NAS 프로토콜

NetApp Solutions

NetApp
April 18, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/netapp-solutions/ehc/ncvs-gc-nas-protocols_overview.html on April 18, 2024. Always check docs.netapp.com for the latest.

목차

NAS 프로토콜 1
NAS 프로토콜 개요 1
NAS 프로토콜의 기본 사항 1
NFS 를 참조하십시오 1
중소기업 12
이중 프로토콜/멀티프로토콜 27
Active Directory 연결을 생성할 때의 고려 사항 28
기타 NAS 인프라스트럭처 서비스 종속성(KDC, LDAP 및 DNS) 32

NAS 프로토콜

NAS 프로토콜 개요

NAS 프로토콜에는 NFS(v3 및 v4.1) 및 SMB/CIFS(2.x 및 3.x)가 포함됩니다. 이러한 프로토콜은 CVS에서 여러 NAS 클라이언트 간에 데이터에 대한 공유 액세스를 허용하는 방법입니다. 또한 Cloud Volumes Service는 NFS 및 SMB/CIFS 클라이언트(이중 프로토콜)에 대한 액세스를 동시에 제공하는 동시에 NAS 공유의 파일 및 폴더에 대한 모든 ID 및 권한 설정을 존중할 수 있습니다. Cloud Volumes Service는 가장 높은 데이터 전송 보안을 유지하기 위해 SMB 암호화 및 NFS Kerberos 5p를 사용하여 전송 중인 프로토콜 암호화를 지원합니다.

> 이중 프로토콜은 CVS에서 사용할 수 있습니다. - 성능만 지원됩니다.

NAS 프로토콜의 기본 사항

NAS 프로토콜은 여러 클라이언트의 네트워크 상에서 Cloud Volumes Service on GCP와 같은 스토리지 시스템의 동일한 데이터에 액세스하는 방법입니다. NFS 및 SMB는 정의된 NAS 프로토콜로, Cloud Volumes Service이 서버 역할을 하는 클라이언트/서버 단위로 작동합니다. 클라이언트는 서버에 액세스, 읽기 및 쓰기 요청을 보내고, 서버는 파일에 대한 잠금 메커니즘을 조정하고, 사용 권한을 저장하고, ID 및 인증 요청을 처리할 책임이 있습니다.

예를 들어, NAS 클라이언트가 폴더에 새 파일을 생성하려는 경우 다음과 같은 일반 프로세스가 적용됩니다.

1. 클라이언트가 서버에 디렉터리(권한, 소유자, 그룹, 파일 ID, 사용 가능한 공간, 등). 서버는 요청한 클라이언트 및 사용자에게 상위 폴더에 대한 필요한 권한이 있는 경우 해당 정보로 응답합니다.
2. 디렉토리의 사용 권한이 액세스를 허용할 경우 클라이언트는 생성 중인 파일 이름이 파일 시스템에 이미 있는지 서버에 묻습니다. 파일 이름이 이미 사용 중인 경우 생성이 실패합니다. 파일 이름이 없는 경우 서버는 클라이언트가 계속 진행할 수 있음을 알려 줍니다.
3. 클라이언트는 디렉토리 핸들 및 파일 이름으로 파일을 만들기 위해 서버에 대한 호출을 수행하고 액세스 및 수정 시간을 설정합니다. 서버에서 파일에 고유한 파일 ID를 발급하여 동일한 파일 ID로 다른 파일이 생성되지 않도록 합니다.
4. 클라이언트는 쓰기 작업 전에 파일 특성을 확인하는 호출을 전송합니다. 권한이 허용하는 경우 클라이언트는 새 파일을 씁니다. 프로토콜/응용 프로그램에서 잠금을 사용하는 경우 클라이언트는 다른 클라이언트가 잠금 상태에서 파일에 액세스하지 못하도록 서버에 잠금을 요청합니다. 잠금 상태에서는 데이터 손상을 방지할 수 있습니다.

NFS 를 참조하십시오

NFS는 RFC(Request for Comments)에 정의된 공개 IETF 표준인 분산 파일 시스템 프로토콜로, 누구나 프로토콜을 구현할 수 있도록 합니다.

Cloud Volumes Service의 볼륨은 클라이언트 또는 클라이언트 세트에 액세스할 수 있는 경로를 내보내 NFS 클라이언트에 공유됩니다. 이러한 내보내기를 마운트할 수 있는 권한은 Cloud Volumes Service 관리자가 구성할 수 있는 내보내기 정책 및 규칙에 의해 정의됩니다.

NetApp NFS 구현은 프로토콜의 골드 표준으로 간주되며 수많은 엔터프라이즈 NAS 환경에서 사용됩니다. 다음

섹션에서는 NFS와 Cloud Volumes Service에서 사용할 수 있는 특정 보안 기능 및 구현 방법에 대해 설명합니다.

기본 로컬 **UNIX** 사용자 및 그룹

Cloud Volumes Service에는 다양한 기본 기능을 위한 여러 기본 UNIX 사용자 및 그룹이 포함되어 있습니다. 이러한 사용자 및 그룹은 현재 수정 또는 삭제할 수 없습니다. 현재 새 로컬 사용자 및 그룹을 Cloud Volumes Service에 추가할 수 없습니다. 기본 사용자 및 그룹 외부의 UNIX 사용자 및 그룹은 외부 LDAP 이름 서비스에서 제공해야 합니다.

다음 표에서는 기본 사용자 및 그룹과 해당 숫자 ID를 보여 줍니다. LDAP 또는 이러한 숫자 ID를 다시 사용하는 로컬 클라이언트에서는 새 사용자 또는 그룹을 생성하지 않는 것이 좋습니다.

기본 사용자: 숫자 **ID**	기본 그룹: 숫자 **ID**
• 루트: 0 • pcuser: 65534 • 아무도 없다: 65535	• 루트: 0 • 데몬: 1 • pcuser: 65534 • 아무도 없다: 65535

NFSv4.1을 사용하는 경우 NFS 클라이언트에서 디렉토리 목록 명령을 실행할 때 루트 사용자가 아무도 표시되지 않을 수 있습니다. 이는 클라이언트의 ID 도메인 매핑 구성 때문입니다. 의 섹션을 참조하십시오 NFSv4.1 및 그 누구도 사용자/그룹을 대상으로 하지 않습니다 이 문제에 대한 자세한 내용 및 해결 방법을 확인하십시오.

루트 사용자입니다

Linux에서 루트 계정은 Linux 기반 파일 시스템의 모든 명령, 파일 및 폴더에 액세스할 수 있습니다. 이 계정의 강력한 기능 때문에 보안 모범 사례에 따라 루트 사용자를 비활성화하거나 제한해야 하는 경우가 많습니다. NFS 내보내기에서 루트 사용자가 파일과 폴더에 가지고 있는 파워는 내보내기 정책과 규칙, 루트 스쿼시(root squash)라는 개념을 통해 Cloud Volumes Service에서 제어할 수 있습니다.

루트 스쿼싱 기능을 사용하면 NFS 마운트에 액세스하는 루트 사용자가 익명 숫자 사용자 65534에 스쿼트됩니다(“ 섹션 참조)익명 사용자") 및 은(는) 현재 CVS - Performance를 사용하는 경우에만 사용할 수 있습니다. 이 경우 내보내기 정책 규칙 생성 중 루트 액세스에 대해 Off를 선택합니다. 루트 사용자가 익명 사용자에게 스쿼트되면 chown 또는 을 실행할 수 있는 액세스 권한이 더 이상 없습니다 "setuid/setgid 명령(고정 비트)" NFS 마운트의 파일 또는 폴더와 루트 사용자가 생성한 파일 또는 폴더에 anon UID가 소유자/그룹으로 표시됩니다. 또한 루트 사용자가 NFSv4 ACL을 수정할 수 없습니다. 그러나 루트 사용자는 chmod 및 삭제된 파일에 대한 명시적 권한이 없는 액세스 권한을 계속 가집니다. 루트 사용자의 파일 및 폴더 권한에 대한 액세스를 제한하려면 NTFS ACL을 사용하여 볼륨을 사용하고, "root"라는 Windows 사용자를 생성하고, 파일 또는 폴더에 원하는 권한을 적용하는 것이 좋습니다.

익명 사용자

익명(anon) 사용자 ID는 유효한 NFS 자격 증명 없이 도착하는 클라이언트 요청에 매핑된 UNIX 사용자 ID 또는 사용자 이름을 지정합니다. 여기에는 루트 스쿼싱 사용 시 루트 사용자가 포함될 수 있습니다. Cloud Volumes Service의 anon 사용자는 65534입니다.

이 UID는 일반적으로 Linux 환경의 사용자 이름 'nobody' 또는 'nfsnobody'와 관련이 있습니다. Cloud Volumes Service는 로컬 UNIX 사용자 ' pcuser ' 로 65534도 사용합니다(“ 절 참조)기본 로컬 UNIX 사용자 및 그룹"). LDAP에서 일치하는 유효한 UNIX 사용자를 찾을 수 없는 경우 Windows에서 UNIX로의 이름 매핑의 기본 대체 사용자입니다.

Linux의 사용자 이름과 UID 65534의 Cloud Volumes Service 간 사용자 이름 차이로 인해 65534에 매핑된 사용자의 이름 문자열이 NFSv4.1을 사용할 때 일치하지 않을 수 있습니다. 따라서 일부 파일 및 폴더에 대해 사용자로 'nobody'가 표시될 수 있습니다. 자세한 내용은 " 단원을 참조하십시오NFSv4.1 및 그 누구도 사용자/그룹을 대상으로 하지 않습니다"를 참조하십시오.

액세스 제어/내보내기

NFS 마운트에 대한 초기 엑스포트/공유 액세스는 엑스포트 정책 내에 포함된 호스트 기반 엑스포트 정책 규칙을 통해 제어됩니다. 호스트 IP, 호스트 이름, 서브넷, 넷그룹 또는 도메인이 정의되어 NFS 공유를 마운트하는 액세스 권한과 호스트에 허용되는 액세스 수준을 허용합니다. 엑스포트 정책 규칙 구성 옵션은 Cloud Volumes Service 레벨에 따라 다릅니다.

CVS-SW의 경우 내보내기 정책 구성에 다음 옵션을 사용할 수 있습니다.

- * 클라이언트 일치. * 쉼표로 구분된 IP 주소 목록, 쉼표로 구분된 호스트 이름, 서브넷, 넷그룹, 도메인 이름 목록.
- * RO/RW 액세스 규칙 * 내보내기에 대한 액세스 수준을 제어하려면 읽기/쓰기 또는 읽기 전용 을 선택합니다. CVS - 성능은 다음 옵션을 제공합니다.
- * 클라이언트 일치. * 쉼표로 구분된 IP 주소 목록, 쉼표로 구분된 호스트 이름, 서브넷, 넷그룹, 도메인 이름 목록.
- * RO/RW 액세스 규칙. * 읽기/쓰기 또는 읽기 전용 을 선택하여 내보내기에 대한 액세스 수준을 제어합니다.
- * 루트 액세스(켜기/끄기). * 루트 스쿼시를 구성합니다(“ 절 참조)루트 사용자입니다"를 참조하십시오.)
- * Protocol type. * 이 옵션은 NFS 마운트에 대한 액세스를 특정 프로토콜 버전으로 제한합니다. 볼륨에 대해 NFSv3과 NFSv4.1을 모두 지정할 때 두 확인란을 모두 비워 두거나 두 확인란을 모두 선택합니다.
- * Kerberos 보안 수준(Kerberos 활성화 가 선택된 경우). * 읽기 전용 또는 읽기-쓰기 액세스에 대해 krb5, krb5i 및 /또는 krb5p의 옵션을 제공합니다.

변경 소유권(chown) 및 변경 그룹(chgrp)

Cloud Volumes Service의 NFS에서는 루트 사용자만 파일 및 폴더에 대해 chown/chgrp를 실행할 수 있습니다. 다른 사용자는 자신이 소유한 파일에서도 'Operation not mitted(작업이 허용되지 않음)' 오류를 볼 수 있습니다. 루트 스쿼시를 사용하는 경우(“ 섹션에서 다룹니다루트 사용자입니다”), 루트가 비루트 사용자에게 스쿼트되고 chown 및 chgrp에 대한 액세스가 허용되지 않습니다. 현재 Cloud Volumes Service에는 루트 이외의 사용자에 대한 chown 및 chgrp를 허용하는 대안이 없습니다. 소유권을 변경해야 하는 경우 이중 프로토콜 볼륨을 사용하고 보안 스타일을 NTFS로 설정하여 Windows 측의 권한을 제어할 수 있습니다.

권한 관리

Cloud Volumes Service는 모드 비트(예: rwx의 경우 644, 777 등)와 NFSv4.1 ACL을 모두 지원하여 UNIX 보안 스타일을 사용하는 볼륨의 NFS 클라이언트에 대한 사용 권한을 제어합니다. 이러한 사용자(chmod, chown 또는 nfs4_setfacl 등)에 대해 표준 권한 관리가 사용되며 이를 지원하는 모든 Linux 클라이언트와 함께 작동합니다.

또한 NTFS로 설정된 이중 프로토콜 볼륨을 사용하는 경우 NFS 클라이언트는 Windows 사용자에 대한 Cloud Volumes Service 이름 매핑을 활용할 수 있으며, 이 이름 매핑은 NTFS 권한을 확인하는 데 사용됩니다. Cloud Volumes Service를 Windows 사용자 이름에 올바르게 매핑하려면 유효한 UNIX 사용자 이름이 필요하기 때문에 이를 위해서는 Cloud Volumes Service에 대한 LDAP 연결이 필요합니다.

NFSv3에 대한 세부적인 **ACL** 제공

모드 비트 사용 권한은 소유자, 그룹 및 다른 모든 관련자만 사용할 수 있습니다. 즉, 기본 NFSv3에 대해 세부적인 사용자 액세스 제어를 사용할 수 없습니다. Cloud Volumes Service는 POSIX ACL 또는 확장된 특성(예: chattr)을

지원하지 않으므로 NFSv3을 사용하는 다음 시나리오에서만 세분화된 ACL을 사용할 수 있습니다.

- 유효한 UNIX와 Windows 사용자 간 매핑을 사용하는 NTFS 보안 스타일 볼륨(CIFS 서버 필요)
- NFSv4.1 ACL은 관리 클라이언트 마운트 NFSv4.1을 사용하여 ACL을 적용하여 적용됩니다.

두 방법 모두 UNIX ID 관리를 위한 LDAP 연결과 유효한 UNIX 사용자 및 그룹 정보를 채워야 합니다(섹션 참조) ""LDAP"") 및 은 CVS - 성능 인스턴스에서만 사용할 수 있습니다. NFS에서 NTFS 보안 스타일 볼륨을 사용하려면 SMB 연결이 구성되어 있지 않더라도 이중 프로토콜(SMB 및 NFSv3) 또는 이중 프로토콜(SMB 및 NFSv4.1)을 사용해야 합니다. NFSv3 마운트에서 NFSv4.1 ACL을 사용하려면 프로토콜 유형으로 'both(NFSv3/NFSv4.1)'를 선택해야 합니다.

일반 UNIX 모드 비트는 NTFS 또는 NFSv4.x ACL이 제공하는 사용 권한과 동일한 수준의 세분성을 제공하지 않습니다. 다음 표에서는 NFSv3 모드 비트와 NFSv4.1 ACL 간의 사용 권한 세분화를 비교합니다. NFSv4.1 ACL에 대한 자세한 내용은 을 참조하십시오 "NFS4_ACL-NFSv4 액세스 제어 목록".

NFSv3 모드 비트	**NFSv4.1 ACL**
• 실행 시 사용자 ID를 설정합니다 • 실행 시 그룹 ID를 설정합니다 • 바꾼 텍스트 저장(POSIX에 정의되지 않음) • 소유자에 대한 읽기 권한 • 소유자의 쓰기 권한 • 파일의 소유자에 대한 권한을 실행하거나 디렉터리에서 소유자를 찾기(검색) 권한을 실행합니다 • 그룹에 대한 읽기 권한 • 그룹에 대한 쓰기 권한 • 파일의 그룹에 대한 권한을 실행하거나 디렉터리의 그룹에 대한 검색 권한을 찾습니다 • 다른 사람의 읽기 권한 • 다른 사람에 대한 권한을 작성합니다 • 파일의 다른 사람에 대한 권한을 실행하거나 디렉터리에서 다른 사람에 대한 검색 권한을 찾습니다	ACE(액세스 제어 항목) 형식(허용/거부/감사) * 상속 플래그 * directory-inherit * file-inherit * no-propagate-inherit * inherit-only 권한 * 읽기-데이터(파일)/목록-디렉토리(디렉토리) * 쓰기-데이터(파일)/생성-파일(디렉토리) * 추가-데이터(파일)/생성-하위 디렉토리(디렉토리) * 실행(파일)/변경-디렉토리(디렉토리) * 삭제 * delete-child * read-attributes * write-named-attributes * write-named-acner-write-write-acl-write-write-write-write-acl-write-write-write-write-acl-write-write-write-write-

마지막으로, RPC 패킷 제한에 따라 NFS 그룹 멤버 자격(NFSv3 및 NFSv4.x에서 모두)은 AUTH_SYS에 대한 기본값 최대 16으로 제한됩니다. NFS Kerberos는 최대 32개의 그룹과 NFSv4 ACL을 제공하므로 사용자 및 그룹 ACL(ACE당 최대 1024개 항목)을 세부적으로 적용하여 제한을 제거할 수 있습니다.

또한 Cloud Volumes Service는 지원되는 최대 그룹을 32개까지 확장할 수 있도록 확장된 그룹 지원을 제공합니다. 이를 위해서는 유효한 UNIX 사용자 및 그룹 ID가 포함된 LDAP 서버에 대한 LDAP 연결이 필요합니다. 이 구성을 구성하는 방법에 대한 자세한 내용은 을 참조하십시오 "NFS 볼륨 생성 및 관리" Google 문서.

NFSv3 사용자 및 그룹 ID

NFSv3 사용자 및 그룹 ID는 이름이 아닌 숫자 ID로 와이어를 통해 제공됩니다. Cloud Volumes Service는 NFSv3을 사용하는 이러한 숫자 ID에 대해 사용자 이름 확인을 수행하지 않으며 UNIX 보안 스타일 볼륨에서는 모드 비트만 사용합니다. NFSv4.1 ACL이 있으면 NFSv3을 사용하더라도 ACL을 제대로 해결하려면 숫자 ID 조회 및/또는 이름

문자열 조회가 필요합니다. NTFS 보안 스타일 볼륨에서 Cloud Volumes Service는 유효한 UNIX 사용자로 숫자 ID를 확인한 다음 유효한 Windows 사용자에게 매핑하여 액세스 권한을 협상해야 합니다.

NFSv3 사용자 및 그룹 **ID**의 보안 제한

NFSv3에서는 클라이언트와 서버가 숫자 ID로 읽기 또는 쓰기를 시도하는 사용자가 유효한 사용자인지 확인할 필요가 없으며 암시적으로 신뢰됩니다. 이렇게 하면 숫자 ID를 스푸핑하여 파일 시스템이 잠재적 위반으로 열립니다. 이와 같은 보안 문제를 방지하기 위해 Cloud Volumes Service에서 몇 가지 옵션을 사용할 수 있습니다.

- NFS용 Kerberos를 구현하면 사용자가 사용자 이름 및 암호 또는 keytab 파일로 인증하여 Kerberos 티켓을 받아 마운트에 액세스할 수 있도록 합니다. Kerberos는 CVS에서 사용 가능 - 성능 인스턴스와 NFSv4.1에서만 지원됩니다.
- 엑스포트 정책 규칙에 따라 호스트 목록을 제한하면 NFSv3 클라이언트가 Cloud Volumes Service 볼륨에 액세스할 수 있는 범위가 제한됩니다.
- 이중 프로토콜 볼륨을 사용하고 NTFS ACL을 볼륨에 적용하면 NFSv3 클라이언트가 숫자 ID를 유효한 UNIX 사용자 이름으로 확인하게 되어 액세스 마운트에 대한 올바른 인증이 필요합니다. 이를 위해서는 LDAP를 설정하고 UNIX 사용자 및 그룹 ID를 구성해야 합니다.
- 루트 사용자를 스쿼팅하면 루트 사용자가 NFS 마운트에 수행할 수 있는 손상을 제한하지만 위험을 완전히 제거할 수는 없습니다. 자세한 내용은 " 단원을 참조하십시오루트 사용자입니다."

궁극적으로 NFS 보안은 고객이 제공하는 프로토콜 버전으로 제한됩니다. NFSv3은 일반적으로 NFSv4.1보다 더 우수한 성능을 제공하지만, 같은 수준의 보안을 제공하지 않습니다.

NFSv4.1

NFSv4.1은 NFSv3과 비교할 때 다음과 같은 이유로 더욱 뛰어난 보안 및 안정성을 제공합니다.

- 임대 기반 메커니즘을 통한 통합 잠금
- 상태 저장 세션
- 단일 포트에서 모든 NFS 기능 지원(2049)
- TCP 전용
- ID 도메인 매핑
- Kerberos 통합(NFSv3은 Kerberos 사용 가능, NFS에만 해당, NLM 같은 보조 프로토콜에는 사용할 수 없음)

NFSv4.1 종속성

NFSv4.1의 추가 보안 기능 덕분에 NFSv3을 사용할 필요가 없는 몇 가지 외부 의존성이 발생했습니다(Active Directory와 같은 SMB의 의존도 필요 방식과 유사).

NFSv4.1 ACL

Cloud Volumes Service는 NFSv4.x ACL을 지원하므로 다음과 같은 일반적인 POSIX 스타일 사용 권한에 비해 뚜렷한 이점을 제공합니다.

- 파일 및 디렉토리에 대한 사용자 액세스를 세부적으로 제어
- NFS 보안 강화
- CIFS/SMB와의 상호 운용성 향상

- AUTH_SYS 보안을 사용하여 사용자당 16개 그룹의 NFS 제한을 제거합니다
- ACL은 GID(Group ID) 확인이 필요하지 않으므로 GID 리무진을 효과적으로 제거할 수 있습니다. 따라서 Cloud Volumes Service가 아닌 NFS 클라이언트에서 ACL을 제어할 수 있습니다. NFSv4.1 ACL을 사용하려면 클라이언트의 소프트웨어 버전이 이를 지원하고 적절한 NFS 유틸리티가 설치되어 있어야 합니다.

NFSv4.1 ACL과 **SMB** 클라이언트 간의 호환성

NFSv4 ACL은 Windows 파일 레벨 ACL(NTFS ACL)과 다르지만 유사한 기능을 제공합니다. 그러나 멀티 프로토콜 NAS 환경에서 NFSv4.1 ACL이 있고 동일한 데이터 세트의 NFS 및 SMB(이중 프로토콜 액세스)를 사용 중인 경우에는 SMB2.0 이상을 사용하는 클라이언트에서 Windows 보안 탭의 ACL을 보거나 관리할 수 없습니다.

NFSv4.1 ACL의 작동 방식

참고로 다음 용어가 정의되어 있습니다.

- * 액세스 제어 목록(ACL). * 권한 항목의 목록입니다.
- * ACE(액세스 제어 항목).* 목록에 있는 권한 항목.

SetAttr 작업 중에 클라이언트가 파일에서 NFSv4.1 ACL을 설정하면 Cloud Volumes Service는 개체에 해당 ACL을 설정하여 기존 ACL을 대체합니다. 파일에 ACL이 없으면 파일에 대한 모드 권한은 owner@, group@ 및 everyone@에서 계산됩니다. 파일에 기존 SUID/SGID/고정 비트가 있으면 영향을 받지 않습니다.

GETATTR 작업 중에 클라이언트가 파일에서 NFSv4.1 ACL을 받으면 Cloud Volumes Service는 오브젝트와 연결된 NFSv4.1 ACL을 읽고 ACE 목록을 생성하고 목록을 클라이언트에 반환합니다. 파일에 NT ACL 또는 모드 비트가 있는 경우 ACL은 모드 비트에서 구성되며 클라이언트로 반환됩니다.

ACL에 거부 ACE가 있는 경우 액세스가 거부되고 ACE 허용 이 있는 경우 액세스가 부여됩니다. 그러나 ACL에 ACE가 없는 경우에도 액세스가 거부됩니다.

보안 설명자는 SACL(보안 ACL) 및 DACL(임의 ACL)으로 구성됩니다. NFSv4.1이 CIFS/SMB와 상호 운용될 경우 DACL은 NFSv4와 CIFS에 매핑된 일대일 매핑입니다. DACL은 allow 및 deny ACE로 구성됩니다.

NFSv4.1 ACL이 설정된 파일 또는 폴더에서 기본적인 "chmod"를 실행하면 기존 사용자 및 그룹 ACL이 유지되지만 기본 소유자 @, group@, everyone@acls는 수정됩니다.

NFSv4.1 ACL을 사용하는 클라이언트는 시스템의 파일 및 디렉토리에 대한 ACL을 설정하고 볼 수 있습니다. ACL이 있는 디렉터리에 새 파일이나 하위 디렉터리가 만들어지면 해당 개체는 해당 ACL로 태그가 지정된 ACL의 모든 ACE를 상속합니다 "상속 플래그".

파일 또는 디렉토리에 NFSv4.1 ACL이 있으면 해당 ACL을 사용하여 파일 또는 디렉토리에 액세스하는 데 사용되는 프로토콜에 관계없이 액세스를 제어할 수 있습니다.

파일 및 디렉토리는 ACE에 올바른 상속 플래그가 지정된 경우 상위 디렉토리의 NFSv4 ACL에서 ACE를 상속합니다 (적절한 수정 사항이 있을 수 있음).

NFSv4 요청의 결과로 파일 또는 디렉토리가 생성되면 결과 파일 또는 디렉토리의 ACL은 파일 생성 요청에 ACL이 포함되어 있는지 또는 표준 UNIX 파일 액세스 권한만 포함되는지에 따라 달라집니다. ACL은 상위 디렉토리에 ACL이 있는지 여부에도 따라 달라집니다.

- 요청에 ACL이 포함된 경우 해당 ACL이 사용됩니다.
- 요청에 표준 UNIX 파일 액세스 권한만 있고 상위 디렉토리에 ACL이 없는 경우 클라이언트 파일 모드를 사용하여

표준 UNIX 파일 액세스 권한을 설정합니다.

- 요청에 표준 UNIX 파일 액세스 권한만 있고 상위 디렉토리에 상속할 수 없는 ACL이 있는 경우, 요청에 전달된 모드 비트를 기반으로 하는 기본 ACL이 새 개체에 설정됩니다.
- 요청에 표준 UNIX 파일 액세스 권한만 포함되어 있지만 상위 디렉토리에 ACL이 있는 경우 ACE에 적절한 상속 플래그가 지정된 경우 상위 디렉토리의 ACL에 있는 ACE는 새 파일 또는 디렉토리에 의해 상속됩니다.

ACE 권한

NFSv4.1 ACL 사용 권한은 일련의 대문자 및 소문자 값('rxtncy' 등)을 사용하여 액세스를 제어합니다. 이러한 문자 값에 대한 자세한 내용은 을 참조하십시오 "방법: NFSv4 ACL 사용".

umask 및 **ACL** 상속을 사용하는 **NFSv4.1 ACL** 동작

"NFSv4 ACL을 사용하면 ACL 상속을 제공할 수 있습니다". ACL 상속은 NFSv4.1 ACL이 설정된 개체 아래에 생성된 파일 또는 폴더가 의 구성에 따라 ACL을 상속할 수 있음을 의미합니다 "ACL 상속 플래그입니다".

"umask(umask" 관리자 개입 없이 디렉터리에서 파일과 폴더를 만들 수 있는 권한 수준을 제어하는 데 사용됩니다. 기본적으로 Cloud Volumes Service에서는 umask 가 에 따라 예상되는 동작을 나타내는 상속된 ACL을 재정의할 수 있도록 합니다 "RFC 5661".

ACL 형식 지정

NFSv4.1 ACL에는 특정한 형식이 있습니다. 다음은 파일에 설정된 ACE 예제입니다.

```
A::ldapuser@domain.netapp.com:rwatTnNcCy
```

앞의 예제는 의 ACL 형식 지침을 따릅니다.

```
type:flags:principal:permissions
```

A의 유형은 "허용"을 의미합니다. 이 경우 보안 주체가 그룹이 아니며 상속을 포함하지 않으므로 상속 플래그가 설정되지 않습니다. 또한 ACE는 감사 항목이 아니므로 감사 플래그를 설정할 필요가 없습니다. NFSv4.1 ACL에 대한 자세한 내용은 을 참조하십시오 "http://linux.die.net/man/5/nfs4_acl".

NFSv4.1 ACL이 제대로 설정되지 않았거나 클라이언트 및 서버에서 이름 문자열을 확인할 수 없는 경우 ACL이 예상대로 작동하지 않거나 ACL 변경이 적용되지 않고 오류가 발생할 수 있습니다.

샘플 오류에는 다음이 포함됩니다.

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

명시적 거부

NFSv4.1 권한에는 소유자, 그룹 및 모든 사용자에 대한 명시적 거부 특성이 포함될 수 있습니다. 따라서 NFSv4.1 ACL은 기본적으로 -deny를 사용하기 때문에 ACL이 명시적으로 ACE에 의해 부여되지 않으면 거부됩니다. 명시적

거부 특성은 액세스 ACE를 명시적 또는 명시적으로 재정의합니다.

거부 ACE는 Ddes 특성 태그로 설정됩니다.

아래 예에서 group@은 모든 읽기 및 실행 권한을 허용하지만 모든 쓰기 액세스는 거부됩니다.

```
sh-4.1$ nfs4_getfacl /mixed
A::ldapuser@domain.netapp.com:ratTnNcCy
A::OWNER@:rwaDxtTnNcCy
D::OWNER@:
A:g:GROUP@:rxtncy
D:g:GROUP@:waDTC
A::EVERYONE@:rxtncy
D::EVERYONE@:waDTC
```

거부 ACE는 혼란스럽고 복잡할 수 있으므로 가능하면 피해야 합니다. 명시적으로 정의되지 않은 ACL 허용 은 암시적으로 거부됩니다. 거부 ACE가 설정되면 사용자에게 액세스 권한이 부여될 것으로 예상되는 경우 액세스가 거부될 수 있습니다.

앞의 ACE 집합은 모드 비트에서 755와 동일하며, 이는 다음을 의미합니다.

- 소유자에게는 모든 권한이 있습니다.
- 그룹은 읽기 전용입니다.
- 다른 사람들은 읽기 전용입니다.

그러나 사용 권한이 775 상응 권한으로 조정되더라도 모든 사용자에 대해 명시적 거부 설정이 설정되어 있으므로 액세스가 거부될 수 있습니다.

NFSv4.1 ID 도메인 매핑 종속성

NFSv4.1은 ID 도메인 매핑 논리를 보안 계층으로 활용하여 NFSv4.1 마운트에 액세스하려는 사용자가 실제로 자신들이 주장하는 사용자인지 확인합니다. 이 경우 NFSv4.1 클라이언트에서 들어오는 사용자 이름 및 그룹 이름에 이름 문자열이 추가되고 Cloud Volumes Service 인스턴스로 보내집니다. 사용자 이름/그룹 이름 및 ID 문자열 조합이 일치하지 않으면 사용자 및/또는 그룹이 클라이언트의 '/etc/idmapd.conf' 파일에 지정된 기본 nobody 사용자로 충돌합니다.

이 ID 문자열은 특히 NFSv4.1 ACL 및/또는 Kerberos를 사용하는 경우 적절한 권한 준수를 위한 요구 사항입니다. 따라서 적절한 사용자 및 그룹 이름 ID 확인을 위해 클라이언트와 Cloud Volumes Service 간에 일관성을 유지하기 위해 LDAP 서버와 같은 이름 서비스 서버 종속성이 필요합니다.

Cloud Volumes Service는 정적 기본 ID 도메인 이름 값인 ddefaultv4iddomain.com 를 사용합니다. NFS 클라이언트는 ID 도메인 이름 설정에 대해 DNS 도메인 이름으로 기본 설정되지만, '/etc/idmapd.conf'에서 ID 도메인 이름을 수동으로 조정할 수 있습니다.

Cloud Volumes Service에서 LDAP가 활성화된 경우 Cloud Volumes Service는 NFS ID 도메인을 자동화하여 DNS에서 검색 도메인에 대해 구성된 대로 변경할 수 있으며, 다른 DNS 도메인 검색 이름을 사용하지 않는 한 클라이언트를 수정할 필요가 없습니다.

Cloud Volumes Service가 로컬 파일 또는 LDAP에서 사용자 이름 또는 그룹 이름을 확인할 수 있는 경우 도메인

문자열이 사용되고 일치하지 않는 도메인 ID는 아무도 입력할 수 없습니다. Cloud Volumes Service가 로컬 파일 또는 LDAP에서 사용자 이름 또는 그룹 이름을 찾을 수 없는 경우 숫자 ID 값이 사용되며 NFS 클라이언트가 이름을 제대로 확인합니다(NFSv3 동작과 유사).

클라이언트의 NFSv4.1 ID 도메인을 Cloud Volumes Service 볼륨에서 사용 중인 도메인과 일치하도록 변경하지 않고도 다음과 같은 동작이 발생합니다.

- 로컬 UNIX 사용자 및 그룹에 정의된 루트와 같이 Cloud Volumes Service에 로컬 항목이 있는 UNIX 사용자 및 그룹이 nobody 값으로 스쿼트됩니다.
- LDAP에 항목이 있는 UNIX 사용자 및 그룹(Cloud Volumes Service가 LDAP를 사용하도록 구성된 경우)은 DNS 도메인이 NFS 클라이언트와 Cloud Volumes Service 간에 서로 다른 경우 아무도 사용하지 않습니다.
- 로컬 항목이나 LDAP 항목이 없는 UNIX 사용자 및 그룹은 숫자 ID 값을 사용하고 NFS 클라이언트에 지정된 이름으로 확인합니다. 클라이언트에 이름이 없으면 숫자 ID만 표시됩니다.

다음은 이전 시나리오의 결과입니다.

```
# ls -la /mnt/home/prof1/nfs4/
total 8
drwxr-xr-x 2 nobody nobody 4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root   4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835   9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:06 root-user-file
```

클라이언트 및 서버 ID 도메인이 일치하면 동일한 파일 목록이 표시됩니다.

```
# ls -la
total 8
drwxr-xr-x 2 root   root         4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root         4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835         9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 apache apache-group    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 root   root            0 Feb  3 12:06 root-user-file
```

이 문제와 해결 방법에 대한 자세한 내용은 “ 절을 참조하십시오NFSv4.1 및 그 누구도 사용자/그룹을 대상으로 하지 않습니다.”

Kerberos 종속성

NFS에서 Kerberos를 사용하려면 Cloud Volumes Service에서 다음 권한이 있어야 합니다.

- Kerberos KDC(메일 센터 서비스)용 Active Directory 도메인
- LDAP 기능에 대한 UNIX 정보로 채워진 사용자 및 그룹 속성이 있는 Active Directory 도메인(Cloud Volumes Service의 NFS Kerberos에는 적절한 기능을 위해 사용자 SPN-UNIX 사용자 매핑이 필요합니다.)
- Cloud Volumes Service 인스턴스에 대해 LDAP가 설정되었습니다

- DNS 서비스에 대한 Active Directory 도메인입니다

NFSv4.1 및 그 누구도 사용자/그룹을 대상으로 하지 않습니다

NFSv4.1 구성에서 가장 흔히 발생하는 문제 중 하나는 'user:group'의 'nobody:nobody'의 조합으로 'ls'를 사용하여 파일 또는 폴더가 목록에 표시되는 것입니다.

예를 들면 다음과 같습니다.

```
sh-4.2$ ls -la | grep prof1-file
-rw-r--r-- 1 nobody nobody    0 Apr 24 13:25 prof1-file
```

숫자 ID는 99입니다.

```
sh-4.2$ ls -lan | grep prof1-file
-rw-r--r-- 1 99 99    0 Apr 24 13:25 prof1-file
```

경우에 따라 파일의 소유자가 올바르지만 '아무도'가 그룹에 표시되지 않을 수 있습니다.

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r-- 1 prof1  nobody    0 Oct  9  2019 newfile1
```

아무도 없나요?

NFSv4.1의 'nobody' 사용자는 nfsnobody 사용자와 다릅니다. "id" 명령을 실행하여 NFS 클라이언트가 각 사용자를 보는 방법을 볼 수 있습니다.

```
# id nobody
uid=99(nobody) gid=99(nobody) groups=99(nobody)
# id nfsnobody
uid=65534(nfsnobody) gid=65534(nfsnobody) groups=65534(nfsnobody)
```

NFSv4.1에서는 'nobody' 사용자가 'idmapd.conf' 파일에 정의된 기본 사용자이며 사용할 모든 사용자로 정의할 수 있습니다.

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

이 문제가 발생하는 이유는 무엇입니까?

이름 문자열 매핑을 통한 보안은 NFSv4.1 작업의 핵심 요소이므로 이름 문자열이 제대로 일치하지 않을 때 기본 동작은 일반적으로 사용자와 그룹이 소유한 파일 및 폴더에 액세스할 수 없는 사용자에게 스쿼시를 하는 것입니다.

파일 목록에서 사용자 및/또는 그룹에 대해 'nobody'가 표시되는 경우 이는 일반적으로 NFSv4.1에서 잘못 구성된 항목이 있음을 의미합니다. 케이스 민감도는 여기에서 확인할 수 있습니다.

예를 들어 user1@CVSDEMO.LOCA L(uid 1234, gid 1234)이 내보내기에 액세스하는 경우 Cloud Volumes Service에서 user1@CVSDEMO.LOCA L(uid 1234, gid 1234)을 찾을 수 있어야 합니다. Cloud Volumes Service의 사용자가 USER1@CVSDEMO.LOCA L인 경우 일치하지 않습니다(대문자 user1과 소문자 user1 비교). 대부분의 경우 클라이언트의 메시지 파일에서 다음을 볼 수 있습니다.

```
May 19 13:14:29 centos7 nfsidmap[17481]: nss_getpwnam: name
'root@defaultv4iddomain.com' does not map into domain 'CVSDEMO.LOCAL'
May 19 13:15:05 centos7 nfsidmap[17534]: nss_getpwnam: name 'nobody' does
not map into domain 'CVSDEMO.LOCAL'
```

클라이언트와 서버는 모두 사용자가 실제로 자신이 주장하는 사람이라는 데 동의해야 합니다. 따라서 클라이언트가 보는 사용자에게 Cloud Volumes Service가 보는 사용자와 동일한 정보가 있는지 확인하려면 다음을 확인해야 합니다.

- * NFSv4.x ID domain. * Client:'idmapd.conf' file; Cloud Volumes Service는 defaultv4iddomain.com 파일을 사용하며 수동으로 변경할 수 없습니다. NFSv4.1과 함께 LDAP를 사용하는 경우 Cloud Volumes Service는 ID 도메인을 AD 도메인과 동일한 DNS 검색 도메인이 사용 중인 것으로 변경합니다.
- * 사용자 이름 및 숫자 ID. * 이 옵션은 클라이언트가 사용자 이름을 찾는 위치를 결정하고 이름 서비스 스위치 구성(client: ' nsswitch.conf' 및/또는 로컬 passwd 및 group 파일)을 활용합니다. Cloud Volumes Service는 이를 수정할 수 없지만 활성화된 경우 구성에 LDAP를 자동으로 추가합니다.
- * 그룹 이름 및 숫자 ID. * 이 옵션은 클라이언트가 그룹 이름을 찾는 위치를 결정하고 이름 서비스 스위치 구성(client: ' nsswitch.conf' 및/또는 로컬 passwd 및 group 파일)을 활용합니다. Cloud Volumes Service는 이를 수정할 수 없지만 활성화된 경우 구성에 LDAP를 자동으로 추가합니다.

거의 모든 경우에 클라이언트의 사용자 및 그룹 목록에 'nobody'가 표시되면 Cloud Volumes Service와 NFS 클라이언트 간의 사용자 또는 그룹 이름 도메인 ID 변환입니다. 이 시나리오를 방지하려면 LDAP를 사용하여 클라이언트와 Cloud Volumes Service 간의 사용자 및 그룹 정보를 확인합니다.

클라이언트의 **NFSv4.1**에 대한 이름 **ID** 문자열을 보는 중입니다

NFSv4.1을 사용하는 경우 앞서 설명한 대로 NFS 작업 중에 이름 문자열 매핑이 발생합니다.

NFSv4 ID에 대한 문제를 찾기 위해 '/var/log/messages'를 사용하는 것 외에도 을 사용할 수 있습니다 "nfsidmap -l" NFSv4 도메인에 올바르게 매핑된 사용자 이름을 보려면 NFS 클라이언트에서 명령을 실행하십시오.

예를 들어, 이 명령은 클라이언트에서 찾을 수 있는 사용자 및 Cloud Volumes Service가 NFSv4.x 마운트에 액세스하는 이후의 명령 출력입니다.

```
# nfsidmap -l
4 .id_resolver keys found:
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

NFSv4.1 ID 도메인(이 경우, 즉 NetApp-user)에 제대로 매핑되지 않는 사용자가 동일한 마운트에 액세스하여 파일을 만지려고 하면 'nobody:nobody'가 예상한 대로 할당됩니다.

```
# su netapp-user
sh-4.2$ id
uid=482600012(netapp-user), 2000(secondary)
sh-4.2$ cd /mnt/nfs4/
sh-4.2$ touch newfile
sh-4.2$ ls -la
total 16
drwxrwxrwx  5 root   root   4096 Jan 14 17:13 .
drwxr-xr-x. 8 root   root     81 Jan 14 10:02 ..
-rw-r--r--  1 nobody nobody    0 Jan 14 17:13 newfile
drwxrwxrwx  2 root   root   4096 Jan 13 13:20 qtree1
drwxrwxrwx  2 root   root   4096 Jan 13 13:13 qtree2
drwxr-xr-x  2 nfs4   daemon 4096 Jan 11 14:30 testdir
```

nfsidmap-l 출력에서는 디스플레이에 사용자 pcuser가 표시되지만 NetApp-user는 표시되지 않습니다. 이는 엑스포트 정책 규칙('65534')의 익명 사용자입니다.

```
# nfsidmap -l
6 .id_resolver keys found:
  gid:pcuser@CVSDEMO.LOCAL
  uid:pcuser@CVSDEMO.LOCAL
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

중소기업

"중소기업" 는 이더넷 네트워크를 통해 여러 SMB 클라이언트에 중앙 집중식 사용자/그룹 인증, 권한, 잠금 및 파일 공유를 제공하는 Microsoft에서 개발한 네트워크 파일 공유 프로토콜입니다. 파일 및 폴더는 다양한 공유 속성으로 구성할 수 있고 공유 수준 권한을 통해 액세스 제어를 제공하는 공유를 통해 클라이언트에 제공됩니다. SMB는 Windows, Apple 및 Linux 클라이언트를 비롯하여 프로토콜을 지원하는 모든 클라이언트에 제공될 수 있습니다.

Cloud Volumes Service는 SMB 2.1 및 3.x 버전의 프로토콜을 지원합니다.

액세스 제어/**SMB** 공유

- Windows 사용자 이름이 Cloud Volumes Service 볼륨에 대한 액세스를 요청하면 Cloud Volumes Service는 Cloud Volumes Service 관리자가 구성한 방법을 사용하여 UNIX 사용자 이름을 찾습니다.
- 외부 UNIX ID 공급자(LDAP)가 구성되어 있고 Windows/UNIX 사용자 이름이 동일한 경우 Windows 사용자

이름은 추가 구성 없이 1:1을 UNIX 사용자 이름으로 매핑합니다. LDAP가 설정되면 Active Directory를 사용하여 사용자 및 그룹 객체에 대한 UNIX 속성을 호스팅합니다.

- Windows 이름과 UNIX 이름이 동일하게 일치하지 않으면 Cloud Volumes Service에서 LDAP 이름 매핑 구성을 사용할 수 있도록 LDAP를 구성해야 합니다(섹션 참조) ""비대칭 이름 매핑에 LDAP 사용"")를 클릭합니다.
- LDAP를 사용하지 않는 경우 Windows SMB 사용자는 Cloud Volumes Service의 기본 로컬 UNIX 사용자 "pcuser"로 매핑됩니다. 즉, 멀티프로토콜 NAS 환경에서 pcuser로 매핑되는 사용자가 Windows에서 작성한 파일이 UNIX 소유권을 pcuser로 표시합니다. 여기에 있는 'pcuser'는 사실상 리눅스 환경(UID 65534)의 'nobody' 사용자입니다.

SMB만 사용하는 배포에서는 "pcuser" 매핑이 계속 발생하지만 Windows 사용자 및 그룹 소유권이 올바르게 표시되고 SMB 전용 볼륨에 대한 NFS 액세스가 허용되지 않으므로 문제가 되지 않습니다. 또한 SMB 전용 볼륨은 생성된 후 NFS 또는 이중 프로토콜 볼륨으로의 전환을 지원하지 않습니다.

Windows는 Active Directory 도메인 컨트롤러에서 사용자 이름 인증에 Kerberos를 사용합니다. 이 경우 AD DC와 사용자 이름/암호 교환이 필요하며 이는 Cloud Volumes Service 인스턴스 외부에 있습니다. Kerberos 인증은 SMB 클라이언트가 '\\서버 이름' UNC 경로를 사용하는 경우 사용되며 다음 조건이 적용됩니다.

- 서버 이름 에 대한 DNS A/AAAA 항목이 있습니다
- SMB/CIFS 액세스에 유효한 SPN이 SERVERNAME에 존재합니다

Cloud Volumes Service SMB 볼륨이 생성되면 섹션에 정의된 대로 시스템 계정 이름이 생성됩니다 ""Cloud Volumes Service가 Active Directory에 표시되는 방식"" Cloud Volumes Service는 DDNS(동적 DNS)를 활용하여 DNS에 필요한 A/AAAA 및 PTR 항목을 생성하고 시스템 계정 보안 주체에 필요한 SPN 항목을 생성하기 때문에 해당 시스템 계정 이름도 SMB 공유 액세스 경로가 됩니다.

> PTR 항목을 작성하려면 Cloud Volumes Service 인스턴스 IP 주소에 대한 역방향 조회 영역이 DNS 서버에 있어야 합니다.

예를 들어, 이 Cloud Volumes Service 볼륨은 '\\cvs-east-433d.cvsdemo.local' UNC 공유 경로를 사용합니다.

Active Directory에서는 Cloud Volumes Service에서 생성한 SPN 항목이 다음과 같습니다.

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

DNS 정방향/역방향 조회 결과입니다.

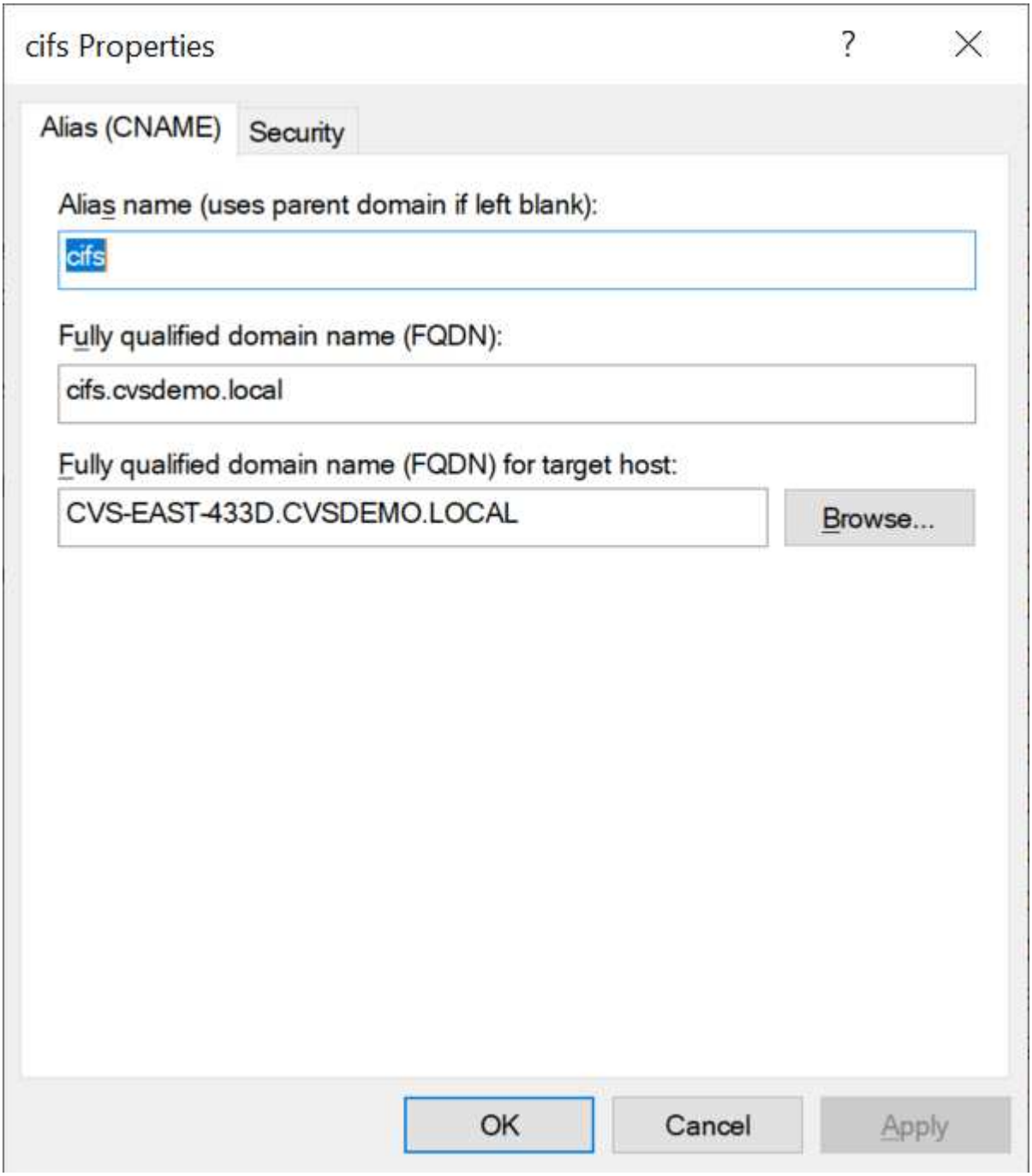
```
PS C:\> nslookup CVS-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
Address:  10.xx.0.xx
Name:    CVS-EAST-433D.CVSDEMO.LOCAL
Address:  10. xxx.0. x
```

선택적으로 Cloud Volumes Service에서 SMB 공유에 대한 SMB 암호화를 설정/요구하여 더 많은 액세스 제어를 적용할 수 있습니다. 엔드포인트 중 하나가 SMB 암호화를 지원하지 않는 경우 액세스가 허용되지 않습니다.

SMB 이름 별칭 사용

경우에 따라 최종 사용자가 Cloud Volumes Service에 사용 중인 컴퓨터 계정 이름을 알아야 하는 보안 문제가 발생할 수 있습니다. 또는 최종 사용자에게 더 간단한 액세스 경로를 제공하려는 경우도 있습니다. 이 경우 SMB 별칭을 생성할 수 있습니다.

SMB 공유 경로에 대한 별칭을 만들려는 경우 DNS에서 CNAME 레코드로 알려진 별칭을 활용할 수 있습니다. 예를 들어 이름이 \\cvs-east-433d.cvssdemo.local이 아닌 공유에 액세스하기 위해 \\cifs"를 사용하되 Kerberos 인증을 계속 사용하려면 기존 A/AAAA 레코드를 가리키는 DNS의 CNAME과 기존 컴퓨터 계정에 추가된 추가 SPN이 Kerberos 액세스를 제공합니다.



CNAME을 추가한 후 생성되는 DNS 정방향 조회 결과입니다.

```
PS C:\> nslookup cifs
Server:  ok-activedirectory.us-east4-a.c.cv-solution-architect-
lab.internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
Aliases:  cifs.cvsdemo.local
```

새 SPN을 추가한 후 생성되는 SPN 쿼리입니다.

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        cifs/cifs.cvsdemo.local
        cifs/cifs
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

패킷 캡처에서는 CNAME에 연결된 SPN을 사용하여 세션 설정 요청을 볼 수 있습니다.

431	4.156722		SMB2	308	Negotiate Protocol Response
432	4.156785		SMB2	232	Negotiate Protocol Request
434	4.158108		SMB2	374	Negotiate Protocol Response
435	4.160977		SMB2	1978	Session Setup Request
437	4.166224		SMB2	322	Session Setup Response
438	4.166891		SMB2	152	Tree Connect Request Tree: \\cifs\IPC$
439	4.168063		SMB2	138	Tree Connect Response

```
    realm: CVSDEMO.LOCAL
  ⌄ sname
      name-type: kRB5-NT-SRV-INST (2)
    ⌄ sname-string: 2 items
        SNameString: cifs
        SNameString: cifs
  ⌄ enc-part
      etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
```

SMB 인증 방언

Cloud Volumes Service는 다음을 지원합니다 "방언" SMB 인증의 경우:

- LM
- NTLM
- NTLMv2
- Kerberos

SMB 공유 액세스를 위한 Kerberos 인증은 사용할 수 있는 가장 안전한 인증 수준입니다. AES 및 SMB 암호화를 활성화하면 보안 수준이 더욱 높아집니다.

또한 Cloud Volumes Service는 LM 및 NTLM 인증에 대한 이전 버전과의 호환성을 지원합니다. Kerberos가 잘못 구성된 경우(예: SMB 별칭 생성 시), 공유 액세스는 NTLMv2와 같은 취약한 인증 방법으로 되돌아갑니다. 이러한 메커니즘은 보안성이 떨어지기 때문에 일부 Active Directory 환경에서는 비활성화됩니다. 취약한 인증 방법을 사용하지

않도록 설정하고 Kerberos를 제대로 구성하지 않으면 다시 사용할 유효한 인증 방법이 없기 때문에 공유 액세스가 실패합니다.

Active Directory에서 지원되는 인증 수준을 구성/보는 방법에 대한 자세한 내용은 을 참조하십시오 "네트워크 보안: LAN Manager 인증 레벨".

권한 모델

NTFS/파일 권한

NTFS 권한은 NTFS 로직을 따르는 파일 시스템의 파일 및 폴더에 적용되는 권한입니다. 기본 또는 고급 에서 NTFS 권한을 적용할 수 있으며 액세스 제어를 위해 허용 또는 거부 로 설정할 수 있습니다.

기본 사용 권한은 다음과 같습니다.

- 모든 권한
- 수정
- 읽기 및 실행
- 읽기
- 쓰기

ACE라고 하는 사용자 또는 그룹에 대한 사용 권한을 설정하면 ACL에 상주합니다. NTFS 권한은 UNIX 모드 비트와 동일한 읽기/쓰기/실행 기본 사항을 사용하지만 소유권 가져오기, 폴더 만들기/데이터 추가, 속성 쓰기 등과 같은 보다 세분화된 확장 액세스 제어(특수 권한이라고도 함)로 확장할 수도 있습니다.

표준 UNIX 모드 비트는 NTFS 권한과 동일한 수준의 세분화 수준을 제공하지 않습니다(예: ACL에서 개별 사용자 및 그룹 개체에 대한 권한을 설정하거나 확장 속성을 설정할 수 있음). 그러나 NFSv4.1 ACL은 NTFS ACL과 동일한 기능을 제공합니다.

NTFS 권한은 공유 권한보다 더 구체적이며 공유 권한과 함께 사용할 수 있습니다. NTFS 권한 구조에서는 가장 제한적인 권한이 적용됩니다. 따라서 사용자 또는 그룹에 대한 명시적 변명의 경우 액세스 권한을 정의할 때 전체 제어보다 우선합니다.

NTFS 권한은 Windows SMB 클라이언트에서 제어됩니다.

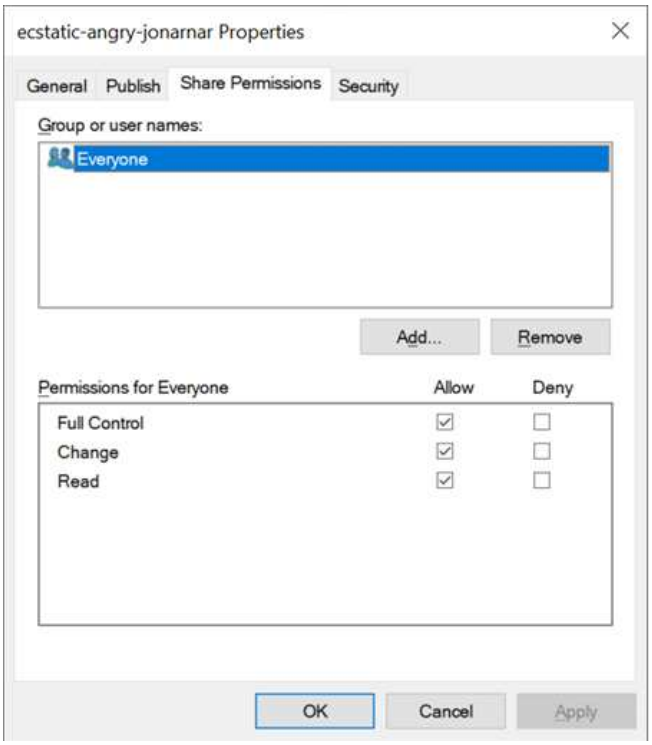
공유 권한

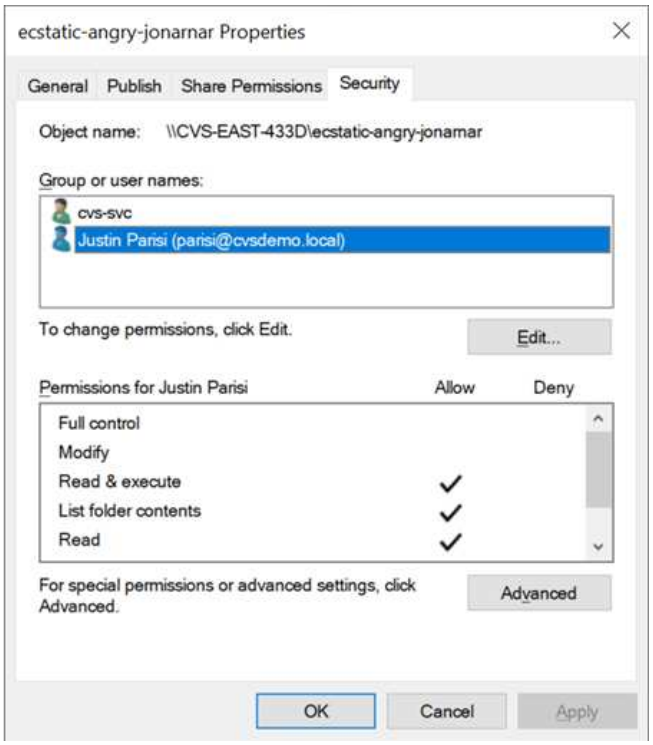
공유 권한은 NTFS 권한(읽기/변경/모든 제어만 해당)보다 더 일반적이며, SMB 공유의 초기 항목을 제어합니다. 이는 NFS 내보내기 정책 규칙의 작동 방식과 유사합니다.

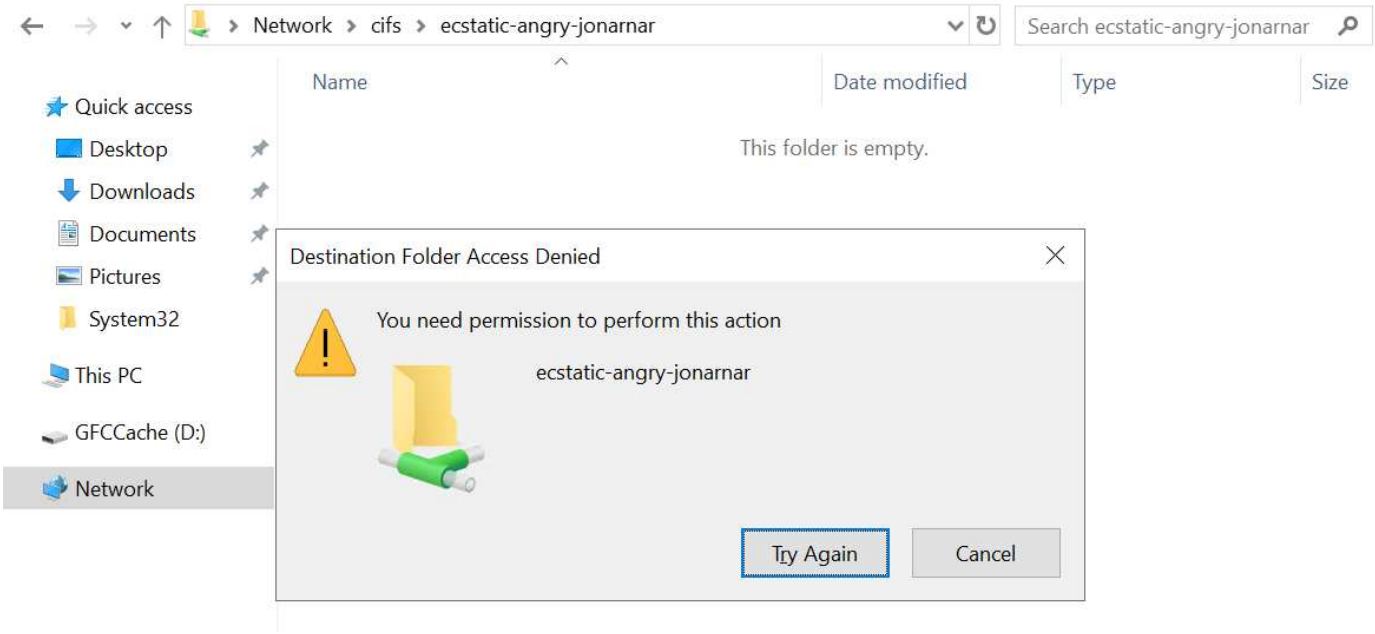
NFS 내보내기 정책 규칙은 IP 주소 또는 호스트 이름과 같은 호스트 기반 정보를 통해 액세스를 제어하지만 SMB 공유 권한은 공유 ACL에서 사용자 및 그룹 ACE를 사용하여 액세스를 제어할 수 있습니다. Windows 클라이언트 또는 Cloud Volumes Service 관리 UI에서 공유 ACL을 설정할 수 있습니다.

기본적으로 공유 ACL 및 초기 볼륨 ACL에는 모든 권한이 있는 모든 사용자가 포함됩니다. 파일 ACL은 변경되어야 하지만 공유 권한은 공유의 객체에 대한 파일 권한에 의해 무시됩니다.

예를 들어, 사용자가 Cloud Volumes Service 볼륨 파일 ACL에 대한 읽기 액세스만 허용되는 경우 다음 그림과 같이 공유 ACL이 모든 권한이 있는 사용자로 설정되어 있어도 파일 및 폴더 생성에 대한 액세스가 거부됩니다.







최상의 보안 결과를 얻으려면 다음을 수행하십시오.

- 공유 및 파일 ACL에서 모든 사용자를 제거하고 대신 사용자 또는 그룹에 대한 공유 액세스를 설정합니다.
- 개별 사용자 대신 그룹을 사용하여 액세스 제어를 수행할 수 있어 관리가 용이하고 그룹 관리를 통해 ACL을 공유할 사용자를 더 빠르게 제거/추가할 수 있습니다.
- 공유 권한에 있는 ACE에 대한 덜 제한적이고 보다 일반적인 공유 액세스를 허용하고 보다 세분화된 액세스 제어를 위한 파일 권한을 가진 사용자 및 그룹에 대한 액세스를 잠급니다.
- 명시적 거부 ACL은 ACL 허용 을 재정의하므로 일반적인 사용을 피합니다. 파일 시스템에 대한 액세스를 신속하게 제한해야 하는 사용자 또는 그룹의 명시적 거부 ACL 사용을 제한합니다.
- 에 주의를 기울이십시오 "ACL 상속" 사용 권한을 수정할 때 설정; 파일 수가 많은 디렉토리 또는 볼륨의 최상위

레벨에서 상속 플래그를 설정하면 해당 디렉토리 또는 볼륨 아래의 각 파일에 상속된 사용 권한이 추가되었음을 의미합니다. 의도하지 않은 액세스/거부 및 각 파일이 조정될 때 권한 수정 장기 이탈과 같은 원치 않는 동작이 발생할 수 있습니다.

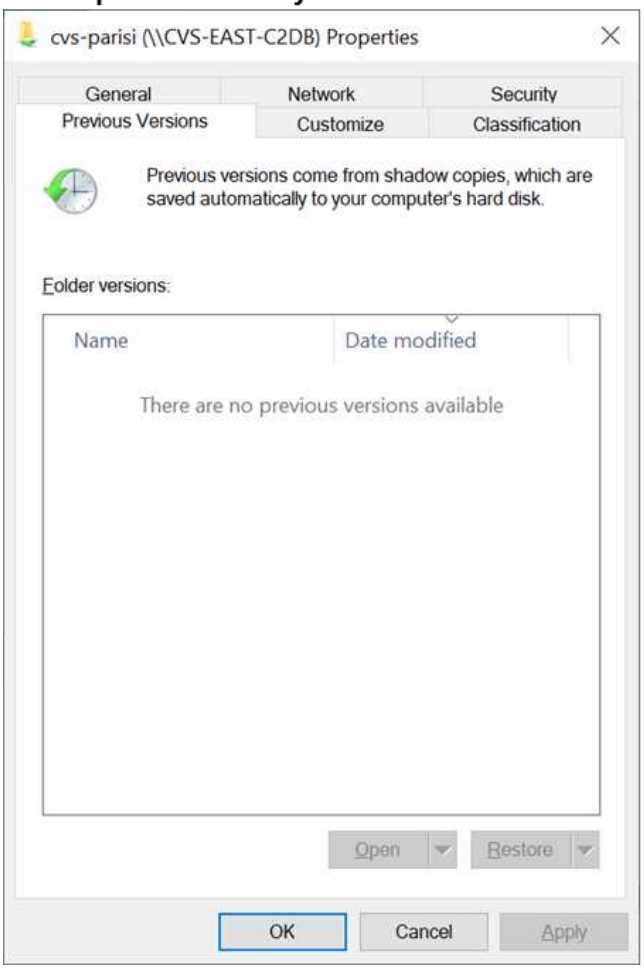
SMB는 보안 기능을 공유합니다

Cloud Volumes Service에서 SMB 액세스가 가능한 볼륨을 처음 생성하면 해당 볼륨을 보호하기 위한 일련의 선택 사항이 표시됩니다.

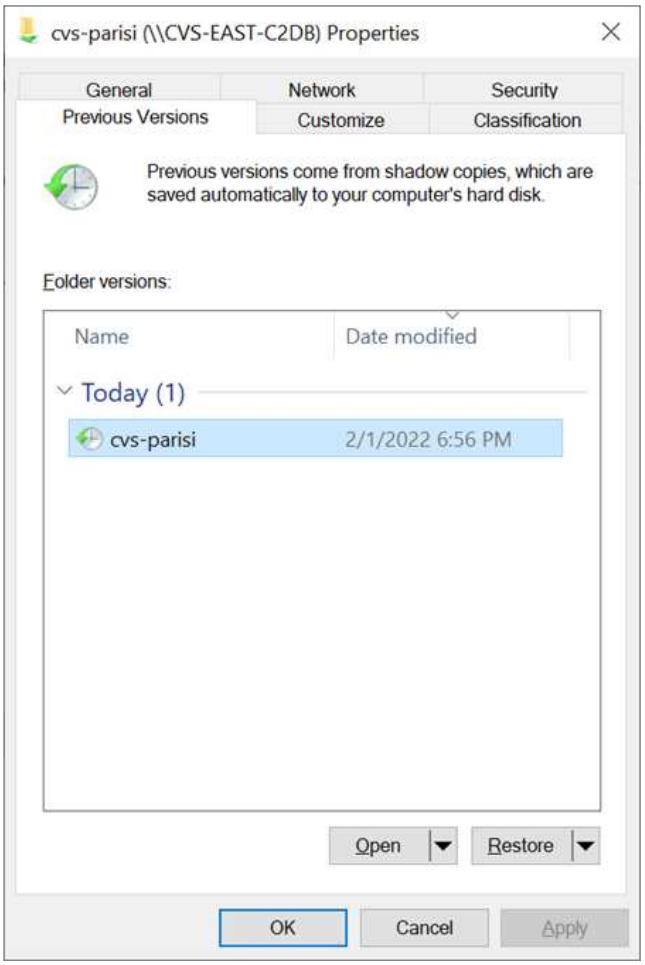
이러한 선택 사항 중 일부는 Cloud Volumes Service 레벨(성능 또는 소프트웨어)에 따라 달라지며 다음과 같은 옵션이 있습니다.

- * 스냅샷 디렉토리를 표시합니다(CVS - 성능 및 CVS - SW 모두에서 사용 가능). * 이 옵션은 SMB 클라이언트가 SMB 공유의 스냅샷 디렉토리에 액세스할 수 있는지 여부를 제어합니다('\\server\share\~snapshot' 및/또는 Previous Versions 탭). 기본 설정은 선택되지 않습니다. 즉, 볼륨이 기본적으로 `~snapshot' 디렉토리에 대한 액세스를 숨기거나 허용하지 않으며 볼륨의 이전 버전 탭에 스냅샷 복사본이 나타나지 않습니다.

Snapshot directory visible: Unchecked



Snapshot directory visible: Checked



보안 상의 이유, 성능상의 이유(AV 스캔에서 이러한 폴더 숨기기) 또는 기본 설정을 위해 최종 사용자로부터 스냅샷 복사본을 숨기는 것이 좋습니다. Cloud Volumes Service 스냅샷은 읽기 전용이므로 이러한 스냅샷이 표시되는 경우에도 최종 사용자는 스냅샷 디렉토리의 파일을 삭제하거나 수정할 수 없습니다. 스냅샷 복사본이 생성된 시점의 파일 또는 폴더에 대한 파일 권한이 적용됩니다. 파일 또는 폴더의 사용 권한이 Snapshot 복사본 간에 변경되면 변경 내용이 Snapshot 디렉토리의 파일 또는 폴더에도 적용됩니다. 사용자 및 그룹은 권한에 따라 이러한 파일 또는 폴더에 액세스할 수 있습니다. 스냅샷 디렉토리에서 파일을 삭제하거나 수정할 수는 없지만 스냅샷 디렉토리에서 파일 또는

폴더를 복사할 수는 있습니다.

- * SMB 암호화 활성화(CVS - 성능 및 CVS - SW 모두에 사용 가능). * SMB 공유에서 SMB 암호화는 기본적으로 비활성화되어 있습니다(선택 취소됨). 이 확인란을 선택하면 SMB 암호화가 활성화됩니다. 즉, SMB 클라이언트와 서버 간의 트래픽은 협상된 가장 높은 암호화 수준으로 전송 중에 암호화됩니다. Cloud Volumes Service는 SMB에 대해 최대 AES-256 암호화를 지원합니다. SMB 암호화를 활성화하면 SMB 클라이언트에서 성능 저하가 발생할 수 있으며, 이는 대략 10~20% 범위에서 나타날 수도 있고 그렇지 않을 수도 있습니다. 테스트 결과, 성능 저하가 허용 가능한지 여부를 확인하는 것이 좋습니다.
- * SMB 공유 숨기기(CVS - 성능 및 CVS - SW 모두에 사용 가능) * 이 옵션을 설정하면 SMB 공유 경로가 일반 탐색에서 숨겨집니다. 즉, 공유 경로를 모르는 클라이언트는 기본 UNC 경로("\\CVS-SMB" 등)에 액세스할 때 공유를 볼 수 없습니다. 이 확인란을 선택하면 SMB 공유 경로를 명시적으로 알고 있거나 그룹 정책 개체에서 정의한 공유 경로를 가진 클라이언트만 액세스할 수 있습니다(난독 처리를 통한 보안).
- * ABE(액세스 기반 열거) 사용(CVS-SW만 해당). * SMB 공유를 숨기는 것과 비슷하지만, 공유 또는 파일이 개체에 액세스할 권한이 없는 사용자 또는 그룹에서만 숨겨지는 것을 제외하고는 차이가 있습니다. 예를 들어, Windows 사용자 'Joe'가 권한을 통한 읽기 액세스를 최소한 허용하지 않으면 Windows 사용자 'Joe'는 SMB 공유나 파일을 전혀 볼 수 없습니다. 이 기능은 기본적으로 비활성화되어 있으며 확인란을 선택하여 활성화할 수 있습니다. ABE에 대한 자세한 내용은 NetApp 기술 자료 문서를 참조하십시오 "ABE(Access Based Enumeration)는 어떻게 작동합니까?"
- * 지속적으로 사용 가능한(CA) 공유 지원 활성화(CVS - 성능만 해당) * "지속적으로 사용 가능한 SMB 공유" Cloud Volumes Service 백엔드 시스템의 노드 간에 잠금 상태를 복제하여 페일오버 이벤트 중에 애플리케이션 중단을 최소화할 수 있는 방법을 제공합니다. 이 기능은 보안 기능이 아니지만 전반적으로 더 뛰어난 복원력을 제공합니다. 현재 이 기능에는 SQL Server 및 FSLogix 애플리케이션만 지원됩니다.

숨겨진 기본 공유

SMB 서버가 Cloud Volumes Service에서 생성되면 서버가 생성됩니다 "숨겨진 관리 공유" ($ 명명 규칙 사용) - 데이터 볼륨 SMB 공유 이외에 생성됩니다. 여기에는 C$(네임스페이스 액세스) 및 IPC$(Microsoft Management Console(MMC) 액세스에 사용되는 RPC(원격 프로시저 호출)와 같은 프로그램 간 통신을 위한 명명된 파이프 공유)가 포함됩니다.

IPC$ 공유는 공유 ACL을 포함하지 않으며 수정할 수 없습니다. RPC 호출 및 에 엄격하게 사용됩니다 "Windows에서는 기본적으로 이러한 공유에 대한 익명 액세스를 허용하지 않습니다".

C$ 공유는 기본적으로 BUILTIN/Administrators 액세스를 허용하지만, Cloud Volumes Service 자동화는 공유 ACL을 제거하고, C$ 공유에 대한 액세스를 통해 Cloud Volumes Service 파일 시스템에 마운트된 모든 볼륨을 볼 수 있으므로 다른 사람에게 액세스를 허용하지 않습니다. 따라서 '\\server\C$'로 이동하려고 하면 실패합니다.

로컬/BUILTIN 관리자/백업 권한이 있는 계정

Cloud Volumes Service SMB 서버는 일부 도메인 사용자 및 그룹에 액세스 권한을 적용하는 로컬 그룹(예: BUILTIN\Administrators)이 있다는 점에서 일반 Windows SMB 서버와 유사한 기능을 유지합니다.

백업 사용자에 추가할 사용자를 지정하면 해당 Active Directory 연결을 사용하는 Cloud Volumes Service 인스턴스의 BUILTIN\Backup Operators 그룹에 사용자가 추가되고 이 그룹에 이 사용자가 추가됩니다 "SeBackupPrivilege 및 SeRestorePrivilege를 참조하십시오".

사용자를 보안 권한 사용자 에 추가하면 사용자에게 SeSecurityPrivilege 가 부여되며, 이 권한은 와 같은 일부 응용 프로그램 사용 사례에 유용합니다 "SMB 공유의 SQL Server".

Backup Users

Provide a comma separated list of domain users or a domain group name that require elevated privileges to access volumes created by Cloud Volumes Service.

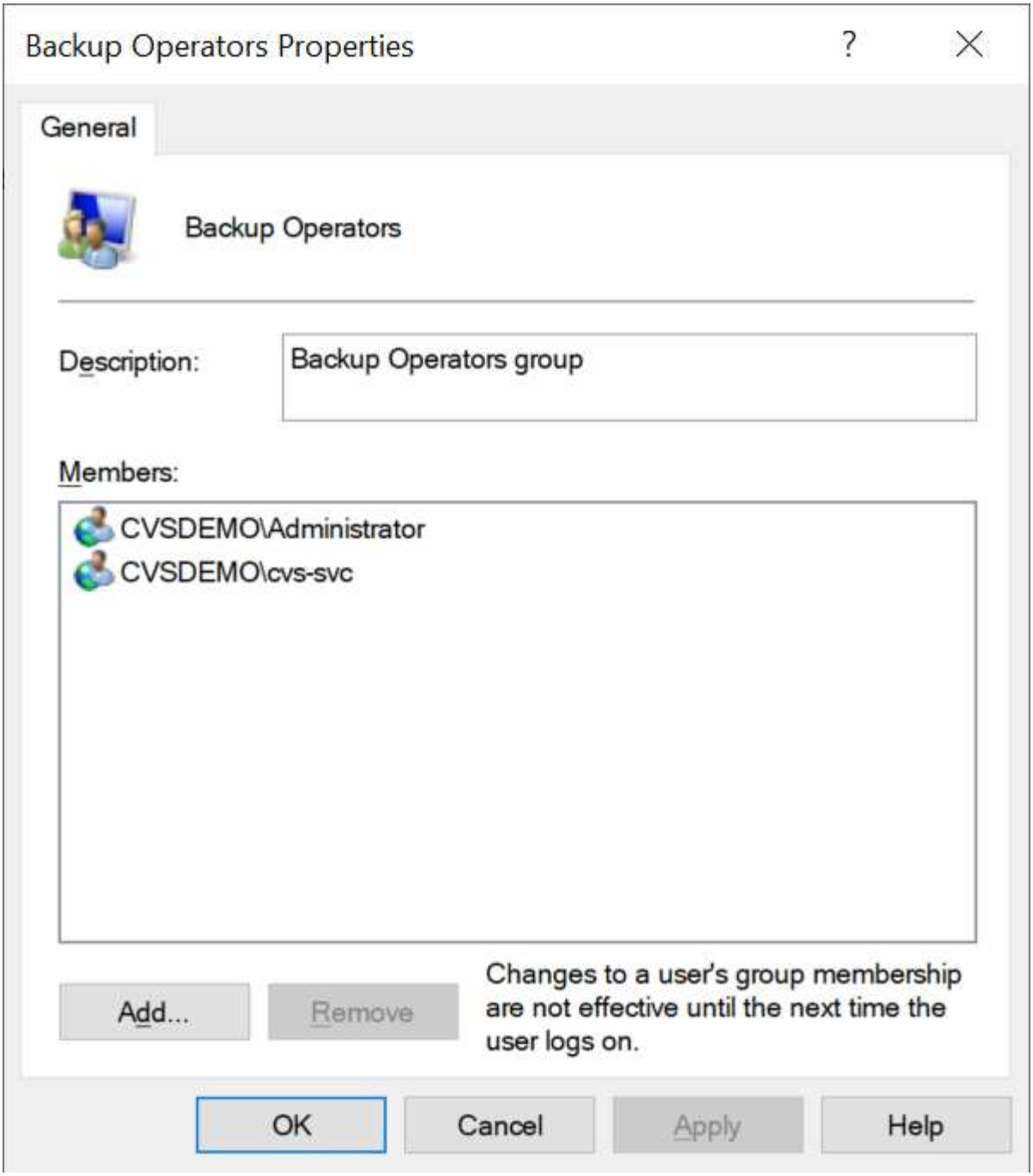
Accountnames
administrator,cvs-svc

Security Privilege Users

Provide a list of comma separated domain user accounts that require elevated privileges to manage security log for the Active Directory associated with Cloud Volumes Service.

Accountnames
administrator,cvs-svc

적절한 권한이 있는 MMC를 통해 Cloud Volumes Service 로컬 그룹 구성원 자격을 볼 수 있습니다. 다음 그림에서는 Cloud Volumes Service 콘솔을 사용하여 추가된 사용자를 보여 줍니다.

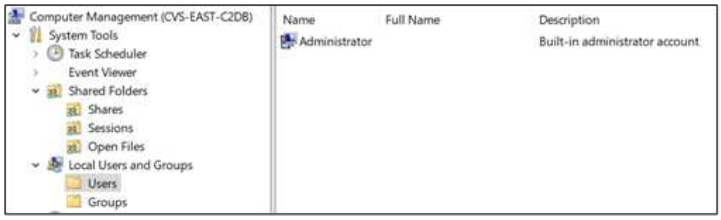


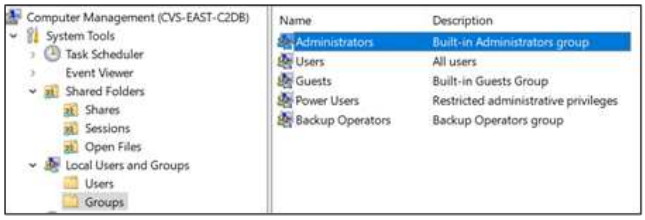
다음 표에서는 기본 BUILTIN 그룹 목록과 기본적으로 추가되는 사용자/그룹을 보여 줍니다.

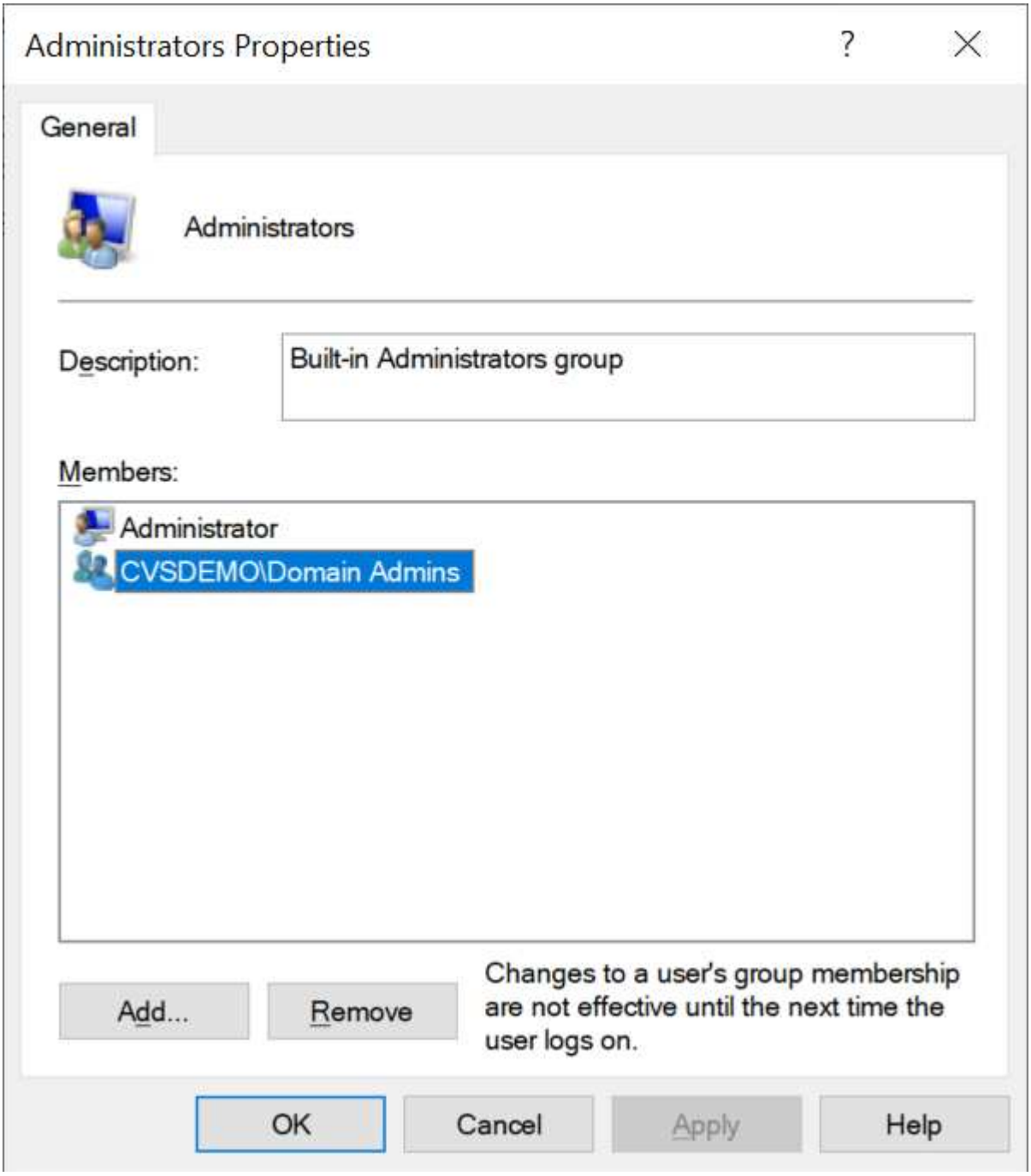
로컬/**BUILTIN** 그룹	기본 멤버
BUILTIN\Administrators *	Domain\Domain Admins입니다
BUILTIN\Backup Operators *	없음
BUILTIN\Guest입니다	도메인\도메인 게스트입니다
BUILTIN\고급 사용자	없음
BUILTIN\도메인 사용자	도메인\도메인 사용자

- Cloud Volumes Service Active Directory 연결 구성에서 그룹 멤버십이 제어됩니다.

MMC 창에서 로컬 사용자 및 그룹(및 그룹 구성원)을 볼 수 있지만 개체를 추가 또는 삭제하거나 이 콘솔에서 그룹 구성원을 변경할 수는 없습니다. 기본적으로 도메인 관리자 그룹 및 관리자만 Cloud Volumes Service의 BUILTIN\Administrators 그룹에 추가됩니다. 현재 수정할 수 없습니다.







MMC/컴퓨터 관리 액세스

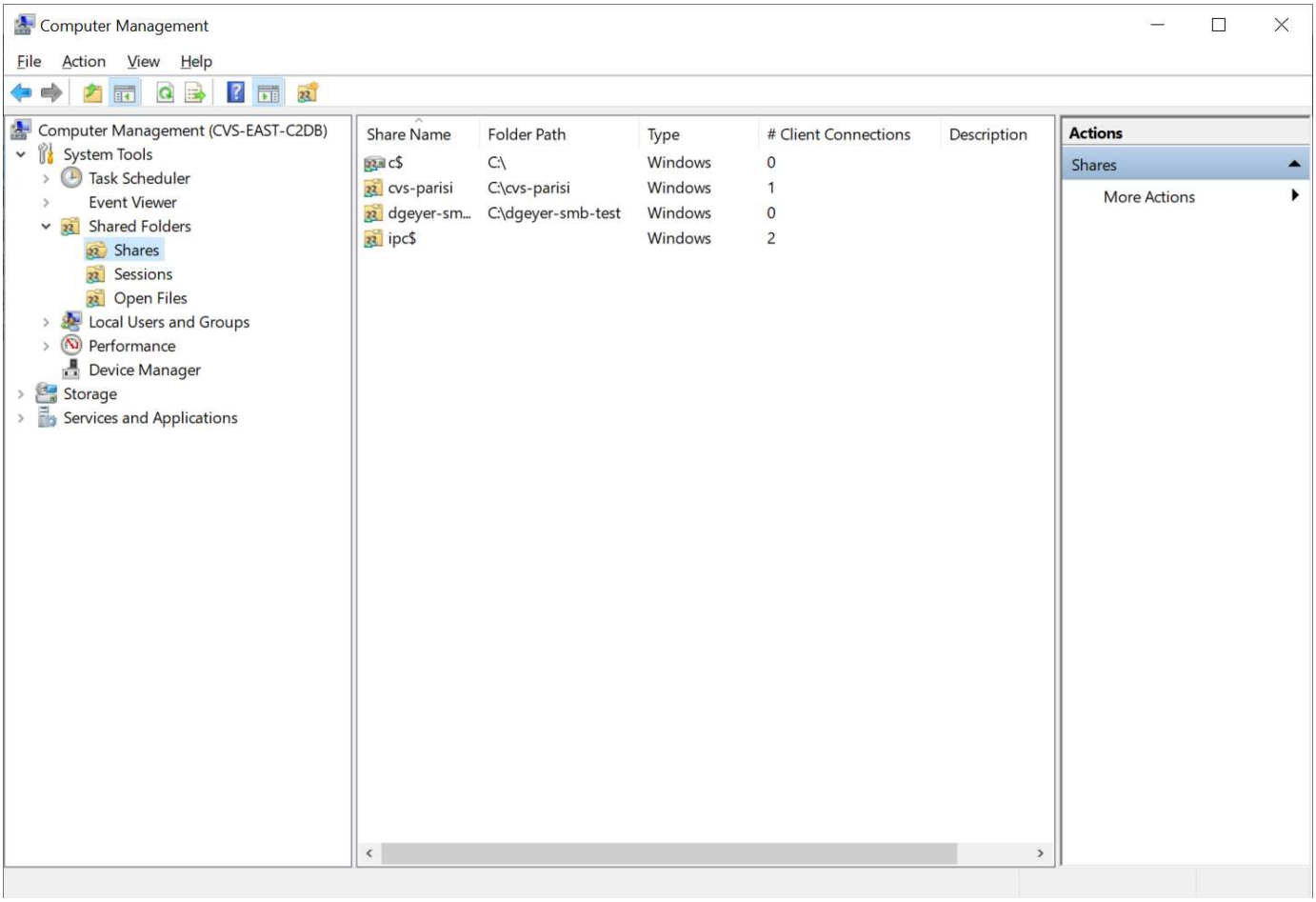
Cloud Volumes Service의 SMB 액세스는 공유를 보고, 공유 ACL을 관리하고, SMB 세션 및 열린 파일을 확인/관리할 수 있는 컴퓨터 관리 MMC에 대한 연결을 제공합니다.

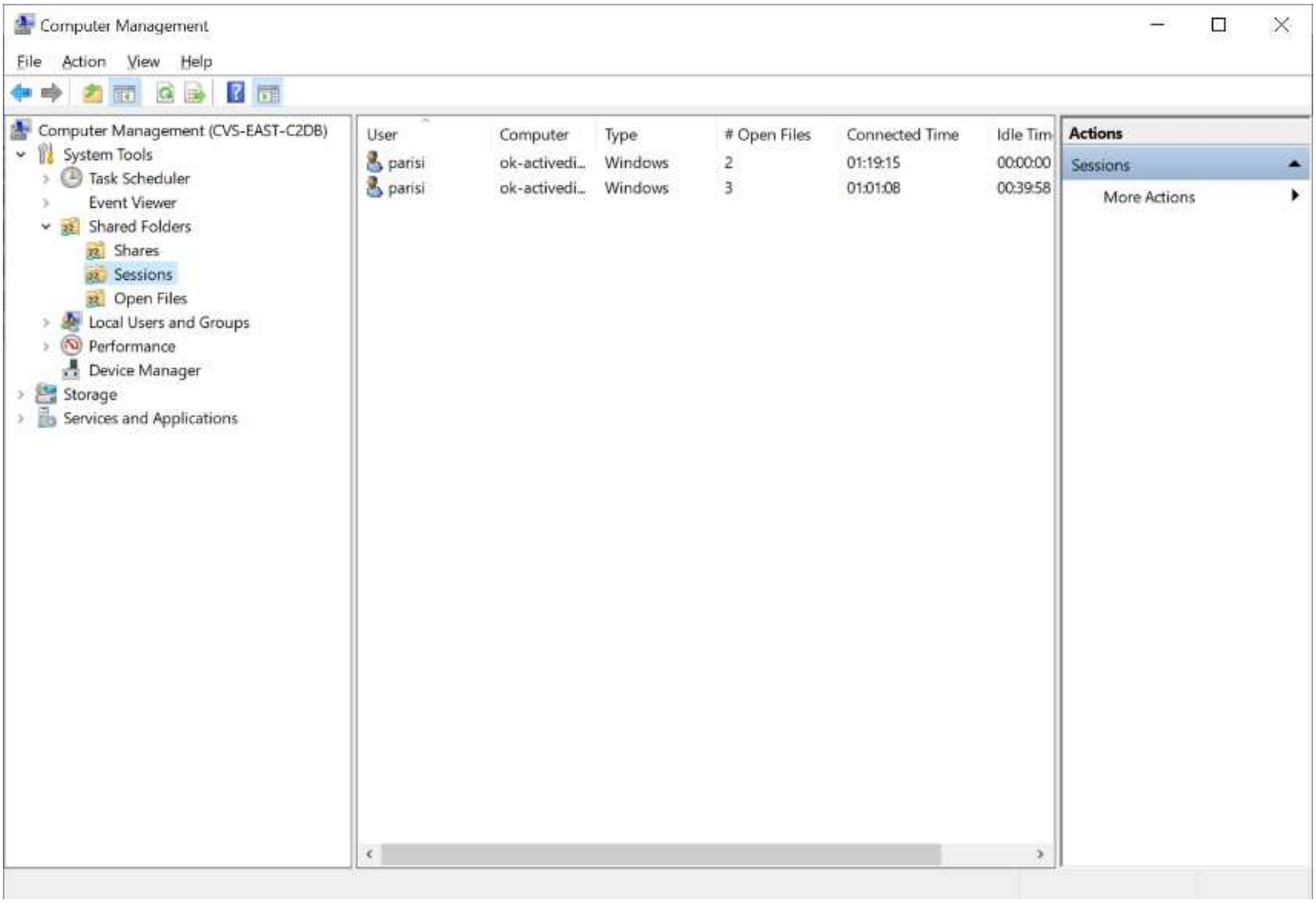
MMC를 사용하여 Cloud Volumes Service에서 SMB 공유 및 세션을 보려면 현재 로그인한 사용자가 도메인 관리자여야 합니다. 다른 사용자는 MMC에서 SMB 서버를 보거나 관리할 수 있으며 Cloud Volumes Service SMB 인스턴스에서 공유 또는 세션을 보려고 할 때 사용 권한 없음 대화 상자를 받을 수 있습니다.

SMB 서버에 연결하려면 컴퓨터 관리를 열고 컴퓨터 관리를 마우스 오른쪽 단추로 클릭한 다음 다른 컴퓨터에 연결을 선택합니다. 그러면 Cloud Volumes Service 볼륨 정보에 있는 SMB 서버 이름을 입력할 수 있는 컴퓨터 선택 대화 상자가 열립니다.

적절한 권한이 있는 SMB 공유를 보면 Active Directory 연결을 공유하는 Cloud Volumes Service 인스턴스에서 사용 가능한 모든 공유가 표시됩니다. 이 동작을 제어하려면 Cloud Volumes Service 볼륨 인스턴스에서 SMB 공유 숨기기 옵션을 설정합니다.

지역당 하나의 Active Directory 연결만 허용됩니다.





다음 표에는 MMC에서 지원/지원되지 않는 기능 목록이 나와 있습니다.

지원되는 함수	지원되지 않는 함수
• 공유 보기 • 활성 SMB 세션을 봅니다 • 열린 파일을 봅니다 • 로컬 사용자 및 그룹을 봅니다 • 로컬 그룹 구성원 자격을 봅니다 • 시스템의 세션, 파일 및 트리 연결 목록을 열거합니다 • 시스템에서 열려 있는 파일을 닫습니다 • 열려 있는 세션을 닫습니다 • 공유 생성/관리	• 새 로컬 사용자/그룹을 생성합니다 • 기존 로컬 사용자/그룹 관리/보기 • 이벤트 또는 성능 로그를 봅니다 • 스토리지 관리 • 서비스 및 애플리케이션 관리

SMB 서버 보안 정보

Cloud Volumes Service의 SMB 서버는 Kerberos 클록 편중, 티켓 사용 기간, 암호화 등 SMB 연결에 대한 보안 정책을 정의하는 일련의 옵션을 사용합니다.

다음 표에는 이러한 옵션, 기능, 기본 설정 및 Cloud Volumes Service를 사용하여 수정할 수 있는 경우 등이 나와

있습니다. 일부 옵션은 Cloud Volumes Service에는 적용되지 않습니다.

보안 옵션	기능	기본값	변경할 수 있습니까?
최대 Kerberos 클럭 비뚤어짐(분)	Cloud Volumes Service와 도메인 컨트롤러 간의 최대 시간 편중 시간 차이가 5분을 초과하면 Kerberos 인증이 실패합니다. 이 값은 Active Directory 기본값으로 설정됩니다.	5	아니요
Kerberos 티켓 수명(시간)	갱신이 요구되기 전에 Kerberos 티켓이 유효한 상태로 유지되는 최대 시간입니다. 10시간 전에 갱신이 발생하지 않으면 새 티켓을 받아야 합니다. Cloud Volumes Service는 이러한 갱신을 자동으로 수행합니다. Active Directory 기본값은 10시간입니다.	10	아니요
최대 Kerberos 티켓 갱신(일)	새 승인 요청이 필요해지기 전에 Kerberos 티켓을 갱신할 수 있는 최대 일수입니다. Cloud Volumes Service는 SMB 연결에 대한 티켓을 자동으로 갱신합니다. 7일은 Active Directory 기본값입니다.	7	아니요
Kerberos KDC 연결 시간 초과(초)	KDC 연결이 시간 초과되기 전의 시간(초)입니다.	3	아니요
수신 SMB 트래픽에 서명 필요	SMB 트래픽에 서명 필요 로 설정합니다. true로 설정하면 서명을 지원하지 않는 클라이언트가 연결되지 않습니다.	거짓	
로컬 사용자 계정에 암호 복잡성 필요	로컬 SMB 사용자의 암호에 사용됩니다. Cloud Volumes Service는 로컬 사용자 생성을 지원하지 않으므로 이 옵션은 Cloud Volumes Service에는 적용되지 않습니다.	참	아니요
Active Directory LDAP 연결에 start_TLS를 사용합니다	Active Directory LDAP에 대한 TLS 연결 시작을 활성화하는 데 사용됩니다. Cloud Volumes Service에서는 현재 이 설정을 지원하지 않습니다.	거짓	아니요

보안 옵션	기능	기본값	변경할 수 있습니까?
Kerberos를 사용하도록 AES-128 및 AES-256 암호화를 사용합니다	Active Directory 연결에 AES 암호화를 사용할지 여부를 제어하고 Active Directory 연결을 생성 /수정할 때 Active Directory 인증에 AES 암호화 사용 옵션을 사용하여 제어합니다.	거짓	예
LM 호환성 수준	Active Directory 연결에 대해 지원되는 인증 방언의 수준입니다. 자세한 내용은 " 단원을 참조하십시오SMB 인증 방언"를 참조하십시오.	NTLMv2 - KRB	아니요
수신 CIFS 트래픽에 SMB 암호화 필요	모든 공유에 SMB 암호화가 필요합니다. 이 기능은 Cloud Volumes Service에서 사용되지 않으며 대신 볼륨별로 암호화를 설정합니다(“ 절 참조)SMB는 보안 기능을 공유합니다").	거짓	아니요
클라이언트 세션 보안	LDAP 통신에 대한 서명 및 /또는 봉인을 설정합니다. 이 설정은 현재 Cloud Volumes Service에 설정되어 있지 않지만 향후 릴리즈에서 필요할 수 있습니다. Windows 패치로 인한 LDAP 인증 문제에 대한 해결 방법은 섹션에서 설명합니다 ""“LDAP 채널 바인딩.”".	없음	아니요
SMB2가 DC 연결에 대해 설정됩니다	DC 연결에 SMB2를 사용합니다. 기본적으로 사용됩니다.	System - 기본값입니다	아니요
LDAP 조회	여러 LDAP 서버를 사용하는 경우 조회 추적을 통해 첫 번째 서버에서 항목을 찾을 수 없을 때 클라이언트가 목록의 다른 LDAP 서버를 참조할 수 있습니다. 현재 Cloud Volumes Service에서는 지원되지 않습니다.	거짓	아니요
보안 Active Directory 연결에 LDAPS를 사용합니다	SSL을 통한 LDAP 사용을 활성화합니다. 현재 Cloud Volumes Service에서 지원되지 않습니다.	거짓	아니요

보안 옵션	기능	기본값	변경할 수 있습니까?
DC 연결에 암호화가 필요합니다	성공적인 DC 연결을 위해 암호화가 필요합니다. Cloud Volumes Service에서 기본적으로 비활성화되어 있습니다.	거짓	아니요

이중 프로토콜/멀티프로토콜

Cloud Volumes Service는 적절한 액세스 권한을 유지하면서 동일한 데이터 세트를 SMB 및 NFS 클라이언트 모두에 공유할 수 있는 기능을 제공합니다 ("이중 프로토콜")를 클릭합니다. 이는 프로토콜 간 ID 매핑을 조정하고 중앙 집중식 백엔드 LDAP 서버를 사용하여 Cloud Volumes Service에 UNIX ID를 제공하는 방식으로 수행됩니다. Windows Active Directory를 사용하여 Windows 및 UNIX 사용자를 모두 편리하게 제공할 수 있습니다.

액세스 제어

- * 공유 액세스 제어. * NAS 공유에 액세스할 수 있는 클라이언트 및/또는 사용자 및 그룹을 결정합니다. NFS의 경우 엑스포트 정책과 규칙을 사용하여 클라이언트 엑스포트 액세스를 제어합니다. NFS 내보내기는 Cloud Volumes Service 인스턴스에서 관리됩니다. SMB는 CIFS/SMB 공유를 사용하고 ACL을 공유하여 사용자 및 그룹 레벨에서 보다 세부적인 제어를 제공합니다. 을 사용하여 SMB 클라이언트의 공유 레벨 ACL만 구성할 수 있습니다 "MMC/컴퓨터 관리" Cloud Volumes Service 인스턴스에 대한 관리자 권한이 있는 계정(섹션 참조) "" 로컬/BUILTIN 관리자/백업 권한이 있는 계정.")를 클릭합니다.
- * 파일 액세스 제어. * 파일 또는 폴더 수준에서 권한을 제어하고 항상 NAS 클라이언트에서 관리합니다. NFS 클라이언트는 기존 모드 비트(rwx) 또는 NFSv4 ACL을 사용할 수 있습니다. SMB 클라이언트는 NTFS 권한을 활용합니다.

NFS와 SMB 모두에 데이터를 제공하는 볼륨의 액세스 제어는 사용 중인 프로토콜에 따라 다릅니다. 이중 프로토콜의 사용 권한에 대한 자세한 내용은 “ 절을 참조하십시오권한 모델.”

사용자 매핑

클라이언트가 볼륨에 액세스하면 Cloud Volumes Service는 들어오는 사용자를 반대 방향으로 유효한 사용자에게 매핑하려고 시도합니다. 이는 프로토콜 간에 적절한 액세스를 결정하고 액세스를 요청하는 사용자가 실제로 자신이 주장하는 사용자인지 확인하기 위해 필요합니다.

예를 들어, "joe"라는 Windows 사용자가 SMB를 통해 UNIX 사용 권한이 있는 볼륨에 액세스하려고 하면 Cloud Volumes Service는 검색을 수행하여 "joe"라는 해당 UNIX 사용자를 찾습니다. 이 파일이 있으면 Windows 사용자 Joe로 SMB 공유에 기록되는 파일이 NFS 클라이언트의 UNIX 사용자 Joe로 나타납니다.

또는 UNIX 사용자인 "Joe"가 Windows 사용 권한이 있는 Cloud Volumes Service 볼륨에 대한 액세스를 시도할 경우 UNIX 사용자는 유효한 Windows 사용자에게 매핑할 수 있어야 합니다. 그렇지 않으면 볼륨에 대한 액세스가 거부됩니다.

현재 LDAP를 사용하는 외부 UNIX ID 관리에는 Active Directory만 지원됩니다. 이 서비스에 대한 액세스 구성에 대한 자세한 내용은 을 참조하십시오 "AD 연결을 생성하는 중입니다".

권한 모델

이중 프로토콜 설정을 사용하는 경우 Cloud Volumes Service는 볼륨에 대한 보안 스타일을 사용하여 ACL 유형을 결정합니다. 이러한 보안 스타일은 지정된 NAS 프로토콜을 기반으로 설정되거나, 이중 프로토콜의 경우 Cloud Volumes Service 볼륨 생성 시 선택하는 것입니다.

- NFS만 사용하는 경우 Cloud Volumes Service 볼륨은 UNIX 사용 권한을 사용합니다.
- SMB만 사용하는 경우 Cloud Volumes Service 볼륨은 NTFS 권한을 사용합니다.

이중 프로토콜 볼륨을 생성하는 경우 볼륨 생성 시 ACL 스타일을 선택할 수 있습니다. 이 결정은 원하는 권한 관리를 기반으로 해야 합니다. 사용자가 Windows/SMB 클라이언트의 권한을 관리하는 경우 NTFS 를 선택합니다. 사용자가 NFS 클라이언트 및 chmod/chown을 사용하려는 경우 UNIX 보안 스타일을 사용합니다.

Active Directory 연결을 생성할 때의 고려 사항

Cloud Volumes Service를 사용하면 Cloud Volumes Service 인스턴스를 외부 Active Directory 서버에 연결하여 SMB 및 UNIX 사용자 모두의 ID 관리를 수행할 수 있습니다. Cloud Volumes Service에서 SMB를 사용하려면 Active Directory 연결을 생성해야 합니다.

이 구성은 보안을 고려해야 하는 몇 가지 옵션을 제공합니다. 외부 Active Directory 서버는 온-프레미스 인스턴스 또는 클라우드 네이티브 서버가 될 수 있습니다. 온-프레미스 Active Directory 서버를 사용하는 경우, 도메인을 외부 네트워크(예: DMZ 또는 외부 IP 주소)에 노출하지 마십시오. 대신 을 사용하여 사내 네트워크에 대한 보안 전용 터널 또는 VPN, 단방향 포리스트 트러스트 또는 전용 네트워크 연결을 사용합니다 "개인 Google 액세스". 에 대한 자세한 내용은 Google Cloud 설명서를 참조하십시오 "Google Cloud에서 Active Directory를 사용하는 모범 사례".

> CVS-SW를 사용하려면 Active Directory 서버가 동일한 지역에 있어야 합니다. CVS-SW에서 다른 지역으로 DC 연결을 시도하면 시도가 실패합니다. CVS-SW를 사용할 때는 Active Directory DC를 포함하는 Active Directory 사이트를 생성한 다음 Cloud Volumes Service에서 사이트를 지정하여 교차 지역 DC 연결 시도를 방지해야 합니다.

Active Directory 자격 증명

NFS용 SMB 또는 LDAP가 활성화된 경우 Cloud Volumes Service는 Active Directory 컨트롤러와 상호 작용하여 인증에 사용할 컴퓨터 계정 개체를 생성합니다. 이는 Windows SMB 클라이언트가 도메인에 가입하는 방식과 다르지 않으며 Active Directory의 OU(조직 구성 단위)에 동일한 액세스 권한이 필요합니다.

대부분의 경우 보안 그룹은 Cloud Volumes Service와 같은 외부 서버에서 Windows 관리자 계정 사용을 허용하지 않습니다. 경우에 따라 Windows 관리자 사용자는 보안 모범 사례로 완전히 비활성화됩니다.

SMB 시스템 계정을 생성하는 데 필요한 권한입니다

Cloud Volumes Service 컴퓨터 개체를 Active Directory에 추가하려면 도메인에 대한 관리 권한이 있거나 있는 계정입니다 "컴퓨터 계정 객체를 생성 및 수정하는 위임된 권한" 지정된 OU에 대한 필수 구성 요소입니다. Active Directory의 제어 위임 마법사를 사용하여 다음과 같은 액세스 권한이 있는 컴퓨터 개체를 생성/삭제할 수 있는 사용자 지정 작업을 만들어 이 작업을 수행할 수 있습니다.

- 읽기/쓰기
- 모든 자식 개체를 생성/삭제합니다
- 모든 속성 읽기/쓰기

- 암호 변경/재설정

이렇게 하면 정의된 사용자에 대한 보안 ACL이 Active Directory의 OU에 자동으로 추가되고 Active Directory 환경에 대한 액세스가 최소화됩니다. 사용자가 위임된 후에는 이 창에서 해당 사용자 이름과 암호를 Active Directory 자격 증명으로 제공할 수 있습니다.

> Active Directory 도메인에 전달되는 사용자 이름과 암호는 컴퓨터 계정 개체 쿼리 및 생성 중에 Kerberos 암호화를 사용하여 보안을 강화합니다.

Active Directory 연결 세부 정보입니다

를 클릭합니다 "Active Directory 연결 세부 정보" 다음과 같은 컴퓨터 계정 배치에 대한 특정 Active Directory 스키마 정보를 관리자에게 제공하는 필드를 제공합니다.

- * Active Directory 연결 유형. * Cloud Volumes Service 또는 CVS 성능 서비스 유형의 볼륨에 대해 영역의 Active Directory 연결이 사용되는지 여부를 지정하는 데 사용됩니다. 기존 연결에서 이 설정을 잘못 설정하면 사용하거나 편집할 때 제대로 작동하지 않을 수 있습니다.
- * 도메인. * Active Directory 도메인 이름입니다.
- * 사이트. * 보안 및 성능을 위해 Active Directory 서버를 특정 사이트로 제한합니다 "고려 사항". Cloud Volumes Service는 현재 Cloud Volumes Service 인스턴스가 아닌 다른 영역에 있는 Active Directory 서버에 대한 Active Directory 인증 요청을 허용하지 않으므로 여러 Active Directory 서버가 여러 지역에 걸쳐 있는 경우 이 작업이 필요합니다. 예를 들어, Active Directory 도메인 컨트롤러는 CVS-Performance만 지원하는 영역에 있지만 CVS-SW 인스턴스에서 SMB 공유를 원할 수 있습니다.
- DNS 서버 * 이름 조회에 사용할 DNS 서버.
- NetBIOS 이름(선택 사항).* 필요한 경우 서버의 NetBIOS 이름입니다. 이 기능은 Active Directory 연결을 사용하여 새 컴퓨터 계정을 만들 때 사용됩니다. 예를 들어 NetBIOS 이름이 CVS-East로 설정된 경우 컴퓨터 계정 이름은 CVS-East-{1234}가 됩니다. 섹션을 참조하십시오 "Active Directory에 Cloud Volumes Service가 표시되는 방식" 를 참조하십시오.
- * OU(조직 단위) * 컴퓨터 계정을 만들 특정 OU. 이 기능은 컴퓨터 계정에 대해 특정 OU에 제어를 위임하는 경우에 유용합니다.
- * AES 암호화. * AD 인증에 AES 암호화 사용 확인란을 선택하거나 선택 취소할 수도 있습니다. Active Directory 인증에 AES 암호화를 사용하면 사용자 및 그룹 조회 중에 Cloud Volumes Service에서 Active Directory로 통신하는 데 추가적인 보안을 제공할 수 있습니다. 이 옵션을 활성화하기 전에 도메인 관리자에게 문의하여 Active Directory 도메인 컨트롤러가 AES 인증을 지원하는지 확인하십시오.

> 기본적으로 대부분의 Windows 서버는 약한 암호(예: DES 또는 RC4-HMAC)를 비활성화하지 않지만 약한 암호를 비활성화하도록 선택하는 경우 Cloud Volumes Service Active Directory 연결이 AES를 사용하도록 구성되었는지 확인합니다. 그렇지 않으면 인증 실패가 발생합니다. AES 암호화를 사용하도록 설정하면 약한 암호가 비활성화되지 않고 대신 Cloud Volumes Service SMB 시스템 계정에 AES 암호화에 대한 지원이 추가됩니다.

Kerberos 영역 세부 정보

이 옵션은 SMB 서버에는 적용되지 않습니다. 대신, Cloud Volumes Service 시스템에 NFS Kerberos를 구성할 때 사용됩니다. 이러한 세부 정보가 채워지면 NFS Kerberos 영역이 구성되고(Linux의 krb5.conf 파일과 유사), Active Directory 연결이 NFS Kerberos 메일 센터(KDC) 역할을 하므로 Cloud Volumes Service 볼륨 생성에 NFS Kerberos가 지정될 때 사용됩니다.

Windows 이외의 KDC는 현재 Cloud Volumes Service에서 사용할 수 없습니다.

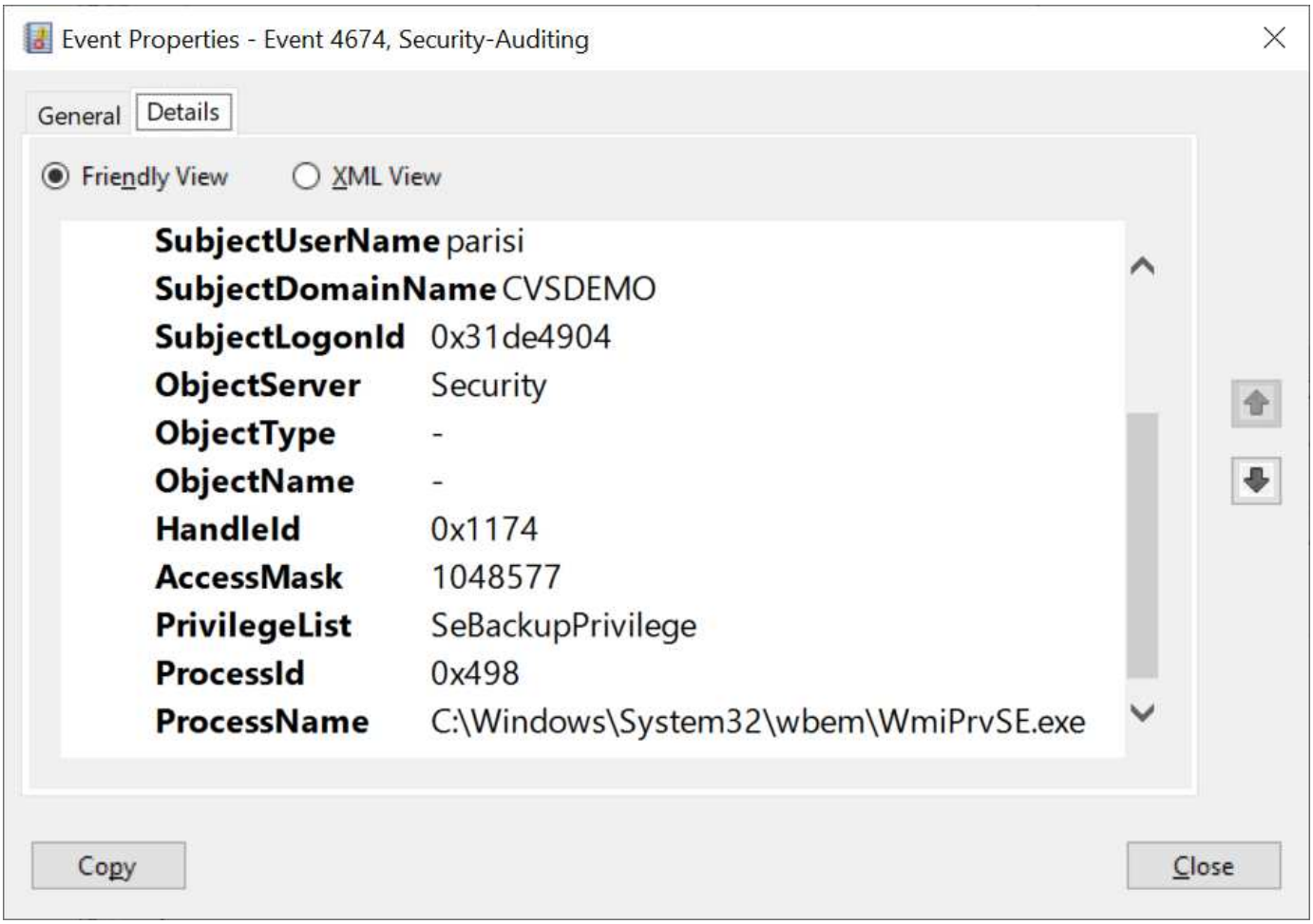
지역

영역을 사용하면 Active Directory 연결이 있는 위치를 지정할 수 있습니다. 이 영역은 Cloud Volumes Service 볼륨과 동일한 영역이어야 합니다.

- * LDAP를 사용하는 로컬 NFS 사용자 * 이 섹션에는 LDAP를 사용하는 로컬 NFS 사용자를 허용하는 옵션도 있습니다. UNIX 사용자 그룹 구성원 지원을 NFS(확장 그룹)의 16개 그룹 제한 이상으로 확장하려면 이 옵션을 선택하지 않아야 합니다. 그러나 확장된 그룹을 사용하려면 UNIX ID에 대해 구성된 LDAP 서버가 필요합니다. LDAP 서버가 없는 경우 이 옵션을 선택되지 않은 상태로 둡니다. LDAP 서버가 있고 로컬 UNIX 사용자(예: 루트)도 사용하려면 이 옵션을 선택합니다.

백업 사용자

이 옵션을 사용하면 Cloud Volumes Service 볼륨에 대한 백업 권한이 있는 Windows 사용자를 지정할 수 있습니다. NAS 볼륨의 데이터를 올바르게 백업 및 복원하려면 일부 애플리케이션에 백업 권한(SeBackupPrivilege)이 필요합니다. 이 사용자는 볼륨의 데이터에 대한 높은 수준의 액세스 권한을 가지고 있으므로 고려해야 합니다 "해당 사용자 액세스에 대한 감사를 설정합니다". 활성화된 감사 이벤트는 이벤트 뷰어 > Windows 로그 > 보안에 표시됩니다.



보안 권한 사용자

이 옵션을 사용하면 Cloud Volumes Service 볼륨에 대한 보안 수정 권한이 있는 Windows 사용자를 지정할 수

있습니다. 일부 응용 프로그램에는 보안 권한(SeSecurityPrivilege)이 필요합니다 ("SQL Server와 같은")를 클릭하여 설치 중에 권한을 적절하게 설정합니다. 이 권한은 보안 로그를 관리하는 데 필요합니다. 이 권한은 SeBackupPrivilege 권한만큼 강력하지는 않지만 NetApp이 권장합니다 "사용자의 사용자 액세스 감사" 필요한 경우 이 권한 수준을 사용합니다.

자세한 내용은 을 참조하십시오 "새 로그온에 할당된 특수 권한".

Active Directory에 Cloud Volumes Service가 표시되는 방식

Cloud Volumes Service는 Active Directory에 일반 컴퓨터 계정 개체로 표시됩니다. 명명 규칙은 다음과 같습니다.

- CIFS/SMB 및 NFS Kerberos는 별도의 시스템 계정 객체를 생성합니다.
- LDAP가 설정된 NFS는 Active Directory에서 Kerberos LDAP 바인드를 위한 컴퓨터 계정을 생성합니다.
- LDAP가 있는 이중 프로토콜 볼륨은 LDAP 및 SMB의 CIFS/SMB 시스템 계정을 공유합니다.
- CIFS/SMB 시스템 계정은 시스템 계정에 대해 이름-1234(10자 이름에 하이픈이 추가된 4자리 임의 ID)의 명명 규칙을 사용합니다. Active Directory 연결에서 NetBIOS 이름 설정을 사용하여 이름을 정의할 수 있습니다(“ 절 참조)Active Directory 연결 세부 정보입니다").
- NFS Kerberos에서는 nfs-name-1234를 명명 규칙(최대 15자)으로 사용합니다. 15자 이상을 사용하는 경우 이름은 nfs-duncated-name-1234입니다.
- NFS 전용 CVS - LDAP가 설정된 성능 인스턴스는 CIFS/SMB 인스턴스와 동일한 명명 규칙을 사용하여 LDAP 서버에 바인딩하기 위한 SMB 시스템 계정을 생성합니다.
- SMB 컴퓨터 계정이 생성되면 숨겨진 기본 관리자 공유가 생성됩니다(섹션 참조) ""“숨겨진 기본 공유”")도 생성되지만(c$, admin$, ipc$) 해당 공유는 할당된 ACL이 없으며 액세스할 수 없습니다.
- 컴퓨터 계정 개체는 기본적으로 CN=Computers에 배치되지만 필요한 경우 다른 OU를 지정할 수 있습니다. 자세한 내용은 " 단원을 참조하십시오SMB 시스템 계정을 생성하는 데 필요한 권한입니다"Cloud Volumes Service에 대한 컴퓨터 계정 개체를 추가/제거하는 데 필요한 액세스 권한에 대한 정보를 제공합니다.

Cloud Volumes Service가 Active Directory에 SMB 컴퓨터 계정을 추가하면 다음 필드가 채워집니다.

- CN(지정된 SMB 서버 이름 포함)
- dNSHostName(SMBserver.domain.com 포함)
- msDS-SupportedEncryptionTypes (AES 암호화가 활성화되지 않은 경우 DES_CBC_MD5, RC4_HMAC_MD5 허용; AES 암호화가 활성화된 경우 DES_CBC_MD5, RC4_HMAC_MD5, AES128_CTS_HMAC_SHA1_96, AES256_CTS_HMAC_SHA1_96은 SMB용 시스템 계정과 티켓 교환에 허용됨)
- 이름(SMB 서버 이름 포함)
- sAMAccountName(SMBserver$ 사용)
- servicePrincipalName(호스트 /smbserver.domain.com 및 Kerberos에 대한 호스트/smbserver SPN 포함)

컴퓨터 계정에서 약한 Kerberos 암호화 유형(enctype)을 비활성화하려면 컴퓨터 계정의 MSDS-SupportedEncryptionTypes 값을 다음 표의 값 중 하나로 변경하여 AES만 허용할 수 있습니다.

MSDS - SupportedEncryptionTypes 값입니다	**Enctype**이 활성화되었습니다
2	DES_CBC_MD5
4	RC4_HMAC

MSDS - SupportedEncryptionTypes 값입니다	**Enctype**이 활성화되었습니다
8	AES128_CTS_HMAC_SHA1_96만 해당
16	AES256_CTS_HMAC_SHA1_96만 해당
24	AES128_CTS_HMAC_SHA1_96 및 AES256_CTS_HMAC_SHA1_96
30	DES_CBC_MD5, RC4_HMAC, AES128_CTS_HMAC_SHA1_96 및 AES256_CTS_HMAC_SHA1_96

SMB 시스템 계정에 대해 AES 암호화를 활성화하려면 Active Directory 연결을 생성할 때 AD 인증에 AES 암호화 사용을 클릭합니다.

NFS Kerberos에서 AES 암호화를 사용하도록 설정하려면 "Cloud Volumes Service 설명서를 참조하십시오".

기타 **NAS** 인프라스트럭처 서비스 종속성(**KDC, LDAP** 및 **DNS**)

NAS 공유에 Cloud Volumes Service를 사용하는 경우 적절한 기능을 위해 외부 종속성이 필요할 수 있습니다. 이러한 종속성은 특정 상황에서 적용됩니다. 다음 표에는 다양한 구성 옵션과 종속 항목이 필요한 항목이 나와 있습니다.

구성	종속성이 필요합니다
NFSv3만 해당	없음
NFSv3 Kerberos만 해당	Windows Active Directory: * KDC * DNS * LDAP
NFSv4.1만 해당	클라이언트 ID 매핑 구성(/etc/idmap.conf)
NFSv4.1 Kerberos만 해당	• 클라이언트 ID 매핑 구성(/etc/idmap.conf) • Windows Active Directory: KDC DNS LDAP
SMB만 해당	Active Directory: * KDC * DNS
멀티프로토콜 NAS(NFS 및 SMB)	• 클라이언트 ID 매핑 구성(NFSv4.1 전용; /etc/idmap.conf) • Windows Active Directory: KDC DNS LDAP

시스템 계정 개체에 대한 **Kerberos** 키 탭 회전/암호 재설정

SMB 시스템 계정의 경우 Cloud Volumes Service는 SMB 시스템 계정에 대한 주기적인 암호 재설정을 예약합니다. 이러한 암호 재설정은 Kerberos 암호화를 사용하여 발생하며, 오후 11시부터 오전 1시 사이에 임의 시간에 매주 일요일 일정에 따라 작동합니다. 이러한 암호 재설정은 Kerberos 키 버전을 변경하고, Cloud Volumes Service 시스템에 저장된 키 탭을 회전하며, Cloud Volumes Service에서 실행되는 SMB 서버의 보안을 더욱 강화할 수 있도록 도와줍니다. 시스템 계정 암호는 무작위배정되며 관리자에게 알려져 있지 않습니다.

NFS Kerberos 시스템 계정의 경우 KDC와 새 키 탭이 생성/교환될 때만 암호 재설정이 적용됩니다. 현재 Cloud Volumes Service에서는 이 작업을 수행할 수 없습니다.

LDAP 및 Kerberos와 함께 사용할 네트워크 포트

LDAP 및 Kerberos를 사용하는 경우 이러한 서비스에서 사용 중인 네트워크 포트를 확인해야 합니다. 에서 Cloud Volumes Service에서 사용 중인 포트의 전체 목록을 찾을 수 있습니다 "보안 고려 사항에 대한 Cloud Volumes Service 문서".

LDAP를 지원합니다

Cloud Volumes Service는 LDAP 클라이언트 역할을 하며 UNIX ID에 대한 사용자 및 그룹 조회를 위해 표준 LDAP 검색 쿼리를 사용합니다. Cloud Volumes Service에서 제공하는 표준 기본 사용자 이외의 사용자 및 그룹을 사용하려면 LDAP가 필요합니다. NFS Kerberos를 사용자 보안 주체(예: user1@domain.com 사용할 계획이라면 LDAP도 필요합니다. 현재 Microsoft Active Directory를 사용하는 LDAP만 지원됩니다.

Active Directory를 UNIX LDAP 서버로 사용하려면 UNIX ID에 사용할 사용자 및 그룹에 필요한 UNIX 속성을 채워야 합니다. Cloud Volumes Service에서는 에 따라 특성을 쿼리하는 기본 LDAP 스키마 템플릿을 사용합니다 "RFC-2307-bis". 따라서 다음 표에서는 사용자 및 그룹에 채울 최소 필수 Active Directory 속성과 각 속성이 사용되는 특성을 보여 줍니다.

Active Directory에서 LDAP 속성을 설정하는 방법에 대한 자세한 내용은 을 참조하십시오 "이중 프로토콜 액세스 관리."

속성	기능
UID *	UNIX 사용자 이름을 지정합니다
uidNumber *	UNIX 사용자의 숫자 ID를 지정합니다
gidNumber *	UNIX 사용자의 기본 그룹 숫자 ID를 지정합니다
objectClass *	사용 중인 개체 유형을 지정합니다. Cloud Volumes Service에서는 "사용자"를 개체 클래스 목록에 포함해야 합니다(기본적으로 대부분의 Active Directory 배포에는 포함됨).
이름	계정에 대한 일반 정보(실제 이름, 전화 번호 등, gecos라고도 함)
unixUserPassword	NAS 인증을 위한 UNIX ID 조회에 사용되지 않으므로 설정할 필요가 없습니다. 이렇게 설정하면 구성된 unixUserPassword 값이 일반 텍스트로 설정됩니다.
unixHomeDirectory	사용자가 Linux 클라이언트에서 LDAP에 대해 인증할 때 UNIX 홈 디렉토리의 경로를 정의합니다. UNIX 홈 디렉토리 기능에 LDAP를 사용하려면 이 옵션을 설정합니다.
LoginShell입니다	사용자가 LDAP에 대해 인증할 때 Linux 클라이언트의 bash/profile 셸에 대한 경로를 정의합니다.

- 는 Cloud Volumes Service의 적절한 기능을 위해 특성이 필요함을 나타냅니다. 나머지 속성은 클라이언트 측 전용입니다.

속성	기능
CN *	UNIX 그룹 이름을 지정합니다. LDAP에 Active Directory를 사용하는 경우 개체를 처음 만들 때 설정되지만 나중에 변경할 수 있습니다. 이 이름은 다른 개체와 같을 수 없습니다. 예를 들어, user1이라는 UNIX 사용자가 Linux 클라이언트의 user1이라는 그룹에 속해 있는 경우 Windows에서는 cn 특성이 같은 두 개체를 허용하지 않습니다. 이 문제를 해결하려면 Windows 사용자의 이름을 고유한 이름(예: user1-UNIX)으로 바꿉니다. Cloud Volumes Service의 LDAP는 UNIX 사용자 이름에 uid 속성을 사용합니다.
gidNumber *	UNIX 그룹 숫자 ID를 지정합니다.
objectClass *	사용 중인 개체 유형을 지정합니다. Cloud Volumes Service에서는 개체 클래스 목록에 그룹을 포함해야 합니다. 이 특성은 기본적으로 대부분의 Active Directory 배포에 포함됩니다.
memberUid	UNIX 그룹의 구성원인 UNIX 사용자를 지정합니다. Cloud Volumes Service에서 Active Directory LDAP를 사용할 경우 이 필드는 필요하지 않습니다. Cloud Volumes Service LDAP 스키마는 그룹 구성원 자격에 구성원 필드를 사용합니다.
구성원 *	그룹 구성원 자격/보조 UNIX 그룹에 필요합니다. 이 필드는 Windows 그룹에 Windows 사용자를 추가하여 채워집니다. 그러나 Windows 그룹에 채워진 UNIX 특성이 없는 경우 UNIX 사용자의 그룹 구성원 목록에는 포함되지 않습니다. NFS에서 사용할 수 있어야 하는 모든 그룹은 이 표에 나열된 필수 UNIX 그룹 속성을 채워야 합니다.

- 는 Cloud Volumes Service의 적절한 기능을 위해 특성이 필요함을 나타냅니다. 나머지 속성은 클라이언트 측 전용입니다.

LDAP 바인딩 정보

LDAP에서 사용자를 쿼리하려면 Cloud Volumes Service가 LDAP 서비스에 바인딩(로그인)해야 합니다. 이 로그인에는 읽기 전용 권한이 있으며 디렉토리 조회를 위해 LDAP UNIX 속성을 쿼리하는 데 사용됩니다. 현재 LDAP 바인딩은 SMB 컴퓨터 계정을 통해서만 가능합니다.

'CVS 성능' 인스턴스에만 LDAP를 사용하도록 설정하고 NFSv3, NFSv4.1 또는 이중 프로토콜 볼륨에는 LDAP를 사용할 수 있습니다. LDAP 지원 볼륨을 성공적으로 배포하려면 Cloud Volumes Service 볼륨과 동일한 영역에 Active Directory 연결을 설정해야 합니다.

LDAP가 활성화된 경우 특정 시나리오에서 다음이 발생합니다.

- Cloud Volumes Service 프로젝트에 NFSv3이나 NFSv4.1만 사용되는 경우 Active Directory 도메인 컨트롤러에서 새 컴퓨터 계정이 생성되고 Cloud Volumes Service의 LDAP 클라이언트는 시스템 계정 자격 증명을 사용하여 Active Directory에 바인딩됩니다. NFS 볼륨 및 숨겨진 기본 관리 공유에 대해 SMB 공유가 생성되지 않습니다(섹션 참조) ""숨겨진 기본 공유"")의 공유 ACL이 제거되었습니다.
- Cloud Volumes Service 프로젝트에 이중 프로토콜 볼륨을 사용하는 경우 SMB 액세스용으로 생성된 단일 컴퓨터 계정만 Cloud Volumes Service의 LDAP 클라이언트를 Active Directory에 바인딩하는 데 사용됩니다. 추가 컴퓨터 계정이 생성되지 않습니다.

- 전용 SMB 볼륨이 별도로 생성된 경우(LDAP가 설정된 NFS 볼륨 이전 또는 이후에) LDAP 바인딩의 컴퓨터 계정이 SMB 시스템 계정과 공유됩니다.
- NFS Kerberos도 사용하도록 설정된 경우 두 개의 시스템 계정이 생성됩니다. 하나는 SMB 공유 및/또는 LDAP 바인드이고 다른 하나는 NFS Kerberos 인증입니다.

LDAP 쿼리입니다

LDAP 바인딩은 암호화되지만 일반 LDAP 포트 389를 사용하여 LDAP 쿼리가 일반 텍스트로 회선을 통해 전달됩니다. 이 잘 알려진 포트는 현재 Cloud Volumes Service에서 변경할 수 없습니다. 따라서 네트워크에서 패킷 스니핑에 액세스할 수 있는 사용자는 사용자 및 그룹 이름, 숫자 ID 및 그룹 구성원 자격을 볼 수 있습니다.

그러나 Google Cloud VM은 다른 VM의 유니캐스트 트래픽을 스니프할 수 없습니다. LDAP 트래픽에 활성 중인 VM(즉, 바인딩 가능)만 LDAP 서버의 트래픽을 볼 수 있습니다. Cloud Volumes Service의 패킷 스니핑에 대한 자세한 내용은 섹션을 참조하십시오 ""패킷 감지/추적 고려 사항""

LDAP 클라이언트 구성 기본값

Cloud Volumes Service 인스턴스에서 LDAP가 활성화되면 기본적으로 특정 구성 세부 정보를 사용하여 LDAP 클라이언트 구성이 생성됩니다. 경우에 따라 옵션이 Cloud Volumes Service(지원되지 않음)에 적용되지 않거나 구성할 수 없습니다.

LDAP 클라이언트 옵션입니다	기능	기본값	변경할 수 있습니까**?**
LDAP 서버 목록	쿼리에 사용할 LDAP 서버 이름 또는 IP 주소를 설정합니다. Cloud Volumes Service에는 사용되지 않습니다. 대신 Active Directory 도메인을 사용하여 LDAP 서버를 정의합니다.	설정되지 않았습니다	아니요
Active Directory 도메인	LDAP 쿼리에 사용할 Active Directory 도메인을 설정합니다. Cloud Volumes Service는 DNS의 LDAP에 대한 SRV 레코드를 활용하여 도메인에서 LDAP 서버를 찾습니다.	Active Directory 연결에 지정된 Active Directory 도메인으로 설정합니다.	아니요
기본 Active Directory 서버	LDAP에 사용할 기본 Active Directory 서버를 설정합니다. Cloud Volumes Service에서 지원되지 않습니다. 대신 Active Directory 사이트를 사용하여 LDAP 서버 선택을 제어할 수 있습니다.	설정되지 않았습니다.	아니요

LDAP 클라이언트 옵션입니다	기능	기본값	변경할 수 있습니까**?**
SMB 서버 자격 증명을 사용하여 바인딩합니다	SMB 시스템 계정을 사용하여 LDAP에 바인딩합니다. 현재 Cloud Volumes Service에서 지원되는 유일한 LDAP 바인딩 방법입니다.	참	아니요
스키마 템플릿	LDAP 쿼리에 사용되는 스키마 템플릿입니다.	MS-AD-BIS	아니요
LDAP 서버 포트입니다	LDAP 쿼리에 사용되는 포트 번호입니다. Cloud Volumes Service는 현재 표준 LDAP 포트 389만 사용합니다. LDAPS/포트 636은 현재 지원되지 않습니다.	389	아니요
LDAPS가 활성화되어 있습니다	SSL(Secure Sockets Layer)을 통한 LDAP가 쿼리 및 바인딩에 사용되는지 여부를 제어합니다. 현재 Cloud Volumes Service에서 지원되지 않습니다.	거짓	아니요
쿼리 시간 제한(초)	쿼리 시간이 초과되었습니다. 쿼리가 지정된 값보다 오래 걸면 쿼리가 실패합니다.	3	아니요
최소 바인딩 인증 레벨	지원되는 최소 바인딩 레벨입니다. Cloud Volumes Service는 LDAP 바인딩에 컴퓨터 계정을 사용하고 Active Directory는 기본적으로 익명 바인딩을 지원하지 않으므로 이 옵션은 보안을 위해 사용되지 않습니다.	익명	아니요
DN 바인딩	단순 바인딩이 사용될 때 바인딩에 사용되는 사용자/고유 이름(DN)입니다. Cloud Volumes Service는 LDAP 바인딩에 시스템 계정을 사용하며 현재 단순 바인딩 인증을 지원하지 않습니다.	설정되지 않았습니다	아니요

LDAP 클라이언트 옵션입니다	기능	기본값	변경할 수 있습니까**?**
기본 DN	LDAP 검색에 사용되는 기본 DN입니다.	Windows 도메인이 DN 형식(즉, DC=domain, DC=local)으로 Active Directory 연결에 사용됩니다.	아니요
기본 검색 범위	기본 DN 검색에 대한 검색 범위입니다. 값은 기본, onelevel 또는 하위 트리를 포함할 수 있습니다. Cloud Volumes Service는 하위 트리 검색만 지원합니다.	하위 트리	아니요
사용자 DN	사용자가 LDAP 쿼리를 검색하는 DN을 정의합니다. 현재 Cloud Volumes Service에서는 지원되지 않으므로 모든 사용자 검색은 기본 DN에서 시작됩니다.	설정되지 않았습니다	아니요
사용자 검색 범위	사용자 DN 검색에 대한 검색 범위입니다. 값은 기본, onelevel 또는 하위 트리를 포함할 수 있습니다. Cloud Volumes Service는 사용자 검색 범위 설정을 지원하지 않습니다.	하위 트리	아니요
그룹 DN	그룹 검색이 LDAP 쿼리를 시작하는 DN을 정의합니다. 현재 Cloud Volumes Service에 대해 지원되지 않으므로 모든 그룹 검색이 기본 DN에서 시작됩니다.	설정되지 않았습니다	아니요
그룹 검색 범위	그룹 DN 검색에 대한 검색 범위입니다. 값은 기본, onelevel 또는 하위 트리를 포함할 수 있습니다. Cloud Volumes Service는 그룹 검색 범위 설정을 지원하지 않습니다.	하위 트리	아니요
넷그룹 DN입니다	넷그룹이 LDAP 쿼리를 검색하는 DN을 정의합니다. 현재 Cloud Volumes Service에 대해 지원되지 않으므로 모든 넷그룹 검색은 기본 DN에서 시작됩니다.	설정되지 않았습니다	아니요

LDAP 클라이언트 옵션입니다	기능	기본값	변경할 수 있습니까**?**
넷그룹 검색 범위입니다	넷그룹 DN 검색에 대한 검색 범위입니다. 값은 기본, onelevel 또는 하위 트리를 포함할 수 있습니다. Cloud Volumes Service에서는 넷그룹 검색 범위 설정을 지원하지 않습니다.	하위 트리	아니요
LDAP를 통해 start_tls를 사용합니다	포트 389를 통한 인증서 기반 LDAP 연결에 Start TLS를 활용합니다. 현재 Cloud Volumes Service에서 지원되지 않습니다.	거짓	아니요
Netgroup-by-host 조회를 설정합니다	넷그룹을 확장하여 모든 구성원을 나열하는 대신 호스트 이름별로 넷그룹 조회를 설정합니다. 현재 Cloud Volumes Service에서 지원되지 않습니다.	거짓	아니요
Netgroup-by-host DN입니다	넷그룹별 검색이 LDAP 쿼리를 시작하는 DN을 정의합니다. Cloud Volumes Service에 대해 현재 호스트별 넷그룹이 지원되지 않습니다.	설정되지 않았습니다	아니요
Netgroup-by-host 검색 범위입니다	Netgroup-by-host DN 검색에 대한 검색 범위입니다. 값은 기본, onelevel 또는 하위 트리를 포함할 수 있습니다. Cloud Volumes Service에 대해 현재 호스트별 넷그룹이 지원되지 않습니다.	하위 트리	아니요
클라이언트 세션 보안	LDAP에서 사용하는 세션 보안 수준(서명, 봉인 또는 없음)을 정의합니다. LDAP 서명은 Active Directory에서 요청하는 경우 CVS - 성능에서 지원됩니다. CVS-SW는 LDAP 서명을 지원하지 않습니다. 두 서비스 유형 모두에서 봉인은 현재 지원되지 않습니다.	없음	아니요

LDAP 클라이언트 옵션입니다	기능	기본값	변경할 수 있습니까**?**
LDAP 조회 추적	여러 LDAP 서버를 사용하는 경우 조회 추적을 통해 첫 번째 서버에서 항목을 찾을 수 없을 때 클라이언트가 목록의 다른 LDAP 서버를 참조할 수 있습니다. 현재 Cloud Volumes Service에서는 지원되지 않습니다.	거짓	아니요
그룹 구성원 필터	LDAP 서버에서 그룹 구성원을 검색할 때 사용할 사용자 지정 LDAP 검색 필터를 제공합니다. 현재 Cloud Volumes Service에서는 지원되지 않습니다.	설정되지 않았습니다	아니요

비대칭 이름 매핑에 **LDAP**를 사용합니다

Cloud Volumes Service는 기본적으로 특별한 구성 없이 양방향으로 동일한 사용자 이름을 가진 Windows 사용자와 UNIX 사용자를 매핑합니다. Cloud Volumes Service가 유효한 UNIX 사용자(LDAP 사용)를 찾을 수 있는 한 1:1 이름 매핑이 발생합니다. 예를 들어, 윈도우 사용자인 'johnsmith'를 사용하는 경우, Cloud Volumes Service가 LDAP에서 johnsmith라는 UNIX 사용자를 찾을 수 있다면, 해당 사용자에 대한 이름 매핑이 성공하면, johnsmith로 생성된 모든 파일/폴더에 올바른 사용자 소유권이 표시됩니다. 또한 사용 중인 NAS 프로토콜에 관계없이 "johnsmith"에 영향을 주는 모든 ACL이 적용됩니다. 이것을 대칭 이름 매핑이라고 합니다.

비대칭 이름 매핑은 Windows 사용자 및 UNIX 사용자 ID가 일치하지 않는 경우를 나타냅니다. 예를 들어, 윈도우 사용자인 주스미스(jsmith)가 유닉스의 ID를 갖고 있다면, Cloud Volumes Service는 그 변이에 대한 정보를 얻을 수 있는 방법이 필요합니다. Cloud Volumes Service는 현재 정적 이름 매핑 규칙 생성을 지원하지 않으므로, LDAP를 사용하여 Windows 및 UNIX ID 모두의 사용자 ID를 조회하여 파일 및 폴더의 올바른 소유권과 예상되는 권한을 확인해야 합니다.

기본적으로 Cloud Volumes Service는 이름 맵 데이터베이스 인스턴스의 ns-switch에 LDAP를 포함하므로 비대칭 이름에 LDAP를 사용하여 이름 매핑 기능을 제공하려면 Cloud Volumes Service의 모양을 반영하기 위해 일부 사용자/그룹 속성만 수정하면 됩니다.

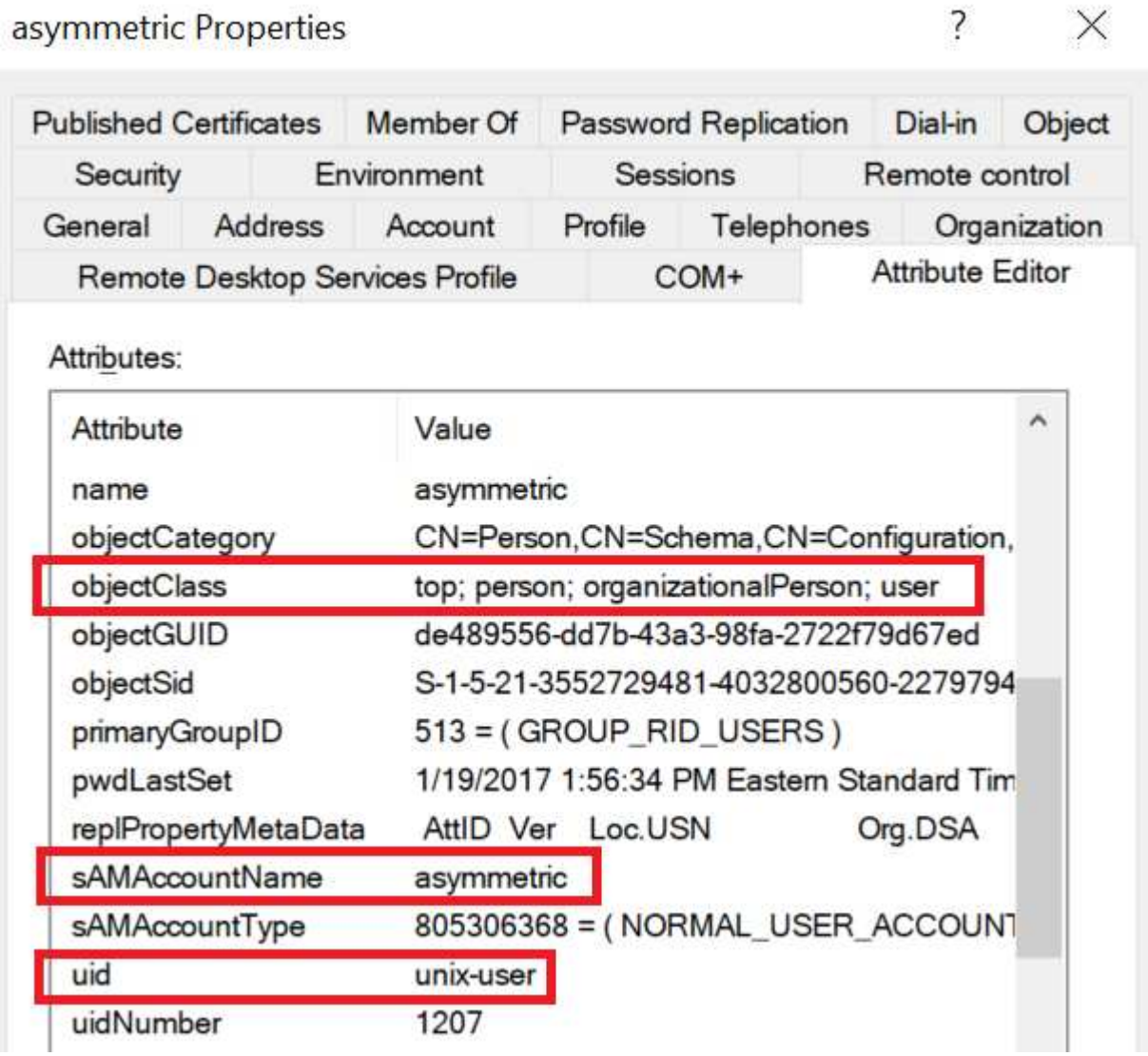
다음 표에서는 비대칭 이름 매핑 기능을 위해 LDAP에 채워야 하는 특성을 보여 줍니다. 대부분의 경우 Active Directory는 이미 이 작업을 수행하도록 구성되어 있습니다.

Cloud Volumes Service 특성입니다	기능	**Cloud Volumes Service**에서 이름 매핑에 사용하는 값입니다
Windows에서 UNIX로의 객체 클래스	사용 중인 개체의 형식을 지정합니다. (즉, 사용자, 그룹, posixAccount 등)	사용자를 포함해야 합니다(필요한 경우 다른 값을 여러 개 포함할 수 있음).
Windows에서 UNIX로의 속성	그러면 생성 시 Windows 사용자 이름이 정의됩니다. Cloud Volumes Service는 Windows에서 UNIX로의 조회에 이 기능을 사용합니다.	여기에서 변경할 필요가 없습니다. sAMAccountName은 Windows 로그인 이름과 동일합니다.
UID	UNIX 사용자 이름을 정의합니다.	원하는 UNIX 사용자 이름입니다.

Cloud Volumes Service는 현재 LDAP 조회에서 도메인 접두사를 사용하지 않으므로 LDAP 이름 맵 조회에서 여러 도메인 LDAP 환경이 제대로 작동하지 않습니다.

다음 예에서는 Windows 이름 "비대칭", UNIX 이름 "UNIX-user"를 가진 사용자와 SMB 및 NFS에서 파일을 쓸 때 나타나는 동작을 보여 줍니다.

다음 그림에서는 LDAP 특성이 Windows 서버에서 어떻게 표시되는지 보여 줍니다.



NFS 클라이언트에서 UNIX 이름을 쿼리할 수 있지만 Windows 이름은 쿼리할 수 없습니다.

```
# id unix-user
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
# id asymmetric
id: asymmetric: no such user
```

NFS에서 UNIX-USER로 파일을 쓸 때 NFS 클라이언트의 결과는 다음과 같습니다.

```
sh-4.2$ pwd
/mnt/home/ntfssh-4.2$ touch unix-user-file
sh-4.2$ ls -la | grep unix-user
-rwx------  1 unix-user sharedgroup     0 Feb 28 12:37 unix-user-nfs
sh-4.2$ id
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
```

Windows 클라이언트에서 파일 소유자가 올바른 Windows 사용자로 설정되어 있는지 확인할 수 있습니다.

```
PS C:\ > Get-Acl \\demo\home\ntfs\unix-user-nfs | select Owner
Owner
-----
NTAP\asymmetric
```

반대로, SMB 클라이언트에서 Windows 사용자 '비대칭'으로 생성된 파일은 다음 텍스트에서와 같이 적절한 UNIX 소유자를 표시합니다.

SMB:

```
PS Z:\ntfs> echo TEXT > asymmetric-user-smb.txt
```

NFS:

```
sh-4.2$ ls -la | grep asymmetric-user-smb.txt
-rwx------  1 unix-user         sharedgroup   14 Feb 28 12:43 asymmetric-
user-smb.txt
sh-4.2$ cat asymmetric-user-smb.txt
TEXT
```

LDAP 채널 바인딩

Windows Active Directory 도메인 컨트롤러의 취약점으로 인해 "Microsoft 보안 권고 ADV190023" DC에서 LDAP 바인드를 허용하는 방법을 변경합니다.

Cloud Volumes Service에 미치는 영향은 모든 LDAP 클라이언트와 동일합니다. Cloud Volumes Service는 현재 채널 바인딩을 지원하지 않습니다. Cloud Volumes Service는 협상을 통해 기본적으로 LDAP 서명을 지원하므로 LDAP 채널 바인딩은 문제가 되지 않습니다. 채널 바인딩이 설정된 LDAP에 바인딩하는 데 문제가 있는 경우 ADV190023의 개선 단계를 수행하여 Cloud Volumes Service에서 LDAP 바인딩이 성공하도록 허용합니다.

DNS

Active Directory와 Kerberos 모두 호스트 이름 대 IP/IP 대 호스트 이름 확인에 대한 DNS에 대한 종속성을 가집니다. DNS를 열려면 포트 53이 열려 있어야 합니다. Cloud Volumes Service는 DNS 레코드를 수정하지 않으며 현재 의 사용을 지원하지 않습니다 "다이나믹 DNS" 네트워크 인터페이스.

DNS 레코드를 업데이트할 수 있는 서버를 제한하도록 Active Directory DNS를 구성할 수 있습니다. 자세한 내용은 을 참조하십시오 "Windows DNS 보안".

Google 프로젝트 내의 리소스는 기본적으로 Active Directory DNS와 연결되지 않은 Google Cloud DNS를 사용합니다. 클라우드 DNS를 사용하는 클라이언트는 Cloud Volumes Service에서 반환하는 UNC 경로를 확인할 수 없습니다. Active Directory 도메인에 참가한 Windows 클라이언트는 Active Directory DNS를 사용하도록 구성되어 있으며 이러한 UNC 경로를 확인할 수 있습니다.

Active Directory에 클라이언트를 연결하려면 Active Directory DNS를 사용하도록 해당 DNS 구성을 구성해야 합니다. 필요에 따라 Active Directory DNS로 요청을 전달하도록 Cloud DNS를 구성할 수 있습니다. 을 참조하십시오 "클라이언트가 SMB NetBIOS 이름을 확인할 수 없는 이유는 무엇입니까?"를 참조하십시오.

Cloud Volumes Service는 현재 DNSSEC를 지원하지 않으며 DNS 쿼리는 일반 텍스트로 수행됩니다.

파일 액세스 감사

현재 Cloud Volumes Service에서 지원되지 않습니다.

안티바이러스 보호

클라이언트의 Cloud Volumes Service에서 NAS 공유에 대한 바이러스 백신 검사를 수행해야 합니다. 현재 Cloud Volumes Service와 통합된 기본 바이러스 백신이 없습니다.

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 라이센스와 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 라이센스도 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 라이센스를 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 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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