파일 권한을 사용하여 파일 액세스를 보호합니다
ONTAP 9

NetApp
February 12, 2026

목차

파일 권한을 사용하여 파일 액세스를 보호합니다

ONTAP SMB SVM에 대한 Windows 보안 탭을 사용하여 고급 NTFS 파일 권한 구성

Windows 속성 창의 * Windows 보안 * 탭을 사용하여 파일 및 폴더에 대한 표준 NTFS 파일 권한을 구성할 수 있습니다.

시작하기 전에

이 작업을 수행하는 관리자는 선택한 개체에 대한 권한을 변경할 수 있는 충분한 NTFS 권한이 있어야 합니다.

이 작업에 대해

NTFS 파일 사용 권한 구성은 NTFS 보안 설명자와 연결된 NTFS DACL(임의 액세스 제어 목록)에 항목을 추가하여 Windows 호스트에서 수행됩니다. 그런 다음 보안 설명자가 NTFS 파일 및 디렉터리에 적용됩니다. 이러한 작업은 Windows GUI에서 자동으로 처리됩니다.

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 사용 권한을 적용할 데이터와 공유 이름을 포함하는 공유가 포함된 CIFS 서버 이름을 입력합니다.

      CIFS 서버 이름이 ""cifs_server""이고 공유 이름이 "share1"인 경우 "\\cifs_server\share1"을 입력해야 합니다.

      CIFS 서버 이름 대신 CIFS 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. NTFS 파일 권한을 설정할 파일 또는 디렉터리를 선택합니다.
4. 파일 또는 디렉터리를 마우스 오른쪽 단추로 클릭한 다음 * 속성 * 을 선택합니다.
5. 보안 * 탭을 선택합니다.

   보안* 탭에는 NTFS 권한이 설정된 사용자 및 그룹 목록이 표시됩니다. [사용 권한] 상자에 선택한 각 사용자 또는 그룹에 대해 적용되는 허용 및 거부 권한 목록이 표시됩니다.

6. 고급 * 을 클릭합니다.

   Windows 속성 창에는 사용자 및 그룹에 할당된 기존 파일 권한에 대한 정보가 표시됩니다.

7. 권한 변경 * 을 클릭합니다.

   사용 권한 창이 열립니다.

8. 원하는 작업을 수행합니다.

원하는 작업	다음을 수행합니다.
새 사용자 또는 그룹에 대한 고급 NTFS 권한을 설정합니다	a. 추가 * 를 클릭합니다. b. 선택할 개체 이름 입력 * 상자에 추가할 사용자 또는 그룹의 이름을 입력합니다. c. 확인 * 을 클릭합니다.
사용자 또는 그룹의 고급 NTFS 권한을 변경합니다	a. 사용 권한 항목: * 상자에서 고급 사용 권한을 변경할 사용자 또는 그룹을 선택합니다. b. 편집 * 을 클릭합니다.
사용자 또는 그룹에 대한 고급 NTFS 권한을 제거합니다	a. 사용 권한 항목: * 상자에서 제거할 사용자 또는 그룹을 선택합니다. b. 제거 * 를 클릭합니다. c. 13단계로 건너뜁니다.

새 사용자 또는 그룹에 고급 NTFS 권한을 추가하거나 기존 사용자 또는 그룹에 대한 NTFS 고급 권한을 변경하는 경우 <Object>의 권한 항목 상자가 열립니다.

9. 적용 대상 * 상자에서 이 NTFS 파일 권한 항목을 적용할 방법을 선택합니다.

   단일 파일에 NTFS 파일 권한을 설정하는 경우 * 적용 대상 * 상자가 활성화되지 않습니다. 적용 대상 * 설정은 기본적으로 * 이 개체만 * 으로 설정됩니다.

10. 사용 권한 * 상자에서 이 개체에 설정할 고급 권한에 대해 * 허용 * 또는 * 거부 * 상자를 선택합니다.

    - 지정된 액세스를 허용하려면 * 허용 * 상자를 선택합니다.
    - 지정된 액세스를 허용하지 않으려면 * Deny * 상자를 선택합니다. 다음과 같은 고급 권한에 대한 권한을 설정할 수 있습니다.
    - * 완전 제어 *

      이 고급 권한을 선택하면 다른 모든 고급 권한이 자동으로 선택됩니다(권한 허용 또는 거부).

    - * 폴더 트래버스/파일 실행 *
    - * 폴더 나열/데이터 읽기 *
    - * 읽기 속성 *
    - * 확장 속성 읽기 *
    - * 파일 생성/데이터 쓰기 *
    - * 폴더 생성/데이터 추가 *
    - * 속성 쓰기 *
    - * 확장 속성 쓰기 *

- * 하위 폴더 및 파일 삭제 *
- * 삭제 *
- * 읽기 권한 *
- * 권한 변경 *
- * 소유권 가져오기 *

> 고급 사용 권한 상자 중 하나를 선택할 수 없는 경우 상위 개체에서 사용 권한이 상속되기 때문입니다.

11. 이 개체의 하위 폴더와 파일이 이러한 권한을 상속하도록 하려면 * 이 컨테이너 내의 개체 및/또는 컨테이너에 이 권한을 적용합니다 * 상자를 선택합니다.
12. 확인 * 을 클릭합니다.
13. NTFS 사용 권한 추가, 제거 또는 편집을 마친 후 이 개체에 대한 상속 설정을 지정합니다.
    - 이 개체의 부모 * 상자에서 상속 가능한 사용 권한 포함 을 선택합니다.

      이것이 기본값입니다.
    - 모든 자식 개체 권한을 이 개체의 상속 가능한 권한으로 바꾸기 * 상자를 선택합니다.

      단일 파일에 NTFS 파일 권한을 설정하는 경우 사용 권한 상자에 이 설정이 없습니다.

      > 이 설정을 선택할 때는 주의하십시오. 이 설정은 모든 자식 개체에 대한 기존 사용 권한을 모두 제거하고 이 개체의 사용 권한 설정으로 바꿉니다. 제거하지 않으려는 사용 권한을 실수로 제거할 수 있습니다. 혼합 보안 형식 볼륨 또는 qtree에서 사용 권한을 설정할 때는 특히 중요합니다. 자식 개체에 UNIX 효과적인 보안 스타일이 있는 경우 이러한 자식 개체에 NTFS 권한을 전파하면 ONTAP에서 이러한 개체를 UNIX 보안 스타일에서 NTFS 보안 스타일로 변경하고 해당 자식 개체에 대한 모든 UNIX 권한이 NTFS 권한으로 대체됩니다.

    - 두 상자를 모두 선택합니다.
    - 어느 상자도 선택하지 않습니다.
14. 확인 * 을 클릭하여 * 권한 * 상자를 닫습니다.
15. [확인]을 클릭하여 <개체>* 상자의 * 고급 보안 설정을 닫습니다.

    고급 NTFS 권한을 설정하는 방법에 대한 자세한 내용은 Windows 설명서를 참조하십시오.

관련 정보

- 서버에 NTFS 보안 설명자 만들기
- NTFS 보안 스타일 볼륨의 파일 보안에 대한 정보를 표시합니다
- 혼합 보안 형식 볼륨의 파일 보안에 대한 정보를 표시합니다
- UNIX 보안 스타일 볼륨의 파일 보안에 대한 정보를 표시합니다

SMB NTFS 파일 권한에 대한 ONTAP 명령

ONTAP CLI를 사용하여 파일 및 디렉토리에 대한 NTFS 파일 권한을 구성할 수 있습니다. 따라서 Windows 클라이언트에서 SMB 공유를 사용하여 데이터에 연결할 필요 없이 NTFS 파일 권한을 구성할 수 있습니다.

NTFS 보안 설명자와 연결된 NTFS DACL(임의 액세스 제어 목록)에 항목을 추가하여 NTFS 파일 권한을 구성할 수 있습니다. 그런 다음 보안 설명자가 NTFS 파일 및 디렉터리에 적용됩니다.

명령줄을 사용해서만 NTFS 파일 권한을 구성할 수 있습니다. CLI를 사용하여 NFSv4 ACL을 구성할 수 없습니다.

단계

1. NTFS 보안 설명자를 만듭니다.

   ```
   vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -owner owner_name -group primary_group_name
   -control-flags-raw raw_control_flags
   ```

2. NTFS 보안 설명자에 DACL을 추가합니다.

   ```
   vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
   -rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
   {this-folder|sub-folders|files}
   ```

3. 파일/디렉토리 보안 정책을 생성합니다.

   ```
   vserver security file-directory policy create -vserver svm_name -policy-name
   policy_name
   ```

ONTAP SMB 서버를 통해 파일에 액세스할 때 액세스 제어를 제공하는 UNIX 파일 권한에 대해 알아보세요.

FlexVol 볼륨은 NTFS, UNIX 또는 MIXED의 세 가지 보안 유형 중 하나를 가질 수 있습니다. 보안 스타일에 관계없이 SMB를 통해 데이터에 액세스할 수 있지만 UNIX의 효율적인 보안을 통해 데이터에 액세스하려면 적절한 UNIX 파일 권한이 필요합니다.

SMB를 통해 데이터에 액세스할 때 사용자가 요청된 작업을 수행할 수 있는 권한이 있는지 여부를 결정할 때 여러 액세스 제어가 사용됩니다.

- 권한 내보내기

  SMB 액세스에 대한 내보내기 권한 구성은 선택 사항입니다.

- 공유 권한
- 파일 권한

  사용자가 작업을 수행하려는 데이터에 다음 유형의 파일 권한이 적용될 수 있습니다.

- NTFS입니다
- Unix NFSv4 ACL
- UNIX 모드 비트

NFSv4 ACL 또는 UNIX 모드 비트 세트가 있는 데이터의 경우 데이터에 대한 파일 액세스 권한을 결정하는 데 UNIX 스타일 권한이 사용됩니다. SVM 관리자는 사용자가 원하는 작업을 수행할 권한을 갖도록 적절한 파일 권한을 설정해야 합니다.

혼합 보안 형식 볼륨의 데이터는 NTFS 또는 UNIX의 효과적인 보안 스타일을 가질 수 있습니다. 데이터에 UNIX 유효 보안 스타일이 있는 경우 데이터에 대한 파일 액세스 권한을 결정할 때 NFSv4 사용 권한 또는 UNIX 모드 비트가 사용됩니다.