옵션을 사용하여 **SMB** 서버를 사용자 지정합니다

ONTAP 9

NetApp
April 24, 2024

목차

옵션을 사용하여 **SMB** 서버를 사용자 지정합니다

사용 가능한 **SMB** 서버 옵션

SMB 서버를 사용자 지정하는 방법을 고려할 때 사용할 수 있는 옵션을 파악하는 것이 유용합니다. 일부 옵션은 SMB 서버에서 일반적으로 사용되지만 일부 옵션은 특정 SMB 기능을 설정하고 구성하는 데 사용됩니다. SMB 서버 옵션은 'vserver cifs options modify' 옵션으로 제어됩니다.

다음 목록은 관리자 권한 수준에서 사용할 수 있는 SMB 서버 옵션을 지정합니다.

- * SMB 세션 시간 초과 값 구성 *

  이 옵션을 구성하면 SMB 세션의 연결이 끊기까지의 유휴 시간(초)을 지정할 수 있습니다. 유휴 세션은 사용자가 클라이언트에 열려 있는 파일이나 디렉토리가 없는 세션입니다. 기본값은 900초입니다.

- * 기본 UNIX 사용자 구성 *

  이 옵션을 구성하면 SMB 서버에서 사용하는 기본 UNIX 사용자를 지정할 수 있습니다. ONTAP는 ""pcuser""(UID 65534)라는 기본 사용자를 자동으로 만들고 ""pcuser""(GID가 65534)라는 그룹을 만든 다음 기본 사용자를 ""pcuser"" 그룹에 추가합니다. SMB 서버를 생성하면 ONTAP는 자동으로 ""pcuser""를 기본 UNIX 사용자로 구성합니다.

- * 게스트 UNIX 사용자 구성 *

  이 옵션을 구성하면 신뢰할 수 없는 도메인에서 로그인하는 사용자가 매핑될 UNIX 사용자의 이름을 지정할 수 있으므로 신뢰할 수 없는 도메인의 사용자가 SMB 서버에 연결할 수 있습니다. 기본적으로 이 옵션은 구성되지 않음(기본값 없음)이므로 신뢰할 수 없는 도메인의 사용자가 SMB 서버에 연결하도록 허용하지 않습니다.

- * 모드 비트에 대한 읽기 권한 실행 활성화 또는 비활성화 *

  이 옵션을 설정하거나 해제하면 UNIX 실행 가능 비트가 설정되지 않은 경우에도 SMB 클라이언트가 읽기 액세스 권한이 있는 UNIX 모드 비트를 사용하여 실행 파일을 실행하도록 허용할지 여부를 지정할 수 있습니다. 이 옵션은 기본적으로 비활성화되어 있습니다.

- * NFS 클라이언트에서 읽기 전용 파일을 삭제하는 기능을 활성화 또는 비활성화합니다

  이 옵션을 설정하거나 해제하면 NFS 클라이언트가 읽기 전용 속성이 설정된 파일 또는 폴더를 삭제할 수 있는지 여부를 결정합니다. NTFS 삭제 의미 체계에서는 읽기 전용 특성이 설정된 경우 파일 또는 폴더를 삭제할 수 없습니다. UNIX 삭제 의미 체계는 읽기 전용 비트를 무시하고 상위 디렉토리 권한을 사용하여 파일 또는 폴더를 삭제할 수 있는지 여부를 결정합니다. 기본 설정은 사용 안 함 으로 NTFS 삭제 의미를 가져옵니다.

- * Windows 인터넷 이름 서비스 서버 주소 구성 *

  이 옵션을 구성하면 WINS(Windows Internet Name Service) 서버 주소 목록을 쉼표로 구분된 목록으로 지정할 수 있습니다. IPv4 주소를 지정해야 합니다. IPv6 주소는 지원되지 않습니다. 기본값이 없습니다.

다음 목록은 고급 권한 수준에서 사용할 수 있는 SMB 서버 옵션을 지정합니다.

- * CIFS 사용자에게 UNIX 그룹 권한 부여 *

이 옵션을 구성하면 파일 소유자가 아닌 수신 CIFS 사용자에게 그룹 권한을 부여할 수 있는지 여부를 결정합니다. CIFS 사용자가 UNIX 보안 스타일 파일의 소유자가 아니고 이 매개 변수를 "true"로 설정하면 해당 파일에 대한 그룹 권한이 부여됩니다. CIFS 사용자가 UNIX 보안 스타일 파일의 소유자가 아니고 이 매개 변수가 "false"로 설정된 경우 일반 UNIX 규칙을 적용하여 파일 권한을 부여할 수 있습니다. 이 매개 변수는 권한이 '모드 비트'로 설정되어 있고 NTFS 또는 NFSv4 보안 모드가 있는 파일에는 적용되지 않는 UNIX 보안 스타일 파일에 적용됩니다. 기본 설정은 false입니다.

- * SMB 1.0 * 활성화 또는 비활성화

  SMB 1.0은 ONTAP 9.3에서 SMB 서버가 생성된 SVM에서 기본적으로 비활성화되어 있습니다.

  > ONTAP 9.3부터는 ONTAP 9.3에서 생성된 새 SMB 서버에 대해 SMB 1.0이 기본적으로 사용되지 않습니다. 보안 및 규정 준수 향상을 준비하기 위해 가능한 한 빨리 최신 SMB 버전으로 마이그레이션해야 합니다. 자세한 내용은 NetApp 담당자에게 문의하십시오.

- * SMB 2.x * 활성화 또는 비활성화

  SMB 2.0은 LIF 페일오버를 지원하는 최소 SMB 버전입니다. SMB 2.x를 비활성화하면 ONTAP도 자동으로 SMB 3.X를 비활성화합니다

  SMB 2.0은 SVM에서만 지원됩니다. 이 옵션은 SVM에서 기본적으로 활성화됩니다

- * SMB 3.0 * 활성화 또는 비활성화

  SMB 3.0은 지속적으로 사용 가능한 공유를 지원하는 최소 SMB 버전입니다. Windows Server 2012 및 Windows 8은 SMB 3.0을 지원하는 최소 Windows 버전입니다.

  SMB 3.0은 SVM에서만 지원됩니다. 이 옵션은 SVM에서 기본적으로 활성화됩니다

- * SMB 3.1 * 활성화 또는 비활성화

  Windows 10은 SMB 3.1을 지원하는 유일한 Windows 버전입니다.

  SMB 3.1은 SVM에서만 지원됩니다. 이 옵션은 SVM에서 기본적으로 활성화됩니다

- * ODX 복사 오프로드 설정 또는 해제 *

  ODX 복사 오프로드는 Windows 클라이언트에서 지원하는 데 자동으로 사용됩니다. 이 옵션은 기본적으로 활성화되어 있습니다.

- * ODX 복사 오프로드에 대한 직접 복사 메커니즘 설정 또는 해제 *

  직접 복사 메커니즘은 Windows 클라이언트가 복사 진행 중에 파일이 변경되지 않도록 하는 모드에서 복사본의 소스 파일을 열려고 할 때 복제 오프로드 작업의 성능을 향상시킵니다. 기본적으로 직접 복사 메커니즘은 활성화되어 있습니다.

- * 자동 노드 참조 활성화 또는 비활성화 *

  SMB 서버는 자동 노드 조회를 통해 요청된 공유를 통해 액세스한 데이터를 호스팅하는 노드에 대한 데이터 LIF 로컬 클라이언트를 자동으로 참조합니다.

- * SMB*에 대한 내보내기 정책 활성화 또는 비활성화

이 옵션은 기본적으로 비활성화되어 있습니다.

- * 교차점을 재분석 지점으로 사용하여 활성화 또는 비활성화 *

  이 옵션을 활성화하면 SMB 서버는 재분석 지점으로 SMB 클라이언트에 연결 지점을 노출합니다. 이 옵션은 SMB 2.x 또는 SMB 3.0 연결에만 유효합니다. 이 옵션은 기본적으로 활성화되어 있습니다.

  이 옵션은 SVM에서만 지원됩니다. 이 옵션은 SVM에서 기본적으로 활성화됩니다

- * TCP 연결당 최대 동시 작업 수 구성 *

  기본값은 255입니다.

- * 로컬 Windows 사용자 및 그룹 기능 활성화 또는 비활성화 *

  이 옵션은 기본적으로 활성화되어 있습니다.

- * 로컬 Windows 사용자 인증 활성화 또는 비활성화 *

  이 옵션은 기본적으로 활성화되어 있습니다.

- * VSS 섀도우 복제본 기능 활성화 또는 비활성화 *

  ONTAP는 섀도우 복제본 기능을 사용하여 SMB를 통한 Hyper-V 솔루션을 사용하여 저장된 데이터의 원격 백업을 수행합니다.

  이 옵션은 SVM에서만 지원되며, SMB를 통한 Hyper-V 구성에서만 지원됩니다. 이 옵션은 SVM에서 기본적으로 활성화됩니다

- * 섀도 복사본 디렉토리 수준 구성 *

  이 옵션을 구성하면 섀도우 복제본 기능을 사용할 때 섀도우 복제본을 생성할 디렉토리의 최대 깊이를 정의할 수 있습니다.

  이 옵션은 SVM에서만 지원되며, SMB를 통한 Hyper-V 구성에서만 지원됩니다. 이 옵션은 SVM에서 기본적으로 활성화됩니다

- * 이름 매핑에 대한 다중 도메인 검색 기능을 활성화 또는 비활성화합니다 *

  활성화된 경우, UNIX 사용자가 Windows 사용자 이름의 도메인 부분에서 와일드카드(*)를 사용하여 Windows 도메인 사용자에게 매핑되면(예: *\Joe) ONTAP는 양방향 트러스트가 있는 모든 도메인에서 홈 도메인으로 지정된 사용자를 검색합니다. 홈 도메인은 SMB 서버의 컴퓨터 계정이 포함된 도메인입니다.

  양방향으로 신뢰할 수 있는 모든 도메인을 검색하는 대신 선호하는 신뢰할 수 있는 도메인 목록을 구성할 수 있습니다. 이 옵션을 사용하도록 설정하고 기본 설정 목록을 구성하면 다중 도메인 이름 매핑 검색을 수행하는 데 기본 설정 목록이 사용됩니다.

  기본값은 다중 도메인 이름 매핑 검색을 사용하는 것입니다.

- * 파일 시스템 섹터 크기 구성 *

  이 옵션을 구성하면 ONTAP에서 SMB 클라이언트에 보고하는 파일 시스템 섹터 크기를 바이트 단위로 구성할 수 있습니다. 이 옵션에는 4096과 512의 두 가지 유효한 값이 있습니다. 기본값은 4096입니다. Windows 응용 프로그램이 512바이트의 섹터 크기만 지원하는 경우 이 값을 '512'로 설정해야 할 수 있습니다.

- * 동적 액세스 제어 활성화 또는 비활성화 *

  이 옵션을 활성화하면 DAC(Dynamic Access Control)를 사용하여 중앙 액세스 정책을 스테이징하고 그룹 정책 개체를 사용하여 중앙 액세스 정책을 구현하는 등 SMB 서버의 개체를 보호할 수 있습니다. 이 옵션은 기본적으로 비활성화되어 있습니다.

  이 옵션은 SVM에서만 지원됩니다.

- * 인증되지 않은 세션에 대한 액세스 제한 설정(익명 제한) *

  이 옵션을 설정하면 인증되지 않은 세션에 대한 액세스 제한이 결정됩니다. 제한 사항은 익명 사용자에게 적용됩니다. 기본적으로 익명 사용자에 대한 액세스 제한은 없습니다.

- * UNIX 효과적인 보안(UNIX 보안 스타일 볼륨 또는 UNIX 효과적인 보안이 포함된 혼합 보안 스타일 볼륨)이 있는 볼륨에서 NTFS ACL 표시를 활성화 또는 비활성화합니다. *

  이 옵션을 설정하거나 해제하면 UNIX 보안이 있는 파일 및 폴더의 파일 보안이 SMB 클라이언트에 제공되는 방식이 결정됩니다. 이 옵션을 설정하면 ONTAP는 UNIX 보안 기능이 있는 볼륨의 파일 및 폴더를 NTFS ACL을 사용한 NTFS 파일 보안으로 SMB 클라이언트에 제공합니다. 사용하지 않도록 설정하면 ONTAP는 UNIX 보안이 설정된 볼륨을 파일 보안 없이 FAT 볼륨으로 제공합니다. 기본적으로 볼륨은 NTFS ACL을 사용한 NTFS 파일 보안을 갖는 것으로 표시됩니다.

- * SMB 가짜 열기 기능 활성화 또는 비활성화 *

  이 기능을 사용하면 파일 및 디렉토리에 대한 속성 정보를 쿼리할 때 ONTAP에서 열기 및 닫기 요청을 수행하는 방식을 최적화하여 SMB 2.x 및 SMB 3.0 성능을 향상시킬 수 있습니다. 기본적으로 SMB 가짜 열기 기능이 활성화됩니다. 이 옵션은 SMB 2.x 이상에서 만들어진 연결에만 유용합니다.

- * UNIX 확장 활성화 또는 비활성화 *

  이 옵션을 활성화하면 SMB 서버에서 UNIX 확장이 활성화됩니다. UNIX 확장을 사용하면 POSIX/UNIX 스타일 보안을 SMB 프로토콜을 통해 표시할 수 있습니다. 기본적으로 이 옵션은 비활성화되어 있습니다.

  Mac OSX 클라이언트와 같은 UNIX 기반 SMB 클라이언트가 있는 경우 UNIX 확장을 활성화해야 합니다. UNIX 확장을 사용하면 SMB 서버가 POSIX/UNIX 보안 정보를 SMB를 통해 UNIX 기반 클라이언트로 전송한 다음 보안 정보를 POSIX/UNIX 보안으로 변환합니다.

- * 간단한 이름 검색 지원 활성화 또는 비활성화 *

  이 옵션을 활성화하면 SMB 서버가 짧은 이름으로 검색을 수행할 수 있습니다. 이 옵션을 사용하는 검색 쿼리는 8.3 파일 이름과 긴 파일 이름을 일치시키려고 합니다. 이 파라미터의 기본값은 'false'입니다.

- * DFS 기능 자동 보급에 대한 지원 활성화 또는 비활성화 *

  이 옵션을 활성화 또는 비활성화하면 SMB 서버가 공유에 연결하는 SMB 2.x 및 SMB 3.0 클라이언트에 DFS 기능을 자동으로 보급할지 여부를 결정합니다. ONTAP는 SMB 액세스를 위한 심볼 링크 구현에 DFS 조회를 사용합니다. 활성화된 경우 SMB 서버는 심볼 링크 액세스가 설정되었는지 여부에 관계없이 항상 DFS 기능을 알립니다. 비활성화된 경우 SMB 서버는 클라이언트가 심볼 링크 액세스가 설정된 공유에 연결할 때만 DFS 기능을 알립니다.

- * 최대 SMB 크레딧 수 구성 *

  ONTAP 9.4부터, '-max-credits' 옵션을 구성하면 클라이언트와 서버가 SMB 버전 2 이상을 실행하는 경우 SMB

연결에 부여할 크레딧 수를 제한할 수 있습니다. 기본값은 128입니다.

- * SMB 멀티 채널 * 에 대한 지원 활성화 또는 비활성화

  ONTAP 9.4 이상 릴리스에서 '-is-multichannel-enabled' 옵션을 활성화하면 SMB 서버는 클러스터와 해당 클라이언트에 적절한 NIC가 구축될 때 단일 SMB 세션에 대해 여러 개의 연결을 설정할 수 있습니다. 이렇게 하면 처리량과 내결함성이 개선됩니다. 이 파라미터의 기본값은 'false'입니다.

  SMB 멀티 채널이 활성화되면 다음 매개 변수도 지정할 수 있습니다.

  - 다중 채널 세션당 허용되는 최대 연결 수입니다. 이 매개 변수의 기본값은 32입니다.
  - Multichannel 세션당 공고되는 최대 네트워크 인터페이스 수입니다. 이 매개 변수의 기본값은 256입니다.

SMB 서버 옵션 구성

SVM(스토리지 가상 시스템)에서 SMB 서버를 생성한 후에는 언제든지 SMB 서버 옵션을 구성할 수 있습니다.

단계

1. 원하는 작업을 수행합니다.

SMB 서버 옵션을 구성하려면...	명령 입력...
관리 권한 수준에서 설정합니다	'vserver cifs options modify -vserver_vserver_name options_'
고급 권한 수준에서 설정합니다	a. 세트 프리빌리지 고급 b. 'vserver cifs options modify -vserver_vserver_name options_' c. 'Set-Privilege admin'입니다

SMB 서버 옵션 구성에 대한 자세한 내용은 'vserver cifs options modify' 명령의 man 페이지를 참조하십시오.

SMB 사용자에게 UNIX 그룹 권한 부여 를 구성합니다

들어오는 SMB 사용자가 파일 소유자가 아닌 경우에도 파일 또는 디렉토리에 액세스할 수 있는 그룹 권한을 부여하도록 이 옵션을 구성할 수 있습니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. UNIX 그룹 권한 부여를 적절히 구성합니다.

원하는 경우	명령을 입력합니다
사용자가 파일 소유자가 아니더라도 파일 또는 디렉토리에 대한 액세스를 활성화하여 그룹 권한을 얻습니다	'vserver cifs options modify –grant-unix-group-perms-to-others true'
파일 또는 디렉토리에 대한 액세스를 비활성화하여 사용자가 파일 소유자가 아니더라도 그룹 권한을 얻습니다	'vserver cifs options modify –grant-unix-group-perms-to-others false'

3. 이 옵션이 원하는 값으로 설정되어 있는지 확인합니다. 'vserver cifs options show –fields grant-unix-group-perms-to-others'
4. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

익명 사용자의 액세스 제한을 구성합니다

기본적으로 인증되지 않은 익명 사용자(*null user* 라고도 함)는 네트워크의 특정 정보에 액세스할 수 있습니다. SMB 서버 옵션을 사용하여 익명 사용자의 액세스 제한을 구성할 수 있습니다.

이 작업에 대해

익명 제한 SMB 서버 옵션은 Windows의 RestrictAnonymous 레지스트리 항목에 해당합니다.

익명 사용자는 사용자 이름 및 세부 정보, 계정 정책 및 공유 이름을 포함하여 네트워크의 Windows 호스트에서 특정 유형의 시스템 정보를 나열하거나 열거할 수 있습니다. 다음 세 가지 액세스 제한 설정 중 하나를 지정하여 익명 사용자에 대한 액세스를 제어할 수 있습니다.

값	설명
무제한(기본값)	익명 사용자에 대한 액세스 제한을 지정하지 않습니다.
번호 매기기	익명 사용자에 대해서만 열거를 제한하도록 지정합니다.
"접근 불가"	익명 사용자에 대한 액세스가 제한되도록 지정합니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 익명 제한 설정: 'vserver cifs options modify -vserver_vserver_name_-restrict-anonymous{no-restriction|no-enumeration|no-access}'를 구성합니다
3. 옵션이 원하는 값('vserver cifs options show -vserver_vserver_name_')으로 설정되어 있는지 확인합니다
4. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

관련 정보

사용 가능한 SMB 서버 옵션

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 ONTAP는 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 ONTAP는 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 ONTAP는 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.