルまたはフォルダに対してアクションを実行するためのアクセスを許可または拒否するユーザ、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。DACLには0個以上のAccess Control Entry（ACE；アクセス制御エントリ）が含まれます。

- * システム・アクセス・コントロール・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Access Control Entry（ACE；アクセス制御エントリ）が含まれます。

- * アクセス制御エントリ (ACE) *

ACEは、DACLまたはSACL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、グループ、またはコンピュータ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、グループ、またはコンピュータオブジェクトによって実行される指定された操作の監査時にログに記録される成功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示します。子オブジェクトには継承可能な権限のみが継承されます。親オブジェクトにパーミッションを設定する際に、「適用先」、 `sub-folders`「ファイル」でフォルダ、サブフォルダ、およびファイルを継承できるかどうかを指定できます `this-folder`。

関連情報

"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への監査ポリシーの設定および適用

SVM ディザスタリカバリデスティネーションでローカルユーザまたはグループを使用するファイルとディレクトリのポリシーを適用する際のガイドライン

ファイルとディレクトリのポリシー設定で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る必要がある一定のガイドラインがあります。

ソースクラスタのソース 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 ディザスタリカバリ構成を設定できます。

SVM ディザスタリカバリの 2 つのタイプのうち 1 つを設定できます。

- ID が保持されます

  この設定では、 SVM と CIFS サーバの ID が維持されます。

- ID が破棄されました

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

ID 破棄設定に関するガイドライン

ID 破棄設定では、ローカルユーザ、グループ、権限設定を含む SVM ソースを SVM デスティネーションの CIFS サーバ名に一致するようにローカルドメインの名前（ローカル CIFS サーバ名）を変更する必要があります。たとえば、ソース SVM 名が「 vs1 」で CIFS サーバ名が「 CIFS1 」、デスティネーション SVM 名が「 vs1_dst 」で CIFS サーバ名が「 CIFS1_DST` 」の場合、ローカルユーザ「 CIFS1\user1 」のローカルドメイン名は「 CIFS1_DST` デスティネーション SVM 」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ローカルユーザおよびグループ名が自動的に変更されても、ファイルとディレクトリのポリシー設定（コマンドファミリーを使用してCLIで設定するポリシー）のローカルユーザまたはグループ名は自動的に変更されません `vserver security file-directory`。

たとえば、「vs1」について、パラメータが「`CIFS1\user1`」に設定されたDACLエントリを設定している場合 `-account`、デスティネーションSVMで設定が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ることはありません。

```
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
```

CIFSサーバ名を手動でデスティネーションCIFSサーバ名に変更するには、コマンドを使用する必要があります `vserver security file-directory modify`。

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

ローカルユーザまたはグループを含むパラメータ設定を使用できるファイルとディレクトリのポリシー設定コンポーネントは 3 つあります。

- セキュリティ記述子

  必要に応じて、セキュリティ記述子の所有者とセキュリティ記述子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と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を使用する場合、デスティネーション SVM にアカウント名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。アカウント名に必要な変更を加えるには、コマンドを使用し `vserver security file-directory ntfs modify`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、すべて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は変更できないため、ローカルユーザまたはグループが設定されたすべての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を使用して新しいDACLエントリを作成し、それらの新しいDACLエントリを適切なセキュリティ記述子と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、すべて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は変更できないため、ローカルユーザまたはグループが設定されたすべてのSACL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を使用して新しいSACLエントリを作成し、それらの新しいSACLエントリを適切なセキュリティ記述子と関連付ける必要があります。

ポリシーを適用する前に、ファイルとディレクトリのポリシー設定で使用されているローカルユーザまたはグループに必要な変更を行う必要があります。そうしないと、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（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。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ることができます。

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。

NTFSセキュリティ記述子へのNTFS DACL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随意アクセス制御リスト（ DACL ）のアクセス制御エントリ（ ACE ）の追加は、ファイルまたはフォルダに対する NTFS ACL の設定および適用における 2 番目の手順です。各エントリによって、アクセスが許可または拒否されるオブジェクトが識別され、 ACE で定義されている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または実行できない操作が定義されます。

タスクの内容

セキュリティ記述子のDACL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が作成されて新しいACEが追加されます。

必要に応じて、パラメータで指定し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、DACLエントリをカスタマイズでき `-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）

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

必要に応じて、継承の適用方法を指定することで、 DACL エントリをカスタマイズできます。

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
```

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セキュリティ形式またはmixedセキュリティ形式のボリュームを含む各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
   ```

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。

セキュリティポリシーにタスクを追加する際には、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 へのファイルセキュリティポリシーの適用は、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
   ```

適用したファイルセキュリティの確認

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、それらの設定が意図したとおりになっているかを確認するには、ファイルのセキュリティ設定を確認します。

タスクの内容

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

ステップ

1. ファイルとフォルダのセキュリティ設定を表示します。 `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

オブジェクト	アクセスタイプ	アクセス権	権限の適用先
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
```

セキュリティポリシージョブを管理する際の考慮事項

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確実に成功するように、ポリシーを変更できる条件やできない条件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、変更と、ポリシーの削除または変更が含まれます。

セキュリティポリシーにジョブが存在し、そのジョブが次の状態の場合、そのポリシーまたはポリシーに割り当てられたタスクは変更できません。

- ジョブが実行中または実行中です。
- ジョブが一時停止中の場合
- ジョブが再開され、実行中の状態になります。
- ジョブが別のノードへのフェイルオーバーを待機中の場合。

セキュリティポリシーにジョブが存在する場合、次の状況下では、そのセキュリティポリシーまたは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。
- ポリシージョブが正常に終了しました。

NTFSセキュリティ記述子の管理用コマンド

ONTAP には、セキュリティ記述子を管理するためのコマンドが用意されています。セキュリティ記述子を作成、変更、削除、および表示できます。

状況	使用するコマンド
NTFS セキュリティ記述子を作成します	`vserver security file-directory ntfs create`
既存の NTFS セキュリティ記述子を変更します	`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します	`vserver security file-directory ntfs show`
NTFS セキュリティ記述子を削除します	`vserver security file-directory ntfs delete`

詳細については、コマンドのマニュアルページを参照してください `vserver security file-directory ntfs`。

NTFS DACLアクセス制御エントリの管理用コマンド

ONTAPには、DACLのアクセス制御エントリ（ACE）を管理するためのコマンドが用意されています。ACE はいつでも NTFS DACL に追加できます。また、DACLのACEを変更、削除、および情報表示することで、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 を作成して NTFS DACL に追加します	`vserver security file-directory ntfs dacl add`
NTFS DACL の既存の ACE の変更	`vserver security file-directory ntfs dacl modify`
NTFS DACL の既存の ACE に関する情報を表示します	`vserver security file-directory ntfs dacl show`
NTFS DACL から既存の ACE を削除します	`vserver security file-directory ntfs dacl remove`

詳細については、コマンドのマニュアルページを参照してください `vserver security file-directory ntfs dacl`。

NTFS SACLアクセス制御エントリの管理用コマンド

ONTAPには、SACLのアクセス制御エントリ（ACE）を管理するためのコマンドが用意されています。ACE はいつでも NTFS SACL に追加できます。また、SACLのACEを変更、削除、および情報表示することで、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 を作成して NTFS SACL に追加します	`vserver security file-directory ntfs sacl add`
NTFS SACL の既存の ACE の変更	`vserver security file-directory ntfs sacl modify`
NTFS SACL の既存の ACE に関する情報を表示します	`vserver security file-directory ntfs sacl show`
NTFS SACL から既存の ACE を削除します	`vserver security file-directory ntfs sacl remove`

詳細については、コマンドのマニュアルページを参照してください `vserver security file-directory ntfs sacl`。

セキュリティポリシーの管理用コマンド

ONTAP には、セキュリティポリシーを管理するためのコマンドが用意されています。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は変更できません。

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します	`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`

詳細については、コマンドのマニュアルページを参照してください `vserver security file-directory policy`。

セキュリティポリシータスクの管理用コマンド

セキュリティポリシータスクに関する情報を追加、変更、削除、および表示するためのONTAP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を変更する	`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します	`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`

詳細については、コマンドのマニュアルページを参照してください `vserver security file-directory policy task`。

セキュリティポリシージョブの管理用コマンド

ONTAP には、セキュリティポリシージョブを一時停止、再開、停止、および関連する情報を表示する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ジョブを一時停止します	`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します	`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します	`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を確認できます。
セキュリティポリシージョブを停止します	`vserver security file-directory job stop -vserver vserver_name -id integer`

詳細については、コマンドのマニュアルページを参照してください `vserver security file-directory job`。

著作権に関する情報

商標に関する情報