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
February 12, 2026

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

Storage-Level Access Guardを使用した安全なONTAP SMBファイルアクセスについて学習します

ネイティブのファイルレベル、エクスポート、共有セキュリティによるアクセス保護に加えて、ONTAPがボリュームレベルで適用する第3のセキュリティレイヤーであるStorage-Level Access Guardを設定できます。Storage-Level Access Guardは、適用対象のストレージオブジェクトへのすべてのNASプロトコルからのアクセスに適用されます。

NTFSのアクセス権のみがサポートされています。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 チェックを行うには、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ガードの動作

- Storage-Level Access Guardは、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に適用されます。

  ボリューム内のすべてのファイルまたはディレクトリはStorage-Level Access Guard設定の対象となるため、伝播による継承は必要ありません。

- Storage-Level Access Guard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す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

    環境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に適用されます。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が環境になります。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や監査には影響しません。

  - ディレクトリセキュリティ

    環境ストレージオブジェクト内のすべてのディレクトリに適用されます。このセキュリティを適用しても、ファイルへのアクセスや監査には影響しません。

- 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。

- 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すると、Storage-Level Access Guard セキュリティは表示されません。

このセキュリティは、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、メタデータ内に格納されます。

- ストレージレベルのセキュリティは、システム（Windows または UNIX）管理者であっても、クライアントから取り消すことはできません。

  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 ガードは、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す。
- ボリュームを含む SVM に CIFS サーバが設定されている限り、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 ガードを適用できます。
- ボリュームがボリューム ジャンクション パスの下にマウントされ、そのパスにStorage-Level Access Guardが存在する場合、そのパスの下にマウントされた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ガード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複製されます。
- ウイルススキャナーには特別な配慮があります。

  Storage-Level Access Guardによってオブジェクトへのアクセスが拒否された場合でも、ファイルとディレクトリをスクリーニングするためにこれらのサーバーへの例外的なアクセスが許可されます。

- Storage-Level Access Guardにより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権限、ボリュームに設定されたストレージレベルのアクセスガード権限、およびファイルやディレクトリに適用されたネイティブファイル権限の組み合わせによって決定されます。すべてのセキュリティレベルが評価され、ファイルまたはディレクトリに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、以下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のファイルやフォルダのアクセス制御リスト（ACL）、NFSv4 ACL、またはUNIXモードのビット

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

Storage-Level Access Guardは、クライアント側からは見えないストレージレベルで追加のセキュリティを提供するため、ユーザーや管理者がデスクトップからこのセキュリティを解除することはできません。ストレージレベルでのアクセス制御が有効なユースケースもいくつかあります。

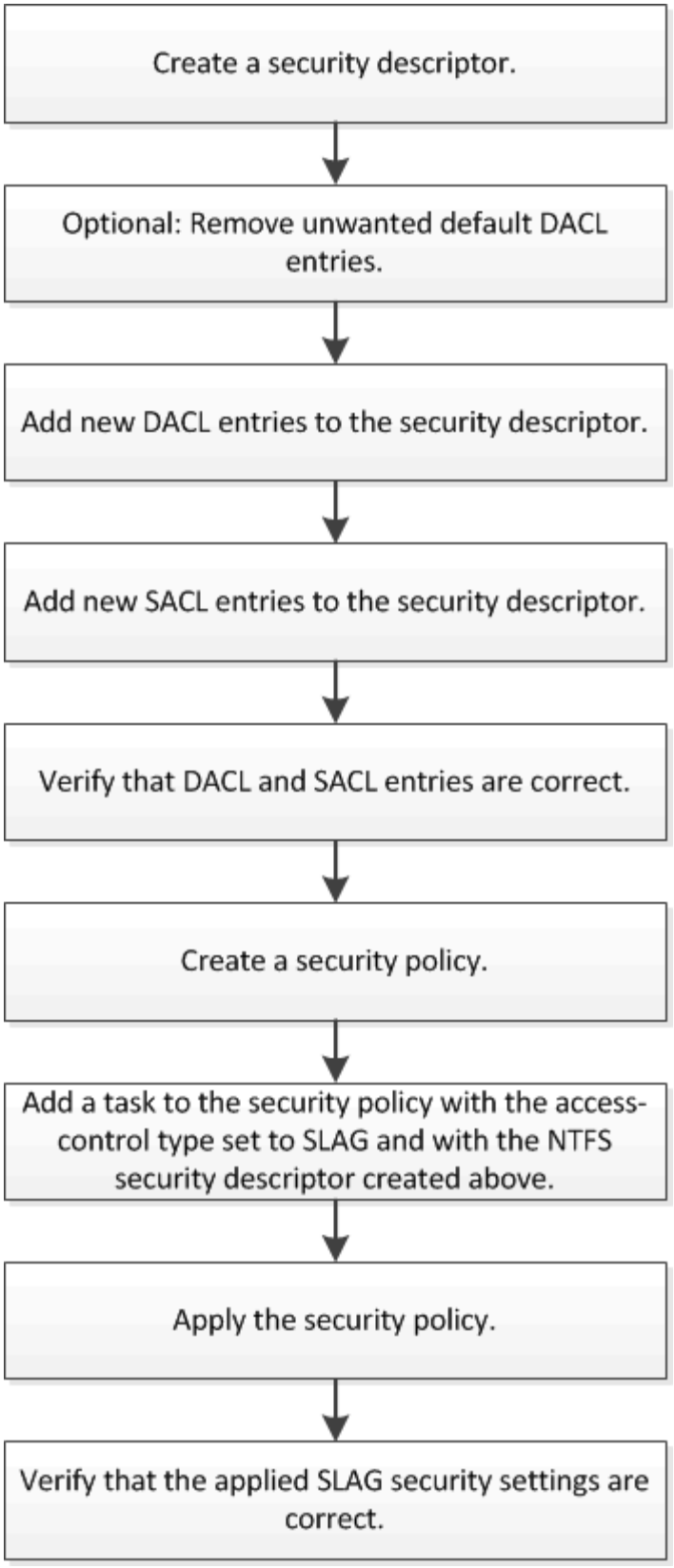
この機能の一般的な使用例には、次のシナリオが含まれます：

- ストレージレベルですべてのユーザーのアクセスを監査および制御することにより、知的財産を保護します
- 銀行やトレーディンググループを含む金融サービス企業向けのストレージ
- 個別の部門用に別々のファイルストレージを備えた政府サービス

- すべての学生ファイルを保護する大学

ONTAP SMBサーバにおけるストレージレベルアクセスガード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ファイル権限や監査ポリシーを設定する際に使用する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

サーバーでStorage-Level Access Guardを設定する

ONTAP SMBサーバでストレージレベルのアクセスガードを設定する

ボリュームまたはqtreeのストレージレベルのアクセス保護を設定する際には、多く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するアクセス セキュリティを提供します。すべてのNASプロトコルからの適用対象のストレージ オブジェクトへのすべてのアクセスにセキュリティが適用されます。

手順

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

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

```
Vserver: vs1

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

セキュリティ記述子は、次の4つのデフォルトDACLアクセス制御エントリ（ACE）を持った状態で作成されます。

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

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    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を設定する際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に設定したくないデフォルトのDACL ACEを削除します。

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

      この例では、セキュリティ記述子から 3 つのデフォルトの DACL ACE（BUILTIN\Administrators 、BUILTIN\Users、および CREATOR OWNER）が削除されます。

      ```
      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. `vserver security file-directory ntfs dacl show`コマンドを使用して、Storage-Level Access Guard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ていることを確認します。

      この例では、コマンドからの出力より、セキュリティ記述子から3つのデフォルトDACL ACEが削除され、NT AUTHORITY\SYSTEMのデフォルトDACL ACEエントリのみが残されていることを確認できます。

      ```
      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. `vserver security file-directory ntfs dacl add`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。

   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. `vserver security file-directory ntfs sacl add`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。

   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. `vserver security file-directory ntfs dacl show`コマンドおよび `vserver security file-directory ntfs sacl show` コマンドをそれぞれ使用して、DACL および SACL ACE が正しく設定されていることを確認します。

   この例では、次のコマンドは、セキュリティ記述子"`sd1`"のDACLエントリに関する情報を表示します：

   ```
   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、次のコマンドは、セキュリティ記述子"`sd1`"のSACLエントリに関する情報を表示します：

   ```
   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. `vserver security file-directory policy create`コマンドを使用してセキュリティ ポリシーを作成します。

   次の例では、「policy1」という名前のポリシーを作成します：

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

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

8. `vserver security file-directory policy task add`コマンドで `-access-control`パラメータを `slag`に設定して、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。

   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「sd1」に割り当てられた「policy1」というポリシーにタスクが追加されます。 /datavol1`パスに割り当てられ、アクセス制御タイプが「`slag」に設定されます。

   ```
   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. `vserver security file-directory policy task show`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 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. `vserver security file-directory apply`コマンドを使用して、Storage-Level Access Guardセキュリティ ポリシーを適用します。

    ```
    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. `vserver security file-directory show`コマンドを使用して、適用されたStorage-Level Access Guardセキュリティ設定が正しいことを確認します。

    この例では、コマンドの出力から、NTFSボリュームにStorage-Level Access Guardセキュリティが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はそのまま残りますが、Storage-Level Access Guardセキュリティは、Storage-Level Access Guard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

- NTFS ファイル セキュリティ、NTFS 監査ポリシー、およびStorage-Level Access Guardを管理するためのコマンド
- サーバ上の Storage-Level Access Guard の設定ワークフロー
- サーバ上の Storage-Level Access Guard に関する情報を表示する
- サーバのStorage-Level Access Guardを削除する

ONTAP SMBサーバにおける有効なSLAGマトリックス

SLAGはボリューム、qtree、またはその両方に設定できます。SLAGマトリックスは、表に記載されているさまざまなシナリオにおいて、どのボリュームまたはqtreeにSLAG設定を適用できるかを定義します。

	AFSのボリューム**SLAG**	スナップショット内のボリューム**SLAG**	**AFS** における **qtree SLAG**	スナップショットの **qtree SLAG**
Access File System（AFS）でのボリューム アクセス	はい	いいえ	該当なし	該当なし
Snapshotでのボリュームアクセス	はい	いいえ	該当なし	該当なし
AFS での qtree アクセス（qtree に SLAG が存在する場合）	いいえ	いいえ	はい	いいえ
AFS での qtree アクセス（qtree に SLAG が存在しない場合）	はい	いいえ	いいえ	いいえ
スナップショットでの qtree アクセス（qtree AFS に SLAG が存在する場合）	いいえ	いいえ	はい	いいえ
スナップショットでの qtree アクセス（qtree AFS に SLAG が存在しない場合）	はい	いいえ	いいえ	いいえ

ONTAP SMB サーバ上のストレージ レベル アクセス ガード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に適用される第3のセキュリティ層です。ストレージレベルのアクセス保護の設定は、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の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。この情報は、設定の検証やファイルアクセスの問題のトラブルシューティングに使用できます。

タスク概要

ストレージ仮想マシン（SVM）の名前と、Storage-Level Access Guard のセキュリティ情報を表示するボリュームまたは qtree へのパスを指定する必要があります。出力は、概要形式または詳細リスト形式で表示できます。

手順

1. ストレージ レベルのアクセス ガード セキュリティ設定を、必要な詳細レベルで表示します：

情報を表示する場合...	入力するコマンド
要約形式	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
詳細	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

例

次の例では、SVM vs1 内のパス `/datavol1`を持つ 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 ガードのセキュリティ情報を表示します：

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control: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
```

次の例は、SVM vs1のパス `/datavol5`にあるmixedセキュリティ形式のボリュームに関するStorage-Level Access Guard情報を表示します。このボリュームの最上位レベルにはUNIX有効セキュリティが設定されています。このボリュームにはStorage-Level Access Guard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
```

ONTAP SMBサーバのストレージレベルアクセスガードを削除する

ストレージレベルでアクセスセキュリティを設定する必要がなくなった場合は、ボリュームまたはqtreeのStorage-Level Access Guardを削除できます。Storage-Level Access Guardを削除しても、通常のNTFSファイルおよびディレクトリのセキュリティは変更または削除されません。

手順

1. `vserver security file-directory show`コマンドを使用して、ボリュームまたはqtreeにStorage-Level Access Guardが設定されていることを確認します。

   ```
   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. `vserver security file-directory remove-slag`コマンドを使用して、Storage-Level Access Guardを削除します。

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

3. `vserver security file-directory show`コマンドを使用して、ボリュームまたはqtreeからStorage-Level Access Guardが削除されていることを確認します。

   ```
   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
```