파일 보안 및 감사 정책에 대한 정보를 표시합니다
ONTAP 9

NetApp
February 12, 2026

목차

파일 보안 및 감사 정책에 대한 정보를 표시합니다 . . . 1
ONTAP SMB 파일 보안 및 감사 정책 보기에 대해 알아보세요 . . . 1
파일 보안에 대한 정보 표시 . . . 1
감사 정책에 대한 정보 표시 . . . 1
스토리지 레벨 액세스 가드(슬래그) 보안에 대한 정보 표시 . . . 1
DAC(Dynamic Access Control) 보안에 대한 정보 표시 . . . 1
NTFS 보안 스타일 볼륨에서 ONTAP SMB 파일 보안에 대한 정보 표시 . . . 2
혼합 보안 스타일 볼륨에서 ONTAP SMB 파일 보안에 대한 정보 표시 . . . 8
UNIX 보안 스타일 볼륨에서 ONTAP SMB 파일 보안에 대한 정보 표시 . . . 11
SMB FlexVol 볼륨의 NTFS 감사 정책에 대한 정보를 표시하는 ONTAP 명령 . . . 14
SMB FlexVol 볼륨의 NFSv4 감사 정책에 대한 정보를 표시하는 ONTAP 명령 . . . 17
ONTAP SMB 파일 보안 및 감사 정책 정보를 표시하는 방법을 알아보세요. . . . 18

파일 보안 및 감사 정책에 대한 정보를 표시합니다

ONTAP SMB 파일 보안 및 감사 정책 보기에 대해 알아보세요

SVM(스토리지 가상 머신)의 볼륨 내에 포함된 파일 및 디렉토리의 파일 보안에 대한 정보를 표시할 수 있습니다. FlexVol 볼륨의 감사 정책에 대한 정보를 표시할 수 있습니다. 구성된 경우 FlexVol 볼륨의 저장소 수준 액세스 가드 및 동적 액세스 제어 보안 설정에 대한 정보를 표시할 수 있습니다.

파일 보안에 대한 정보 표시

다음 보안 스타일을 사용하여 볼륨 및 Qtree(FlexVol 볼륨의 경우) 내에 포함된 데이터에 적용되는 파일 보안에 대한 정보를 표시할 수 있습니다.

- NTFS입니다
- Unix
- 혼합

감사 정책에 대한 정보 표시

다음 NAS 프로토콜을 통해 FlexVol 볼륨의 액세스 이벤트를 감사하기 위한 감사 정책에 대한 정보를 표시할 수 있습니다.

- SMB(모든 버전)
- NFSv4.x

스토리지 레벨 액세스 가드(슬래그) 보안에 대한 정보 표시

스토리지 레벨 액세스 가드 보안은 FlexVol 볼륨 및 qtree 개체에 다음 보안 스타일로 적용할 수 있습니다.

- NTFS입니다
- 혼합
- UNIX(볼륨을 포함하는 SVM에서 CIFS 서버가 구성된 경우)

DAC(Dynamic Access Control) 보안에 대한 정보 표시

동적 액세스 제어 보안은 다음 보안 스타일을 사용하여 FlexVol 볼륨 내의 개체에 적용할 수 있습니다.

- NTFS입니다
- 혼합(오브젝트에 NTFS 유효 보안이 있는 경우)

관련 정보

- Storage-Level Access Guard를 사용하여 안전한 파일 액세스에 대해 알아보세요
- 서버의 Storage-Level Access Guard에 대한 정보 표시

NTFS 보안 스타일 볼륨에서 ONTAP SMB 파일 보안에 대한 정보 표시

NTFS 보안 스타일 볼륨의 파일 및 디렉터리 보안에 대한 정보(보안 스타일 및 효과적인 보안 스타일, 적용되는 권한, DOS 속성 정보 등)를 표시할 수 있습니다. 결과를 사용하여 보안 구성을 확인하거나 파일 액세스 문제를 해결할 수 있습니다.

이 작업에 대해

SVM(스토리지 가상 시스템)의 이름과 파일 또는 폴더 보안 정보를 표시할 데이터의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

- NTFS 보안 스타일 볼륨 및 qtree는 파일 액세스 권한을 결정할 때 NTFS 파일 권한과 Windows 사용자 및 그룹만 사용하므로 UNIX 관련 출력 필드에는 표시 전용 UNIX 파일 권한 정보가 포함됩니다.
- ACL 출력은 NTFS 보안이 설정된 파일 및 폴더에 대해 표시됩니다.
- 볼륨 루트 또는 qtree에서 Storage-Level Access Guard 보안을 구성할 수 있으므로 Storage-Level Access Guard가 구성된 볼륨 또는 qtree 경로의 출력에는 일반 파일 ACL과 Storage-Level Access Guard ACL이 모두 표시될 수 있습니다.
- 또한 동적 액세스 제어가 지정된 파일 또는 디렉터리 경로에 대해 구성된 경우 이 출력에는 동적 액세스 제어 ACE에 대한 정보도 표시됩니다.

단계

1. 파일 및 디렉터리 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 예제는 SVM VS1 경로의 /vol4" 보안 정보를 보여줍니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                                Vserver: vs1
                              File Path: /vol4
                      File Inode Number: 64
                         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
```

다음 예에서는 SVM VS1 경로의 /data/engineering에 대한 확장된 마스크와 함께 보안 정보를 표시합니다.

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

다음 예에서는 SVM VS1 에서 경로 '/datavol1'이 있는 볼륨에 대한 Storage-Level Access Guard 보안 정보를 비롯한 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
```

관련 정보

- 혼합 보안 형식 볼륨의 파일 보안에 대한 정보를 표시합니다
- UNIX 보안 스타일 볼륨의 파일 보안에 대한 정보를 표시합니다

혼합 보안 스타일 볼륨에서 **ONTAP SMB** 파일 보안에 대한 정보 표시

보안 스타일 및 효과적인 보안 스타일, 적용되는 사용 권한, UNIX 소유자 및 그룹에 대한 정보 등 혼합 보안 스타일 볼륨에 대한 파일 및 디렉터리 보안에 대한 정보를 표시할 수 있습니다. 결과를 사용하여 보안 구성을 확인하거나 파일 액세스 문제를 해결할 수 있습니다.

이 작업에 대해

SVM(스토리지 가상 시스템)의 이름과 파일 또는 폴더 보안 정보를 표시할 데이터의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

- 혼합 보안 스타일 볼륨 및 qtree에는 모드 비트 또는 NFSv4 ACL, NTFS 파일 권한을 사용하는 일부 파일 및 디렉토리 등 UNIX 파일 권한을 사용하는 일부 파일 및 폴더가 포함될 수 있습니다.
- 혼합 보안 형식 볼륨의 최상위 수준에는 UNIX 또는 NTFS의 효과적인 보안이 있을 수 있습니다.
- ACL 출력은 NTFS 또는 NFSv4 보안이 설정된 파일 및 폴더에만 표시됩니다.

  모드 비트 권한만 적용된 UNIX 보안을 사용하는 파일 및 디렉토리의 경우 이 필드는 비어 있습니다(NFSv4 ACL 없음).

- ACL 출력의 소유자 및 그룹 출력 필드는 NTFS 보안 설명자의 경우에만 적용됩니다.
- 볼륨 루트 또는 qtree의 효과적인 보안 스타일이 UNIX인 경우에도 스토리지 레벨 액세스 가드 보안을 혼합 보안 스타일 볼륨 또는 qtree로 구성할 수 있으므로 Storage-Level Access Guard가 구성된 볼륨 또는 qtree 경로의 출력에는 UNIX 파일 사용 권한과 Storage-Level Access Guard ACL이 모두 표시될 수 있습니다.
- 명령에 입력한 경로가 NTFS 유효 보안을 사용하는 데이터인 경우 해당 파일 또는 디렉토리 경로에 동적 액세스 제어가 구성되어 있으면 동적 액세스 제어 ACE에 대한 정보도 출력에 표시됩니다.

단계

1. 파일 및 디렉터리 보안 설정을 원하는 수준으로 표시합니다.

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

예

다음 예에서는 SVM VS1 경로 '/projects'에 대한 보안 정보를 확장된 마스크 형식으로 표시합니다. 이 혼합 보안 방식 경로에는 UNIX의 효과적인 보안이 있습니다.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

                Vserver: vs1
              File Path: /projects
      File Inode Number: 78
         Security Style: mixed
        Effective Style: unix
         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: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

다음 예제는 SVM VS1 경로 '/data'에 대한 보안 정보를 보여줍니다. 이 혼합 보안 방식 경로에는 NTFS의 효과적인 보안이 있습니다.

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

                                Vserver: vs1
                              File Path: /data
                      File Inode Number: 544
                         Security Style: mixed
                        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
```

다음 예에서는 SVM VS1 경로의 '/datavol5' 경로에 있는 볼륨에 대한 보안 정보를 표시합니다. 이러한 혼합 보안 유형의 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
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
```

관련 정보

- NTFS 보안 스타일 볼륨의 파일 보안에 대한 정보를 표시합니다
- UNIX 보안 스타일 볼륨의 파일 보안에 대한 정보를 표시합니다

UNIX 보안 스타일 볼륨에서 ONTAP SMB 파일 보안에 대한 정보 표시

UNIX 보안 스타일 볼륨의 파일 및 디렉터리 보안에 대한 정보(보안 스타일 및 효과적인 보안

스타일, 적용되는 사용 권한, UNIX 소유자 및 그룹에 대한 정보 등)를 표시할 수 있습니다. 결과를 사용하여 보안 구성을 확인하거나 파일 액세스 문제를 해결할 수 있습니다.

이 작업에 대해

SVM(스토리지 가상 시스템)의 이름과 파일 또는 디렉토리 보안 정보를 표시할 데이터의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

- UNIX 보안 스타일 볼륨 및 qtree는 파일 액세스 권한을 결정할 때 모드 비트 또는 NFSv4 ACL 중 하나의 UNIX 파일 권한만 사용합니다.
- NFSv4 보안이 설정된 파일 및 폴더에 대해서만 ACL 출력이 표시됩니다.

  모드 비트 권한만 적용된 UNIX 보안을 사용하는 파일 및 디렉토리의 경우 이 필드는 비어 있습니다(NFSv4 ACL 없음).

- NFSv4 보안 설명자의 경우 ACL 출력의 소유자 및 그룹 출력 필드는 적용되지 않습니다.

  NTFS 보안 설명자에만 의미가 있습니다.

- SVM에 CIFS 서버가 구성된 경우 UNIX 볼륨 또는 qtree에서 Storage-Level Access Guard 보안이 지원되므로 '-path' 매개 변수에 지정된 볼륨 또는 qtree에 적용된 Storage-Level Access Guard 보안에 대한 정보가 출력에 포함될 수 있습니다.

단계

1. 파일 및 디렉터리 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 예제는 SVM VS1 경로의 / home 경로에 대한 보안 정보를 표시합니다.

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

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 1
                          Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

다음 예에서는 SVM VS1 경로의 / home 경로에 대한 보안 정보를 확장된 마스크 형식으로 표시합니다.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         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: 1
                         Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

관련 정보

- 보안 스타일 볼륨의 파일 보안에 대한 정보 표시
- 혼합 보안 형식 볼륨의 파일 보안에 대한 정보를 표시합니다

SMB FlexVol 볼륨의 NTFS 감사 정책에 대한 정보를 표시하는 ONTAP 명령

FlexVol 볼륨에서 보안 스타일 및 효과적인 보안 스타일의 정의, 적용되는 권한 및 시스템 액세스 제어 목록에 대한 정보를 포함하여 NTFS 감사 정책에 대한 정보를 표시할 수 있습니다. 결과를 사용하여 보안 구성을 확인하거나 감사 문제를 해결할 수 있습니다.

이 작업에 대해

SVM(스토리지 가상 시스템)의 이름과 감사 정보를 표시할 파일 또는 폴더의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

- NTFS 보안 스타일 볼륨 및 qtree는 감사 정책에 NTFS SACL(시스템 액세스 제어 목록)만 사용합니다.
- NTFS 효과적인 보안이 적용된 혼합 보안 스타일 볼륨의 파일과 폴더에 NTFS 감사 정책이 적용될 수 있습니다.

  혼합 보안 스타일 볼륨 및 qtree에는 모드 비트 또는 NFSv4 ACL, NTFS 파일 권한을 사용하는 일부 파일 및 디렉토리 등 UNIX 파일 권한을 사용하는 일부 파일과 디렉토리가 포함될 수 있습니다.

- 혼합 보안 형식 볼륨의 최상위 수준에는 UNIX 또는 NTFS의 효과적인 보안이 포함될 수 있으며 NTFS SACL이 포함될 수도 있고 포함되지 않을 수도 있습니다.
- 볼륨 루트 또는 qtree의 효과적인 보안 스타일이 UNIX인 경우에도 스토리지 레벨 액세스 가드 보안을 혼합 보안 스타일 볼륨 또는 qtree로 구성할 수 있으므로 Storage-Level Access Guard가 구성된 볼륨 또는 qtree 경로의 출력에는 일반 파일 및 폴더 NFSv4 SACL 및 Storage-Level Access Guard NTFS SACL이 모두 표시될 수 있습니다.
- 명령에 입력한 경로가 NTFS 유효 보안을 사용하는 데이터인 경우 해당 파일 또는 디렉토리 경로에 동적 액세스 제어가 구성되어 있으면 동적 액세스 제어 ACE에 대한 정보도 출력에 표시됩니다.
- NTFS 유효 보안이 있는 파일 및 폴더에 대한 보안 정보를 표시할 때 UNIX 관련 출력 필드에는 표시 전용 UNIX 파일 권한 정보가 포함됩니다.

  NTFS 보안 스타일 파일 및 폴더는 파일 액세스 권한을 결정할 때 NTFS 파일 권한과 Windows 사용자 및 그룹만 사용합니다.

- ACL 출력은 NTFS 또는 NFSv4 보안이 설정된 파일 및 폴더에만 표시됩니다.

  모드 비트 권한만 적용된 UNIX 보안을 사용하는 파일 및 폴더의 경우 이 필드는 비어 있습니다(NFSv4 ACL 없음).

- ACL 출력의 소유자 및 그룹 출력 필드는 NTFS 보안 설명자의 경우에만 적용됩니다.

단계

1. 파일 및 디렉터리 감사 정책 설정을 원하는 수준으로 표시합니다.

정보를 표시하려면...	다음 명령을 입력합니다...
요약 양식	'vserver security file-directory show -vserver vserver_name -path path path'

정보를 표시하려면...	다음 명령을 입력합니다...
를 참조하십시오	'vserver security file-directory show -vserver vserver_name -path path path -expand-mask true'

예

다음 예에서는 SVM VS1 경로의 /Corp 경로에 대한 감사 정책 정보를 표시합니다. 경로에 NTFS 유효 보안이 있습니다. NTFS 보안 설명자는 성공 및 성공/실패 SACL 항목을 모두 포함합니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         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
```

다음 예제는 SVM VS1 경로의 /datavol1 경로에 대한 감사 정책 정보를 표시합니다. 이 경로에는 일반 파일 및 폴더 SACL과 Storage-Level Access Guard SACL이 모두 포함됩니다.

```
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:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         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
```

SMB FlexVol 볼륨의 NFSv4 감사 정책에 대한 정보를 표시하는 ONTAP 명령

보안 스타일 및 효과적인 보안 스타일의 정의, 적용되는 권한 및 SACL(시스템 액세스 제어 목록)에 대한 정보를 포함하여 ONTAP CLI를 사용하여 FlexVol 볼륨에서 NFSv4 감사 정책에 대한 정보를 표시할 수 있습니다. 결과를 사용하여 보안 구성을 확인하거나 감사 문제를 해결할 수 있습니다.

이 작업에 대해

SVM(스토리지 가상 시스템)의 이름과 감사 정보를 표시할 파일 또는 디렉토리의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

- UNIX 보안 스타일 볼륨 및 qtree는 감사 정책에 NFSv4 SACL만 사용합니다.
- UNIX 보안 스타일의 혼합 보안 스타일 볼륨에 있는 파일과 디렉토리에는 NFSv4 감사 정책이 적용될 수 있습니다.

  혼합 보안 스타일 볼륨 및 qtree에는 모드 비트 또는 NFSv4 ACL, NTFS 파일 권한을 사용하는 일부 파일 및 디렉토리 등 UNIX 파일 권한을 사용하는 일부 파일과 디렉토리가 포함될 수 있습니다.

- 혼합 보안 형식 볼륨의 최상위 수준은 UNIX 또는 NTFS의 유효 보안을 가질 수 있으며 NFSv4 SACL을 포함하거나 포함하지 않을 수 있습니다.
- ACL 출력은 NTFS 또는 NFSv4 보안이 설정된 파일 및 폴더에만 표시됩니다.

  모드 비트 권한만 적용된 UNIX 보안을 사용하는 파일 및 폴더의 경우 이 필드는 비어 있습니다(NFSv4 ACL 없음).

- ACL 출력의 소유자 및 그룹 출력 필드는 NTFS 보안 설명자의 경우에만 적용됩니다.
- 볼륨 루트 또는 qtree의 효과적인 보안 스타일이 UNIX인 경우에도 스토리지 레벨 액세스 가드 보안을 혼합 보안 스타일 볼륨 또는 qtree로 구성할 수 있으므로 Storage-Level Access Guard가 구성된 볼륨 또는 qtree 경로의 출력에는 일반 NFSv4 파일 및 디렉터리 SACL과 Storage-Level Access Guard NTFS SACL이 모두 표시될 수 있습니다.
- SVM에 CIFS 서버가 구성된 경우 UNIX 볼륨 또는 qtree에서 Storage-Level Access Guard 보안이 지원되므로 '-path' 매개 변수에 지정된 볼륨 또는 qtree에 적용된 Storage-Level Access Guard 보안에 대한 정보가 출력에 포함될 수 있습니다.

단계

1. 파일 및 디렉터리 보안 설정을 원하는 수준으로 표시합니다.

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

예

다음 예제는 SVM VS1 경로 /lab에 대한 보안 정보를 보여 줍니다. 이 UNIX 보안 스타일 경로에는 NFSv4 SACL이 있습니다.

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

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

ONTAP SMB 파일 보안 및 감사 정책 정보를 표시하는 방법을 알아보세요.

와일드카드 문자(*)를 사용하여 지정된 경로 또는 루트 볼륨 아래에 있는 모든 파일 및 디렉토리의 파일 보안 및 감사 정책에 대한 정보를 표시할 수 있습니다.

와일드카드 문자(*)는 모든 파일 및 디렉터리의 정보를 표시할 아래의 지정된 디렉터리 경로의 마지막 하위 구성 요소로 사용할 수 있습니다. "" * ""로 명명된 특정 파일이나 디렉터리의 정보를 표시하려면 큰따옴표("""") 안에 전체 경로를 제공해야 합니다.

예

와일드카드 문자를 사용하여 다음 명령을 실행하면 SVM VS1 경로의 '/1/' 아래에 있는 모든 파일 및 디렉토리에 대한 정보가 표시됩니다.

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
            Security Style: mixed
           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:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
            Security Style: mixed
           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:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

다음 명령을 실행하면 SVM VS1 의 path '/vol1/a' 아래에 " * "로 명명된 파일의 정보가 표시됩니다. 경로는 큰따옴표(" ")로 묶습니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                Vserver: vs1
              File Path: "/vol1/a/*"
      Security Style: mixed
     Effective Style: unix
      DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
         Unix User Id: 1002
        Unix Group Id: 65533
       Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                 ACLs: NFSV4 Security Descriptor
                       Control:0x8014
                       SACL - ACEs
                         AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                       DACL - ACEs
                         ALLOW-EVERYONE@-0x1f00a9-FI|DI
                         ALLOW-OWNER@-0x1f01ff-FI|DI
                         ALLOW-GROUP@-0x1200a9-IG
```

저작권 정보

상표 정보