파일 및 디렉토리에 적용된 감사 정책에 대한 정보를 표시합니다

ONTAP 9

NetApp
April 24, 2024

목차

파일 및 디렉토리에 적용된 감사 정책에 대한 정보를 표시합니다

Windows 보안 탭을 사용하여 감사 정책에 대한 정보를 표시합니다

Windows 속성 창의 보안 탭을 사용하여 파일 및 디렉터리에 적용된 감사 정책에 대한 정보를 표시할 수 있습니다. 이는 Windows 서버에 있는 데이터에 사용되는 것과 동일한 방법으로, 고객이 익숙한 GUI 인터페이스를 사용할 수 있습니다.

이 작업에 대해

파일 및 디렉터리에 적용된 감사 정책에 대한 정보를 표시하면 지정된 파일 및 폴더에 적절한 SACL(시스템 액세스 제어 목록)이 설정되어 있는지 확인할 수 있습니다.

NTFS 파일 및 폴더에 적용된 SACL에 대한 정보를 표시하려면 Windows 호스트에서 다음 단계를 수행하십시오.

단계

1. Windows 탐색기의 * Tools * 메뉴에서 * Map network drive * 를 선택합니다.
2. 네트워크 드라이브 연결 * 대화 상자를 완료합니다.

   a. 드라이브 * 문자를 선택합니다.

   b. 폴더 * 상자에 감사할 데이터와 공유 이름을 둘 다 포함하는 공유가 포함된 SVM(스토리지 가상 시스템)의 IP 주소 또는 SMB 서버 이름을 입력합니다.

      SMB 서버 이름이 "smb_server"이고 공유 이름이 "hay1"인 경우 \\smb_server\share1"을 입력해야 합니다.

      SMB 서버 이름 대신 SMB 서버에 대한 데이터 인터페이스의 IP 주소를 지정할 수 있습니다.

   c. 마침 * 을 클릭합니다.

   선택한 드라이브가 마운트되고 공유 내에 포함된 파일 및 폴더를 표시하는 Windows 탐색기 창이 준비됩니다.

3. 감사 정보를 표시할 파일 또는 디렉터리를 선택합니다.
4. 파일 또는 디렉토리를 마우스 오른쪽 버튼으로 클릭하고 * 속성 * 을 선택합니다.
5. 보안 * 탭을 선택합니다.
6. 고급 * 을 클릭합니다.
7. 감사 * 탭을 선택합니다.
8. 계속 * 을 클릭합니다.

   감사 상자가 열립니다. 감사 항목 * 상자에는 SACL이 적용된 사용자 및 그룹의 요약이 표시됩니다.

9. 감사 항목 * 상자에서 SACL 항목을 표시할 사용자 또는 그룹을 선택합니다.
10. 편집 * 을 클릭합니다.

    object>에 대한 감사 항목이 열립니다.

11. Access* 상자에서 선택한 개체에 적용된 현재 SACL을 확인합니다.
12. 객체> * 에 대한 * 감사 항목을 닫으려면 * 취소 * 를 클릭합니다.
13. 취소 * 를 클릭하여 * 감사 * 상자를 닫습니다.

CLI를 사용하여 FlexVol 볼륨의 NTFS 감사 정책에 대한 정보를 표시합니다

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. 이 정보를 사용하여 보안 구성을 확인하거나 감사 문제를 해결할 수 있습니다.

이 작업에 대해

파일 및 디렉터리에 적용된 감사 정책에 대한 정보를 표시하면 지정된 파일 및 폴더에 적절한 SACL(시스템 액세스 제어 목록)이 설정되어 있는지 확인할 수 있습니다.

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'
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
```

파일 보안 및 감사 정책에 대한 정보를 표시하는 방법

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 파일 또는 디렉토리의 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
```