



UNIX 보안 스타일 데이터를 위해 **SMB**
클라이언트에 파일 보안을 제공하는 방법을
관리합니다
ONTAP 9

NetApp
April 24, 2024

목차

UNIX 보안 스타일 데이터를 위해 SMB 클라이언트에 파일 보안을 제공하는 방법을 관리합니다.....	1
UNIX 보안 스타일 데이터 개요를 위해 SMB 클라이언트에 파일 보안을 제공하는 방법을 관리합니다.....	1
UNIX 보안 스타일 데이터에 대한 NTFS ACL 표시를 활성화 또는 비활성화합니다	1
ONTAP에서 UNIX 사용 권한을 유지하는 방법	2
Windows 보안 탭을 사용하여 UNIX 사용 권한을 관리합니다.....	2

UNIX 보안 스타일 데이터를 위해 SMB 클라이언트에 파일 보안을 제공하는 방법을 관리합니다

UNIX 보안 스타일 데이터 개요를 위해 SMB 클라이언트에 파일 보안을 제공하는 방법을 관리합니다

SMB 클라이언트에 NTFS ACL 표시를 활성화 또는 비활성화하여 UNIX 보안 스타일 데이터용 파일 보안을 SMB 클라이언트에 제공하는 방법을 선택할 수 있습니다. 각 설정에는 비즈니스 요구 사항에 가장 적합한 설정을 선택해야 한다는 점을 이해해야 합니다.

기본적으로 ONTAP은 UNIX 보안 스타일 볼륨에 대한 UNIX 권한을 SMB 클라이언트에 NTFS ACL로 제공합니다. 다음과 같이 이 방법이 필요한 시나리오가 있습니다.

- Windows 속성 상자의 * 보안 * 탭을 사용하여 UNIX 권한을 보고 편집하려는 경우

UNIX 시스템에서 작업이 허용되지 않는 경우 Windows 클라이언트에서 권한을 수정할 수 없습니다. 예를 들어 UNIX 시스템에서는 이 작업을 허용하지 않으므로 소유하지 않는 파일의 소유권을 변경할 수 없습니다. 이 제한 사항으로 인해 SMB 클라이언트가 파일 및 폴더에 설정된 UNIX 권한을 우회하지 못합니다.

- 사용자는 Microsoft Office와 같은 특정 Windows 응용 프로그램을 사용하여 UNIX 보안 스타일 볼륨에서 파일을 편집 및 저장하고 있습니다. 여기서 ONTAP은 저장 작업 중에 UNIX 권한을 유지해야 합니다.
- 사용자 환경에는 사용 중인 파일에 대해 NTFS ACL을 읽을 것으로 예상되는 특정 Windows 애플리케이션이 있습니다.

경우에 따라 UNIX 사용 권한을 NTFS ACL로 표시하지 않도록 설정할 수 있습니다. 이 기능을 비활성화하면 ONTAP은 UNIX 보안 스타일 볼륨을 SMB 클라이언트에 FAT 볼륨으로 제공합니다. UNIX 보안 스타일 볼륨을 SMB 클라이언트에 FAT 볼륨으로 표시하는 이유는 다음과 같습니다.

- UNIX 클라이언트에서 마운트를 사용하여 UNIX 사용 권한만 변경할 수 있습니다.

UNIX 보안 스타일 볼륨이 SMB 클라이언트에 매핑된 경우에는 보안 탭을 사용할 수 없습니다. 매핑된 드라이브는 파일 권한이 없는 FAT 파일 시스템으로 포맷된 것 같습니다.

- 액세스 파일 및 폴더에 NTFS ACL을 설정하는 SMB를 통해 애플리케이션을 사용 중이며, UNIX 보안 스타일 볼륨에 데이터가 있는 경우 오류가 발생할 수 있습니다.

ONTAP가 볼륨을 FAT로 보고하는 경우 응용 프로그램은 ACL을 변경하지 않습니다.

관련 정보

[FlexVol 볼륨에서 보안 스타일 구성](#)

[Qtree에서 보안 스타일 구성](#)

UNIX 보안 스타일 데이터에 대한 NTFS ACL 표시를 활성화 또는 비활성화합니다

UNIX 보안 스타일 데이터(UNIX 보안 스타일 볼륨 및 UNIX 효과적인 보안이 포함된 혼합 보안

스타일 볼륨)를 위해 SMB 클라이언트에 NTFS ACL 표시를 활성화 또는 비활성화할 수 있습니다.

이 작업에 대해

이 옵션을 설정하면 ONTAP는 효율적인 UNIX 보안 스타일을 사용하는 볼륨의 파일 및 폴더를 NTFS ACL을 갖는 것으로 SMB 클라이언트에 제공합니다. 이 옵션을 비활성화하면 볼륨이 SMB 클라이언트에 FAT 볼륨으로 표시됩니다. 기본값은 NTFS ACL을 SMB 클라이언트에 제공하는 것입니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. UNIX NTFS ACL 옵션 설정을 구성합니다. 'vserver cifs options modify -vserver_vserver_name_-is-unix-NT -acl-enabled{true|false}'
3. 옵션이 원하는 값('vserver cifs options show -vserver_vserver_name_')으로 설정되어 있는지 확인합니다
4. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

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.

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.