# 보안 스타일이 데이터 액세스에 미치는 영향

## ONTAP 9

NetApp
September 12, 2024

# 목차

# 보안 스타일이 데이터 액세스에 미치는 영향

## 보안 스타일 및 효과

UNIX, NTFS, 혼합 및 통합 등 네 가지 보안 유형이 있습니다. 각 보안 스타일은 데이터에 대한 사용 권한이 처리되는 방식에 다른 영향을 줍니다. 용도에 맞는 적절한 보안 스타일을 선택할 수 있도록 다양한 효과를 이해해야 합니다.

보안 스타일은 클라이언트 유형이 데이터에 액세스할 수 있거나 액세스할 수 없는 형식을 결정하지 않는다는 점을 이해하는 것이 중요합니다. 보안 스타일은 ONTAP에서 데이터 액세스를 제어하는 데 사용하는 권한 유형과 이러한 권한을 수정할 수 있는 클라이언트 유형만 결정합니다.

예를 들어, 볼륨이 UNIX 보안 스타일을 사용하는 경우에도 SMB 클라이언트는 ONTAP의 멀티 프로토콜 특성으로 인해 데이터에 액세스(적절하게 인증 및 승인)할 수 있습니다. 그러나 ONTAP에서는 UNIX 클라이언트만 기본 툴을 사용하여 수정할 수 있는 UNIX 권한을 사용합니다.

| 보안 스타일 | 사용 권한을 수정할 수 있는 클라이언트입니다 | 클라이언트가 사용할 수 있는 권한 | 결과적으로 효율적인 보안 스타일을 제공합니다 | 파일에 액세스할 수 있는 클라이언트입니다 |
|---|---|---|---|---|
| Unix | NFS 를 참조하십시오 | NFSv3 모드 비트 | Unix | NFS 및 SMB |
| | | NFSv4.x ACL | | |
| NTFS입니다 | 중소기업 | NTFS ACL | NTFS입니다 | |
| 혼합 | NFS 또는 SMB | NFSv3 모드 비트 | Unix | |
| | | NFSv4.ACL | | |
| | | NTFS ACL | NTFS입니다 | |
| 통합(ONTAP 9.4 및 이전 릴리즈에서 무한 확장 볼륨에만 해당) | NFS 또는 SMB | NFSv3 모드 비트 | Unix | |
| | | NFSv4.1 ACL | | |
| | | NTFS ACL | NTFS입니다 | |

FlexVol 볼륨은 UNIX, NTFS 및 혼합 보안 스타일을 지원합니다. 보안 스타일이 혼합 또는 통합된 경우 사용자가 보안 스타일을 개별적으로 설정하므로 사용자가 마지막으로 권한을 수정한 클라이언트 유형에 따라 유효 사용 권한이 달라집니다. 권한을 수정한 마지막 클라이언트가 NFSv3 클라이언트인 경우 사용 권한은 UNIX NFSv3 모드 비트입니다. 마지막 클라이언트가 NFSv4 클라이언트인 경우 사용 권한은 NFSv4 ACL입니다. 마지막 클라이언트가 SMB 클라이언트인 경우 사용 권한은 Windows NTFS ACL입니다.

통합 보안 스타일은 ONTAP 9.5 이상 릴리스에서 더 이상 지원되지 않는 무한 볼륨에서만 사용할 수 있습니다. 자세한 내용은 을 참조하십시오 FlexGroup 볼륨 관리 개요.

ONTAP 9.2부터 vserver security file-directory 명령에 대한 'show-Effective-permissions' 매개 변수를 사용하면 지정된 파일 또는 폴더 경로에서 Windows 또는 UNIX 사용자에게 부여된 유효한 권한을 표시할 수 있습니다. 또한 선택적 매개 변수 '-share-name'을 사용하면 유효 공유 권한을 표시할 수 있습니다.

ONTAP는 처음에 일부 기본 파일 권한을 설정합니다. 기본적으로 UNIX, 혼합 및 통합 보안 스타일 볼륨의 모든 데이터에 대한 효과적인 보안 스타일은 UNIX이고, 기본 보안 스타일에 의해 허용되는 대로 클라이언트에 의해 구성될 때까지 유효 사용 권한 유형은 UNIX 모드 비트(별도로 지정하지 않는 경우 0755)입니다. 기본적으로 NTFS 보안 스타일 볼륨의 모든 데이터에 대한 효과적인 보안 스타일은 NTFS이며 ACL을 통해 모든 사람에게 모든 권한을 제공할 수 있습니다.

## 보안 스타일을 설정하는 위치 및 시기

보안 스타일은 FlexVol 볼륨(루트 또는 데이터 볼륨) 및 qtree에서 설정할 수 있습니다. 보안 스타일은 생성 시 수동으로 설정하거나 자동으로 상속하거나 나중에 변경할 수 있습니다.

## SVM에 사용할 보안 유형을 결정합니다

볼륨에 사용할 보안 스타일을 결정하는 데 도움이 되도록 두 가지 요소를 고려해야 합니다. 기본 요소는 파일 시스템을 관리하는 관리자 유형입니다. 2차 요소는 볼륨의 데이터에 액세스하는 사용자 또는 서비스의 유형입니다.

볼륨에 보안 스타일을 구성할 때는 최상의 보안 스타일을 선택하고 사용 권한 관리 문제를 피하기 위해 환경의 요구 사항을 고려해야 합니다. 다음 고려 사항을 통해 결정을 내릴 수 있습니다.

| 보안 스타일 | 다음 경우에 선택... |
| --- | --- |
| Unix | • 파일 시스템은 UNIX 관리자가 관리합니다.<br>• 대부분의 사용자는 NFS 클라이언트입니다.<br>• 데이터에 액세스하는 애플리케이션은 UNIX 사용자를 서비스 계정으로 사용합니다. |
| NTFS입니다 | • 파일 시스템은 Windows 관리자가 관리합니다.<br>• 대부분의 사용자는 SMB 클라이언트입니다.<br>• 데이터에 액세스하는 응용 프로그램은 Windows 사용자를 서비스 계정으로 사용합니다. |
| 혼합 | 파일 시스템은 UNIX 관리자와 Windows 관리자 모두에서 관리되며 사용자는 NFS 클라이언트와 SMB 클라이언트로 구성됩니다. |

## 보안 스타일 상속의 작동 방식

새 FlexVol 볼륨 또는 qtree를 생성할 때 보안 스타일을 지정하지 않으면 보안 스타일이 다른 방식으로 상속됩니다.

보안 스타일은 다음과 같은 방식으로 상속됩니다.

- FlexVol 볼륨은 SVM이 포함된 루트 볼륨의 보안 스타일을 상속합니다.

- qtree는 포함된 FlexVol 볼륨의 보안 스타일을 상속합니다.
- 파일 또는 디렉토리는 포함된 FlexVol 볼륨 또는 qtree의 보안 스타일을 상속합니다.

# ONTAP에서 UNIX 사용 권한을 유지하는 방법

## 현재 UNIX 사용 권한이 있는 FlexVol 볼륨의 파일을 Windows 응용 프로그램에서 편집하고 저장하면 ONTAP에서 UNIX 사용 권한을 보존할 수 있습니다.

Windows 클라이언트의 응용 프로그램이 파일을 편집하고 저장할 때 파일의 보안 속성을 읽고, 새 임시 파일을 만들고, 해당 속성을 임시 파일에 적용한 다음 임시 파일에 원래 파일 이름을 지정합니다.

Windows 클라이언트가 보안 속성에 대한 쿼리를 수행할 때 UNIX 권한을 정확하게 나타내는 생성된 ACL을 받습니다. 이 생성된 ACL의 유일한 목적은 파일이 Windows 애플리케이션에 의해 업데이트되므로 파일의 UNIX 사용 권한을 보존하여 결과 파일이 동일한 UNIX 사용 권한을 갖도록 하는 것입니다. ONTAP는 생성된 ACL을 사용하여 NTFS ACL을 설정하지 않습니다.

# Windows 보안 탭을 사용하여 UNIX 사용 권한을 관리합니다

## SVM에서 혼합 보안 스타일 볼륨 또는 qtree의 파일 또는 폴더에 대한 UNIX 권한을 조작하려는 경우 Windows 클라이언트의 보안 탭을 사용할 수 있습니다. 또는 Windows ACL을 쿼리하고 설정할 수 있는 응용 프로그램을 사용할 수도 있습니다.

- UNIX 사용 권한 수정

  Windows 보안 탭을 사용하여 혼합 보안 스타일 볼륨 또는 qtree에 대한 UNIX 권한을 보고 변경할 수 있습니다. 기본 Windows 보안 탭을 사용하여 UNIX 권한을 변경하는 경우 변경하기 전에 먼저 편집할 기존 ACE(모드 비트를 0으로 설정)를 제거해야 합니다. 또는 고급 편집기를 사용하여 권한을 변경할 수도 있습니다.

  모드 권한을 사용하는 경우 나열된 UID, GID 및 기타(컴퓨터에 계정이 있는 다른 모든 사용자)에 대한 모드 권한을 직접 변경할 수 있습니다. 예를 들어, 표시된 UID에 r-x 권한이 있는 경우 UID 권한을 rwx로 변경할 수 있습니다.

- UNIX 권한을 NTFS 권한으로 변경합니다

  Windows 보안 탭을 사용하면 파일 및 폴더에 UNIX 유효 보안 스타일이 있는 혼합 보안 스타일 볼륨 또는 qtree의 UNIX 보안 개체를 Windows 보안 개체로 대체할 수 있습니다.

  원하는 Windows 사용자 및 그룹 개체로 대체하려면 먼저 나열된 모든 UNIX 권한 항목을 제거해야 합니다. 그런 다음 Windows 사용자 및 그룹 개체에서 NTFS 기반 ACL을 구성할 수 있습니다. 모든 UNIX 보안 개체를 제거하고 혼합 보안 스타일 볼륨 또는 qtree의 파일 또는 폴더에 Windows 사용자 및 그룹만 추가하면 파일 또는 폴더의 효과적인 보안 스타일이 UNIX에서 NTFS로 변경됩니다.

  폴더에 대한 권한을 변경할 때 기본 Windows 동작은 이러한 변경 내용을 모든 하위 폴더 및 파일에 전파하는 것입니다. 따라서 보안 스타일의 변경 사항을 모든 하위 폴더, 하위 폴더 및 파일에 전파하지 않으려면 전파 선택 사항을 원하는 설정으로 변경해야 합니다.