



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 ONTAP 9

NetApp
December 20, 2024

目次

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	1
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	1
ストレージレベルのアクセス保護の使用のユースケース	2
ストレージレベルのアクセス保護の設定ワークフロー	3
ストレージレベルのアクセス保護の設定	5
SLAGノテキヨユニカンスルマトリックス	11
ストレージレベルのアクセス保護に関する情報を表示する	11
ストレージレベルのアクセス保護の削除	14

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

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

ネイティブファイルレベルのセキュリティとエクスポートおよび共有のセキュリティを使用したアクセスの保護に加えて、ボリュームレベルで ONTAP によって適用される第 3 のセキュリティレイヤとして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：すべての NAS プロトコルから適用されるストレージオブジェクトへの環境アクセスを保護します。

NTFSのアクセス権限のみがサポートされます。ONTAP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にアクセスするUNIXユーザのセキュリティチェックを実行するには、UNIXユーザがボリュームを所有するSVM上のWindowsユーザにマッピングされている必要があります。

ストレージレベルのアクセス保護の動作

- ストレージレベル環境のアクセス保護：ストレージオブジェクト内のすべてのファイルまたはすべてのディレクトリを保護します。

ボリューム内のすべてのファイルまたはディレクトリがストレージレベルのアクセス保護設定の影響を受けるため、伝播による継承は必要ありません。

- ストレージレベルのアクセス保護は、ボリューム内のファイルのみ、ディレクトリのみ、またはファイルとディレクトリの両方に適用されるように設定できます。

- ファイルとディレクトリのセキュリティ

ストレージオブジェクト内のすべてのディレクトリとファイルを環境に格納します。これがデフォルト設定です。

- ファイルセキュリティ

ストレージオブジェクト内のすべてのファイルを環境します。このセキュリティを適用しても、ディレクトリへのアクセスとディレクトリの監査には影響しません。

- ディレクトリセキュリティ

ストレージオブジェクト内のすべてのディレクトリを環境します。このセキュリティを適用しても、ファイルへのアクセスとファイルの監査には影響しません。

- 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。

- 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のセキュリティは表示されません。

有効な権限を決定するために、ストレージオブジェクトレベルで適用され、メタデータに格納されます。

- 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。

このセキュリティは、ストレージ管理者のみが変更できるように設計されています。

- ストレージレベルのアクセス保護は、NTFS または mixed セキュリティ形式のボリュームに適用できません。
- ストレージレベルのアクセス保護を UNIX セキュリティ形式のボリュームに適用できるのは、そのボリュームが含まれている SVM で CIFS サーバが設定されている場合に限られます。
- ボリュームがボリュームジャンクションパス以下にマウントされていて、そのパスにストレージレベルのアクセス保護が存在している場合、その下にマウントされているボリュームには伝播されません。
- 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は、SnapMirror データレプリケーションおよび SVM レプリケーションによってレプリケートされます。
- ウィルススキャンについては特別な免除があります。

ファイルやディレクトリのスクリーニングを行うこれらのサーバに対しては、ストレージレベルのアクセス保護によってオブジェクトへのアクセスが拒否されていても、例外的なアクセスが許可されます。

- ストレージレベルのアクセス保護によってアクセスが拒否された場合、FPolicy 通知は送信されません。

アクセスチェックの順序

ファイルまたはディレクトリへのアクセスは、エクスポートまたは共有の権限、ボリュームで設定されているストレージレベルのアクセス保護権限、ファイルやディレクトリに適用されるネイティブのファイル権限の各影響の組み合わせによって決まります。すべてのレベルのセキュリティが評価されて、ファイルまたはディレクトリの有効な権限が決定されます。セキュリティアクセスチェックは、次の順序で実行されます。

1. SMB 共有または NFS エクスポートレベルの権限
2. ストレージレベルのアクセス保護
3. NTFSのファイル/フォルダのAccess Control List (ACL ; アクセス制御リスト)、NFSv4 ACL、またはUNIXモードビット

ストレージレベルのアクセス保護の使用のユースケース

ストレージレベルのアクセス保護は、ストレージレベルでの追加セキュリティを提供します。このセキュリティはクライアント側からは見えないため、ユーザや管理者がデスクトップから取り消すことはできません。一部のユースケースでは、ストレージレベルでアクセス制御を行える機能が役立ちます。

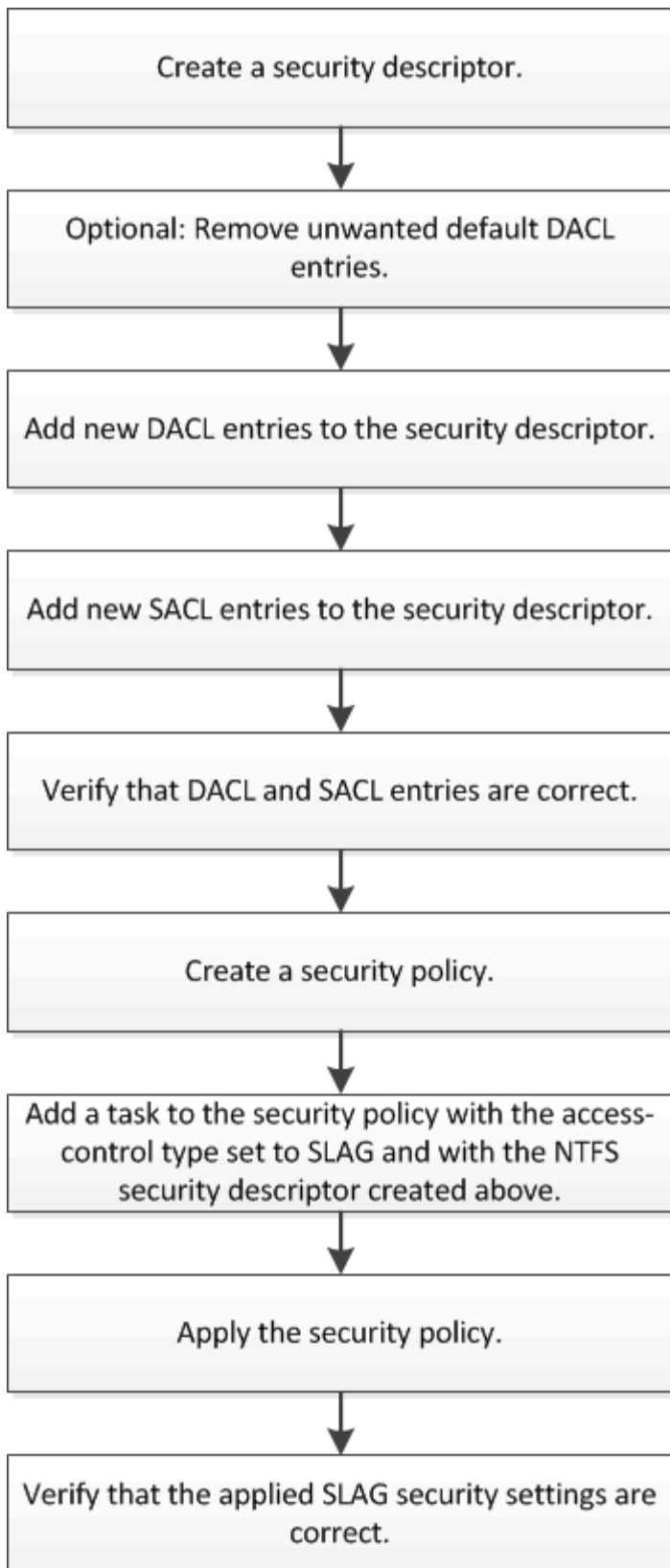
この機能の一般的なユースケースとしては、次のようなシナリオがあります。

- すべてのユーザーのアクセスをストレージ・レベルで監査および制御することにより、知的財産を保護します
- 銀行や証券会社など、金融サービス企業のストレージの場合
- 部門ごとに個別のファイルストレージを使用する行政サービス

- すべての学生のファイルを保護する大学

ストレージレベルのアクセス保護の設定ワークフロー

ストレージレベルのアクセス保護（SLAG）を設定するワークフローでは、NTFSファイル権限と監査ポリシーの設定に使用するONTAP CLIコマンドと同じコマンドを使用します。対象のファイルやディレクトリのアクセスを設定する代わりに、対象のStorage Virtual Machine（SVM）ボリュームのSLAGを設定します。



関連情報

[ストレージレベルのアクセス保護の設定](#)

ストレージレベルのアクセス保護の設定

ボリュームまたはqtreeにストレージレベルのアクセス保護を設定するには、いくつかの手順に従う必要があります。ストレージレベルのアクセス保護は、ストレージレベルで設定されるアクセスセキュリティのレベルを提供します。すべてのNASプロトコルから適用先のストレージオブジェクトへのすべてのアクセスに適用されるセキュリティを提供します。

手順

1. コマンドを使用して、セキュリティ記述子を作成し `vserver security file-directory ntfs create` ます。

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

```
Vserver: vs1
```

NTFS Security Descriptor Name	Owner Name
-----	-----
sd1	-

セキュリティ記述子は、次の4つのデフォルトDACL Access Control Entry (ACE; アクセス制御エントリ) で作成されます。

```
Vserver: vs1
```

```
NTFS Security Descriptor Name: sd1
```

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
BUILTIN\Administrators	allow	full-control	this-folder, sub-folders, files
BUILTIN\Users	allow	full-control	this-folder, sub-folders, files
CREATOR OWNER	allow	full-control	this-folder, sub-folders, files
NT AUTHORITY\SYSTEM	allow	full-control	this-folder, sub-folders, files

ストレージレベルのアクセス保護の設定時にデフォルトのエントリを使用しない場合は、セキュリティ記述子に独自のACEを作成して追加する前に、デフォルトのエントリを削除できます。

2. セキュリティ記述子から、ストレージレベルのアクセス保護セキュリティで設定したくないデフォルトのDACL ACEを削除します。

- a. コマンドを使用して、不要なDACL ACEを削除します `vserver security file-directory ntfs dacl remove`。

この例では、セキュリティ記述子から BUILTIN\Administrators、BUILTIN\Users、CREATOR OWNER の3つのデフォルト DACL ACE を削除しています。

```
vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
-access-type allow -account builtin\users vserver security file-directory
ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
builtin\administrators vserver security file-directory ntfs dacl remove
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
```

- b. コマンドを使用して、ストレージレベルのアクセス保護セキュリティに使用しないDACL ACEがセキュリティ記述子から削除されたことを確認します `vserver security file-directory ntfs dacl show`。

この例では、コマンドの出力によって、3つのデフォルトDACL ACEがセキュリティ記述子から削除され、NT AUTHORITY\SYSTEMデフォルトDACL ACEエントリのみが残されていることが確認されます。

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

```
Vserver: vs1
NTFS Security Descriptor Name: sd1

Account Name      Access   Access   Apply To
                  Type    Rights
-----
NT AUTHORITY\SYSTEM
                  allow    full-control    this-folder, sub-folders,
files
```

3. コマンドを使用して、セキュリティ記述子に1つ以上のDACLエントリを追加します `vserver security file-directory ntfs dacl add`。

この例では、セキュリティ記述子に2つのDACL ACEを追加しています。

```
vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
-access-type allow -account example\engineering -rights full-control -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs dacl add
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
-rights read -apply-to this-folder,sub-folders,files
```

4. コマンドを使用して、セキュリティ記述子に1つ以上のSACLエントリを追加します `vserver security file-directory ntfs sacl add`。

この例では、セキュリティ記述子に2つのSACL ACEを追加しています。


```
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
-access-type failure -account "example\Domain Users" -rights read -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. コマンドと `vserver security file-directory ntfs sacl show`` コマンドを使用して、DACL ACEとSACL ACEがそれぞれ正しく設定されていることを確認します ``vserver security file-directory ntfs dacl show``。

この例では、次のコマンドを実行すると、セキュリティ記述子「`d1`」の DACL エントリに関する情報が表示されます。

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

```
Vserver: vs1
NTFS Security Descriptor Name: sd1

Account Name      Access      Access      Apply To
Type              Rights
-----
EXAMPLE\Domain Users
                allow      read        this-folder, sub-folders,
files
EXAMPLE\engineering
                allow      full-control  this-folder, sub-folders,
files
NT AUTHORITY\SYSTEM
                allow      full-control  this-folder, sub-folders,
files
```

この例では、次のコマンドを実行すると、セキュリティ記述子「`d1`」の SACL エントリに関する情報が表示されます。

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

```
Vserver: vs1
NTFS Security Descriptor Name: sd1

Account Name      Access      Access      Apply To
                  Type        Rights
-----
EXAMPLE\Domain Users
                  failure    read        this-folder, sub-folders,
files
EXAMPLE\engineering
                  success    full-control  this-folder, sub-folders,
files
```

6. コマンドを使用して、セキュリティポリシーを作成し `vserver security file-directory policy create` ます。次に、「policy1」という名前のポリシーを作成する例を示します。

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

7. コマンドを使用して、ポリシーが正しく設定されていることを確認します `vserver security file-directory policy show`。

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

```
Vserver      Policy Name
-----
vs1          policy1
```

8. コマンドでパラメータをに設定 `slag`して` -access-control、セキュリティ記述子が関連付けられた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。`

ポリシーには複数のストレージレベルのアクセス保護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。

この例では'セキュリティ記述子 "d1" に割り当てられている "policy1 " という名前のポリシーにタスクが追加されますアクセス制御タイプが「`slag`」に設定されたパスに割り当てられ`/datavol1`'ます。

```
vserver security file-directory policy task add -vserver vs1 -policy-name
policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode
propagate -ntfs-sd sd1
```

9. コマンドを使用して、タスクが正しく設定されていることを確認します `vserver security file-directory policy task show`。

```
vserver security file-directory policy task show -vserver vs1 -policy-name policy1
```

```
Vserver: vs1
Policy: policy1
```

Index	File/Folder	Access	Security	NTFS	NTFS
Security	Path	Control	Type	Mode	Descriptor
Name					
1	/datavol1	slag	ntfs	propagate	sd1

10. コマンドを使用して、ストレージレベルのアクセス保護セキュリティポリシーを適用し `vserver security file-directory apply` ます。

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

セキュリティポリシーを適用するジョブがスケジュールされます。

11. コマンドを使用して、適用されたストレージレベルのアクセス保護セキュリティ設定が正しいことを確認し `vserver security file-directory show` ます。

この例では、コマンドの出力から、ストレージレベルのアクセス保護セキュリティがNTFSボリュームに適用されていることがわかります /datavol1。Everyoneにフルコントロールを許可するデフォルトのDACLは残っていますが、ストレージレベルのアクセス保護セキュリティは、ストレージレベルのアクセス保護設定で定義されたグループへのアクセスを制限（および監査）します。

```
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:0x8004
Owner: BUILTIN\Administrators
Group: BUILTIN\Administrators
DACL - ACEs
ALLOW-Everyone-0x1f01ff
ALLOW-Everyone-0x10000000-OI|CI|IO

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
```

関連情報

[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](#)

[ストレージレベルのアクセス保護の設定ワークフロー](#)

[ストレージレベルのアクセス保護に関する情報の表示](#)

SLAG ノテキヨウニカンスルマトリックス

SLAG は、ボリューム、 qtree 、またはその両方に対して設定できます。次の表に、さまざまな状況について、ボリュームまたは qtree に SLAG 構成を適用できるかどうかを示します。

	AFS 内のボリューム SLAG	Snapshot コピー内のボリューム SLAG	AFS 内の qtree SLAG	Snapshot コピー内の qtree SLAG
AFS 内のボリュームへのアクセス	はい	いいえ	N/A	N/A
Snapshot コピー内のボリュームへのアクセス	はい	いいえ	N/A	N/A
AFS 内の qtree へのアクセス (qtree に SLAG が設定されている場合)	いいえ	いいえ	はい	いいえ
AFS 内の qtree へのアクセス (qtree に SLAG が設定されていない場合)	はい	いいえ	いいえ	いいえ
Snapshot コピー内の qtree へのアクセス (qtree に SLAG が設定されている場合)	いいえ	いいえ	はい	いいえ
Snapshot コピー内の qtree へのアクセス (qtree に SLAG が設定されていない場合)	はい	いいえ	いいえ	いいえ

ストレージレベルのアクセス保護に関する情報を表示する

ストレージレベルのアクセス保護は、ボリュームまたは qtree に適用される 3 番目のセキュリティレイヤです。ストレージレベルのアクセス保護設定は、Windows のプロパティウィンドウでは表示できません。ストレージレベルのアクセス保護セキュリティに関する情報を表示するには、ONTAP CLI を使用する必要があります。この情報を使用し

て、構成の検証や、アクセス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せん。

タスクの内容

Storage Virtual Machine (SVM) の名前、およびストレージレベルのアクセス保護セキュリティ情報を表示するボリュームまたは qtree のパスを入力する必要があります。出力は要約形式で表示することも、詳細なリストとして表示することもできます。

ステップ

1. ストレージレベルのアクセス保護セキュリティ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	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>
詳細を表示	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>

例

次の例では、SVM vs1のパスにあるNTFSセキュリティ形式のボリュームのストレージレベルのアクセス保護セキュリティ情報を表示します /datavol1。

```
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:0x8004
          Owner: BUILTIN\Administrators
          Group: BUILTIN\Administrators
          DACL - ACEs
                ALLOW-Everyone-0x1f01ff
                ALLOW-Everyone-0x10000000-OI|CI|IO

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
```

次の例では、SVM vs1のパスにあるmixedセキュリティ形式のボリュームに関するストレージレベルのアクセス保護の情報を表示します /datavol15。このボリュームの最上位には、UNIX 対応のセキュリティが設定されています。ボリュームにはストレージレベルのアクセス保護セキュリティが設定されています。

```

cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5

      Vserver: vs1
      File Path: /datavol5
File Inode Number: 3374
      Security Style: mixed
      Effective Style: unix
      DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 755
Unix Mode Bits in Text: rwxr-xr-x
      ACLs: 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

```

ストレージレベルのアクセス保護の削除

ストレージレベルのアクセスセキュリティの設定が不要になった場合は、ボリュームや qtree からストレージレベルのアクセス保護を削除できます。ストレージレベルのアクセス保護を削除しても、通常の NTFS のファイルやディレクトリのセキュリティは変更されたり削除されたりしません。

手順

1. コマンドを使用して、ボリュームまたは qtree にストレージレベルのアクセス保護が設定されていることを確認します `vserver security file-directory show`。

```
vserver security file-directory show -vserver vs1 -path /datavol2
```



```

Vserver: vs1
File Path: /datavol2
File Inode Number: 99
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:0xbf14
Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
SACL - ACEs
AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
DACL - ACEs
ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

Storage-Level Access Guard security
DACL (Applies to Directories):
ALLOW-BUILTIN\Administrators-0x1f01ff
ALLOW-CREATOR OWNER-0x1f01ff
ALLOW-EXAMPLE\Domain Admins-0x1f01ff
ALLOW-EXAMPLE\Domain Users-0x120089
ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
DACL (Applies to Files):
ALLOW-BUILTIN\Administrators-0x1f01ff
ALLOW-CREATOR OWNER-0x1f01ff
ALLOW-EXAMPLE\Domain Admins-0x1f01ff
ALLOW-EXAMPLE\Domain Users-0x120089
ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

2. コマンドを使用して、ストレージレベルのアクセス保護を削除します `vserver security file-directory remove-slag`。

```
vserver security file-directory remove-slag -vserver vs1 -path /datavol2
```

3. コマンドを使用して、ボリュームまたはqtreeからストレージレベルのアクセス保護が削除されたことを確認します `vserver security file-directory show`。

```
vserver security file-directory show -vserver vs1 -path /datavol2
```

```
Vserver: vs1
File Path: /datavol2
File Inode Number: 99
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:0xbf14
Owner: BUILTIN\Administrators
Group: BUILTIN\Administrators
SACL - ACEs
    AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
DACL - ACEs
    ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
    ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```

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。