Storage-Level Access Guard를 사용하여 파일 액세스를 보호합니다

ONTAP 9

NetApp
April 24, 2024

목차

Storage-Level Access Guard를 사용하여 파일 액세스를 보호합니다

Storage-Level Access Guard를 사용하여 파일 액세스를 보호합니다

기본 파일 수준 및 내보내기/공유 보안을 사용하여 액세스를 보호하는 것 외에도 ONTAP가 볼륨 수준에서 적용한 세 번째 보안 계층인 스토리지 수준 액세스 가드를 구성할 수 있습니다. Storage-Level Access Guard는 모든 NAS 프로토콜에서 해당 프로토콜이 적용된 스토리지 객체에 액세스하는 데 적용됩니다.

NTFS 액세스 권한만 지원됩니다. ONTAP에서 UNIX 사용자에 대한 보안 검사를 수행하여 스토리지 수준 액세스 가드가 적용된 볼륨의 데이터에 액세스하려면 UNIX 사용자는 볼륨을 소유한 SVM에서 Windows 사용자에게 매핑해야 합니다.

Storage-Level Access Guard 동작

- Storage-Level Access Guard는 스토리지 개체의 모든 파일 또는 모든 디렉토리에 적용됩니다.

  볼륨의 모든 파일 또는 디렉토리에는 Storage-Level Access Guard 설정이 적용되기 때문에 전파를 통한 상속은 필요하지 않습니다.

- 저장소 수준 액세스 가드를 구성하여 파일에만 적용하거나 디렉터리에만 적용하거나 볼륨 내의 파일과 디렉터리에 모두 적용할 수 있습니다.
  - 파일 및 디렉터리 보안

    스토리지 객체 내의 모든 디렉토리 및 파일에 적용됩니다. 기본 설정입니다.

  - 파일 보안

    스토리지 객체 내의 모든 파일에 적용됩니다. 이 보안을 적용해도 디렉터리에 대한 액세스 또는 감사에는 영향을 주지 않습니다.

  - 디렉터리 보안

    스토리지 객체 내의 모든 디렉토리에 적용됩니다. 이 보안을 적용해도 파일에 대한 액세스 또는 감사에는 영향을 주지 않습니다.

- Storage-Level Access Guard는 사용 권한을 제한하는 데 사용됩니다.

  추가 액세스 권한은 제공하지 않습니다.

- NFS 또는 SMB 클라이언트의 파일 또는 디렉토리에 대한 보안 설정을 볼 경우 Storage-Level Access Guard 보안이 표시되지 않습니다.

  스토리지 객체 레벨에서 적용되고 유효 사용 권한을 결정하는 데 사용되는 메타데이터에 저장됩니다.

- 시스템(Windows 또는 UNIX) 관리자도 클라이언트에서 스토리지 수준 보안을 취소할 수 없습니다.

스토리지 관리자만 수정할 수 있습니다.

- NTFS 또는 혼합 보안 스타일을 사용하는 볼륨에 스토리지 수준 액세스 가드를 적용할 수 있습니다.
- 볼륨이 포함된 SVM에 CIFS 서버가 구성되어 있는 경우 UNIX 보안 스타일을 사용하는 볼륨에 Storage-Level Access Guard를 적용할 수 있습니다.
- 볼륨이 볼륨 접합 경로 아래에 마운트되고 해당 경로에 Storage-Level Access Guard가 있는 경우 그 아래에 마운트된 볼륨으로 전파되지 않습니다.
- Storage-Level Access Guard 보안 설명자는 SnapMirror 데이터 복제 및 SVM 복제를 통해 복제됩니다.
- 바이러스 스캐너용 특별한 디스펜션이 있습니다.

  저장소 수준 액세스 가드가 개체에 대한 액세스를 거부하더라도 이러한 서버에서 파일과 디렉토리를 선별하기 위해 예외적인 액세스가 허용됩니다.

- 스토리지 레벨 액세스 가드로 인해 액세스가 거부되면 FPolicy 알림이 전송되지 않습니다.

액세스 확인 순서

파일 또는 디렉토리에 대한 액세스는 내보내기 또는 공유 권한, 볼륨에 설정된 Storage-Level Access Guard 권한, 파일 및/또는 디렉토리에 적용되는 기본 파일 권한의 합집합에 의해 결정됩니다. 모든 보안 수준을 평가하여 파일 또는 디렉터리에 있는 유효한 권한을 결정합니다. 보안 액세스 검사는 다음 순서로 수행됩니다.

1. SMB 공유 또는 NFS 엑스포트 레벨 사용 권한
2. 스토리지 레벨 액세스 가드
3. NTFS 파일/폴더 ACL(액세스 제어 목록), NFSv4 ACL 또는 UNIX 모드 비트

Storage-Level Access Guard 사용 사례

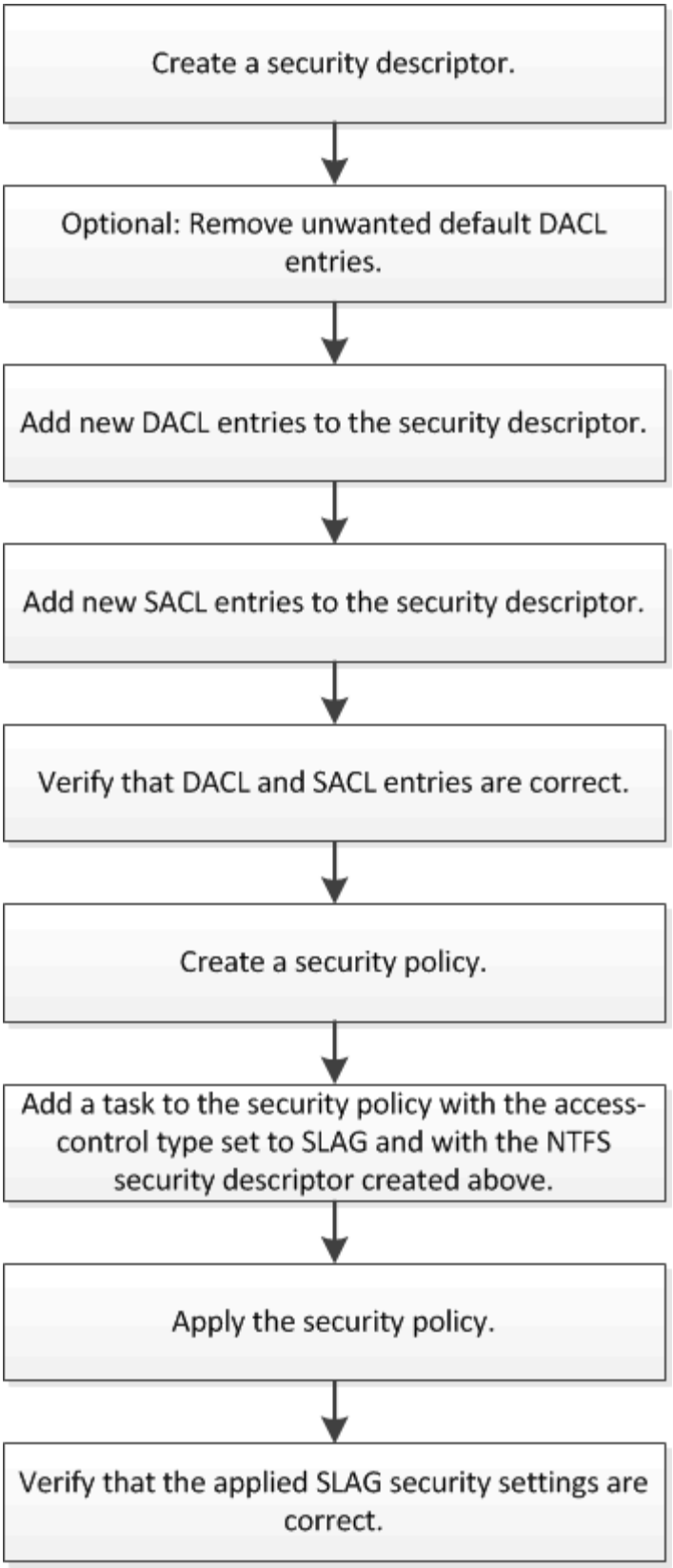
Storage-Level Access Guard는 클라이언트 측에서 볼 수 없는 스토리지 수준에서 추가 보안을 제공하므로 사용자 또는 관리자가 데스크톱에서 해당 보안을 취소할 수 없습니다. 스토리지 레벨에서 액세스를 제어하는 기능이 유용하다고 볼 수 있는 특정 사용 사례가 있습니다.

이 기능의 일반적인 사용 사례는 다음과 같습니다.

- 스토리지 수준에서 모든 사용자의 액세스를 감사 및 제어하여 지적 재산권을 보호합니다
- 은행 및 거래 그룹을 비롯한 금융 서비스 기업을 위한 스토리지
- 정부 서비스 및 개별 부서용 개별 파일 스토리지
- 모든 학생 파일을 보호하는 대학

Storage-Level Access Guard를 구성하는 워크플로우

스토리지 레벨 액세스 가드(slag)를 구성하는 워크플로에서는 NTFS 파일 권한 및 감사 정책을 구성하는 데 사용하는 것과 동일한 ONTAP CLI 명령을 사용합니다. 지정된 대상에서 파일 및 디렉토리 액세스를 구성하는 대신 지정된 SVM(스토리지 가상 머신) 볼륨의 슬래그를 구성합니다.



관련 정보

Storage-Level Access Guard 구성

Storage-Level Access Guard를 구성합니다

볼륨 또는 qtree에 스토리지 레벨 액세스 가드를 구성하려면 여러 단계를 수행해야 합니다. Storage-Level Access Guard는 스토리지 레벨에서 설정된 액세스 보안 수준을 제공합니다. 모든 NAS 프로토콜에서 적용된 스토리지 객체에 대한 모든 액세스에 적용되는 보안을 제공합니다.

단계

1. 'vserver security file-directory NTFS create' 명령을 사용하여 보안 설명자를 생성합니다.

   '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              -
   ```

   보안 설명자는 다음 네 가지 기본 ACE(DACL 액세스 제어 항목)를 사용하여 만들어집니다.

   ```
   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
   ```

   Storage-Level Access Guard를 구성할 때 기본 항목을 사용하지 않으려면 보안 설명자에 고유한 ACE를 만들고 추가하기 전에 해당 항목을 제거할 수 있습니다.

2. Storage-Level Access Guard 보안으로 구성하지 않으려는 보안 설명자에서 기본 DACL ACE 중 하나를 제거합니다.

a. 'vserver security file-directory NTFS DACL remove' 명령을 사용하여 불필요한 DACL ACE를 제거합니다.

   이 예제에서는 세 개의 기본 DACL ACE가 보안 설명자인 BUILTIN\Administrators, BUILTIN\Users 및 Creator Owner에서 제거됩니다.

   '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-directory vs1-access-directs builtl-creator' vserver security file-directs -directs -ntfs -directs -ntfs -directs -directs -creator

b. 'vserver security file-directory NTFS DACL show' 명령을 사용하여 스토리지 수준 액세스 가드 보안에 사용하지 않을 DACL ACE가 보안 설명자에서 제거되었는지 확인합니다.

   이 예제에서 명령의 출력은 NT AUTHORITY\SYSTEM DEFAULT DACL ACE 항목만 남겨 두고 세 개의 기본 DACL ACE가 보안 설명자에서 제거되었는지 확인합니다.

   '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' 명령을 사용하여 하나 이상의 DACL 항목을 보안 설명자에 추가합니다.

   이 예제에서는 보안 설명자에 두 개의 DACL ACE가 추가됩니다.

   '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-access-type allow-account" example\Domain Users"-read-folders 폴더에 대한 읽기 권한

4. 'vserver security file-directory NTFS SACL add' 명령을 사용하여 하나 이상의 SACL 항목을 보안 설명자에 추가합니다.

   이 예제에서는 두 개의 SACL ACE가 보안 설명자에 추가됩니다.

   '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-access-type success-account example\engineering-folders full-control-folders

5. 'vserver security file-directory NTFS DACL show' 및 'vserver security file-directory NTFS SACL show' 명령을 각각 사용하여 DACL 및 SACL ACE가 올바르게 구성되었는지 확인합니다.

   이 예제에서 다음 명령은 보안 설명자 "'Sd1'"의 DACL 항목에 대한 정보를 표시합니다.

'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
```

이 예제에서 다음 명령은 보안 설명자 "'sd1'"에 대한 SACL 항목에 대한 정보를 표시합니다.

'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' 명령을 사용하여 보안 정책을 생성합니다.

   다음 예제에서는 ""정책1""이라는 정책을 만듭니다.

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

7. 'vserver security file-directory policy show' 명령을 사용하여 정책이 올바르게 구성되었는지 확인합니다.

   'vserver security file-directory policy show'를 선택합니다

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

8. 을 사용하여 연결된 보안 설명자가 있는 작업을 보안 정책에 추가합니다 `vserver security file-directory policy task add` 명령과 함께 `-access-control` 매개 변수를 로 설정합니다 `slag`.

   정책에 둘 이상의 Storage-Level Access Guard 작업이 포함될 수 있지만 파일 디렉터리 및 Storage-Level Access Guard 작업을 모두 포함하도록 정책을 구성할 수는 없습니다. 정책에는 모든 스토리지 레벨 액세스 가드 작업 또는 모든 파일 디렉토리 작업이 포함되어야 합니다.

   이 예제에서는 보안 설명자 'Sd1'에 할당된 "정책1"이라는 정책에 작업이 추가됩니다. 액세스 제어 유형이 '슬래그'로 설정된 '/datavol1' 경로에 할당됩니다.

   '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' 명령을 사용하여 작업이 올바르게 구성되었는지 확인합니다.

   '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' 명령을 사용하여 Storage-Level Access Guard 보안 정책을 적용합니다.

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

    보안 정책을 적용할 작업이 예약됩니다.

11. 'vserver security file-directory show' 명령을 사용하여 적용된 Storage-Level Access Guard 보안 설정이 올바른지 확인합니다.

    이 예제에서 명령의 출력은 스토리지 레벨 액세스 가드 보안이 NTFS 볼륨 '/datavol1'에 적용되었음을 보여 줍니다. 모든 사용자에게 모든 권한을 허용하는 기본 DACL이 그대로 유지되더라도 Storage-Level Access Guard 보안은 Storage-Level Access Guard 설정에 정의된 그룹에 대한 액세스를 제한(및 감사)합니다.

    '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
```

관련 정보

CLI를 사용하여 SVM에서 NTFS 파일 보안, NTFS 감사 정책 및 Storage-Level Access Guard를 관리합니다

Storage-Level Access Guard를 구성하는 워크플로우

Storage-Level Access Guard에 대한 정보 표시

Storage-Level Access Guard 제거

효과적인 슬래그 매트릭스

볼륨 또는 qtree 또는 둘 다에서 슬래그를 구성할 수 있습니다. 슬래그 매트릭스는 표에 나열된 다양한 시나리오에서 적용 가능한 슬래그 구성인 볼륨 또는 qtree를 정의합니다.

	AFS에서 볼륨 슬래그	스냅샷 복사본의 볼륨 슬래그	**AFS**에서 **qtree** 슬래그	스냅샷 복사본에서 **qtree** 슬래그 발생
AFS(Access File System)에서 볼륨 액세스	예	아니요	해당 없음	해당 없음
스냅샷 복사본의 볼륨 액세스	예	아니요	해당 없음	해당 없음
AFS에서 qtree 액세스(qtree에 슬래그가 있는 경우)	아니요	아니요	예	아니요
AFS에서 qtree 액세스(qtree에 슬래그가 없는 경우)	예	아니요	아니요	아니요
스냅샷 복사본에서 qtree 액세스(qtree AFS에 슬래그가 있는 경우)	아니요	아니요	예	아니요
스냅샷 복사본에서 qtree 액세스(qtree AFS에 슬래그가 없는 경우)	예	아니요	아니요	아니요

Storage-Level Access Guard에 대한 정보를 표시합니다

Storage-Level Access Guard는 볼륨 또는 qtree에 적용되는 세 번째 보안 계층입니다. Windows 속성 창을 사용하면 저장소 수준 액세스 가드 설정을 볼 수 없습니다. ONTAP CLI를 사용하여 스토리지 레벨 액세스 가드 보안에 대한 정보를 확인해야 합니다. 이 정보는 구성을 확인하거나 파일 액세스 문제를 해결하는 데 사용할 수 있습니다.

이 작업에 대해

SVM(Storage Virtual Machine)의 이름과 스토리지 레벨 액세스 가드 보안 정보를 표시할 볼륨 또는 qtree의 경로를 입력해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

단계

1. Storage-Level Access Guard 보안 설정을 원하는 수준으로 표시합니다.

정보를 표시하려면...	다음 명령을 입력합니다...
요약 양식	'vserver security file-directory show -vserver_vserver_name_-path_path_'
세부 정보가 확장됩니다	'vserver security file-directory show -vserver_vserver_name_-path_path_-expand-mask true'

예

다음 예에서는 SVM VS1 에서 경로 '/datavol1'을 사용하여 NTFS 보안 스타일 볼륨에 대한 Storage-Level Access Guard 보안 정보를 표시합니다.

```
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
```

다음 예에서는 SVM VS1 경로의 '/datavol5' 경로에서 혼합 보안 형식 볼륨에 대한 Storage-Level Access Guard 정보를 표시합니다. 이 볼륨의 최상위 수준에는 UNIX의 효과적인 보안이 있습니다. 이 볼륨에는 Storage-Level Access Guard 보안이 있습니다.

```
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
```

Storage-Level Access Guard를 제거합니다

저장소 수준에서 액세스 보안을 더 이상 설정하지 않으려면 볼륨 또는 qtree에서 저장소 수준 액세스 가드를 제거할 수 있습니다. Storage-Level Access Guard를 제거해도 일반 NTFS 파일 및 디렉터리 보안은 수정하거나 제거되지 않습니다.

단계

1. 'vserver security file-directory show' 명령을 사용하여 볼륨 또는 qtree에 Storage-Level Access Guard가 구성되어 있는지 확인합니다.

   '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' 명령을 사용하여 Storage-Level Access Guard를 제거합니다.

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

3. 'vserver security file-directory show' 명령을 사용하여 볼륨 또는 qtree에서 Storage-Level Access Guard가 제거되었는지 확인합니다.

   '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
```